STOCKHOLMS UNIVERSITET

KUNGL TEKNISKA HÖGSKOLAN

Loggar som bevisning

Per Falk
Roger Lindblom

Institutionen för
Data- och systemvetenskap

Submitted to Stockholm University in partial fulfilment of the requirements for the degree of Master of Science in Computer and Systems Sciences

Masters' series
No. 05-04-DSV-SU
Februari 2005

Value of audit trails as evidence[1]

Per Falk & Roger Lindblom
Department of Computer and System Sciences
Stockholm University / Royal Institute of Technology
February 2005

Abstract

Within crime investigations about fraud, robbery, homicide etc. the evidence is usually questioned. However, this seems not be the case in computer crime where audit trail often is an important piece of evidence. On the contrary it seems like the evidence in this case is not questioned at all and that the analysis only come about from the audit trails. This mean that the organisations audit trail today is accepted without a trial of its consistency. In the interviews that have been made, with as well forensic as technical personnel, indicates that it within the legal authority exits a little knowledge about the principles of information technology and that the audit is fairly vulnerable for different types of manipulation. The objective for this thesis has therefore been to develop guiding principles that increase the possibility to appreciate an organisations audit trail before a legal trial. Thus we have a discussion about legal terms as well as the technology of information security. The interdisciplinary approach means that the target group involve both legal and technical personnel. One of the most important conclusions from the conducted interviews and analysis of topical court cases is that it do not seems to exits any case there some part have doubted the consistency of the audit trail. Neither the suspect, his/her defender or some other part seems to demand any more detailed investigation of what kind of technical and administrative solutions that are used at the generation of topical audit trails. However, the subject will likely be a problem in the future since questioning of the audit trail quality is expected. By looking into the problems today the legal authorities hopefully can be one step before the future. One way to meeting this future development is to use the writer's suggestion of extended audit trail documentation. The value as evidence will thereby increase and also involve the environment that the audits have been created within.

Keywords: IT-security, Audit trail, Accountability, Value as evidence, Information quality.

[1] This thesis corresponds to 20 weeks of full-time work for each of the authors

Loggar som bevisning[2]

Per Falk & Roger Lindblom
Institutionen för data- och systemvetenskap
Stockholms universitet / Kungliga Tekniska Högskolan
Februari 2005

Sammanfattning

I samband med brottsutredningar kring bedrägerier, rån, mord m.m. ifrågasätts vanligen på vilket sett aktuella bevis har tillkommit. Detta verkar dock inte vara fallet i samband med utredningar kring IT-relaterad brottslighet där olika typer av loggar ofta står för en viktig del av bevisföringen. Tvärtom verkar det som om loggar som bevis inte ifrågasätts och att analysen av dem endast sker utifrån loggutdraget. Detta innebär att organisationernas loggutdrag idag godtas som bevis utan att prövning skett av riktigheten. De intervjuer som har genomförts under arbetets gång med såväl juridisk som teknisk personal pekar även mot att det finns en hel del okunskap hos rättsvårdande instanser kring principerna för informationsteknologi samt att loggar i sig är förhållandevis sårbara för olika typer av manipulering. Målsättningen har därför varit att ta fram riktlinjer som ökar möjligheten för att kunna värdera en organisations loggutdrag inför en juridisk prövning. Således rör vi oss såväl kring juridiska begrepp som tekniken kring informationssäkerhet. Den tvärvetenskapliga ansatsen innebär att målgruppen för arbetet är både juridisk samt teknisk personal. En av de viktigaste slutsatserna som dragits av genomförda intervjuer samt analys av aktuella rättsfall är att det hittills inte verkar vara några fall där någon ifrågasatt loggutdragens riktighet. Varken den misstänkte, dennes försvarare eller någon av aktörerna hos de rättsvårdande instanserna verkar idag begära någon närmare granskning av vilka tekniska samt administrativa lösningar som brukas vid generering av aktuella loggar. Dock kommer området med största sannolikhet bli ett problem i framtiden i och med att ett ifrågasättande av kvaliteten hos anförda loggutdrag troligtvis är att vänta. Genom att idag se närmare på problemen kring loggning kan rättsväsendet förhoppningsvis ligga ett steg före den framtida utvecklingen. Ett sätt att möta denna framtid är att nyttja det förslag till utökade loggutdrag som författarna redovisar. Bevisvärdet av morgondagens loggutdrag kommer därmed att till stor del baseras på den miljö vari loggarna genererats.

Nyckelord: IT-säkerhet, Loggutdrag, Logganalys, Spårbarhet, Bevisvärde, Informationskvalitet.

[2] Uppsatsen motsvarar 20 poäng för vardera författare

Förord

Författarna vill med dessa rader rikta ett speciellt tack till handledaren Yngve Mondfeldt, som genom sitt stora engagemang och sin kunskap varit oss till stor hjälp. Under våra diskussioner kring loggutdrag som bevisbärande dokument har denne bidragit med viktiga synpunkter kring ämnet informationssäkerhet. Dessa diskussioner har väckt nya frågor hos författarna och på så sätt bidragit till möjligheten att uppnå uppsatsens problem, syfte och mål. Vi vill även rikta ett stort tack till Nils-Erik Pettersson vid TSA (Totalförsvarets Signalskyddssamordning) som under arbetet gång fungerat som ett viktigt ”bollplank”.

Per Falk och Roger Lindblom
Stockholm, februari 2005

Innehållsförteckning

1. Bakgrund

1.1 Inledning

Eftersom en av författarna till denna uppsats arbetar på Rikspolisstyrelsen har denne erfarenhet av att arbeta med logganalyser mot polisanställda som misstänks för att ha överträtt sina befogenheter vid nyttjande av polisiära tekniska informationssystem (ITS). I analysarbetet ingår bland annat att utreda och dokumentera den loggning som användaren genererat sedan denne gjort slagningar i olika polisiära informationssystem.

Samma författare har tidigare arbetat som brottsutredare med utredningar som i huvudsak bestått av våldsbrott som mord, våldtäkter och rån. I samband med dessa utredningar har det varit en regel, snarare än ett undantag, att den misstänkte och dennes försvarare ifrågasatt på vilket sätt en viss bevisning tagits fram, bevisningens värde och om bevisningen tagits fram på ett korrekt sätt. Detta ifrågasättande har inte sällan en utgångspunkt i det faktum att det från den misstänktes sida räcker med att så ett tvivel i åklagarens bevisning för att ett åtal skall kunna ogillas. När logganalyser har presenterats har det inte vid något tillfälle inträffat att någon ifrågasatte hur analysen gått till eller om det loggutdrag som analysen byggde på var korrekt, d.v.s. om loggen verkligen visade vad användaren gjort i systemet.

Vid samtal med åklagare, utredare och advokater, som i uppsatsen benämns som rättsvårdande instanser, ställde vi inledningsvis ett antal frågor med inriktning på deras inställning till loggutdraget som bevisning. Det framkom då att ingen av dem kunde erinra sig att man varken själv, eller vid något tillfälle hört talas om att någon anna betvivlat äktheten av ett loggutdrag. Om ingen part (målsäganden och åklagare eller den misstänkte och dennes försvarare) eller domstolen ifrågasätter loggutdragen som bevisning kommer de på ett eller annat sätt att tillmätas värdet av bevis. Detta sker antingen som en länk i en beviskedja eller som självständig skriftlig bevisning. På så sätt skiljer den sig loggutdragen inte från annan skriftlig bevisning.

Med ledning av de rättsvårdande instansernas begränsade insikt i loggutdragens betydelse som bevisning inför svenska domstolar är det berättigat att ställa sig frågan om organisationernas loggutdrag idag verkligen har ett sanningsinnehåll som gör att de ensamma kan utgöra enda underlaget för en logganalys. Om man svarar ja på den frågan innebär det ett antagande som bygger på det faktum att datorer och människor aldrig gör fel. Eftersom det knappast finns någon som håller med om detta antagande blir frånvaron av ifrågasättandet av loggutdragen än mer ologisk. Vi, författarna av denna uppsats, antar att orsaken till det okritiska förhållningssättet till loggutdragen är okunskap kring hur IT-relaterade informationssystem fungerar med avseende på generering, transport, lagring och hantering av logguppgifter. Vi har vidare ställt oss frågan varför en människa egentligen accepterar att bli dömd p.g.a. uppgifter som genererats av en maskin. Varför tillmäter ett informationssystem, med dess mänskliga beroenden, en sådan auktoritet att människor okritiskt använder dess loggutdrag som enda underlaget för en logganalys?

1.2 Problemdiskussion

Om vårt antagande stämmer, nämligen att det är ovanligt att man i samband med förundersökning och huvudförhandling ifrågasätter riktigheten i ett loggutdrag, skulle detta kunna bero på att loggutdragen i allmänhet är korrekta. Det kan å andra sidan tyda på okunskap, som i sådana fall leder till att den åtalade, åklagaren, advokaten samt domstolen okritiskt antar en organisations loggutdrag som bevis.

Om man i diskussionen kring hanteringen av loggutdragen och logganalyserna tar med begrepp som administratörer, ITS-teknik, operativsystem och program, d.v.s. plattformar och applikationer, samt olika former av autenticeringsmetoder för verifiering av en IT-användares identitet, finner vi att det finns ett antal svagheter i antagandet att systems loggutdrag, utan kritisk granskning, kan accepteras som enda bevisning under förundersökningar och huvudförhandlingar. Vid en första anblick kan det konstateras att det finns ett antal tillfällen längs loggens väg, från ursprung till presentation, där den kan tänkas vara editerbar eller på annat sätt möjlig att förändra. Framför allt finns det fler aspekter som måste vägas in i en logganalys än enbart loggutdragen från aktuella system.

Att man inte ifrågasätter loggutdragen som en organisation levererat kan tyda på att man redan känner till alla kringliggande faktorer som kan påverka riktigheten hos ett loggutdrag, samt hur systemens loggar har hanterats från det att den skapas till det att den förevisats. Å andra sidan kan det okritiska förhållningssättet bero på dess raka motsats, nämligen att detta är någonting som man inte alls känner till och inte ens kan ifrågasätta eftersom man inte känner till hur riktigheten hos loggar och loggutdrag kan ifrågasättas.

Visar det sig att de rättsvårdande instanserna inte känner till dessa faktorer, men ändå avstår från att ifrågasätta riktigheten hos en organisations loggutdrag, kan detta knappast bero på annat än okunskap. Denna okunskap består i sådana fall av vilka möjligheter det finns att, medvetet eller omedvetet, påverka innehållet i en logg eller i ett loggutdrag. I uppsatsen kommer vi därför att försöka förklara loggens väg i termer av transport, lagring och hantering, där begreppet hantering bland annat omfattar sådant manuellt arbete som syftar till att göra logganalysen mer lättförståelig genom att manuellt eller maskinellt bearbeta de uppgifter som finns i ett loggutdrag. Vi vill med andra ord påvisa att det är möjligt att påverka riktigheten i en logg och i ett loggutdrag genom de brister som finns i tekniska informationssystem om man inte bygger in speciella skydd mot dessa hot.

1.3 Problem

Hur värderar de rättsvårdande instanserna en organisations loggutdrag?

1.4 Syfte

Syftet med uppsatsen är att väcka debatt och aktualisera det faktum att de rättsvårdande instanserna idag saknar grundläggande kunskap om modern IT-teknologi, samt saknar relevant kunskap om de loggenererande organisationernas tekniska och administrativa miljö, för att kunna göra en bevisvärdering av organisationernas loggutdrag.

1.5 Mål

Målet med uppsatsen är att ta fram riktlinjer som gör det möjligt att bättre kunna värdera sanningsinnehållet i en organisations loggutdrag och därmed på ett säkrare sätt kunna fastställa loggutdragets bevisvärde.

1.6 Avgränsning

Uppsatsen omfattar endast interna nät och organisationer som har en egen systemutveckling, och som därmed förutses ha kunskap och resurser att själva kunna ställa krav på, och utveckla lösningar för hantering av loggar och ta ansvar för riktigheten i ett loggutdrag.

Vi exkluderar loggar som skapas på klienten i ett klient – server system. Dessa exkluderas eftersom riktigheten förutsätter att organisationen lyckats skapa säkra klienter, vilket bedöms vara svårt att realisera.

I uppsatsen diskuteras analysen av ett loggutdrag i termer av transport, lagring, hantering samt övrigt. En begränsning blir därför att vi utgår från att loggarna som genererats av en dators programkod är korrekt. Det innebär att vi utgår från att det redan skett en valideringsprocess gällande riktigheten hos de loggar som systemet genererar.

I denna uppsats ingår inga förslag till tekniska lösningar som skulle kunna ligga till grund för hur en organisation skall leverera ett loggutdrag med tillräcklig hög riktighet. I stället har vi valt att peka ut ett antal områden som bör säkras för att en organisation som levererar loggutdragen skall kunna skapa underlag för en bevisvärdig logganalys. Vi har även tagit fram en ny modell för hur morgondagens logganalyser skall gå till, vilken avsevärt skiljer sig från dagens analys.

1.7 Målgrupp

Denna uppsats riktar sig inte enbart till människor med en teknisk bakgrund, utan till all personal som i sitt arbete, på ett eller annat sätt, kommer i kontakt med loggutdrag. Av den anledningen innehåller uppsatsen bland annat en teoretisk referensram som är tänkt att ge en grundläggande förståelse om bland annat vilken teknik som ligger bakom valet av vissa komponenter och tekniska lösningar samt vilken lagstiftning och regler som styr polisens arbete under en förundersökning.

Tekniken som beskrivs i den tekniska referensramen är inte heltäckande, men relativt ingående i de delar den omfattar. Vi motiverar detta med att det är nödvändigt att ha en grundläggande förståelse för dessa delar för att kunna förstå den diskussion och de slutsatser vi kommer fram till. Ett loggutdrags tillförlitlighet och möjlighet till påverkan i ett nätverk är ett tämligen avancerat område som inte är förståeligt utan djupare tekniska kunskaper. Att det därutöver tillkommer en manuell hantering under själva logganalysen är ytterligare en aspekt att beakta.

1.8 Disposition

Nedan presenteras arbetets upplägg på ett översiktligt sätt så att läsaren skall få en större förståelse för hur vi valt att strukturera vår undersökning. För varje kapitel presenterar vi ett antal punkter som behandlas:

Kapitel 1: Bakgrund
- Vad är problemet?
- Varför skriver vi om ämnet?
- Vad är våra avgränsningar?

Kapitel 2: Metod
- Vilka är de forskningsmetodiska problemen?
- Vilket forskningsmetodiskt upplägg har vi valt för vårat arbete?

Kapitel 3: Praktiskt tillvägagångssätt
- Hur har vi rent praktiskt lagt upp vårat arbete?
- Vilka har valts ut för en intervju?
- Hur har intervjuerna gått till?

Kapitel 4: Teoretisk referensram - Loggning
- Varför loggar man?
- Vad använder man loggar till?
- Vilka typer av loggar finns?

Kapitel 5: Teoretisk referensram - Förundersökning
- Allmänt om förundersökning
- Förundersökningens riktighet och sakinnehåll
- Bevisvärde
- Data- och informationskvalitet

Kapitel 6: Teoretisk referensram – Hot mot datakvalitet
- Attacker mot data i ett nätverk
- Säkerhetstjänster
- Säkerhetsmekanismer

Kapitel 7: Teoretisk referensram – Informationssäkerhet
- Informationssäkerhet vs förundersökning

Kapitel 8: Teoretisk referensram – Teknik
- OSI-modellen
- Protokoll
- Nätverkskomponenter
- Kryptering
- Metoder för integritetsskydd
- PKI

Kapitel 9: Empiri
- Sammanställning av genomförda intervjuer inom rättsväsendet
- Sammanställning av genomförda intervjuer inom informationssäkerhetsområdet
- Genomgång av rättsfall angående interna dataintrång inom polisen
- Genomgång av rättsfall angående interna dataintrång inom övriga organisationer

Kapitel 10: Analys
- Exempel på konkret och abstrakt bevisning
- Kan ett loggutdrag ifrågasättas
- Vem ansvarar för att loggutdragen är korrekta

Kapitel 11: Slutsats
- En summering av de övergripande slutsatser som har gjorts utifrån den insamlade empirin

Kapitel 12: Förslag till morgondagens logganalys
- Förslag på metod för logganalys som skulle öka ett loggutdrags bevisvärde

Kapitel 14: Avslutande kommentar
- Hur goda är våra slutsatser?

Kapitel 16: Innehållsförteckning
- Förteckning över samtliga källor som använts under arbetet (publicerade/icke publicerade/informanter)

Bilagor:
- Sammanfattningar av genomförda intervjuer
- Manual för intervjuer
- Tabell över genomgångna rättsfall angående interna dataintrång inom polisen

1.9 Begreppsdefinitioner och förklaringar

I samband med denna uppsats kommer vi att återkomma till ett antal begrepp som läsaren bör ha kännedom om. Vissa av dessa definitioner är satta av författarna själva[3] medan andra är mer vedertagna definitioner som hämtats ur litteraturen. När så skett redogör vi för källan, medan de definitioner som saknar källa är satta av författarna själva.

Nedan följer en definition av en rad olika begrepp. Dessa utgör en förutsättning för att kunna förstå den diskussion som förs i uppsatsen:

Administratör *Varje operativsystem kräver ett eller flera konton. Det konto som har den högsta behörigheten är administratören. Kontot har fullständiga rättigheter i hela datorn. Administratören kan skapa andra konton och är i allmänhet ansvarig för underhållet av datorn. Nya konton kan knytas till administratörsgruppen och många systemfunktioner och rättigheter kan inte utföras från andra konton än administratörskontot [Bott & Siechert, 2001].*

Värt att nämna att det finns operativsystem, t.ex." Trusted Solaris", som är uppbyggda kring principen att ingen administratör skall ha rättigheter till samtliga tjänster. Istället existerar av säkerhetsskäl flera administratörer inom samma system I vårt arbete så kommer vi därför normalt att avse någon som har administrativa rättigheter till ett system när vi talar om administratör.

Analysresultat *Resultatet av en logganalys som beskriver den tekniska och administrativa miljö där organisationens loggar skapats, lagrats och hanterats. Analysresultatet utgör tillsammans med förundersöknings-protokollet den grund som åklagaren behöver för att kunna värdera bevisvärdet av organisationens loggutdrag.*

Applikation *En applikation är ett program som designats för ett visst ändamål. För att en applikation på ett säkert sätt skall kunna ta del av till exempel en dators resurser krävs det att applikationen körs på ett operativsystem som tillhandahåller tjänster som applikationen kan nyttja.*

Arkivering *För att kunna arkivera loggdata så att den är åtkomlig i framtiden krävs att de lagras på ett minnesresistent lagringsmedia som till exempel band eller disk.*

För att uppnå spårbarhet tillbaka i tiden krävs ett regelverk eller en policy hos organisationen som anger hur länge loggarna skall lagras. Datainspektionens krav är att organisationernas loggar skall sparas i minst två år. Organisationerna kan därutöver lagra loggarna under längre tid om de finner det motiverat. Värt att nämnas är att enligt arkivlagen (främst militär tillämpning) skall loggar från hemliga system arkiveras i 10 år och från kvalificerat hemliga system i 25år.

[3] Ibland är dessa av en mer förklarande karaktär snarare än en regelrätt definition

Befogenhet *Många gånger ger en behörighet en användare möjlighet att få åtkomst till fler uppgifter ur ett IT-system än vad som är behövliga för att genomföra en arbetsuppgift. Genom ett skriftligt regelverk kan man reglera behörigheten, d.v.s. rättigheterna i systemet, mer än vad systemets BKS (Behörighets-och kontrollsystem) gör. Vad som är befogat begränsas med ett regelverk som anger när och under vilka förutsättningar användare får nyttja sin behörighet.*

Behörighet *Behörigheten utgör användarens rättigheter i ett i ett IT-system. Ett BKS-system är ett sätt att begränsa en användares behörighet i systemet. En begränsning kan vara att enbart ge användaren läsbehörighet, men i övrigt ge tillgång till hela systemets datainnehåll. Då det t.ex. inte i förväg går att avgöra vilka individer som kommer att bli sjuka eller begå brott måste användaren, i förväg, ges läsbehörighet till hela systemet innehåll. Detta kan missbrukas varför behörigheten på något sätt måste begränsas. En användares behörighet kan begränsas genom inskränkningar i användarens befogenhet.*

Bevisvärde *Graden av en objektiv sanning att ett visst påstående eller föremål innehar den sanningshalt som påstås. Den som innehar den slutliga tolkningsrätten i denna fråga är våra allmänna domstolar.*

Data *Representation av fakta, begrepp eller instruktioner i form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel [SIS HB 550, 2003].*

Logghantering *I samband med hanteringen av loggutdrag förekommer ofta manuell hantering, som översättning eller annat manuellt arbete som överföring av data mellan olika applikationer i utredarens dator. Med hantering omfattas även överföring mellan olika media samt annan förflyttning av dataförsändelser via internpost eller liknande. Exempel på detta är när en organisation skickar en CD-skiva, innehållande de loggar som polisen beställt.*

Information *Innebörd av data [SIS HB 550, 2003].*

Logg *Insamlad information om de operationer som utförs i ett system [SIS HB 550, 2003]. En loggfil kan bestå av flera loggposter. De loggar som behandlas i denna uppsats omfattar främst den information man kan hämta ur säkerhetsloggen.*

En logg kan vara av olika typ, ex systemlogg och säkerhetslogg. Loggning är processen för att skriva in loggposter i systemets olika loggar. Av detta följer att begreppen loggposter och loggar är en delmängd av loggutdraget men samtidigt ett resultat av processen loggning.

Logganalys *Logganalysen syftar till att ta fram sådana uppgifter om organisationens tekniska och administrativa IT-miljö så att det är möjligt att kunna värdera sanningsinnehållet i ett loggutdrag.*

Loggning *Förande av logg [SIS HB 550, 2003].*

Loggutdrag *Loggutdraget består av de loggar som ett system en gång programmerats att samla in och som i denna uppsats främst omfattar säkerhetsloggen. När systemens loggar lyfts ut ur systemen för presentation utgör dessa tillsammans ett loggutdrag.*

Loggutdraget kan i sig innehålla mer information än säkerhetsloggen, men då det är användarens aktiviteter vi vill spåra lägger vi i denna uppsats en begränsning i loggutdragets definition till att normalt endast omfatta säkerhetsloggen.

Organisation *I denna uppsats avser vi med termen organisation större enheter som till exempel företag, kommuner, landsting och myndigheter med förmåga att leverera ett loggutdrag.*

Plattform *En plattform bygger på en dator med tillhörande operativsystem. Exempel på operativsystem är HP-Unix, Linux, Microsoft, Solaris med flera. Begreppet plattform kan även basera på en dator med viss tillhörande processor som till exempel Intel baserad plattform [Dyson, 1999].*

Riktighet *Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörningar har förändrats. Riktighet är en del av begreppet informationssäkerhet [SIS HB 550, 2003].*

Rättsvårdande instans *Med en rättsvårdande instans avses i denna uppsats polis, åklagare, domstol och advokatbyrå.*

Sanningsinnehåll *Nivån av en objektiv sanning som förundersökningen har som mål att identifiera.*

Spårbarhet *Med spårbarhet avses verksamheten och dess tillhörande system som skall innehålla funktioner som gör att det är möjligt att på ett entydigt sätt härleda utförda operationer till enskilda individer [Krisberedskapsmyndigheten I, 2003].*

Säkerhetslogg *Grundläggande krav på en säkerhetslogg utgörs av spårbarhet av registrerad användaridentitet, uppgift om in–och utloggning samt datum och tidpunkt om detta. Utöver dessa grundläggande krav är det brukligt att systemägaren beslutar över vilka andra aktiviteter som skall registreras i säkerhetsloggen. Exempel på sådana aktiviteter kan vara felaktiga och lyckade inloggningsförsök, IP-adress, Mac-adress, behörighetstilldelningar och förändringar av behörighetstilldelning [Krisberedskapsmyndigheten II, 2003].*

Transport *Sedan en logg genererats måste den transporteras till en plats för fysisk lagring. Detta sker i olika medier, t.ex. radio och kablar med koppar eller optofibrer. Transport omfattar inte fysisk transport av databärande media.*

Utökat loggutdrag *Loggutdraget och annan data som beskriver organisationens IT-miljö i termer av lagring, transport, hantering och övrigt. Ett utökat loggutdrag består i sin enklaste utformning endast av organisationens loggutdrag, men kan även innehålla data från andra källor som inpasseringssystem och arbetstidslistor m.m.*

2. Metod

Eftersom vår undersöknings primära syfte är att framföra ny kunskap är det av yttersta vikt att vi noga går igenom upplägget samt genomförandet av vår undersökning. Detta främst för att ge våra slutsatser större trovärdighet hos läsaren genom att visa att våra slutsatser är välgrundade men även för att underlätta för vidare forskning där andra vidareutvecklar vårat material. I detta kapitel följer därför en genomgång över den metod vi valt att använda i vår undersökning. Metoden kan ses som vårat redskap för att försöka besvara de frågeställningar vi satt upp och genom att definiera den innan vi påbörjar vår insamling av empiri så kan vi säkerställa ett metodiskt och systematiskt arbete. Hellevik [Hellevik, 1980] sammanfattar på ett bra sätt de grundkrav som bör ställas på en metod som skall användas i ett samhällsvetenskapligt forskningsarbete:

- *Det måste finnas en överrensstämmelse med den verklighet som undersöks*
- *Man måste göra ett systematiskt urval av informationen*
- *Man ska kunna utnyttja informationen på bästa sätt*
- *Resultaten ska presenteras på sådant sätt att andra kan kontrollera och granska hållbarheten*
- *Resultaten ska möjliggöra ny kunskap och medvetenhet om de samhälleliga förhållanden man står inför för att detta ska kunna leda till ett fortsatt forsknings- och utvecklingsarbete och till ökad förståelse*

Vi har löpande försökt använda ovanstående punkter som en sorts ”checklista” vid framtagningen av vår metod i ett försök att göra en sorts kvalitetssäkring av våra val. Nedan kommer vi att gå igenom de val vi gjort vad gäller vår metodansats i förhållande till Hellviks uppsatta kriterier.

Det kanske viktigaste kravet för en forskningsmodell är att det måste finnas en överensstämmelse mellan modellen och den verklighet som undersöks. Detta är dock inte så lätt som det kan låta i och med att forskaren vid vissa komplexa undersökningsansatser helt enkelt inte vet om det finns en hundraprocentig överensstämmelse. I vårat fall är däremot detta inte något större problem eftersom vår problemställning är relativt klar och lätt att konkretisera. Följaktligen kan vi relativt enkelt se huruvida vår modell överensstämmer med verkligheten i och med att vi valt att arbeta med intervjuer med sakkunniga och representativa personer. Resultatet av dessa intervjuer har sedan på ett överskådligt sätt sammanställts för läsaren.

På samma sätt har vi relativt enkelt kunnat göra ett systematiskt urval av informationen i och med att våra informanter gjort ett ”urval” i samband med intervjuerna och tagit upp vad de tycker är relevant ur deras perspektiv. Dock kan vi sägas ha gjort ett sorts urval i samband med att informanterna valdes ut i förhållande till vilken kunskap de förväntades sitta inne med.

Kravet på att informationen måste utnyttjas på bästa sätt kan även det vara svårt för den enskilde forskaren att avgöra. Vi har som ovan beskrivits valt att primärt arbeta med intervjuer eftersom vi anser att vi på så sätt i aktuellt fall får fram ny information på ett bra sätt. Informationen som sedan blivit frukten av dessa intervjuer har sedan diskuterats och analyserats för att slutligen presenteras som en del av arbetets slutsatser.

I och med detta har det följaktligen förts en löpande diskussion mellan oss själva vilken information som skall tas upp i arbetet. Detta har förhoppningsvis lett till att endast relevanta data presenterats.

I arbetet har referenser genomgående lagts ut för att underlätta för läsaren att på egen hand kontrollera våra uppgifter för att granska vad som ligger bakom våra slutsatser. Referenserna är utöver detta även till för att läsaren själv kunna söka vidare för att få mer information kring ett ämne. Som ovan beskrivits har även sammanställningar över samtliga intervjuer lagts som bilaga och referenser har även här utnyttjats i arbetet när information från dessa har använts. Samtliga sammanställningar av intervjuer har blivit godkända av respektive informant för publicering i arbetet.

Vad gäller kravet på att vår modell måste leda till ny kunskap samt kunna leda till fortsatt forskning kring området hoppas vi genom att uppfylla de övriga ovanstående punkterna på ”checklistan” att även detta mål uppfylls. Genom att använda referenser samt noga förklara vårat upplägg och hur vi kommer fram till våra slutsatser är vår målsättning att läsaren skall förstå hur den nya kunskapen kommit till. Detta kommer även leda till att kompletterande forskning möjliggörs i och med att det klart och tydligt skall framgå hur långt detta arbete har fört ”kunnandet” på detta område framåt. Genom att nämnda sammanfattningar av intervjuer bifogas som bilagor erbjuds även läsaren att ta del av samma ingångsvärden som vi fått fram under arbetet. Det är därmed fritt för läsaren att göra en egen analys för att därigenom upptäcka eventuellt förhållanden och dra egna slutsatser.

I nästa avsnitt kommer vi att gå igenom vårat metodupplägg för en djupare förståelse kring varför vi utformat vår undersökning på det sätt som vi gjort.

2.1 De grundläggande vetenskapliga synsätten

Vad gäller metodik brukar man i litteraturen ta upp två grundläggande vetenskapliga synsätt vad gäller samhällsvetenskaplig forskning. De två synsätten är positivism och hermeneutik och kan ses om två motpoler på en linjär axel och är således varandras motparter. Det är dock sällan som ett undersökningsupplägg är strikt positivistiskt eller hermeneutikiskt utan istället blir upplägget ofta en hybrid av dem båda med tonvikt åt något håll. Vi tänkte börja vår genomgång av våra metodval genom att använda oss Jacobsens [Jacobsen, 2002] modell över hur man kan klassificera ett upplägg enligt vart på ovan nämnda axel som undersökningsansatsen befinner sig. Denna klassificering görs genom att besvara fyra problem som vi nedan kommer att gå igenom. Problemen kommer att beskrivas och återkoppling kommer sedan att ske under den resterande delen av kapitlet för att slutligen avsluta med att summera svaren på dessa problem. De fyra problemen är som följer:

- **Metodikens första problem:** ***Induktiv kontra Deduktiv datainsamling***

Problemet rör vilken strategi som är bäst lämpad för att få grepp om verkligheten. Den ena strategin kan kallas för deduktion och kan sammanfattas med ”från teori till empiri” medan strategin induktion går ”från empiri till teori”. Vad det handlar om är huruvida forskaren har vissa förväntningar på det som skall studeras och i med detta sätt upp en teori som han/hon sedan genom undersökningen går ut och prövar eller om han/hon istället går in i undersökningen helt förutsättningslöst och skapar teorierna efter hand som information analyseras. Det handlar således om vilka förkunskaper forskaren har när han/hon tar sig an problemet.

- **Metodikens andra problem: *Holism kontra Individualism***

Problemet hänger samman med hur forskaren förväntas se på de sociala fenomen som skall studeras. Förespråkarna av individualism hävdar att fenomen alltid kan förklaras genom att studera enskilda individers motiv och beteende studeras medan de som föredrar en mer holistiskt ansats menar att en djupare förståelse endast kan uppnås genom att studera hur människor i grupp fungerar och uppträder i olika sammanhang. Detta eftersom problemet alltid står under inflytande av det komplexa samspelet mellan enskilda individer och det speciella sammanhang de ingår i. Den individualistiska ansatsen kommer därmed inte att få full förståelse för problemet i och med dess exklusion av kontext.

- **Metodikens tredje problem: *Närhet kontra Distans***

Genom att distansera sig från det som undersöks hävdar de som förespråkar distans att undersökningseffekter, dvs. att upplägget på något sätt påverkar undersökningens resultat, kan minimeras och helst helt elimineras. Eftersom det är en helt objektiv verklighet som skall studeras får denna inte på något sätt störas av forskaren. Mot detta resonemang finns de som hävdar att undersökningseffekter ändå alltid på ett eller annat sätt uppstår samt att forskaren i och med distansen riskerar att missa viktig förståelse för problemet. Istället bör närhet till det som undersöks eftersträvas för att därigenom gå djupare in i individens reflektioner kring sin verklighet.

- **Metodikens fjärde problem: *Ord kontra Siffror***

En vanlig uppdelning av den information som samlas in är i vilken form insamlingen sker. Empirin som består av numeriska värden[4] brukar kallas för kvantitativa data medan empiri bestående av ord, framförallt meningar, brukar betecknas som kvalitativ. Utgångspunkten för den kvantitativa skolan är att den sociala verkligheten alltid kan mätas genom metoder och instrument som ger oss information i form av siffror. Slutsatser kan sedan dras genom att statistiskt behandla empirin och på så sätt få fram generaliserbara fakta. Den kvalitativa skolan hävdar i sin tur att den kvantitativa metoden inte mäter någonting annat en forskarens förståelse för företeelsen i och med att metodens informationsinsamling av siffror förutsätter en operationalisering av forskarens teori. De menar istället att vi aldrig kan få en total förståelse för ett socialt fenomen ifall vi inte observerar individerna och låter dem tala med egna ord.

2.2 Reliabilitet - Validitet

För att uppnå trovärdighet hos läsaren måste undersökningen uppfattas som reliabel. Med reliabilitet menas att empirin måste vara tillförlitlig och trovärdig, undersökningen måste helt enkelt gå att lita på [Holme & Solvang, 1997]. Om samma undersökning teoretiskt ytterligare genomförs en gång med samma resultat som följd innebär detta att undersökningen är just reliabel. Detta är speciellt användbart i samband med statistiska enkätundersökningar där man kontrollerar resultatet från olika urvalsgrupper för att se om de stämmer överens, t.ex. vid en opinionsundersökning inför ett riksdagsval etc. I vårat fall med kvalitativa intervjuer fyller dock detta inte samma funktion i och med att det inte är lika viktigt med statistisk representativitet. Hade istället uppgifter varit att t.ex. överföra de åsikter som vi upptäcker hos våra informanter till en bredare massa så skulle ett representativt urval av informanterna vara avgörande. Med hjälp av kvalitativa intervjuer är vi istället ute efter en djupare kunskap om hur de olika individernas upplever det studerade problemet.

[4] Empirin behöver inte alltid bestå av numeriska värden men skall kunna ”kodas” till sådana vid en analys.

Trots detta måste vi dock ha begreppet aktuellt när vi designar vårat undersökningsupplägg så att det inte medför något systematiskt fel från vår sida som ofrivilligt vinklar resultatet. Något som är viktigt ur vårat perspektiv är dock att det kan vara svårt att upprepa mätningar på levande varelser eftersom det kan ha skett en påverkan efter förra testtillfället vilket medför att samma värden inte kommer att uppnås, detta i jämförelse med t.ex. en klinisk studie i laboratoriemiljö.

En mer generell definition av reliabilitet skulle därför kunna vara att ”*mätinstrumentet inte skall ge slumpmässiga fel*” [Wallén, 1996]. I vårat fall är det intervjuer som är vårat mätinstrument och för att reliabilitetssäkra dessa måste vi minimera faktorer som kan störa processen. Detta är viktigt ur vårat hänseende eftersom det finns en risk för olika typer av undersökningseffekter. Undersökningseffekter [Jacobsen, 2002] på undersökningens resultat uppstår som en produkt skapat av vårat eget upplägg av undersökningen. Företeelsen kan sägas vara ett uttryck för att upplägget på något sätt utövar en negativ påverkan på fenomenet vi undersöker[5]. Resultatet blir att vi inte kommer att mäta det vi avsåg att mäta, dvs. vi har ofrivilligt byggt in ett systematiskt fel i vår undersökningsmodell. Detta benämns även som att undersökningen inte är valid [Wallén, 1996].

2.3 Utveckling av problemställning

För att välja en utformning av en undersökning använder sig Jacobsen [Jacobsen, 2002] av två olika dimensioner, nämligen klar kontra oklar problemställning samt beskrivande kontra förklarande problemställning. Vid betraktelse ser läsaren att den problemställning vi satt upp i kapitel 1 är relativt klar i och med att den är relativt enkel att konkretisera. Detta till skillnad mot en oklar problemformulering där just detta blir svårare. Exempel på en sådan oklar frågeställning skulle kunna vara: "*Hur fungerar arbetsprocessen vid polisens logganalysgrupp*?” Här är frågeställningen en aning svårare att omedelbart översätta till olika typer av variabler samt enheter.

Vidare har vår frågeställning även formen av en beskrivande problemställning i och med att svaret på frågan är av beskrivande art (deskriptiv)[6]. Vi vill helt enkelt försöka beskriva vad de rättsvårdande instanserna kräver av ett loggutdrag. Skulle problemställningen istället vara av formen ”*Varför håller inte ett loggutdrag som bevis vid en rättslig process*” hade denna varit av en förklarande karaktär (kausal)[7]. Tillskillnad från den beskrivande problemställningen skulle forskaren i detalj behöva förklara problemet i form av all problematik som ingår i dess kontext och inriktat sig på ett orsaks verkan förhållande. Den beskrivande problemställningen förhåller sig istället på en mer ytlig nivå och nöjer sig med att endast konstatera att något förhåller sig på ett visst sätt [Jacobsen, 2002].

Efter att ha konstaterat att vår problemställning är både klar och beskrivande ser vi i figur 1 att vi i vårat arbete bör ”*beskriva omfång, frekvens och utveckling*” av det fenomen vi skall studera, d.v.s. rättsvårdande instansers syn på loggutdrag. Följaktligen kommer vi att försöka identifiera problemområden inom ämnet loggutdrag samt förmedla en bild över hur det förhåller sig idag med det aktuella problemet (*metodikens 1:a problem*).

[5] Många forskare menar dock att det i praktiken är omöjligt att helt avlägsna all undersökningseffekt på grund av att någon sorts relation/kontakt alltid kommer att ske mellan forskare och forskningsobjekt. Det bör dock alltid eftersträvas att minimera undersökningseffekten genom att se över sitt upplägg [Jacobsen, 2002].
[6] En deskriptiv undersökning formuleras ofta som ”Hur ser ett tillstånd ut”? [Jacobsen, 2002].
[7] En kausal undersökning formuleras ofta som ”Varför ser ett tillstånd ut som det gör”? [Jacobsen, 2002].

Figur 1 Beskrivning av dimensionerna beskrivande - förklarande och klar - oklar problemställning. Baserar sig på Jacobsens figur [Jacobsen, 2002].

2.4 Extensiv utformning – Intensiv utformning

Nästa avgörande [Jacobsen, 2002] har att göra med huruvida vi vill närma oss problemställningen genom att satsa på en undersökning med många enheter[8] (extensiv) och istället få variabler[9] eller istället genomföra en undersökning där vi istället satsar på många variabler (intensiv) och istället få enheter. Naturligtvis skulle man även kunna tänka sig en kombination av de båda vilket dock troligtvis skulle leda till en omfattande samt tidsödande undersökning med ett komplicerat analysarbete. Vanligtvis måste därför upphovsmännen bakom en undersökning på grund av ekonomiska och/eller tidsmässiga begränsningar inrikta sig mot antingen ett extensivt eller intensivt tillvägagångssätt, så är även i vårt fall.

I och med vår målsättning att beskriva det fenomen som vi studerar ligger nyckeln till problemet i att få en övergripande förståelse för problemet. Detta uppnås enklast genom en intensiv uppläggning med ett mindre antal enheter och istället ett större antal variabler. Den intensiva uppläggningen utmärks av att vi går på djupet av problemet med några få enheter och därigenom få en så fullständig bild som möjligt av en situation, ett fenomen eller händelse. Tonvikten ligger på att få grepp om individens uppfattning och tolkning av fenomenet (*metodikens 2:a problem*) [Jacobsen, 2002].

[8] I det här fallet är det de informanter som vi intervjuat som blir lika med begreppet enhet.
[9] De centrala beståndsdelarna i en problemställning kan brytas ned i variabler som kan sägas bygga upp den företeelse vi vill undersöka. I en undersökning som baserar sig på intervjuer som i vårat fall kan varje fråga sägas utgöra en variabel.

Vidare är vi här till skillnad från den extensiva uppläggningen inte ute efter att kunna generalisera vårat resultat eller att uttala oss om hur många som upplever ett fenomen på det ena eller det andra sättet. Därigenom är vi inte på samma sätt beroende av ett representativt urval med ett större antal enheter.

Den intensiva utformningen kan i sin tur delas upp i två olika typer, nämligen fallstudier och små-N-studier. Av dessa två är det den sist nämnda som passar oss bäst i och med att vi vill ha så många nyanser som möjligt av det problem som vi studerar i och med att fallstudierna ofta fokuserar sig kring en specifik händelse. Små-N-studier innebär istället att forskaren väljer ut mellan fem till tio enheter med avsikt att få en så mångfacetterad bild som möjligt av problemet. Målsättningen bör vara att enheterna skall komma från så många olika kontexter som möjligt. I vårat fall blir dessa kontexter de olika typer av organisationer som våra informanter har sin bakgrund inom, dvs. polis, åklagare, advokat mm. Därigenom säkerställs att det undersökta fenomenet belyses från olika vinklar och utgångspunkter [Jacobsen, 2002].

2.5 Insamlingssätt

Vid en beskrivande problemställning måste forskaren göra ett val över vilket typ av förhållande han/hon vill beskriva. Eftersom vi valt att genomföra intervjuer av en grupp av människor under en relativt begränsad tid[10] kan vi sägas genomföra ett sorts ”tvärsnittsstudie”. Följaktligen får vi endast reda på våra informanters åsikter om problemområdet vid tiden för den intervju som genomförs. Denna till skillnad från en så kallad ”tidsseriestudie” som följer utveckling över tid och därför hade det här blivit aktuellt med flera intervjuer med samma informant vid flera tillfällen. Vid den problemställning som vi har finns dock inga såna krav på förändring över tid och därför räcker det med att reda ut den åsikt som våra informanter har idag.

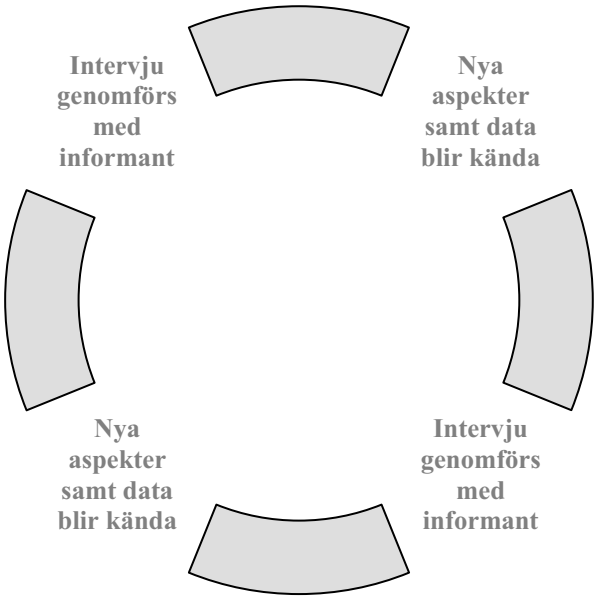
2.6 Kvantitativa data – Kvalitativa data

Nästa val som vi ställs för är huruvida kvantitativa data bestående av numeriska värden eller kvalitativa data bestående av ord/meningar bör samlas in. Mycket av detta val hänger redan på de beslut som vi har tagit ovan. Med tanke på att vi anser det som lämpligt att ha en intensiv undersökning av kausal karaktär bör kvalitativa data samlas in genom intervjuer. Detta eftersom vi vill låta våra informanter uttrycka just sin syn på det aktuella problemområdet. Deras åsikter är svåra att konkretisera till en enkät eftersom vi i förväg inte vet vad de kommer att säga. Istället låter vi dem presentera sin åsikt med egna ord vilket vi sedan sammanställer vid vår analys. Slutresultatet kommer bli en redogörelse avseende vad som i huvudsak är de största problemen samt var i kontexten de ligger.

En fördel med den kvalitativa ansatsen, till skillnad från den kvantitativa ansatsen, att de ansvariga före insamlandet av empiri inte på samma sätt behöver strukturerar upp vilken information som skall samlas in. Detta eftersom olika typer av enkäter[11] är den kvantitativa ansatsens främsta verktyg. Följaktligen måste forskarna ha identifierat fenomenets aktuella variabler för att kunna strukturera en enkät och det kanske är just detta som är den kvantitativa ansatsens största problem. Forskaren måste nämligen "trycka in" hela fenomenets verklighet i form av frågor på en enkät.

[10] Tidpunkten för vår insamling av empiri kan sägas vara från 040101 – 040901.
[11] Enkäten är nämligen ett försök att konkretisera problemställningen så att det går att undersöka empiriskt [Jacobsen, 2002].

Vid kvalitativ ansats behöver vi istället endast delvis identifiera aktuella variabler[12] utan kan istället rikta in forskningen efterhand som ny kunskap framkommer under tiden intervjuerna genomförs. Genom valet av att samla in kvalitativa data genom intervjuer har vi, som beskrivits ovan, gjort ett val att samla in vår empiri i form av ord (*metodikens 4:e problem*).



Figur 2 visar den cirkel som kvalitativ datainsamling utgör.

Figur 2 illustrerar hur vi genom kvalitativ datainsamling via intervjuer har möjlighet att styra in forskningen efter hand som ny kunskap blir känd. I och med detta kallas denna ansats för öppen ansats till skillnad från en enkätundersökning som är att betrakta som en slutens ansats. Vid en sluten ansats som t.ex. en kvantitativ datainsamling genom en enkätundersökning är risken att forskarens bild över vilka variabler som är viktiga och som representerar fenomenet inte stämmer överens med verkligheten. Hos den öppna ansatsen försöker forskaren istället att så lite som möjligt styra över vilken information som samlas in. Den kvalitativa undersökningen blir således betydligt mer flexibel och går därför i högre grad ner på djupet av det studerade fenomenet i och med att metoden lägger större vikt vid detaljer, nyanser samt det unika oss varje enhet. Undersökningen sätter till skillnad från den kvantitativa skolan få begränsningar på de svar en uppgiftslämnare kan ge [Jacobsen, 2002]. I och med valet av ett intensivt upplägg med intervjuer innebär det en mindre distans till de deltagande individerna än om vi istället skulle ha valt att samla in kvantitativa data genom t.ex. en enkät (*metodikens 3:e problem*).

[12] Dessa variabler blir i praktiken våra frågor vid de intervjuer som hålls vid undersökningen.

2.7 Summering av de fyra metodproblemen

Som en avslutning på detta kapitel skall vi nu göra en återkoppling till de fyra metodiska problem som togs upp i avsnitt 2.1 genom att gå igenom och besvara dem problem för problem. Problemen var som följer:

- **Metodikens första problem:** ***Induktiv kontra Deduktiv datainsamling***

I och med vår frågeställning ”*Hur värderar de rättsvårdande instanserna en logganalys och vad förväntar sig dessa instanser av organisationer som tar fram denna”?* kan vi sägas gå från empiri till teori. Detta eftersom vi inte har någon klart utformad teori utan sätter oss istället in i problemet med öppna sinnen. Således har vi en induktiv ansats för vår studie.

- **Metodikens andra problem:** ***Holism kontra Individualism***

Vår problemställning medför att vi snarare är ute efter olika individers åsikter kring problemområdet för att därigenom skapa oss en bild över den kontext som gäller kring bevisvärdering av loggutdrag. Någon djupare förståelse kring hur inblandade informanter interagerar med sin omgivning blir i det här fallet ointressant vilket medför att vi har ett individualistiskt angreppssätt snarare än ett holistiskt.

- **Metodikens tredje problem:** ***Närhet kontra Distans***

I och med vårat val att använda oss av intervjuer istället för enkäter för insamling av empiri så för detta med sig en större grad av närhet i förhållande till distans. Följaktligen ökar då risken för olika typer av intervjuareffekt där vi oavsiktligt på något sätt utövar påverkan på våra informanter. Vid vår typ av frågeställning är dock fördelen med att samla in empiri genom intervju betydligt större än denna risk.

- **Metodikens fjärde problem:** ***Ord kontra Siffror***

I och med vår önskan att få fram nyanserad kvalitativa data genom intervjuer behandlas vår insamlade empiri i ordform. Detta till skillnad från olika typer av enkäter där kvantitativa data i form av siffror är vanligast. Dock är vi här ute att få en förståelse för problemets kontext till skillnad från att samla in statistik vilket gör att den kvalitativa empirin lämpligast.

3. Praktiskt tillvägagångssätt

I detta kapitel kommer vi att gå igenom undersökningens praktiska upplägg vad gäller hur informanter valts ut, intervjuer genomförts samt slutligen hur det insamlade materialet analyserats. Anledningen till detta är att läsaren skall få en djupare förståelse för hur vi kommit fram till våra slutsatser.

3.1 Urval

Vid urval av personer till genomförda intervjuer har vi valt personer ur olika yrkesgrupper som på ett eller annat sätt kommer i kontakt med ett loggutdrag. Ett medvetet val i detta arbete har varit att kontakta informanter inom både det juridiska samt tekniska världen. Detta för att kunna säkerställa en så nyanserad bild som möjligt av problematiken kring loggning från så många synvinklar som möjligt.

Många av våra informanter inom de rättsvårdande instanserna har valts ut genom de kontakter Lindblom byggt upp genom sitt arbete inom polisen som våldsutredare och IT-säkerhetsspecialist. Detta ansågs som en ”smidig” lösning som skulle spara tid men även möjliggöra intervjuer med personer som annars kan vara svåra att nå. Övriga informanter har kontaktats i och med deras medverkan i ett antal tidningsartiklar som behandlat problematiken kring loggning[13].

Sammanfattningar av samtliga intervjuer ligger insorterade som bilagor i slutet av uppsatsen efter vilken organisation informanten arbetar inom. Sorteringen möjliggör för läsaren att ta del av de olika yrkesgruppernas åsikter kring vår problemställning. Fördelningen våra intervjuer har varit på följande sätt:

3.1.1 Informanter inom polisens utredningsavdelningar

De intervjuade personerna (bilaga A) arbetar inom polisen och har i sitt arbete kommit i kontakt med loggar. De intervjuade utredarna utgörs av följande personer:

1. ***Jim Keyzer**, kriminalinspektör vid Länskriminalens IT-brotts grupp i Stockholm.*
2. ***Ingemar Leijon**, kriminalinspektör vid bedrägeriroteln i Kristianstad.*
3. ***Per-Erik Bergnér**, poliskommissarie vid enheten för interna utredningar i Stockholm.*

3.1.2 Informanter inom åklagarmyndigheten

De intervjuade personerna (Bilaga B) arbetar inom olika enheter inom åklagarmyndigheten i Stockholm. Dessa är utvalda eftersom de mer än allmänna åklagare förväntas komma i kontakt med loggar i sitt arbete. De intervjuade åklagarna utgörs av följande personer:

4. ***Christer Ekelund**, Chefsåklagare vid Polisenheten inom åklagarmyndigheten i Stockholm.*
5. ***Kay Engfeldt**, vice Chefsåklagare vid Polisenheten inom åklagarmyndigheten i Stockholm.*
6. ***Håkan Roswall**, kammaråklagare (IT-åklagare) vid internationella kammar-åklagaren, Stockholm.*

[13] Gäller intervjuer som genomfördes vid Datainspektionen samt Danderyds Sjukhus

3.1.3 Informanter inom advokatbyråer

De intervjuade personerna (Bilaga C) utgörs av advokater inom rättsväsendet. Dessa är utvalda eftersom deras namn ofta figurerat som försvarare i de domar som författarna tagit del av under förarbetet till denna uppsats. De förväntas av den anledningen ha en större erfarenhet av loggar än vad en advokat förväntas ha som väljs ut på måfå. De intervjuade advokaterna utgörs av:

7. ***Johan Ericsson**, brottsmålsadvokat vid advokatfirman Advokaterna.*
8. ***Ola Salomonsson**, brottmålsadvokat vid advokatbyrån Advokatfirman Peter Ahltin, Ola Salomonsson, Per Liljeqvist HB.*
9. ***Per Durling**, brottmålsadvokat (f.d. åklagare och domare), advokatfirman Per Durling, Stockholm.*

3.1.4 Informanter inom informationssäkerhetsområdet

I syfte att bredda uppsatsen har vi valt att intervjua konsulter inom informations-säkerhetsområdet (Bilaga D) eftersom dessa kommer i kontakt med olika organisationer i sitt arbete. Informanterna inom detta område är:

10. ***André Richardsson**, teknikkonsult vid Ekelöw Infosecurity AB, Stockholm*
11. ***Mats Söderholm och Mattias Olsson**, teknikkonsulter vid konsultföretaget FKC AB, Stockholm*

3.2 Genomförande av intervjuer

Vid den inledande kontakten med våra informanter har vikt lagts vid att inte i detalj gå in på inriktning av arbetet vad gäller våra misstankar om att logghantering i flera fall är bristande ur rättssynpunkt. Detta för att inte i förväg ”färga” informanternas inställning till problem-området och därmed påverka slutresultatet av intervjun.

Eftersom vi velat ha fram undersökningspersonernas egna uppfattningar har målsättningen varit att dessa i största möjliga mån själva fått styra över utvecklingen av intervjuerna. Således har vi inte kunnat nyttja oss av någon standardiserad intervju utan nöjt oss med att i förväg försöka skriva ner en sorts manual [Holme & Solvang, 1997] som utan någon ordning dem emellan behandlat ett antal ämnen som vi velat klara av under intervjun. Detta har resulterat i att vi i intervjuerna förutom fått svar på våra förut bestämda frågor även fått information angående säkerhet och loggning som legat strax utanför vår frågeställning. Intervju manualen ligger i sin helhet under bilaga E.

Eftersom vissa av våra intervjuer berörde information som kan uppfattas som känslig beslutades vid arbetets inledning att inte använda oss av någon form av inspelning eftersom detta kunde verka hämmande på informanterna. Istället fördes löpande anteckningar under intervjuerna. Målsättningen var sedan att renskriva anteckningarna snarast efter intervjuernas genomförande. Slutprodukten är en sammanfattning över intervjun och denna har slutligen skickats till informanten som gjort ändringar på sådant som vi missförstått eller som av annan anledning behövts skrivas om eller tas bort. Följaktligen är samtliga sammanfattningar av intervjuer som presenteras i arbetes bilaga godkända av respektive informant.

I vårat arbete har vi även gjort en granskning av större delen av alla rättsfall angående interna dataintrång inom polisen i Stockholms- samt Gotlands län mellan 1994 – 2003[14]. Denna granskning har genomförts med syfte att ge oss en bild av vilket resonemang de svenska domstolarna fört vad gäller loggars bevisvärde. Av speciellt intresse har de fall där anklagade har nekat skuld trots att loggutdragen talat emot dem. Dessa fall har i sin tur specialgranskats i och med att vi tagit del av förundersökningsprotokoll. Vi har även gått igenom ett par rättsfall inom organisationer utanför polisväsendet, främst inom sjukvård och kommun. Dessa domar är fall som vi blivit uppmärksammade på genom våra intervjuer under arbetets gång och som har bedömts som särskilt intressanta ur vår synvinkel.

3.3 Metodkritik

En invändning mot vårat arbetssätt skulle kunna vara att nyttjande av våra kontakter resulterat i att inte blivit något naturligt urval av informanter till intervjuerna. Resultatet skulle i och med detta kunna blir ”snedfördelat” och inte speglar verkligheten. Vi betraktar dock inte detta som ett större problem då vi inte eftersträvat att göra några statistiska mätningar som kräver att enheterna[15] väljs ut med ett slumpmässigt urval eller liknande för att uppnå generaliserbarhet [Holme & Solvang, 1997]. Informanterna har i samtliga fall[16] haft värdefull kunskap och varit fördelade över en rad olika organisationer vilket gör att den risken får anses som försumbar.

Vad gäller risken för att vi skulle kunna ha framkallat någon form av intervjueffekt [Jacobsen, 2002], som t.ex. att informanten gett svar som han/hon tror tillfredställer intervjuaren, anser vi att den risken är mycket liten eftersom det stora flertalet av informanterna agerar inom det juridiska systemet och bör därför vara väl förtrogna med vikten av att ge en objektiv och saklig framställan. I vissa fall tror vi även att det varit till vår fördel att informanterna valts ut i det egna kontaktnätet eftersom vi då i vissa fall har kunnat föra mycket ”öppnare” diskussioner än vad som annars varit fallet. Vid en samlad bedömning av valet att nyttja det egna kontaktnätet vid urval av informanter så konstaterar vi att fördelarna vida överträffat nackdelarna.

[14] Enheten för interna utredningar i Stockholm har både Stockholm och Gotlands län som upptagningsområde vilket medfört att vi på ett smidigt sätt kunnat ta det av fler domar. Vi har medvetet valt att skriva att ”större delen” av aktuella fall har gåtts igenom. Detta eftersom det vissa förundersökningsprotokoll helt enkelt har saknats hos de arkiv som använts. Eftersom målsättningen inte har varit att göra en komplett undersökning utan endast skapa oss en uppfattning angående dessa interna intrång så har detta från vår sida inte uppfattats som något större problem.

[15] I detta fall är enheterna synonymt med informanterna.

[16] Vad gäller de konsulter som vi intervjuat så kan de betraktas vara bland de främsta i landet på området.

4. Teoretisk referensram: Loggning

Den teoretiska referensramen syftar till att ge läsaren grund att stå på när det gäller att tillgodogöra sig vår presentation av problemen kring loggning. I avsnittet nedan presenteras en genomgång av loggning och spårbarhet. Eftersom uppsatsen riktar sig mot såväl juridiska som tekniska yrkesgrupper är kapitlet uppbyggd på en relativ grundläggande nivå.

4.1 Allmänt om loggutdrag och spårbarhet

Rent generellt kan sägas att syftet med loggning är att kunna reda ut *vad* som gjorts samt *hur*, *när* och av *vem*. Dessa frågor kommer att utgöra ett viktigt underlag vid misstanke om säkerhetsrelaterade incidenter och det är därför av yttersta vikt att säkerställa skyddet mot manipulering av loggar under hela vägen från det att loggen genereras till presentation. Detta för att arkiverade loggar skall kunna tillmätas ett bevisvärde vid en eventuell rättegång.

I samband med loggning återkommer en grundläggande frågeställning som ansvarig måste ta ställning till. Denna fråga är vilka aktiviteter hos en användare eller administratör som skall loggas. Det optimala vore naturligtvis om alla händelser i ett system loggades, men detta skulle innebära stora loggmängder och samtidigt innebära större kostnader i tid, pengar och resurser för att kunna analysera en sådan stor datamängd. Den ansvariga måste därför göra en avvägning för att hitta rätt balans i sin verksamhets loggning.

En systemmiljö är ofta komplex med flera underliggande system. För att utföra en effektiv loggning i ett sådant fall kan det bli nödvändigt att kombinera olika typer av loggar för att få en klar bild över olika skeenden. Exempel på olika typer av loggar som skulle kunna kombineras beskrivs enligt följande [H Säk IT, 1997].

- **Säkerhetsloggar**

Används för kontroll av åtkomst och behörighet. Säkerhetsloggar används huvudsakligen för att kunna spåra obehörig användning av ett system samt avgränsa misstänkta.

- **Driftloggar**

Används för uppföljning av funktionssäkerhet. Driftloggar används tillsammans med driftjournaler för att övervaka driften av ett IT-system och ge uppgifter om tillgänglighet, kapacitet och utnyttjande av systemet.

- **Transaktionsloggar**

Används för att spåra bearbetning. Transaktionsloggar används för att återställa informationen efter ett haveri, identifiera detaljförändringar. De skall även kunna utgöra underlag vid ekonomisk revision.

- **Tillträdesloggar**

Används för kontroll av tillträde till och från skyddade utrymmen. Är ett viktigt komplement till säkerhetsloggar.

Det är även viktigt att förstå att loggning inte alltid går ut på att spåra händelser i efterhand, ibland flera år, utan inriktningen kan även vara övervakning i realtid med en larmfunktion vilken varnar vid en t.ex. en attack eller övriga onormala händelser. Syftet blir då att vidta åtgärder för att begränsa verkningarna av händelsen.

Loggning kan inom en organisation även ha en förebyggande effekt eftersom kännedomen om att användaraktiviteterna i ett system loggas, förhoppningsvis avskräcker vissa från att överskrida sina befogenheter. Detta är naturligtvis under förutsättning att användarna informerats om att loggning sker.

Krisberedskapsmyndigheten har gett ut rekommendationer för vad som lägst bör vara uppfyllt vad gäller loggning och spårbarhet för att system skall uppfylla kraven på s.k. basnivå. Basnivå definieras som den ”*säkerhetsnivå som minst måste uppnås för ett IT-system som bedöms nödvändigt för att upprätthålla en viss verksamhets basförmåga*”. Ambitionen är att denna nivå skall vara balanserad och generellt ge en acceptabel säkerhetsnivå. Genom att göra en risk- och sårbarhetsanalys i varje enskilt fall säkerhetsställs om denna basnivå är tillräcklig [Krisberedskapsmyndigheten II, 2003].

Loggning och spårbarhet på basnivå innebär följande:

- Det skall finnas en säkerhetslogg som registrerar användaridentitet, uppgift om inloggning och utloggning samt datum och tidpunkt för dessa.

- Systemägaren[17] skall fastställa vilka händelser utöver ovanstående som skall registreras i IT-systemets säkerhetslogg (t.ex. felaktiga inloggningsförsök eller förändring i behörighet).

- Den centrala systemägaren ska säkerställa att IT-systemet är konstruerat så att uppgift om användaridentitet samt datum och tidpunkter för in- och utloggningar kan registreras i en säkerhetslogg.

- För säkerhetsloggar skall systemägaren besluta:
  - *Hur ofta de skall analyseras*
  - *Vem som ansvarar för analyser av dem*
  - *Hur länge de skall sparas*
  - *Hur de skall sparas*
  - *Hur de ska förvaras*

- För transaktionsloggar skall systemägaren besluta:
  - *Hur ofta de ska analyseras*
  - *Vem som ansvarar för analyser av dem*
  - *Hur länge de ska sparas*
  - *Hur de ska förvaras*

[17] Definieras enligt Krisberedskapsmyndigheten som ”*Organisationens chef eller av denne särskilt utsedd aktör med ansvar för anskaffning, ny-/vidare-/avveckling, förvaltning, drift, säkerhet och användning i övrigt av ett IT-system inom ramen för antagna mål och ekonomiska ramar*”

Slutsatsen av ovan nämnda är att loggning är ett ämne som kan ta stora resurser i anspråk för en organisation med stora mängder känslig information såsom t.ex. militära underrättelsedata, forskningsresultat, brottsregister m.m. För denna typ av organisationer kan det bli aktuellt att ha anställda som på heltid underhåller samt övervakar loggdata på grund av dess omfattning. Eftersom loggar ingår i det loggutdrag som skall kunna användas som grund för bevis vid en eventuell rättegång kommer höga krav ställas på systemens ”administratörer” eftersom dessa kan ge sig själva access till alla tjänster som körs på en plattform eller applikation. Därmed kan de i både teori och praktik ändra dess innehåll. Därför måste administrativa samt tekniska lösningar utarbetas kring denna problematik för att säkerställa loggarnas tillförlitlighet.

5. Teoretisk referensram: Förundersökning

Den teoretiska referensramen syftar till att ge läsaren en grund att stå på när det gäller att tillgodogöra sig vår presentation av problemen kring begreppet förundersökning. Eftersom uppsatsen riktar sig till yrkesgrupper som kommer i kontakt med loggutdrag är dessa som regel bekant med begreppet förundersökning. För de läsare som inte ingår i denna grupp lämnas i detta kapitel en inledande beskrivning av begreppet samt dess koppling till IT-relaterad bevisning.

5.1 Allmänt om förundersökningar

I detta arbete kommer vi att återkomma till begreppet förundersökning. En förundersökning är, som framgår av namnet, endast en förberedande brottsutredning. Den slutliga undersökningen av det brott som utredningen gäller kommer att ske i rätten. Förundersökningens huvuduppgift är därför att ge åklagaren ett underlag för bedömning i åtalsfrågan [Bring et al, 1995].

Under förundersökningen håller polisen förhör med en mängd personer. Dessa kan höras som misstänkta, målsäganden, vittnen eller vad som kallas för ”*i sak*”. Det finns tillfällen när man behöver hämta in information om en människa av personer som inte är direkt inblandade i det brott som förundersökningen omfattar, och som då varken är misstänkt, målsäganden eller vittne. Dessa förhör brukar kallas för att personen hörs ”i sak” vilket innebär att denne lämnar sina uppgifter till förhörsledaren, där uppgifterna omfattar själva sakfrågan som utreds. Under förundersökningen genomförs ofta ett antal tvångsbeslut i form av gripanden, anhållanden, häktning och husrannsakan m.m. Dessa regleras var för sig i lag och är de redskap som polisen använder för att samla in bevis. Allt detta redovisas skriftligen i ett förundersökningsprotokoll. Det innebär med tiden ett protokoll som växer i omfattning allteftersom polisen vidtar olika åtgärder. Ett slutgiltigt förundersökningsprotokoll omfattar inte sällan flera hundra sidor text och bilder där utredarna dokumenterat förhör, tekniska undersökningsresultat, fotografier, experters utlåtanden m.m. I utredningar där loggutdrag ingår kommer dessa att utgöra en del av det skriftliga materialet i förundersökningsprotokollet.

5.2 Förundersökningens syfte

Rättegångsbalkens (RB) 23:e kapitel reglerar området förundersökning. I dess andra paragraf anges att syftet med en förundersökning är att utreda:

- *Vem som skäligen kan misstänkas för brottet.*
- *Om tillräckliga skäl för åtal föreligger mot den misstänkte.*
- *Att målet kan beredas så att bevisningen kan förebringas i ett sammanhang vid huvudförhandlingen*

En förundersökning skall inte enbart omfatta de omständigheter som talar emot den misstänkte, utan även det som talar för den misstänkte skall beaktas och tas tillvara. Vidare bör undersökningen bedrivas på ett sådant sätt att inte någon onödigt utsätts för misstanke eller drabbas av kostnad eller olägenhet [RB 34:4].

Det finns ett antal principer som skall vara styrande under en förundersökning. Dessa finns för att skydda den enskilde från maktmissbruk, godtycke och större integritetskränkningar än vad som är nödvändigt för att genomföra ett effektivt beivrande av det brott som utredningen gäller [Bring et al, 1995]. Dessa är:

Behovsprincipen	*som anger att tvång inte får användas om det inte är nödvändigt med hänsyn till syftet med åtgärden.*
Hänsynsprincipen	*som innebär att arbetet med utredningen skall göras så diskret som möjligt. Denna del är inskriven i RB 23:4 st 2 p.1.*
Legalitetsprincipen	*vilken i korthet innebär ”inget brott, inget straff utan lag”. Denna legalitetsprincip är lagfäst i regeringsformen. Brott i sig definieras som en gärning som är belagd med straff i Brottsbalken(BrB) eller i annan lagstiftning [BrB 1:1]..*
Objektivitetsprincipen	*som är inskriven i RB 23:4, och som innebär att man under förundersökningen skall ta tillvara både det som talar för och det som talar emot den misstänkte.*
Oskuldsprincipen	*vilket innebär att en misstänkt skall betraktas som oskyldig fram till det att motsatsen är bevisad i en rättegång. Denna princip är fastställd i internationella överenskommelser som ratificerats av Sverige.*
Proportionalitetsprincipen	*anger att om tvång måste användas så skall det stå i proportion till det som ändamålet omfattar.*
Skyndsamhetsprincipen	*som regleras i RB 23:4, st 2 p.1 och som innebär att förundersökningen skall bedrivas så snabbt som möjligt.*
Ändamålsprincipen	*som anger att en myndighets befogenhet att använda tvång uteslutande skall vara knutet till det ändamål för vilket tvångsmedlet beslutats. Man kan således inte använda tvång som påtryckningsmedel för att framtvinga ett erkännande.*

Ett förundersökningsprotokoll är inte enbart ett samlat dokument som visar vad som framkommit under förundersökningen utan det fungerar även som ett kontrollinstrument. Protokollet skall ge en autentisk bild av det som framkommit under förundersökningen. Av den anledningen är det av stor vikt att de åtgärder som vidtagits av polis och åklagare har dokumenterats så att det i efterhand finns en möjlighet att granska det som skett under utredningen.

Förundersökningskungörelsen är styrande över vad som skall antecknas i förundersöknings-protokollet, vilket anger att detta område är tämligen reglerat. I grund och botten är den kontrollåtgärd som ett samlat dokument medger av en väsentlig betydelse för tilltron till rättsväsendet [Bring et al, 1995]. Dess samlade dokumentation innebär en möjlighet för den misstänkte och dennes försvarare att bemöta åklagarens bevisning med de argument som de kan hämta ur förundersökningsprotokollet.

I grund och botten har polisen mycket stort inflytande över vad som rapporteras till åklagaren. För att denne skall kunna bygga ett åtal av det som framkommit under förundersökningen är det viktigt att åklagaren kan lita på de uppgifter som denne får från polisen.

Det är av den anledningen som polisen har en skyldighet att förse åklagaren med ett material som är relevant och adekvat [Bring et al, 1995].

I och med att det är polisen som är ansvarig för att ta fram den bevisning och de uppgifter som en förundersökning kan leda fram till är det även polisen som har det yttersta ansvaret för att uppgifterna i förundersökningsprotokollet är riktiga. För den som inte är insatt i denna hantering kan det te sig konstigt att även felaktiga och direkt osanna uppgifter kan ingå som en del i förundersökningsprotokollet. Det beror på att polisen är skyldig att redovisa de uppgifter som faktiskt kommer fram under förundersökningen, även om strävan naturligtvis är att ta fram en så objektiv sanning som möjligt.

5.3 Sakinnehåll och sanningsinnehåll

En förundersökning kan till stora delar vara byggd på felaktiga påståenden och lögner, men ändå vara korrekt till sitt sakinnehåll. Det innebär att den på ett korrekt sätt återger vad människor berättat i förhör och i övrigt korrekt beskriver vad utredningen kommit fram till. Följaktligen innebär en lögn från den misstänkte att förundersökningen är korrekt till sitt sakinnehåll så länge förhöret återger vad den misstänkte verkligen berättat, även om sanningsinnehållet naturligtvis är lågt.

Målet med förundersökningen är att skapa ett förundersökningsprotokoll med så hög sanningshalt som möjligt. Genom att motbevisa den misstänktes lögner når förundersökningen en högre nivå av sanningsvärde eftersom man genom detta inte behöver bygga sanningshalten på den misstänktes berättelse. Även vitten kan komma med felaktiga vittnesuppgifter. Dessa kan vara medvetna eller omedvetna. Styrkan i vittnesförhören ökar om fler vittnen säger samma sak. Av den anledningen hör man fler vittnen än bara ett när fler vittnen finns. Objektivitetsprincipen innebär, som vi ovan beskriver, att även sådan information som talar för den misstänkte skall tas med i förundersökningsprotokollet. Av den anledningen måste förundersökningen bedrivas objektivt från utredarnas sida. Annars kan denna princip inte efterlevas.

Om lögner och bristfälliga iakttagelser är hot mot sanningsvärdet i den muntliga bevisningen, som dokumenteras i förhör, finns liknande hot mot den IT-relaterade bevisningen. Dessa hot kan grunda sig på det faktum att även administratörer och användare kan ljuga och manipulera systemen de arbetar med. Det finns även en möjlighet att teknisk utrustning kan fallera o.s.v. Den typ av IT-relaterad bevisning som vår uppsats berör är de loggar som genereras som ett resultat av en användares aktiviteter i ett tekniskt informationssystem.

All typ av bevisning som presenteras i ett förundersökningsprotokoll har, eller kan ha, olika nivåer av bevisvärde. Problematiken med sanningshalt och sakinnehåll gäller all bevisning, såväl muntlig, skriftlig som teknisk. För att rätt kunna värdera bevisningens sanningshalt vidtar man olika åtgärder i syfte att se om t.ex. en berättelse kan bekräftas eller motbevisas. På samma sätt kan man vidta åtgärder för att se om loggutdraget från ett informationssystem kan bekräftas eller motbevisas. Dessa åtgärder medger en möjlighet att på ett mer genomgripande sätt värdera förundersökningsprotokollets sanningsinnehåll och riktighet.

Även en organisations loggutdrag kan vara korrekt till sitt sakinnehåll, men ändå felaktig till sitt sanningsinnehåll om det återger ett felaktigt påstående. Detta kan jämföras med lögnen i ett förhör, som rätt dokumenterad är korrekt i sak men har ett lågt sanningsinnehåll.

Även om ingen medvetet manipulerat med ett systems loggar resulterar ett loggutdrag som inte är sanningsenlig i ett påstående som är felaktigt. Loggar person A in i ett system med person B:s användarnamn och lösenord kommer loggarna som skapas att vara korrekta till sitt sakinnehåll, men felaktiga till sitt sanningsinnehåll eftersom de i loggutdraget pekar ut fel person som ansvarig för de aktiviteter som loggats.

Målet att ta fram ett förundersökningsprotokoll med så högt sanningsinnehåll som möjligt innebär att den IT-relaterade bevisningen måste hanteras på samma sätt som övrig bevisning. Eftersom även den IT-baserade bevisningen kan ha olika bevisvärde måste den behandlas med samma medel som t.ex. den muntliga bevisningen. En organisations loggutdrag kan endast värderas om man under förundersökningen ställer krav på information om den tekniska och administrativa miljö där systemens loggar har genererats och hanterats. I detta ligger även att ta reda på hur man skyddat loggarna mot de hot som kan tänkas finnas i tekniska informationssystem.

Eftersom målet med uppsatsen är att ta fram riktlinjer för att öka möjligheten att göra en bättre bevisvärdering av en organisations loggutdrag är en förutsättning att identifiera vilka områden som kan påverka dess riktighet och sanningsinnehåll.

5.3.1 Miljö

För att kunna göra en någorlunda korrekt bevisvärdering av t.ex. ett vittnesförhör räcker det inte med att enbart förhöra vittnet om dennes iakttagelser. Man måste utöver iakttagelserna även ta reda på vilken relation vittnet kan tänkas ha till den som berättelsen omfattar och vad som skulle kunna motivera vittnet att lämna sin berättelse. Således måste vittnesförhöret beaktas utifrån den miljö som vittnet befinner sig i. Miljön kan tänkas påverka vittnets berättelse eftersom det i miljön kan finnas faktorer som påverkar vittnets berättelse. Dessa kan utgöras av hot, relationer, känslor och lojalitet m.m.

På samma sätt kommer miljön att påverka möjligheten att göra en korrekt bevisvärdering av ett loggutdrag. Miljön kan i detta fall bestå av t.ex. organisationens nätverkslösningar, interna regelverk och tekniska lösningar som bland annat kommer att påverkar administratörers möjlighet till åtkomst av data. Motsvarande krav på sakinnehåll och sanningsinnehåll när det gäller loggar beskrivs i uppsatsen i termer av data- och informationskvalitet.

5.4 Allmänt om begreppet kvalitet

Inom många organisationer utgör den samlade informationen en av de största tillgångarna för organisationens verksamhet och möjlighet att uppnå uppsatta mål. För informationsberoende organisationer innebär det många gånger att den som har den bästa informationen har ett försprång före den som har sämre information. Av den anledningen blir det allt viktigare att veta vilken information det är som organisationen behöver, vilken kvalitet informationen har och vad bristerna i informationens kvalitet medför för konsekvenser.

Det yttersta målet med informationssäkerhet är att säkerställa att rätt användare får rätt information i rätt tid. Innehållet i vår uppsats handlar mycket om att rätt data i rätt tid är. För att kunna läsa ut rätt information av ett loggutdrag krävs det att de data som loggutdraget består av är korrekt. Med vårat sätt att uttrycka det måste aktuella data dessutom vara sanningsenliga.

När man talar om informationskvalitet är det egenskaperna hos informationen man är ute efter. Egenskaperna hos informationen kan vara kvantitativa, vilket innebär att de kan beräknas, som t.ex. ålder. Egenskaperna hos informationen kan även vara kvalitativa, vilket innebär att dess värde baseras på en bedömning. Vad som i en given situation är rätt kvalitet hos informationen är beroende på vem som för ögonblicket är användare av informationen samt vad den skall användas till. Olika användare kommer att ha olika behov av informationen, och därmed olika krav. Dessa krav kan t.ex. variera i fråga om riktighet och relevans [SIS HB 550, 2003].

I uppsatsen följer vi SIS HB 550 [SIS HB 550, 2003] diskussion genom att göra skillnad på data- respektive informationskvalitet på följande sätt:

Datakvalitet *Datakvalitet är relaterad till representationen av fakta genom att beröra egenskaper hos data i det databehandlande systemet. Begreppet datakvalitet berör då egenskaper som definitioner, detaljeringsgrad samt i vilken utsträckning data är korrekt.*

Informationskvalitet *Informationens kvalitet är relaterad till tolkningen eller innebörden av den datamängd som behandlas. Det innebär att man måste ta hänsyn till att den information som användaren för tillfället behandlar tolkas och påverkar användaren. Informationskvalitet ser därför till datas meningsinnehåll vilket innebär att den är beroende av användarens tolkning samt vad användaren skall använda informationen till.*

Vad vi kommer fram till efter ovan genomgångna definitioner är att informationskvalitet berör uppgifternas betydelse, eftersom de måste tolkas, medan datakvalitet är en delmängd av informationskvalitet. Ett sätt att säkerställa datakvalitet när man diskuterar loggutdrag är att ge loggdata ett integritetsskydd. Ett annat sätt är att användaren autenticerar sig för målsystemet på ett mer säkert sätt genom t.ex. en förstärkt inloggning med ett smart kort.

Ett integritetsskydd garanterar loggarnas innehåll eftersom det skyddar dem mot förändring, radering eller tillförsel av falska loggar. Detta räcker dock inte för att kunna dra en korrekt slutsats av ett loggutdrag eftersom det mycket väl kan vara så att irrelevanta händelser är upphov till loggdata, och då har man ingen nytta av att den felaktiga informationen ges ett integritetsskydd. Av den anledningen kan man säga att begreppet datakvalitet är en delmängd av begreppet informationskvalitet.

Vad man kommer fram till när man diskuterar data- och informationskvalitet är att:

1. *datakvaliteten är beroende av informationssystemets kvalitet*
2. *användaren som utövar en viss funktion i organisationen tolkar, använder och påverkas av den data som denne tar del av. I vilken utsträckning som användaren förstår problemet, och därutöver vilken data som behövs, påverkar resultatet av tolkningen, d.v.s. informationskvaliteten.*

Användaren måste vara medveten om relationen mellan vilken information denne borde få av systemet och den information som systemet faktiskt ger. Detta gäller inte minst den som har till uppgift att analysera loggutdragen.

Författarens egna erfarenheter av logganalyser ger vid handen att den som har till uppgift att medverka i analysdelen av ett loggutdrag bör vara medveten om följande:

- Det optimala fallet innebär en perfekt genomförd analys med tillgång till alla relevanta data för att lösa en arbetsuppgift. Så är sällan fallet eftersom en logganalytiker oftast inte har fullständig förståelse för problemet eller tillgång till alla relevanta data.

- En mer realistisk ansats är att logganalytikern får tillgång till den mängd data som denne anser sig behöva för att kunna genomföra en aktuell arbetsuppgift. Nackdelen med denna ansats är att analysresultatet kommer att stå i nivå med analysledarens förmåga att förstå problemet. Om logganalytikern inte förstått problemet fullt ut blir lösningen inte bättre än vad dennes förmåga att förstå problemet medger.

- Ytterligare en inskränkning från det optimala är att logganalytikern inte får tillgång till all den information som denne anser sig behöva. Detta kan t.ex. bero på att man inte förstår att tillgängliga data är relevanta. Den information som man kommer att använda sig i detta fall överensstämmer då inte med logganalytikerns kravspecifikation eller med den information som är tillgänglig.

5.4.1 Logganalysen

För att kunna utläsa rätt informationsvärde av loggposterna i ett loggutdrag krävs att de data som loggutdraget består av är korrekt och har ett högt sanningsinnehåll. Detta eftersom ett loggutdrag bestående av korrekta loggar kräver datakvalitet då datakvaliteten är kopplad till loggutdragets sanningsinnehåll.

Ett loggutdrag kan innehålla många fler parametrar än bara ett systems loggar. När så sker kallar vi detta i denna uppsats för ett utökat loggutdrag. Denna del utgör vårt förslag för hur morgondagens logganalyser skall gå till. Utan att föregå innebörden av ett utökat loggutdrag är det författarna åsikt att det inte möjligt att värdera bevisvärdet av den information som man kan läsa ur loggutdraget om man samtidigt inte känner till hur den tekniska och administrativa miljön ser ut hos den organisation som levererat loggutdraget.

Exempel på andra parametrar som kan ingå i ett utökat loggutdrag är val av autenticering för identifiering och auktorisation samt vilka administratörer som har åtkomst till systemets olika loggar. Därmed kan man se varje parameter i det utökade loggutdraget som data. Under analysen ges dessa parametrar ett informationsvärde genom den tolkning och värdering som logganalytikern gör av materialet. Analysen resulterar i ett analysresultat där miljön kring loggutdraget sammanställs. Analysresultatet kan sedan ingå som en del i förundersöknings-protokollet. Tillsammans med övrig information som framkommit under förundersökningen är det möjligt att göra en bedömning av bevisvärdet av loggutdraget genom att bedöma i vilken grad dess sanningsinnehåll är korrekt.

I detta arbete måste man komma ihåg att det är svårt att genomföra den optimala logganalysen eftersom det kräver att analytikern har fullständig förståelse för problemet och tillgång till alla data. I detta ingår även att logganalytikern förstår att den datamängd som finns tillgänglig är av betydelse för analysen. Grundkravet för alla data är att tillgängliga data är korrekta till sitt sanningsinnehåll. Att ha förståelse för att kunna ifrågasätta det är en del av den kunskap analytikern måste ha för att komma i närheten av en bra genomförd analys.

Vi kommer därför fram till att logganalytikerns kunskap och erfarenhet kommer att påverka resultatet av logganalysen eftersom det är denne som läser ut ett informationsvärde av all sammanställda data som ett utökat loggutdrag innebär.

6. Teoretisk referensram: Hot mot datakvalitet

Under de senaste åren har avancemanget inom data- och kommunikationsteknologi medfört ökade användarkrav inom samtliga områden som täcks av dessa begrepp. Som en konsekvens av detta har användare och organisationer som nyttjar dessa tekniker blivit mer och mer beroende av de tjänster som tillhandahålls i informationssystemen.

Med anledning av de många olika komponenter, resurser och användare som förekommer i ett datoriserat nätverk har det lett till att nätverken blivit mål för attacker och otillåtna operationer, vilket medfört att begrepp som integritet och skydd av resurser har blivit vikiga aspekter att ta hänsyn till. Allt fler datoriserade system, med sina tillhörande komponenter, distribueras ut inom organisationerna varefter de länkas ihop med tidigare system till en arkitektur som tillhandahåller en mängd olika tjänster åt användarna. Sådana system kallas vanligtvis för distribuerade system eftersom en enkel arbetsuppgift kan resultera i operationer mellan processer som exekveras på flera olika system i nätverket. Funktionen för olika operationer ligger således spridd bland komponenterna i nätverket och är inte alltid centraliserad till en enda enhet.

Det internationella ramverk för säkerhet i distribuerade system är OSI-modellen, vilken vi beskriver under den teoretiska referensramen ”Teknik”. Målet med OSI-modellen är att tillhandahålla en generell beskrivning för överföring av signaler (kommunikation) mellan olika system så att en tillförlitlig kommunikation mellan applikationer och processer kan tillhandahållas. För att detta skall vara möjligt krävs det att man ständigt ser över vilka säkerhetstjänster och protokoll som måste användas för att kunna skydda de resurser och de data som utbytes mellan kommunicerande system [Muftic et al, 1993].

6.1 OSI-modellens säkerhetsarkitektur

För att de som är ansvariga för att hantera säkerhetsbehoven inom en organisations nätverk skall kunna utvärdera, och välja lämpliga säkerhetsprodukter, krävs det något systematiskt sätt att definiera säkerhetsbehoven och komma fram till vilka lösningar som krävs för att täcka dessa. X.800 standarden (security Architecture for OSI) definierar ett sådant systematiserat angreppssätt. Eftersom X.800 standarden utvecklades som en internationell standard så har ett flertal leverantörer tagit fram säkerhetslösningar som svarar mot X.800 standardens strukturerade definitioner av säkerhetstjänster och mekanismer [Stallings, 2003].

X.800 standarden fokuserar på begrepp som attacker mekanismer och tjänster. Dessa kan definieras enligt följande:

Attack	*Ett angrepp mot systemet som kan härledas från ett identifierat hot.*
Hot	*Ett hot är en potentiell fara som kan exponera en identifierad sårbarhet.*
Säkerhetsattack	*Vilket angrepp som helst som äventyrar säkerheten av informationen hos en organisation.*

Säkerhetsmekanism *En mekanism som är designad för att upptäcka, förhindra eller återställa en skada efter en attack.*

Säkerhetstjänst *En tjänst som ökar säkerheten hos data som processas och överförs inom en organisation. Tjänsterna är avsedda att möta säkerhetsattacker och använder sig av en eller flera säkerhetsmekanismer för att tillhandahålla aktuell tjänst.*

6.2 Attacker mot data i ett nätverk

Det finns ett antal säkerhetsrelaterade attacker som kan riktas mot den information och de resurser och som finns i ett nätverk. Dessa delas enligt RFC 2828 och X.800 standarden in i termerna *passiva och aktiva attacker* [Stallings 2003].

6.2.1 Passiv attack

Passiva attacker sker till sin natur genom att tjuvlyssna eller övervaka överföringar inom nätverket. Målet med denna typ av verksamhet är att inhämta information ur det material som överförs. Passiva attacker är svåra att upptäcka eftersom de inte påverkar någon del av den trafik som skickas inom nätverket [Stallings, 2003]. Ett sätt att skydda sig mot denna typ av attacker är att använda sig av kryptering. Det kan göras genom att tunnla trafiken så som man gör i en VPN (Virtual Private Network) lösning. Vi går inte närmare in på denna lösning annat än att VPN, tillsammans med IPSec (IPSecurity), är ett effektivt sätt att skydda informationen som skickas mellan olika nätverk. Detta eftersom VPN ESP[18] i tunnel mode, kapslar in hela meddelandet från applikationsnivån och tillhörande TCP- och IP huvud i ett nytt IP paket. Detta sker på gateway nivå varför en trafikanalys endast kommer att se trafik som är adresserad mellan två gateway på respektive LAN (Local Area network). Det innebär att all information som visar avsändare och mottagare på respektive lokala nätverk inte går att utläsa.

Två typer av passiva attacker är ”avslöjanden om meddelandens innehåll” och ”trafikanalys”.

6.2.1.1 Avslöjanden om meddelandens innehåll (Avlyssning)

Denna typ av passiv attack kan ta sig former som avlyssning av ett telefonsamtal eller avlyssning av nättrafiken så att innehållet i ett e-postmeddelande eller innehållet i överförda filer kan snappas upp. Informationen röjs därför till en obehörig person.

6.2.1.2 Trafikanalys

Kan en angripare inte komma åt innehållet i ett meddelande kan denne under vissa förutsättningar få ut en del information av innehållet i de pakethuvuden som skapas under paketens vandring nedåt i OSI-modellens protokollstack. Sådan information är i klartext även om meddelandet i sig skulle vara krypterat. Allt beror på var någonstans i stacken man satt in krypteringsfunktionen (se närmare beskrivning om kryptering i den teoretiska referensramen angående teknik).

[18] IPSec specifikationen består av ett antal dokument. De viktigaste av dessa utgörs av RFC 2401, FRC 2402, FRC 2406 och FRC 2408 [Stallings, 2003]. Att tunnla trafiken innebär generellt att man kapslar in ett paket i ett annat paket. Med ESP (Encapsulating Security Payload) kapslad det ursprungliga IP-pakete in i ett nytt varvid hela innehållet i det ursprungliga paketet krypteras.

Information som kan läsas ut ur pakethuvudena är källa, mottagare, meddelandets längd, typ av applikation som används på applikationsnivå, IP-adress och MAC-adress m.m. Genom analys av sådana data kan en angripare läsa ut mönster i trafiken som ger svar på frågor när viss information sänds och vem som är avsändare och mottagare.

6.2.2 Aktiv attack

En aktiv attack innebär att en angripare modifierar innehållet i de dataströmmar som flödar i nätverket eller skapar falska paket. Dessa angreppssätt kan delas upp i fyra kategorier: maskerad, reply, modifiering och förnekande av tjänst (DOS).

6.2.3 Maskerad

En maskerad attack sker när en entitet (användare, process) utger sig för att vara någon annan entitet. En maskerad attack föregås vanligtvis av någon av de andra aktiva attackerna innan själva maskerad attacken genomförs. Exempel på detta är när användaren först sniffar nätverket för att komma åt autenticeringsdata (credentials). Dessa data kan även spelas in för att sedan användas i en reply attack.

6.2.4 Reply

Genom en passiv attack kan en angripare spela in trafik genom avlyssning. Denna information kan sedan användas för att lura BKS-funktioner[19] och därigenom uppnå obehörig åtkomst till ett system genom att angriparen nu kan utge sig för att vara en behörig användare. Detta innebär att angriparen lurar den kontrollmekanism som fastställer åtkomsträttigheterna för en användare genom att t.ex. skicka inspelad trafik innehållande sådana värden att denne kan komma åt resurser i ett system som annars vore oåtkomliga.

6.2.5 Modifiering av meddelanden

Detta angreppssätt innebär att en angripare kan förändra delar av ett legalt meddelande som transporteras i nätverket. Det innebär även att angriparen kan försena eller förändra innehållet i meddelandet som snappats upp. Syftet kan vara att skapa en otillåten effekt genom att t.ex. ändra ett innehåll i ett meddelande från ”Tillåt Mr Lindblom att läsa all sekretessbelagd information om Mr Falk” till ”Tillåt Mr Ericsson att läsa all sekretessbelagd information om Mr Falk”. Ett annat exempel är att byta ut, ta bort eller lägga till vissa delar i en loggpost så att det ser ut som om Lindblom loggat in i systemet i stället för Falk.

6.2.6 Förnekande av tjänst (DOS)

Denna typ av attack förhindrar eller hämmar en användare att nå en viss tjänst. Den här attacken kan ha ett speciellt mål som t.ex. att blockera trafiken till tjänst som tillhandahåller loggfunktionen.

[19] BKS - BehörighetsKontrollSystem

6.3 Säkerhetstjänster

RFC 2828 definierar en säkerhetstjänst som en process- eller kommunikationstjänst som tillhandahålls av systemet för att ge en specifik form av skydd mot systemets resurser. X.800 standarden delar dessa tjänster i fem kategorier och fjorton specifika tjänster (services).
Delar av de säkerhetstjänster som ingår i X.800 standarden beskrivs närmare i den teoretiska referensramen om teknik. Vi har valt att inte foga in dessa i detta avsnitt eftersom de delar som beskrivs i X.800 standarden endast beskrivs till sin funktion. I den tekniska referensramen beskriver vi dem på ett sätt som är mer anpassat till uppsatsens mål.

6.3.1 Autenticering

Autenticeringstjänsten skall försäkra att kommunikationen är autentisk. I de fall där trafiken utgörs av ett enstaka meddelande, som en varning eller en larmsignal, innebär funktionen att försäkra mottagaren om att meddelandet kommer från den avsändare som framgår av meddelandet. I sådana fall där kommunikationen är dubbelriktad innebär det två saker. För det första tillhandahåller tjänsten en försäkran om att avsändaren och mottagaren är dem som de utger sig för att vara. För det andra innebär tjänsten en försäkran om att förbindelsen mellan de två parterna innebär att en tredje person inte kan maskera sig för att utge sig för att vara en av de två legala parterna, något som vanligtvis benämns som Man-In-the-Middle.

6.3.1.1 Autenticering av en jämlik entitet

Denna funktion tillhandahåller en funktion för att bestyrka identiteten på den man kommunicerar med (peer entity). Funktionen används vid upprättandet av kommunikationen och tillhandahåller en möjlighet till förtroende så att en entitet inte utger sig för att vara någon annan (maskerad) eller en oauktoriserad återspelning (reply) av en tidigare genomförd (inspelad) kommunikation.

6.3.1.2 Autenticering av data

Denna metod tillhandahåller en funktion för att bestyrka att källan till en viss mängd data är den som utger sig för att vara källan. Funktionen i sig innebär inte skydd mot duplicering eller modifiering av data.

6.3.2 Accesskontroll

Accesskontroll i nätverk innebär att tjänsten ger en möjlighet att begränsa och kontrollera åtkomst till tjänster som applikationer som körs på servrar. För att förhindra för utomstående att nå sådana resurser som denne inte har rätt till krävs en identifiering av alla entiteter som försöker nå en sådan resurs. På så sätt kan rättigheter skräddarsys för varje användare.

6.3.3 Sekretess

Sekretess innebär att man krypterar informationen så att den därmed ges ett skydd mot passiva attacker som avlyssning. Kryptering kan ske på olika nivåer i OSI-modellen, och beroende på var någonstans man sätter in denna skyddsåtgärd kommer det att få olika effekter (se närmare i den teoretiska referensramen angående teknik). Kryptering kan omfatta all användardata ner till att endast omfatta vissa meddelanden eller vissa delar av ett meddelande. Vill man, utöver användardata, även skydda sig mot trafikanalyser måste man välja metoder som skyddar det ursprungliga IP-huvudet med käll- och destinationsadress, t.ex. med den metod som beskrivs under avsnittet om passiva attacker.

6.3.4 Integritet

Liksom vid kryptering kan integritet omfatta hela meddelandet eller endast vissa meddelanden eller delar av ett meddelande. En kommunikationsorienterad integritetstjänst som hanterar strömmar av meddelanden försäkrar att meddelanden som mottagits på respektive sida av kommunikationen är fri från duplicering, modifiering, förändring i ordningsföljd och omspelning (reply). När det gäller skydd mot omspelning av inspelade meddelanden bygger det på en teknik med slumptal och tidstämplar. Ett visst slumptal är bara giltigt under en viss tidsintervall, vilket innebär att mottagarsystemet känner igen ett slumptal som den tidigare mottagit om tidsangivelsen för detta ännu inte gått ut. Alla övriga slumptal som på detta sätt känns igen kommer att tolkas som reply attacker. Vi går inte in på den tekniken närmare än så.

Man kan göra en distinktion mellan en integritetstjänst med eller utan skydd för återvinning (recovery). Eftersom integritetstjänster vanligtvis relaterar till aktiva attacker är vi egentligen ute efter att upptäcka förändringar så att detta kan förhindras. Om en överträdelse av integriteten hos ett meddelande upptäcks kan det räcka med att vi nås av ett meddelande om detta varvid en mänsklig åtgärd tar vid och vidtar erfordriga åtgärder. Ett annat alternativ är att bygga in mekanismer som återställer förlust av data. Det sistnämnda är oftast att föredra. I grund och botten går tjänsten ut på att ett meddelande som mottagits garanterat inte har förändrats under överföring.

6.3.5 Oavvislighet (nonrepudiation)

En tjänst som tillhandahåller oavvislighet förhindrar att antingen den sändande eller mottagande parten kan förneka att ett meddelande sänts. Mottagaren kan med denna teknik bevisa att den påstådda avsändaren sänt meddelandet. Samtidigt kan sändaren av ett meddelande bevisa att den påstådda mottagaren faktiskt mottagit meddelandet.

6.4 Säkerhetsmekanismer

Figur 3 listar delar av de säkerhetsmekanismer som definieras i X.800 standarden. Mekanismerna är hämtade ur X.800 standarden, men den svenska översättningen är hämtad ur SIS HB 550, 2003 [SIS HB 550, 2003].

Specifika säkerhetsmekanismer (X.800)
Kryptering Omvandling av klartext till kryptotext genom ett krypteringssystem och aktuell kryptonyckel i syfte att förhindra obehörig åtkomst av konfidentiell information
Digital signatur Omvandling av ett meddelande på ett sätt som endast användaren kan utföra och som tillåter mottagaren att kontroller meddelandets äkthet, innehåll och avsändarens identitet.
Åtkomstkontroll Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till olika resurser.
Riktighet Egenskaper att informationen inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats.
Autenticeringsinformation Information som används för att fastställa en uppgiven identitets giltighet.
Traffic Padding Insättandet av bitar i gap av dataströmmar i syfte att frustrera och försvåra försök till trafikanalys.
Routing kontroll Möjlighet att välja vägval för routing för vissa datapaket och möjlighet till att ändra routing val när säkerhetsrelaterade överträdelser är att vänta.
Notarization Användandet av en pålitlig tredjepart för att försäkra vissa egenskaper hos data som skickas i nätverket.

Figur 3 Delar av säkerhetsmekanismer ur X.800 standarden**.** Figuren bygger på en bild hämtad ur Network Security Essentials [Stallings 2003].

Tabellen i figur 4 baseras på X.800 standarden och visar relationerna mellan säkerhetstjänster och säkerhetsmekanismer. Hoten som finns mot ett nätverk möts på så sätt med de mekanismer som ingår i de olika säkerhetstjänsterna.

	Mekanismer						
Tjänst	**Kryptering**	**Digital signatur**	**Åtkomst-kontroll**	**Autenticerings-information**	**Traffic padding**	**Routing kontroll**	**Notarization**
Autenticering av en jämlik entitet	JA	JA			JA		
Autenticering av data	JA	JA					
Åtkomstkontroll			JA				
Riktighet	JA					JA	
Riktighet av trafikflöde	JA				JA	JA	
Dataintegritet	JA	JA	JA				
Oavvislighet		JA	JA				
Tillgänglighet			JA	JA			

Figur 4 Relationen mellan säkerhetstjänster och säkerhetsmekanismer [Stallings, 2003].

6.5 Sammanfattning

Genom de hot som identifieras i X.800 standarden finner vi att oskyddad trafik i ett nätverk är öppen för ett flertal angreppssätt. De säkerhetstjänster och säkerhetsmekanismer som standarden definierar är motåtgärder för att möta hoten mot datakvaliteten inom organisationens nätverk. I denna uppsats är det organisationens loggdata som skall skyddas, men hoten och motåtgärderna är naturligtvis tillämpbara på allt data i organisationens nätverk.

Vill en organisation skapa en hög nivå av informationssäkerhet kan detta ske med hjälp av de säkerhetstjänster och säkerhetsmekanismer som vi tagit upp under X.800 standarden.

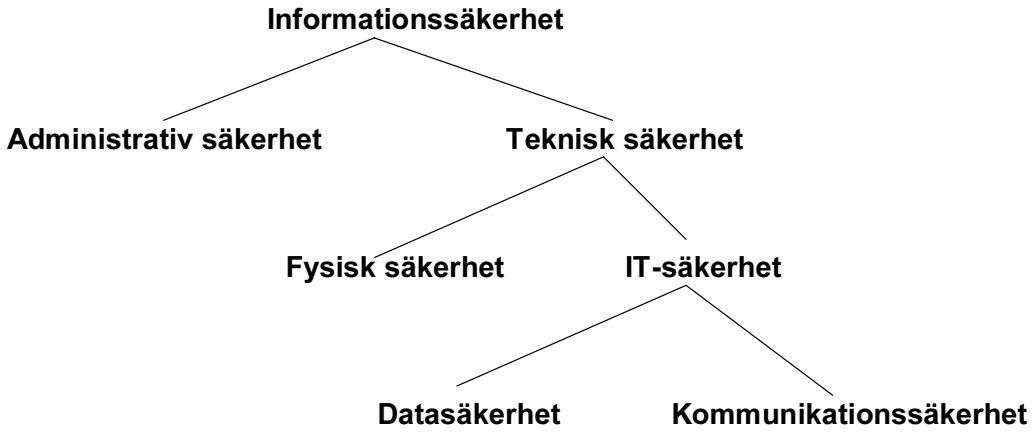
7. Teoretisk referensram: Informationssäkerhet

Den teoretiska referensramen angående informationssäkerhet syftar till att ge läsaren en förståelse för vilka grundläggande begrepp som normalt används när man diskuterar informationssäkerhet. Ett av begreppen man talar om när det gäller informationssäkerhet är spårbarhet. Det är hanteringen och värderingen kring denna del av informationssäkerheten som uppsatsen handlar om. För att detta skall vara möjligt måste organisationens information skyddas på ett sådant sätt att den inte kan förändras eller kommas åt av obehöriga. Av den anledningen är även begrepp som sekretess, oavvislighet och riktighet (integritet) av största vikt för att över huvud taget ha någon nytta av spårbarheten inom organisationens system.

De begrepp som definieras i figur 5 utgör grunden för att ett informationssystem skall kunna leverera ett material som kan generera ett pålitligt analysresultat av ett loggutdrag. De funktioner en organisation bygger in under respektive del har som mål att säkra de grundläggande begreppen tillgänglighet, sekretess, riktighet och spårbarhet. Det är detta som begreppet informationssäkerhet ytterst står för.

7.1 Allmänt om informationssäkerhet

Begreppet informationssäkerhet är något som, beroende på ändamål, kan beskrivas på olika sätt. Den klassiska bilden av informationssystem visas i figur 5.



Figur 5 Begreppet informationssäkerhet med utgångspunkt från skyddsåtgärdernas miljö [SIS HB 550, 2003].

När man diskuterar begreppet informationssäkerhet utgår man från att delar av informationen inom organisationen, i något avseende, är kritisk. Beroende på vilken organisation som berörs kommer dessa att definiera olika verksamhetskritiska områden och mål som kan skadas om viss information skulle komma obehöriga till del, förstöras, förändras eller göras otillgänglig.

Eftersom information för många organisationer är av central betydelse för att dessa skall kunna bedriva en fungerande verksamhet samt uppfylla sina mål, är det av vikt att informationen kan skyddas mot avsiktliga och oavsiktliga hot. Skyddet av informationen blir därmed en angelägenhet för vilken organisation det än må vara.

När vi talar om utnyttjandet av en organisations information förutsätter det i detta sammanhang tillgång till en fungerande teknisk struktur, d.v.s. ett IT-system. Skyddet av organisationens informationsbehandlande tekniska system benämns ofta som IT-säkerhet. Begreppen i figur 5 beskrivs i termologi för informationssäkerhet [SIS HB 550, 2003] på följande sätt.

Datasäkerhet	*säkerhet beträffande skydd av datorsystem och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling.*
Informationssäkerhet	*säkerhet beträffande informationstillgångar (information, program, tjänster och fysiska tillgångar) rörande förmågan att upprätta önskad sekretess (konfidentialitet), riktighet, tillgänglighet, spårbarhet och oavvislighet. Informationssäkerhet delas upp i administrativ säkerhet och teknisk säkerhet.* *Informationssäkerheten består antingen av administrativ säkerhet eller av teknisk säkerhet. Följer man den tekniska säkerheten når man begreppen fysisk säkerhet och IT-säkerhet.*
IT-säkerhet	*säkerhet beträffande IT-system med förmågan att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.*
Kommunikationssäkerhet	*säkerhet i samband med överföring av data.*

När begreppet system används omfattar denna term normalt alla tekniska komponenter i ett IT-system. Det är även denna definition av begreppet system vi använder i uppsatsen.

7.2 Informationssäkerhet vs förundersökning

En förundersökning, som helt eller delvis bygger på IT-relaterad bevisning, kommer ursprungligen från en organisation som har sin egen nivå av informationssäkerhet. En organisation som har en hög nivå av informationssäkerhet har bättre förutsättningar att skydda sina data från de hot som diskuteras under den teoretiska referensramen angående hot mot datakvalitet i nätverk. En organisation med lägre nivå av informationssäkerhet kommer att ha sämre förutsättningar att skydda sina data mot dessa hot.

En organisation med hög informationssäkerhet har en administrativ och teknisk säkerhet som klarar av att säkerställa organisationens data i termer av tillgänglighet, sekretess, riktighet, spårbarhet och oavvislighet. Kan dessa områden säkras har organisationen de förutsättningar som krävs för att kunna ta fram en IT-relaterad bevisning som är skyddad mot förändring och insyn. Informationssäkerhet är en förutsättning för att logganalysen skall kunna leverera ett analysresultat som ger åklagaren de förutsättningar som behövs för att denne skall kunna bevisvärdera organisationens loggutdrag.

En viktig fråga som man måste ställa sig när man diskuterar loggutdragens riktighet är om autenticeringen är tillräcklig stark för att man skall kunna lita på att händelser som loggats verkligen utförts av den som loggen anger. Om så inte är fallet spelar det mycket liten roll hur mycket resurser organisationen lagt ner på att stärka sin informationssäkerhet eftersom allt redan faller på det första steget. Kan vi inte lita på att det verkligen är person A som ligger bakom trafiken som loggutdraget visar så har vi mycket liten nytta av detta.

En organisation med en lägre nivå av informationssäkerhet kommer att ha brister inom något av de grundläggande begreppen som ryms inom området informationssäkerhet. Av den anledningen finns det en risk för att de hot som vi diskuterat under den teoretiska referensramen kan realiseras. Beroende var någonstans i organisationen denna brist finns gör att bristen kan påverka logganalysen på ett eller annat sätt, och i en negativ bemärkelse.

Vad som till slut avgör om en organisation har en tillräckligt hög informationssäkerhet är svårt att i förväg avgöra. I de fall där organisationens loggutdrag resulterar i en värdering som resulterar i att loggutdraget har ett bevisvärde kan detta avgöras i domstol. Fälls den misstänkte mot sitt nekande på loggutdraget som grund är detta en bekräftelse på att informationssäkerheten inom organisationen är tillräckligt hög inom de områden som berör loggutdraget och dess hantering. Frias den misstänkte är det en förhoppning att domstolen anger varför så att organisationen kan ta lärdom om var det brustit någonstans i dess informationssäkerhet.

Eftersom loggutdragen kommer att ingå som en del i en förundersökning innebär det att värderingen av dess bevisvärde kommer att kunna värderas på olika sätt beroende på vad som i övrigt framkommit under utredningen. Om loggutdraget utgör den enda bevisningen mot den misstänkte måste man ställa mycket stora krav på informationssäkerhet för att loggutdragen ensamt skall kunna svara upp mot sitt innehåll.

8. Teoretisk referensram: Teknik

Den teoretiska referensramen syftar till att ge läsaren grund att stå på när det gäller att tillgodogöra sig vår presentation av problemen kring loggning. I avsnittet nedan presenteras en genomgång av IT-säkerhetsrelaterad teknik.

Huvudsyftet med att ta med en teknisk referensram i denna uppsats är att försöka förklara för läsaren varför man inte utan vidare kan lita på de uppgifter som loggas i ett loggutdrag. IP-adress, datornamn är t.ex. sådana uppgifter som kan ändras på en klient så att dessa värden loggas i stället för de ursprungliga. Med den förteckning som i allmänhet finns inom större organisationer, och som binder enskilda individer till vissa IP-nummer eller datornamn pekar loggarna genom dessa förändringar ut fel person som ansvarig för trafiken. Att förstå vilka loggposter som kan vara förändrade är en kombination av vilken nivå av informationssäkerhet organisationen har samt vilken kunskap den eller de personer har om teknik och organisationens tekniska och administrativa lösningar.

Uppsatsen riktar sig till yrkesgrupper som i sitt arbete kommer i kontakt med IT-relaterad bevisning. De flesta av dem är inte tekniker, varför denna del anses som nödvändig. Den är dock begränsad på så sätt att de områden som beskrivs inte beskrivs heltäckande utan endast med målet att ge läsaren en förståelse för de delar vi beskriver.

Eftersom det finns ett antal faktorer att ta hänsyn till när man gör logganalysen är syftet med den tekniska referensramen att läsaren skall få en ”aha” upplevelse när det gäller denna förståelse.

8.1 Allmänt om tekniken i denna referensram

I denna uppsats återkommer vi till termer som lagring, transport och hantering. Det är tre grundläggande begrepp som är väsentliga för att en organisation skall kunna skaffa sig kontroll av de data som dess loggar kommer att utgöras av. För att kunna förstå delar av den teknik som ligger bakom en loggs transport inom en organisations nätverk, samt vilka komponenter och vilken teknik som kan användas, innehåller uppsatsen en grundläggande tekniks del som tar upp delar av detta teknikområde. Detta är ingen heltäckande beskrivning, utan de delar som vi anser är nödvändiga att känna till för att kunna följa den diskussion vi för i uppsatsen.

8.2 OSI modellen

En av de äldsta modeller som finns för att definiera de olika nätverkslagren och deras protokoll är den så kallade OSI-modellen[20]. Arbetet med att ta fram denna modell påbörjades under 1970-talet under den Internationella standardiseringsorganisationen ISO[21] där syftet med standarden var att ta fram ett ramverk för kommunikation mellan datorer. Dess arbete genererade 1984 det vi i dag kallar för OSI-modellen [Fitzgerald, 1999].

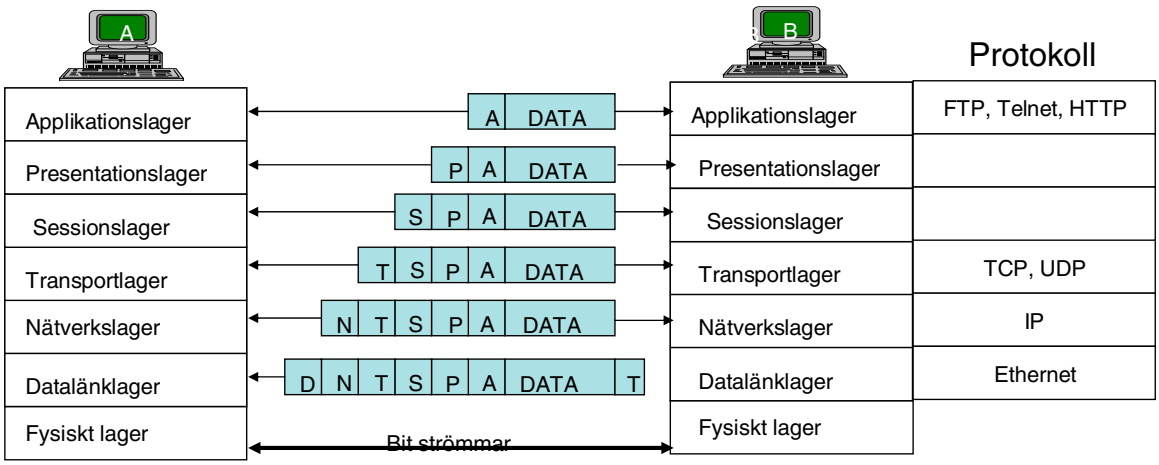
[20] OSI – Open System Interconnection
[21] ISO – the International Standards Organization

OSI-modellen är en modell som förklarar hur kommunikationen mellan två datorer fungerar. Ett av syftena med modellen är att göra systemen öppna för varandra, så att olika system kan använda modellen oberoende av den underliggande arkitekturen. Företagsspecifika system omöjliggör kommunikation med utrustning tillverkade av andra företag och det är just detta som man med OSI-modellen har velat undvika. Man bör observera att OSI-modellen (se figur 6) är just en modell och inte ett protokoll [Burd, 1998].

Varje lager i modellen använder sig av tjänster som tillhandahålls av lagret nedanför. Om man räknar det nedersta lagret, det fysiska lagret, som är det första lagret, innebär det att lager N använder sig av tjänster från lagret N^{-1}. De tjänster som finns implementerade i lager N^{-2} är alltså okända för tjänsterna i lager N [Burd, 1998]. Fördelen med OSI-modellens uppbyggnad är att utrustning som arbetar under ett speciellt skikt kan bytas ut utan att utrustningen i andra skikt behöver påverkas [Hedemalm, 2001].

Kommunikationen mellan två datorer på applikationsnivå är en skenbar kommunikation. För användarna av en applikation som skickar information mellan varandra ser det ut som om de skickar informationen till varandras applikationsskikt. I verkligheten packas informationen om ända ner till det nedersta skiktet (fysiska) innan informationen överförs till mottagarsidan [Hedemalm, 2001].

Anta att dator A vill kommunicera med dator B inom ett nätverk. OSI-modellens uppbyggnad innebär att varje lager i OSI-modellen i dator A kommunicerar med motsvarande lager hos dator B. För att detta skall vara möjligt lägger varje skikt till ett huvud framför datamängden som skall skickas, eller en trailer som läggs till efter datamängden. Informationen i huvudet eller trailern på respektive nivå innehåller protokollspecifik information. Det innebär att ett meddelande som skapas i applikationsskiktet hos dator A kommer att få ett extra huvud för varje nivå nedåt i stacken som meddelandet passerar. På mottagarsidan kommer dator B att läsa protokollinformationen i varje paket på samma nivå i stacken som det skapades i hos dator A. Detta gör att den information som skapas på en nivå hos dator A är adresserad till samma nivå hos dator B. Det innebär vidare att varje nivå bara är intresserad av den information som är aktuell för just den egna nivån. Vad som skapats på applikationsnivån kommer endast att läsas och behandlas av motsvarande skikt på mottagarsidan [Pohlmann, 2001].



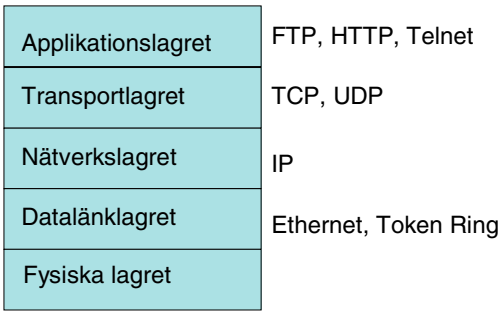
Figur 6 OSI modellen. Figuren är skapad av författarna men bygger på delar av en bild hämtad ur boken Security in Computing [Pfleeger, 2000].

Nedan går vi kortfattat in på den så kallade TCP/IP-modellen, vilket är ett alternativ sätt att visa vilka skikt som används i en protokollstack. I denna uppsats kommer vi däremot mer konsekvent att använda oss av OSI-modellen när vi refererar till en modell.

8.3 TCP/IP modellen

OSI-modellen är endast en teoretisk modell för att förenkla förståelsen av datakommunikationen mellan datorer. Då det i praktiken visat sig svårt att skapa användbara protokoll som till fullo följer OSI-modellen har en övergång skett till att det vanligaste protokollet idag är TCP/IP[22] protokollen. TCP/IP modellens lager avviker från OSI modellen [Hedemalm, 2001]. Det har även visat sig vara svårt att integrera TCP/IP med ett nätverk som strikt baseras på OSI [Burd, 1998].

Jämför man TCP/IP modellen, eller Internet modellen som den även kan kallas, med OSI-modellen visar det sig att TCP/IP modellen inte täcker de lägre lagren från OSI modellen. Detta beror på att designen av TCP/IP modellen använder sig av existerande standarder som Ethernet och Token Ring för det fysiska lagret och datalänk lagret [SYBEX, 2002]. I figur 7 visas en modifierad modell av TCP/IP-modellen som även innehåller de två nedersta skikten. De visar att det finns olika TCP/IP-modeller att referera till.



Figur 7 En modifierad TCP/IP modell med vanliga protokoll. Bilden baserar sig på en Internetkälla [Web 1].

8.4 Terminologi

Beroende vilka protokoll vi kommer att diskutera i denna del så benämns de olika datapaketen med olika termer. Generellt används annars följande termer.

Enligt RFC 1180 är en drivrutin är en programvara som kommunicerar direkt med nätverkslagrets utrustning medan en modul är en programvara som kommunicerar direkt med drivrutiner, nätverksapplikationen eller med andra moduler. RFC 1180 delar upp datamängden på följande sätt.

- **Datalänk nivå (Ethernet)** Ramar (frames)
- **Mellan Ethernets drivrutin och IP-modulen** IP-paket
- **Mellan IP-modul och UDP-modul** UDP-datagram
- **Mellan IP-modulen och TCP-modulen** TCP-segment
- **På applikationsnivå** Applikationsmeddelande

[22] TCP/IP – Transmission Control Protocol and Internet Protocol

För enkelhetens skull kommer vi i denna uppsats att prata om datapaket oavsett var någonstans i protokollstacken vi befinner oss i.

8.5 Protokoll

All kommunikation mellan datorer sker med hjälp av olika protokoll. Protokollen är ett slags regelverk som anger för en sändande och mottagande dator hur informationen skall skapas för att den skall vara förståelig på mottagarsidan. De flesta av oss känner inte till om kommunikationen mellan den egna datorn och andra datorer sker över kopparkabel, optisk fiber, satellit eller rent av en kombination av dessa. Orsaken till att vi inte behöva ta hänsyn till sådana omständigheter möjliggörs av att själva kommunikationen är skild från det medium som vi använder för att överföra informationen. Genom att använda oss av protokoll som tillåter oss att tänka på en högre nivå av kommunikation behöver vi inte bry oss så mycket om hur kommunikationen går till längre ner bland protokollen i OSI-modellen. Hur det går till döljs bland hård- och mjukvara på både den sändande och mottagande datorn. Den mjuk- och hårdvara som är involverad i denna process kallas för protokollstackar. Dessa utgör i sig en arkitektur uppdelad i olika lager [Pfleeger, 2000] (se figur 6).

OSI och TCP/IP är två exempel på protokollstackar som fungerar på detta sätt. Inom OSI och TCP/IP modellerna är protokoll en sorts språk som används för att kommunicera inom ett skikt i modellen hos den sändande och mottagande datorn. Det innebär att ett skikt i modellen kommunicerar med samma skikt på sändande och mottagande dator. Styrkan med ett protokoll är att det kan användas för kommunikation oavsett vilka faktiska kommunikationsmetoder som används. Så är fallet även med ett vanligt språk. Om vi betraktar det svenska språket som ett protokoll så kan vi kommunicera med varandra med hjälp av reglerna i protokollet som det svenska språket innehåller antingen muntligt, per brev eller via telefon. Dessa olika sätt att kommunicera utgör olika former av kommunikationsmetoder. Vi kan kommunicera via dessa hjälpmedel, men däremot kan vi inte kommunicera direkt med telefonen eller papperet. Samma sak gäller för protokollen i t.ex. OSI-modellen. Protokollet ligger till grund för kommunikationen mellan den sändande och mottagande parten, men fungerar således inte som en kommunikation till de underliggande lagren, något som här kan jämföras med telefonen eller brevet [Hedemalm, 2001].

8.6 Transportnivå (Nivå fyra i OSI-modellen)

På transportnivå diskuterar vi i denna uppsats två protokoll, TCP (Transmission Control Protocol) och UDP (User Datagram Protocol). Den största skillnaden mellan dessa protokoll är att TCP står för en förbindelseorienterad överföring medan UDP är förbindelselös. Att UDP är förbindelselös innebär att protokollet inte kräver bekräftelse på att ett paket kommit fram. Båda använder sig av portar, men man skall komma ihåg att dessa står för olika saker. T.ex. kan samma port anropas på en viss IP-adress med TCP och UDP samtidigt [Mitrovic, 2003]. Två helt separata tjänster kan på så sätt dela på samma portnummer.

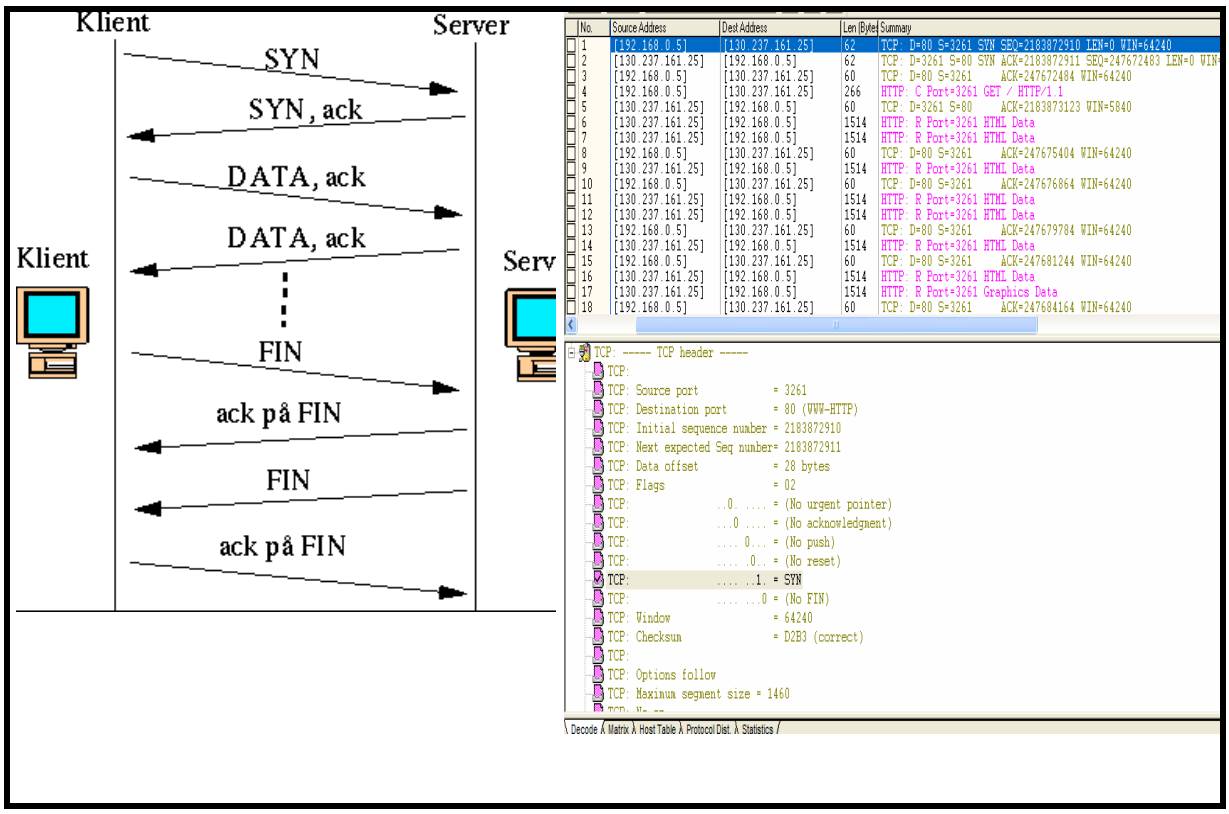
8.6.1 TCP protokollet

TCP bryter ner data i mindre paket, numrerar dem och försäkrar att varje paket på ett pålitligt sätt transporteras till mottagande dator. Där packar TCP upp varje paket och sätter ihop dem i rätt ordning. TCP står således för en säker förbindelse mellan två datorer. För att kunna garantera detta är TCP-protokollet designat för att klara av att återställa förlorad, skadad eller redundant data.

När en TCP anslutning upprättas sker en process som utförs i tre steg, vilket även kallas för TCP:s handskakningsprocess [McClure et la, 2003].

1. Det första steget återges i figur 8 som visar hur den sändande datorn (klient) skickar ett SYN-paket, vilket innebär att SYN-flaggan i TCP huvudet är satt.
2. Det andra steget är att den mottagande dator (server) svarar med att skicka ett SYN/ACK paket, vilket innebär att flaggorna SYN och ACK är satta i TCP huvudet i paketet som returneras. Detta försätter servern i ett SYN_RECV, även kallat för ett halvöppet läge, vilket innebär att servern förbereder sig för en uppkoppling genom att säkra ett antal resurser inför den kommande uppkopplingen.
3. Det tredje steget innebär att klienten avslutar anslutningen genom att skicka tillbaka en ACK, varvid anslutningen mellan klient och server är upprättad.

Varje paket (segment på TCP-nivå) tilldelas ett sekvensnummer som indikerar paketets plats i den sekvens av paket som kommer att sändas från den sändande datorn. Sändande och mottagande dator har sina egna sekvensnummer eftersom den mottagande datorn blir en sändande dator i trafiken tillbaka. Dessa sekvensnummer är avgörande för att mottagande datorn skall kunna bygga ihop paketen ingen så att de kommer i rätt ordning, oavsett vilken ordning de anländer i. Ett paket som av någon anledning försvunnit längs vägen, eller som av mottagande dator inte godkänns, innebär att sändande dator inte får någon ACK (acknowledge) för detta paket. Det innebär att den sändande datorn skickar om samma paket, med samma sekvensnummer som det förlorade paketet hade. En ACK består av ett eget nummer och indikerar vilket paket (segmentnummer) som ges en ACK [Panko et al, 2004]. Utöver sekvensnummer och ACK:ar använder sig TCP av kontrollsummor för att garantera att inga data har förändrats under vägen. Denna checksummekontroll är något som upprepas på datalänknivå [Fitzgerald, 1999].



Figur 8 Visar inledande och avslutande TCP-trafik genom sniffning av nätverkstrafiken mot adressen www.dsv.su.se. Den vänstra delen av bilden visar schematiskt hur TCP sätter upp och avslutar en förbindelse. [Web 2].

8.6.2 Portar

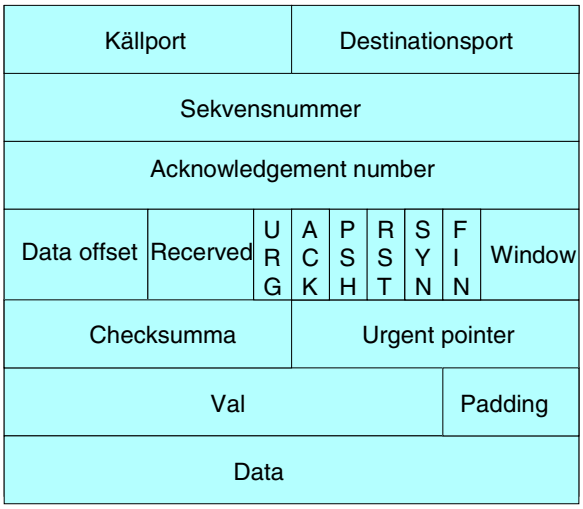
Ett viktigt koncept som återkommer när man talar om kommunikationsprotokoll som TCP och UDP på transportnivå är begreppet portar. Dessa är väsentliga i kommunikationen mellan olika datorer. En server måste klara av att kommunicera med många klienter samtidigt. Om inte det vore möjligt skulle en klient lägga beslag på hela serverkapaciteten medan de andra inte skulle ha en chans att nå servern. Det finns även vissa applikationer som behöver kommunicera över fler än en kommunikationskanal, t.ex. FTP[23] (File Transfer Protocol) som arbetar på port 20 och 21 [Pohlmann, 2001].

För att kunna möta kravet på fler kommunikationskanaler har varje dator en uppsättning portar. En dator har i teorin 65.535 (2^{16} - 1) portar, vilka logiskt kan jämföras med ett antal lägenhetsdörrar i ett höghus. Huset har en adress, i datorns värld IP-adress, vilket gör att man på samma gatuadress kan adressera väldigt många lägenheter. Bakom varje port döljer sig en tjänst. Exempel på sådana tjänster är HTTP[24] (Hyper Text Transfer Protocol) som i regel finns bakom port 80 och SMTP[25] (Simple Mail Transfer Protocol) på port 25.

Huvudet i TCP-paketet innehåller bland annat två 16-bitars fält för portnummer (se figur 9). Ett fält för källport och ett fält för destinationsport. När applikationslagret anropar transportlagret via en av sina applikationer kommer TCP-huvudets källport och destinationsport att innehålla värdet av ett heltal.

[23] Protokollet nvänds för att logga in på en annan dator och hämta och skicka filer mellan dessa
[24] Protokollet ligger till grund för överföring av dokument i World Wide Web.
[25] Protokollet är TCP/IP:s protokoll för e-post.

Det innebär att den mottagande datorn, när den packar upp paketet på TCP-nivå, kommer att se till att paketet hamnar hos samma applikation hos mottagaren som det skapades på hos avsändaren [Pohlmann, 2001]. Destinationsporten är även anropsporten på den tjänst som anropas i ett klient – server system



Figur 9 TCP huvudet enligt RFC 793 [Web 11]. Valda fält har av författarna översatts till svenska.

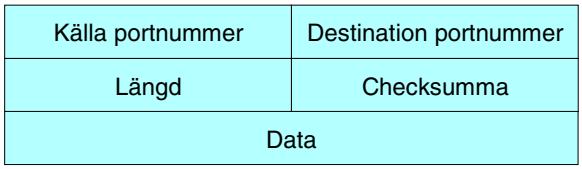
8.6.3 UDP

UDP är ett förbindelselöst kommunikationsprotokoll som på transportprotokollnivå tillhandahåller en envägskommunikation mellan den sändande- och mottagande datorn. Även UDP kan särskilja mellan olika tjänster genom val av portar (se figur 10).

UDP genererar inga ”acknowledgement” transportpaket eller annan information som skulle kunna tala om för den sändande datorn att paketet kommit fram. Det här innebär att protokollet inte är speciellt pålitligt. Då det även är ett protokoll som är lätt att manipulera så bör det i vissa situationer undvikas [Pohlmann, 2001]. Att protokollet ändå används beror på dess låga ”overhead”[26]. Protokollet används för flera välkända protokoll på applikationsnivå. Exempel är SNMP[27] (Simple Network Management Protocol) och TFTP (Trivial File Transfer Protocol) [Web 3]. Ytterligare exempel på användningsområde är DNS-anrop, något som vi går igenom under avsnittet om DNS samt när man vill eftersträva en enkelriktad trafik mellan en sändande och mottagande dator.

Protokollet försöker inte begränsa mängden data som skickas ut av ett applikationsprogram vilket innebär att protokollet inte på något sätt försöker undvika att nätet blir överbelastat. Nätverket kan därmed belastas maximalt varför UDP vanligtvis används som transportprotokoll vid videoöverföring. Om ett eller annat paket försvinner på vägen gör inte så mycket eftersom detta knappast kommer att upptäckas [Web 4].

[26] Innehållet i pakethuvudena som skapas under ett pakets väg nedåt i protokollstacken innehåller olika mycket information. En del av informationen i pakethuvudet används över huvud taget inte, varför mängden onödig information även blir mindre i ett mindre pakethuvud.
[27] SNMP står för Simple Network Management Protocol och är ett enkelt protokoll för nätövervakning. (Därmed inte sagt att nätövervakning är enkelt!) Protokollet är enkelt eftersom det (ungefär som HTTP) bara består av enkla frågor, kommandon och svar [Web 14]



Figur 10 UDP-huvud enligt RFC 768 [Web 12]. Fältnamnen har av författarna översatts till svenska.

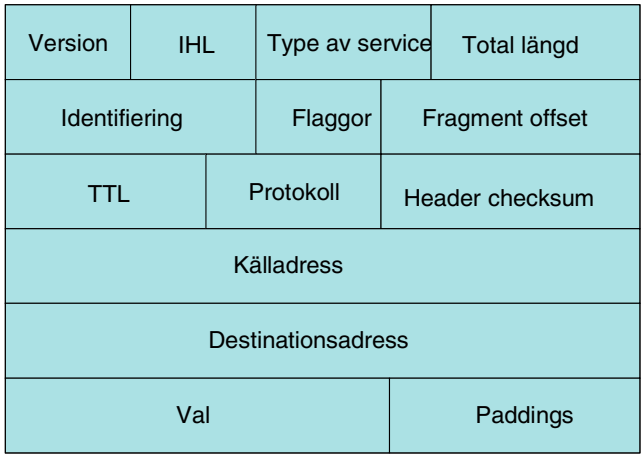
8.7 Nätverksnivå (Nivå tre i OSI-modellen)

I detta arbete kommer vi begränsa oss till att endast gå in på IP-protokollet när det gäller nätverksprotokoll. Övriga protokoll utelämnas därmed.

8.7.1 IP protokollet

IP-protokollet är det protokoll som vanligtvis används inom nätverkslagret. IP-protokollet är ett så kallat förbindelselöst protokoll eftersom paketen som skickas iväg från en dator inte har någon som helst logik inbyggd som meddelar den sändande datorn om paketet lyckats ta sig fram eller inte. Den logiken står TCP för och det är därför som TCP och IP protokollen är så starkt förknippade med varandra [Pohlmann, 2001]. IP lägger på sitt eget huvud på paketen under deras väg nedåt i stacken (se figur 11).

IP-protokollet tillhandahåller routing och adressering (se närmare beskrivning under avsnitten routing och IP-adressering). IP-protokollet används på alla datorer i ett TCP/IP nät när ett paket passerar mellan en avsändande och mottagande dator (t.ex. routrar) eftersom varje paket måste packas upp till IP-nivå för att en dator skall veta om paketet är adresserat till jus denna dators IP-adress eller inte (se figur 6). TCP-protokollet kommer däremot bara att användas på den sändande och mottagande datorn eftersom TCP endast blir involverat när paketen skall skickas vidare eller tas emot från applikationslagret [Fitzgerald, 1999].



Figur 11 IP huvudet enligt RFC 791 [Web 13]. Lämpliga fält har av författarna översatts till svenska.

8.7.2 Statisk tilldelning av IP-adresser

När en dator tilldelas sin nätverksadress (IP-adress) kan det antingen ske manuellt på datorn eller automatiskt via nätverket. Ett sätt är att datorn ges en statisk IP-adress genom att en administratör skriver in datorns IP-adress direkt i datorn. Det innebär att datorn alltid kommer att ha samma IP-adress varje gång den anropar nätverket, även om den bootas om.

8.7.3 Dynamisk tilldelning av IP-adresser

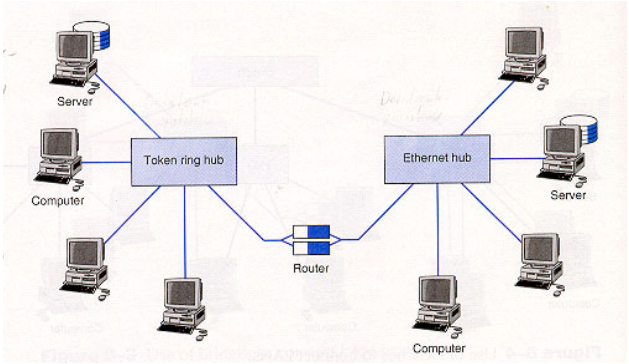
Det andra sättet att tilldela en dator en IP-adress är genom en dynamisk adresstilldelning. Datorn ställs då in i ett läge där den vet om att den kommer att tilldelas en dynamisk IP-adress varje gång datorn accessar nätverket. Med detta slipper man att konfigurera varje dator manuellt.

Bootp (Bootstrap Protocol) och DHCP[28] (Dynamic Host Configuration Protocol) är två vanliga protokoll som används för att underlätta adresseringen av datorer i TCP/IP nät. De fungerar på så sätt att en speciell programvara finns installerad på varje klient som är instruerad att kontakta en bootp eller DHCP server varje gång klienten kopplar upp sig mot nätverket. Det meddelande som klienten skickar till servern frågar efter en unik IP-adress. Servern som är inställd på att svara på dessa förfrågningar skickar tillbaka en unik IP-adress med tillhörande subnätmask. Både Bootp och DHCP servern kan konfigureras så att den alltid skickar ut samma IP-adress till en dator varje gång som just den datorn frågar efter en ny adress. Detta sker genom att Bootp eller DHCP servern läser av klientens MAC-adress (Media Access Control Adress) i samband med klientens anrop (se avsnittet 8.10 om adresstilldelning). Ett annat alternativ är att klienten tilldelas nästa lediga IP-adress med tillhörande subnätmask för varje anrop. Då kommer en klient att tilldelas olika IP-adresser vid sina anrop [Fitzgerald, 1999].

För att få spårbarhet till vilken användare som är innehavare av ett visst IP-nummer måste dessa bokföras manuellt så att man i efterhand kan kontrollera vilken IP-adress som är knuten till en viss användare. Detta kräver en administration där organisationen har samlat på sig information som innebär att man känner till både MAC-adress och IP-adress på den dator som en användare arbetar vid. Byter man ut nätverkskortet till ett annat kommer denna spårbarhet att gå förlorad om inte det manuella registret uppdateras. Det finns även programvara i dag som gör det möjligt att skriva över vissa närverkskorts MAC-adress.

8.7.4 Routing

En router är en dator som arbetar på nätverksnivån (nivå 3) vilket innebär att varje router måste ha en egen IP-adress (se figur 12). En router klarar av att förbinda olika nätverk med varandra som använder samma eller olika datalänk protokoll (Token ring, Ethernet) men som har samma nätverksprotokoll (IP, IPX) [Fitzgerald, 1999].



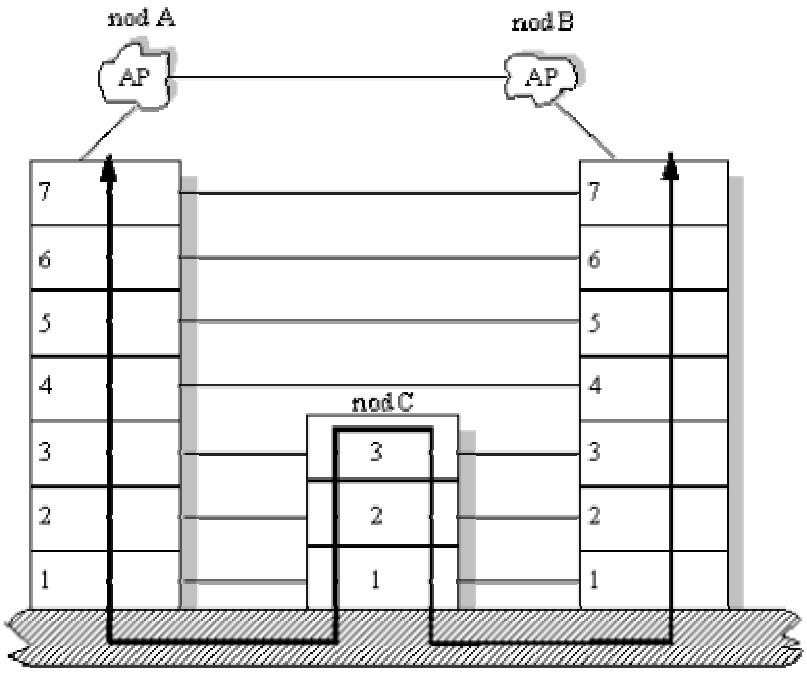
Figur 12 Bilden visar en router som förbinder två nät med två olika datalänkprotokoll, Ethernet och Token Ring **[**Fitzgerald, 1999].

[28] Bootp och DHCP är protokoll som används för att automatiskt bland annat kunna tilldela datorer en IP-adress.

I många nätverk finns det flera olika vägar för ett paket att ta sig fram via. Routing är den process som används för att fastställa den väg ett paket skall ta för att nå slutdestinationen. Varje dator längs vägen som tillhandahåller denna routingtjänst har en tabell som kallas för routingtabell. En stor fördel med dessa routingtabeller är att de kan fastställa den bästa vägen mellan nätverken där det finns flera olika möjligheter för ett paket att komma fram. Genom att routern känner till både sin egen och destinationsadressens placering kan den titta i sin tabell och komma fram till vilken väg som är möjlig eller lämpligast för paketet för att komma fram [Fitzgerald, 1999].

I kapitlet angående datalänklagrets adressering tar vi upp det faktum att datorer inom samma LAN inte adresserar varandra med IP-nummer utan med dess datalänk adress (MAC-adress). Det är någonting vi inte märker eftersom nätverkslagrets kommunikation med datalänklagret sköter det åt oss. Det finns dock några olika alternativ som gör att logiken i nätverket kommer att fungera olika beroende på om det rör sig om en känd adress inom samma subnät, en känd adress i ett annat subnät eller en helt okänd adress. Se avsnittet om trafiken i nätverket.

Då ett paket skall sändas mellan två datorer, även kallade noder[29] i ett nätverk (t ex noderna A och B), i ett nätverk är det mycket troligt att paketet passerar en mellanliggande nod (nod C) innan det når slutdestinationen (se figur 13). Nod C kan t.ex. utgöras av en router. Den verkliga vägen som paketen tar från nod A till nod B illustreras med den tjocka svarta pilen i bilden. Lagren ovanför nätverkslagret på nod C kommer här varken att se eller märka att paketen passerat noden på vägen från A till B. Om man skulle analysera huvudet i datalänkpaketet (Ethernet) så skulle man märka att avsändande och mottagande MAC-adress i trafiken mellan A och C skulle vara olika jämfört med adresserna på motsvarande nivå mellan C och B.



Figur 13 Mellanliggande nod C har kunskap om att paketen passerar sin nod på IP-nivå, men inte högre upp i stacken innan meddelandet når slutdestinationen (nod B)

[29] Varje nod i ett nätverk är en teknisk utrustning som har en egen IP-adress.

8.8 Datalänknivå (Nivå två i OSI-modellen)

I detta arbete kommer vi begränsa oss till att i huvudsak gå in på Ethernet när det gäller datalänk nivå. Exempel på övriga protokoll benämns endast kortfattat.

8.8.1 Ethernet

Det finns ett antal olika protokoll som kan användas på datalänk nivå. Den vanligaste är Ethernet, övriga kan t.ex. vara Token Ring, PPP[30] (Point-to-Point Protocol) och SLIP (Serial Line IP Protocol). Gemensamt för dessa protokoll är att de är synkrona. Det finns även asynkrona datalänkprotokoll och skillnaden mellan synkrona och asynkrona protokoll är att de synkrona protokollen sätter samman hela block med data till små paket, vilka sänds iväg sedan den sändande och mottagande datorn synkroniserats. Asynkrona paket däremot innebär att varje tecken sänds iväg ett och ett med tillhörande start och stoppbit för att indikera start och stopp av tecknet [Fitzgerald, 1999].

8.8.2 Kollisionsskydd

För att förhindra kollision mellan flera datorer som sänder samtidigt i ett Ethernet nät används ett protokoll som heter CSMA/CD [31]. Tekniken är enkel, vänta med att sända till det att bussen är fri från trafik. Ingen får sända när någon annan dator sänder. Skulle två eller fler datorer sända samtidigt känner tekniken av detta och tilldelar var och en av datorerna en slumpmässig tid som dessa måste vänta innan de får sända igen [Fitzgerald, 1999].

8.8.3 ARP-förfrågan

All kommunikation mellan datorerna inom subnätet, som i vissa fall omfattar hela det lokala nätverket, sker på datalänknivå. (se avsnittet 8.10 om adresstilldelning). För att kunna sända ett meddelande inom det egna nätverket måste den sändande datorn känna till datalänklagrets adress hos den mottagande datorn. För att få reda på den adressen kommer den sändande datorn att skicka ut ett broadcastanrop[32] till samtliga datorer i det egna subnätet (se avsnittet 8.10.3 om datalänklagrets adressering). Meddelandet som sänds i broadcastanropet skickas med ett protokoll som heter Adress Resolution Protocol (ARP) och arbetar på ungefär följande sätt. Du som har IP-adress xxx.xxx.xxx.xxx var vänlig och skicka mig din datalänk adress (MAC-adress).

En ARP-förfrågan görs endast vid utgående trafik eftersom det är då som IP-huvudet och Ethernethuvudet skapas. Varje dator i subnätet kommer att höra denna ARP-förfrågan, oavsett om näten är switchade eller hubbade. Under tiden köas det utgående IP-paketet i avvaktan på att ARP-förfrågan skall ge ett svar [Web 16].

Den dator som har den efterfrågade IP-adressen kommer att höra förfrågan eftersom den skickas ut till alla datorer som finns i subnätet. Den efterfrågade datorn kommer att besvara anropet genom att skicka med sin MAC-adress. Det framgår av subnätmasken om mottagande dators IP-adress ligger i det egna subnätet eller utanför. Ligger den utanför kommer den sändande datorn att adressera default gatewayen i stället.

[30] PPP är ett protokoll som tillhandahåller en standardmetod för transport av olika multiprotokoll över en punkt till punkt förbindelse [Web 15].
[31] CSMA/CD - Carrier Sense Multiple Access with Collision Detection
[32] Broadcastanrop utgörs av ett anrop till alla datorer som sitter på samma subnät eller LAN [Fitzgerald, 1999].

Alla datorer i subnätet eller i det lokala nätverket känner till vägen ut från subnätet eller det lokala nätverket t.ex. default gatewayen mot andra subnät eller mot Internet om en sådan koppling finns [Fitzgerald, 1999] (se avsnittet 8.9 om grundkonfigurering av datorer i ett TCP/IP-nät).

För att inte ARP-anropen skall behövas skickas ut varje gång en dator vill sända data lagrar varje dator tidigare svar i en ARP-tabell. Denna tabell lagras i datorns minne. I tabellen mappas IP-nummer mot MAC-adresser varför en kontroll först sker i ARP-tabellen innan ett ARP-anrop går ut. Du kan själv kontrollera din ARP-tabell genom att öppna kommandotolken och skriva kommandot ”arp –a” (utan citattecken). Där kommer du troligen åtminstone att finna MAC-adressen till din default gateway. Har du ett eget LAN kan du pinga en IP-adress inom det egna subnätet varefter du kommer att finna att din ARP-tabell har uppdaterats. Tabellen är inte statisk och det innebär att den ligger kvar en tid för att sedan försvinna. Nästa gång du anropar en IP-adress byggs ARP-tabellen upp igen. ARP-förfrågning är något som kan missbrukas, vilket vi tar upp under avsnittet om ARP-spoofing.

8.9 Grundkonfigurering av datorer i ett TCP/IP nät

När en dator skall installeras i ett TCP/IP baserat nätverk krävs det ett antal inställningar för att den skall kunna kommunicera inom nätverket. Dessa inställningar omfattar konfigurering på nätverksnivå och information om routing. Dessa inställningar omfattar nedan information vilken antingen kan ställas in manuellt eller via installationsfiler, bootp eller DHCP [Fitzgerald, 1999].

1. ***IP-adress***
2. ***Subnätmask***
3. ***IP-adress till en DNS-server för översättning av applikationslagrets adressering till nätverkslagrets adressering.***
4. ***IP-adress till en Gateway[33] för att leda ut den trafik som är avsedd för mottagare utanför det egna subnätet.***

8.10 Adresstilldelning

Innan man kan sända ett meddelande till en annan dator måste man känna till den mottagande datorns adress. Beroende på vilken nivå vi talar om i OSI modellen ser adresseringen olika ut beroende på vilket lager vi befinner oss på. Vi talar om tre olika adresser [Fitzgerald, 1999]:

Adress	**Exempel på programvara**	**Exempel av adress**
Applikationslager	Browser	www.dsv.su.se
Nätverkslager	TCP/IP	130.237.161.25
Datalänklager	Ethernet	00-0C-00-F5-03-5A-

Figur 14 Olika typer av adresser

Varje dator i det lokala nätverket, eller ute på Internet, måste ha en unik adress. Då talar vi inte bara om nätverksadressen utan samtliga adresser som visas i figur 14 måste vara unika. När det gäller nätverksadresser måste en dator på ett lokalt nätverk ha en unik nätverksadress inom nätverket och en dator på Internet måste ha en unik nätverksadress på Internet. Det innebär att det är friare att tilldela nätverksadresser inom en organisation eftersom dessa kan tilldelas utan att kollidera med adresserna på Internet.

[33] Vi använder ordet Gateway, men i praktiken kan det lika gärna vara en router eller switch [Fitzgerald, 1999].

Detta under förutsättning att organisationens nätverk antingen är ett slutet nät eller att accesspunkten ut mot Internet sker via en brandvägg/router som nyttjar NAT-protokollet[34] eller en någon annan lösning som t.ex. en applikationsproxy placerad mellan det interna nätverket och routern mot Internt [Panko et al, 2004].

8.10.1 Applikationslagrets adressering

Applikationslagrets adress är till för att fylla ut människans begräsningar. Egentligen skulle det räcka med nätverksadressen, men människan är inte skapt på det sättet att hon minns speciellt många nätverksadresser. I stället döper vi våra datorer enligt en viss namnstandard som är mer anpassad till människan. En applikationsadress som www.dsv.su.se är för de allra flesta lättare att minnas än dess motsvarande nätverksadress 130.237.161.25.

När en användare arbetar i t.ex. en browser skriver denne in applikationsadressen i URL-fältet[35] för nå t.ex. en webbserver eller FTP-server. Programmet använder dessa data när den skall upprätta en session mellan klienten och den anropade servern. Vad användaren inte märker är att programmet byter ut applikationsadressen mot serverns nätverksadress. Detta sker antingen genom att datorn tittar i sin egen tabell, vilket förutsätter att adressen adresserats tidigare, eller genom att applikationen sänder ett speciellt UDP-paket till närmaste DNS-server (se avsnitt 8.11 om Damain Name Server) som ber servern att skicka tillbaka nätverksadressen som är kopplad till applikationsadressen i DNS-serverns databas [Fitzgerald, 1999].

8.10.2 Nätverkslagrets adressering

IP-protokollet är ett nätverksprotokoll som ligger på nivå tre i OSI modellen. En adress på nätverksnivå består av 32 bitar och är indelad i fyra oktetter. Adressen innehåller en nätverksdel och en värddatordel. Varje oktett beskrivs i intervallet 0 – 255 och separeras med en punkt. Ett exempel på en nätverksadress, vanligtvis kallad för IP-adress, är 147.186.219.82.

Det går inte utan vidare att se på en IP-adress och utläsa vilken del av adressen som utgör nätverksdelen och vilken del som utgör värddatordelen. För att kunna göra det krävs ytterligare en 32 bitars nummerserie som vanligtvis kallas för subnätmask. Även subnätmasken är uppdelad i fyra oktetter där varje oktett separeras med en punkt och beskrivs i intervallet 0 – 255. Av subnätmasken kan man bestämma vilken del av IP-adressen som utgörs av nätverksdelen och värddatordelen [Fitzgerald, 1999].

Man kan jämföra IP-adressens nätverksdel med en gatuadress och värddatordelen med en specifik lägenhet på gatuadressen. Ett paket skall levereras till en viss lägenhet på Polhemsgatan 32. På så sätt kan en annan lägenhet på Kungsgatan ha samma lägenhetsnummer, men särskiljas genom en annan gatuadress, vilket i datorernas värld motsvaras av nätverksdelen, som i sin tur utläses av subnätmasken.

[34] NAT står för *Network Address Translation* eller nätadressöversättning. Det är ett sätt att ansluta många datorer till en Internetanslutning och samtidigt råda bot på den förmenta bristen på IP-adresser. NAT är en funktion som byggs in i den router som ansluter det lokala nätet till Internet.

[35] En Uniform Resource Identifier (URI) identifierar och pekar mot en resurs på Internet (eller Intranet). En URI kan vara av tv typer, antingen Uniform Resource Locator (URL) eller Uniform Resource Name (URN). URL är vanligast och anger som identifikation en resurs globalt unika adress medan URN använder resursens globalt unika namn [Leupold et al, 2004].

En subnätmask som har värdet 255.255.255.0 anger att de tre första oktetterna av IP adressen utgörs av nätverksdelen. Kvar finns i teorin 2^8 = 256 tillgängliga datorer, vilket här kan jämföras med att det på Polhemsgatan 32 finns 256 möjliga lägenhetsnummer.

Ett exempel på en IP-adress med tillhörande subnätmask är IP-adressen 147.186.219.82 och subnätmasken 255.255.255.224. Att den sista oktetten i subnätmasken inte är satt till 0 (noll) innebär att man har tagit en del av den sista oktetten till att omfatta nätverksdelen. Om vi omvandlar 224 till det binära talsystemet blir det lättare att se vad subnätmasken betyder.

En byte består av åtta bitar, och en byte med det decimala värdet 224 beskrivas enligt det binära talsystemet på följande sätt:

```
128   64   32   16   8   4   2   1
-----------------------------------------
  1    1    1    0   0   0   0   0
```

128 + 64 + 32 = 224

Av ovan binära upplägg finner vi att man i detta fall utnyttjat de tre första bitarna i den sista oktetten till att omfatta nätverksdelen. I teorin finns det 2^5 = 32 möjliga kombinationer kvar att laborera med, men i praktiken blir det bara 30 olika värddatoradresser kvar i och med att kombinationen av bara ettor och nollor i de sista fem bitarna av den sista oktetten inte kan räknas till värddatoradresser. Kombinationen av fem ettor används i subnätet för broadcast[36] och kombinationen av fem nollor används till nätverksadressen. Figur 15 visar ett exempel på hur man räknar ut vilka subnät en given IP-adress och en subnätmask ger upphov till. IP-adressen är satt till 147.186.219.82, vilket inte direkt framgår av figuren, och subnätmasken 255.255.255.224. Som framgår av bilden är det endast den sista oktetten som får olika värden beroende på vilket värde de tre första bitarna i den sista oktetten genererar. De tre markerade första bitarna i den sista oktetten ger de värden som framgår av den sista oktetten i den vänstra kolumnen. Vi skall se vilka subnät som går att generera med ledning av aktuellt IP-nummer.

IP-adress per subnät	**Sista oktetten binärt**	**Anmärkning**
147.186.219.0	**000**00000	Ej tillåten
147.186.219.32	**001**00000	
147.186.219.64	**010**00000	
147.186.219.96	**011**00000	
147.186.219.128	**100**00000	
147.186.219.160	**101**00000	
147.186.219.192	**110**00000	
147.186.219.224	**111**00000	Ej tillåten

Figur 15 visar giltiga kombinationer av subnät till subnätmasken 255.255.255.224 [37]

Figur 15 visar att subnätmasken 255.255.255.224 ger en möjlighet till sammanlagt sex olika subnät. I vart och ett av subnäten finns det ett utrymme för 2^5 = 32 olika kombinationer av binära tecken, vilket i detta fall ger ett teoretiskt utrymme av 32 olika värddatoradresser i respektive subnät.

[36] Broadcast är en speciell form av paket som skickas till samtliga datorer på samma LAN
[37] http://ppz.sajtech.nu/howtos/scripting%20&%20C/subnet.html

Detta är inte helt sant i och med kombinationen av enbart nollor är reserverad för subnätadressen och kombinationen av enbart ettor är reserverad för broadcastanrop i varje subnät. Kvar blir ett spann av 30 tillängliga värddatoradresser i respektive subnät.

Broadcastanropen är en förutsättning för att datorerna skall kunna kommunicera med varandra inom LAN:et. Vi beskriver detta lite närmare under avsnittet om datalänklagrets adressering under avsnitt 8.10.3, där vi bland annat kommer att diskutera ARP-tabellen.

För varje subnät kan man, utefter vad som angivits ovan, komma fram till innehållet i figur 16 och 17. Genom att följa samma resonemang för respektive subnät finner man ganska lätt vilka tillgängliga IP-adresser ett visst subnät har, men även inom vilket subnät ett visst IP-nummer hör hemma.

IP-adress	**Beskrivning**	**Sista oktetten i IP-adressen**
147.186.219.32	Första subnätet	binärt 001**00000**
147.186.219.33	Första noden	binärt 001**00001**
147.186.219.62	Sista noden	binärt 001**11110**
147.186.219.63	Broadcast	binärt 001**11111**

Figur 16 visar adresspannet för första subnätet

IP-adress	**Beskrivning**	**Sista oktetten i IP-adressen**
147.186.219.64	Första subnätet	binärt 010**00000**
147.186.219.65	Första noden	binärt 010**00001**
	Sista noden	binärt 010**11110**
147.186.219.95	Broadcast	binärt 010**11111**

Figur 17 visar adresspannet för andra subnätet o.s.v.

8.10.3 Datalänklagrets adressering

Datalänklagret arbetar på nivå två i OSI-modellen. Inom detta lager finns ett antal protokoll tillgängliga. Exempel på datalänk protokoll är Ethernet, Token Ring och PPP. All adressering inom t.ex. ett Ethernet nät i det lokala nätverket (LAN) sker via datalänklagrets MAC-adress. Detta utgörs av ett 48 bitars långt tal som är unikt för varje nätverkskort. Adresserna för nätverkskorten tilldelas av IEEE[38] och är uppdelad i två delar. Den första halvan (24 bitar) talar om vilken tillverkare som tillverkat kortet medan den andra halvan utgörs av ett 24 bitars långt löpnummer. En MAC-adress anges med hexadecimala värden. Ett exempel på en MAC-adress är 00-10-A4-9B-62-90. Denna adress ”bränns” vanligtvis in i nätverkskortet redan vid tillverkningen, varför det vanligtvis är en statisk adress som kommer tillsammans med nätverkskortet. Byter man nätverkskort får man således en ny nätverksadress. Detta stämmer dock inte alltid, något vi tar upp under avsnitt 8.15 som beskriver ARP-spoofing.

8.11 DNS

En DNS (Domain Name Server) har som huvuduppgift att översätta applikationslagrets adressering till nätverkslagrets adressering, d.v.s. till IP-adresser. En dator gör en DNS-förfrågan genom att sända ett UDP-paket till DNS-servern på port 53. Om man t.ex. skriver in applikationslagrets adressering www.dsv.su.se kommer datorn att skicka iväg UDP-paketet till DNS-servern. Det svar som datorn vill ha tillbaka är IP-adressen till dsv.su.se.

[38] IEEE står för *Institute for Electric and Electronic Engineers* och är en sammanslutning av folk och företag inom elektricitet, elektronik och datorer, huvudsakligen i USA.

Om inte den anropade DNS-servern känner till adressen så skickar den förfrågan vidare uppåt i hierarkin. Webbläsaren kan sedan använda Data-och Systemvetenskapliga linjens IP-adress vid Stockholms universitet för att kontakta dess webbserver [Strebe et al, 2000]

En DNS-server arbetar efter en hierarkisk modell med ett antal root-servrar. Dessa hanterar toppdomäner[39] som .com, .gov, .net, .edu, .org, .nu, .se och så vidare. Företag, organisationer, och för all del enskilda personer, kan ansöka om namn direkt under toppdomänen som www.aftonbladet.se [Fitzgerald, 1999]. Namngivningen av en applikationsadress följer ett visst mönster. Normalt skriver man applikationsadressen på följande sätt:

www.organisation.toppdomän (www.aftonbladet.se)

Om adressen finns på WWW (World Wide Web) brukar datoradressen börja med www. Den andra delen är oftast namnet på organisationen eller företaget som är innehavare av adressen. Den tredje delen utgörs av toppdomänen som kan utgöras av beteckningen för det land där datorn finns belägen.

På samma sätt som innehavarna av en toppdomän kan skapa domäner kan innehavaren av en domän skapa underdomäner. Underdomäner upprättas i företagets eller organisationens DNS-server. Innehavaren av domänen bestämmer själv regler för hur underdomäner skapas och vilka regler som gäller för deras förvaltning och användning. Underdomänen ansluts till domänen med en punkt mellan domänen och underdomänen. Ett exempel på detta är applikationsadressen www.dsv.su.se. Dsv är här en underdomän till su (Stockholms Universitet) som i sin tur är en subdomän till se (landsdomän Sverige). Liksom för domäner och toppdomäner kan endast vissa tecken användas. Svenska tecken - å, ä och ö - kan inte användas i domännamn.

Om DNS-servern inte känner till den angivna nätverksdressen kommer den att anropa aktuell toppdomän. Toppdomänen skall känna till de nätverksadresser som är knutna till toppdomänen. I ett exempel med applikationsadressen www.dsv.su.se kan man räkna med att toppdomänen .se känner till .su varför den skickar begäran vidare till .su. Underdomänen .su kommer att kunna returnera nätverksadressen för .dsv. Svaret länkas tillbaka via den kedja som bildats från den först anropade DNS-servern, vilket i detta exempel är Internetleverantörens DNS-server. Servrarna längs tillbakavägen kommer att lagra nätverksadressen till www.dsv.su.se i sina tabeller så att inte nästa förfrågan till www.dsv.su.se måste gå samma väg. På så sätt minskas belastningen på toppdomänerna [Fitzgerald, 1999].

Med egen DNS-teknik är det möjligt att bygga en domänhantering inom det interna nätverket. Om man däremot vill kunna adresseras via Internet bör man ansluta sig till Internets domänsystem som sköts av Internet Society och administreras av IANA (Internet Assignment Number Authority),. Dessa har delegerat ansvar för en rad olika toppdomäner, dels de med landskoder och de amerikanska toppdomänerna (com, org, net, edu, mil m.m.) till olika organisationer eller företag.

[39] Toppdomäner är den översta nivån i Internets domännamnsystem Toppdomäner finns av två slag: nationella som representerar ett visst land och generella som inte styrs av nationsgränser. Toppdomänen .se, som används för den svenska delen av Internet, är en nationell toppdomän. Den vanligen förekommande domänen, .com, är däremot en generell toppdomän.

En ny organisation, IKANN (Internet Corporation for Assigned Names and Numbers), har bildats för att ta över huvudansvaret för toppdomänerna från IANA som fortfarande skall sköta olika praktiska uppgifter vad gäller Internet-parametrar som protokollnummer, IP-nummer, portnummer, SNMP-nummer och en del annat.

Den svenska toppdomänen ".se" innehas i dag av II-stiftelsen och är det organ som definierar regler och villkor för registrering och användning av domäner i Sverige. Alla innehavare av domäner betalar en avgift för registerhållning och drift av de DNS-serversystem som II-stiftelsen driver. II-stiftelsen har bildat ett aktiebolag som sköter registrering och administration av domäner. Aktiebolaget heter NIC-SE AB. Det bolaget är det som fakturerar årsavgifter och administrerar databasen [Web 5].

8.12 Nätverkskomponenter

I ett nätverk finns ett antal olika komponenter som med sin programvara är en förutsättning för att trafiken i nätverket skall fungera. I denna uppsats nämner vi kort några komponenter vilka vi nedan beskriver lite närmare. Främsta skälet att dessa tagits med är att ge läsaren en förståelse av vad skillnaden är mellan så kallade switchade och hubbade nät, samt hur detta påverkar möjligheten till att ”sniffa” nätverkstrafiken.

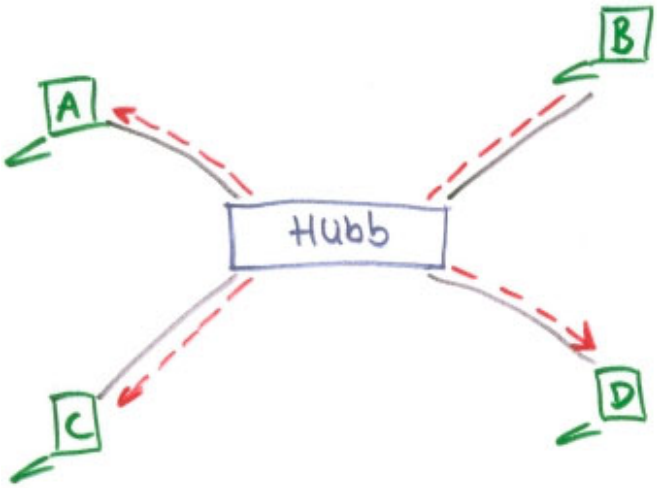
8.12.1 Gateway

En gateway arbetar på nätverksnivå (nivå tre) och använder nätverksadresser för att vidarebefordra meddelanden. En gateway används för att koppla samman två eller flera nätverk som använder samma eller olika datalänk och nätverksprotokoll. Den är därför mer komplex än en router, och benämningen används ofta felaktigt då router många gånger är ett mer korrekt val [Web 4].

8.12.2 Hubbade nät

En hubb (se figur 18) är en komponent i det lokala nätverket som arbetar i det fysiska skiktet (nivå ett) i OSI-modellen [Fitzgerald 1999]. Den förmedlar all trafik mellan datorer som kopplats till hubben. En hubb klarar inte av att göra en logisk koppling mellan en sändande och mottagande dator vilket innebär att all trafik som en dator skickar ut på nätverket kommer att höras av samtliga datorer som är kopplade till ett hubbat nät. Detta innebär att du kan koppla in dig var som helst i det lokala nätverket, eller subnätet, och från denna punkt kunna lyssna av all trafik i nätet.

Då alla i ett ”hubbat” nät hör all trafik i nätet ökar risken för kollisioner i takt med att antalet klienter blir fler och trafikintensiteten ökar. För att skydda sig mot detta använder sig t.ex. datalänkprotokollet Ethernet en teknik som beskrivs under avsnittet 8.8.2 som omfattar kollisionsskydd i Ethernet.

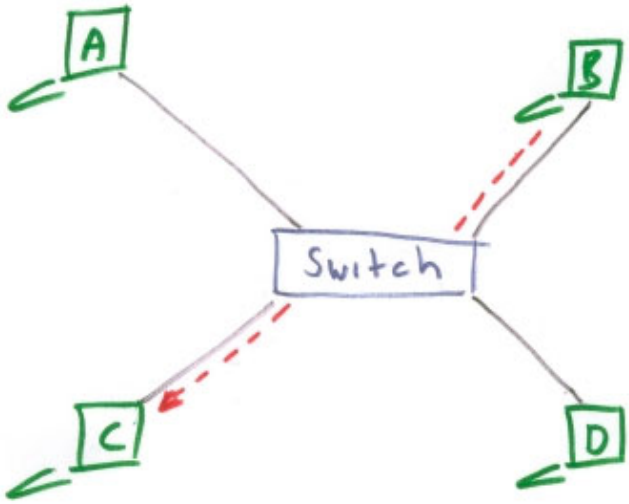


Figur 18 Bilden visar trafiken i ett ”hubbat” nät där alla datorerna i nätverket kan höra vad en annan dator sänder[Web 4].

8.12.3 Switchade nät

En switch (se figur 19) är en komponent i det lokala nätverket som arbetar på datalänk nivå (nivå två) i OSI-modellen [Fitzgerald, 1999]. Genom att byta ut hubben mot en switch uppnår man vissa förbättringar i ett lokalt nätverk. Genom detta förfarande har nu varje dator en egen punkt-till-punkt förbindelse med switchen. Den enskilde datorn kommer endast av nås av broadcast trafik (trafik riktad till alla i subnätet) och den trafik som är adresserad till just denna dators MAC-adress. Om alla delade på en 10 Mbps förbindelse i ett hubbat nät har varje dator i ett switchat nät en egen 10 Mbps förbindelse.

Den insatte inser naturligtvis att om förbindelsen till servern eller en default gateway även den är 10 Mbps så kommer samtliga datorer som kommunicerar mot en server eller en default gateway att dela på denna bandbredd. Det är således längs denna sträcka man riskerar en flaskhals [Fitzgerald, 1999]. Det är även längs denna sträcka en sniffer kan göra störst skada i och med att den mesta trafiken av allt att döma kommer att gå den vägen.



Figur 19 Bilden visar trafiken i ett ”switchat” nät där dator B kommunicerar med dator C [Web 4].

8.13 Sniffning av nätverk

En sniffer är ett verktyg som används för att avlyssna trafik i ett nätverk. Populära sniffrar är tcpdump, Sniffer Wireless och Ethereal. En sniffer är mycket användbart när man vill felsöka nätverk eller bara samla data om vilken trafik som nätverket används till.

När man sniffar ett nätverk kan man höra all trafik som sker i nätverket. I normala fall tar ett nätverkskort bara emot den trafik som är adresserad till den egna MAC-adressen, men genom att ställa om nätverkskortet till ett läge som kallas promiscous mode tar nätverkskortet emot all data, även de som inte är adresserad till den egna MAC-adressen. Programvaran (sniffern) t.ex. Ethereal visualiserar informationen som den lyssnar av och bygger upp den så att man kan se pakethuvud och den datamängd som användaren skapade högre upp i OSI-modellen. Därmed blir all data som inte har ett skydd av kryptering synlig. Det gäller även för lösenord som transporteras inom nätverket i klartext, utan skydd av kryptering.

8.14 IP-spoofing

Många system loggar IP-adressen från den klient som genererat trafiken. Data om källadress och mottagaradress följer med i TCP och IP huvudet under en session. Detta kan loggas för att i efterhand kunna visa varifrån en viss uppkoppling skett [Fitzgerald, 1999].

En angripare vill som regel inte skylta med sin egen IP adress eftersom en publik IP-adress tilldelats av en ISP på ett sätt att den i allmänhet går att spåra till ägaren som kan vara en privat eller juridisk person. Även om detta inte pekar ut den enskilda personen som genererat trafiken så anger IP-numret från vilken dator trafiken genererats. I större organisationer med privata IP-adresser, som inte är publika på Internet, krävs administrativa rutiner för att kunna mappa ett visst IP-nummer till en enskild användare.

Ett vanligt misstag bland datoranvändare är att ”IP-spoofing[40]” kan användas för att dölja användarens egen IP-adress när denna surfar, chattar eller skickar e-post via Internet. Detta är inte sant eftersom man inte kan skapa en normal nätverkstrafik mellan den sändande dator och mottagaren genom att manipulera källadressen i IP-huvudet. Den handskakningsprocess som inleder en TCP anslutning är beroende av en kommunikation med källadressen i och med att den skickar tillbaka ett SYN/ACK paket innan sessionen är upprättad.

En liknelse kan göras mellan en person som vill prenumerera på en tidning. Abonnenten kan lura tidningsutgivaren genom att ange en felaktig adress. Tidningen kommer då att skickas till den angivna adressen, men den som beställt tidningen får den inte skickad hem till sig. På samma sätt förhåller det sig med IP-adresseringen under kommunikationen på Internet. Det är fullt möjligt att ändra på IP-adressen i paketen som skickas ut på Internet, men svaren som mottagande system skickar iväg når inte avsändarens dator, utan skickas till den IP-adress som angivits.

Att kunna byta IP-adress inom en organisation är däremot sällan speciellt svårt. Det man först måste ta reda på är vilken form av nätverksadressering som organisationen tillämpar. Beroende på hur noderna i nätverket får sin adresstilldelning kan detta utnyttjas. Genom subnätmasken ser man direkt hur stort spann subnätet har.

[40] Begreppet IP-spoofing innebär att en angripare kan utge sig för att vara en pålitlig klient där kontrollen baseras enbart på IP-adressen.

Därmed är det möjligt att tillfälligtvis ta ett IP-nummer som inte är knutet till en viss person, eller ett IP-nummer som är knutet till en annan person. IP-numret är av den anledningen lätt att förändra, vilket kommer att påverka sanningsinnehållet av loggutdragen, och i sin förlängning dess bevisvärde.

I dag är det vanligt att brandväggar eller routrar använder sig av NAT-protokoll vilket gör att all trafik inifrån ett LAN, utifrån sett, ser ut att komma från en och samma IP-adress. Bakom routern eller brandväggen kan det i själva verket dölja sig hundratals datorer där varje dator försetts med ett privat IP-nummer som inte går att accessa direkt från andra sidan routern eller brandväggen.

8.15 ARP-spoofing

ARP-spoofing bygger på det faktum att adresseringstekniken inom ett LAN bygger på datalänklagrets adress, nämligen MAC-adressen i ett Ethernet nät. Med denna metod är det möjligt för en angripare att låtsas vara en annan dator genom att ”låna” en annan dators identitet.

En dator på ett IP och Ethernet baserat LAN har två adresser, en IP-adress och en MAC-adress (Ethernet adress). MAC-adressen använder sig av Ethernet protokollet när det ska skicka data. Det sker via så kallade ramar (frames). En sådan ram är max 1500 byte lång och varje ram innehåller en MAC-adress för både sändare och mottagare [Web 6].

I avsnittet om datalänklagrets adressering, avsnitt 8.10.3, gick vi igenom vad en ARP-förfrågan och en ARP-tabell är för någonting. ARP-spoofing bygger på dessa broadcast anrop. Den ARP-tabell som en dator i nätverket bygger upp använder inte enbart på egna förfrågningar, utan den kan även uppdateras av de ARP-förfrågningar som andra datorer ställer. På så sätt kan dator A som frågar efter dator B:s MAC-adress även uppdatera dator C:s ARP-tabell i och med att alla i nätverket/subnätet kommer att höra både frågan och svaret. Nackdelen är att nu vet alla som hört B:s svar till A vilken MAC-adress dator B har. Det är detta som utnyttjas vid ARP-spoofing. Denna ARP-trafik skulle vara väldigt betungande för nätverket om det hela tiden gick ut nya ARP-förfrågningar. För att minimera trafiken på nätverket så använder de flesta operativsystem en buffer (ARP-tabell) som samlar på ARP-svar, även om det inte var de själva som skickat en förfrågan. På så vis så behöver ARP-trafiken inte bli så hög [Web 6].

Genom att sända ut falska ARP-svar på någon dators förfrågan så kan andra datorer få för sig att de kommunicerar med en annan dator. På detta sätt märker vare sig sändare eller mottagare att det är fel dator som fått paketet [Web 6].

Det finns webbplatser på Internet som säljer verktyg som kan förändra en dators MAC-adress. Ett sådant verktyg heter SMAC och det fungerar på så sätt att det endast förändrar den mjukvarubaserade MAC-adressen. Det förändrar med andra ord inte den hårdvarubaserade som finns inbränd på nätverkskortet [Web 7].

Det finns även kända metoder att via ARP-protokollet omdirigera trafiken mellan datorerna, så att en angripare kan ställa om switchen så att den tror att angriparens dator är default gatewayen. Från angriparens dator leds sedan trafiken ut till default gatewayen. I detta läge hör angriparen all trafik [McClure et al, 2003].

8.16 Trafiken i nätverket

Efter att ha gått igenom ett antal olika protokoll och funktioner i ett nätverk ger vi nedan tre exempel hur de olika protokollen och komponenterna i ett nätverk arbetar utifrån olika förutsättningar. I exemplen nedan utgår vi från att klienten anropar en webbserver, och därmed kommunicerar med sin browser på applikationsnivå. Exemplen nedan är oberoende av val av applikation på applikationsnivå.

8.16.1 Känd adress inom samma subnät

I det här fallet antar vi att klienten anropar en webbserver som är placerad inom samma subnät. Klienten har tidigare anropat servern varför klienten har serverns adresser sparad i sin adresstabell.

När applikationslagrets programvara, i det här fallet en browser, adresserar webbservern har användaren adresserat servern med dess applikationsadress, t.ex. www.dsv.su.se. När de olika skikten som presenteras under OSI-modellen bryter ner informationen från applikationsnivån kommer nätverkslagret först att söka igenom sin egen adresstabell för att finna om applikationsadressens nätverksadress finns i dess tabell. I detta exempel gör den det. Adressen som hämtas ut tabellen kommer att jämföras med subnätets subnätmask vilken kommer att indikera att webbservern finns inom samma subnät [Fitzgerald, 1999].

Nätverkslagrets programvara kommer att söka i datalänklagrets adresstabell (ARP-tabell) för att matcha IP-adressen mot dess MAC-adress. Därefter kommer nätverkslagret att kapsla in TCP paketet i ett IP-paket för att sedan förpassa det ner till datalänklagret. Datalänklagret kommer att kapsla in paketet i ett datalänk paket tillsammans med datalänklagrets MAC-adress till webbservern.

8.16.2 Känd adress men på ett annat subnät

Även här utgår vi från att klienten tidigare har anropat servern, varför klienten har serverns adresser sparad i sina adresstabeller. När paketet når nätverkslagret kommer IP-protokollet att jämföra IP-adressen med sin subnätmask för att då finna att mottagande dator ligger utanför det egna subnätet. Varje paket som skall skickas någonstans utanför subnätet måste sändas till default gatewayen, vars jobb är att öppna paketet till sin IP-nivå och via sina routingtabeller förpassa paketet vidare till rätt destination. Innan detta kan ske kommer nätverkslagret på den sändande datorn i subnätet att titta i sin ARP-tabell för att där hämta MAC-adressen till default gatewayen. Av den anledningen kommer nätverkslagrets adressering att innehålla den sändande datorns IP-adress som källa och den slutliga mottagardatorns IP-adress som destinationsadress. Däremot kommer den sändande datorns MAC-adress att ha default gatewayens MAC-adress som destinationsadress och inte slutmottagarens MAC-adress.

Default gatewayen kommer att ta emot paketet på datalänk nivå, genomföra sedvanlig felkontroll genom att jämföra att checksumman är korrekt, för att därefter skicka paketet vidare uppåt till nätverkslagret. Nätverkslagret kommer att läsa IP-adressen i destinationsfältet i IP-huvudet bara för att finna att detta paket inte är avsett för default gatewayen. Genom att titta i sin routingtabell vet gatewayen vart paketet skall skickas vidare. Paketet kommer därför att förpassas tillbaka till datalänk lagret. IP-huvudet förblir oförändrat, men det kommer nu att skapas ett nytt datalänkhuvud.

Denna process kommer att upprepas för varje nod som paketet passerar under sin väg från sändande dator till den slutliga mottagardatorn. Det nya datalänkhuvudet kommer att innehålla default gatewayens MAC-adress som källa och nästa nods MAC-adress som ligger längs vägen på väg till destinations IP-adressen [Fitzgerald, 1999].

8.16.3 Okänd adress

Om vi följer exemplen ovan med användaren som anropar en webbserver så kommer denne att mata in applikationsadressen i browserns adressfält. Det som är nytt i detta exempel är att applikationsadressen är ny och inte tidigare finns lagrad hos klienten. Klientens nätverkslager och datalänklager känner inte till webbserverns IP- och MAC-adress.

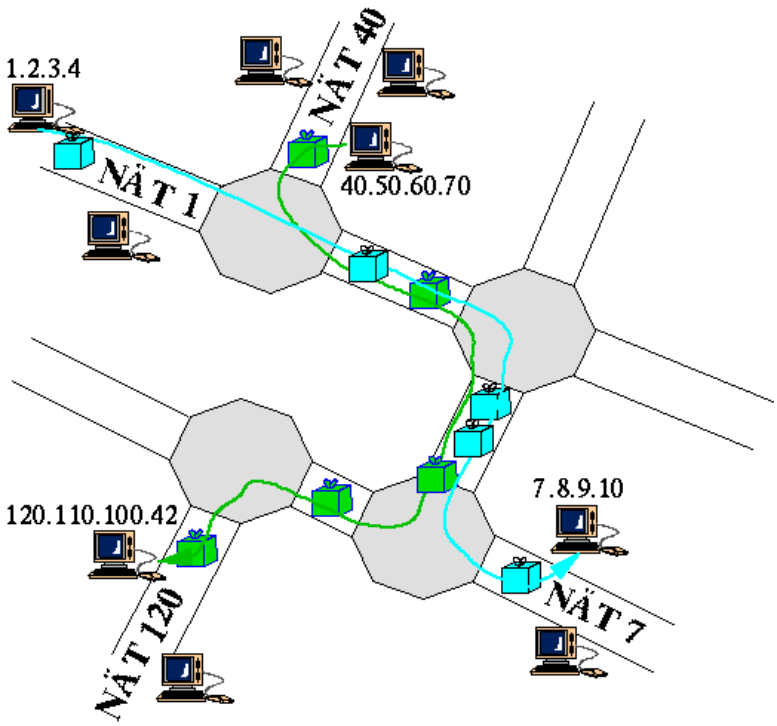
När paketet transporterats ner från applikationslagret, genom transportlagret och når nätverkslagret kommer nätverkslagret att söka i sin adresstabell. I och med att applikationsadressen är ny kommer nätverkslagrets adresstabell inte att innehålla någon IP-adress som mappar applikationsadressen. I det här fallet kommer nätverkslagret att skicka iväg en DNS-förfrågan som kommer att skickas till en DNS-server.

Under avsnittet om grundkonfigurering av datorer i ett TCP/IP nät, avsnitt 8.9, anges under punkten tre att DNS-servern är ett av fyra konfigurationsområden på nätverksnivå som en dator måste känna till för att kunna fungera i nätet. Därför är denna IP-adress känd för klienten. Eftersom default gatewayen är en del av det egna subnätet sker adresseringen av paketen på datalänknivå. Det innebär att den sändande datorn måste kontrollera i sin ARP-tabell för att konvertera dennes IP-adress till dess datalänkadress. Finns den inte där måste skickas det ut en ARP-förfrågan som kommer att uppdatera ARP-tabellen.

Genom att jämföra med sin subnätmask kommer nätverkslagret att finna att DNS-servern ligger utanför det egna subnätet. Nätverkslagret kommer av den anledningen att skicka ner DNS-paketet till datalänklagret som skickar paketet vidare till default gatewayen.

Paketet kommer att routas vidare i nätet tills det kommer fram till DNS-servern. Där kommer frågan att processas och ett matchande IP-nummer kommer att skickas tillbaka till den ursprungliga IP-adressen, d.v.s. till den klient på subnätet som skickade ut DNS-förfrågan.

När klienten tagit emot svaret på sin DNS-förfrågan kommer nätverkslagret att uppdatera sin adresstabell så att nästa förfrågan till samma webbserver inte behöver gå vägen via DNS-servern. Nätverkslagret kommer åter att jämföra webbserverns IP-adress med sin subnätmask och i detta exempel finna att den efterfrågade tjänsten ges av en webbserver som ligger inom det egna subnätet. Eftersom tjänsten tidigare inte efterfrågats innehåller ARP-tabellen ingen matchande MAC-adress. Ethernet kommer därför att göra en ARP-förfrågan för att uppdatera sin ARP-tabell. Efter detta kommer kommande paket att kunna transporteras till den aktuella webbservens MAC-adress utan att gå via DNS-servern och nya ARP-förfrågningar. Detta så länge som klientens adresstabeller är uppdaterade. Figur 20 illustrerar hur datapaket skickas mellan olika nätverk.



Figur 20 Bilden visar ett nätverk där dator 1.2.3.4 kommunicerar med dator 7.8.9.10 samt dator 40.50.60.70 som kommunicerar med dator 120.110.100.42. Hexagonerna motsvarar här olika routrar [Web 2].

8.17 Kryptering

I denna uppsats ger vi inte några detaljerade lösningsförslag över hur en organisation skall göra för att skydda trafiken i sina nät. I ställer lyfter vi fram de komponenter och skyddsåtgärder i stort som måste till för att kunna uppnå detta syfte. Det finns olika sätt att skydda loggarna inom en organisation varav integritetsskyddet lyfts fram som ett av de viktigaste skydden [Söderholm & Olsson].

Ett annat viktigt skydd är dock kryptering i och med att lösenordsbaserade system som skickar lösenorden i klartext är mer oskyddade än system som skickar lösenorden i krypterad form. (Se avsnitt 8.13 om sniffning). Av den anledningen kommer vi att ge exempel på vad som händer i ett nätverk beroende på var någonstans man lägger in detta skydd. Som ni kommer att se kan man göra det på olika nivåer i de modeller vi har diskuterat. Beroende på var någonstans man sätter in krypteringsfunktionerna så får man olika effekt.

Kryptering av information är vanligt förekommande när vi diskuterar termen sekretess. Ett lösenord eller klassificerad information måste på något sätt skyddas med speciella lösningar eftersom dessa inte ingår i de protokoll som hittills diskuterats. När det gäller att kryptera information måste vi bestämma oss för vad vi vill kryptera och var krypteringen skall sättas in. I detta avsnitt skiljer mellan länkkryptering och end-to-end kryptering [Stallings, 2003].

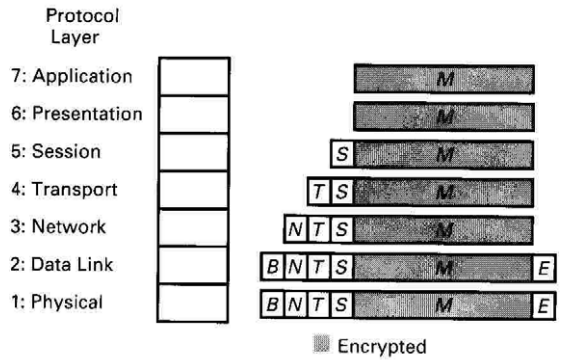
8.17.1 End-to-end kryptering

Om man skulle krytera allt som skickas, inklusive alla huvuden, skulle ingenting fungera. Varje skikt i protokollstacken är beroende av att kunna läsa informationen som finns inom det egna huvudet. Om den informationen är krypterad skulle protokollen inte förstå det som de läser. Det är bara den sändande och mottagande datorn som är innehavare av den symmetriska nyckel som kan kryptera och dekryptera informationen.

Skulle man sprida nyckeln till varje klient och varje nod i nätverket skulle detta förvisso fungera, men det skulle onekligen påverka säkerheten. Av detta resonemang följer att en klient endast kan kryptera den information som skapas av användaren och att de huvuden som skapas när ett paket transporteras nedåt i protokollstacken måste förbli okrypterade.

Vid end-to-end kryptering kommer kryptering och dekryptering att ske på klientnivå, d.v.s. hos den som skapar informationen och den som slutligen läser den. Om man tittar på protokollstacken i figur 21 ser man att detta skyddar de användardata som man skapar. Vid en första anblick ser detta ut att räcka ganska långt. Vad man kanske inte genast tänker på är att man med denna lösning måste bygga in en mjukvarulösning i varje klient, samt ha en nyckeldistribution som distribuerar ut den gemensamma symmetriska nyckeln till varje klient i nätverket. En kryptologisk lösning är t.ex. aldrig säkrare än det sätt som organisationen valt att lösa sin nyckelhantering på.

Med end-to-end kryptering kommer vi att kunna säkra den information som avsändande användare skapat, men det finns fortfarande en svaghet med denna lösning eftersom själva trafikmönstret fortfarande går att avläsa. Med detta menas att om man sniffar nätverkstrafiken kan man fortfarande läsa ut den del av informationen som finns i de olika protokollens huvuden (i figur 21 är dessa ofyllda). Av detta kan man utläsa information som att jag ofta skickar information med vissa protokoll till en viss mottagare. I vissa fall vill man skydda sig mot detta [Stallings, 2003].



Figur 21 End-to-end kryptering [Pfleeger, 2000].

8.17.2 Länkkryptering

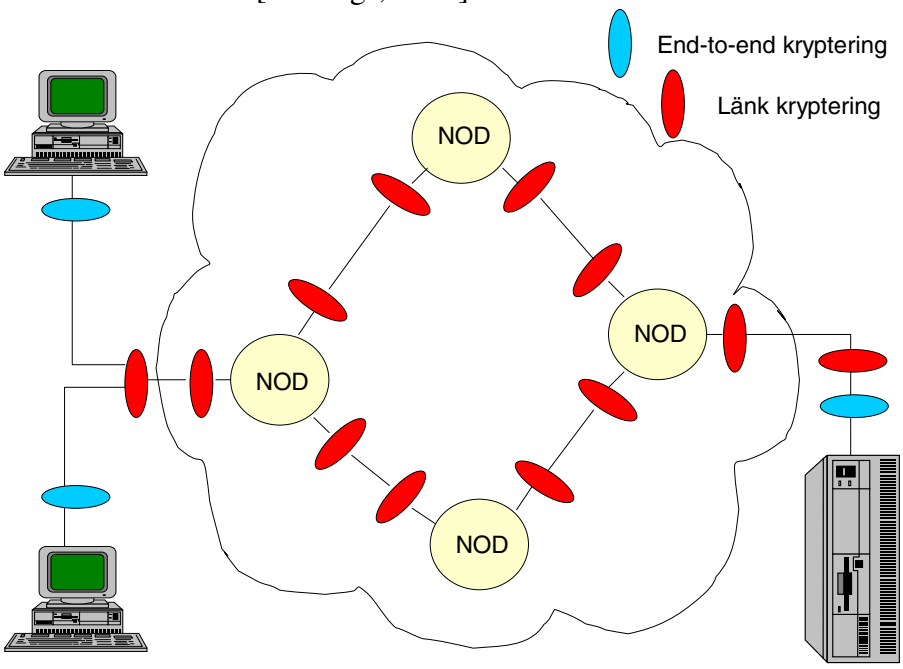
Om man i stället låter trafiken flyta i klartext på de lokala nätverken och krypterar all trafik som passerar default gatewayen når man ett annat resultat. Det krävs hård- och mjukvara både före och efter varje nod och nyckelhanteringen omfattar som regel ett betydligt färre antal noder än om krypteringen ligger på klientnivå. Allt som skickas utanför det lokala nätverket, eller subnätet, kommer att vara krypterat. När vi säger allt så menar vi allt, även huvudena. Hur går då detta ihop. I stycket ovan sade vi att ingenting fungerar om huvudena är krypterade och noderna saknar den symmetriska nyckeln.

För att lösa detta måste varje paket som når en nod först dekrypteras så att paketet under routing kan öppnas till nätverksnivå. Både datalänk- och nätverksnivån måste kunna läsa sina respektive huvuden för att routing skall fungera. Detta innebär att det krävs hård- och mjukvara som krypterar varje paket efter att paketen passerat en nod, och en likadan hård- och mjukvara som dekrypterar varje paket innan en nod.

Därmed blir hela den informationsmängd som användaren skapat vid sin klient, och som är hemlig, läsbar vid varje nod. Detta p.g.a. att allt dekrypterats i syfte att göra de nedre protokollens huvuden läsbara [Stallings, 2003].

8.17.3 Både end-to-end och länkkryptering

Om man däremot kombinerar end-to-end kryptering och länkkryptering kommer användarinformationen att förbli krypterad när noderna dekrypterar och packar upp paketen under routing (se figur 22). På detta sätt skyddar man sig både mot det faktum att användarinformationen blir läsbar vid varje nod samt mönsteranalys vid end-to-end kryptering, men även mot det hot som kan finnas om man inte är beredd att låta trafiken gå i klartext på de lokala nätverken [Stallings, 2003].



Figur 22 End-to-end kryptering i kombination med länk kryptering. Figuren är skapad med hjälp av en figur i boken Network Security Essentials [Stallings,2003].

8.17.4 Symmetrisk kryptering

Vid symmetrisk kryptering så används samma krypteringsalgoritm och en identisk nyckel (privat nyckel) för både kryptering och dekryptering. Både sändaren samt mottagaren måste ha tillgång till den delade nyckeln för att metoden skall fungera. Detta eftersom avsändaren krypterar meddelandet med nyckeln och mottagaren dekrypterar meddelandet med samma nyckel för att där igenom få fram budskapet i klartext. Fördelen med denna form av kryptering är att stora informationsmängder kan hanteras på grund av att mindre processorkraft behövs vid jämförelse med asymmetrisk kryptering. Nackdelen ligger i de administrativa svårigheterna med att distribuera nycklar i ett stort system eftersom alla måste ha alla nycklar och dessutom flera olika uppsättningar så att nycklar efterhand kan bytas ut.

8.17.5 Asymmetrisk kryptering

Vid asymmetrisk kryptering används samma krypteringsalgoritm men olika nycklar används för kryptering och dekryptering. Vid asymmetrisk kryptering används två typer av nycklar, en privat nyckel och en publik nyckel. Precis som i symmetrisk kryptering är den privata nyckel hemlig. Den publika nyckeln är dock öppen och kan läsas av vem som helst. Principen för denna form av kryptering är att avsändaren krypterar meddelandet med mottagarens publika nyckel (som är allmänt känd). Mottagaren dekrypterar sedan meddelandet med sin privata nyckel för att få fram allt i klartext. Observera att det inte är möjligt att kryptera och dekryptera meddelandet med en och samma nyckel i ett nyckelpar bestående av en privat samt en publik nyckel. Eftersom man använder mottagarens publika nyckel vid krypteringen så vet man att endast den med den andra nyckeln i detta nyckelpar, d.v.s mottagarens privata nyckel, kan dekryptera meddelandet. Det är även möjligt att kryptera med sin privata för att sedan dekryptera med den publika nyckeln [Stallings, 2003]. Detta används för autenticering vilket vi kommer att prata mer om nedan

8.17.6 Kvantkryptering

De senaste åren har en helt ny typ av krypto blivit möjligt tack vare kvantmekaniken och redan idag finns två fungerande system på marknaden. Metoden kallas kvantkrypton och betraktas som oknäckbart samt avlyssningssäkert [Axelsson, 2004].

Principen bygger på Heisenbergs osäkerhetsrelation som säger att det är omöjligt att mäta en partikels egenskaper utan att de förändras. Avsändaren skickar en kodnyckel med enskilda ljuspartiklar, fotoner, över en fiberoptisk kabel. Fotonerna är polariserade på två olika sätt, vågrätt/lodrätt samt snett höger/vänster, och genom att mottagaren mäter vilken typ av polarisation de enskilda fotonerna har kan han/hon få fram ett meddelande. Problemet är att denna mätning endast kan göras en gång per foton samt att en vågrätt/lodrätt polariserad foton måste mätas med ett vågrätt/lodrätt filter. Om mottagaren istället skulle använda fel filter så kommer fotonen polarisering att vridas snett och det kommer att bli omöjligt att veta hur fotonen var polariserad före mätningen. Följaktligen måste mottagaren veta vilken typ av polarisering varje foton har för att kunna få fram meddelande i klartext [Axelsson, 2004].

Metoden ger även skydd mot ”sniffning” eftersom en tredje person som sitter mellan avsändaren och mottagaren kommer lämna spår efter sig om denne försöker läsa av fotonernas polarisering. Detta eftersom avsändaren och mottagaren efter sändningen utbyter information om vilka fotoner som hade vilken polarisering. I och med detta kommer det att upptäckas om vissa fotoner har blivit förstörda efter att en tredje part försökt mäta dess polarisation. Har några fotoner blivit förändrade så vet användarna att kodnyckeln är forcerad och att en ny nyckel måste användas. Rent statistiskt så räknar man med att om 75 fotoner såg likadana ut när de skickades som när de kom fram så är sannolikheten för avlyssning mindre än en på en miljard [Axelsson, 2004].

8.18 Metoder för integritetsskydd

När vi talar om kryptering så skyddar det mot så kallade passiva attacker där en angripare kan lyssna av och ta del av data som t.ex. skickas över nätverket. Ett annat krav som ställs när det gäller att skydda informationen är ett skydd mot en mer aktiv attacker som innebär en fara för förfalskning och förändring av informationen. Vi talar i dessa fall om att vi vill ge informationen att integritetsskydd.

Ett meddelande, en fil, ett dokument eller vilka andra data som helst sägs vara autentiska när de är genuina och oförändrade och kommer från sin påstådda källa. Den procedur, som kallas för meddelandeautenticering (Message Authentication), innebär att de kommunicerande parterna kan verifiera att mottagna data är oförändrade. För att klara av det är det främst två saker som måste säkerställas, nämligen att data inte förändrats under transport samt att den påstådda källan är den som den utger sig för att vara. Vi vill på något sätt skapa förutsättningar för att vi kan lita på att sändaren är den som sändaren uppger sig för att vara samt att det som mottagits inte har förändrats under transport och mellanlagring [Stallings, 2003].

8.18.1 Hashalgoritmer

En hashalgoritm tar en sträng av godtycklig längd och omvandlar den till ett värde av fast längd. En kryptologisk säker hashalgoritm ska också ha andra egenskaper som bl.a. att det givet algoritmens output ska vara svårt att hitta algoritmens input, d.v.s. den sträng som matades in i hashalgoritmen. Om input till algoritmen ändras med en bit ska i genomsnitt dess output ändras i hälften av bitarna.

Det finns flera olika hashalgoritmer som i dag svarar mot dessa krav. En vanligt förekommande hashalgoritm är SHA-1. Det är en kryptologiskt säker hashalgoritmer som dessutom är en NIST[41] standard. Inom säkerhet används den t.ex. för att generera krypteringsnycklar och vid lösenordskontroller. Andra exempel på hashalgoritmer är MD5 och HMAC.

8.18.2 Message Authentication Code (MAC)

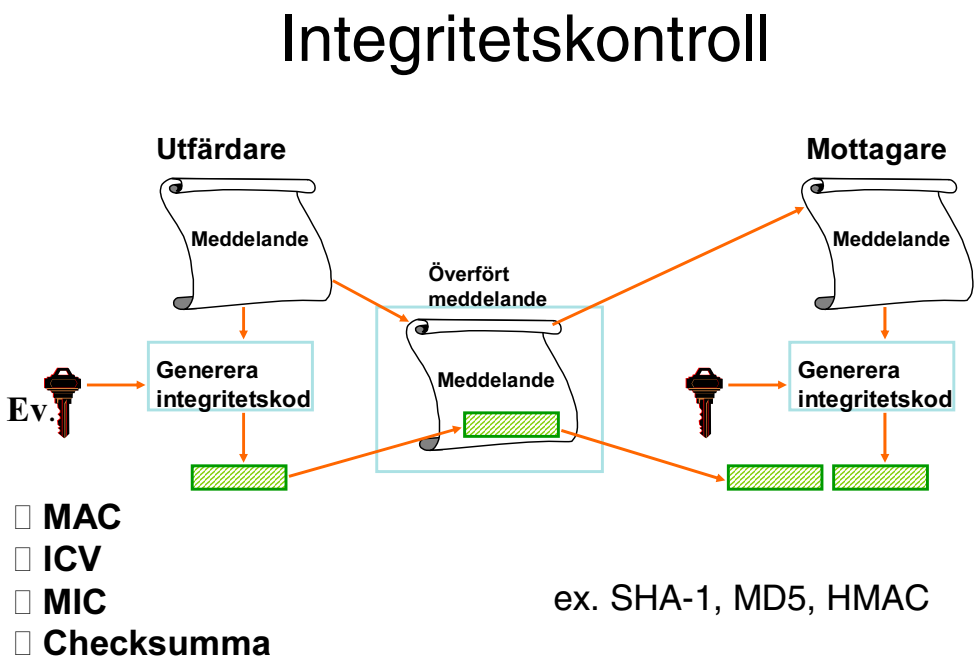
Det räcker oftast inte med att enbart räkna ut en hashsumma av en given informationsmängd. Om hashsumman skickas tillsammans med meddelandet är det bara för en angripare att lista ut vilken algoritm det är som används för att därefter beräkna en ny hashsumma sedan de valda förändringarna gjorts i meddelandet. I och med att mottagaren inte vet det ursprungliga värdet kommer denne heller inte att upptäcka om det ursprungliga värdet förändrats. Det fattas med andra ord något för att skapa det integritetsskydd vi eftersträvar.

Om brukandet av en hashalgoritm kompletteras med en hemlig nyckel kan vi kryptera hashsumman på ett sådant sätt att endast sändaren och mottagaren vet meddelandets ursprungliga hashsumma. Om en angripare längs vägen försöker förändra meddelandet kommer denne inte att kunna generera en ny hashsumma eftersom den måste krypteras med en nyckel som angriparen saknar. Förändringar kan ske, men det kommer att upptäckas hos mottagaren när denne gör sin kontroll.

[41] **NIST** står för *National Institute of Standards and Technology* (http://www.nist.gov/), som är en statlig institution i USA för teknisk standardisering och sorterar under US Department of Commerce. [Web 17].

I figur 23 visas grundprincipen vid beräknandet av en hashsumma samt vid beräknandet av ett MAC värde. Om vi på något sätt krypterar hashsumman får vi vad vi kallar ett MAC värde. MAC värdet beräknas som en funktion av meddelandet och den nyckel som används enligt formeln $MAC_M=F(K_{AB}, M)$. Detta MAC värde kan även användas för autenticering. MAC är en vanlig benämning av detta värde [Stallings, 2003]. Andra vanligt förekommande benämningar är MIC, ICV och checksumma.

Om vi antar att det endast är avsändaren och mottagaren som känner till den hemliga nyckeln så kommer beräknandet av ett MAC värde inte bara att innebära att vi säkrat meddelandets integritet, utan vi har även autenticerat avsändaren. Ingen annan än avsändaren kan nämligen kryptera någonting som mottagaren kan dekryptera och samtidigt få en identisk hashsumma vid beräkning av en ny hashsumma. Därmed har vi uppnått syftet med att dels säkerställa att avsändaren är den som denne utgivit sig för att vara samt funnit en metod för att säkerställa att data inte förändrats under mellanlagring och transport.



Figur 23 Princip för beräkning av hashsumma och MAC [Web 9].

8.19 PKI

PKI[42] kan sägas vara en infrastruktur för säker hantering av öppna nycklar som bland annat möjliggör följande önskvärda egenskaper:

- **Stark autenticering**

  Stark autenticering är till för att försvåra inloggning av obehöriga användare och handlar om att tillföra något som man har till det man vet. Normalt kanske det endast räcker med att använda sig av ett användarnamn och ett lösenord för att få access till ett system, men genom att använda sig av stark autenticering så kan man lägga till kravet på att användaren innehar ett certifikat som bundits till användaren genom en betrodd tredjepart. Ytterligare en faktor som skulle kunna tillföras är något som man är, d.v.s att man lägger till ett biometriförfarande som t.ex. fingeravtryck eller iris.

[42] PKI – Public Key Infrastructure

- **Digital signatur**
  En digital signatur möjliggör en elektronisk motsvarighet till användarens namnunderskrift i och med användandet av en privat nyckel som endast användaren har tillgång till. Genom att kryptera hashsumman av ett meddelande med avsändarens privata nyckel har avsändaren signerat meddelandet. Eftersom mottagaren har tillgång till avsändarens publika nyckel kan denne verifiera att signaturen utförts med certifikatsinnehavarens privata nyckel [Mitrović, 2003]. Se vidare under avsnitt 8.21 om signering.

Det centrala begreppet inom PKI är ”förtroende” eftersom PKI:s främsta uppgift just är att skapa förtroende för digitala identiteter [Mitrović, 2003]. Det är även inom detta centrala begrepp som det stora problemet ligger när det gäller PKI, nämligen frågeställningen ”vem kan man lita på”? Problemet uppstår vid samverkan med en extern part eftersom en tredjepartutgivare av certifikat då behövs. Situationen går att likna med att man för det mesta känner större förtroende för en ny kontakt om den blir introducerad av en gemensam vän och det är där en certifieringsinstansen (CA – Certification Authority) kommer in i bilden

En CA:s uppgift kan enkelt sägas vara att underlätta säker kommunikation mellan dess nyttjare. Detta gäller speciellt i de fall två parter ej haft någon tidigare kontakt och således ej har några säkerhetsmekanismer som de kan använda sig av sinsemellan [SIS HB 550, 2003, 2003]. En CA organiseras så att den har ett antal användare som blivit säkert identifierade och registrerade hos denna. I samband med detta godkännande delar CA:n ut ett certifikat som bevisar är denna användare är identifierad och godkänd. Säkerhetsparametrar distribueras till användarna så att kommunikation mellan användarna kan ske på ett säkert sätt eftersom de vet att certifierade användare är lika med godkända användare. CA:n blir i detta fall den centrala noden eftersom det är denna instans som svarar för att ge ut certifikat till godkända användare.

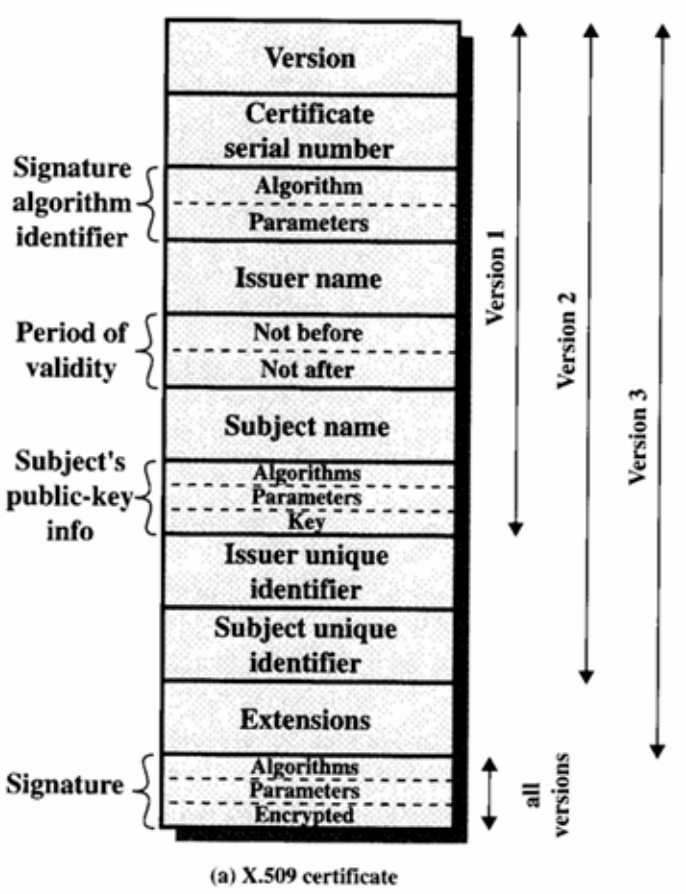
Man bör även beakta problemet med att de olika externa samarbetsparterna eventuellt kan finns utspridda över hela världen[43]. ”Förtroende” för denna tredjepartsutgivare blir då ett bekymmer eftersom en CA som är betrodd i Sverige inte helt säkert är betrodd i Frankrike.

8.19.1 Certifikat

Begreppet certifikat hör hemma i en PKI-miljö och är ett sätt att binda en unik person till dennes publika nyckel. Genom en betrodd part, i det här fallet en CA, kommer CA:n att gå i god för att innehavaren av aktuell publik nyckel tillhör en viss person. Om vi inte litar på detta faller hela tilltron som en PKI-struktur bygger på. Utan denna namnbindning skulle det vara fullt möjligt för en avsändare att skicka ett hemligt meddelande till en person som utger sig för att vara någon annan.

Ett certifikat innehåller olika uppgifter beroende vilken version av X.509 standarden man pratar om. Den senaste versionen i skrivande stund är X.509.v3, vilket innebär version tre (se figur 24). Styrkan i ett certifikat ligger i att det signerats av den betrodda parten, CA:n [Stallings, 2003]. Signeringen följer en teknik som vi går igenom under punkt 8.21.

[43] En CA kan även verka internt inom en organisation.



Figur 24 Versioner av X.509v3 (version tre) certifikaten [Stallings, 2003]

8.19.2 Digitala signaturer samt certifikat

Ett av de vanligaste användningsområdena för asymmetrisk kryptering är autenticering, det vill säga att säkerställa vem som är vem. Autenticering kan ske på många sätt men när det sker med nycklar så kommer man in på begreppet digital signatur. En digital signatur kan sägas vara en elektronisk motsvarighet till en persons underskrift på ett papper. Genom att en avsändare använder sin privata nyckel vid kryptering kan mottagaren säkerställa hans/hennes identitet genom att mottagaren dekryptera med samma persons publika nyckel. Om det dekrypterade meddelandet blir ett förutbestämt värde så bekräftar det avsändares identitet eftersom endast han/hon har tillgång till sin egen privata nyckel. Ingen annan kan ha sänt samma meddelande om inte den privata nyckeln är forcerad. (Se avsnittet 8.21 om signering).

Problemställningarna vad gällande området kring digitala signaturer ligger i att signaturen måste vara svår att förfalska samt att mottagaren inte skall kunna neka till att de mottagit det signerade dokumentet eller motsvarande. Följande process beskrivs i boken ”Handbok i IT-säkerhet” [Mitrović, 2003]. vad gäller standarder för kryptering och ”hashning” i samband med digital signering:

- *Avsändaren beräknar en kontrollsumma på den information som skall signeras via en hashalgoritm.*
- *Kontrollsumman krypteras med avsändarens privata nyckel och läggs till original informationen. Observera att original informationen i detta specifika fall inte är krypterad.*

- *Informationen sänds till avsändaren.*
- *Mottagaren dekrypterar checksumman med avsändarens publika nyckel samt genererar ett nytt hashvärde på den mottagna informationen. Den nya kontrollsumman jämförs därefter mot den dekrypterade kontrollsumman. Om summorna överensstämmer så bekräftar det dels avsändarens identitet samt att meddelandet är autentiskt, d.v.s att ingen information är borttagen, ditlagd eller i övrigt förändrad.*

Ett annat användningsområde för digitala signaturer är så kallade digitala certifikat. Dessa används främst till att verifiera att en publik nyckel tillhör en given person[44]. Certifikatet för en person består av hans/hennes publika nyckel, information om innehavaren, certifikatets giltighetstid samt ett hashat värde av hela innehållet. Detta hashade värde signeras även av en tredje part nämligen certifikat utfärdaren. Den tredje parten, även benämnd ”tillförlitlig tredje part” – TTP[45] eller certifieringsinstans, måste vara betrodd av alla inblandade parter för att certifikatet skall vara trovärdigt. För att hålla reda på vilka certifikat som är giltiga och vilka som skall dras in och upphöra så har man en revokeringslista[46].

Boken ”Handbok i IT-säkerhet” [Mitrović, 2003]. beskriver följande process vid tilldelning av ett certifikat:

- *En användare genererar ett nyckelpar bestående av en publik- samt privat nyckel*
- *En förfrågan, innehållandes nyckelparet, om tilldelning av ett certifikat skickas till TTP*
- *TTP validerar användarens identitet genom t.ex. en fysisk legitimationskontroll*
- *TTP utfärdar ett certifikat till användaren*
- *Användaren lagrar certifikatet i ett aktivt kort eller krypterat på hårddisken etc.*
- *Användaren samt TTP offentliggör certifikatet*

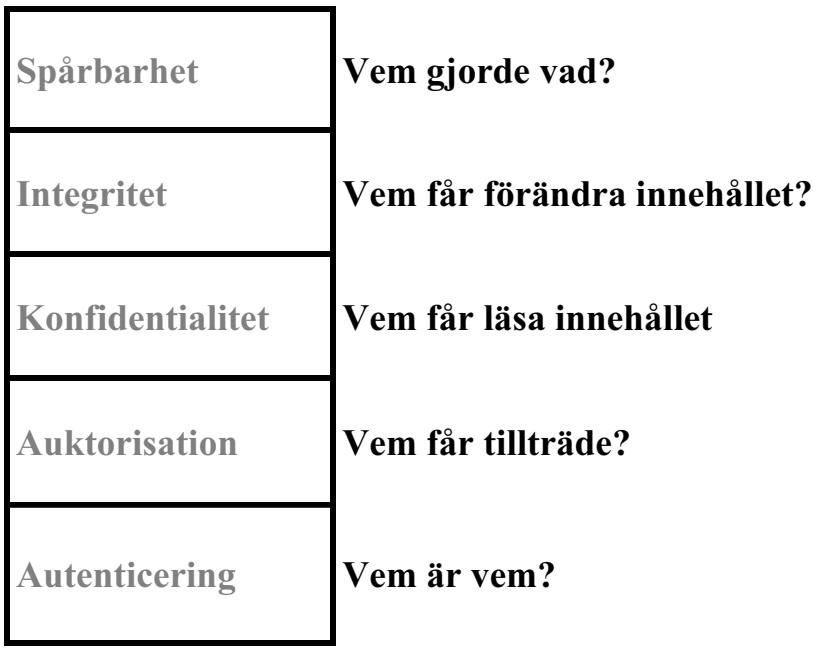
8.20 Autenticering

Eftersom en dator inte kan skilja mellan elektriska signaler från olika användare måste användaren bevisa sig identitet på något sätt. Det finns olika lösningar för hur detta kan gå till, där de olika lösningarna i sin tur har olika grad av säkerhet. Vanligaste sättet att bevisa sin identitet för ett system är att visa att man känner till en hemlighet som delas mellan användaren och systemet, lösenord. Eftersom lösenord måste vara möjliga att minnas så tenderar de flesta av oss att välja lätta lösenord [Pfleeger, 2000].

Lösenord är en kod som bygger på en ömsesidig överenskommelse mellan användaren och systemet. Användaren kan ibland skapa sitt eget lösenord medan det i andra fall kan skapas av systemet. Både längd och format av lösenordet kan variera beroende på inställningar hos systemet eller nivån av säkerhetsmedvetande hos användaren. Ett längre lösenord tar längre tid att knäcka, och blandar man tecken som stora och små bokstäver med andra tecken på tangentbordet blir lösenordet ännu svårare att knäcka, men även svårare att minnas [Pfleeger, 2000]. Det uppstår med andra ord en mänsklig konflikt mellan säkrare lösenord och människans förmåga att minnas dessa.

[44] I detta exempel använder vi en person men certifikatet kan lika gärna gälla en organisation, router, farkost mm
[45] Den internationella beteckningen är ”Certification Authority” - CA
[46] Den internationella beteckningen är ”Certificate revocation list” - CRL

Autenticeringen kan sägas vara den viktigaste delen vad gäller IT-säkerhet eftersom de flesta säkerhetsprinciper är beroende av vem som gör/gjort något i systemet [Graham, 2003]. Precis detta illustrerar figur 25 som har lagt autenticeringen som basen till alla säkerhetsaspekter. Användaren måste alltid autenticera sig för att kunna ges rättigheter i systemet. Om detta ej har skett ligger alla överliggande nivåer i säkerhetstornet blottade.



Figur 25 Säkerhetstornet [Web 20]

Många av våra system idag kräver endast användarnamn och lösenord för autenticering. Bristen i en sådan typ av lösning är uppenbar eftersom ett lösenord ofta är möjligt att gissa sig till eller helt enkelt tillförskaffa sig genom t.ex. ”social engineering”[47]. Följaktligen är det därför relativt lätt att logga in i ett system i skydd av en annan användare. Av denna anledning är det ofta önskvärt att förstärka skyddet i autenticeringsprocesser genom att lägga på ytterligare skyddsmekanismer. Vid diskussioner kring autenticering så brukar man i litteraturen presentera följande sätt för en användare att autenticera sig [Gollman, 1999, Web 20].

- **Någonting som användaren vet**

  Detta är, som vi ovan slagit fast, den enklaste typen av autenticering. Lösenord är allmänt det vanligaste men det skulle även kunna vara VISA-kortets utgångsdatum i samband med ett köp över Internet m.m.

- **Någonting som användaren har**

  Genom att kunna visa upp någonting som användaren har i sin ägo och som kan interagera med systemet så verifierar sig användaren. Oftast består detta av ett smart kort, certifikat eller en dosa för engångslösenord.

[47] Termen syftar till konsten att tillförskaffa sig information genom att på olika sätt dupera människor

- **Någonting som användaren är**

  Användaren autenticerar sig genom att låta systemet mäta hans/hennes fysiska karaktärsgrad. Denna form av metod kallas även för biometri och kan bland annat utföras genom t.ex. skanning av ögats iris, fingeravtryck eller ansiktsformen.

- **Någonting som användaren gör**

  Baserar sig inte på de fysiska karaktärsdragen som ovan utan istället försöker systemet mäta vissa beteendemässiga drag som användaren besitter som t.ex. rörelsemönster. Som exempel skulle man kunna tänka sig ett system i vilken den som skall autenticeras tecknar sin namnteckning på en särskild skärm/platta. Systemet analyserar sedan på vilket sätt vad gäller tid, intervaller samt tryck med ”pennan” som namnteckningen är skriven för att identifiera användaren.

- **Användarens placering**

  Metoden utgår från användarens placering vid inloggningsförfarandet. Lösningen kan fungera så enkelt att vissa användare endast får logga in från vissa stationer (exempelvis det egna kontoret) medan han/hon ej har behörighet att logga in i administratörens station. Det går även att tänka sig mer avancerade lösningar med hjälp av GPS[48] där användarens position sparas ned i loggen men även ligger till grund för huruvida personen skall få tillträde till systemet eller ej.

I litteratur på området så stöter man ofta på begreppet ”stark autenticering” och trots att det inte verkar finns någon vedertagen definition så menar många att stark autenticering uppnås vid en tvåfaktorautenticering, det vill säga att två metoder ur ovanstående lista väljs ut som skydd mot obehörig användning. Organisationer som polisen använder en definition som beskriver stark autenticering som en metod som använder en kryptografisk algoritm och tillhörande hemlig nyckel [Web 8]. Standardiseringsinstitutet I Sverige [SIS HB 550, 2003, 2003] definierar stark autenticering som ”*autenticering av identitet med hjälp av en kryptografisk algoritm och tillhörande hemlig nyckel”*. Oavsett vilken metod som utnyttjas så går det att slå fast att endast ett användarnamn och lösenord inte räknas som stark autenticering utan att det krävs något mer för att garantera säkerheten kring autenticering. Generellt kan man säga att ju känsligare information som ett system hanterar och ju allvarligare hoten är, desto högre krav ställs det på åtkomstskyddet [SIS HB 550, 2003].

Tillfällen när det kan vara aktuellt för två parter att autenticera sig för varandra är när man vill förhindra möjligheten till en attack som heter ”Man-In-The-Middle”. I korthet går en sådan attack till på så sätt att en angripare ställer sig i mitten mellan de två kommunicerande parterna. För klienten utger sig angriparen för att vara servern, och för servern utger sig angriparen för att vara klienten. De uppfångade klientanropen fångas upp och besvaras med förfalskade serversvar. På så sätt kan en användare bli lurad att avge sitt lösenord [McClure et al, 2003].

[48] **GPS** står för *Global Positioning System* och är ett militärt system av navigationssatellit?er (RNSS), tillhörandes USA [Web 18].

Motåtgärder mot MIT attacker kan ske genom att både klient och server skickar sina certifikat till varandra i samband med autenticeringen. SSL[49] (Security Socket Layer) innehåller som tillval en dubbelsidig autenticering, men bygger på att både klienten och servern är innehavare av den andra partens CA:s certifikat för att kunna kontrollera att certifikaten är äkta och utgivna av en betrodd part. En annan metod är att förse parterna med så kallade fördefinierade nycklar, vilka motsvarar certifikaten om dessa garanterat kan hållas hemliga. Vad som framgår i nedan (avsnitt 8.20.1) är att det inte räcker med att parterna skickar över sina certifikat till varandra. För att en autenticering skall ske krävs ett utbyte av data som krypteras och dekrypteras med parternas privata och publika nycklar.

8.20.1 Exempel på tillämpning av stark autenticering

X.509 standarden inkluderar tre olika alternativa autenticeringsmetoder. Var och en av dem drar nytta av den PKI-struktur som finns uppbyggd inom organisationen, eller mellan organisationerna. I de exempel som följer angående envägs- tvåvägs- och trevägsautenticering förutsätts det att de två parterna känner till varandras publika nycklar. Åtkomsten till de publika certifikaten kan ske via en katalog eller genom att dessa skickas tillsammans med det meddelande som klienten initierar [Stallings, 2003].

8.20.1.1 Envägsautenticering

Envägsautenticeringen innebär en enda överföring av information från användaren (A) till mottagaren (B) och fastställer följande.

1. *Identiteten på A och att meddelandet är genererat av A.*
2. *At meddelandet är avsett för B.*
3. *Integritet och originalitet (att det inte sänts flera gånger) av meddelandet.*

Som ett minimum krävs följande information i det initierade meddelandet mellan A och B (se figur 26).

t_A — *En tidstämpel. Tidstämpeln i meddelandet består av ett tidsintervall (när meddelandet skapats och vald giltighetstid). För att undvika replay attacker får inte samma slumptal användas inom aktuellt tidsintervall. Skulle det komma ett nytt autenticeringsmeddelande från (vad det verkar) samma part med samma slumptal och giltighetstid så kan det inte vara en giltig avsändare utan är ett replay försök.*

r_A — *Ett slumptal slumpas fram hos klienten. Slumptalet är till för att förhindra en replay attack, och är förknippat med* **t_A**. *Målsystemet kan lagra slumptalet till det att giltighetstiden i tidstämpeln har gått ut. Därmed kommer förnyade autenticeringsförsök med samma slumptal att uppfattas som replay attacker.*

ID_B — *Identiteten på målsystemet, d.v.s. serverns ID.*

[49] SSL är en lösning som ger möjlighet till en krypterad förbindelse mellan klient- och serverapplikationer på Internet (Dyson, 1999).

Hela autenticeringsmeddelandet signeras med avsändarens privata nyckel $K_{Ap}(t_A, r_A, ID_B)$. Genom att B har tillgång till A:s publika nyckel, och även litar på att denna nyckel tillhör A genom att lita på den CA som signerat A:s certifikat, så kan målsystemet B autenticera A genom att beräkna ett eget hashvärde på den informationsmängd som A skickat. Därefter kan B jämföra detta varde med det signerade hashvärdet som A krypterat med sin privata nyckel, men först måste B dekryptera det krypterade hashvärdet med A:s publika nyckel. Om värden överensstämmer har A bevisat sin identitet för målsystemet B, och A har därmed autenticerat sig för målsystemet B.

8.20.1.2 Tvåvägsautenticering

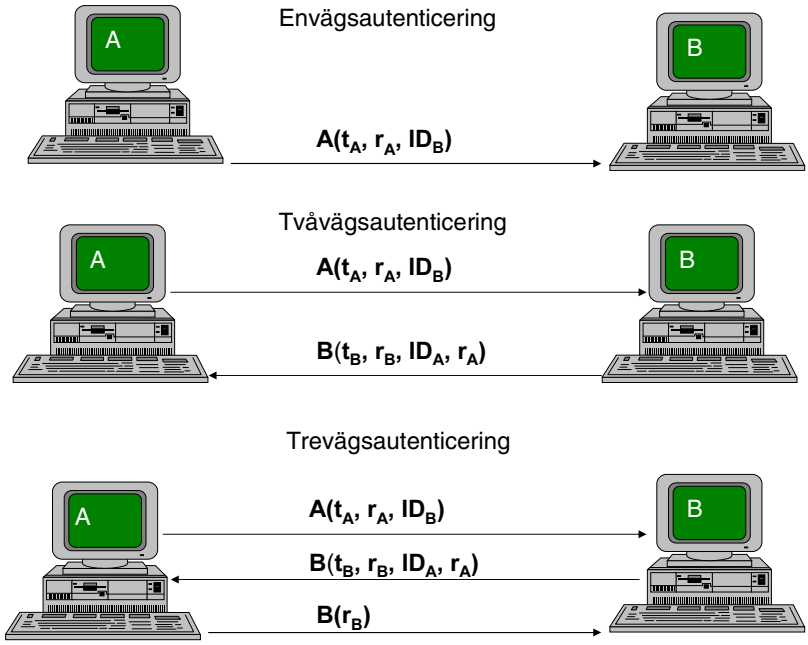
En tvåvägsautenticering innebär att även mottagaren B autenticerar sig för avsändaren A. Denna metod kallas även för ömsesidig autenticering. Vad som tillkommer till de tre uppräknade posterna under envägs autenticeringen är följande.

4. *Identiteten på B och att det mottagna meddelandet är genererat av B.*
5. *Att meddelandet är avsett för A.*
6. *Integritet och originalitet*

Det mottagna meddelandet från B innehåller slumptalet från A för att validera svaret. Det innehåller även en tidstämpel (t_B) och ett slumptal (r_B) genererat av B samt identiteten på A. B:s meddelande är signerat med B:s privata nyckel $K_{BP}(t_B, r_B, ID_A, r_A)$.

8.20.1.3 Trevägsautenticering

I en trevägsautenticering svarar A på B:s meddelande genom att skicka ett meddelande som endast innehåller en signerad kopia av B:s genererade slumptal.



Figur 26 Stark autenticering enligt X.509 [Stallings, 2003].

8.21 Signering

Ett vanligt återkommande begrepp när man talar om autenticering och integritet är signering. Att signera någonting innebär att avsändaren krypterar hashsumman som räknas ut av en viss informationsmängd så att denna skyddas. För detta ändamål används hashalgoritmer som MD5, SHA-1 och HMAC. Krypteringen av hashsumman kan ske med antingen symmetrisk eller asymmetrisk kryptering. Begreppet MAC blir därmed aktuellt.

I figur 24 visas ett certifikat där rutan längst ner innehåller begreppet ”signature” (signatur). Eftersom informationen i certifikatet måste vara läsbart kan certifikatet i sig inte krypteras. Samtidigt vill man vara säker på att ingen information i certifikatet förändrats. Detta löses genom att CA beräknar en hashsumma på hela certifikatet och sedan krypterar hashsumman med sin privata nyckel. Genom detta förfarande är certifikatet signerat av CA.

Alla i en PKI-miljö har tillgång till CA:s certifikat, och därmed dess publika nyckel. Varje gång ett certifikat behöver användas kommer klienten eller servern att validera om det rör sig om ett äkta certifikat genom att först beräkna en egen hashsumma på certifikatet, dekryptera MAC-värdet (i PKI-miljön kallas detta värde för MIC) med CA:s publika nyckel och sedan jämföra de båda hashsummorna. Är de lika är certifikatet äkta.

Ytterligare jämförelser görs för att kontrollera om certifikatet är giltigt eftersom det av olika anledningar kan vara revokerat (återkallat). Detta t.ex. på grund av att certifikatets giltighetsperiod gått ut eller för att man misstänker att något av nyckelparen kan ha kommit i fel händer [Stallings, 2003].

8.22 Skadlig kod

När vi pratar om skadlig kod avser vi sådan kod som genererar händelser som inte är önskvärda och som vi saknar kontroll över. Vanligtvis ställer sådan kod till med skada, men inte alltid. Den skadliga koden kan benämnas som virus, trojaner, webbtrojaner och maskar. Det finns en viss skillnad mellan dessa, och även om vi i denna uppsats mest pratar om trojaner så kan t.ex. en mask som sprids via e-post, Messenger tjänster, fildelningsprogram eller säkerhetshål i operativsystemen ställa till med lika stor skada.

En trojan är en programvara som medvetet innehåller funktioner som inte framgår av beskrivningen av programvaran. Dess syfte är oftast att underlätta intrång i andra människors datorer. Tre av de mest kända trojanerna är Back Orifice, NetBus och SubSeven. Gemensamt för dessa trojaner är att de som regel installeras som tjänster bakom kända portar och att klientprogramvaran som körs på angriparens dator kan skanna stora delar av ett nät i syfte att leta efter infekterade datorer, d.v.s. efter datorer som svarar med aktuell tjänst bakom angivna portar. De datorer som svarar upprättar en förbindelse med klienten hos angriparen och den angripna datorn fungerar nu som en server. Via trojanen har angriparen åtkomst till samtliga resurser på den smittade datorn. Det innebär att en angripare utifrån kan köra de applikationer som den legala användaren kör på sin egen dator.

Vanligtvis döljer sig ovan namngivna trojaners portar ovanför portnummer 1.024, vilket innebär att en brandvägg som är konfigurerad att inte släppa igenom trafik på högre portnummer ganska effektivt kommer att stoppa anropen utifrån. En trojan som inte följer just detta mönster, utan självständigt anropar sin ”husse” kommer att initiera trafiken från insidan av brandväggen. Sådana anrop är brandväggen inte alltid konfigurerad att stoppa, eftersom det mesta som initieras från insidan släpps igenom.

För att åskådliggöra hur lätt det är för en person att ändra administratörslösenordet på en dator, och därmed kunna installera vilken kod som helst, tar vi upp en diskussion angående olika typer att programvara som är åtkomlig på Internet för detta ändamål. Syftet med diskussionen är att läsaren skall förstå att ett lösenord på datorn inte hindrar den som har fysisk åtkomst till datorn att komma åt och ändra dess säkerhetsrelaterade parametrar.

Den tyska programmeraren Klaus Knopper har skrivit en programvara som inte behöver installeras på hårddisken. Istället för att installera Linux på hårddisken har Knopper gjort en Linux-version som kan köras från en CD/ROM. Därmed berör den över huvud taget inte själva hårddisken. Teknologin kallas "live CD" teknologi därför att du kör programvaran från en CD/ROM [Web 10].

KNOPPIX är en kompilation av GNU[50]/Linux programvara. Den känner automatisk igen och stödjer många typer av skärmkort, ljudkort, SCSI-enheter[52] och annan utrustning som finns i din dator. Den laddar ett mini Linux operativsystem som bootar en dator varpå det nya operativsystemet läses in i datorns RAM-minne.

Det finns även andra verktyg för att boota om en dator. Ytterligare en länk varifrån man kan tanka ner en bootbar programvara är från Peter Nordahls webbsida http://home.eunet.no/pnordahl/ntpasswd/. Han har skapat ett verktyg som kan boota om en dator och bland annat byta ur lösenorden i SAM[53]-databasen. Verktyget kan även redigera registret.

Den mest kraftfulla bootbara programvara vi funnit hittills i vårt sökande efter denna typ av verktyg är "Super WinPE Plus 2004 Multi-Bootable All-In-One CD". Det är en multi bootbar CD som samlat fyra olika versioner av Windows Preinstallation Environment (WinPE) i en enda CD. WinPE utgörs av ett minimalt operativsystem som är baserat på Windows XP:s kärnan. Det ger en komplett Win32 miljö med möjlighet till nätverkskoppling och ett grafiskt gränssnitt. Det stödjer filsystem som FAT/FAT32/NTFS/CDFS.

Med hjälp av boot verktyget kan man boota om en dator varefter det finns ett antal olika alternativ att välja mellan. Ett är att fritt röra sig på datorns hårddisk där det finns möjlighet att ta del av all information samt installera ny programvara. Det medger t.ex. en möjlighet att ta sig till C:\WINDOWS\system32\config där man på ett enkelt sätt kan byta ut både SAM-databasen och/eller någon av loggdatabaserna. Det innebär att man därefter kan boota om datorn sedan man fört över sin egen SAM-databas med sina egna lösenord till datorn, varefter systemet är öppet för angriparen genom att denne nu kan logga in med sitt eget konto och lösenord. Man kan även göra installationer direkt från CD/ROM-skivan. När man är klar skriver man in den gamla SAM-databasen och loggdatabaserna varpå ingen kan märka x att någon förändring skett, vare sig i loggar eller SAM-databas.[54.]
En nyligen utgiven doktorsavhandling av Caroline Linda Allinson vid Queensland University of Technology [Allinson, 2004] tar upp ett antal sätt att manipulera en dators säkerhet, varav

[50] **GNU** står för "GNU's Not Unix" (GNU är inte UNIX), och är ett projekt styrt av FSF (Free Software Foundation) med målet att skapa ett Unix-liknande operativsystem som helt bygger på fri programvara.
[52] SCSI (Small Computer System Interface) är ett gränssnitt som medger en metod att koppla en dator till en extern enhet genom att endast behöva använda en port [Dyson, 1999].
[53] SAM (Security Accounts Manager) utgör hos operativsystemet Windows det säkerhetssystem som hanterar och tillhandahåller access till konton. Konton lagras i SAM-databasen [Dyson, 1999].
[54] Däremot torde en grundlig analys av hårddisken kunna ge ledtrådar till detta

möjligheten att komma åt lösenordsfilen genom att boota om datorn är ett sätt att installera okänd kod på klienten.

En faktor som ökar sannolikheten för en organisation att få in elak kod i sitt nät är om organisationen har en kopplig mot Internet. Färsk undersökning hävdar idag att de flesta attackerna mot en organisation kommer via nätverket från utsidan. Samtidigt indikerar det mesta att de mest kostsamma attackerna genereras från insidan av en organisation via så kallade insiders [Alberts & Dorofee, 2003].

9. Empiri

I detta kapitel samanställer vi den information som framkommit vid våra intervjuer samt genomgång av utvalda rättsfall. Resultatet från intervjuerna presenteras utifrån de olika yrkeskategorierna som intervjuats medan resultat av rättsfallen redovisas separat. Observera att intervjuerna återfinns i sin helhet under bilagorna till arbetet. Läsaren kan där fördjupa sig i de olika informanternas synpunkter angående loggning.

9.1 Sammanställning av genomförda intervjuer

9.1.1 Informanter inom polisens utredningsavdelningar

Bergnér, som ofta arbetar med förundersökningar som omfattar loggar, har aldrig blivit presenterad för hur händelsekedjan ser ut inom polisens egen organisation när det gäller en logg väg från födelse till det att den når enheten. Där behandlas i regel loggutdragen vidare genom manuellt arbete. Han känner inte till hur en logg skulle kunna manipuleras bortsett från den manuella hanteringen som loggen utsätts för sedan den nått hans enhet. Där konverterar han dem i regel från textformat till Excel. Bergnér känner inte till att någon någonsin ifrågasatt loggens riktighet. [Bergnér]

Inte heller Keyzer känner till något fall där en misstänkt ifrågasatt loggarna med innebörden att dessa skulle ha varit felaktiga. I övrigt menar Keyzer att loggutdragets bevisvärde starkt förknippat med den misstänktes inställning till brottsmisstanken. Det är skillnad om den misstänkte erkänner det som loggen anger eller om denne förnekar. Dessutom är frågan kopplad till den aktuella organisationens interna regelverk som styr befogenheten att få ta del av viss information.

Keyzer är medveten om att det finns goda möjligheter att manipulera en logg. Framför allt är detta möjligt vid den manuella hanteringen. Så sker ofta inom den organisation som lämnar över loggen till polisen, och då loggen endast tas emot utan att Keyzer eller hans kollegor varit med om själva framtagandet så inser han att de saknar kontroll på informationens äkthet i det loggmaterial som lämnas över. Man tvingas då att lita på loggarna och den organisation som lämnar över dem. Att ifrågasätta dem av egen kraft förekommer inte. En inkommen CD-skiva med loggar, eller färdigutskrivna papper med loggar, från en organisation kommer att få en framskjutande roll i en förundersökning. Detta oavsett autenticeringsmetod eller kännedom om vem som tagit fram loggarna. Vidare medger han att man som regel har större tilltro till en logg som kommer från en större organisation som IBM, än från mindre kända organisationer. [Keyzer]

Även Leijon menar att det är viktigt att komma ihåg att den misstänktes inställning är av vikt för frågan om vad det är som loggutdragen visar. Ifrågasättande leder som regel till fördjupade kontroller. Det är dock Leijons uppfattning att loggutdragen inte behandlas mer kritiskt bara för att den misstänkte förnekar de handlingar som loggen visar. I stället är det tvärt om. Ett förnekande möts med loggutdraget som underlag för att ifrågasätta den misstänktes berättelse. Lägger man fram ett loggutdrag så behandlas det normalt som ett bevisbärande dokument som ingen ifrågasätter. Förnekar den misstänkte blir loggen ett bevis mot denne. [Leijon]

Första gången Bergnér blev medveten om att en logg kan vara fel var i anledning av loggkontrollen mot polisanställda i Anna Lindh ärendet. En av författarna till denna uppsats gjorde honom då för första gången uppmärksammad på att loggarna inte var korrekta. Bland annat visade det sig att dessa var framtagna med olika script, och att vissa loggutdrag endast visade svaren på en slagning, och inte vilken fråga som ställdes. [Bergnér]

När det gäller frågan vem som ansvarar för innehållet i loggutdragen så anser Leijon att ansvaret för hans del startar när han fått loggutdragen i sin hand. Sedan man fått dessa i sin besittning är utgångspunkten otvetydigt att loggarnas innehåll är sanningsriktig. Det är ingenting som man ifrågasätter. Vidare så ställer man inga frågor med innebörden att värdera informationen som finns i loggarna, frågor som hur användaren bevisat sin identitet för målsystemet m.m. utan tilltron till loggen är total oavsett autenticeringsmetod. Vidare berättar Leijon att man inte heller ställer frågor om hur de lokala nätverken ser ut hos de organisationer som genererat loggutdragen. Man litar på loggutdragen och av den anledningen ställer man varken frågor om näten är switchade eller hubbade eller om lösenorden transporteras i klartext i nätverket. Varken Leijon eller hans kollegor ställer denna typ av frågor. Han berättar även att han ofta kommer i kontakt med loggar i form av telefonlistor och transaktionsloggar från teleaktörer och banker. Vanligtvis skickas dessa per post, antingen utskrivna på papper eller på CD-skiva. Det händer vanligtvis att han hanterar loggarna manuellt i syfte att göra dem mer lättförståeliga. [Leijon]

Bergnér anser att loggutdragen i regel är svårhanterliga. Dess komplexitet medför att det kan bli svårt för en domstol att tolka dem. Det händer att domstolarna inte har förstått loggutdragen och därmed valt att fria framför att fälla. Juridisk personal utgår från att loggarna är korrekta eftersom de inte haft någon anledning att ifrågasätta dessa. De måste kunna lita på att loggarna är korrekta. [Bergnér]

Leijon hänvisade till det så kallade Perstorpsärendet för att visa hur sårbara system är som endast bygger på lösenordsbaserad inloggning. Med mycket enkla medel kunde gärningsmannen lura sin chef att logga in i kommunens ekonomisystem med sitt administratörskonto och lösenord. Gärningsmannen kunde se över chefens axel vilket lösenord som användes, varefter detta lösenord kom att användas när gärningsmannen gjorde överföringar till olika konton från kommunens ekonomisystem på cirka 20 miljoner kronor. [Leijon]

När det gäller brott mot behörighet eller befogenhet inom en organisation brukar man be den egna organisationen att plocka fram loggarna som visar detta. Dessa lämnas sedan över till polisen. I undantagsfall är det Keyzers avdelning som tar fram loggarna. Detta sker endast om datorerna tagits i beslag så att maskinen rent fysiskt finns i polisens ägo. I dag finns det en reell möjlighet att en trojan legat bakom trafiken som genererats från en viss användares dator. Av den anledningen undersöker man i dag rutinmässigt beslagtagna hårddiskar för att se om det finns trojaner, eller spår av trojaner, på hårddisken. Vidare så ser Keyzer en logg mer som en pekare på att någonting har hänt, och i och med att de ofta kan ta aktuell dator i beslag finner de oftast bevis på hårddisken som gör att man inte är beroende av loggen på samma sätt som man vore utan en beslagtagen dator. [Keyzer]

På Keyzers avdelning arbetar man mycket mot speciella IT-åklagare vilket är viktigt eftersom dessa har större kunskaper inom IT-området än vad vanliga allmänna åklagare har. IT-åklagarna är mer kunniga inom området och kan därför vara mer ifrågasättande och kan även bedöma materialet annorlunda än vad en allmän åklagare kan göra. [Keyzer]

9.1.2 Informanter inom åklagarmyndigheten

Det har aldrig hänt att någon som loggutdragen omfattar hävdat att loggutdragen skulle ha varit felaktiga. Bland dem som försvarar sig, vilket ofta är personer med bra datorkunskap, är den vanligaste förklaringen att loggutdragen i sig kanske är riktiga, men att händelserna som loggats utförts av någon annan. Om en misstänkt lämnar denna förklaring, och det inte finns någon annan bevisning, är det Roswalls uppfattning att denne då kan gå fri. Om det av någon anledning endast är på så sätt att det är loggen som utgör bevisningen och den misstänkte inte gör några medgivanden så kommer det att bli mycket svårt att få en fällande dom. Roswall är generellt motvillig till att bygga upp ett åtal enbart på loggar eftersom det inte finns någon logg som är 100 procent säker. Det krävs kompletterande bevisning som stödjer en logg. [Roswall]

Inte heller Ekelund känner inte till att någon någonsin ifrågasatt äktheten i en logg. Vidare menar han att när det gäller loggar ligger det en okunskap med i botten i och med att denna form av teknik inte är känd för vem som helst och den misstänkte vet helt enkelt inte vad han skall ifrågasätta. Den vanligaste formen av försvar om man nekar till brottet är att hävda att slagningen i stället utförts av någon annan. [Ekelund]

Engfeldt menar på att eftersom det hittills inte hänt att en misstänkt har nekat till en slagning som bygger på ett loggutdrag så har det inte blivit någon diskussion om loggarnas riktighet. Eftersom det inte skett något ifrågasättande av loggarna bör detta indikera på att loggutdragen är korrekta. Det ligger i det generella arbetet att det material som presenteras för åklagaren är framtaget på ett korrekt sätt och att det därmed inte skall kunna innehålla några felaktigheter. Vidare menar Engfeldt att en av orsakerna till att det inte blivit någon diskussion om loggarnas riktighet bör vara att de i regel är svåra att förstå. Till detta kommer att kunskapen om hur loggen genereras och hanteras är ett tämligen okänt område, och då den misstänkte inte ifrågasätter denna kedja leder det till att det i allmänhet inte blir någon diskussion om loggarna. Denna frånvaro av ifrågasättande har även lett till att det inte funnits någon anledning till att ta ställning till olika autenticeringsmetoder. Av samma anledning har det heller inte varit aktuellt att som åklagare sätta sig in i frågor som hur en logg transporteras eller annars hanteras från sin födsel till presentation. [Engfeldt]

När det gäller frågan om vad som skulle hända om en misstänkt ifrågasatte ett loggutdrag så menar Roswall att om en misstänkt person nekar till en anklagelse så måste åklagarsidan börja söka efter alternativa förklaringar. Exempel på sådana är att se vilka autenticeringsmetoder som använts, att leta efter trojaner eller att se vilka möjligheter det finns för någon annan att se den misstänktes lösenord över axeln. [Roswall]

Även Engfeldt tillfrågades hur han som åklagare skulle ställa sig i åtalsfrågan om en misstänkt person förnekar loggutdraget med motiveringen att denne inte ligger bakom den trafik som loggutdraget påstår. Antingen är loggarna korrupta eller så har trafiken orsakats av någon annan. Som svar på denna fråga svarade Engfeldt att det vid alla bevisvärdering finns en huvudregel som säger att man skall lita på vad den misstänkte har att säga så tillvida att det denne säger kan lämnas utan avseende eller motbevisas. Kan man lämna den misstänktes berättelse utan avseende eller motbevisa den kan man bortse från vad den misstänkte säger. Det innebär att man som åklagare i ett fall där loggutdraget ifrågasätts blir tvungen att göra en djupare undersökning kring möjligheten för någon annan att ligga bakom den trafik som loggutdraget anger.

För detta arbete skulle man vara tvungen att involvera sakkunnig personal som gör en undersökning kring möjligheten att manipulera systemet eller systemen i fråga. Engfeldt exemplifierar sitt resonemang med radarn som kom på 70-talet och som gav polisen en möjlighet att fånga bilister som körde för fort på ett annat sätt än tidigare. En av dem som fastnade i denna kontroll i ett tidigt skede var en radartekniker som starkt ifrågasatte den nya tekniken. Av den anledningen gjordes det en omfattande undersökning där man gick igenom de argument som mannen framförde och närmare undersökte vilka fel den nya tekniken kunde ha. Resultatet blev att domstolen fällde teknikern och alla andra som senare åtalades med nämnda teknik. Engfeldt är övertygad om att någonting liknande skulle inträffa om någon börjar ifrågasätta dagens loggar så som den tidens radarteknik ifrågasattes på 70-talet. [Engfeldt]

Ekelund menar i sin tur att när det gäller bevisvärdering av en logg så behandlas den på samma sätt som alla annan skriftlig bevisning. Så länge som ingen påstår någonting annat litar man på den skriftliga bevisningen. Ifrågasätts inte loggens riktighet kommer den att tillmätas ett bevisvärde. En logg kommer däremot inte att tillmätas samma bevisvärde som t.ex. DNA eller ett fingeravtryck eftersom en logg inte kan peka ut den fysiska person som utfört slagningen, utan den talar bara om att systemet använt på ett visst sätt.

När det gäller manuellt arbete med loggar förklarar Ekelund att det ofta förekommer för att göra ett loggutdrag mer lättförståeligt. I ett moment där man vet att det krävs en manuell hantering som t.ex. översättning av en transaktionskod, ligger det en medvetenhet hos åklagaren om att sådant arbete kan leda till misstag. Det innebär att om en misstänkt skulle säga att materialet är felaktigt så måste man kontrollera detta. Som åklagare måste man dock lita på det material som polisen lämnar över i samband med en förundersökning. Den som hanterar, tar fram något som lämnas över till åklagarsidan under en förundersökning gör det med ett tjänstemannaansvar [Ekelund].

Också Engfeldt förklarar att när något hanterats manuellt på detta sätt ligger det alltid en medvetenhet om att något kan ha gjorts fel. Här ligger det ett stort ansvar hos den misstänkte. Om denne inte ifrågasätter materialet så finns det inte heller någon anledning att ifrågasätta det från åklagarsidan heller. [Engfeldt]

Ett problem med brottet dataintrång är att det är ett bötesbrott. Av den anledningen utdelas i vanliga fall ingen offentlig försvare till personer som misstänks för dataintrång. Undantagsvis kan det ske om ärendet t.ex. bedöms vara av svårare typ. Detta medför problem eftersom det många gånger är svårt för den misstänkte att försvara sig själv när bevisningen utgörs av allmänt svårförståelig teknik som loggar innebär. [Roswall]

Engfeldt instämmer i ovanstående men tillägger att för stora krav på att kalla in teknikexperter skulle kunna leda till att utredningskostnaderna blir för stora i förhållande till brottets påföljd. I sig är detta en avskrivningsgrund. Om det däremot skulle börja visa sig bli en vanlig företeelse bland misstänkta att ifrågasätta loggutdragen skulle man av allt att döma bli tvungen att ta den kostnaden. [Engfeldt]

I de fall där organisationer använder sig av grupplösenord uppstår det problem. Erfarenheterna härifrån är hämtade från sjukvården och apoteksbolaget. Detta resulterar i att åtal inte kan väckas eftersom vem som helst kan söka access till systemet i skydd av ett gemensamt användarkonto. Därför är det av stor vikt att det inom organisationerna finns skriftliga regler som reglerar när en användare får ta del av känslig information.

Saknas dessa så kan det vara ett hinder mot en fällande dom. Den misstänkte kan då hävda att denne inte kände till regler och rutiner, och i en miljö där det saknas skriftliga rutiner kan det vara svårt att bevisa motsatsen. [Roswall]

Polisen är klart överrepresenterad när det gäller förundersökningar som avser dataintrång. Ett skäl till detta är att polisen genom sitt interna regelverk i princip kriminaliserat att felaktig hantering av organisationens system. Det finns ingen annan organisation som Engfeldt känner till som har en lika hård reglering som polisen. Engfeldt förklarar även att i loggutredningen[55]avseende personal inom polisväsendet som slagit på den så kallade 24-åringen och 35-åringen har Engfeldt handlagt ett 80-tal förundersökningar. Ingen av dessa resulterade i ett åtal, utan alla kunde ange rimliga skäl till varför de utfört slagningarna. I dagsläget har tre personer fällts för dataintrång sedan de gått in i olika system som har koppling till aktuell loggutredning. Dessa har mer eller mindre utfört slagningarna av nyfikenhet. Ingen av de ärenden som Engfeldt handlagt har inneburit att någon har ifrågasatt loggutdragen. Alla har medgivit slagningarna men framfört olika skäl till varför de genomförts. [Engfeldt]

Roswalls erfarenhet är att loggarna han tar del av är av skiftande kvalitet. Detta gör det svårt för åklagarsidan att få fram fakta som visar vad som har hänt. I många fall loggas endast delar av systemet vilket gör att det många gånger inte går att få fram annat än delar av ett händelseförlopp. Följden kan bli att åtal inte kan väckas eftersom åklagarsidan inte kan bevisa hur något har genomförts. [Roswall]

Vid IT-relaterade brott är det viktigt att åklagaren ger en sorts introduktion till grundläggande datateknik/nätverksteknologi. Detta för att det skall vara möjligt för domare och nämndemän att följa åklagarens resonemang. De svenska domstolarna har mycket låga kunskaper om IT och det är Roswalls erfarenhet att domstolarnas ledamöter alltid utgår från sig själva när de skall fatta sina beslut. Det som de inte förstår själva vill de inte heller lägga någon annan till last. [Roswall]

[55] Angående mordet på tidigare utrikesminister Anna Lindh

9.1.3 Informanter inom advokatbyråer

Ericssons uppfattning är den att när det gäller bevisning i form av loggutdrag, och den teknik som detta omfattar, så är det ett område som juridisk personal undviker eftersom man är rädd för att ge sig in på ett område som man inte behärskar. Resonemangen kring dessa frågor är något som snabbt kan bli för komplicerat. Av samma anledning är det svårt att angripa åklagarens bevisning i och med att man inte alltid förstår den. Man är helt enkelt rädd för att ställa fel frågor och därmed försvåra situationen för sin klient. Resultatet blir att han som advokat i sådana ärenden blir återhållsam. [Ericsson]

Även Durling saknar kunskaper om modern IT-teknik, vilket är signifikativt för stora delar av personalen som i dag arbetar som åklagare, brottsmålsadvokater och domare. Hans uppfattning är den att ett loggutdrag från en användares aktiviteter i ett system är ett mycket svårangripligt bevis. För att kunna ifrågasätta ett loggutdrag krävs det en kunskap som i normala fall inte finns bland de aktörer som förekommer i svenska domstolar. För att kunna angripa ett loggutdrag krävs därför expertkompetens, något som är dyrt för försvaret om denna kunskap åberopas från deras sida. [Durling]

Som advokat har Salomonsson inte ställt frågor innebörden om hur materialet som loggutdragen utgörs av tagits fram. Han har av den anledningen inte satt sig in i hur loggens väg från födsel till presentation sett ut. Om en klient i framtiden skulle börja ifrågasätta ett loggutdrag har Salomonsson själv inte den kunskapen som skulle behövas för att kunna ifrågasätta dessa. Begrepp som hubbade och switchade nät, lösenords transport i klartext i lokala nätverk eller olika formers autenticering är okända begrepp för honom. Denna typ av kunskap saknas i allmänhet inom advokatvärlden. Salomonsson har inte mött någon kollega som har några djupare kunskaper om informationsteknik [Salomonsson].

Ericsson hänvisar till tekniken kring DNA som han tycker kan jämställas med loggutdragen som bevisning. Om man inte förstår tekniken går det inte att föra ett effektivt försvar. Ett annat exempel på en form av loggutdrag är telefonlistor från teleaktörerna. Dessa förekommer i dag i stor utsträckning i förundersökningar och de har ett högt bevisvärde. I flera fall har det hänt att dessa värderas högre än ett ögonvittne. Det har visat sig att det förekommer konstigheter kring dessa loggar. Ett exempel är att en telefon enligt loggarna, som Ericsson varit med och tagit del av, visat sig varit både påslagen och avslagen samtidigt. Trots att leverantörerna erkänner att det sker ”krascher” i deras system så påverkar inte detta tilltron till telefonutdragen. Detta har inte uppmärksammats av rättsväsendet, och Ericsson uppfattar det som om man blunder för detta. Området är helt enkelt för svårt för att kunna ifrågasättas. [Ericsson]

Även Durling drar en parallell till andra former av bevis och jämför med ett fingeravtryck som åberopas som bevisning vilket är lätt att förstå. Det har avsatts av en unik individ och säkrats med en erfaren metod för att sedan identifieras av en specialutbildad tekniker. I slutändan kan utlåtandet kontrolleras i och med att det säkrade fingeravtrycket och jämförelseavtrycket finns kvar. Hela kedjan är känd, dokumenterad och lätt att följa. När det gäller IT-relaterad bevisning är varken kedjan eller tekniken känd, och för att ifrågasätta sådan bevisning krävs kompetens som normalt sett inte finns bland dagens aktörer i en domstol. Till detta kommer att brottet dataintrång är ett bötesbrott vilket innebär att den misstänkte normalt inte ens tilldelas en offentlig försvarare.

Durling jämför även med DNA-bevisningen med loggar eftersom den bakomvarande tekniken även där är okänd. Man kan ifrågasätta var DNA har hittats, men inte tekniken för hur den identifierar en unik individ. [Durling]

Salomonsson utgår från den berättelse och inställning som klienten har när han bygger upp ett försvar i ett ärende som dataintrång. I de fallen har han inte tänkt på att materialet som loggutdragen står för skulle kunna vara manipulerat. Han har alltid utgått från att loggmaterialet som presenterats i förundersökningarna har varit korrekt. Detta under förutsättning att ingenting annat talar emot detta. Det har dock aldrig hänt att t.ex. en polisman, eller någon annan som misstänks för dataintrång, ifrågasatt en logg genom att hävda att den inte skulle vara korrekt eller liknande. [Salomonsson]

Inte heller Ericsson kan komma ihåg något specifikt ärende där någon ifrågasatt ett loggutdrags riktighet. De vanligaste förklaringarna är i stället att trafiken som loggarna omfattar utförts i det egna kontot av någon annan. Han har heller inte varit med om att man ifrågasatt vilka möjligheter administratörerna har i de system som genererat aktuella loggar. [Ericsson]

En förutsättning för att rätten skall hänga med i en huvudförhandling där loggen utgör bevisning är att den kan presenteras av åklagaren på ett enkelt sätt. Denna förmåga skiljer sig avsevärt bland åklagarna. [Ericsson]

I och med att Durling medger att han inte är bekant med IT-relaterad bevisning så innebär det att olika former av autenticeringstekniker inte är känd. Vilka tekniker man kan använda för att låta användaren bevisa sin identitet för målsystemen kan därför varken ifrågasättas eller värderas. I dag krävs det specialkunskaper för att kunna hantera sådana mål. [Durling]

9.1.4 Informanter inom informationssäkerhetsområdet

I detta avsnitt har vi valt att presentera intervjuerna i form av en sammanställning över vad som bör beaktas i ett system vad gäller loggning. Syftet med denna sammanställning är att identifiera problem i samband med logghantering. Därmed så bör läsaren observera att sammanställningen inte gör anspråk på att redovisa kompletta lösningar kring de identifierade problemen. Istället skall sammanställningen ses som vägledning för vad en organisation bör beakta i sin strävan mot en säkrare logghantering. Sammanställningen baserar sig på de intervjuer som genomfördes med IT-säkerhetskonsulterna Olsson, Richardsson samt Söderholm.

Allmänt kan sägas att samtliga konsulter som intervjuats är övertygade om att ett helt säkert system inte går att bygga i och med att en mänsklig faktor alltid kommer att vara inblandad i administrationen av systemet. Därför kan man inte utan vidare lita på en logg. Richardsson har varit med i ett flertal interna utredningar[56] hos företag och organisationer där en administratör kunnat misstänkas för att ha lagt skulden på en oskyldig användare eller i övrigt gjort otillåtna åtgärder.

I och med att denna typ av incident har inträffat så går det inte att utesluta att det händer igen. En fysisk person kommer alltid att ha tillträde till en eller flera servrar som systemet körs på och detta innebär att det alltid kommer att finnas risk för att loggdata manipuleras genom olika otillåtna åtgärder. Vidare har Richardsson ofta ställt sig frågan varför administratör i många fall ses som en helt oantastlig människa. Ofta ges administratörer behörighet att kunna göra ”allt” på en server utan att det ifrågasätts eller att andra kontrollåtgärder byggs in för att övervaka administratörerna.

För att exemplifiera problematiken med att det inte går att lita på en logg så skall vi åter ge ett exempel som Richardsson målade upp under intervjun. Exemplet går ut på att en installerad trojan på en klient skulle kunna möjliggöra för en intern/extern angripare att få access till systemet genom den nedsmittade klienten. Följaktligen används en oskyldigs persons användare och all verksamhet som angriparen utför kommer genom loggen att knytas till denne. Angriparens access skulle även kunna ske samtidigt som användaren sitter och gör sina normala arbetsuppgifter. Vittnen kommer således förmodligen att finnas som pekar ut att personen i fråga verkligen satt vid sin klient och arbetade vid den tidpunkt som loggen pekar ut för de åtgärder som angriparen vidtagit.

Exemplet visar att så mycket mer än vad loggen säger måste belysas för att en utredning skall kunna bli trovärdig. Nätverk, servrar samt klienter måste miniutöst undersökas. Trojanen i exemplet ovan skulle i och för sig kunna upptäckas vid en undersökning men det finns trojaner som avinstallerar sig själv och har det gått lång tid från detta så är det inte säkert att spåren av den finns kvar.

[56] Dessa företag/organisationer har valt att sköta utredningen internt i och med att de inte velat ha dålig publicitet. Därför har bevisföringen (loggarna) i dessa fall ej prövats i någon rättsinstans utan endast lätt till interna åtgärder.

Således krävs det att alla komponenter i hela händelsekedjan är säkrade för att en logg skall kunna betraktas som pålitlig och trovärdig. Åtgärder måste därför vidtagas på en rad olika områden. Klienterna måste säkras så de inte bär på någon okänd programvara, nätverket skall inte kunna ”sniffas” utan att det upptäcks, loggarnas integritet måste kunna garanteras i samband med transport i systemet osv. Nedan följer en sammanställning av de kritiska problemområden som förmedlats under intervjuerna med de tre konsulter som ingått i informantgruppen. Samanställningen beskriver deras gemensamma tekniska samt administrativa råd för att skapa ett säkrare samt mer genomtänkt loggsystem där eventuella risker minimeras.

- **Lagring av loggfiler på separat system**

Normalt lagras loggfilerna på samma server som systemet som genererar loggarna körs på. Är så fallet går det inte att garantera integriteten hos loggarna eftersom administratören då förmodligen har access till samtliga filer på aktuell server. Även om loggfilerna på något sätt ligger skyddade i servern (t.ex. för administratören okänt lösenord) finns risken att administratören eller en tredje part installerar programvara[57] med avsikt att få kontroll över dessa filer. Om loggfilerna däremot ligger separerade från huvudsystemet på en egen extern server så försvåras ovannämnda exempel avsevärt.

Ännu bättre vore ett system där säkerheten är utlagd på flera servrar. En server används vid autenticering, en annan vid åtkomst och en tredje för loggning. Det kan också bli aktuellt med att en sekundär loggserver loggar aktiviteten i den primära loggservern. På så sätt blir det svårare för en insider eller extern angripare att dölja ett intrång i och med att komplexiteten i systemet höjs. Med ovanstående resonemang så ser läsaren att det därför är omöjlig att garantera en loggs äkthet så länge systemen inte är separerade (se mer under avsnitt separation av administratörsroller mellan system).

- **Skydd mot att lagrad loggdata är åtkomligt via nätverket**

Det räcker inte att endast lagra loggdata i en extern server. Loggarna bör även skyddas mot att data är åtkomlig via nätverket. Åtkomlighet av loggarna via nätverket kan ske om loggservern har vissa åtkomlig tjänster öppna[58]. Att förhindra denna kontakt kan ske genom en traditionell brandväggslösning eller genom att enkelrikta nätverkstrafiken så att det endast går att skicka meddelanden till loggservern och inte tvärtom. Man behöver även en lösning där loggarna skrivs till ett icke förändligt lagringsmedium för att skydda loggarnas integritet när de väl är lagrade. Värt att påpeka är dock att detta inte ger något skydd mot att felaktiga värden skrivs ned i samband med att loggarna anländer till den externa loggservern eftersom de kan ha blivit manipulerade på vägen eller när de skapades.

- **Fysiskt skydd av servrar**

Samtliga konsulter anser att en person i stort sett kan göra vad som helst med loggfilerna om han/hon får fysisk tillgång till maskinen de ligger på. Detta gör skydd mot fysiskt åtkomst till en av de viktigaste punkterna i denna sammanställning. Vid fysiskt tillträde kan en person ta en ”image” (spegelbild) av hårddisken för att sedan sitta i hemmet och analysera den för att sedan återkomma och utnyttja de svagheter som hittats. T.ex. kan ny programvara installeras vilket kan medföra att personen uppnår administratörsrättigheter och därigenom kan manipulera loggarna.

[57] Vi syftar här på så kallade “rootkit:s” som möjliggör förändring eller förstöring av loggdata.
[58] Sådana tjänster kan vara öppna både avsiktligt eller oavsiktligt genom oaktsamhet.

En lösning på detta är att reglera den fysiska åtkomsten till vissa maskiner genom att ha dem inlåsta och därigenom reglera tillträdet. En server som innehåller samtliga loggfiler skulle t.ex. kunna vara placerad i en videoövervakad bur vilken administratören eller analysgruppen måste gå in i vid underhåll eller analys.

- **Fysiskt skydd av nätverket**

Det skall inte utan vidare gå att koppla in utrustning i nätverket i ett försök att t.ex. ”sniffa” nätverkstrafiken. Därför måste åtgärder tas för att säkra sådana punkter där inkoppling skulle kunna ske. Vad gäller nätverksuttag vid arbetsplatser så måste dessa på något sätt spärras mot att okänd utrustning ansluts genom t.ex. att endast godkänna vissa typer av MAC-adresser. Detta är dock svårare än man kan tro i och med att MAC-adressen genom relativt enkla åtgärder kan manipuleras. En ”sniffer” skulle även kunna kopplas in emellan olika användare eller vid strategiska punkter i nätverket där mycket trafik passerar. I ett sådant fall skulle en tänkbar lösning kunna vara att använda sig av ljusdetektering, d.v.s. detektorer som larmar om någon öppnar förseglade skåp eller borrar i kablar m.m.

- **Krypterad nätverkstrafik**

Någon form av krypteringsteknik bör användas på all trafik som går i nätverket. Primärt är detta för att förhindra någon från att ta del av hemlig information men krypteringen kan även användas för att säkerställa autenticering mellan olika delar av systemet.

- **Rätt konfiguration**

Det är av yttersta vikt att servrar, brandväggar m.m. konfigureras på rätt sätt eftersom fel konfiguration kan innebära oerhörda säkerhetsluckor. Av den anledningen är det viktigt att inte driftsätta dessa i det ordinarie nätet innan dess konfiguration noggrant testats i ett separat nät som ligger helt skilt från det ordinarie nätet. Vid tester av konfigureringen skall tjänster som inte används stängas av eller avinstalleras. Checksummor räknas sedan ut på alla filer i den rätt konfigurerade versionen för att kunna upptäcka om konfigurationen ändras (Se avsnitt 8.18.2).

- **Skydd av loggar under transport i nätverket**

Vare sig de genererade loggarna först lagras lokalt eller om de direkt överförs till ett externt lagringsmedium så är loggarna i samband med denna transport i ett utsatt läge. I fallet med den lokala lagringen måste loggarna, i ett mer omfattande loggningssystem, förr eller senare lokalt skrivas över och loggarna måste därmed flyttas över till en sekundär lagringsplats. Ett grundläggande krav i samband med denna transport är att loggarnas integritet måste garanteras, dvs. ett skydd måste finnas mot att loggdata kan läggas till, tas bort eller förändras. Viktigt är att ställa sig frågan hur man skall garantera att samtliga loggar förts över och att inte vissa av dem försvunnit under denna hantering[59].

När loggarna förs över till ett separat lagringsmedia kan detta ske antingen i realtid eller vid vissa fastställda tillfällen. Dessa tillfällen skulle kunna vara vissa bestämda tidpunkter eller när en viss mängd data har lagrats. Vid överföringen måste någon form av mekanism finnas hos det externa lagringssystemet som skickar en kvittens på att loggen är mottagen och att den är oförändrad. Först därefter kan huvudsystemet radera sina loggdata.

[59] Viktigt är att påpeka att detta inte bara gäller vid påverkan av en tredje part utan även som skydd mot brister i programvaran

Viktigt är även att någon form av ömsesidig autenticering sker mellan huvudsystemet och lagringssystemet eftersom huvudsystemet måste vara säker på att det skickar loggdata till ett lagringssystem som har rätt att ta emot loggdata men även att lagringssystemet är säker på att det är huvudsystemet som skickar loggarna. Allt detta för att hindra att falska loggposter läggs in i säkerhetsloggarna. Denna mekanism är kritisk och det gäller att noga kontrollera säkerheten kring denna mekanism när det gäller vilka som har rättigheter att stänga av systemet eller i övrigt hantera det.

En lösning när det gäller loggarnas integritet är att signera dessa. Om överföringen sker i realtid måste varje loggpost signeras i motsats till om överföringen sker blockvis vilket innebär att endast blocket signeras.

- **Checksummor på alla vitala systemfiler**

För att säkerställa att inga vitala systemfiler blivit utbytta eller förändrade på grund av att t.ex. ett ”rootkit” installerats så bör kryptografiska checksummor beräknas på samtliga filer. Checksummorna skall beräknas när filerna installeras och ett ändrat värde på en checksumma kommer således att tyda på att en förändring av filens sammansättning har skett. De autentiska checksummorna skall självklart förvaras i ett säkerhetsskåp. Med jämna mellanrum bör sedan filerna på servern kontrolleras mot originalvärdena. Dock måste man komma ihåg att denna uppgift sköts av en fysisk person vilket innebär att denne inte ensam bör göra denna typ av arbete (se avsnittet längre ner angående tvåhandsfattning).

- **Stark autenticering**

Grundsynen på en logg måste vara att den visar vad som har skett och vem som har gjort det. En logg tillskänks högre trovärdighet vad gäller vem som utfört en åtgärd ju starkare autenticering som har använts. Många av de vanligaste autenticeringsmetoder som används idag är egentligen relativt enkla att ta sig förbi. Lösenord kan enkelt ”snappas upp” genom att se över axeln på en person som loggar in på sin användare, kvarglömda smarta kort kan lånas i smyg o.s.v. Är autenticeringsmetoden för svag kommer man att kunna angripa trovärdigheten oss en logg oavsett hur starkt skydd som byggts upp kring systemet i form av fysiskt skydd av servrar, administrativa säkerhetslösningar m.m. I ett sådant fall spelar det ingen roll att det som loggats är helt korrekt.

Således är autenticeringsprocessen inom ett system en mycket viktig del när det gäller en loggs bevisvärde. Skall en logg kunna tillmätas någon form av betydelse så måste man kunna lita på systemets autenticering. Men det bör samtidigt tilläggas att om det finns luckor i säkerheten, vad gäller systemet i övrigt, så spelar det heller inte här någon roll hur stark autenticeringen är. Om användaren loggat in med lösenord eller genom en avläsning av näthinnan kommer vara helt ointressant. Talesättet ”*en kedja är inte starkare än den svagaste länken*” illustrerar situationen väl. Problemet måste således ses ur ett helhetsperspektiv.

Samtidigt måste naturligtvis autenticeringen stå i förhållande till vad som systemet skall skydda. Därför kan det bli aktuellt att ha olika typer av autenticering beroende vilka system som anropas eller vilka användare det är som anropar systemet. Bland annat skulle man kunna tänka sig att en administratörsanvändare kräver en kraftfullare typ av autenticering än en normal användare inom ett system på grund av den omfattande behörighet administratörerna kan ha. I sådana fall skulle det kunna vara aktuellt med videoövervakning eller dylikt för att kunna bestyrka att det verkligen var en specifik individ som låg bakom en inloggning och inte endast personens lösenord samt smarta kort.

Videoövervakning kan med rätta tyckas vara en extrem åtgärd och förmodligen skulle teknik som t.ex. biometri eller liknande kunna fylla ut gapet mellan smart kort och denna typ av lösning. Dock erbjuder videoövervakning fördelen med ett konkret bevis för att någon varit på plats och kan därför vara en nödvändighet i vissa miljöer med extremt känslig information osv.

- **Loggarnas lagringsformat**

Ett stort problem i många organisationer idag är att de olika typerna av loggar är av olika format. Detta försvårar analysen vid samkörning avsevärt. Förklaring till det hela torde ligga i att nya typer av loggar tillkommit över tid. En annan anledning kan helt enkelt vara att systemet inte är särskilt genomtänkt och följaktligen finns ingen grundläggande strategi över vad man vill uppnå med loggarna. En annan sak som är viktig att tänka på är att val av format måste ställas i relation till hur länge loggarna skall arkiveras. Hos t.ex. vissa av försvarsmaktens organisationer finns krav på att loggarna skall gå att läsa om 25 år vilket innebär att teknik för att läsa aktuellt format då måste finnas.

- **Gemensam systemklocka**

När logganalys sker av loggposter genererade av flera underliggande system kan det ibland vara så att samma person har olika användarnamn i olika system. Vid en analys kommer denna underlättas avsevärt om en gemensam systemklocka används vid tidsangivelser i loggposterna. Om så ej är fallet kommer det bli mycket svårt, eller till och med omöjligt, att redovisa en persons rörelser i de olika systemen. Om en gemensam systemklocka används måste även åtgärder vidtagas för att transport av tidsangivelser på ett säkert sätt distribueras till de olika underliggande systemen.

- **Separation av administratörsroller**

Administratörsrollerna mellan olika delsystem bör delas upp så att ingen person tillåts vara administratör på hela systemet. Rent praktiskt kan detta innebära att en person administrerar loggarna, en annan administrerar behörigheter och en tredje driften. För att dra ned på antalet administratörer kan naturligtvis en person ha flera olika typer av administratörsroller men de får inte tillhöra samma system. Således kan en person administrera säkerhetsloggarna på system A och samtidigt dela ut behörigheter på system B men det viktiga är att t.ex. administratören för säkerhetsloggarna inte har någon användare för systemet vars loggar hann/hon analyserar.

Vidare bör ”vattentäta skott” mellan dessa personer eftersträvas och det ultimata är därför om dessa personer inte tjänstgör på samma avdelning eller liknade. Syftet med denna separering av administratörsroller är naturligtvis att försvåra ett internt intrång av en eller flera administratörer[60] där dessa försöker dölja detta genom att manipulera säkerhetsloggarna.

Det finns idag vissa operativsystem där grundtanken just är att ingen skall ha tillgång till allt. Exempel på sådana operativsystem är Trusted Solaris (Solaris), AEX (IBM) och SE Linux (Linux). Fokus vad gäller dessa operativsystem ligger här på administratörsrollerna.

- **”Tvåhandsfattning”**

I vissa kritiska system räcker det inte att separera administratörsrollerna eller ha en stark autenticeringsprocess utan det kan bli nödvändigt att införa en så kallad ”tvåhandsfattning”.

[60] Observera att syftet med detta intrång inte behöver vara av egen personlig vinning utan man måste även ta med möjligheten till att den egna personalen utsätts för utpressning etc.

Detta innebär att det krävs två eller fler administratörer/användare för att utföra vissa typer av arbeten. Naturligtvis skall autenticeringsprocessen vara utformad på så sätt att ingen av de inblandade administratörerna/användarna på egen hand kan utföra de typer av arbeten som ”tvåhandsfattning” har införts för. Det kan fungera så enkelt att de inblandade parterna har en egen del av ett gemensamt lösenord men det kan även vara så att det krävs ett smart kort, fingeravtrycksmätning eller liknade från var och en. ”Tvåhandsfattningen” behöver inte bara gälla vid inloggning utan bör även gälla vid fysiskt tillträde till viktig maskinvara i samband med uppgraderingar reparationer o.s.v. Detta för att förhindra att icke tillåten programvara/utrustning installeras eller på annat sätt utnyttjas.

- **Inpasserings system**

Ett inpasseringssystem bör finnas i den byggnad som systemet fungerar i. Allra helst bör ett sådant system inte bara logga tillträde till byggnaden utan även rörelser mellan olika avdelningar. Därigenom går det att begränsa personalens fysiska tillgång av känslig utrustning till att endast omfatta de maskiner som ligger inom deras ansvarsområde. Inpasseringen kan även användas för att utesluta en person från eventuella misstankar genom att inpasseringen visar att personen inte ens var i byggnaden vid det aktuella tillfället. Tänkbart skulle även kunna vara att koppla ihop inpasseringssystemet med känsliga datasystem i och med att en person som inte gått in i en byggnad/avdelning inte heller kan logga in i systemet. Vidare så har vi tidigare diskuterat riskerna med fysisk tillgång till viktig maskinvara i och med möjligheten att installera programvara eller olika typer av utrustning. Ett inpasseringssystems uppgifter i det här fallet skulle kunna vara att just begränsa tillträdet till servrar så att endast vissa administratörer kommer åt vissa servrar.

- **Manuell driftlogg**

En manuell driftlogg bör föras där administratören skriver vad som har gjorts samt syftet med åtgärden. På så sätt kan loggarna kompletteras med en ordinarie skriftlig signatur samt att innehållet i den manuella driftloggen kan kontrolleras mot vad systemet säger har genomförts.

- **Loggning av rätt saker**

Det är viktigt att klara ut vilken information som skall loggas i ett system. Det kan tänkas vara frestande att logga så mycket som möjligt men man bör tänka på att loggposterna måste gå att analysera på ett effektivt sätt. Om för mycket data loggas riskerar man att de som sköter analysen ”drunknar” i information till följd att viktig logginformation förblir oupptäckt.

- **Övervakning av avvikelser**

En speciell analysgrupp[61] bör finnas som regelbundet analyserar insamlat loggmaterial i syfte att upptäcka anomalier i den normala trafiken eller i övrigt misstänkta händelser för att utifrån dessa vidtagna åtgärder. Svårigheten med detta är att många av dem som gjort otillåtna åtgärder i systemet många gånger har behörigheten till att utföra åtgärderna men för det aktuella tillfället saknar befogenhet. Ett exempel för att illustrera detta skulle kunna vara en polisman som gör en ”slagning” i polisens spaningsregister av ren nyfikenhet. Polismannen gör normalt flera ”slagningar” i systemet per dag i sin normala yrkesutövning men dessa är då alltid relaterade till hans/hennes arbetsuppgifter. Han/hon har således behörighet att göra dessa ”slagningar” eftersom han/hon tilldelats en behörighet samt befogenhet till densamma så länge det är att betrakta som en tjänsteåtgärd.

[61] Kan utefter tillgängliga resurser bestå av en eller flera personer

Vad gäller den icke tjänstrelaterade ”slagningen” så finns således behörighet men inte befogenhet och det är detta som i många fall försvårar upptäckt i samband med analys. Svårigheten ligger därför i att spåra upp en åtgärd som personen normalt får utföra och därför döljer sig i den normala systemtrafiken. Således gäller det vid analysarbetet att försöka upptäcka eventuella avvikelser från den normala trafiken på nätverket. Genom att använda sig av så kallade ”data mining” verktyg så letar användaren efter statistiska avvikelser vad gäller användarnas beteende. Det gäller således att försöka kartlägga verksamheten för att se vad som är normalt användande för att sedan försöka hitta mönster vad gäller användandet av det som utgörs av icke sanktionerade sökningar.

För att illustrera detta med ett enkelt exempel så skulle man kunna tänka sig att ett journalsystem inom sjukvården skall slå larm till analysgruppen ifall en anställd söker på namn istället för personnummer. I vanliga fall har vårdpersonalen alltid tillgång till personnummer genom de tillfälliga journaler som sätts upp vid ankomsten till ett sjukhus. Därför skulle en namnförfrågan kunna vara en indikation på att någon söker i journalsystemet efter sin granne eller liknande.

Andra typer av problem när det gäller analysdelen är vem som skall utföra denna analys samt hur kontrollen av denna person skall gå till. Således krävs det att analysgruppen består av mer än en person vilket gör att ovan nämnda ”tvåhandsfattning” kan användas. Problem uppstår även i system med mycket högt sekretessvärde eftersom det material som analysgruppen går igenom kan innehålla känslig information. Således måste det klaras ut vilken typ av information analysgruppen får ta del av. Exempelvis skulle man kunna tänka sig en situation där analysgruppen får ta del av vilka användare som har skickat e-post samt till vilka detta skett. De får däremot inte gå in och avläsa innehållet i e-posten.

- **Säkra integriteten hos loggutdrag**

Vid all logganalys måste materialet på något sätt behandlas manuellt. För att garantera att utdragen inte förändras, vare sig avsiktligt eller oavsiktligt vid denna behandling, så krävs att en hashsumma på något sätt beräknas på de aktuella filerna. Detta för att garantera att filerna inte har förändrats under hanteringen.

Slutligen ser inte konsulterna loggarna som ett bevis utan mer som en indikation på att något har hänt. Indikationen måste sedan kompletteras med andra typer av bevisföring för att stärka vad loggarna säger. Sådana typer av bevis kan t.ex. vara videoövervakning, vittnesmål eller spår i utpekad klient (hårddisk). Går det inte att finna kompletterande bevis kommer det förmodligen inte att gå att peka ut en enskild person eftersom loggarna endast pekar mot en användare och/eller en klient, således gå det inte att binda en fysisk person till en händelse.

Det är också viktigt att påkalla uppmärksamhet mot problemet av eventuella i fel i källkoden för vissa systemen, så kallade ”buggar”. Frågan är om det går att garantera att ett system är helt fritt från ”buggar”? Troligtvis är detta inte möjligt, men skulle så vara fallet måste det ställas mot de resurser som finns eftersom ett sådant arbete troligtvis blir mycket kostsamt. Värt att nämnas kan vara den juridiska tvist utanför Sverige som Richardsson [Richardsson] tog upp i sin intervju. I det aktuella fallet så hävdade en bank att deras system var helt säkert varpå den andra parten som var en av bankens kunder begärde att få ta del av den säkerhetsgranskning som måste ha gjorts för att ha täckning för detta påstående. Banken vägrade dock att lämna ut något sådant med följd att de förlorade målet till fördel för kunden.

9.2 Genomgång av utvalda rättsfall

9.2.1 Inledning

En viktig del av vårt arbete är att försöka utröna vilken vikt som domstolar/åklagare lägger vid de loggutdrag som presenteras under en rättegång eller förundersökning. Med andra ord är vi ute efter bevisvärdet av en logg. För att kunna ta reda på detta har vi granskat utvalda brottsmål angående dataintrång för att därigenom försöka skaffa oss en överblick kring problemet. Eftersom vi i avsnitt 1.6 exkluderade klientloggar har vi sökt fall som rört olika typer av statliga organisationer och således inte fall där privatpersoner begått dataintrång i från hemmet. Bland de granskade fallen kommer huvuddelen ifrån interna dataintrång inom polisen där anställda slagit i känsliga register utan tillåtelse.

Målsättningen har här varit att granska det stora flertalet av de förundersökningar som gjorts angående interna dataintrång inom polisen i Stockholms och Gotlands län mellan 1994 – 2003[62]. Dessa domar och aktuella förundersökningsprotokoll har rört polismän samt civilanställda inom Stockholms samt Gotlands län och har inhämtats genom enheten för interna utredningar[63]. De polismän samt civilanställda som arbetar inom detta upptagningsområde motsvarar cirka 30 procent av hela landets personal [Web 19]. Från dessa förundersökningsprotokoll har vi valt att närmare studera de ärenden som till strafföreläggande eller åtal och studerat dessa närmre. De förundersökningar som inte har gått vidare enligt ovan är således fall där brott inte kunnat styrkas och därför aldrig gått vidare till en juridisk prövning.

Som ett komplement till dessa rättsfall har vi analyserat ett fåtal fall inom sjukvård, försäkringskassan, socialtjänsten samt kommun. Dessa fall har tagits fram på rekommendation från personer vi intervjuat eller i övrigt kommit i kontakt med under arbetets gång. Dessa rättsfall har bedömts som särskilt intressanta ur vårt perspektiv. Dock måste analysen av dessa fall läsas med en viss försiktighet eftersom de endast utgör ett fall bland flera och att långtgående slutsatser därför är svåra att göra.

Analysen av samtliga fall syftar till att försöka klargöra vilket värde rätten lägger på ett loggutdrag samt vilket resonemang de för när de resonerar kring personens skuld i samband med dessa interna intrång.

[62] Aktuella förundersökningsprotokoll (FU-protokoll) samt domar har inhämtats via enheten för interna utredningar (CU) i Stockholm samt Stockholms tingsrätt/hovrätt. I och med att det inte går att göra sökningar på brottstyp hos tingsrätten/hovrätten har vi först varit tvungna att ”spåra” upp aktuella FU-protokoll i CU:s arkiv för att sedan använda oss av dessa för att ta fram rätt dom. CU har dock uppgivet att vissa FU-protokoll kan ha saknats i arkivet vilket kan ha gjort att vår genomgång av interna dataintrång mellan 1994 – 2003 ej blivit komplett. Vår bedömning är dock att vi behandlat det stora flertalet av aktuella domar och att slutsatser dragna ur materialet trots detta är representativa för samtliga interna dataintrång inom Stockholms och Gotlands län.

[63] Enheten för interna utredningar i Stockholm har både Stockholm och Gotlands län som upptagningsområde vilket medfört att vi på ett smidigt sätt kunnat ta det av fler domar.

9.2.2 Interna dataintrång inom polisen

Poliser samt övriga civilanställda inom polisväsendet är klart överrepresenterade i brottsstatistiken vad gällande interna dataintrång [Engstedt]. Dock handlar det enligt Stefan Kronqvist [Kronqvist, 2003] inte om att dessa är mer ”brottsbenägna” utan förklaringen står istället att finna i den organisation som är uppbyggd inom polisen för analys av loggdata. Polisen har i förhållande till flera andra organisationer en mycket rigorös användarkontroll vilket gör att överträdelser av bestämmelserna ofta upptäcks. Tilläggas bör även att polisen har en mycket ”tuff” anmälningspolicy där alla felsteg anmäls [Engfeldt]. De register som polisanställda har tillgång till har även förmodligen rent generellt ett större informationsvärde än register inom de flesta andra organisationer. Mörkertalet inom organisationer med begränsad eller obefintlig loggning kan med ovanstående resonemang förväntas vara stort.

Efter genomgång av alla aktuella förundersökningsprotokoll som vi hittat har vi beställt hem domar från aktuella tingsrätter/hovrätter för de fall som lett till åtal. Dessa har systematiskt gåtts igenom och förts in i en tabell (Bilaga E) efter visa parametrar som vi satt upp. Parametrarna är som följer:

Diarienummer
Diarienumret anges så att läsare på egen hand skall kunna beställa hem domar som han/hon vill studera närmare. I de flesta fall anges K-numret (polisens ärendenummer i K-registret) som hänvisning där detta inte gått att finna har AI-numret eller B-numret istället angetts (ärendenummer hos enheten för interna utredningar i Stockholm). Med hjälp av diarienumret kan läsaren i bilaga F även se vid vilken tingsrätt/hovrätt domen förkunnats vid.

Påföljd – *Fälld, Friad, Föreläggande*
Påföljden visar vad som förkunnandes vid domen. Den misstänkte kan fällas, frias eller få ett strafföreläggande. Strafföreläggande innebär att den misstänkte redan under förundersökningen erkänt och därför går inte åtalet vidare till domstol. I stället utdöms ett bötesbelopp av åklagaren. Strafföreläggande kan ske vid misstanke om brott som endast medför böter på straffskalan.

Inställning till delgiven brottsmisstanke –*Erkänner, Förnekar, Erkänner omständigheter*
Inställning till delgiven brottsmisstanke handlar om hur den misstänkte ställer sig till den brottsmisstanke som delgivits honom/henne. Således kan personen erkänna, förneka eller erkänna faktiska omständigheter vilket innebär att personen erkänner att han/hon gjort detta men att uppsåtet inte var brottsligt.

Inställning till logg – *Bestrider, Medger*
Inställningen till loggen visar huruvida den misstänkte anser att loggutdraget som presenteras är riktigt eller ej. En person som medger anser följaktligen att loggen visar vad som hänt medan en person som bestrider anser att loggen inte stämmer av en eller annan anledning.

Vid genomgången av materialet letade vi primärt efter fall där någon rättslig instans tagit ställning till bevisvärdet av en logg. Således har vi sökt efter fall där den misstänkte på något sätt bestridit det presenterade loggutdraget.

Tre av de genomgångna fallen svarar mot detta kriterium och nedan följer en genomgång av dessa tre fall. Läsaren måste dock ha klart för sig att de citat som presenteras endast är utdrag ur förhör och inte på något vis representerar en helhet. Vi har dock genom att ta med dem försökt ge beskrivningen av fallen mer substans än vad endast en sammanställning i vanlig text skulle ha gett.

- **Sollentuna Tingsrätt K 239806-96 (C*itat nedan är endast utdrag ur förhör*)**

En polisman fälls för dataintrång för ”slagningar” som hon gjort på personer i hennes bekantskapskrets. Eftersom den misstänkte arbetar i en sambandscentral har det ingått i hennes arbetsuppgifter att genomföra slagningar på uppdrag av poliser på ”fältet”. I förhören hävdar hon att alla de ”slagningar” som hon är misstänkt för just har skett genom att förfrågningar kommit utifrån via radio. Eftersom hon genomför ett stort antal kontroller per arbetspass så hävdar hon att det helt enkelt är omöjligt för henne att komma ihåg alla ärenden när hon av utredarna ombeds förklara ”slagningarna”. I förhören förklarar hon sig enligt följande på frågan om kontrollerna varit en tjänsteåtgärd:

> **Polismannen:** ”*Jag vet inte. Jag…jag…liksom du får ursäkta, jag kan inte svara. Det är över ett år sedan. Jag kan inte svara på exakt vad det är*”
>
> **Polismannen:** ”*Jag gör…om jag jobbar dag, , natt, kväll går våra pass, då gör jag 100 – 150 slagningar. Nu begär du att jag ska komma ihåg sen ett år tillbaka när jag gör på mina tre pass 100 – 150 slagningar när jag sitter i radion*”

Sollentuna tingsrätt valde här att inte tro på kvinnas förklaringar eftersom de ansåg att hon rimligtvis borde komma ihåg om hon blivit uppmanad att ”slå” på personer i hennes omgivningskrets. Dessutom ansågs det märkligt att det endast skulle ha dykt upp ärenden på hennes anhöriga just under hennes arbetspass i sambandscentralen. Vidare så skulle även patrullerna ha haft tillgång till personnummer (genom ID) om det varit ett ärende i vilket de anropade sambandscentrealen för en kontrollfråga. Så har det inte varit i de aktuella fallen eftersom den kvinnliga polismannens användare istället använt sig av personernas namn för att ta fram uppgifter. Således har autenticeringen i kombination med vem kvinnan slagit på och när detta skett lett fram till en fällande dom med hjälp av loggarna.

- **Svea Hovrätt K 23751-96 (C*itat nedan är endast utdrag ur förhör*)**

En polisman fälls för dataintrång på grund av att en ”slagning” genomförts med mannens behörighetskort. Polismannen själv nekar till att han över huvudtaget gjort någon slagning utan hävdar istället att han vet att en kollega (som även var målet för slagningen) gjort den aktuella slagningen (minns dock inte vid vilken tidpunkt) när hon varit inloggad på mannens användare. Han kan dock inte minnas vid vilken tidpunkt denna slagning skall ha skett. Vidare så är det även kollegan som var den person som slagningen berörde och polismannen hävdar att kollegan skulle ha gjort den aktuella slagningen på sig själv som en sorts demonstration. Kollegan själv säger sig vara helt säker på att hon aldrig gjort denna slagning.

Kollegan förklarar följande vid ett förhör på frågan angående om det var brukligt att man lånade ut sitt privata smarta kort till varandra på avdelningen i samband med inloggning i systemet.

> **Förhörsledaren:** ”*Var det brukligt vid X att man lånade behörighetskort av varandra när man skulle slå på datorn*?”:
>
> **Kollegan:** *”Nej alla har ju ett eget, det brukar då inte vi göra i alla fall utan vi har vårt eget”*

Vidare förklarar hon angående kollegans påstående om att hon skulle ha slagit på sig själv i ett förevisande syfte:

> **Kollegan:** ”*Nej just det, nej, nej det kan jag inte komma ihåg att jag har gjort. Det utesluter jag*”

Den misstänkte förklarar i förhör själv enligt följande på frågan om han kan tänka sig ett strafföreläggande[64]:

> **Polismannen** ”*Ja det är ju så här att jag… jag har ju nu inte gjort det här. Jag har inte gjort den här slagningen. Ja jag… jag är ju bunden på det viset då att det är mitt kort va och det har slagits, det går inte och komma ifrån, men rent fysiskt så har inte jag gjort det här. Jag har inte gjort den här slagningen. Det är ju det som är…*”

I detta fall stod ord mot ord eftersom båda parter kraftigt dementerar att de skulle ha gjort den aktuella slagningen. Svea hovrätt såg det, på grund av loggutdragen, som styrkt att den misstänktes användare gjort slagningen och eftersom ”*sannolikheten för att någon utan X:s vetenskap kunnat använda dennes kort och personliga lösen är så ringa att det enligt tingrättens mening inte kan finnas annan förklaring till vad som hänt än att X själv vidtagit åtgärden*”. Resultatet blev i detta fall att en fällande dom utdelades.

Det intressanta med denna dom är att detta är den enda dom vi funnit i vårt urval där någon fällts mot sitt nekande med loggen som den i huvudsak enda bevisningen[65]. Man kan här fråga sig huruvida utslaget av denna dom betyder att den aktuella autenticeringsmetoden (lösenord i kombination med behörighetskort) ur juridiskt perspektiv är tillräckligt för att binda någon till en händelse? Det skulle nämligen kunna vara slutsatsen eftersom det inte finns någon annan bevisning. Dock är det en annan sak som särskiljer sig här i jämförelse med underliggande dom K-106595-97. Den misstänkte polismannen medgav för förhörsledaren att det inte finns någon praxis av att byta kort emellan kollegerna eller göra ”slagningar” med hjälp av andra användare som redan är inloggade. Polismannen förklarar att ingen annan än han använt kortet förutom de gånger där han varit med och då har, enligt han själv, inga ”slagningar” gjorts på kollegan. Följaktligen verkar hovrätten då gått på linjen att loggen visar vad som hänt och vem som ligger bakom.

[64] Som förklarats tidigare i uppsatsen så kan den misstänkte vid brott som endast medför böter på straffskalan erkänna brott mot att inget åtal sker samt att åklagaren istället sätter ett bötesbelopp.
[65] Den ovanstående domen K-239806-96 var förvisso även den fällande mot ett nekande men skillnaden är här att i detta fall fanns en del i bevisningen i den stora mängden slagningar som gjorts och där huvuddelen på något sätt var anhöriga eller på andra sätt relaterade till kvinnan

- **Stockholms Tingsrätt K 106595-97 (Citat nedan är endast utdrag ur förhör)**

En civilanställd inom polisen frias från anklagelserna om dataintrång trots att loggutskrifter visar att hon gjort ett stort antal ”slagningar” på andra anställda inom polisen. Vid förhör framkommer att det blivit en slags otillåten ”praxis” att logga in på sin dator med sitt behörighetskort för att sedan förbli inloggad trots att personen lämnar sin arbetsplats. Vidare förklarar hon i förhör:

> **Civilanställd:** *”-Ja, det är ju så här att när man loggar in sin kort – eller man stoppar in sitt kort i datan – så sitter det tyvärr ofta i där alltså. Jag har ju liksom så mycket annat också att sköta så jag brukar sätta in mitt kort i datan, springer iväg, gör en massa ärenden, kommer tillbaks och det händer ofta att jag glömmer mitt kort kvar i datan, så man får hämta i en ask, som man kan ha till dagen efter eller (ohörbart ord) efter. Så det är mycket möjligt att andra kan gå in så här”*
>
> **Civilanställd:***”Absolut och det händer väldigt ofta att man lånar varandras kort”*

Förhörsledaren påpekar att datorn skall ”låsa sig” vid inaktivitet efter ett visst tidsintervall men i det aktuella fallet går det att komma åt två av registren utan att behöva göra en inloggning med hjälp av lösenord. Det enda som behövs är ett behörighetskort vilket den misstänkte, enligt ovan, hävdade ofta lämnades kvar på arbetsplatsen.

Vår tolkning är att den civilanställde friades av Stockholm tingsrätt eftersom det blev omöjligt att knyta de olika ”slagningarna” till henne som person. Teoretiskt skulle vem som helst av hennes kollegor kunnat ha gjort slagningarna. Ett sätt att komma tillrätta med detta problem skulle kunna vara att förstärka de lokala reglerna vad gäller ansvar för alla ”slagningar” som genomförts med aktuellt behörighetskort. I nuläget verkar det generellt som att en användare misstänkt för intrång kan gå fri om det kan antas att andra kan ha använt sig av dennes behörighet. Om starka lokala föreskrifter finns vad gäller rutiner kring användandet av smarta kort m.m. s borde det i princip kunna gå att åtala personen vad gäller tjänstefel eller motsvarande.

Dock bör det påpekas att det i detta fall verkar ha räckt med att endast använda sig av behörighetskortet för att komma åt de aktuella registren och inte ett lösenord därtill. Frågan är hur tingsrättens utslag skulle ha förändrats vid ett scenario där lösenord även hade krävts? Vår bedömning är att utslaget förmodligen inte skulle ha ändrats om de misstänkta, precis som ovan, målar upp ett scenario där de anställda frekvent ger varandra sina lösenord (för att t.ex. snabba upp arbetet). Till saken hör även att de aktuella personerna som ”slagningarna” rörde sig om var polismän och inte personer som gick att knyta till den civilanställdes privatliv eller motsvarande. Följaktligen skulle fler än hon kunnat haft motiv till att göra dessa slagningar (jämför med K 239806-96).

9.2.3 Kommentar av genomgångna domar

Vid en analys av tabellen i bilaga F så går det att konstatera att det inte är särskilt vanligt att misstänkta bestrider de loggutdrag som presenteras som bevis. I det aktuella fallet kan det självklart förklaras med att många av de inblandade är polisman samt att alla på något sätt är anställda inom polisväsendet. Det kan därför finnas en högre vilja att samarbeta med utredarna än vad som t.ex. skulle vara fallet vid fall utanför organisationen.

Bland de få som bestridit att loggarna visar vad som hänt så är den vanligaste förklaringen att det förvisso är den misstänktes användare som finns i loggutdragen men att det inte är han/hon som har gjort slagningen. Istället har någon annan gjort slagningen samtidigt som den riktige användaren fortfarande varit inloggad. Inget av de fall där någon förnekat sin skuld har tagit upp möjligheten till att det skulle vara ett tekniskt fel som ligger bakom loggutdraget. Detta styrks även av samtliga intervjuer som genomförts inom rättsväsendet. Förklaringen till detta torde stå att finna i att man inte ifrågasätter tekniken eftersom man inte känner till tekniken. Det kan helt enkelt vara så att dessa personer utgår från att tekniken alltid gör ”rätt” och därmed skyller misstankarna på en annan person.

Sammantaget kan man konstatera att det är svårt att dra några långtgående slutsatser av en analys av dessa tre rättsfall. Det som är intressant är dock att rätten endast verkar ha tagit hänsyn till problematiken med att en okänd person skulle ha använt sig av en användare om den misstänkte tagit upp denna möjlighet under utredningen. I annat fall verkar rätten utgå ifrån att det är den misstänkte som gjort ”slagningarna” precis som loggutdragen visar. Detta problem är även något som bekräftas av kriminalkommissarie Bergnér [Bergnér] som menar på att de flesta fall där andra kan ha gjort de aktuella ”slagningarna” på grund av vissa omständigheter ofta skrivs av eftersom det ej går att styrka att den misstänkte verkligen har gjort de aktuella slagningarna. Det bör emellertid påpekas att de personer som ”slagningarna” gällt oftast har kunnat sammankopplas med den misstänktes bekantskapskrets vilket förhöjt bevisvärdet.

9.3 Övriga interna dataintrång

Nedan presenteras en analys av de fall som vi under arbetet blev uppmärksammade om i samband med de intervjuer som genomfördes. Analysen gör inga anspråk av att på något sätt vara heltäckande vad gäller samtliga domar på området utan utgör endast en mindre del. Dock bör tilläggas att domarna i sig är de som juridisk personal bedömt som värdefulla och intressanta ur vår utgångspunkt. Undantaget är domen angående en anställd vid Perstorps kommun som vi själva hört talas om och sökte information omkring[66]. Eftersom vi i dessa fall endast tagit del av domarna och inte förundersökningsprotokollet så kan vi i dessa fall inte presentera några utdrag ur förhör m.m.

[66] Bland annat genomfördes intervjun med kriminalinspektör Ingemar Leijon med utgångspunkt från detta fall.

- **Hovrätten för Västra Sverige B 1056-01 Sjukvården**

Fallet är framtaget på inrådan av Ragnar Lindblad, IT-chef vid Danderyd Sjukhus, och är enligt honom det enda fallet av internt dataintrång inom sjukvården som fått rättsligt efterspel. I det aktuella fallet fälldes en sjuksköterska vid Sahlgrenska sjukhuset i Göteborg av Göteborgs tingsrätt (B-11913-99) för dataintrång med friades sedermera av hovrätten för Västra Sverige på grund av det oklara regelverk som fanns på Sahlgrenska sjukhus vid den aktuella tidpunkten. Under ett arbetspass tog kvinnan del av dåvarande integrationsministern Leif Blombergs journal för att enligt hennes egen utsago leta efter lämpliga medicinska formuleringar som hon kunde använda sig av i sitt eget journalskrivande. Hovrätten ansåg det som styrkt att kvinnan begått dataintrång men dock av lindrig art. Detta eftersom det genom förhör framkommit att viss utbildning i sjukhusets regi hållits med hjälp av riktiga journaler, något som i sig är olagligt. Det har även förekommit att läkare uppmanat sjuksköterskor att ta del av icke aktuella vårdtagares[67] journaler.

I och med detta ansågs att det inte går att belasta sjuksköterskan eftersom dataintrånget är att betrakta som ringa. Problemet ligger här kring de oklara regler som fanns runt journalhanteringen på sjukhuset och visar på ett bra sätt att det inte endast räcker med en omfattande loggning utan detta måste även kompletteras med ett starkt internt regelverk för vad de anställda har befogenhet att utföra.

- **Västmanlands Tingsrätt B 4759-01 Försäkringskassan**

En man fälls av Västmanlands tingsrätt för att ha utfört cirka 30 sökningar i Försäkringskassans register som inte har varit relaterade till hans arbetsutövning. Mannen själv har förklarat att "slagningarna" dels varit en del av hans arbete men även varit en komplott emot honom från hans arbetskamraters sida med syfte att misstänkliggöra honom. Komplotten skulle dels gått till som så att andra använt hans användare när han tillfälligt lämnat sin dator men även också genom att de skulle ha lagt akter på hans skrivbord som inte ingick i hans arbetsområde. Han har sedan sökt information i Försäkringskassans system angående dessa akter i och med att han inte visste om att det inte var hans akter. Det skulle även vid något tillfälle ringt en polis och bett om att få ut adressuppgifter. Den misstänkte hävdade även att han tagit på sig mer arbete än vad som låg under hans ansvarsområde vilket då även skulle kunna förklara vissa av "slagningarna". Vidare uppgav han att det i samband med förflyttningar på arbetsplatsen kunnat vara så att han ibland svarat på andras telefoner, skrivit ned namn och fråga, för att sedan gå till sin stationära arbetsplats och utförs sökningen.

Vidare konstaterade undersökningen att sökningarna ofta gjorts med namn istället för personnummer. Normalt utgår eventuella sökningar i systemet från någon typ av akt eller papper vilket innehåller aktuell persons personnummer, därav märkligheten att sökningar gjorts på namn istället för som normalt personnumren. Merparten av personerna som varit föremål för sökningarna i systemet har även olika typer av relationer till den misstänkte. Bland annat har tre av personerna varit inblandad i en vräkningsprocess riktad mot den misstänkte. Ett antal bor i närheten av denne. En annan står bakom en anmälan riktad mot den misstänkte o.s.v.

[67] Med icke aktuella vårdtagare avser vi här patienter som sjuksköterskan inte var delaktig kring vården av

I några av de ovanstående fallen har den misstänkte i princip medgivit att han tagit fram uppgifterna för personligt bruk. Det är dessa som den fälland domen stödjer sig på eftersom det går att utesluta att de övriga skulle kunna ha med förfrågningar och arbetsuppgifter att göra. Dock har polisen vid undersökningen inte kunnat hitta något stöd för påståendet att "fientliga" kollegor skulle försökt misskreditera honom. Erkännandet i kombination med loggarna har här lett till en fällande dom och tingsrätten har inte behövt ta ställning till de övriga fallen. Tilläggas kan att autenticeringen i det aktuella fallet har bestått av smart kort samt ett lösenord.

- **Svea Hovrätt B-7095-02 Socialtjänsten**

Denna dom är framtagen på rekommendation av en av kommunförbundets jurister, ointressant vem, och är intressant ur synvinkeln att en socialsekreterare blivit fälld för dataintrång trots att det saknats klara skriftliga anvisningar som tydliggjorde när en tjänsteman har rätt att gå in i klienternas dataakter. Bakgrunden är en socialsekreterare som anklagades för att ha gjort cirka 65 slagningar på sin sambos tidigare fru under en tre års period. Socialsekreteraren medgav att hon gjort cirka 10 slagningar men hävdade att hon inte förstod att hon därigenom skulle ha gjort något olagligt eftersom hon inte lämnade informationen vidare.

Vidare nekade hon till att hon gjort fler än cirka 10 slagningar och hävdade att någon annan måste ha gjort de resterande vilket möjliggjorts genom att hon enligt egen utsago lämnat sitt lösenord på en lapp bredvid datorn varför det varit lätt för någon annan att nyttja hennes användarnamn. I både tingsrätten samt hovrätten finner man det styrkt att det just är socialsekreteraren som gjort de aktuella slagningarna och håller det som osannolikt att någon annan skulle ha gjort dessa. Tingsrätten samt hovrätten anser även att socialsekreteraren borde ha förstått att hennes handling var straffbar i och med hennes yrkesutövning samt hennes utbildning som socionom.

Denna dom är intressant med hänseende till att den sjuksköterskan i Göteborg som dömdes i tingrätten för att ha gjort otillåtna "slagningar" på före detta integrationsminister Leif Blomqvist (se dom B 1056-01) vid dennes hjärnblödning senare friades i hovrätten. Hovrätten ansåg att de skriftliga anvisningarna vid sjukhuset var otydliga och sjuksköterskan kunde därför inte lastas för sina "slagningar". Dessa två domar verkar därför gå helt emot varandra men ger ändå en tydlig fingervisning om vikten att ha tydliga dokument som styr verksamheten.

- **Helsingsborgs tingsrätt B-2697-03 Kommun**

Detta ärende ligger till grund för intervjun med kriminalinspektör Leijon [Leijon]. Ärendet gäller ett försök till grovt bedrägeri vid Perstorps kommun i Skåne som ägde rum maj 2003.

En av de anställda socialsekreterarna misstänktes samt polisanmäldes den 20 maj 2003 för att ha gjort felaktiga utbetalningar av socialstöd. De felaktiga utbetalningarna skulle ha pågått under en tid och motsvarade flera miljoner kronor. Denna polisanmälan var kulmen på en längre tids oklarheter kring socialsekreterarens ärenden.

I och med polisanmälan så avsåg de ansvariga på kommunen att göra en mer omfattande undersökning av samtliga fall som socialsekreteraren handlagt för att eventuellt hitta fall som dittills inte var kända. Denna interna utredning avsågs starta efter den 22 maj.

På morgonen den 23:e konstaterades att ett kraftigt vattenläckage uppkommit under natten i socialtjänstens lokaler. Inte heller gick det att få igång datasystemet som användes i det dagliga arbetet. En extern IT-specialist tillkallades, som på plats misstänkte någon form av sabotage, bland annat på grund av avsiktligt uppkomna vattenskadan. Därför gjordes inte uppstarten av systemet på ordinarie sätt vilket i efterhand visade sig klokt. Väl inne i systemet drog IT-specialisten slutsatsen att någon under natten manipulerat IT-systemet och beordrat utbetalningar den 23:e (alltså samma dag som det upptäcktes) via bankgiro på motsvarande cirka 20 miljoner kronor. Genom ett snabbt ingripande av bankgirot lyckades cirka 17 miljoner kronor stoppas innan utbetalning skedde, men under tiden tillstånd för detta söktes för denna åtgärd hann dock 3 miljoner kronor gå iväg.

Utredningen visade sedan att någon eller några på natten tagit sig in med hjälp av IT-chefens extranyckel som på oklara omständigheter försvunnit från dennes skrivbord ett antal dagar innan. Därefter har någon loggat in med den ovan nämnda socialsekreterarens användarkonto samt även loggat in på socialsekreterarens chefs användarkonto som till viss del hade administratörsrättigheter. Därefter beordrades systemet att utföra utbetalningar nästkommande dag på motsvarande cirka 20 miljoner kronor. Vidare genomfördes även sabotage mot systemet genom att portar för support stängdes samt att samtliga användares rättigheter raderades. Även åtgärder mot systemets backup system vidtogs. Den vattenläcka som även mötte personalen påföljande morgon var förmodligen ett sätt att avleda uppmärksamheten från de betalningar som skulle utföras under morgontimmarna när banktjänsterna öppnade.

I och med att IT-specialisten misstänkte sabotage så genomfördes inte uppstarten av systemet på ordinarie sätt utan istället såg han till att säkra eventuella bevis i systemets loggar. Hade detta inte skett så finns möjligheten att all information gått förlorad och att bedrägeriet lyckats. Den ovan nämna socialsekreteraren fälldes senare bland annat för att har utfört ”kuppen” genom att polisen bland annat fann utdrag över vilka utbetalningarna, som skulle gå till vem, i hans hem. Vidare fann polisen även rester av ett brev där den misstänkte konstaterade att han inte skulle kunna bli fälld eftersom namn och lösenord inte räcker för att kunna knyta en person till ett brott vilket också var den aktuella autenticeringsmetoden vid socialkontoret.

Vid en samlad bedömning av alla bevis[68] fann tingsrätten socialsekreteraren skyldig till bedrägeriförsöket som inträffade under natten den 22 maj. Motivet kan ha varit att i en sista ”kupp” försöka tillförskansa sig en större summa pengar i och med att han redan blivit avslöjad för sina bedrägerier som ägt rum innan den 22 maj 2003.

Anledningen till att författarna tagit upp detta fall är för att påvisa hur lätt det var för en insider att genomföra ett allvarligt bedrägeriförsök på grund av den svaga autenticeringen som användes vid det aktuella systemet. Autenticeringsmetoden bestod i detta aktuella fall av användarnamn, som gick att lista ut eftersom alla användarnamn hade samma utformning på användarnamnet, samt ett lösenord. På något sätt tycks socialsekreteraren ha kommit över dennas användarnamn och lösenord som gav en mycket hög behörighet i systemet, för att sedan använda dessa vid bedrägeriförsöket.

[68] Utredningen var relativt komplex och vi kommer därför inte presentera en redogörelse för all bevisning i och med att den inte är IT-relaterad. Följaktligen faller detta utanför inriktningen för detta arbete.

Bland annat berättar socialsekreterarens chef om att socialsekreteraren ofta rört sig i närheten av hennes arbetsplats när hon loggat in med sin administratörsidentitet[69].

Bedrägeriet kunde här ha undvikits genom åtgärd som att ha infört ett aktivt kort i och med att det då skulle ha krävt något som socialsekreterarens chef haft med sig. Det är även intressant att påpeka att det under intervjun med Datainspektionen [Hellberg & Malmqvist] framkom att det inom socialtjänsten idag endast används en autenticeringsform som bygger på lösenord. Trots detta så konstaterar man från Datainspektionens sida att det hittills fungerat rätt bra på grund av deras vana att arbeta med sekretess men att det finns uppbenbara svårigheter att juridiskt identifiera en enskild individ.

[69] Bland annat har socialsekreteraren vid ett antal tillfällen uppgivit att han glömt sitt lösenord och då anmält detta till sin chef för att få en tillfällig användare. Vid dessa tillfällen har hans chef behövt gå in i systemet som administratör för att åtgärda detta. Socialsekreteraren har då uppehållit sig i närheten när inloggningen gjordes.

10. Analys

I detta kapitel går vi igenom och analyserar den empiri vi presenterat i kapitel 9. Materialet presenteras utefter de huvudfrågor vi kunnat identifiera för att underlätta för läsaren att få en överblick.

10.1 Synen på dagens loggutdrag

Eftersom det i dag inte sker någon kontroll av loggutdragens sanningsinnehåll blir uppsatsens problemområde tämligen lätt att analysera. Samtliga respondenter inom de rättsvårdande instanserna utgår från att loggutdragen är korrekta till sitt sak- och sanningsinnehåll. Med sakinnehåll avser vi i fortsättningen att loggningen verkligen sker till följd av det som systemet utsätts för, oavsett om det är den riktige kontoinnehavaren som utför trafiken eller ej. Trycker användaren på tangent A skall systemet logga bokstaven A o.s.v. Med sanningsinnehåll avses att loggutdraget stämmer överens med verkligheten.

Att utgå från att loggutdragen är korrekta till sit sak- och sanningsinnehåll innebär i författarnas ögon att kraven, även om de inte direkt uttalas, är absoluta. Att Loggutdragen behandlas som om de vore korrekta, innebär att hela ansvaret indirekt läggs på dem som genererar dem. Detta krav ställs med andra ord tyst och utan kontroll. Att säga att författarna identifierat detta krav i form av en upprättad kravspecifikation är fel. I stället kan konstateras att det är en upptäckt av en ren konsekvens över hur man behandlar loggutdraget i rättskedjan. Är det då korrekt av författarna att dra denna slutsats? Vi anser själva att det är den enda rimliga slutsatsen man kan dra. Att inte ifrågasätta loggutdragen när man är i den positionen att man kan göra det kan inte innebära annat än att man utgår från att något ifrågasättande inte behövs.

Av de intervjuer vi hållit med personer anställda inom rättsväsendet framgår det att förståelsen för hur tekniken kring hur en logg genereras, transporteras och hanteras är begränsad [Salomonsson, Durling, Bergnér, Keyzer]. Logganalyserna behandlas dock på samma sätt som annan skriftlig bevisning och den jämförelse som har gjorts är att man ser på loggutdragen med ungefär samma ögon som ett läkarintyg [Bergnér]. Där skriver en känd och identifierbar person ner de dokumenterade skadorna som denne i sin erkända yrkesutövning funnit på sin patient, och med detta intyg kan åklagaren föra en talan i rätten som går ut på att offret haft sådana skador som beskrivs i rättsintyget utan att läkaren behöver inställa sig för att vittna.

Logganalyserna ses som en skriftlig bevisning. Vid åberopandet av skriftlig bevisning gäller detta som bevis så länge som ingen hävdar någonting annat. Skulle den ifrågasättas möts detta med argument, och eventuell annan bevisning, från den andra parten varefter det till slut är domstolen som bedömer hur den åberopade bevisning skall bedömas. På så sätt ses loggutdragen som vilken annan skriftlig bevisning som helst [Ekelund].

Ett exempel på skriftlig bevisning som förekommer i vissa mål är ett intyg som skrivits av en tekniker med speciella kunskaper om identifiering av fingeravtryck. Ett skriftligt intyg som binder en unik individ till ett visst säkrat fingeravtryck följer vissa regler. Utan att närmare gå in på dessa går det i korthet ut på att det måste finnas ett minsta antal identifierbara punkter bland papilarlinjerna (linjerna i huden) i ett säkrat fingeravtryck. Är de under ett visst antal, om det så endast saknas ett, så förklaras fingeravtrycket oidentifierbart.

Finns det minst ett visst fastslaget antal identifierade punkter anses fingeravtrycket som identifierbart till en unik individ. Det finns således inga grader av sannolikhet när det gäller identifierade fingeravtryck i Sverige.

Den skriftliga bevisning som polisen får fram under en förundersökning kan med andra ord se olika ut. Därmed kan bevisningen även vara olika svår att förstå. I ett försök att försöka förklara detta exemplifierar vi olika former av bevisning under begrepp som konkret och abstrakt bevisning. Dessa uttryck är våra egna och har ingen egentlig vedertagen koppling till hur bevisningen i allmänhet diskuteras. Även om ett loggutdrag, med svart text på ett vitt papper, är synnerligen konkret, så döljer det sig en ocean av omständigheter bakom detta papper som inte utan vidare framkommer genom att man bara titta på loggutdraget och dess innehåll.

10.2 Konkret bevisning

Om vi tänker oss en mordutredning, där en man hittats mördad i köket i sin lägenhet, är det en normal rutin att lägenheten undersöks av tekniker. Leker man med tanken att det på köksbordet, invid den döde, hittas ett dricksglas där man säkrar flera fingeravtryck kommer dessa avtryck att undersökas och granskas av en specialutbildad tekniker. Denne har rätt att besluta om de identifierade fingeravtrycken tillhör en viss individ. I detta exempel visar det sig att fingeravtrycken är av sådan kvalitet att de är identifierbara och att person A kan bindas till fingeravtrycken på glaset.

Detta är ett exempel som författarna väljer att kalla för konkret bevisning där händelsekedjan är kända och lätt att följa. Vem som helst kan förstå att fingeravtrycken inte direkt binder person A till mordet. Glaset kan ha kommit dit långt innan mordet. Person A behöver därmed inte ha någonting som helst med mordet att göra. Glaset kan till och med ha placerats på bordet efter mordet. Det blir en sak för utredarna att försöka komma fram till när fingeravtrycken hamnade på glaset.

Om det uppstår en diskussion om bevisvärdet av det säkrade och identifierade fingeravtrycket kommer det att bli en diskussion om detta i rätten. Där kommer försvaret att kunna föra en linje som kanske går tvärt emot vad åklagaren påstår. I detta exempel är innehållet av denna diskussion inte så väsentlig, det intressanta är att den är lätt att följa och att förstå. Alla i rätten kan på ett påtagligt sätt följa med i denna diskussion i och med att alla stegen är konkreta och sedan tidigare kända.

För att ytterligare förtydliga och förklara för domare och nämndemän kan parterna välja att kalla in de tekniker som arbetat med att ta fram bevisningen. Dessa kan förklara sina steg och metoder genom att visa fotografier över hur det såg ut på mordplatsen, var glaset stod någonstans, var på glaset avtrycken säkrats och vilken metod som använts för detta. Samtliga steg är konkreta och väl kända för all personal som skall ta del av denna diskussion. Skulle någonting inte vara klart är det inte svårt att ställa kompletterande frågor eftersom alla stegen är tämligen lätta att förstå.

10.3 Abstrakt bevisning

Motsatsen till konkret bevisning blir i detta exempel något författarna kallar för abstrakt bevisning. Varken konkret eller abstrakt bevisning är någonting som direkt används inom rättsväsendet, men dessa ord passar dock bra för att beskriva ytterligheter i en värld där bevisningen kan uttrycka sig i olika former.

Om vi diskutera en logg som bevisning försvinner de flesta av de konkreta steg som vi kan följa i ovan stycke. Abstraktionsnivån höjs till en nivå som man av allt att döma inte är vana vid i våra domstolar [Salomonsson, Durling].

Ett loggutdrag är i författarnas ögon ett slutresultat av en lång kedja händelser, en kedja som inte utan vidare är känd för dem som inte har kunskap om den teknik som omfattar området. Detta slutresultat, i form av ett papper med text, är i sig någonting konkret och som ses som vilken annan skriftlig bevisning [Ekelund].

Oavsett hur domstolarna behandlar ett loggutdrag så innebär skapandet av en logg att koden för en applikation eller ett operativsystem en gång har skrivits på ett sådant sätt att viss information loggas. För att vara säker på att rätt information loggas måste applikationen eller operativsystemet ha validerats så att detta kan garanteras. Även om valideringsprocessen är exkluderad i denna uppsats så hamnar resonemanget redan här på en nivå som innebär begrepp som kodning i högnivåspråk, kompilerad kod till maskinkod och olika former av tester som skall ligga till grund för att rätt information loggas. Dessa processer ingår inte i denna uppsats eftersom var och en av dem självständigt kommer att kunna generera ansatser till nya forskningsfrågor, och därmed egna uppsatser.

Denna uppsats startar när informationen som samlas i en logg genereras. Dessa loggar kommer att variera i fråga om format då en logg kan vara antingen binär eller textuell.[70] För att informationsinnehållet som loggen omfattar skall kunna användas måste dess data transporteras via nätverk eller buss till ett lagringsmedia bestående av t.ex. disk eller band. Under denna transport kan olika transportprotokoll användas (TCP eller UDP) och beroende på trafikintensitet kan UDP-protokollet vara ett mindre lyckat val eftersom det saknar krav på att skickade paket skall ”ackas”, d.v.s. bekräftas att de mottagits [Söderholm & Olsson].

Binära filer måste kanske konverteras till text för att de skall bli läsbara och förståeliga hos analyssidan eftersom dessa kanske saknar den programvara som kan läsa loggen på plattformen som genererat den. Ytterligare manuell hantering kan ske för att göra loggen mer läsbar för människan, och det som slutligen presenteras på ett papper åberopas som skriftlig bevisning.

Om man börjar bakifrån och endast tittar på själva loggutdraget ser man inte alla de steg som passerats för att kunna presentera loggutdraget i detta format. För att överhuvudtaget kunna ifrågasätta ett loggutdrag krävs det en kunskap som idag endast finns hos vissa specialister inom polisen och åklagarsidan [Keyzer, Durling, Salomonsson]. Samma sak gäller för den som skall försvara loggutdragen och gå god för att dessa inte är korrupta.

[70] En binär fil skiljer sig från en textuell fil eftersom den binära filen behöver en speciell programvara för att kunna läsas. Vanliga textfiler kan läsas i vilken texteditor som helst även om de i sig kan variera i fråga om textformat.

10.4 Kan loggutdragen ifrågasättas?

På grund av den egna kompetensen efterfrågas i allmänhet inte något av de steg som presenterats i stycket ovan av någon av parterna i en domstol idag [Salomonsson, Engfelt, Durling, Roswall]. Att informationen i loggutdragen passerat ett okänt antal steg kan ingen människa se genom att enbart ta del av de utskrivna Excelbladen som presenteras i ett förundersökningsprotokoll.

Det lättaste sättet att ifrågasätta loggutdragen och logganalysen är naturligtvis hur den manuella bearbetningen går till [Keyzer, Leijon, Bergnér, Ekelund]. Ett sätt att hantera loggutdragen manuellt är att plocka ut endast den information som är relevant för utredningen och därefter presentera loggposterna rad för rad i ett Excel ark. Ett annat sätt är att skriva av de loggar man fått på papper och bearbeta dem i sin dator. Då är risken för att man skriver av fel värden stor [Leijon]. Om någonting skulle gå fel i denna del kan någon av parterna alltid begära att få ta del av de originalloggar som den manuella hanteringen utgått ifrån. Därför måste dessa alltid sparas.

Det viktigaste en organisation som levererar ett loggutdrag har att garantera, när det gäller loggposter, är loggarnas integritet. Det skall ställas mot det faktum att var och en som har fysiskt åtkomst till en dator på olika sätt, i teorin och i verklighet, kan manipulera det mesta som körs på aktuell maskin [Söderholm & Olsson, Richardsson]. Detta faktum utgör en stor utmaning för en organisation som vill ta fram så säkra loggar som möjligt. Behovet av den mänskliga handpåläggningen i en distribuerad datorarkitektur innebär en rad sårbarhets-områden vilka med rätta skulle kunna diskuteras.

Frågor som med fördel kan diskuteras när man analyserar sanningsinnehållet i ett loggutdrag är hur många tekniker det är som haft tillgång till de plattformar och applikationer som skapat och lagrat aktuella loggar i ett loggutdrag. Man skulle vidare kunna diskuterat backup hanteringen som ligger till grund för en säker förvaring av genererade loggar. Man skulle kunna ifrågasätta vilket integritetsskydd man givit loggarna under deras lagring och transport i nätet, och vilket hot och vilka risker det finns om sådana integritetsskydd saknas. Man skulle kunna diskuterat möjligheten att koppla in främmande utrustning i nätet för att på så sätt sniffa till sig användarnas lösenord, och man skulle framför allt kunna diskuterat vilken autenticeringsmetod som ligger bakom autenticeringen till den känsliga information som loggkontrollen kontrollerade, och som pekar ut en unik kontoinnehavare som ansvarig för den trafik som förflutit mellan kontot och målsystemen.

Om vi stannar här och inte går djupare än så, finner den insatte att vi med denna exemplifiering givit ett antal områden där ett loggutdrag faktiskt kan ifrågasättas. I grund och botten går denna frågeställning ut på att säkerställa om den organisation som tagit fram, och presenterat loggutdragen, har haft kontroll på informationen i alla led.

10.5 Avsaknad av kritisk bevisvärdering

Om vi lämnar polisens organisation och återgår till en mer generell diskussion så känner vi vid det här laget till att loggar samlas in av polisen från olika organisationer som banker, företag, myndigheter och teleaktörer [Keyzer, Leijon].

Vad händer den dag ett loggutdrag ifrågasätts med motiveringen att den misstänkte inte utan vidare litar på ett papper med ett textinnehåll som visar att en viss trafik utförts med den misstänktes konto.

Hur skall man då ställa sig till det faktum att informationen tagits fram av oidentifierade människor i en miljö som saknar insyn och med metoder som ingen känner till [Leijon, Keyzer]. Skulle någon annan bevisning som presenteras inom svenska domstolar benämnas som bevis som tagits fram på liknande sätt? En liknelse kring denna huvudfråga har identifierats kring den DNA-bevisning som i dag förekommer i våra domstolar [Ericsson].

Intervjuerna med personer inom rättsväsendet har visat att det i dag inte ingår någon kontroll av den information som polisen får fram genom loggutdrag i form av t.ex. telefonlistor, transfereringar och loggkontroller för åtkomst till olika system [Keyzer, Leijon, Engfeldt, Bergnér, Ekelund]. I vanliga fall görs nästan alltid en värdering i form av en bedömning av sannolikheten att en viss bevisning verkligen håller för vad den påstår. Man ställer frågor till ett vittne för att se om det kan finnas kopplingar mellan vittnet och vad denne har iakttagit. Detta för att kunna göra bedömningen om vittnet har en relation till det som berättelsen omfatta, eller på annat sätt står i en förbindelse som kan påverka vittnets berättelse. Ett exempel på detta är att det i Rättegångsbalkens 36 kap, 6 § står angivet att den som är släkt till en viss nivå, sambo eller gift med den som berättelsen omfattar, inte behöver vittna i en domstol över det som vittnet sett. Det är givetvis av vikt att en sådan relation lyfts fram i förhöret. Detta för att alla fakta skall finnas tillgängliga för att kunna göra en värdering av bevisvärdet i den berättelse som har lämnats.

Andra exempel på kopplingar som inte omfattas av RB 36:6 är t.ex. vänskap, ekonomiska förhållanden och hot. Den allmänna vittnesplikten tar inte hänsyn till sådana förhållanden, men det kan individen tänkas göra. Den relation man kan finna mellan vittnet och den som berättelsen omfattar kan på ett eller annat sätt göra att trovärdigheten till vittnet antingen stärks eller minskas. En relation som tidigare arbetskamrat gör att det är lättare att sätta tilltro till en identifiering eftersom vittnet sett den aktuella personen många gånger tidigare. Med detta börjar vi förstå att den tekniska och administrativa miljön hos organisationen är något som måste beaktas vid värderingen av ett loggutdrag.

Vid resonemanget med fingeravtrycket på glaset förs ett resonemang om det går att utreda när glaset kom dit [Durling]. Vid andra sammanhang när man t.ex. säkrar DNA så gäller samma sak. Saliv från utandningsluft i en rånarluva gör inte den utpekade till gärningsman. Man kan bara konstatera att dennes DNA finns i den luva som använts i samband med rånet. Helt klart blir personen skäligen misstänkt, men annan stödbevisning måste säkerligen till för att leda till en fällande kom.

Gemensamt för ovanstående resonemang är att man i samband med den mesta bevisning för ett sannolikhetsresonemang kring bevisningen. Inget sådant verkar ske när det gäller logganalyser. Dock anses vissa större organisationer har större tillförlitlighet vid leverans av loggutdrag, som t.ex. IBM, jämfört med mindre organisationer. Då skall man komma ihåg att den uppgiften kommer från en utredare vid Länskriminalens IT-rotel i Stockholm, och som därmed räknas till en av experterna inom svensk polis. Men inte heller vid denna enhet gör man skillnad på informationsvärdet i en logganalys beroende på valet av autenticeringsteknik [Keyzer].

Ett bevis som enbart ett loggutdrag utgör kommer dock inte att tillmätas samma stora värde som t.ex. DNA eller ett fingeravtryck. Detta beroende på att ett loggutdrag aldrig ensamt kan peka ut den fysiska personen som gjort slagningen. Loggen talar framförallt om att ett IT-system använts på ett visst sätt.

Av den anledningen är det tveksamt om en person som förnekar all inblandning i ett loggärende skulle kunna åtalas med enbart loggutdraget som bevis [Ekelund, Roswall].

10.6 Vem ansvarar för att loggutdragen är korrekta?

Genom intervjuerna med personal från de tre yrkesgrupperna polis, åklagare och advokat har vi tagit med den personal som har möjlighet att värdera, analysera och påverka den bevisning som förekommer i en förundersökning. Det är polisens utredare som håller förhör, tar i beslag och redovisar utredningen till åklagaren när den är klar. Innan detta kan ske skall den misstänkte och dennes försvarare delges hela utredningen enligt Rättegångsbalken 23 kap, 18 §. I samband med detta har den misstänkte och dennes försvarare, i de fall en offentlig försvarare utses, möjlighet att begära kompletteringar av utredningen. Först när dessa uttryckligen godkänt förundersökningsprotokollet, eller att förundersökningsledaren bestämmer att eventuella invändningar inte skall beaktas, kan åklagaren väcka åtal. Om åklagaren på objektiva grunder kan emotse en fällande dom kommer denne att kunna väcka åtal.

Om man tittar lite närmare på denna kedja så finner man att det finns ganska goda möjligheter att under resans gång rätta till eventuella felaktigheter. Detta i och med att systemet är uppbyggt kring en förundersökning där samtliga steg i utredningen återfinns i den samlade dokumentation som förundersökningsprotokollet utgörs av RB 23 kap, 21 § (Rättegångsbalken). Vem bär då huvudansvaret för att materialet som presenteras i förundersökningsprotokollet är korrekt?

Den som hanterar, tar fram eller lämnar över någonting till åklagaren har ansvaret för att det som lämnas över är korrekt. I och med att det är polisen som lämnar över förundersökningen till åklagaren ligger detta tjänstemannaansvar på de utredare som handlagt utredningen. Om ingen ifrågasätter ett loggutdrag kommer man att lita på den skriftliga bevisning som loggutdraget står för. Därmed ligger det även ett ansvar hos den som förundersökningen är riktad mot samt dennes försvarare [Ekelund].

Eftersom loggutdragen generellt är svåra att förstå är det vanligt att dessa bearbetas manuellt i samband med analysarbetet. I detta arbete finns det en förståelse för, och en medvetenhet om, att något kan gå fel. I övrigt följer loggutdragen samma principer som all annan skriftlig bevisning. Man kan på så sätt jämföra loggutdragen med ett skriftligt förhör. Om uppgifterna i förhöret skulle vara felaktiga, men ingen ifrågasätter dessa, är det troligt att ingen annan heller gör detta. Det ställs således stora krav på noggrannhet hos alla personer som arbetat med loggutdrag som åberopas som bevisning i en huvudförhandling [Ekelund].

Om den misstänkte nekar till anklagelserna och hävdar att denne är oskyldig så måste åklagarsidan börja söka efter alternativa förklaringar. Ett förnekande av loggutdragen skulle innebära att man är tvungen att titta närmare på autenticeringsrutiner, trojaner, kompletterande vittnesförhör eller se om det finns möjlighet för andra att ta del av t.ex. ett lösenord [Roswall, Engfeldt].

IT-åklagare har i allmänhet den kunskap och erfarenhet som behövs för att kunna värdera IT-relaterad bevisning på ett sätt som allmänna åklagare saknar [Keyzer]. Den stora arbetsbördan gör dock att de tio IT-åklagarna i Stockholm endast hinner med att ta sig an de mest komplicerade åtalen.

Det händer därför ofta att allmänna åklagare, utan speciell IT-kompetens, väcker åtal i IT-relaterade brott. Dessa har sällan den kompetens som krävs för att förstå den bevisning som förundersökningen kan innehålla [Roswall]. Allmänna åklagare, utan IT-kompetens, kommer i större utsträckning att accepterar det material de får på grund av sin bristande kompetens inom området. De kan inte ifrågasätta eller bedöma materialet på samma sätt som en IT-åklagare [Keyzer].

Per-Erik Bergnér, som under flera år arbetat som internutredare inom Stockholmspolisen, har aldrig fått någon närmare undervisning eller presentation av hur loggarna hanteras inom svensk polis. Eftersom han inte har denna kunskap vet han heller inte hur en logg transporteras och lagras inom polisens system innan den till slut når honom. I stället ser han loggutdragen som ett rättsintyg. Loggutdraget är framtaget av en expert på samma sätt som ett rättsintyg är skrivet av en läkare. I stället för att läkaren får vittna om offrets skador i domstolen kan åklagaren använda sig av rättsintyget som därmed har samma styrka. Loggutdragen ses därmed med samma ögon som ett rättsintyg. Därmed är inte utredaren ansvarig för att loggutdragen är korrekta när de kommer till denne. Utredaren är ansvarig för den manuella hantering som denne ligger bakom i syfte att göra loggutdragen mer lättförståeliga [Bergnér].

Bergnér är den polis som arbetat med förundersökningarna mot de polisanställda som fastnade i loggkontrollerna i samband med Anna Lindh ärendet. Första gången han blev medveten om att ett loggutdrag kunde vara felaktigt var när det gjordes ett omtag av loggutdragen eftersom dessa visade sig vara ofullständiga. Det framkom då att det fanns olika script för att ta fram loggutdragen vilket skapade delvist ofullständiga, men framför allt olika loggutdrag. För att upptäcka detta krävdes en kunskap som Bergnér själv inte innehade.

När ett loggutdrag når polisen i samband med olika utredningar om brott tas dessa emot av polisen utan att man känner till hur dessa tagits fram [Keyzer]. Jim Keyzer är medveten om att det finns goda möjligheter att loggutdragen kan vara manipulerade när de når polisen. Främst är det möjligt att göra i samband med den manuella hantering som ofta sker hos den organisation som levererar utdragen. Loggutdragen har tagits fram av en tekniker inom en främmande organisation utan att Keyzer eller någon från hans avdelning varit närvarande. De har med andra ord ingen som helst kontroll på informationen när de får loggutdragen, utan tvingas att lita på att dessa är korrekta när de kommer. Dessa loggutdrag kommer att få en framskjutande roll i den utredning som ärendet omfattar. Utdragens betydelse står dock i förhållande till den misstänktes inställning. Det har dock hittills aldrig hänt att någon ifrågasatt riktigheten hos ett loggutdrag [Keyzer].

Ingemar Leijon är van att få in loggutdrag från teleoperatörer och banker. Dessa loggutdrag tas fram av administratörer inom respektive organisationer och skickas oftast med vanlig post till honom. Eftersom han är van vid att arbeta med materialet i en dator begär han in loggutdragen på CD-skiva medan de flesta andra på hans avdelning ber om att få dem på papper. Detta på grund av att kollegorna inte har lika stor datorvana. Leijon säger uttryckligen att ansvaret över loggutdragen hamnar hos honom i samband med det att han tar emot dem. Hur materialet hanterats eller bearbetats innan det når honom ligger inte inom hans ansvarsområde.

När man tar emot loggutdragen från en organisation utgår man alltid ifrån att dessa är korrekta och sanningsenliga. Loggutdragen man får in på detta sätt är ingenting som man ifrågasätter.

Man utgår aldrig från att dessa skulle kunna vara felaktiga. Av den anledningen ställer man inte några frågor som skulle kunna vara till hjälp för att värdera loggutdragets bevisvärde. Med detta avses frågor som hur användaren/användarna bevisat sin identitet för målsystemen eller om trafiken i organisationens lokala nätverk går i klartext. Man litar helt enkelt på att loggutdragen är sanningsriktiga utan att ta reda på vare sig autenticeringsmetod eller hur trafiken skyddas i organisationens nät [Leijon].

I och med att ingen hittills ifrågasatt riktigheten i ett loggutdrag bör detta indikera att loggutdragen är korrekta. När det gäller loggutdragen blir det i regel ingen diskussion om dem i rätten, och en av orsakerna skulle kunna vara att de är så svåra att förstå. Till detta tillkommer att kunskapen om hur loggen genereras och hanterats är ett tämligen okänt område, men då den misstänkte inte ifrågasätter loggutdragen eller dess sammanfattningar leder detta till att det i allmänhet inte blir någon diskussion i detta ämne. Det ligger dock i det generella arbetet att det material som presenteras för åklagaren i olika utredningar är framtaget på ett korrekt sätt och därmed skall vara korrekt. Av den anledningen lägger även Engfeldt ansvaret på de utredare som handlagt den aktuella förundersökningen [Engfeldt].

Om det i framtiden börjar inträffa att den misstänkte ifrågasätter loggutdragens riktighet kommer detta att leda till samma ställningstagande som gäller i övriga fall en misstänkt nekar till en anklagelse. Vid all bevisvärdering finns en huvudregel som säger att man skall lita på vad den misstänkte har att säga så tillvida att det denne säger kan lämnas utan avseende eller motbevisas. Det innebär att man som åklagare, i ett fall där loggutdraget ifrågasätts, blir tvungen att göra en djupare undersökning kring möjligheten för någon annan att ligga bakom den trafik som loggutdraget anger. För detta arbete skulle man vara tvungen att involvera sakkunnig personal som gör en undersökning kring möjligheten att manipulera systemet eller systemen i fråga [Engfeldt].

Det underlag som tas fram kommer att ligga till grund för åklagarens ställningstagande i åtalsfrågan. Kan den misstänktes berättelse motbevisas genom den fördjupade förundersökningen kan åtal väckas, annars inte. På så sätt skiljer sig inte resonemanget kring loggutdragen som bevis från annat resonemang kring bevisvärdering.

Samtidigt är det som så att dataintrång är ett bötesbrott. Det innebär att den misstänkte sällan tilldelas en offentlig försvarare. I ärenden med IT-relaterad bevisning kan det därför vara svårt att försvara sig då man sällan förstår tekniken som ligger bakom [Roswall].

Advokaten ses i allmänhet som en garanti för rättssäkerheten i våra domstolar. I samband med slutdelgivningen enligt RB 23:18 har den misstänkte, tillsammans med sin försvarare, rätt att komma med synpunkter på utredningen. De kan då begära kompletteringar i form av nya eller kompletterande vittnesförhör o.s.v. Möjligheten för att en advokat skall kunna vara sin klient behjälplig i de fall där bevisningen bygger på IT-relaterad bevisning är dock liten. Den kompetens som krävs för att kunna ifrågasätta ett loggutdrag finns normalt inte inom personalen som arbetar som åklagare, advokater eller domare [Durling]. För advokat Durlings egen del utgör ett loggutdrag ett mycket svårangripligt bevis. Enligt denne krävs det i dag specialkompetens för att kunna hantera sådana här mål.

Även Johan Ericsson vittnar om de svårigheter han upplever med att försvara klienter som är misstänkta för brott där bevisningen helt eller delvis är IT-relaterad. Han finner det svårt att angripa åklagarens bevisning i och med att han inte alltid förstår den.

Detta gör att han agerar återhållsamt för att inte riskera att klienten hamnar i en värre situation genom att ställa fel frågor. Hans uppfattning av denna typ av bevisning är att juridisk personal undviker problemet eftersom man är rädd för att ge sig in på ett område som man inte behärskar. Detta trots att loggar av olika slag har ett mycket högt bevisvärde. Detta gäller speciellt så kallade telefonlistor som t.ex. visar hur en person ringt med sin mobiltelefon. Trots att teleaktörerna medgivit att deras system kraschat, och att loggutdragen visat att telefonen varit både på och av samtidigt, har dessa loggar i vissa fall till och med vägt tyngre än vittnesbevisning [Ericsson].

Ola Salomonsson säger att han inte vet hur han skall agera den dag en klient ifrågasätter riktigheten i ett loggutdrag. För egen del har han inte den kunskapen att han kan göra det. Den typ av kunskap som det kräver saknas i dag i allmänhet inom advokatvärlden. Han har över huvud taget aldrig tänkt i de banorna att loggarna eller loggutdragen skulle kunna vara manipulerat eller av andra orsaker felaktigt. Som skäl till detta anger han vidare att det aldrig hänt att en klient har ifrågasatt riktigheten i ett loggutdrag [Salomonsson].

10.7 Input i logganalysen

Ingen av de informanter vi intervjuat har tagit med någon ytterligare input i logganalysen än loggutdraget. Informanternas förklaringar till detta är olika. Ett skäl är att det inte har funnits någon anledning till detta eftersom ingen hittills har ifrågasatt loggutdragen. Huvudskälet är dock att man litar blint på att loggutdraget är korrekt, varför något behov att lägga in fler parametrar i analysen inte varit nödvändiga. Anledningen till detta är att det i dag saknas kunskap bland de rättsvårdande instanserna som gör att dessa inte är medvetna om att fler variabler i logganalysen skulle kunna generera en helt annan slutsats [Engfeldt].

Trots att Perstorpsärendet (Helsingborgs tingsrätt B 2697-03) visar hur sårbara system är som endast identifierar användaren med lösenord har det inte föranlett att detta är något man frågar efter när man tar emot ett loggutdrag. Man litar på att loggutdraget är korrekt trots tidigare vetskap om att en för svag autenticering kan innebära att trafiken i systemet genererats av någon annan än kontoinnehavaren [Leijon].

De enda som vill ha in mer information i logganalyserna är de informationsexperter som vi intervjuat. Dessa ser inte loggen som ett bevis utan som en pekare på att någonting inträffat. I stället för att lita på loggutdraget använder man detta för att söka efter information som kan tänkas återfinnas på hårddisken.

10.8 Teknikexperternas åsikter

Skillnaden mellan hur de rättsvårdande instanserna och tekniksäkerhetsexperterna ser på loggutdragen är markant. För att en logg skall vara någorlunda trovärdig krävs det enligt experterna att hela händelsekedjan är säkrad för att en logg skall kunna betraktas som pålitlig och trovärdig. Åtgärder måste därför vidtagas på en rad olika områden. Klienterna måste säkras så de inte bär på någon okänd programvara, nätverket skall inte kunna ”sniffas” utan att det upptäcks, loggarnas integritet måste kunna garanteras i samband med transport i systemet och autenticeringen av användare och administratörer ses som en avgörande del när det gäller loggutdragens trovärdighet. Brister det redan i autenticeringen spelar det ingen roll hur mycket teknik och säkerhet man byggt in i systemen. Kan man inte lita på att loggen pekar ut rätt användare har de mycket litet bevisvärde [Söderholm & Olsson].

Eftersom en administratör har stora rättigheter på den dator som denne är administratör på kan denne, beroende på rättigheter, göra saker som vanliga användare inte kan göra. Administratörens möjligheter till förändringar är något som sällan ifrågasätts. Dess närvaro är nödvändig för att systemen skall fungera, men en administratör som inte följer regelverken kan göra hur stor skada som helst. Bland annat kan en administratör generera trafik som loggas på en enskild användare så att det i loggarna ser ut som om det är denne som genererat trafiken. Vidare kan en administratör radera loggar och installera programvaror på servern. Exempel på programvaror som kan påverka loggarna är så kallade root kits som därutöver kan dölja processer som körs på datorn [Richardsson].

Generellt kan sägas att loggarna i sig inte ses som det främsta bevisbärande underlaget, utan dessa ses mer som en pekare på att någonting hänt. Bevisningen hämtas i stället på den hårddisk som suttit i aktuell dator. Av den anledningen kan IP-adressen användas för att peka ut en användares dator varefter en undersökning görs av hårddisken i syfte att söka spår efter den trafik som loggutdraget indikerar.

Eftersom informanterna med en teknisk bakgrund är så medvetna om vilka hot som finns mot den trafik som transporteras i ett nätverk är de medvetna om hur ett loggutdrag kan ifrågasättas. Den kompetens som dessa besitter kommer dock inte de rättsvårdande instanserna tillgodo eftersom dessa sällan efterfrågar deras kompetens. Anledningen till detta har visat sig vara flera. För det första är det få som har sådan kunskap inom området att de förstår att ett loggutdrag över huvud taget kan ifrågasättas. För det andra är brottet dataintrång ett bötesbrott, något som innebär att den misstänkte normalt inte tilldelas en offentlig försvarare. Den misstänkte står därmed ensam att försvara sig utan hjälp av en advokat. Det har dock visat sig att en advokat i detta fall inte är någon garanti för ett bättre ifrågasättande eftersom inte heller dessa vet hur de skall bete sig för att ifrågasätta ett loggutdrag. Vidare är teknikexperter dyra att anlita varför kostnaderna ofta framstår som för stora i förhållande till brottets art. Den misstänkte kan därför utan vidare inte räkna med att kostnaderna för dennes försvar betalas av staten, vilket närmast skulle vara en självklarhet om brottet vore allvarligare än endast ett bötesbrott.

Intervjuerna med informationssäkerhetsexperterna har visat att det finns en mängd områden som måste säkras för att en logg skall komma i närheten av att tillmätas någon form av betydelse. Att lita på ett loggutdrag så som man i dag gör inom de rättsvårdande instanserna är något som inte existerar inom deras värld. Att bygga system som genererar fullkomligt tillförlitliga loggar går knappast att bygga [Richardsson, Söderholm & Olsson].

10.9 Den tekniska samt administrativa miljön

Anledningen till att författarna valt att ta med en teknisk del i uppsatsen (avsnitt 8) är att visa hur viktigt det är att behärska delar av den teknik som råder i ett nätverk för att kunna värdera sanningsinnehållet i ett loggutdrag. Loggarnas sakinnehåll exkluderas i uppsatsen eftersom den processen innebär tester i den avslutande delen av systemutvecklingsfasen där man kontrollerar att loggarna loggar rätt saker.

Den teoretiska referensramen angående teknik visar att det rör sig om en ganska komplicerad värd som beskriver var loggen föds, transporteras och lagras. Den teoretiska referensramen om hot mot datakvaliteten i ett nätverk har visat att det finns ett antal hot mot de data som hanteras mellan datorerna i ett nätverk. Dessa hot kan mötas med olika säkerhetstjänster som tillhandahålls för att ge en specifik form av skydd mot systemens resurser.

Kopplingen mellan datakvalitet och förundersökning innebär att man måste börja behandla IT-relaterad bevisning på samma kritiska sätt som all annan skriftlig bevisning. Att någonting står skrivet på ett papper innebär inte att det är sant. Det görs alltid en form av bevisvärdering. En läkare som skriver ut ett rättsintyg kan mycket väl resultera i en bevisvärdering som är mycket låg om det visar sig att läkaren har en relation till den som är misstänkt eller på annat sätt kan kopplas till intyget. Några sådana värderingar verkar inte finnas när det gäller ett loggutdrag.

Ett loggutdrag som visar vem som loggat in i systemet, när det skett och varifrån det skett utgör ofta en del av säkerhetsloggen för ett system. Vad användaren gjort i systemet återfinns ofta i andra loggar, som applikationsloggen. Detta är dock inte skrivet i sten eftersom varje systemägare fritt kan definiera loggarnas namn och vad respektive logg skall innehålla. Erfarenheter av logganalyser på Riskpolisstyrelsen visar att så är fallet. Den information som anges i detta stycke räcker för att åtala en polisanställd för brott mot befogenheten om denne misstänks för att ha utfört en slagning i ett system utan giltig anledning. Om loggutdraget skall kunna tillmätas någon form av bevisvärde förutsätts att det är riktigt. Det innebär att det i verkligheten är aktuell person som loggat in i systemet och utför den trafik som loggats från angiven dator. Att så verkligen är fallet är dock ingen självklarhet. Trafiken kan mycket väl vara genererad av någon annan än kontoinnehavaren, vilket förutsätter att loggutdragets sanningsinnehåll är falskt.

Den teoretiska referensramen om teknik är tänkt att ge läsaren en förståelse av att det är svårt att bygga system som ger loggutdrag med ett sanningsinnehåll som är sant. Några av informanterna hävdar att detta är omöjligt eftersom det alltid finns människor inblandade genom behovet av administration och förvaltning [Söderholm & Olsson]. Detta sker genom administratörer som har stora rättigheter i operativsystemen som applikationerna körs på, samt i själva applikationerna. Dessa personer är en förutsättning för att systemen skall fungera, men utgör samtidigt ett hot genom deras rättigheter i systemen och applikationerna.

Eftersom man idag inte ifrågasätter vare sig riktigheten eller sanningsinnehållet i ett loggutdrag blir kopplingen till tekniken någonting som inte inryms i dagens logganalyser. Av den anledningen gör vi kopplingen mellan loggutdragens sanningsinnehåll och val av teknik i kapitel 12 där vi redogör våra förslag för morgondagens logganalys. Vi nöjer oss i denna analysdel med att konstatera att någon hänsyn till val av teknik i dag inte tas när man skall värdera loggutdragens bevisvärde. Den främsta anledningen till detta är att man inte har den kunskap som krävs för att klara av detta.

Med anledning av det som framkommit under intervjuerna med informanterna har författarna diskuterat fram ett antal områden som kan ligga till grund för en bättre bedömning av loggutdragens bevisvärde. Dessa områden skulle kunna fungera som ytterligare input i analysarbetet genom att använda sig av något som skulle kunna kallas för ett utökat loggutdrag i logganalysen. Nedan diskuteras och motiveras varför det utökade loggutdraget måste se ut som det gör. För respektive punkt i detta avsnitt för vi ett närmare resonemang i syfte att visa på vilket sätt aktuellt område kan tillföra något i detta avseende. Om X.800 standarden generellt talar om en säker arkitektur för OSI-nät så är förslaget på ett utökat loggutdraget nedan specifikt anpassade till logganalysen.

Transport

- *Går lösenordet mellan klient och server i klartext?*
- *Kan man sniffa nätverkstrafiken eller finns det skydd mot inkoppling av ny* utrustning *i det lokala nätverket?*
- *Har organisationen ”hubbade” eller ”switchade” lokala nätverk?*
- *Finns stöd för att ge loggen ett integritetsskydd under transport?*

Lagring

- *Hur skyddar man de servrar eller andra lagringsmedier som lagrar loggarna?*
- *Hur många administratörer har åtkomst till maskinvara eller media som lagrar loggarna?*
- *Finns stöd inbyggt för att ge loggen ett integritetsskydd under lagring?*

Hantering

- *Hur har den manuella hanteringen av loggen gått till?*
- *Finns det stöd för spårbarhet av den manuella hanteringen?*

Övrigt

- *Är klientens placerad på så sätt att det visuellt går att avläsa lösenord som användaren skriver?*
- *Hur har användaren autenticerat sig för målsystemet?*
- *Hur har målsystemet autenticerat sig för användaren?*
- *Har klienten någon form av boot skydd (omstartsskydd) som förhindrar nedladdning av främmande programvara?*
- *Finns det antivirusprogram på klienten?*
- *Har organisationen koppling till Internet?*
- *Vid autenticering med lösenord, låses kontot vid ett visst antal misslyckade inloggningsförsök?*
- *Finns det möjlighet att finna spår på användarens hårddisk som styrker loggen?*

10.9.1 Transport

10.9.1.1 Klartext i nätverket

I den teoretiska referensramen angående teknik beskriver författarna i övergripande termer hur trafiken i ett TCP/IP nät går till. Det är av stor vikt att den som ger sig in i en bevisvärdering av ett loggutdrag, eller på annat sätt deltar i analysen av ett loggutdrag, skall kunna göra en korrekt bedömning och ställa de rätta kontrollfrågorna.

När man skall värdera ett loggutdrag utifrån frågeställningen hur nätverkstrafiken ser ut hos den organisation som levererat ett loggutdrag måste man minst vara medveten om hur ett normalt konfigurerat TCP/IP nätverk fungerar. För detta hänvisar vi till den teoretiska referensramen om teknik i kapitel 8. Man måste vidare känna till vilka skydd som kan implementeras för att organisationen skall kunna uppnå en högre nivå av informationssäkerhet, och då vi här talar om nätverkstrafik, den tekniska säkerheten (se kapitel 7).

Om trafiken över nätverket mellan en klient och server går i klartext är det fullt möjligt att lyssna av dessa om trafiken sker i en miljö där det är möjligt att koppla in ny utrustning på det lokala nätverket.

Styrs adresstilldelningen av en DHCP är det som regel bara att trycka in nätverkskabeln i nätverksuttaget eftersom konfigurationen av den nya utrustningen sköts automatiskt. På så sätt har man ett omedelbart tillträde till nätverket. Det enda man behöver göra är att konfigurera sin dator så att den accepterar dynamisk tilldelning av IP-adress. Vid statisk adresstilldelning krävs en del efterforskningar i form av default gateway och subnät.

FTP och SSH (Secure Shell) är exempel på vanliga protokoll på applikationsnivå som kan används för att administrera plattformar i en organisation. FTP har den svagheten att den skickar användarnamn och lösenord i klartext över nätverket. Finns ingen ”end-to-end” kryptering inbyggd i klient och server kommer denna trafik att skickas i klartext (se kapitel 8.17).

Ett avlyssnat lösenord till ett konto på t.ex. en Unix-server kan få förödande konsekvenser. Många servrar kör Unix som operativsystem, och dessa måste många gånger administreras från en central punkt. SSH har den fördelen att protokollet krypterar trafiken mellan klient och server, varför detta ur ett säkerhetsperspektiv är att föredra. På plattformen finns ett antal konton. Om kontoinnehavaren är med i den så kallade ”SUDO-gruppen[71]” kan denne logga in på servern med sitt eget användarkonto och lösenord, för att därefter med kommandot SUDO byta till root rättigheter (administratör). Detta kan ske med samma lösenord som man använt för att logga in på sitt konto. Med denna vetskap finner man att lösenord som skickas i klartext över ett nätverk kan få stora konsekvenser eftersom en administratör med fulla rättigheter kan göra allt på en dator.

Eftersom det inte är ovanligt att lösenord överförs i klartext är detta ett reellt hot. Protokoll som FTP, POP3 (Post Office Protocol)[72] och SMTP (Simple Mail Transfer Protocol) är exempel på vanligt förekommande protokoll vilka alla har den egenskapen att de skickar lösenorden i klartext. Applikationer som ligger till grund för åtkomst i egenutvecklade system måste antingen utnyttja befintliga tjänster i nätverket eller vara skrivna på ett sådant sätt att informationen skyddas. Finns inga generella skydd i nätverket ligger hela ansvaret hos applikationen.

10.9.1.2 Hubbade eller switchade nät

I kapitel 8.12 anges några nätverkskomponenter som används i ett nätverk för att trafiken skall kunna fungera. Eftersom större nätverk är uppdelade i subnät måste dessa särskiljas med en t.ex. en gateway. För att undvika att alla datorer i subnätet har en egen kabel till gatewayen kopplar man samman dessa i något som kallas för topologier. En topologi är stjärnnät och en annan topologi är ringnät. Vi talar här bara om stjärnnät vilket innebär att varje dator har en kabel dragen till en kopplingspunkt som kan vara en hubb eller en switch. Dessa fungerar helt olika avseende hur trafiken hanteras i subnätet.

I kapitel 8.12 och 8.12.3 anges skillnaderna mellan dessa båda tekniker. Vad som är viktigt att känna till är att valet av kopplingspunkter påverkar möjligheten att lyssna av nätverkstrafiken på ett högst påtagligt sätt. Det är svårare att sniffa av lösenord i ett switchat nät än ett hubbat nät. Ofta krävs åtkomst till de korskopplingsskåp där switchen är placerad, och många organisationer är medvetna om detta och håller dem låsta.

---

[71] I Unix kan administratören sätta upp ett regelverk som anger att valda kontoinnehavare får köra kommandon mot operativsystemet som annars endast kan köras med root tillhörighet.

[72] POP3 är ett vanligt protokoll som används för att hämta post i en e-postlåda till användarens egen dator. Användaren autenticerar sig genom att ange ett användarnamn och ett lösenord. Detta sker transperent för användaren av protokollet. POP3 fungerar tillsammans med SMTP. [Dyson, 1999]

Att en switch är säkrare än en hubb innebär dock inte att ett switchat nät är säkert bara för att man bytt ut hubben mot en switch. Det finns metoder för att lura switchen vilket gör att detta är ännu ett exempel på att logganalytikern måste vara kunnig inom nätverkstekniker (se avsnitt 8.15).

10.9.1.3 Integritetsskydd

Det är ingen självklarhet att bestämma vad det är för någonting som en organisation skall logga. Klart är dock att loggarna kan genereras både hos klienten och hos de system som användaren anropar. En del organisationer har inga klientloggar eftersom man räknar med klienten inte går att skydda på ett sådant sätt att dess integritet kan garanteras. I stället utförs all loggning av de system som anropas. Andra organisationer loggar både vad som händer hos klienten och det som händer i målsystemet.

Finns inget skydd i form av t.ex. signering av en logg, eller en grupp av loggar, är det i teorin möjligt att förändra loggarna under transport och lagring. Utan integritetsskydd går det att skapa falska loggar i syfte att skjuta trovärdigheten för loggarna i sank. Detta är möjligt om det finns en möjlighet att koppla in otillåten mjuk- och hårdvara i nätet mellan sändande och mottagande system [Söderholm & Olsson]. I kapitel 8.18 beskrivs den teknik närmar som kan användas för att skydda integriteten hos data som transporteras i ett nätverk.

10.9.2 Lagring

10.9.2.1 Serverskydd

Så fort en människa har fysisk åtkoms till en dator har denne möjlighet att påverka säkerheten i datorn [Richardsson, Söderholm & Olsson]. Beroende på vilka skyddsmekanismer som vidtagits är en enskild dator olika sårbar. De loggar som ligger lagrade på samma server som applikationen som genererat dem är i regel mer sårbara än om den lagras på en annan dator. Detta förutsätter att en och samma administratör inte har åtkomst till de bägge datorerna, utan enbart den ene. Exempel på serverskydd är inlåsning i bur med begränsad fysiskt åtkomst. Ett annat skydd är en krypterad hårddisk som även fungerar som ett boot skydd. Ett tredje skydd är signerade binära filer, som t.ex. *.exe filer som inte tillåts exekvera utan ett giltigt certifikat [Richardsson].

Extremt känsliga system, som en CA i ett PKI-system, vilken är den enhet som signerar användarnas certifikat, måste skyddas maximalt. Kan man inte garantera att CA:s privata nyckel är säker faller hela förtroendekedjan i en PKI-struktur. För att skydda en organisations CA kan man lösa detta genom inlåsning i speciella burar bakom tjocka väggar och låsta dörrar. Genom videoövervakade områden kan man hålla kontroll så att endast ett fåtal får tillträde till i kombination med olika former av två eller trehandsfattningar. D.v.s. att det krävs två eller kanske tre personer i kombination för att kunna genomföra en förändring på servern.

Vissa organisationer lagrar sina data i krypterad form. Detta ställer på längre sikt krav på att det är möjligt att återställa data okrypterad form. Lagras även loggarna i krypterad form måste dessa antingen dekrypteras innan de läses ut för analys eller skickas i krypterad form. Om sistnämnda gäller så att dekrypteringen sker på annat håll kommer frågor som nyckelhantering och nyckeldistribution in i bilden. Frågor som alltid är av en vital del av hur hela säkerhetskedjor hänger samman.

10.9.2.2 Tilldelningen av administratörers rättigheter

En dator måste kunna administreras av en administratör, annars kommer den förr eller senare att stanna. En dator är ingen statisk installation, utan den kräver hela tiden service och underhåll, inte minst därför att den som regel verkar i en miljö som inte är statisk. En plattform, t.ex. Unix eller Windows, som är bärare av en applikation som genererar loggar, skall inte lagra de aktuella loggarna på den egna disken [Richardsson]. Innan dessa diskutrymmen fylls måste de föras över till andra lagringsmedier. Då är det viktigt att det finns något som garanterar att all information förts över, och att denna överföring i sig är skyddad mot manipulation. Sker det en ömsesidig autenticering av systemen, eller vad finns det för skydd som garanterar att loggarna lagras på rätt ställe och att loggarna kommer från rätt ställe [Söderholm & Olsson].

Av ovan anledning bör det utredas hur serverskyddet ser ut. Lämpliga frågor att ställa är om en separering mellan producerande (applikationsbärande) och informationsbärande (logglagrande) servrar har gjorts. Hur många administratörer har tillträde till respektive server samt om dessa har tillträde till fler än bara den ena servern? Kort sagt, hur har man mött hotet från en eller flera onda administratörer.

10.9.2.3 Integritetsskydd under lagring

En logg som är åtkomlig för en administratör kan även editeras (förändras) av en administratör om inte speciellt skydd byggts in för detta ändamål. Speciella operativsystemsloggar skyddas normalt av operativsystemet, men bara när operativsystemet är igång. Stänger man av datorn kan datorn bootas om (startas om) med speciell programvara varefter informationen på detta sätt kan bli åtkomlig. Speciella rootkit kan göra samma sak utan att servern tas ner. Har man däremot ett integritetsskydd av loggen som inte bara omfattar en logg unikt för sig, utan en kedja av sådana så kan man ge en möjlighet till upptäckt om delar av en loggmängd raderas eller förändras eller att nya loggar läggs till [Richarsson, Söderholm & Olsson].

10.9.3 Hantering

10.9.3.1 Manuell hantering

Avsnittet om manuell hantering kan egentligen göras hur långt som helst. Den som arbetat med denna typ av ärenden behöver bara använda sin fantasi för hur informationen kan förändras längs denna väg. Det behöver inte vara med uppsåt, det kan vara mänskliga misstag och programmeringsfel som orsakar dessa.

Med hantering avser vi all form av hantering av loggen efter det att den lyfts ut från sin så kallade original lagringsplats. I allmänhet är det frågan om ett backup band som loggen ligger på, men det kan även vara en raidade[73] eller speglade (kopierad) hårddiskar. Vad som tillkommer är hur loggarna skickas från det ene lagringsmediet till ett annat. Som regel är det en speciell administratör som tar fram loggen. Den måste sedan transporteras till mottagaren som beställt den. Det kan ske via nätverk eller fysiskt på CD/ROM eller liknande. Att skicka en CD/ROM osignerad i ett internkuvert är ingen bra lösning eftersom vem som helst då kan plocka upp den, öppna den i sin egen dator, göra förändringar eller borttag för att därefter bränna ner informationen på en ny CD/ROM.

[73] RAID (Redundant Array of Inexpensive Disks) är en metod att använda flera hårddiskar och på så sätt skapa redundant lagring av data [Dyson, 1999].

Genom intervjuerna med personal inom rättsväsendet vet vi att loggarna många gånger kommer till utredarna med vanlig post [Leijon, Keyzer].

Det handlar således om att en organisation som presenterar en logg måste kunna redovisa för hur den manuella hanteringen av loggarna har gått till. För detta krävs någon form av manuell logg som visar alla stegen i händelsekedjan, och där varje steg kan bindas till en unik individ. Vad har skett med loggen, när, varför och av vem.

En stor fördel när vi talar om den manuella hanteringen är att originalen, d.v.s. de utföranden loggutdragen hade innan de bearbetades manuellt, kan sparas. På så sätt kan man alltid kontrollera om den manuella hanteringen förändrat loggarnas innehåll under hanteringen.

10.9.4 Övrigt

10.9.4.1 Exponerade lösenord

Om en användare sitter i ett kontorslandskap, eller flera delar på ett rum, finns risken att användaren exponerar sitt lösenord när denne loggar in på sitt konto. Ett exempel på när en användares lösenord kunde läsas av är i ärendet från Perstorps kommun (se avsnitt 9.3) I den utredningen framkom det att gärningsmannen lyckades lura sin chef att logga in i kommunens ekonomisystem med sitt administrationskonto. Gärningsmannen kunde då se vilket lösenord som chefen loggade in med och det var med hjälp av detta lösenord som denne senare loggade in i ekonomisystemet och gjorde överföringar till olika konton på cirka 20 miljoner kronor [Leijon]. Loggarna som skapades var helt korrekta, men om autenticeringen är för svag kommer vi inte att ha någon större bevisvärde av dessa loggar [Söderholm & Olsson]. I detta fall gick det att utredningsvägen att komma fram till att någon annan utfört de överföringarna som loggarna visade. Loggarna från ekonomisystemet var korrekta till sitt sakinnehåll, men falska till sitt sanningsinnehåll då loggarna pekade ut den misstänktes chef vilket i det här fallet var helt felaktigt.

10.9.4.2 Autenticering

På grund av att en dator inte kan skilja mellan elektriska signaler från en användare och en annan användare måste användaren bevisa sin identitet på något sätt. Det finns olika lösningar för hur detta kan gå till där de olika lösningarna i sin tur har olika grad av säkerhet. Vanligaste sättet att bevisa sin identitet för ett system är att visa att man känner till en hemlighet som delas mellan användaren och systemet (se avsnitt 8.20).

För att en logg skall kunna tillmätas någon form av betydelse gäller att man kan lita på autenticeringen av användaren [Söderholm & Olsson]. Med en för svag autenticering avses författarna egentligen all autenticering som bygger enbart på någonting som innehavaren vet. Detta i kombination med krav där loggning krävs för att ge spårbarhet i användarnas hantering av systemet i syfte att kunna använda loggutdraget som bevis i en domstol.

I många organisationer är syftet med en logg att fria oskyldiga samt att kunna fälla dem som överträtt sina befogenheter i systemet. Vad man kanske inte tänker på är att det krävs samma styrka i en logg för att fälla någon som att fria någon. Grunden för all logghantering sker i autenticeringen.

Om man inte kan lita på att den som loggat in i systemet verkligen är den rätta innehavaren till kontot, då har man mycket lite nytta av loggen för syftet att fria eller fälla en användare[74] [Söderholm & Olsson]. Ju känsligare information ett system hanterar desto högre krav ställs det på åtkomstskyddet´(se avsnitt 8.20).

I den teoretiska referensramen angående teknik går i igenom ämnet autenticering i avsnitt 8.20. Ämnet utgör en grundläggande del av området IT-säkerhet och måste enligt författarna vara en av de första grundläggande frågorna som en logganalytiker ställer sig då denne tar del av loggutdraget.

10.9.4.3 Autenticering av målsystem

Det är inte bara av vikt att användaren autenticerar sig för målsystemet. Det kan många gånger vara viktigt att målsystemet autenticerar sig för användaren. Detta sker genom en så kallad ömsesidig autenticering, vilket innebär att både användare och mottagarsystem autenticerar sig för varandra. Detta förfarande förhindrar en så kallad ”Man-In-The-Middle attack” (se avsnitt 8.20).

10.9.4.4 Bootskydd

När en dator startas upp kallas det för att den bootas. Själva uppstartsprocessen är en ganska avancerad process som vi avstår från att beskriva i denna uppsats. Vad som är intressant är att en dator inte behöver någon hårddisk för att bootas. Det går nämligen alldeles utmärkt att boota och köra ett annat operativsystem från t.ex. CD/ROM-skiva genom att läsa in detta i datorns RAM-minne [Richardsson].

Okänd och skadlig kod kan komma in i datorn på detta sätt (se avsnitt 8.22). I dag är det en regel att man letar efter kända trojaners signaturer eller signifikativ kod vid kontroll av beslagtagna datorer i datorrelaterade utredningar. Syftet är att leta efter spår av nuvarande eller tidigare Trojaner eller annan kod som kan påverka sannolikheten att det är den misstänkte som lagrat eller genererat viss information på den beslagtagna hårddisken [Keyzer].

Det som är viktigt att komma ihåg när det gäller datorer som kan bootas med annan programvara är att de skydd som i normala fall kan finnas installerade, t.ex. MS GINA[75] eller annan extern leverantörs GINA, inte utgör något hinder. Dessa skydd ”sover” på hårddisken och exekverar inte förrän de läses in i RAM-minnet. Med bootbara program aktiveras inget av dessa skydd, varför hela hårddisken är åtkomlig.

10.9.4.5 Antivirusprogram

Om en angripare ges fysisk åtkomst till en dator är möjligheterna små att skydda operativsystemets, informationens och applikationernas integritet. Det vi skrivit om i ovan avsnitt vittnar om den saken. Likaså är det något som André Richardsson tar upp i sin intervju.

[74] Däremot skall man vara medveten om att även opålitliga loggar, inklusive klientloggar, kan utgöra ledtrådar och i vissa fall förmodligen även kan användas som indicier.
[75] GINA - Grafisk inloggningsruta mot operativsystemet

Ett sätt att minska riskerna för den skada som skadlig kod (se avsnitt 8.22) kan orsaka är att klienten är utrustad med ett antivirusprogram. Dessa känner ingen de vanligaste formerna av skadlig kod, vilket av allt att döma skulle leda till upptäckt om man lagrar en trojan på så sätt som beskrevs i avsnittet ”Bootskydd”. Dagens antivirusprogram kommer dock inte att känna igen nya eller okända trojaner eller annan form av skadlig kod, vilket gör att ett antivirusprogram inte ger ett fullständigt skydd mot det vi kallar för skadlig kod. Vad man bör tänka på är att det finns legala program som är Trojaner. Dessa omfattas inte av antivirusprogrammen eftersom de säljs legalt på marknaden.

10.9.4.6 Internet

Organisationer med högsäkerhetssystem har ofta ingen koppling mot Internet. Detta med anledning av att hoten mot organisationens informationsbärande system är alltför stora och att risken med en koppling mot Internet anses som större än den nytta det skulle kunna innebära. Trafiken som initieras från insidan av en brandvägg lämnar en länk öppen in, och detta är ett faktum som gör att okänd kod kan komma in i en organisation även om man har antivirusprogram på insidan. Mycket kommer att vila på hur brandväggen mot Internet är konfigurerad, om det överhuvudtaget finns någon (se avsnitt 8.22).

Om en organisation har en koppling mot Internet är det en källa till risker att få in skadlig kod i organisationens datorer, och då främst på klientsidan. Kommer loggutdragen från en organisation som har en koppling mot Internet måste man vara medveten om att detta kan vara en faktor som man måste ta med när man skall bedöma logganalysens värde.

10.9.4.7 Kontoutelåsning

Ett minikrav man enligt författarna bör ställa när det gäller autenticering genom lösenord är att det inte skall vara möjligt att upprepa hur många felaktiga inloggningsförsök som helst. Efter ett antal, t.ex. tre till fem, misslyckade inloggningsförsök skall kontot låsas, för att därefter inte gå att öppna förrän kontoinnehavaren kontaktar en administratör som kan öppna kontot.

Frånvaron av kontoutelåsning gör det möjligt att köra program som genom ”Brute force” attack testar alla möjliga kombinationer av tecken i syfte att till slut finna rätt lösenord. Detta leder till att ett lösenord inte stoppar en angripare, utan på sin höjd orsakar en fördröjning.

Om det saknas skydd mot felaktiga inloggningsförsök ökar det enligt författarna sannolikheten att en angripare kan bereda sig tillträde till ett system genom en annan persons användarkonto. Långa och svåra lösenord tar längre tid att knäcka eller lista ut så länge de inte följer enkla mönster på tangentbordet, men är samtidigt svårare för människan att komma ihåg. Av den anledningen tenderar de flesta av oss att välja lätta lösenord (se avsnitt 8.20).

10.9.4.8 Undersökning av hårdvara

Tekniker med stor insikt i informationsteknologin ser inte loggen i sig som ett bevis utan mer som en pekare på att någonting har hänt [Keyzer, Richardsson]. Kan en logg däremot styrkas av andra loggar kan denna kedja byggas starkare [Söderholm & Olsson].

En teknisk undersökning av användarens hårddisk innebär att loggarna måste kunna visa från vilken IP-adress eller MAC-adress som trafiken initierats. Genom att undersöka klientens hårddisk är det möjligt att finna spår av information som styrker loggarna.

Att flera användare delar på en klient är naturligtvis något som kan ställa till det i detta fall, men genom att finna spår som styrker loggarna hamnar man i ett bättre läge eftersom den egentliga bevisningen därmed fysiskt ligger på hårddisken och till vissa delar kommer att kunna återskapas.

10.9.4.9 Systemanrop

Av egna erfarenheter kan författarna referera till att en del organisationer i dag i allt större utsträckning övergår till något som på serversidan kallas för tjänster. Det innebär att användaren autenticerar sig för ett system men att systemet i sig sedan kommunicerar med ett eller flera underliggande system. Detta märker inte användaren, men lösningen påverkar valet av loggning. Om loggningen av aktiviteterna sker i mottagarsystemet och samtliga underliggande system måste det finnas någon parameter som skickas med anropen som gör att loggarna kan kopplas samman. Saknas detta finns endast tidstämpeln kvar, vilket med all sannolikhet inte kommer att räcka för att påvisa ett en logg i ett underliggande tjänstesystem hör samman med en logg i det anropande systemet.

Tjänsteanropen mellan det målsystem som användaren interagerar med och mellan målsystem och underliggande tjänstesystem innebär att tjänstesystemen bara ser att det är målsystemet som anropa och begärt en viss tjänst. Här kan man välja att låta användarens ID (t.ex. personnummer) följa med och loggas i underliggande tjänstesystem, men man kan även skicka med andra data som transaktions-ID. Loggas användarens ID i målsystemet kan detta hämtas från målsystemets loggar. Skapar sedan målsystemet ett transaktions-ID och detta skickas med i samband med tjänsteanropen skapar detta en möjlighet att identifiera ett helt transaktionsled. En användaraktivitet kan därmed skiljas mellan andra aktiviteter som samma användare genererat i samma system.

10.10 Genomgångna domar

Vid en analys av tabellen i bilaga F så går det att konstatera att det inte är särskilt vanligt att misstänkta bestrider de loggutdrag som presenteras som bevis. Detta skulle kunna förklaras med att många av de inblandade är polisman samt att alla på något sätt är anställda inom polisväsendet. Det kan därför finnas en högre vilja att samarbeta med utredarna än vad som t.ex. skulle vara fallet vid fall utanför organisationen.

Bland de få som bestrider att loggarna visar vad som hänt är den vanligaste förklaringen att det förvisso är den misstänktes användare som finns i loggutdragen men att det inte är han/hon som har gjort slagningen. I stället är det någon annan som utfört slagningen samtidigt som den riktige användaren fortfarande varit inloggad. Inget av de fall där någon förnekat sin skuld har tagit upp möjligheten till att det skulle kunna vara ett tekniskt fel som ligger bakom loggutdraget eller att trafiken genererats i den misstänktes konto genom svagheter i autenticeringen eller av administratörer i systemet. Detta styrks även av samtliga intervjuer som genomförts inom rättsväsendet. Förklaringen till detta torde stå att finna i att man inte ifrågasätter tekniken eftersom man inte känner till den. Det kan helt enkelt vara så att dessa personer utgår från att tekniken alltid gör ”rätt” och därmed skyller misstankarna på en annan person.

Sammantaget kan man konstatera att det är svårt att dra några långtgående slutsatser av en analys av dessa tre rättsfall. Det som är intressant är dock att rätten endast verkar ha tagit hänsyn till problematiken med att en okänd person skulle ha använt sig av en användare om den misstänkte tagit upp denna möjlighet under utredningen.

I annat fall verkar rätten utgå ifrån att det är den misstänkte som gjort ”slagningarna” precis som loggutdragen visar. Detta problem är även något som bekräftas av kriminalkommissarie Bergnér [Bergnér]. som menar på att de flesta fall där andra kan ha gjort de aktuella ”slagningarna” på grund av vissa omständigheter ofta skrivs av eftersom det ej går att styrka att den misstänkte verkligen har gjort de aktuella slagningarna. Det bör emellertid påpekas att de personer som ”slagningarna” gällt oftast har kunnat sammankopplas med den misstänktes bekantskapskrets vilket förhöjt bevisvärdet.

I de fall som ovan gåtts igenom är det två viktiga punkter som återkommer som bakomliggande faktorer vad det gäller att förklara varför problem uppstod. Genom att försöka komma tillrätta med dessa två punkter är det vår mening att många av de ovan beskrivna interna dataintrången inte skulle ha inträffat, eller åtminstone avsevärt försvårats, om nedanstående punkter beaktats. De två identifierade faktorerna är val av autenticering samt oklart internt regelverk.

- **För svag autenticering**

  På grund av alltför svag autenticering har det i vissa fall inte gått att bevisa vem som ligger bakom den aktuella trafiken. Kravet med att kunna bevisa att en specifik person utfört en specifik åtgärd ligger i och för sig extremt högt men önskvärt är ändå en autenticeringsmetod som motsvarar kravet på stark autenticering. I många av de beskrivna fallen har PIN-kod samt smarta kort använts, vilket är att betrakta som stark autenticering. Dock gäller det att inte enbart stirra sig blind på detta och invagga sig själv i falsk säkerhet eftersom problemet ofta inte ligger i graden av säkerhet hos kortet utan istället hur det används. Ett kort som lämnas kvar i kortläsaren innebär en ”single sign on” funktion som ger access till samtliga system som autenticerar användaren via kortet. Den legala användaren låser upp den skyddade delen av det smarta kortet med sin PIN-kod. När det väl är gjort är denna funktion åtkomlig om kortet lämnas kvar i kortläsaren.

  Om man har ett system med allt för svag autenticering spelar det ingen roll hur mycket teknik och resurser en organisation lägger ner på att skydda sina loggar. Kan man inte lita på att det är N.N som ligger bakom den trafik som loggarna visar spelar det ingen roll hur mycket arbete som lagts ned på att garantera att loggarna är korrekta. Tilltron till dessa kommer att stå i proportion till den autenticeringsmetod som används för att accessa målsystemen [Söderholm & Olsson].

  I dag tar man inte hänsyn till hur autenticeringen gått till när man läser ett loggutdrag. Det är någonting som man över huvud taget inte reflekterar över [Keyzer, Durling]. Av den anledningen överväger man inte ens möjligheten att trafiken som visas av loggarna kan ha genererats av någon annan än den som loggutdraget pekar ut. Den mest simpla förklaring som skulle kunna vara förklaringen till ett loggutdrag övervägs inte, nämligen att det är någon annan än den misstänkte som loggat in i systemet med dennes användarnamn och lösenord.

  Problem uppstår ofta när personal lämnar sin arbetsplats utan att logga ut. Det viktiga med detta problem är det kan uppstå såväl när autenticeringen är svag som stark. Därför gäller det att lägga till teknik/rutiner som gör det smarta kortet ännu säkrare vad gällande dess användande och som minskar risken för att användaren lämnar sin arbetsplats inloggad. Förslag på tänkbara[76] lösningar på problemet skulle kunna vara följande:

[76] Förslagen är allmänt kända och därför endast tänkbara förslag på hur problemet kan lösas.

○ ***Fysisk förbindelse mellan person och smart kort***
Genom att använda sig av något sorts band eller länk mellan person och det smarta kort så påminns personen om kortet när denne vill lämna arbetsplatsen. Dras kortet ut skall klienten omedelbart låsas.

○ ***Smart kort sammanfogas med passersystemet***
Genom att sammanfoga det smarta kortet med eventuellt inpasseringssystem så måste det smarta kortet tas med vid rörelser i en byggnad. Dras kortet ut skall klienten omedelbart låsas.

○ ***Trådlös förbindelse mellan kortläsare och dator***
Trådlös förbindelse finns mellan det smarta kortet och datorn. Fördelen är att användaren slipper lämna ifrån sig kortet utan kan ha den fäst i klädseln. När personen lämnar arbetsplatsen och kommer längre än t.ex. tre meter från arbetsstationen så låses klienten.

Ovanstående tänkbara förslag måste ställas mot å ena sidan det irritationsmoment som kan uppstå ifall användaren tvingas logga in ofta mot värdet på den information som skall skyddas. En balans mellan dessa två poler måste hittas för den aktuella situationen.

- **Oklart internt regelverk**

Nästa problem som identifierats är att det i många fall varit oklara interna regler för vad personalen får och inte får göra. Detta gäller såväl inom polisen som inom sjukvården i och med att det ofta varit klart vilken behörighet en person har men oklart om befogenheten. Ett regelverk måste därför styra upp detta och även klargöra vilka arbetsuppgifter varje individ har. Vidare bör det även ställas högre krav på att ha ansvar för sitt personliga smarta kort. Att lämna sin klient påloggad och därigenom möjliggöra för tredje part att ta del av känslig information borde kunna jämställas med tjänstefel. Problemet har särskilt uppmärksammats inom polisen [Bergnér] i samband med åtal kring personer som misstänkts för dataintrång i och med att de olovligen sökt i polisens register. En stor del av dessa utredningar har kretsat kring huruvida aktuella ”slagningar” varit en del av tilldelade arbetsuppgifter eller inte i och med att regelvärdet varit tvetydigt på den punkten.

10.11 Balanserad säkerhetsnivå

När vi bedömt vilka områden vi valt att belysa i uppsatsen har vi varit medvetna om att det finns ett förhållande mellan säkerhet och kostnad. För höga krav på säkerhet innebär att man kanske inte har råd att implementera de förbättringar som de nya kraven innebär. Det kan i sin tur leda till att säkerheten inte höjs överhuvudtaget eftersom man inte har råd att implementera dem. Av den anledningen kan för höga krav leda till att man står kvar på samma låga nivå som tidigare.

Hoten som finns mot de data som transporteras och hanteras i ett nätverk är dock så pass välkända att det tagits fram standarder som hjälp för de administratörer som har till uppgift att hantera dessa problem. Något man därutöver inte får glömma är att vi i våra allmänna domstolar tillämpas någonting som heter fri bevisprövning. Det innebär bland annat att den bevisning som parterna vill använda sig av bedöms i ett sammanhang.

Av den anledningen får man inte fokusera allt för mycket på enskilda detaljer som t.ex. teknik. Den miljö där loggarna transporterats och lagrats i blir med detta resonemang bara en del av helheten som måste bedömas.

Frågan om vad som är rätt nivå av säkerhet är något som vi i denna uppsats valt att inte värdera eftersom vi inte ger några rekommendationer till hur den tekniska och administrativa miljön skall se ut. De enda som kan värdera denna fråga är våra allmänna domstolar genom de domar som förkunnas i samband med IT-relaterade huvudförhandlingar. En fällande dom där den misstänkte förnekat innebär av allt att döma att informationssäkerheten varit av en sådan kvalité att loggutdraget gått att lita på. Å andra sidan är det ingen garanti då det mycket väl kan vara på så sätt att ingen av parterna haft kunskap att rätt ifrågasätta loggutdragets bevisvärde.

10.12 Muntlig bevisning

Samtliga människor som är inblandade i händelsekedjan från en loggs födelse till presentation kan kallas in att vittna i en domstol. Dessa kan därmed under ed redogöra för vilka åtgärder de vidtagit i samband med sitt ansvarsområde. Tveksamheter kan därmed redas ut genom att man direkt kan ställa frågor till inblandade personer. Detta kräver antingen att parterna i domstolen har förmåga att förstå den teknik som är inblandad och därmed kunna påkalla förhör med dessa personer under förundersökningen eller att analysdelen tagit fram sådan information om organisationens tekniska och administrativa miljö att det redan här framgår vilka personer som gjort vad.

Överträdelser i systemen som t.ex. bygger på för svag autenticering kommer knappast att kunna klarläggas i en domstol om inte direkta misstankar finns mot någon som är ansvarig för något sådant. Däremot kan teknikansvariga kallas in som vittne för att under ed besvara frågor som t.ex. berör säkerhet och administrativa lösningar.

11. Slutsats

I detta kapitel presenterar vi de slutsatser som gjorts av analysen kring arbetets insamlade material. Vi börjar med att repetera den utgångspunkt som vi ställde upp vid arbetets början för att därigenom underlätta för läsaren att se vad vi vill få fram med uppsatsen:

Problem
Hur värderar de rättsvårdande instanserna en organisations loggutdrag?

Syfte
Syftet med uppsatsen är att väcka debatt och aktualisera det faktum att de rättsvårdande instanserna idag saknar grundläggande kunskap om modern IT-teknologi, samt saknar relevant kunskap om de loggenererande organisationernas tekniska och administrativa miljö, för att kunna göra en bevisvärdering av organisationernas loggutdrag.

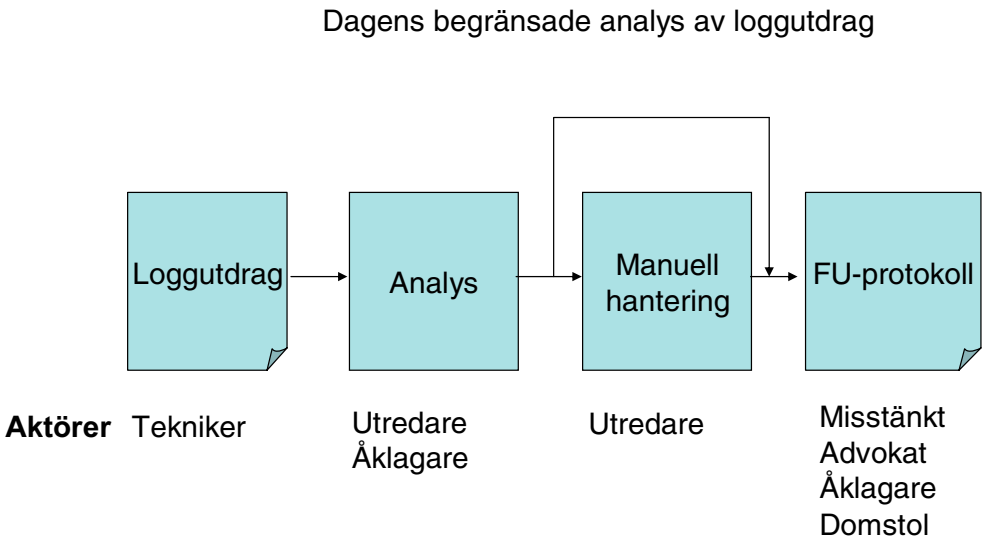
Mål
Målet med uppsatsen är att ta fram riktlinjer som gör det möjligt att bättre kunna värdera sanningsinnehållet i en organisations loggutdrag och därmed på ett säkrare sätt kunna värdera loggutdragets bevisvärde.

När det gäller dagens logganalyser har vi kommit fram till att dessa uteslutande grundar sig på loggutdraget. Loggutdraget utgör i dag det enda underlaget till analysfasen. I dag litar man på att ett loggutdrag som skickas till polisen är korrekt till sitt sanningsinnehåll utan någon som helst kontroll. Detta sker utan att man känner till vem som gjort utdraget, hur det gått till och hur den tekniska och administrativa miljö ser ut hos organisationen som levererat loggutdraget. Vår uppfattning är att i nuvarande situation sker logganalysen på alltför lösa grunder eftersom det enligt oss kräver en ganska djup förståelse av organisationens tekniska och administrativa miljö för att kunna göra en rätt avvägd bedömning av ett loggutdrags bevisvärde.

Denna uppsats visar på en mängd olika hot mot riktigheten av data som transporteras och lagras i ett nätverk. Den beskriver även att riktighet inte är samma sak som sanningsinnehåll, och att riktighet är en delmängd av sanningsinnehållet. Avsaknaden av ifrågasättande av loggutdragen beror dock inte på annat än okunskap eftersom uppsatsen visat att ingen av de rättsvårdande instanserna i dag besitter den kunskap som krävs för att förstå hur ett loggutdrag kan ifrågasättas.

I figur 27 illustreras hur dagens logganalys är uppbyggd. Det verkar inte finnas någon genomtänkt metod för hur loggutdraget skall hanteras, utan all värdering och hantering utgår från att all data i loggutdraget är korrekt. På så sätt är loggutdragets värde redan fastställt när det kommer till polisens utredare. Analysen utgår även endast ifrån den information som loggutdraget är bärare av och all tolkning sker endast ifrån denna information. I dagens information är det även oklart vem det är som skall göra den vederbörliga analysen. Alla steg i kedjan litar på att föregående steg i kedjan gjort en kontroll av loggutdragets sak- och sanningsinnehåll. Samma data som analysen tar emot är det som skickas vidare till nästa steg. En felaktighet som genereras av den organisation som skapar loggutdragen får med andra ord fullt genomslag.

I och med detta är det även tveksamt om det egentligen genomförs någon logganalys i egentlig mening eftersom den information som idag dras ur loggutdraget är vad dess olika kolumner och tecken betyder.



Figur 27 Dagens begränsade logganalys som endast utgår från loggutdraget

I dag är frånvaron av ifrågasatta loggutdrag inget större problem. De informanter som intervjuats säger att de aldrig varit med om att riktigheten i ett loggutdrag ifrågasatts. Detta kan indikera att riktigheten hos loggutdragen av allt att döma är korrekt. Dock kommer det att innebära stora förändringar av hur ärenden som bygger på IT-relaterad bevisning går till den dag den misstänkte, av någon anledning, börjar ifrågasätta riktigheten i loggutdragen. Risken är då stor att varken åklagare eller advokat vet hur de skall försvara/ifrågasätta riktigheten av loggutdraget. Det kommer vidare att leda till behov av sakkunnig personal. Diskussion som kommer att föras i rättssalen riskerar då att ligga på en sådan teknisk nivå att varken domare, nämndemän, åklagare eller advokat kommer att fullt ut förstå resonemanget. Ett ifrågasättande kan även bli ytterst resurskrävande eftersom en grundlig undersökning av ett system hos en organisation som genererat ett loggutdrag inte är en statisk rapport utan kommer mycket snart att bli inaktuell. Om ett loggutdrag ifrågasätts är en sådan kontroll nödvändig. Detta kommer att ske i syfte att försöka utreda om den inställning som den misstänkte framför kan motbevisas eller inte. Undersökningen kommer att ligga till grund för åtalsfrågan i aktuell utredning, men kan inte med automatik åberopas nästa gång ett liknande behov uppstår med anledning av den förändring som organisationen kan ha genomlevt.

Eftersom ingen ifrågasätter loggutdragen har inte loggutdragens bevisvärde prövats i någon egentlig mening. När användaren idag nekar till en slagning så görs det primärt med motiveringen att trafiken måste ha utförts av någon annan. Fokus förflyttas då till vilken annan användare som kan ha utfört slagningen istället för om loggutdraget egentligen har något bevisvärde. Det är dock tveksamt om åklagaren skulle kunna väcka åtal med enbart loggutdraget och dess innehåll som underlag. Detta med anledning av att ett loggutdrag aldrig ensamt kan peka ut den fysiska personen som gjort slagningen då logganalysen endast talar om att ett IT-system använts på ett visst sätt.

Eftersom alla stegen i rättskedjan skjuter ansvaret för att säkerställa att loggutdragen är korrekta av föregående steg i kedjan så blir den misstänktes inställning i sakfrågan av yttersta vikt. En närmare kontroll av loggutdragen kommer endast att ske på den misstänktes begäran. Ifrågasätts eller förstås den ej av den misstänkte eller dennes försvarare kommer loggutdraget att tillmätas ett bevisvärde mot den misstänkte. Den misstänktes inställning blir därför helt avgörande för vilken kontroll som skall ske och det blir därmed även svårt att i förväg täcka alla sätt ett loggutdrag kan ifrågasättas på.

Vidare är dataintrång ett så kallat bötesbrott vilket innebär det att den misstänkte som regel inte tilldelas en offentlig försvarare. Denne måste därmed många gånger själv stå för sitt försvar. Ensam utan försvarare är man i ännu större behov av att aktörerna för de rättsvårdande instanserna tar fram ett material som är korrekt. Någon garanti för att så är fallet finns knappast i dag eftersom ingen aktiv kontroll sker. Att påföljden för brottet dataintrång som regel inte ger mer än böter innebär att vissa regler om åtalsunderlåtelse kan bli aktuella om det visar sig att kostnaderna för att göra en djupare kontroll av ett informationssystem kommer att anses som oskäligt höga i förhållande till brottets påföljd.

En av de viktigaste orsakerna till att folk som åtalats för dataintrång idag frikänns i en domstol är att det, trots valet av autenticering, finns en möjlighet för någon annan att ligga bakom trafiken som loggats. Slutsatsen grundar sig på analysen av de domar som författarna tagit del av, och som redovisas som en bilaga i uppsatsen (se bilaga VII). Antingen har autenticeringen varit för svag, bara lösenord som gått att knäcka eller som gått att tjuvtitta sig till, eller så har den misstänktes förklaring inte gått att motbevisa eller gått att lämna utan avseende. Detta räcker för att författarna skall kunna dra slutsatsen autenticering som enbart bygger på en gemensam hemlighet mellan användare och system (lösenord) inte är tillräckligt om den misstänkte nekar till att själv ligga bakom den loggade trafiken.

En annan viktig faktor till frikännande är även brister i aktuell organisations interna regelverk. Brottet dataintrång (BrB 4 kap, 9 §) talar om fall där någon olovligen bereder sig tillgång till upptagning för automatisk databehandling. Lagen i sig ger inget stöd för vad som är tillåtet eller inte, utan detta måste reglerar av interna begränsningar hos respektive organisation. Om dessa saknas, eller är ”luddigt” skrivna kommer det att vara svårt för en åklagare att göra gällande att en viss aktivitet från användarens sida är att betrakta som dataintrång. En organisation bör därför ha ett skriftligt fastställt regelverk som klargör var gränsen går för användarnas befogenhet i organisationens system.

Vårt arbete har påvisat en mängd möjligheter att manipulera innehållet i en logg. Med detta i baktanke är det viktigt att ett helhetsperspektiv används när det gäller att säkra upp en organisations logghantering. Loggutdragets bevisvärde kommer i slutändan inte vara starkare än loggningskjedjans svagaste länk. Mängden möjligheter till att manipulera innehållet påvisar att en logg inte automatiskt bör betraktas som korrekt. Det är författarnas åsikt att många organisationer idag förmodligen enbart litar på att deras autentisering skall kunna binda en person till en specifikt användande. De efterkommande stegen glöms bort och innebär ett potentiellt riskmoment i en eventuell framtida rättegång.

När en organisation säkrar sin logghantering måste ett helhetsperspektiv användas. Det kommer inte att räcka med en lösenordsinloggning för att kunna åberopa ett loggutdrag som bevisning när den misstänkte nekar, utan det krävs av allt att döma en förstärkt inloggning för att efterkommande led skall kunna tillmätas full betydelse.

Loggen måste därutöver ges ett integritetsskydd under transport och lagring för att kunna svara mot beskyllningar om att dessa förändrats under transport och lagring. Man får inte glömma bort de rättsvårdande instansernas grundläggande värderingar av loggutdragen. De förutsätter att dessa är korrekta, vilket med författarnas ord innebär att de förutsätter att dessa är sanna till sitt sak- och sanningsinnehåll. I brist på förmåga att ifrågasätta loggutdragen säger man att man litar på dem. Hela ansvaret för att så är fallet skjuts därmed på den som levererat loggutdraget till den om gör detta uttalande. Åklagaren syftar på polisen och polisen syftar på den organisation som levererat loggutdragen.

Systemen måste vidare anpassas så att organisationen kan visa att man gjort vad man kan för att minimera administratörernas möjligheter att påverka systemen så att risken för hot från elaksinnade administratörer blir så liten som möjligt. Den manuella hanteringen av loggarna bör dessutom kompletteras med en manuell logg så att man i efterhand kan klargöra vem som haft ansvar för informationen under vilka tidpunkter och vem som gjort vad med informationen vid bearbetning som t.ex. förenkling i form att ta bort sådana data som inte behövs.

För att till en del kompensera bristerna med endast lösenordsinloggning kan mer data än endast IP-adressen hämtas in från klienten. För att kunna logga MAC-adressen måste man byggas in stöd för detta högre upp i protokollstacken eftersom Ethernets pakethuvud bara innehåller MAC-adressen från föregående nod. Om paketen routats längs vägen kommer MAC-adressen i Ethernets pakethuvud att innehålla den senaste routerns MAC-adress och inte avsändarens. Tunna klienter som får sin kod i form av HTML-formaterad text från servern har inte stöd för att läsa av MAC-adressen på klienten. Feta klienter som byggs i syfte att utnyttja processorkraft på klienten kan dock skrivas så att MAC-adressen kan skickas med vid anrop till servern. En logg som kan styrkas av en annan logg kan bygga upp en beviskedja som gör att loggutdragets bevisvärde därmed stärks. Logganalytikern som analyserar loggar som innehåller IP-adress, MAC-adress och datornamn måste vara medveten om att dessa värden som regel går att förändra på klientsidan. Därmed riskerar loggutdragen att peka ut fel dator som ansvarig för den trafik som loggarna avser, vilket innebär att loggutdragens sanningsinnehåll är falskt.

Dagens möjligheter att boota om en dator med hjälp av ett annat operativsystem innebär att det är lätt att installera okänd programvara eller att påverka säkerhetskritiska inställningar på klienten. De innebär att det i dag är ännu svårare än tidigare att bygga upp en miljö med en säker klient. Av den anledningen bör säkerheten kring känslig information säkerställas i de målsystem som klienten kan anropa. Av samma anledning är kravet på en förstärkt inloggning något som blir än mer aktuellt eftersom lösenord lätt kan avslöjas om dold programvara installeras på klienten.

11.1 Problem- syfte och måluppfyllnad

Nedan följer kort författarnas bedömning över hur uppsatsens problemområde, syfte och mål uppnåtts.

Problem
Hur värderar de rättsvårdande instanserna en organisations loggutdrag?

Genom intervjuerna med informanterna inom de rättsvårdande instanserna har det framkommit att man saknar kunskap för att kunna ifrågasätta loggutdragen, och då i huvudsak deras sanningsinnehåll. Samtliga inblandade aktörer i den rättsliga kedjan litar på att loggarnas sanningsinnehåll är sant när de mottar loggarna och förlitar sig helt och hållet till den misstänktes inställning när de gör sina värderingar av loggutdraget. De rättsvårdande instanserna, men undantag av de få som har kunskap om modern IT-teknologi, värderar loggutdragen utifrån ansatsen att dessa är sanna både till sitt sak- och sanningsinnehåll utan någon som helst kontroll.

Syfte
Syftet med uppsatsen är att väcka debatt och aktualisera det faktum att de rättsvårdande instanserna idag saknar grundläggande kunskap om modern IT-teknologi, samt saknar relevant kunskap om de loggenererande organisationernas tekniska och administrativa miljö, för att kunna göra en bevisvärdering av organisationernas loggutdrag.

Genom intervjuerna med informanterna i denna uppsats har denna process redan startats. Uppsatsens eventuella spridning och aktuella område bör leda till att processen fortsätter inom informanternas led sedan uppsatsen distribuerats till dessa. Författarna hoppas att syftet kan leda till att man i framtiden ställer större krav på både autenticering och de efterkommande leden genom ett utökat ifrågasättande av loggutdragens sak- och sanningsinnehåll. Dess sanningsinnehåll kan till stor del ifrågasättas genom författarnas förslag till ett utökat loggutdrag. Kopplingen till spårbarhet som ett hett ämne inom området informationssäkerhet bör leda till att även syftet kan uppnås.

Mål
Målet med uppsatsen är att ta fram riktlinjer som gör det möjligt att bättre kunna värdera sanningsinnehållet i en organisations loggutdrag och därmed på ett säkrare sätt kunna värdera loggutdragets bevisvärde.

Avsnitt 12 redovisar författarnas förslag till morgondagens logganalys. Där tar man i fortsättningen betydligt större hänsyn till den tekniska och administrativa miljön hos den organisation som levererar loggutdragen. Modellen kan byggas ut med ytterligare sakområden och gör inget anspråk på att vara heltäckande, men det är författarnas övertygelse att modellen innebär att även uppsatsens mål är uppnått.

Avslutningsvis vill vi poängtera att det kan vara lätt att missförstå våra slutsatser och tro att vi förkunnar ett tänkande där alla tänkbara tekniska och juridiska ”hål” till 100 procent måste täppas till för att rättssäkerhet skall uppnås. Detta skulle förmodligen bli både omotiverat dyrt och administrativt krångligt. Därför är det viktigt att ha en förståelse för att rätten idag dömer på en helhetsbild av det som framkommit under huvudförhandlingen. Det innebär att argument som motiv m.m. är någonting som man tar hänsyn till.

Det faktum att det finns en relation mellan den misstänkte och den som loggen omfattar är ett försvårande faktum som bland annat motiverar en fällande dom. Detta är anledningen till att ett loggutdrag och ett analysresultat inte skall bedömas som enskilda punkter, utan ses som en del av förundersökningsprotokollet. Det är precis på detta sätt som författarnas rekommendationer till morgondagens logganalyser skall gå till.

Genom att fokusera på helheten, där organisationen som levererar loggutdraget redovisar sin tekniska och administrativa miljö, på ett sått som redovisas i kapitel 12, kan åklagaren ges en rimlig möjlighet att bevisvärdera loggutdraget. En teknisk diskussion till gränsen till absurdum kommer därför aldrig bli aktuell. Syftet med vår uppsats är istället att bidra till en medvetenhet kring problematiken med loggar som bevis och vi överlåter till respektive organisation att välja en säkerhetsnivå som svarar mot organisationens verksamhet och loggningens syften.

12. Förslag till ny logganalys

I den teoretiska referensramen diskuterade vi begrepp som informationssäkerhet och kvalitet. Dessa begrepp är väsentliga eftersom det krävs att en organisation har en hög nivå av informationssäkerhet för att kunna leverera ett loggutdrag som har ett högt bevisvärde. I den teoretiska referensramen om förundersökning skrev vi om syftet med förundersökningen. Ett av dess syften är att utreda om tillräckliga skäl för åtal föreligger mot den som är skäligen misstänkt för brottet. Vi kommer därför in på frågan om vem som skall göra logganalysen. Är det organisationen som levererar loggutdragen eller är det polisen?

12.1 Vem skall göra analysen?

Det är uppenbart att det är polisens utredningspersonal som ansvarar för logganalysen. Det framkommer inte minst i Rättegångsbalkens 23:e kapitel, som bland annat anger syftet med förundersökningen. Att lämna ansvaret för analysarbetet till den organisation som levererar loggutdragen kommer att strida mot kravet på en opartisk hantering av förundersökningen eftersom logganalysen i sådana fall kommer att genereras av den som är part i utredningen. (Se begreppet objektivitetsprincipen i den teoretiska referensramen om förundersökning). Logganalysen syftar till att samla in ytterligare data om organisationens tekniska och administrativa miljö. Ur dessa data skall det vara möjligt att utläsa sådan information att det tillsammans med övriga omständigheter som framkommit under utredningen går att göra en bedömning av loggutdragets bevisvärde. Därmed blir det möjligt att göra en bedömning av loggutdragets egentliga sanningsinnehåll.

12.2 Ny princip för analysen

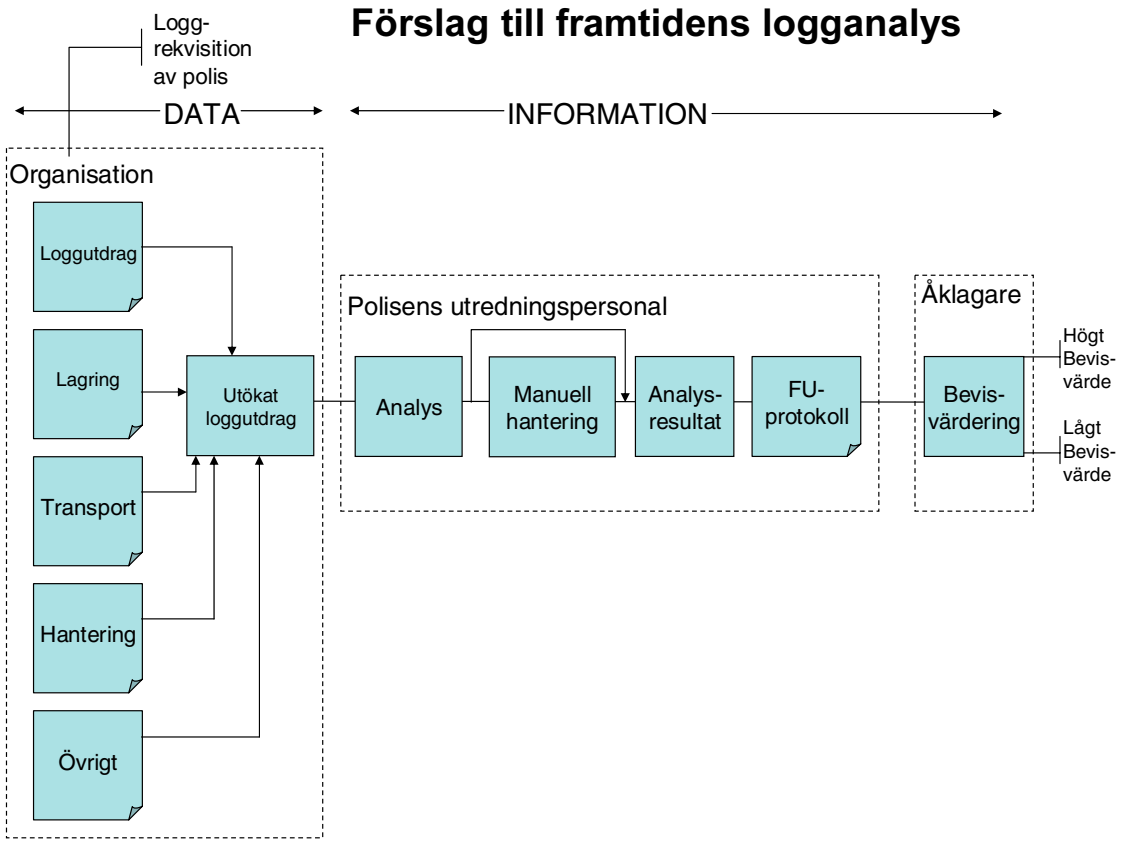
De flesta loggutdrag som kommer till polisens utredare är ett resultat av en begäran från polisen. Det vi föreslår i framtidens logganalys är att denna kompletteras med en lista med motsvarande innehåll vi diskuterade under kapitlet 10.10. Vår diskussion kan ses som ett grundkoncept för de data som logganalysen bör kompletteras med. Erfarenhet och specifik kunskap om organisationen som levererar loggutdraget kan medföra att ytterligare områden måste tas med.

Att vi i detta avsnitt återkommer till att det är polisen som skall stå för analysen beror på att ett loggutdrag så gott som alltid kommer att passera polisens utredningsavdelningar innan ett ärende når de allmänna domstolarna. Det är polisen som bereder ärendet innan det redovisas till åklagaren, och av den anledningen är det naturligt att tankarna bakom det utökade loggutdraget berör polisen.

Under analysen bör polisens utredare ta fram sådan information som gör att det blir möjligt att värdera loggutdraget. Vi kallar denna utökade mängd data för ett utökat loggutdrag. Med den nya arbetsmetoden utgör loggutdraget, och det som organisationen lämnar över som beskrivning av dess tekniska och administrativa miljö, som data (se figur 28). Denna datamängd, som beskrivs under rubrikerna loggutdrag, lagring, transport, hantering och övrigt, utgör input till logganalysen där dessa ges ett informationsvärde genom den mänskliga tolkning som kommer att ske. Informationens huvudsyfte under analysen är att beskriva organisationens tekniska och administrativa miljö.

Det utökade loggutdraget beskriver ingående organisationens aktuella tekniska informationssystem och dess administrativa och manuella lösningar. Analysresultatet blir en del av förundersökningen där bland annat den misstänktes inställning och övrig bevisning finns med. Tillsammans utgör analysresultatet och förundersökningen det material som åklagaren kan bygga sin bevisvärdering på. Det denne skall värdera är bevisvärdet av loggutdraget. Logganalysens resultat ger med detta arbetssätt en möjlighet för åklagaren att värdera loggutdragets bevisvärde eftersom det nu finns en mängd information att värdera tillsammans med loggutdraget. Detta har hittills inte varit möjligt eftersom någon kritisk granskning av loggutdragen inte görs och någon information om organisationens miljö inte efterfrågats.
Skulle en organisation vägra att svara på vissa frågor som utredarna ställer för att kunna genomföra sin logganalys kommer detta onekligen att påverka analysresultatet. Vissa områden kommer då inte att kunna värderas. När ett sådant brisfälligt analysresultat förs in i förundersökningsprotokollet, där övrig bevisning finns, kommer det ändå att vara en grund för åklagarens bevisvärdering. Mycket talar dock för att loggutdraget genom detta får ett lägre bevisvärde eftersom delar av organisationens miljö inte kunnat utredas.

Man får inte glömma bort att det som regel finns goda möjligheter att finna spår av den trafik som loggats på den hårddisk som använts vid interaktionen mellan klient och server. Finns möjlighet att undersöka hårddisken ses detta enigt Roswall [Roswall] och Keyzer [Keyzer] som det egentliga beviset medan loggarna mer eller mindre fungerar som en indikation över vad som skett.



Figur 28 Morgondagens logganalys ser endast loggutdraget och övrig information från den organisation som levererat loggutdraget som data.

12.3 Exempel på ett loggutdrag och analysresultat

Exemplet i detta avsnitt skall jämföras med de förhållanden som råder idag. Analysresultatet av ett utökat loggutdrag skiljer sig avsevärt från resultatet av dagens analys som endast grundar sig på innehållet i loggutdraget. Ett loggutdrag som med automatik förutsätts vara korrekt till sitt sak- och sanningsinnehåll kommer att ges ett helt annat värde efter den utökade loggutdraget enligt exemplet nedan.

Antag att man ur loggutdraget kan utläsa att användare A loggade in i organisationens lönesystem den 12 januari 2004 klockan 14.24.43 och där tog del av löneuppgifter tillhörande anställd C. Användare A ändrade grundlönen för anställd C från 27.400 kronor per månad till 32.000 kronor per månad. Klockan 14.33.52 loggade användare A ut från aktuellt system.

Ett loggutdrag som enbart värderas utefter sitt textinnehåll innebär att man utgår från att loggutdragets sanningsinnehåll är sant. Visserligen är detta något som kommer att påverkas av den misstänktes berättelse, men om man leker med tanken att denne säger sig inte minnas aktuell slagning och därmed inte kan svara på frågan om denne erkänner eller förnekar brott.

Om utredarna eller analytikerna i stället angriper loggutdraget utifrån det författarna lyfter fram som ett utökat loggutdrag är det författarnas övertygelse om att åklagaren därmed kommer att ges ett betydligt bättre underlag att värdera loggutdraget jämfört med det sätt som man ser på dem idag.

För att förtydliga skillnaderna mellan dagens synsätt och författarnas modell ges följande exempel på vad den utökade loggkontrollen kan generera för analysresultat.

Det aktuella systemet är ett lösenordsbaserat system där användare A sitter i ett kontorslandskap tillsammans med sju kollegor. Placering av skärm och tangentbord gör att det är teoretiskt möjligt att se inloggningsdata när en användare loggar in i systemet genom att skärmarna är vända mot både besökare och arbetskamrater. Den tekniska analysen av nätverket har fastställt att användare A tjänstgör i ett hubbat subnät med en DHCP. Organisationen saknar skydd mot inkoppling av ny utrustning i nätverket, vilket innebär att vem som helst kan koppla in en dator i nätverket och automatiskt erhålla en IP-adress och övrig nätverkskonfigurering. Organisationens DHCP saknar loggning varför det inte finns någon spårbarhet över vilken utrustning som DHCP:n utdelat IP-adresser till.

Det hubbade nätet gör att det var som helst i subnätet går att lyssna av trafiken mellan användare och målsystem. Trafiken i det system logganalysen avser går okrypterad i nätverket. Detta innebär att lösenordet som användaren skriver för att logga in i målsystemet skickas i klartext, vilket innebär att den som sniffar nätverket kan lyssna av lösenorder oavsett var någonstans i subnätet denne kopplar in sig.

Det finns 28 administratörer på den server som administrerar lönesystemet. Samtliga administratörer har fullständiga rättigheter till systemets samtliga funktioner. Loggarna lagras på samma maskin som applikationen vilket innebär att samtliga administratörer har tillträde till loggarna. Dessa lagras som vanliga textfiler, vilket innebär att det inte behövs något specialskrivet program för att läsa eller editera loggarna. Dessa kan editeras (ändras) av samtliga administratörer utan att det märks eftersom de lagras utan integritetsskydd.

En gång varje vecka skickas loggarna från servern till sitt slutliga lagringsmedium. Detta är en bandrobot. Loggarna lagras sedan tre år hos organisationen. Det saknas rutiner för att kontrollera att lagrade loggar är korrekta. Av den anledningen kan organisationen inte svara på frågan om samtliga loggar backats upp eller inte.

När en användare nekar till en slagning, med motiveringen att denne inte minns slagningen och/eller att trafiken måste ha utförts av någon annan, skjuts fokus till vilken annan användare det kan tänkas vara som utfört slagningen. Fokus läggs inte på om loggutdraget egentligen har något bevisvärde. Det kan till och med vara som så att det är en administratör som utfört förändringen i systemet och därefter skapat en falsk logg. Någon fokus på sådana aspekter finns inte när man utgår från att loggutdraget är korrekt.

Den åklagare som väcker åtal med detta utökade loggutdrag som bevisning kommer, enligt författarnas bedömning, att ha mycket liten chans att vinna målet när denna analys ligger med i förundersökningsprotokollet. Logganalysen har visat att det som loggutdraget påstår kan ifrågasättas på en mängd punkter. Dess sanningsinnehåll kan på en rad punkter ifrågasättas. Det som vi i detta exempel beskriver av organisationens system framgår inte om man bara, som i dag, tittar på loggutdragets sakinnehåll.

Det som kan vara till den misstänktes nackdel är den övriga bevisningen som kan förekomma. Detta är något man väger in även i dag. Av den anledningen bygger författarnas metod på att analysresultatet av det utökade loggutdraget ses som en del av förundersökningen. Det kan finnas en relation mellan den misstänkte och den som systemet visar att man ändrat lönen på och det kan förekomma vittnesförhör som visar att den misstänkte skrutit om sina bravader. I sådana fall är det annan bevisning som är det främsta underlaget för ett eventuellt åtal från åklagarens sida, men även om sådan bevisning finns kommer analysen att visa inom vilka områden loggutdraget kan angripas.

Om de förslag till ytterligare input i logganalysen som författarna lyfter fram i detta kapitel följs kommer den åklagare som till sist skall fatta beslut i åtalsfrågan med ledning av analysresultatet att ha ett betydligt bättre underlag för detta beslut än vad denne har i dag. I dagsläget tas ingen kringliggande information om organisationernas tekniska och administrativa miljö fram över huvud taget. Denna kringliggande information kommer att vara till hjälp i bedömningen om den berättelse som den misstänkte lämnar kan lämnas utan bifall, motbevisas eller måste beaktas. Ett ifrågasättande av loggutdragens riktighet kommer att tvinga fram krav på ytterligare information [Engfeldt, Roswall]. Detta skulle mycket väl kunna vara den typ av information som åklagarna efterlyser i sina intervjuer, utan att närmare ange vad det är för ytterligare information som de egentligen avser. Vår bedömning är att åklagarna inte har den kunskap som krävs för att definiera dessa områden. Denna uppsats kan därför ses som en hjälp att definiera dessa områden.

13. Avslutande kommentar

Avslutningsvis vill i återknyta till avsnitt 2.2 genom att föra en diskussion kring undersökningens reliabilitet och validitet samt vad våra slutsatser egentligen är värda. Som vi skrev i metodkapitlet så är en undersökning reliabel ifall dess empiri är tillförlitlig och trovärdig och densamme valid ifall det som man avsåg att mätas faktiskt har mätts. Frågan som då uppkommer är huruvida kvalitén på vår empiri når upp till dessa krav. Vi har genomgående under arbetet försökt att presentera vår empiri på ett så objektivt sätt som möjligt och hela tiden vägt för och emot. Utöver detta har stor vikt även lagts vid att följa god praxis vad gällande det forskningsmetodiska upplägget och därmed noga presentera de metodval som gjorts.

Vidare har vi till största delen valt ut informanter med en mycket god inblick i de problem som finns kring bevisvärdering av loggar. Det stora flertalet av informanterna arbetar med denna typ av frågor i sitt dagliga arbete vilket gör att sakkännedomen är mycket god. Kvalitén på intervjuerna i sig bedöms även de som goda. Inte minst innebär det faktum att en av författarna arbete inom polisen bidragit till att vi fått engagerade och uppriktiga svar på våra frågor. Något som läsaren kan sakna är dock avsaknaden av intervjuer med informanter från domstolarna. Det hade varit intressant att få med deras åsikter och erfarenheter som input i uppsatsen. En avgränsning fick dock göras eftersom uppsatsen redan utan sådan medverkan är omfattande. Vår bedömning är dock att deras medverkan endast skulle kunna påverka uppsatsens slutsatser marginellt.

Allt detta gör att reliabiliteten samt validiteten med stor sannolikhet kan betraktas som tillfredställande. Dock överlåter vi till läsarna att själva bedöma huruvida genomgånga slutsatser är befogade eller inte. Arbetet får dock betraktas som fruktsamt i och med att det genererat ett förslag på hur polisens logganalysarbete skulle kunna bedrivas i framtiden och därmed är det mål[77] som sattes upp i kapitel 1 uppfyllt. Vidare så anser vi även att arbetet givit svar på vår problemformulering[78] i och med att vi genom våra intervjuer klarlagt de olika informanternas syn på loggutdragets värde samt funktion.

[77] "*Målet med uppsatsen är att ta fram riktlinjer som gör det möjligt att bättre kunna värdera riktigheten och sanningsinnehållet i en organisations loggutdrag och därmed på ett säkrare sätt kunna fastställa loggutdragets bevisvärde*"

[78] "*Hur värderar de rättsvårdande instanserna en organisations loggutdrag och vad förväntar sig dessa instanser av organisationer som tar fram detta*"?

14. Källförteckning

14.1 Publicerade källor

[Alberts & Dorofee, 2003]
Alberts Christopher, Dorofee Audrey, *Managing Information Security Risks, The OCTAVE Approach*, Upper Saddle River, New Jersey, USA, 2003

[Allinson, 2004]
Allinson Caroline Linda, *"Legislative and Security Requirements of Audit Material for Evidentiary Purpose"*, Queensland university of Technology, April 2004

[Axelsson, 2004]
Axelsson Maria Gunther, "*Fysiker kläcker oknäckbara koder*", Dagens Nyheter, 11 april 2004

[Bring et al, 1995]
Bring Thomas, Diesen Christian, Klerhag Pia, Schelin Lena, Sederholm Eva Linda, "*Förundersökning*", Författarna och Juristförlaget JF AB, Stockholm, 1995

[Bott & Siechert, 2001]
Bott Ed, Siechert Carl, **"***Microsoft Windows XP - utan och innan"*,
Pagina, Stockholm , 2001

[Burd, 1998]
Burd Stephen D, "*Systems architecture"*, Cource Technology ITP, Canada, 1998

[Dyson, 1999]
Dyson Peter, *Dictionary of Networking*, SYBEX Inc, Alameda, USA

[Fitzgerald, 1999]
Fitzgerald Dennis, *Business Data Communications and Networking, sixth edition*, John Wiley & sons, Inc, USA, 1999

[Gollman, 1999]
Gollman Dieter, "*Computer Security*", John Wiley & sons Ltd, England, 1999

[Hedemalm, 2001]
Hedemalm Gunnar, "*Nätverk och kommunikation från grunden", 5:e upplagan*, Pagina förlag AB, Sundbyberg, 2001

[Hellevik, 1980]
Hellevik, O., "*Forskningsmetode i sosiologi og statsvitenskap*", Universitetsforlaget, Oslo, 1980. Svensk översättning: "Forskningsmetoder i sociologi och statsvetenskap", Natur och Kultur

[Holme & Solvang, 1997]
Holme, I.M., & Solvang, B.K., "*Forskningsmetodik – Om kvalitativa och kvantitativa metoder*", studentlitteratur, Lund, 1997

[H Säk IT, 1997]
Handbok för försvarsmaktens säkerhetsskyddstjänst Informationsteknologi, Försvarsmakten, andra tryckningen 1997.

[Jacobsen, 2002]
Jacobsen, D.I., ”*Vad, hur och varför? – Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*”, Studentlitteratur, Lund, 2002

[Krisberedskapsmyndigheten I, 2003]
Krisberedskapsmyndigheten, *IT-och sårbarhet*, KBM temaserie 2003:5, Stockholm

[Krisberedskapsmyndigheten II, 2003]
Krisberedskapsmyndigheten, ”*Basnivå för IT-Säkerhet (BITS)*”, KBM Rekommenderar 2003:2, Stockholm

[Kronqvist, 2003]
Kronqvist Stefan, ”*Brott och digitala bevis*”, Nordstedts juridik, Stockholm, 2003

[Leupold et al, 2004]
Leupold Ralf, Lindström Mathias, *Single Sign-On i webbtjänstmiljö*, Stockholms Universitet / Kungliga Tekniska Högskolan, 2004.

[McClure et al, 2003]
McClure Stuart, Scambray Joel, Kurtz George, ”*Hacking i fokus*”, 3:e utgåvan, Paginas Fförlags AB, Sundbyberg, 2002

[Mitrović, 2003]
Mitrovic Predrag, ”*Handbok i IT-säkerhet*”, 3:e upplagan, Pagina förlag AB, Göteborg, 2003

[**Muftic et al, 1993**]
Muftic Sead, Ahmed Patel. Sanders Peter, Rafael Colon, Jan Heijnsdijk Unto Pulkkinen, “*Security Architecture for Open Distributed Systems*”, John Wiley & Son Ltd, England, 1993

[Panko et al, 2004]
Panko, Raymond R, “*Corporate Computer and Network Security*”, Upper Saddle River, New Jersey, USA, 2004

[Pfleeger, 2000]
Pfleeger Charles P, “*Security in Computing*”, Prentice Hall PTR, Upper Saddle River, New Jersey, USA, 2000

[Pohlmann, 2001]
Pohlmann Norbert, ”*Firewall Systems*”, MITP-Verlag GmbH, Bonn, 2001

[SIS HB 550, 2003, 2003]
SIS HB 550, 2003, “*Terminologi för informationssäkerhet*”, SIS Förlag AB, 2003

[Stallings, 2003]
Stallings William, “*Networ Security Essentials*”, second edition, Pearson Education, Inc, Upper Saddle River, New Jersy, USA, 2003

[Strebe et al, 2000]
Strebe Matthew, Parkins Charles, ”*Brandväggar 24/7*”, Pagina förlag AB, Göteborg, 2000

[SYBEX, 2002]
SYBEX, “*Networking Completet*”, third edition, Sybex Inc, Alameda, USA.z George, 2002

[[Wallén, 1996]
Wallén, G., ”*Vetenskapsteori och forskningsmetodik*”, Studentlitteratur, Lund, 1996

14.2 Icke publicerade källor

[Web 1]
http://www.nada.kth.se/kurser/kth/2D1392/02-03/lectures/IPTCPUDP.pdf

[Web 2]
http://www.lysator.liu.se/~kjell-e/tekla/linux/security/tcpip.html

[Web 3]
http://www.google.se/search?q=buffere:UCCVeg5TVYAJ:www.javvin.com/protocolUDP.html+rfc+udp&hl=sv

[Web 4]
http://www.rejas.se/liskola/datorkommunikation/

[Web 5]
http://www.intranetika.com/intranetika/dns/dns-sweden.shtml

[Web 6]
http://www.susning.nu/ARP-spoof

[Web 7]
http://www.klcconsulting.net/smac/

[**Web 8**]
http://www.polisen.se/static/fap/FAP174_1_RPSFS2000_34.pdf

[Web 9]
Källa: F2 moment Säk2b, Ulrika Norman, DSV-SU

[Web 10]
http://www.knopper.net/knoppix/

[Web 11]
http://www.ietf.org/rfc/rfc0793.txt?number=793

[Web 12]
http://www.ietf.org/rfc/rfc0768.txt?number=768

[Web 13]
http://www.ietf.org/rfc/rfc0791.txt?number=791

[Web 14]
http://www.hannu.se/site/snmp_info.htm

[Web 15]
http://rfc1993.x42.com/

[Web 16]
http://www.ietf.org/rfc/rfc1180.txt?number=1180

[Web 17]
http://www.susning.nu/NIST

[Web 18]
http://www.susning.nu/GPS

[**Web 19**]
http://www.polisen.se/inter/mediabuffere/4347/4734/3928/RPS_pdf_Arsredovisning2003_040513.pdf

[**Web 20**]
http://www.sans.org/rr/whitepapers/authentication/1070.php

14.3 intervjuer

- **Informanter inom polisens utredningsavdelningar (Bilaga A)**

[Keyzer]
Jim Keyzer, kriminalinspektör vid Länskriminalens IT-brotts grupp i Stockholm.

[Leijon]
Ingemar Leijon, kriminalinspektör vid bedrägeriroteln i Kristianstad.

[Bergnér]
Per-Erik Bergnér, poliskommissarie vid enheten för interna utredningar i Stockholm.

- **Informanter inom åklagarmyndigheten (Bilaga B)**

[Ekelund]
Christer Ekelund, Chefsåklagare vid Polisenheten inom åklagarmyndigheten i Stockholm.

[Engfeldt]
Kay Engfeldt, vice Chefsåklagare vid Polisenheten inom åklagarmyndigheten i Stockholm.

[Roswall]
Håkan Roswall, kammaråklagare (IT-åklagare) vid internationella kammaråklagaren, Stockholm.

- **Informanter inom advokatbyråer (Bilaga C)**

[Ericsson]
Johan Ericsson, brottsmålsadvokat vid advokatfirman Advokaterna, Stockholm.

[Salomonsson]
Ola Salomonsson, brottmålsadvokat vid advokatbyrån Advokatfirman Peter Ahltin, Ola Salomonsson, Per Liljeqvist HB, Stockholm.

[Durling]
Per Durling, brottmålsadvokat (f.d. åklagare och domare), advokatfirman Per Durling, Stockholm.

- **Informanter inom informationssäkerhetsområdet (Bilaga D)**

[Richardsson]
André Richardsson, teknikkonsult vid Ekelöw Infosecurity AB, Stockholm

[Söderholm & Olsson]
Mats Söderholm och Mattias Olsson, teknikkonsulter vid konsultföretaget FKC AB, Stockholm

Bilaga A

Intervjuer: Polisens utredningsavdelningar

Intervju

Person: **Jim Keyzer, Kriminalinspektör**
Plats: **Kungsholmsgatan 37, Stockholm**
Tidpunkt: **8 April, 2004 Klockan 09.10 – 10.40**

Jim Keyzer är kriminalinspektör och arbetar med IT-relaterad brottslighet vid länskriminalens IT-brottsgrupp. Arbetsuppgifterna blandas med egna utredningar, undersökning av beslagtagna datorer och annan lagringsmedia och att hjälpa distrikten i Stockholms län med brottsutredningar med IT-inslag [IT-brottsutredningar]. Brottet dataintrång är dock dedikerat till Jims avdelning vilket innebär att misstänkta brott med denna brottsrubricering utreds centralt oavsett var de begåtts inom Stockholms län. (Egen kommentar: I vart fall enligt TjF 2002:08 127-G, vilket inte alltid följs!)

Det är vanligt att Jim kommer i kontakt med olika former av loggar i sitt arbete. I och med att de flesta loggarna kommer från beslagtagna hårddiskar är det de själva som tar fram dessa loggar. Ett exempel på sådana loggar är loggar från chattprogrammen ICQ, MSN, IRC. De flesta användarapplikationer skapar egna loggar, eller har i vart fall en möjlighet för användaren att välja om denne vill logga valda delar och det är något som man utnyttjar i aktuella utredningar.

Fördelen med att ha en beslagtagen dator är att ur dess hårddisk kunna säkerställa den information som vissa loggar avser. Det innebär att man inte alltid är så beroende av loggen som bevis i och med att man kan visa vilka data som hårddisken lagrat. Antingen som allokerade eller oallokerade filer.

På frågan om Jim genom sitt arbete kommer i kontakt med organisationer som själva har en verksamhet som genererar loggar som ligger till grund för brottsutredningarna svarade Jim ja. Det rör sig om olika företag som anmäler att de blivit utsatta för [olaga]. dataintrång eller att de funnit anställda som lagrat barnpornografiskt innehåll på företagets datorer. Ofta [Oftast]. är det dock olika teleoperatörer som anmäler att de blivit utsatta för dataintrång eller s.k. DOS-attacker. Övriga företag är betydligt restriktivare när det gäller viljan att anmäla liknande brott.

Jim är väl medveten om skillnaden mellan behörighet och befogenhet. Rutinerna vid en anmälan om att en anställd inom en myndighet eller företag brutit mot sina befogenheter är att man först kontrollerar vilka de interna bestämmelserna är. Detta är en förutsättning för att kunna driva ett ärende om dataintrång vidare då lagstiftningen i detta fall bygger på att den misstänkte olovligen bereder sig tillträde till den information som aktuellt system omfattar. I samband med dessa utredningar blir det aktuellt med att ta fram loggutdrag som kan visar att den misstänkte tagit sig in i aktuellt eller aktuella system.

När det gäller brott mot behörighet brukar man be företagen att själva presenterar loggarna. I undantag plockar rotelns egna personal ut uppgifterna i och med att man inte alltid vet hur aktuella system fungerar och att man inte vill riskera att göra något som påverkar systemet för aktuellt företag eller organisation. Undantaget är om man tagit maskiner i beslag. Loggutdragen ombes skickas som ”rådata”, vilket innebär att loggarna skickas obearbetade i det format som aktuellt system genererat dem i.

Man begär då in loggfilen från de aktuella dygnen och man ber i regel att företaget bränner en CD med de aktuella loggarna om det går. Ibland händer det att företaget skickar in loggfilerna på papper i form av Excelark.

Ett exempel på företag som Jim kommer i kontakt med är Lunar Works (Siten Lunarstorm). Det händer titt som tätt att han från företaget begär ut loggar ur ett aktuellt konto. Han brukar då få en lista från företaget som har sitt huvudkontor i Varberg. I loggutdraget framgår bland annat IP-adress och vid vilka tidpunkter inloggning skett [vilken teleoperatör som är aktuell för vidare spårning i vissa fall vara angiven, annans så tar vi reda på detta själva]. Det brukar gå bra att utreda varifrån informationen har skickats från i och med att det som regel går att identifiera den dator som tilldelats den dynamiska IP-adressen av aktuell ISP. Slipade ungdomar som nekar till anklagelserna och hävdar att de har många kompisar hemma är svåra att få fällda och då kommer man inte längre. Förvånansvärt många erkänner dock att de ligger bakom aktuell information när de ser loggutdragen som pekar ut deras egen dator.

När det gäller information som IP-adress och MAC-adress sätter Jim stor tilltro till dessa uppgifter. Det är med hjälp av dessa uppgifter som de kan identifiera de datorer som ligger bakom den trafik som genereras över Internet. Dock finns det en del problem med vissa ISP aktörer som t.ex. Telia som fram till i dag inte fullt ut uppdaterar sina kundregister när deras abonnenter flyttar. Det kan t.ex. framgå av deras loggar och system att en viss IP-adress tilldelats en abonnent som bor söder om Stockholm medan samme person i realiteten sedan några månader flyttat till en adress norr om Stockholm. Abonnenten har då tagit sitt gamla telefonabonnemang med sig när denne flyttat, men Telia har inte uppdaterat sitt kundregister. Det kan då bli en trovärdighetskonflikt med loggen om ISP aktören samtidigt säger att innehavaren bor på fel sida om staden gentemot den information som aktören levererar.

Jim berättade att man som regel inte är så sårbar mot förklaringar från den misstänkte som går ut på att någon spoofat dennes IP-adress eller MAC-adress i och med att man som regel tagit datorn i beslag. Det går då ofta att på ett eller annat sätt plocka fram information från datorns hårddisk som styrker påståendet i aktuella loggutdrag då tidigare och senare surfning på Internet lämnar spår på hårddisken med tidigare nedladdade HTML-sidor t.ex. Spåren på hårddisken kan tillsammans med loggutdrag från ISP:en styrka att en viss händelse skett [Ur dessa kan man läsa ut IP –och MAC-adresser som styrker loggutdraget från aktuella ISP aktörer.].

På Jims avdelning behandlar man inte loggutdragen annorlunda beroende på valet av autenticeringsmetod. Han medger dock att man sätter större tilltro till dem om de tagits fram av en organisation som t.ex. IBM än om de kommer från en mindre känd organisation som kanske i första hand inte sysslar med informationsteknologi.

Jim säger sig vara medveten om att det finns goda möjligheter att manipulera ett loggutdrag. Framför allt är detta möjligt att göra under den manuella hantering som ofta sker innan loggutdragen hamnar på hans avdelning.

De har då tagits fram av någon tekniker på en främmande organisation utan att de själva varit närvarande. Det har med andra ord ingen som helst kontroll på informationens äkthet, utan tvingas lita på den när den kommer. En inkommen CD-skiva med loggfiler eller utskriften kommer att få en framskjutande roll i utredningen.

Det har dock som Jim känner till hittills aldrig hänt att någon ifrågasatt loggfilerna med innebörden om att dessa skulle ha varit felaktiga. Man litar på dem men andra invändningar kan komma. T.ex. kan en chatt logg som visar vilken information som skrivits förklaras med att det är någon annan som skrivit dessa rader.

Jim ombads att ge sin egen syn på ett loggutdrag som bevis. Han berättade att loggen på hans avdelning som regel måste ställas tillsammans med annan bevisning. En logg ses mer som en pekare på att någonting har hänt, och i och med att de ofta kan ta aktuell dator i beslag finner de oftast bevis på hårddisken som gör att man inte är beroende av loggen på samma sätt som man vore utan en beslagtagen dator.

I övrigt är loggutdragets bevisvärde starkt förknippat med den misstänktes inställning till brottsmisstanken. Det är skillnad om den misstänkte erkänner det som loggen anger eller om denne förnekar. Dessutom är frågan ibland kopplad till den aktuella organisationens interna regelverk som styr befogenheten att få ta del av viss information.

I dag är det en reell möjlighet att en Trojan ligger bakom fyndet av viss information på en beslagtagen dator. Trojanen kan utgöra den mjukvara som gör det möjligt för en obehörig att komma åt aktuell dator utan att innehavaren känner till det. Av den anledningen är det idag rutin att undersöka en beslagtagen dator i syfte att se om det finns eller har funnits Trojaner på dess hårddisk. Förvånansvärt ofta finner man att datorn har eller har haft en Trojan eller annan icke-önskad programkod. Detta skapar egentligen enorma möjligheter för den misstänkte att skylla innehållet på hårddisken på någon annan.

Denna förklaring ligger som Jim känner till bara bakom en friande dom hittills. Bakgrunden är en anmälan från polis i Nya Zeeland [tysk anmälan]. om att en viss IP-adress tillgängliggjort [lagrat] barnporrbilder. Den [tyska] informationen hade tagits fram genom att den misstänkte nyttjade en mjukvara som gör det möjligt att gå in på varandras hårddiska och hämta och lämna information. Tyskarna hade tagit sig in i aktuell persons dators hårddisk och kopierat katalog och dess struktur och vid analys funnit barnporr på datorn. När datorn togs i beslag visade loggen att datorn vid aktuell tidpunkt haft rollen som server, vilket den får när någon annan släpps in med denna mjukvara. Under huvudförhandlingen blev det klart att någon annan haft möjligheten att ta sig in på mannens dator, och därmed fanns möjligheten för att någon annan kunnat lagra informationen som tyskarna hittade. Likheten med en Trojan är slående, och då man vid kontroll av hårddisken inte hittade någon barnporr, utan endast hade tyskarnas uppgifter, friades mannen. Försvaret hade bland annat fått reda på att Trojanen Back Orifice kan avinstallera sig själv. Som Jim vet har det inte varit aktuellt med ett omtag av en logg på någon av parternas begäran. Det är ingen som har begärt denna möjlighet.

Jim jobbar mest mot speciella IT-åklagare, vilka är åklagare som har speciella kunskaper inom IT-relaterad brottslighet. Därmed har de större förståelse för tekniken än vad en vanlig allmänåklagare har. Namn på åklagare som Jim arbetar med är t.ex. Håkan Rosvall som är kunnig och nyfiken vilket gör att han har kunskap och intresse nog för att kunna ställa egna relevanta frågor och inte enbart blint lita på den bevisning som presenteras. Han kan ställa egna frågor och göra en egen bedömning om materialet är korrekt eller inte.

En allmän åklagare accepterar mera det som de får. IT-åklagarna har mer kunskap och kan bedöma materialet på ett annat sätt.

Enligt Stockholmspolisens interna ärendefördelningsmodell är det bestämt att alla ärenden rörande dataintrång skall handläggas på Länskriminalens IT-brotts grupp. Nu sker så inte alltid till hundra procent, men de flesta ärendena rörande dataintrång kommer till Jims avdelning.

Intervju slut klockan 10.40

Intervju

Person: **Ingemar Leijon, Kriminalinspektör**
Plats: **Polhemsgatan 32, Stockholm**
Tidpunkt: **15 April, 2004 Klockan 10.00 – 11.50**

Ingemar Leijon arbetar som kriminalinspektör vid bedrägeriroteln i Kristianstad som tillhör polismyndigheten i Skåne. Genom sitt arbete, som i huvudsak består av bedrägeriutredningar, kommer han ofta i kontakt med loggutdrag från olika organisationer som visar vad en viss person gjort i olika system. Vanligtvis kommer dessa loggutdrag från banker, men även från andra organisationer som teleoperatörer.

När ett ärende kommer in till roteln skrivs i regel en anmälan. Därefter görs en snabb genomgång över vilka personer som är aktuella att höra och vilka organisationer som är aktuella att kontakta i syfte att få in underlag som kan komma att användas som bevis. Normalt kontaktar man då banker, kronofogdar och teleoperatörer m.fl. i syfte att beställa ut kontoutdrag m.m. vilka är att jämställa med loggutdrag. Vanligast är kontoutdrag från banker där utdragen är kopplade till en viss person.

På frågan hur dessa loggutdrag når Ingemar och hans kollegor svarade Ingemar med att det kan gå till på lite olika sätt beroende på hur van utredaren är att använda datorer. Vanligtvis ringer Ingemar och etablerar en personlig kontakt med den tekniker som får i uppgift att ta fram aktuella loggutdrag. Detta gör han bland annat i syfte att bygga upp en personlig kontakt som ofta är värdefull längre fram då loggutdrag ofta är svåra att tyda. Då är det bra att redan från början ha en kontakt som känner till vem utredaren är och som är någorlunda insatt i ärendet men som framför allt kan berätta hur loggutdragen skall tydas.

Ingemar brukar beställa loggutdragen på någon form av datamedia i och med att han är tämligen van med att kunna bearbeta materialet i sin egen dator. Han brukar få en CD-skiva skickad till sig med posten varefter han sedan har möjligheten att söka och sammanställa materialet på sin dator. På frågan om loggutdragen skickas assurerade eller liknande via posten svarade Ingemar nej. De brukar skickas som vanlig post. Filerna på CD-skivan är vanligen i Word eller Excel format.

Andra utredare, som inte har samma vana med att arbeta med datorer, beställer loggutdragen på papper. De flesta gör på detta sätt då väldigt många utredare fortfarande har dålig datavana. Loggutdragen beställs vanligtvis per fax, men även per post. Dessa bearbetas inte i lika stor utsträckning manuellt utan ingår vanligtvis helt eller delvis i förundersökningsprotokollet i det utförande de hade vid ankomsten.

Eftersom loggutdragen ofta är ganska svåra att förstå krävs det ofta att dessa kan förenklas så att åklagaren och domstolens medlemmar skall ha lättare att förstå dem. Med förenkling avses vanligtvis att det digitala materialet bearbetas manuellt så att det material som presenteras i förundersökningsprotokollet är mer begränsat och lättförståeligt.

Samtidigt kan man presentera materialet mer visuellt i form av diagram för att på detta sätt ge en snabbare inblick i vad det är loggutdragen innehållet. På så sätt kan man begränsa informationsmängden så att det mesta som inte är relevant plockas bort.

Originalen som skickats från den organisation som plockat fram loggarna finns dock alltid kvar varför det alltid finns en möjlighet för försvaret att ta del av det materialet även om det inte skulle ingå i sin helhet i förundersökningsprotokollet.

Vanligtvis är det inga problem med att få ut loggutdragen från banker och liknande organisationer. Mest problem är det med teleaktörerna i och med att det i Telelagen står angivet att vissa uppgifter endast kan inhämtas från dessa om minimistraffet är två års fängelse i straffskalan.

På frågan när Ingemar känner att ansvaret för informationsinnehållet hamnar inom hans kontroll svarade han med att det är när han fått materialet tillsänt sig. Vanligtvis sker detta när CD-skivan anlänt med posten, men det händer även att han är närvarande när loggarna tas ut. Ibland är det en fördel att på platsen där loggarna är åtkomliga kunna titta på materialet tillsammans med en tekniker så att en viss sållning kan ske på plats. Då plockas det material ut som Ingemar ser som varande relevant. Han får då i allmänhet materialet på en CD-skiva, och sedan den lämnats över ansvarar han för materialet. Hur materialet hanterat eller bearbetats inom den organisation varifrån han får materialet ligger inte inom hans ansvarsområde.

Sedan man fått loggutdragen i sin besittning är utgångspunkten otvetydigt att loggarnas innehåll är sanningsriktiga. Det är ingenting man ifrågasätter. Arbetet påbörjas med andra ord inte med att man loggarna är sanningsenliga. Man utgår aldrig från att loggarna skulle vara felaktiga, utan dessa är startpunkten i förhållande till det arbete som loggarna sedan genererar på utredningssidan.

Man ställer sig aldrig frågan på vilket sätt användaren bevisat sin identitet för målsystemet som genererat loggen, utan tilltron till loggen är total oavsett autenticeringsmetod. Ingemar har aldrig hört talas om att någon av hans kollegor ställer denna typ av frågor i samband med hanteringen av loggutdrag. Det här innebär att man heller inte bedömer loggutdragens informationsvärde beroende på valet av autenticeringsmetod, utan dessa ligger till grund för de påståenden som kommer att kunna riktas mot den enskilde under utredningen eftersom loggutdragen har ett bevisvärde i och med att de visar vad en unik användare gjort i aktuella system.

Ingemar fick svara på frågan om man brukar utreda hur trafiken i de lokala nätverk, som inom organisationen transporterar användarens förfrågan till respektive målsystem eller server, skyddas. På den frågan svarade Ingemar nej. Intervjuvarna konkretiserade frågan genom att ange att syftet i sådana fall skulle vara att ta reda på om de lokala nätverken är hubbade eller switchade och om trafiken på de lokala nätverken sker okrypterat eller om de skyddas av någon form av kryptering. På detta svarade Ingemar med att hans svar tidigare som innebär att man litar på loggutdragen hänger samman med denna fråga. Man undersöker inte dessa faktorer utan man utgår från att de loggutdrag som aktuell organisation överlämnar motsvarar vad som i verkligheten faktiskt har hänt. Man litar helt enkelt på att loggutdragen är sanningsriktiga utan att ta reda på vare sig autenticeringsmetod eller hur trafiken skyddas i organisationernas lokala nät.

Man måste komma ihåg att den misstänktes inställning är viktig i förhållande till vad loggutdragen visar. Det har hänt i utredningar som Ingemar drivit att man gjort kompletterande och mer djupgående undersökningar kring loggarnas bevisvärde beroende på den misstänktes inställning till det denne anklagas för.

Ingemar refererade under intervju till en utredning som avslutades under 2003 och som under intervjun går under namnet Perstorpsärendet. Det handlar om en anställd inom Perstorps kommun som var nära att komma över i stort sett hela kommunens innestående kontantkapital genom att gärningsmannen kommit över administratörslösenord till kommunens ekonomisystem.

Gärningsmannen, som nu är dömd för brotten, hävdade bland annat att någon annan utfört transaktionerna i hans namn. Det innebär att loggarna i sig inte ifrågasattes utan att den misstänkte, under utredningsstadiet och under huvudförhandlingarna, hävdade att loggarna inte hade något bevisvärde i och med att de inte kunde styrka att det var han som utfört transaktionerna då loggarna bygger på endast användarnamn och lösenord.

Ingemar kan inte erinra sig att någon någonsin ifrågasatt loggen som bevis. Varken han själv eller någon annan han känner till har någonsin varit med om detta. Han har heller inte den uppfattningen att loggutdragen behandlas mer kritiskt om den misstänkte förnekar de påstådda handlingarna som loggutdragen visar. Det är snarare tvärt om, om man lägger fram ett loggutdrag så behandlas det normalt som ett bevisbärande dokument som ingen ifrågasätter. Förnekar den misstänkte blir loggen ett bevis mot denne.

Man lämnar dock inte den misstänktes inställning utan att ha försökt att kontrollera den. Ett förnekande, eller en avvikande förklaring från den misstänktes sida i förhållande till logg-utdragen, leder till att man, som i Perstorpsutredningen, gör mer djupgående undersökningar i syfte att se om det går att finna mer stöd i det som loggarna visar eller inte.

Under Perstorpsutredningen visade det sig hur sårbara system är som endast autenticerar användaren med användarnamn och lösenord. Gärningsmannen i Perstorpsutredningen hade med mycket enkla medel lärt sig administratörslösenorden till kommunens ekonomisystem genom att helt enkel titta över axeln på chefen vid ett antal tillfällen då denne loggade in i systemet. Därmed var hela ekonomisystemet öppet för gärningsmannen då han senare förde över 20 miljoner kronor till olika konton. Det enda han behövde göra var att logga in med chefens användarnamn och lösenord.

Den skada som gärningsmannen orsakade i systemen var omfattande. Gärningsmannen hade stora datakunskaper och kunskaper om hur kommunens system fungerade. Som administratör kunde han i samband med den stora överföringen även radera samtliga användarkonton inom kommunen samt låsa ute Tito Enators ingång till kommunens system, dvs det företag som ger kommunen support och som på andra sätt är kommunen behjälplig beträffande kommunens system. Gärningsmannen raderade dock inga transaktioner, vilket får ses som en miss från dennes sida. Troligen beror detta på att han inte kände till exakt alla de steg som krävdes för att genomföra detta. Hade han haft den fulla kunskapen så medför behörigheten som administratör att denne hade kunna raderat de loggfiler som innehöll de utförda transaktionerna. Hjälpen i applikationen visar hur man går tillväga, men den informationen var dock gammal i och med att systemet uppgraderats utan att innehållet i hjälpen var uppdaterad.

Under intervjun ställde intervjuarna frågan till Ingemar vad denne ser för möjligheter i att kunna påverka informationsinnehållet i en logg under termer som lagring, transport och hantering. På frågan svarade Ingemar med att det största möjligheten att förändra informationen givetvis är under hanteringen av data då den bland annat genomgår manuella förändringar som när han själv arbetar med loggen för att den skall bli mer lättförståelig.

Han ser även möjligheter till att förändra data under lagring, då han genom egen erfarenhet, och genom Perstorpsutredningen, funnit hur lätt det är att komma åt daga på någon annans konto genom att se vilket lösenord denne slår in på tangentbordet i samband med inloggning. D.v.s. genom att antingen komma åt ett amin konto eller genom att utföra slagningar mot system i någon annan kontoinnehavares namn genom att logga in med dennes användarnamn och lösenord.

Under intervjun diskuteras andra former av autenticeringsmetoder, och på frågan om Ingemar känner till fler än användarnamn och lösenord så känner han till att det finns så kallade smarta kort och inloggning via biometri.

Intervjun slut klockan 11.50

Intervju

Person: **Per-Erik Bergnér, Kriminalkommissarie**
Plats: **Kungsbron 21, Stockholm**
Tidpunkt: **26 Februari, 2004 Klockan 12.20 – 14.00**

Bergnér är kriminalkommissarie och arbetar vid enheten för interna utredningar i Stockholm. I och med detta utreder han bland annat ärenden där anställda inom polisen misstänks för dataintrång.

Reglerna för olaga dataintrång är oklara. I lagtexten står det att du gör dig skyldig till brott när du olovligen bereder dig tillgång till ett system. Problemet är dock att det är svårt att definiera vad som menas med olovligen. I definitionen av ”befogenhet” talar man om ”tilldelade arbetsuppgifter”, dvs. att användaren måste kunna ta del av innehållet i registren för att kunna lösa sin arbetsuppgift. Följaktligen kan användaren ha behörighet till ett register men arbetsuppgiften ger ej befogenhet att använda detta.

Ett bra exempel på konflikt mellan befogenhet och behörighet är när en polisman förbereder sig inför ett besök oss en kriminell person som gjort en anmälan genom att gå in i systemen och ta del av olika register. Problemet ligger i att polismannen nu gör en ”slagning” på målsäganden eftersom han/hon vet att denne kan vara en farlig person. Ett sådant scenario skulle hamna i gränszonen på om ”slagningen” skulle vara tillåten. I efterhand blir det alltid en tolkningsfråga gentemot FAP: en[79] och denna tolkning kan bli olika runt om i landet.

Loggutdragen är svårhanterliga och i allmänhet svåra att förstå. Detta är ett problem i och med att inte så många instanser har rätt att arbeta med dessa. Dess komplexitet medför även att det kan bli svårt för en domstol att tolka dem. Förundersökningar rörande dataintrång måste vara pedagogiska och struktureras så den kan förstås av de åklagare som leder förundersökningarna, advokater, domare och inte minst de som berörs i form av skälig misstanke. I vissa fall har domstolar inte förstått loggarna och därmed vari brottet består, vilket har medfört att åtal har ogillats.

Juridisk personal utgår ifrån att loggutdrag är korrekta eftersom de inte haft anledning att ifrågasätta dessa. De måste kunna lita på att det som anges i loggutdraget är korrekt.

Ett annat problem vad gäller FAP: en är förbudet för polisanställda att slå i offentliga register t.ex. mantal eller bilregistret. Nyligen avkunnades en dom för dataintrång när en person gjort ”slagningar” efter mantalsuppgifter på tre grannar. Problemet är att han använde sig av polisens system trots att han kunde ha ringt eller bett en kollega och lagligt fått fram samma information enligt offentlighetsprincipen. Slagningen blir olaglig eftersom den sker med egen inloggning i polisens system trots en regel i FAP som medger viss användning av polisens IT-system för privat bruk och som inte inskränker på tjänsten.

[79] Föreskrift och Allmänna råd för Polisen – Styr bland annat hur polisens system får användas

Under utredningar så förekommer det oftast manuell hantering av loggarna. Man gör en sammanställning av de aktuella loggutskrifterna, som kommer i pappersform och inte sällan omfattar tusentals poster med kodad information.

Idag har Bergnér börjat begära loggarna i textformat på CD-rom för att kunna konvertera dem till Excel format. Det finns en risk finns i denna hantering eftersom delar av loggen riskerar att falla bort i samband med kopieringar mellan filformaten eller på grund av den mänskliga faktorn. Bland annat kan nämnas problem med filter i Excel där andra textfält bryter filtreringsmöjligheten.

Det har enligt Bergnér hittills aldrig hänt att någon ifrågasatt loggarnas riktighet. Den förväntade påföljden för dataintrång är böter och samhället förordnar inte alltid en offentlig försvarare för den typen av mål, trots att brottet har skett i tjänst och dessutom riskerar en arbetsrättslig påföljd. Den enskilde skall då gå upp ensam i en domstol och bemöta anklagelserna som bygger på en bevisning som domstolen och de inblandade aktörerna själva har svårt att förstå. Det går i regel inte heller att överklaga när det gäller bötesbrott.

De vanligaste förklaringarna vid misstanke om interna dataintrång är enligt Bergnér:

- *Jag minns inte att jag har gjort ”slagningen”*
- *Någon annan kan ha använt min ID*
- *Har gjort en ”slagning” åt någon annan men vet ej hur en SUD-”slagning”[80] går till*
- *Jag anser att detta ingår i mina arbetsuppgifter som ”spanare”, ”radiooperatör”, ”kriminalunderrättelsepolis”, ”stationsbefäl” eller bara som ”polis med intresse för tjänsten”*

Vad är en SUD värd om man påstår att ngn begärt slagningen och där den som påstås ha begärt den förnekar. Detta är troligen aldrig prövat. Personal vid KUT och LKC avdelningarna minns ofta inte slagningen eller i vilket ärende den är gjord. Dessa skrivs av. Går ej bevisa att det är olagliga slagningar. Underlåtenhet att använda SUD är inte heller prövat rättsligt.

Vad kan ligga bakom ett antagande om att loggen är fel? I utredningen rörande vilka som slagit på de två för mordet på Anna Lind häktade personerna var loggarna på 35: åringen (231 loggutdrag) inte fullständiga. Det visade sig att olika personer vid avdelningen som tar fram loggarna inte använder sig av ett och samma script, utan av olika. I detta fall hade ett script som inte tog fram en i varje enskilt fall komplett slagning använts. Vi såg frågan men ej fullständiga svaret. Såg ej hela vägen. Det var första gången Bergnér fann ett skäl till att kunna ifrågasätta loggutdragen. Mångfalden av loggar hade gjort att Bergnér hade fått en annan inblick och förmåga att läsa loggar. Tidigare hade han för dålig kunskap för att kunna göra detta.

Bergnér har aldrig blivit presenterad för hur hela händelsekedjan vad gäller loggen från det att den skapas till presentation. Han känner inte heller till hur den skulle kunna manipuleras bortsett ifrån möjligheten i den manuella hanteringen.

[80] SUD används vid ”slagning” på uppdrag av annan person. Den andre personen identitet skall då uppges för systemet i samband med ”slagningen”.

Vidare så ser han loggen som ett motsvarighet till ett rättsintyg[81]. Loggintyget ligger som underlag av en sakkunnig. Detta i stället för att den som tagit fram loggunderlagen från aktuella system vittnar vid domstolen så lämnar han över ett intyg där det framgår vad systemen loggat. Det vore önskvärt att den sakkunnige som tar fram loggutdraget också på något sätt skriver ett undertecknat intyg till CD-romskivan, datafilen eller papperskopian och som sedan kan ligga kvar som original i akten för kontroll vid ett eventuellt ifrågasättande – ett sakkunnigutlåtande.

Bevisningen måste kunna gå att presentera i rätten och i förundersökningen. Ofta är det för mycket information vilket medför att den måste filtreras för att vara lättbegriplig. Samtidigt får inte filtreringen göras så att den inverkar på den juridiska bedömningen, som alltid måste åvila en åklagare eftersom det handlar om ”brott i tjänsten”.

Oftast är det dessutom som så att den som man slagit på inte är part i utredningen och därmed skall hans namn och personnummer maskeras så att det inte syns i ett offentligt material. Ett typiskt exempel är just den pågående utredningen om vilka som har gjort slagningar efter mordet på Anna Lindh. Den först häktade personen, som visade sig vara oskyldig; är ju inte part i utredningen och hans personuppgifter faller under sekretessbestämmelserna. Samma sak gäller de lite mer dagliga ärendena där föremålet för slagningen är en granne eller före detta fruns nya partner.

Bergnér tillfrågades om han känner till om man någon gång gjort omtag av loggutdrag. På den frågan svarade han med att det endast är Roger Lindblom, i samband med Anna Lindh loggarna, som begärde omtag i och med att de första loggutdragen visade sig vara ofullständiga och framtagna med ett script som gav ett annat resultat än andra loggutdrag i utredningen. Den första var ofullständig, kräver kunskap om loggarna inom den aktuella organisationen. Dessutom gav omtaget anledning till att upprätta ytterligare en anmälan eftersom det tillkom ytterligare en person.

Intervjun slut klockan 14.00

[81] Ett rättsintyg är ett dokument där en rättsläkare eller annan läkare i ord och bild beskriver vilka skador en person haft vi undersökningstillfället, samt besvarar specifika frågor från beställaren som frisk för framtida med och liknande.

Bilaga B

Intervjuer: Åklagarmyndigheten

Intervju

Person: **Christer Ekelund, Chefsåklagare**
Plats: **Kungsbron 21, Stockholm**
Tidpunkt: **11 Februari, 2004 Klockan 15.20 – 16.20**

Christer Ekelund är chefsåklagare på Polisenheten vid åklagarmyndigheten i Stockholm och arbetar enbart med ärenden som hanteras vid avdelningen för interna utredningar i Stockholm. Genom sitt arbete kommer han i kontakt med användare inom polisen som misstänks för bland annat olaga dataintrång sedan de använt sin behörighet på ett felaktigt sätt i olika system. I detta arbete kommer Christer ofta i kontakt med loggutdrag, vilka tillhandahålls av tekniker och utredare.

När det gäller bevisvärdet av en logg så behandlas den frågan egentligen på samma sätt som all annan skriftlig bevisning. Så länge ingen påstår något annat litar man på att den skriftliga bevisningen står för vad den påstår. Samma sak gäller en logg. Ifrågasätts den inte kommer den att tillmätas ett bevisvärde. Om detta kommer att ske som ett led i en beviskedja eller som ett självständigt bevis är upp till vad som i övrigt framkommer i utredningen. Skulle den misstänkte t.ex. säga att han slagit så pass mycket i sitt arbete att han inte minns alla slagningar, men ändå inte förneka slagningen, skulle loggen med all sannolikhet användas som bevis för att slagningen utförts.

För att exemplifiera detta med att en logg kan jämställas med annan skriftlig bevisning kan nämnas att om en tekniker finner ett fingeravtryck på en brottsplats och fingeravtrycket identifieras som tillhörande en viss person, så utgår man ifrån att både teknikern på brottsplatsen säkrat avtrycket och hanterat materialet enligt alla konstens regler och att den tekniker som identifierar fingeravtrycket gjort en säker identifiering enligt de regler som gäller. Det är först om denna kedja ifrågasätts som man får titta närmare på säkrandet av avtrycket och hanteringen och/eller identifieringen. Ifrågasätter inte någon denna kedja tillmäts fingeravtrycket det bevisvärd som det har i dag.

Samma sak gäller en logg. Om ingen påstår att den tillkommit på ett felaktigt sätt, eller på annat sätt bestrider den, kommer den att tillmätas ett bevisvärde. Dock kommer ett bevis som en logg utgör inte att tillmätas samma stora värde som t.ex. DNA eller ett fingeravtryck i och med att en loggutskrift aldrig ensamt kan peka ut den fysiska person som gjort slagningen. Loggutskriften talar bara om att IT-systemet använts på viss sätt.

Som åklagare måste man lita på att det material som polisen lämnar över till dem är framtaget på ett professionell och korrekt sätt. Den som hanterar, eller tar fram något som lämnas över till åklagaren under en förundersökning, gör det med ett tjänstemannaansvar. Det gäller allt från förhör till skriftlig bevisning. Om innehållet i ett förhör skulle vara oriktigt och den hörde inte bestrider dess innehåll kommer troligtvis heller ingen annan att göra det, om det inte av andra skäl finns anledning att titta närmare på materialet. Man måste lita på att det polisen lämnat över är korrekt.

Christer känner inte till att man någonsin ifrågasatt äktheten i en logg, d.v.s. att någon skulle ha påstått att den är korrupt eller liknande. När det gäller teknik som loggar ligger det även en okunskap med i botten i och med att denna form av teknik inte är känd för vem som helst. I stället är det vanligare att användaren säger att slagningen utförts av någon annan. Detta kan t.ex. ske om det smarta kortet lämnats kvar i datorn vid en fikarast innan skärmsläckaren låser klienten. I det fallet är det ingen som ifrågasätter loggens riktighet, däremot påstår man att någon annan utfört slagningen i registret. Arbetet kompletteras då som regel med att om det på något sätt går att kontrolleras detta påstående.

I Christers arbete händer det ofta att polisen överlämnar ett loggutdrag som visar en viss användares slagningar i visst eller vissa system. För polisens del innefattar loggutdragen en transaktionskod som i sig inte säger någonting, utan som måste översättas. I ett moment där man vet att det kräves en mänsklig aktivitet som översättning ligger en medvetenhet i att det kan ske misstag. Det betyder att om en misstänkt säger att materialet som presenteras är felaktigt så måste man naturligtvis kontrollera detta.

För Christers del handlar det ofta om att göra en logg mer lättbegriplig för andra människor, speciell för dem som skall döma i en rättegång. Av den anledningen finns det ett intresse från hans sida att materialet som en logg utgöra kan presenteras på ett mer lättbegripligt sätt än i termer av siffror och bokstäver. Det kan t.ex. gå till på så sätt att man återgenererar trafiken mot aktuella system och tar fram avpersonifierade skärmdumpar. Även här kommer det i sådana fall att ske en manuell hantering, men som bygger på ett loggutdrag. Detta är ett manuellt arbete som i regel utförs av en utredare, och även här kan misstag begås. Det kan med andra ord bli som så att en logg som är framtagen kan tolkas på ett felaktigt sätt av den som återgenererar trafiken mot systemen, men om inte heller detta ifrågasätts av den misstänkte, åklagaren, försvararen eller domaren kommer även skärmdumparna som bygger på loggen att tillmätas ett bevisvärde.

En logg kan tillmätas ett bevisvärde både som ett led i en beviskedja och som enskilt bevis. Det beror helt på vad som i övrigt framkommer under utredningen. Ifrågasätts inte dess riktighet kommer den att tillmätas någon form av bevisvärde, detta oavsett om den är korrekt eller inte. Det måste alltså ställas stora krav på noggrannhet på alla personer som arbetat med den loggpresentation som åberopas som bevisning vid huvudförhandlingen.

Intervju slut klockan 16.20

Intervju

Person: **Kay Engfeldt, Vice Chefsåklagare**
Plats: **Kungsbron 21, Stockholm**
Tidpunkt: **10 Mars, 2004 Klockan 14.00 – 15.25**

Kay Engfeldt arbetar som vice chefsåklagare på Polisenheten vid åklagarmyndigheten i Stockholm, och arbetar i dag enbart med ärenden som hanteras vid avdelningen för interna utredningar i Stockholm. Genom sitt arbete som åklagare kommer Kay i kontakt med användare inom polisen som misstänks för bland annat olaga dataintrång. I detta arbete kommer han i kontakt med loggutdrag, vilka tillhandahålls av tekniker och utredare. Kay har i huvudsak arbetat med polisrelaterade brottsutredningar sedan 1993. Under denna tid har han även arbetat på JO, och hade vid JO ärenden som var relaterade till poliser, åklagare och domare.

På frågan om det stämmer att polisen är överrepresenterad när det gäller förundersökningar och domar angående olaga dataintrång svarade Kay tveklöst ja. En starkt bidragande orsak till detta är att polisen genom Rikspolisstyrelsen regelverk är tämligen ensamma om att ha så starka interna föreskrifter som reglerar användningen av polisiära system. Föreskrifterna och allmänna råd för Polisen (FAP 171-1, 4 Kap, 1 §) anges t.ex. att register som omfattar känslig information endast får användas för att fullfölja en tilldelad arbetsuppgift. . Därmed har polisen i princip kriminaliserat all felaktig användning av polisiära system. Någon motsvarighet till sådana interna bestämmelser finns t.ex. inte inom vare sig Åklagar-myndigheten eller Kriminalvårdsstyrelsen. Kay har heller inte hört talas om att andra myndigheter har liknande föreskrifter för sin personals styrning av deras befogenheter. En nackdel med att kriminalisera alla överträdelser av personalens befogenheter är att det inom brottet olaga dataintrång inte finns något ringa brott. Därmed är åklagaren tvungen att väcka åtal i de fall där den misstänkte inte accepterar ett strafföreläggande. I vissa fall skalle det vara med lämpligt med att ärendet hanteras internt inom polisen som ett disciplinärende i stället för att en allmän åklagare skall behöva driva ärendet som ett allmänt åtal i domstolen.

En annan bidragande orsak är att de anställda inom polisen är drygt 20.000 personer, vilket gör polisen till en av Sveriges största arbetsgivare inom ramen för svenska myndigheter. Ytterligare en orsak till polisens överrepresentation i antalet ärenden som berör olaga dataintrång är dessutom att polisen har en ganska effektiv logghantering och en intern utredningsavdelning bestående av professionella utredare som står under styrning av åklagare som Kay och hans kollegor. Ett hårt regelsystem gör dessutom att möjligheten till att hantera ärenden med misstankar mot polisen är starkt begränsade. Dessutom är det som så att de polisiära systemen i sig innehåller information som i sig är mycket känslig, något som kan vara frestande att använda i ett antal olika situationer som inte har med tjänsten att göra.

Kay har haft många ärenden angående felaktiga slagningar i polisens system. I allmänhet är dessa ganska enkla utredningar. Ett typiskt ärende innebär att det kommer in en anmälan till polisen med ett påstående om att en namngiven anställd inom polisen sagt sig känna till både det ena och det andra om anmälaren eller någon annan namngiven person. Då påståendena om att anmälaren förekommer i olika register ofta stämmer görs en kontroll om den anmälda personen hämtat informationen från något av polisens system, och ofta visar det sig att loggutdragen styrker påståendet i anmälan. Den namngivne personen hörs av personalen vid polisens interna utredningar, och hittills har det aldrig hänt att någon någon förnekat att de utfört slagningen i angivna system då loggutdraget presenteras. I stället lämnas olika förklaringar till varför slagningen eller slagningarna i de angivna systemen utförts.

I och med att den misstänkte hittills aldrig har nekat till slagningen har det inte blivit någon diskussion om loggutdragets riktighet. När den misstänkte medger slagningen är det inte nödvändigt att åberopa loggutdraget som skriftlig bevisning, utan det blir i stället förhöret med den misstänkte som utgör grunden för åtalet.

Det första som Kay vill ha reda på i dessa ärenden, sedan anmälan passerat hans bord och han beslutat om att inleda förundersökning, är att få reda på den misstänktes inställning till det som framgår av loggutdraget. I och med att den misstänkte hittills aldrig ifrågasatt loggutdraget, utan i stället medgivit slagningarna, bör detta indikera att loggutdragen i sig är korrekta. I vart fall ger detta förfarande inte Kay någon anledning att själv ifrågasätta loggutdragens riktighet. Dessutom ligger det i det generella arbetet att det material som presenteras för åklagaren i olika utredningar är framtaget på korrekt sätt och därmed skall vara korrekt. Detta gäller både loggutdrag och annan information som kan tjäna som bevisning i ett ärende.

För att försäkra sig om att den misstänkte skall kunna ge ett riktigt svar på frågan om denne utfört aktuella slagningar brukar Kay begära att utredarna vi den interna utredningsenheten skickar loggutdraget till den som utfört slagningarna så att denne i lugn och ro kan ta ställning till frågan om denne utfört dem. I teorin skall det kunna komma förklaringar som att denne påstår att slagningarna utförts av någon annan och att den misttänkte varit ledig aktuell dag, men sådana berättelser har hittills inte kommit.

Nästa fråga som Kay ställer är om slagningen i aktuellt eller aktuella register bygger på en tilldelad arbetsuppgift. FAP 171-1, 4 Kap, 1 § anger att polisen endast får utföra slagningar i känsliga system om tilldelats en arbetsuppgift som ger stöd för detta. Denna formulering är dock under diskussion då den stämmer väldigt dåligt överens med det sätt som polisen arbetar på, och för den delen, förväntas arbeta på. Det är sällan som så att en överordnad står och talar om för en enskild polis vad denne skall göra, utan dagens polis arbetar mycket självständigt.

Kay känner bara till ett enda ärende, de så kallade Wiman ärendet, där någon utfört slagningar i polisens system i ett kommersiellt syfte. Den utredningen blev mycket omfattande, och visade att Wiman utfört slagningar i polisens system för att kartlägga anställda på uppdrag av deras arbetsgivare inom olika privata företag. I Wiman ärendet var det frågan om flera hundra slagningar, men inte heller i det ärendet ifrågasattes riktigheten i loggutdragen.

I syfte att göra loggutdragen mer lättbegripliga händer det ofta att loggutdragen förenklas så att de kan förevisas för rätten och försvaret på ett mer lättbegripligt sätt. I det arbetet ligger ett manuellt arbete, och när det gäller manuellt arbete ligger det alltid en vetskap med i att det kan göras fel, men här ligger det ett stort ansvar hos den som är misstänkt.

I och med att den misstänkte inte ifrågasätter vare sig loggutdrag eller sammanfattningar finns det ingen anledning att ifrågasätta detta material.

Loggen som i dag presenteras från polisens sida är i sig mycket obegriplig. Det krävs en hel del av den utredningspersonal som hanterar ärendet för att den skall kunna göras begriplig. När det gäller loggutdragen blir det i regel ingen diskussion om dem i rätten, och en av orsakerna skulle kunna vara att de är så svåra att förstå. Till detta tillkommer att kunskapen om hur loggen genereras och hanterats är ett tämligen okänt område, och då den misstänkte inte ifrågasätter loggutdragen eller dess sammanfattningar leder detta till att det i allmänhet inte blir någon diskussion i detta ämne.

En jämförelse kan göras med ett rättsintyg som normalt skrivs på svenska för att det skall vara förståeligt för lekmän. Läkarens normala språk är latin, och även om det språket är mer lämpligt för att förklara skadans art och placering föredrar man det mer begränsade språket som svenskan innebär bara för att innehållet skall vara begripligt.

Däremot kunde Kay hänvisa till ett ärende han haft tidigare där taxichaufförer från Taxi Stockholm misstänktes för att ha manipulerar taxameterns kontantsummerare genom att nyttja ett datorprogram som manipulerade den kontantsumma som chauffören mottagit som ersättning för utförda körningar under sitt arbetspass. I och med att de misstänkta i det ärendet ifrågasatte bevisningen gjordes en omfattande utredning där programmerare och andra sakkunniga vittnade. Det hela slutade med att det gick att bevisa att taxametern var manipulerad i och med att de korrekta värdena innan manipulationen av systemet meddelats till Taxi Stockholms huvuddator.

Ärenden som olaga dataintrång är i regel bötesbrott. Det innebär i sig att en utredning liknande den som skedde i Taxi Stockholm ärendet troligen inte kan bli aktuell. En orsak till att inte inleda förundersökning eller att lägga ned en inledd förundersökning är att utredningskostnaderna inte står i proportion till brottets påföljd. I ett ärende med brottsmisstanken olaga dataintrång skulle utredningen i ett liknande fall helt enkelt kunna bli för dyr för att stå i proportion till det bötesbelopp som gärningsmannen skulle komma att dömas till.

I och med att ingen hittills förnekat påstådda slagningar aktuella system har det inte funnits någon anledning till att ta ställning till olika val av autenticeringsmetoder. Det har heller inte varit aktuellt att sätta sig in i frågor som hur loggen transporteras, lagras eller hanteras under sin väg från födsel till presentation. Frånvaron av ifrågasättanden har lett till att allt sådant inte varit nödvändigt.

På frågan om Kay ser något problem med brottet olaga dataintrång svarade han med att dessa i regel är tämligen enkla ärenden med den motivering som anges inledningsvis i hans berättelse. Därtill tillkommer det faktum att det är ett så kallat bötesbrott vilket normalt gör att den misstänkte inte tilldelas en offentlig försvarare. Så är även fallet vid snatteribrott. Vad Kay däremot ser som ett problem är att en misstanke om olaga dataintrång antingen leder till åtal alternativ att det inte händer någonting. Det skulle kunna tolkas som så att slagningen antingen är korret eller inte, men många gånger är motiveringen från användarens sida i gråzonen för vad som är tillåtet, och de interna reglerna säger att dessa ärenden egentligen skall gå vidare för en intern hantering som t.ex. kan leda till enskilda samtal eller en hantering i aktuell ansvarsnämnd.

Detta händer dock väldigt sällan, utan en nedlagd förundersökning gör som regel att ärendet stannar av, och risken är att gränsfallen för vad som är tillåtet att göra med de polisiära systemen tolkas därmed som något tillåtet.

Intervjun slut klockan 15.25

Intervju

Person: **Håkan Roswall, IT-Åklagare**
Plats: **Polishuset, Kungsholmsgatan 37**
Tidpunkt: **14 juni, 2004 klockan 09.00 – 10.30**

Roswall är en av tio[82] speciella IT-åklagare och har sedan hösten 1999 endast haft hand om denna typ av mål. Tidigare har han i sin karriär bland annat tjänstgjort på datainspektionen samt som Eko åklagare. Cirka 60% utav de ärendena som Roswall utreder idag är barnpornograf relaterad brottslighet.

Enligt Roswall så gör företagen fler IT-relaterade anmälningar idag än tidigare. Detta skulle kunna förklaras med att IT användningen växer för varje år men kan även vara ett uttryck för att företagen ser det som mer meningsfullt att anmäla idag än för fem år sedan i och med att det är högre uppklaringsprocent på denna typ av brottslighet idag. IT-åklagarna är helt enkelt bättre förberedda för denna typ av mål idag än för några år sedan. Dock finns det fortfarande företag inom näringslivet som undviker att göra anmälningar på grund av att de inte vill bli förknippade med problem av sina kunder. Istället gör dessa företag egna utredningar för att istället hindra att problemet händer igen.

Erfarenheterna av loggar är att dessa ofta är av väldigt skiftande kvalité vilket gör det svårt för åklagarsidan att få fram vad som har hänt. Om det tex. skall gå att bevisa att någon olovligen tagit del av information så måste det gå att reda ut exakt vad som skett i systemet. I många fall sker endast loggning i delar av systemet vilket gör att viktiga delar i händelseförloppet faller bort. Följden blir att åtal ej kan väckas eftersom åklagarsidan inte kan bevisa hur något har genomförts.

Vid IT-relaterade brott så är det viktigt att åklagaren gör en sorts introduktion till grundläggande datateknik/nätverksteknologi så att domare/nämndemän kan följa åklagarens resonemang. Problemet är dock att IT-åklagarna endast hinner med de mest komplicerade åtalen vilket resulterar i att även ”vanliga” åklagare ofta väcker åtal i IT-brottsmål. Dessa har dock sällan den kompetens som krävs för att hålla en introduktion eller till fullo själv förstå all bevisföring.

Rent generellt så skulle aldrig Roswall bygga ett åtal med endast loggar som bevisning eftersom ingen logg är till 100% säker. Istället krävs andra former av bevis som kan komplettera loggarna. Ofta erkänner dock den misstänkte när han/hon ställs inför loggutdrag och Roswall har aldrig varit med om att någon misstänkt hävdat att loggutdraget skulle vara felaktigt. Bland de som däremot försvarar sig, vilket ofta är personer med bra datakunskaper, så är den vanligaste förklaringen att loggutdraget kanske är riktigt men det var inte han/hon som satt vid ”tangentbordet”.

[82] En försiktig bedömning av Roswall uppskattar att fyra av dessa har mycket bra med kunskaper vad gäller IT

Om den misstänkte i detta fallet står fast vid sin förklaring och ingen annan bevisning finns förutom loggutdraget så tror Roswall att den misstänkte skulle gå fri.

Vidare så ser Roswall problem i framtiden med senarior där kriminella lierar sig med IT-säkerhetspersonal för att utföra olika typer av handlingar och där kanske endast ingen annan bevisning än loggar kommer att finnas. Om de misstänkta då inte gör några medgivanden så kommer det bli mycket svårt att få någon fällande dom. Ibland uppstår emellertid problem på helt andra områden än hur bevisning av ett intrång skall ske. I ett fall uppstod istället frågan angående den misstänktes uppsåt. Brottet dataintrång består bl.a. i att någon "*olovligen bereder sig tillgång till en upptagning för ADB*". För straffansvar krävs uppsåt, dvs en insikt om att man gör något olovligt.

I Internetsammanhang kan det ibland vara svårt att avgöra vad som är lovligt respektive olovligt. Utgångspunkten måste ju alltid vara den att information som är allmänt tillgängligt på Internet är lovlig att accessa för envar, om det inte av någon särskild omständighet framgår att tillgången till informationen är begränsad till en viss kategori. I det aktuella fallet hade en myndighet utlyst en tävling i vilken intresserade kunde redogöra för en affärsidé man avsåg att förverkliga. 20 vinnare skulle få 300 000 kr var. De tävlande skulle anmäla sig samt lämna information om sina projekt via en portal på Internet. För att kunna lämna sina bidrag var den tävlande tvungen att skapa ett användarkonto samt knyta ett lösenord till detta konto. Vid inloggning hamnade den tävlande i ett formulär som skulle fyllas i. Vid varje efterföljande inloggning hamnade den tävlande i sitt formulär. En av de tävlande upptäckte att han via URL-raden på en särskild formulärsida kunde söka efter och accessa samtliga tävlingsbidrag och inte bara sitt eget genom att ändra det specifika projektnummer som fanns angivet i raden. Han berättade om detta för en av sina kamrater som också tilhörde de tävlandes skara. De båda gjorde ett stort antal sökningar på andras ansökningar vid ett flertal tillfällen enligt vad som framkom av loggarna. Såvitt framgick av loggarna hade de båda i vart fall delvis vidtagit åtgärder som uppenbart syftade till att kartlägga bristen i säkerheten på portalen.

Under förhör förnekade de båda brott och menade att informationen var tillgänglig på Internet. De ville inte medge att de förstod att det varit myndighetens mening att varje tävlande bara skulle kunna ta del av egna bidrag. Även om det fanns ett inloggningsförfarande låg informationen allmänt tillgänglig på Internet. De uppgav att de kunnat komma åt vissa bilagor utan att de dessförinnan behövt vara inloggade. Även övrig information hade varit tillgänglig efter det att de loggat ut. Det hade inte krävts någon ny inloggning för access. De hade jobbat med flera olika öppna fönster i webbläsaren samtidigt.

En genomgång av myndighetens portal visade att man använde sessionscookies. Varje session levde 60 minuter på servern. Utloggning skedde via en särskild knapp. Sessionen dödades dock inte ut då användaren tryckte på knappen. Han förflyttades endast till en sida som upplyste om att en fullständig utloggning förutsatte att webbläsaren stängdes. Eftersom sessionen levde kvar i servern även efter en tryck på utloggningsknappen kunde alltså en inloggning via webbläsaren ske med automatik utan att det syntes för den tävlande. Genomgången visade också att den tävlande även efter en inloggning körde på port 80, dvs på webbläsarens aktivitetsrad fanns fortfarande zonen Internet angiven.

Med hänsyn till att automatisk inloggning varit möjlig och då det av webbläsaren framgick att den tävlande efter inloggning fortfarande befann sig i zonen Internet beslutade jag att inte väcka åtal eftersom jag gjorde bedömningen att en domstol inte skulle anse att jag kunnat styrka att de båda konsulterna haft uppsåt till att begå brott.

Eftersom domstolar har mycket låg kunskap om IT är det Roswalls erfarenhet att domstolens ledarmöter alltid utgår från sig själva. Det dom själva inte förstår vill dom inte lägga någon annan till last, oavsett dennes förkunskaper. Sannolikheten för en fällande dom var alltså liten. Problem uppstår i de fall där företag/myndigheter använder sig av grupplösenord för att skydda sina system. Roswall har erfarenheter apoteksbolaget samt sjukvården där denna from av autenticering har använts. Det är även vanligt att personer lånar ”användare” från varandra för att göra verksamheten ”smidigare”. Allt detta resulterar i att åtal ej kan väckas eftersom vem som helst kunnat söka access till systemet i skydd av en annans användarkonto. Därför att det mycket viktigt att det finns ett klart skriftligt regelverk som styr över verksamheten, dvs vem som får ta del av vilken information, handhavande av användarkonton osv.

Det har funnits fall inom sjukvården och socialtjänsten där bestämmelserna angående när man får ta del av känslig information har varit i en mera muntligt form vilket ställt till problem när åtal väckts. Eftersom anvisningen inte har varit skriftlig så har den misstänkte kunnat neka till att han/hon skulle ha kännedom om regelverket. Regelverket har i dessa fall istället varit en sorts muntlig tradition liknande ”att så här brukar vi göra…”

Om den misstänkte nekar till anklagelserna och hävdar att han/hon är oskyldig så måste åklagarsidan börja att söka alternativa förklaringar . Detta skulle kunna innefatta att se över autenticeringsrutiner, leta efter trojaner/”sniffrar”, se över möjligheten att någon annan sett den misstänktes lösenord ”över axeln” samt eventuella vittnesuppgifter. Det har funnits fall där personer misstänkta för barnpornografibrott har frikänts pågrund av att utredarna vid genomgång av den misstänktes persondator funnit installerade trojaner.

Dock innebär inte detta automatiskt ett frikännande utan detta måste ställas mot andra faktorer så som användarmönster av hur bilderna har rangerats osv. Ett problem som skulle kunna bli vanligare i framtiden ur åklagarens synvinkel är att det redan i dag finns trojaner som av installerar sig själv. Vid misstanke om sådan så måste utredarna försöka finna spår av dennes tidigare närvaro genom att genomsöka datorns minnesallokering.

I vanliga fall utdelas ingen offentlig försvarare vid mindre förseelser vad gäller dataintrång[83] men om fallet bedöms vara av en svårare typ så kan domaren tilldela en offentlig försvarare i samband med att förundersökningen startar. Detta kan medföra problem eftersom det kan vara nog så svårt att försvara sig själv och ännu svårare om man inte förstår tekniken som är en del av bevisningen mot mig.

Vad gäller autenticeringsmetoder så är Roswall väl förtrogen med begreppet och känner själv till metoder så som: lösenord, smart kort, biometri samt mätning av tangentnedtryckningar.

Vidare så har Roswall inte varit med om att man tagit int externa experter för att vittna vid ett åtal. Istället så är det utredarna på rikskriminalens IT-brottsgrupp som står för den tekniska kunskapen om så skulle bli fallet.

Intervju slut 10.30

[83] En mindre förseelse skulle i detta fallet kunna vara en sjuksköterska som tagit del av patientinformation fast hon inte är delaktig i vården av densamme

Bilaga C

Intervjuer: Advokatbyråer

Intervju

Person: **Johan Ericsson, Advokat**
Plats: **Hantverkargatan 78**
Tidpunkt: **10 juni, 2004 klockan 09.15 – 10.30**

Ericsson har vid ett flertal tillfällen kommit i kontakt med loggutdrag i samband med utredningar kring barnpornografi och dataintrång. Han betonar dock att han även kommit i kontakt med utdrag i andra typer av brott som man normalt inte förknippar med logghantering och då i form av telefonlistor som tillhandahålls av leverantörerna.

Hans uppfattning angående denna typ av bevisning är att juridisk personal undviker problemet eftersom man är rädd för att ge sig in på ett område som man inte behärskar. Resonemang kring den här typen av frågor kan snabbt bli för komplicerat. I ett aktuellt fall så fördes en diskussion om huruvida en utomstående part skulle kunna ha sparat ned barnpornografiskt material på den misstänktes persondator med hjälp av en trojan. Under rättegången fördes då diskussionen mellan polisens IT-utredare och den misstänkte som själv hade stor kunskap på området. Sådana diskussioner hamnar lätt ovanför den juridiska personalens nivå och blir därför svår att följa.

För övrig så menar Ericsson att det ofta är de personer som har stor kunskap inom data som ifrågasätter bevisningen, vilket å andra sidan kan ses som helt naturligt eftersom de är de enda med kunskapen att göra det. I det aktuella fallet så medgav polisens experter att det teoretiskt är möjligt för någon att med hjälp av NetBus plantera bilder oss en annan persons uppkopplade dator. Rätten valde dock att fälla mannen eftersom bilderna bland annat var strukturerade på sådant sätt att de tydde på aktivt bruk från den misstänktes sida.

Vidare menar Ericsson att mycket i en rättegång hänger på att materialet presenteras på ett bra och pedagogiskt sätt så att det blir begripligt för rätten. Det är även hans erfarenhet att denna presentation kan skilja sig avsevärt mellan olika åklagare i vilken grad detta sker.

Enligt Ericsson så kan han inte minnas några specifika fall där en misstänkt hävdat att loggen skulle vara felaktig. Istället är den vanligaste förklaringen att någon annan gjort den otillåtna åtgärden men med den misstänktes användare och därför anser sig som oskyldig. Denna inställning är även ett mycket effektivt försvar och Ericssons erfarenheter, vad gäller dataintrång inom polisen, är att åtalet lagts ned ifall det kommit fram att den misstänktes användare använts av andra personer, tex. att flera personer frekvent ”gör” slagningar åt varandra.

Ericsson upplever det även som svårt att veta vart han skall angripa åklagarens bevisning i och med att han inte alltid förstår den. I och med detta är han rädd för att ställa fel frågor vilket skulle kunna skada hans klient, resultatet blir istället att han agerar återhållsamt.

Problemet kan jämföras med DNA-tekniken som Ericsson även den upplever som lika problematisk. Om man inte förstår tekniken så går det inte att föra ett så effektivt försvar som man borde kunna göra.

Vidare så har beviskedjan, enligt Ericsson, aldrig ifrågasatts vid någon rättegång. Med detta menar vi händelsekedjan från och med att bevis beslagtas (tex. en persondator) till att tex. ett loggutdrag presenteras vid rättegången. Rent generellt menar Ericsson att den svenska polisen behandlar bevis på ett dåligt sätt i förhållande till tex. USA. I USA skulle tex. vidröra ett bevisföremål med oskyddade händer vara otänkbart om man senare skulle vilja använda DNA från föremålet som bevis vid en rättegång. Om så skulle ske så skulle förmodligen försvaret ta upp möjligheten för att det funna DNA:t blivit nedsmittat pågrund av beröring från andra personer än den misstänkte. I huvud taget ifrågasätts bevis i större omfattning i USA och Ericsson menar att detta förmodligen är en trend som kommer komma till oss.

Om exempel på att bevis borde ifrågasättas i större utsträckning tar Ericsson upp att de ovan nämnda utdrag över telefontrafik som teleleverantörerna delger polisen vid brottsmål. Dessa är en form av loggutdrag som frekvent förekommer i utredningar och som har ett mycket högt bevisvärde i de svenska domstolarna, i flera fall behandlas de som mer trovärdigt en ett ögonvittne och får därför ofta en helt avgörande rott i vissa fall. Problemet är dock att det ibland förekommer ”konstigheter” i utdragen som inte riktigt uppmärksammas av rättsväsendet. Som exempel visar Ericsson under intervjun ett utdrag i vilket det aktuella numret enligt utdraget både varit ”avstängt” samt ”använts” vid samma tillfälle. Som exempel nämner han även fall med oförklarliga överlappningar i telefontrafiken mm.

Trots att leverantörerna medger att det sker ”krascher” i systemet som kan påverka innehållet i utdragen så upplever Ericsson att rätten blundar för detta vilket han upplever som mycket märkligt. Fast ett loggutdrag från tex. polisens interna nätverk och dessa trafiklistor i grunder är samma sak så verkar rätten resonera helt annorlunda. Vid en rättegång skulle troligtvis loggutdraget från polisens interna nät underkännas som bevisning om det blev känt att det sker ”krascher” som påverkar dess innehåll. Inte heller har Ericsson varit med om att administratörernas roll i samband med dessa trafiklistor har ifrågasatts. Vad kan egentligen en trafikadministratör göra i systemet på tex. Comviq:s driftcentral?

Samband med de rättegångar som varit angående interna intrång inom polisen har autenticeringsfrågan förts på tal. Ericssons erfarenhet under dessa rättegångar är att om den misstänkte hävdar att andra kan ha varit inne på hans/hennes användare så frikänns personen eftersom det då inte går att binda någon till brott. De autenticeringsmetoder som Ericsson spontant känner till är lösenord, smart kort samt igenkänning av fingeravtryck.

Vidare berättar Ericsson att det är domaren som avgör huruvida en person misstänkt för olaga dataintrång skall ges en offentlig försvarare eller inte. Det hela varierar från domare till domare och beroende på hur komplext målet är.

Intervju slut 10.30

Intervju

Person: **Ola Salomonsson, Advokat**
Plats: **Skeppsbron 28, Stockholm**
Tidpunkt: **Den 22 juni 2004 klockan 08.10 – 09.30**

Ola Salomonsson arbetar som brottsmålsadvokat och försvarar ibland poliser som misstänks för brott. Genom åren har Salomonsson försvarat ett ganska stort antal poliser. Av dessa ärenden har uppskattningsvis 20 till 25 handlat om olaga dataintrång.

När det gäller poliser som är misstänkta för brottet olaga dataintrång bygger det på polisens interna bestämmelser som innebär att otillåtna slagningar i systemen handläggs av åklagare. Som grund får brottsmisstanken ligger polisens FAP (Polisens föreskrifter och allmänna råd) som anger att en slagning endast är tillåten som ett led i en tilldelad arbetsuppgift. Salomonsson ser detta som en klumpig formulering eftersom det inte är på detta sätt som polisen arbetar. Det förekommer många gånger att poliserna arbetat självständigt, och utefter eget tyckande ansett sig vara berättigade till att genomföra vissa slagningar trots att dessa inte bygger på en av chefen, eller någon annan, tilldelad arbetsuppgift.

När ett ärende om dataintrång kommer till Salomonsson, oavsett vem det är som är misstänkt, så handlägger han dessa ärenden på ungefär samma sätt. Han utgår från den berättelse och inställning som hans klient har. Det innebär att han genom sin roll som försvarare kommer att framhärda den inställning som klienten har. Genom klientens berättelse och det som i övrigt framkommer av förundersökningsprotokollet får han fram uppgifter som ger svar på frågor som vilket regelverk styr klientens åtkomst till systemen, vilket system avser slagningen, vem har man slagit på o.s.v. Han har i samband med detta inte tänkt på att materialet som presenterats i förundersökningsprotokollet i form av loggutdrag skulle kunna vara manipulerat. Han utgår från att det material som loggutdragen utgör i förundersökningsprotokollet är korrekta. Åtminstone så länge som inget annat framkommer som skulle tyda på motsatsen och hittills har det inte skett när det gäller polisiära ärenden. Loggutdragen blir mer ett underlag för den diskussion som han kommer att ha med sin klient, och det är klientens berättelse som kommer att styra hans fortsatta agerande som försvarare.

I de allra flesta fallen innebär olaga dataintrång att ärendet berör polisanställda. I dessa fall är det absolut vanligaste att klienten vidgår slagningen, men hävdar att den av en eller annan anledning är ett led i dennes arbete. Vid en uppskattning anger Salomonsson att det nog rör sig om cirka 80 procent av fallen där polismannen vidgår slagningen, och som anger att det skett på ett korrekt sätt genom de skäl som denne anger. I vissa fall har det hänt att polismannen förnekat slagningen på så sätt att denne framfört lokala rutiner som att man t.ex. delar på en inloggning och att någon annan gjort slagningen då polismannens kort varit påloggat. Exempel på förklaringar är att man inte minns att man utfört slagningen, och att det kan vara som så att någon annan gjort slagningen när polismannens kort varit påloggat. Det blir då en diskussion om vem som kan ha gjort slagningen, och ofta slutar det med att någon annan i rummet kan ha gjort det.

Salomonsson minns inte att någon direkt tagit detta som ett absolut argument annat än att det slutat vid att det är sannolikt att någon annan utfört slagningen o.s.v.

Det har aldrig hänt att en polisman ifrågasatt loggen genom att hävda att loggen inte kan vara korrekt eller liknande. Nekande till utförda slagningar har hittills skett tillsammans med förklaringen att det varit möjligt för andra att slå i systemen med polismannens kort.När det gäller loggutdrag så har Salomonsson själv inte ställt några frågor om hur materialet som loggutdragen utgörs av tagits fram. Han har inte ifrågasatt hur materialet tagits fram, behandlats eller förvarats innan det presenteras hamnar i förundersökningsprotokollet. Av den anledningen blir svaret på frågan om loggens väg från skapelse till presentation något som Salomonsson inte kan besvara med annat än att den för honom inte varit känd. Salomonsson utgår från klientens berättelse, och hittills har det inte hänt att den berättelsen innehåller någonting som tytt på att materialet som presenterats i loggutdragen inte skulle vara korrekt.

Skulle en klient i framtiden neka till en slagning genom att börja ifrågasätta loggutdraget har Salomonsson inte egen kunskap för att kunna ifrågasätta loggutdragen. Sådan kunskap måste då tas in utifrån. Det genererar ökade kostnader och det är inte säkert att dessa kostnader stannar på staten.

Eftersom det är klientens berättelse som ligger till grund för Salomonssons försvar har han hittills inte satt sig in i frågor som påverkar loggutdragets trovärdighet eller styrka. Under intervjun ställdes frågan om Salomonsson ser med olika ögon på ett loggutdrag som bygger på stark autenticering (någonting man har och känner till som kort och PIN-kod) än ett loggutdrag som bygger på inloggning med användarnamn och lösenord. Då dessa begrepp till stora delar var okända för Salomonsson krävdes en förklaring från intervjuaren vad skillnaden består i mellan en stark autenticering och en lösenors inloggning. Det blev en diskussion kring detta ämne som innebar att Salomonsson blev medveten om skillnaden. Dock har han hittills inte tänkt i dessa banor eftersom klienterna inte bestridit loggutdragen på detta sätt.

Eftersom Salomonssons inte haft anledning att närmare sätta sig in i tekniken bakom loggutdragen blev hans svar på frågor kring lösenordens transport i klartext på de lokala nätverken, och om dessa är ”hubbade” eller ”switchade”, någonting som inte kunde besvaras. Han upprepade att han i ärlighetens namn inte har den kunskapen som krävs för att på ett närmare sätt kunna ifrågasätta ett loggutdrag Han har ett arbetssätt som utgår från den misstänktes berättelse.

Denna typ av kunskap saknas i allmänhet inom advokatvärlden. Salomonsson har inte mött någon kollega som har några djupare kunskaper om informationsteknik. Allmänt sett så vet man inte hur man skall bemöta frågor som olika autenticeringsmetoder eftersom man inte vet vad de står för eller innebär. Man ställer som regel inte frågor som om lösenorden transporteras i klartext i nätverken, om organisationen som genererar loggutdragen har ”switchade” eller ”hubbade” nätverk, eller hur den misstänktes dator står placerad och därmed kan exponera sitt lösenord för andra. Återigen, det är Salomonssons uppfattning av advokater i denna fråga utgår från klientens inställning, och ifrågasätter inte klienten materialet så gör advokaten i allmänhet inte det heller.

Skulle man till slut hamna i en situation där den misstänkte nekar till att ha utfört slagningen och börjar ifrågasätta loggkontrollen så vet Salomonsson inte på rakt arm hur han skall agera. Hittills har det dock inte hänt att någon tagit strid mot ett loggutdrag på det sättet. I avsaknad av egen kunskap skulle det i framtiden kunna innebära att Salomonsson tar in en teknikexpert för att få hjälp, men hittills har detta inte skett.

Intervjun avslutad klockan 09.30

Intervju

Person: **Per Durling, Advokat**
Plats: **Hantverkargatan 78, Stockholm**
Tidpunkt: **27 Februari, 2004 Klockan 13.00 – 14.20**

Per Durling har arbetat både som åklagare och brottsmålsadvokat under sitt yrkesliv som jurist. Under delar av året 2003 arbetade han även som domare i Svea Hovrätt, Stockholm. I dag arbetar Per åter som advokat på Advokatfirman, Hantverkargatan 78, Stockholm.

När vi frågade Per om han kunde tänka sig ställa upp på denna intervju var det hans samlade erfarenheter från de olika sidorna i rättskedjan som var av intresse för vårat arbete. De svar som Per gav oss på våra frågor i denna intervju grundar sig dock till största delen från hans erfarenheter i rollen som brottsmålsadvokat.

Pers kunskaper om modern IT-teknik är begränsade, vilket är signifikativt för stora delar av personalen som i dag arbetar som åklagare, brottsmålsadvokater och domare. Per berättade att han ser sig som tillhörande den generation som inte fötts upp med modern IT-teknologi. För Pers del utgör ett loggutdrag från en användares aktiviteter i ett system som mycket svårangripligt om det åberopas som bevis. I loggutdraget anges rad för rad vilka aktiviteter en användare utfört i ett eller flera system, och för att kunna ifrågasätta detta krävs en kunskap som i normala fall inte finns bland de aktörer som förekommer i en svensk domstol. För att angripa ett loggutdrag krävs därför expertkompetens, något som är dyrt för försvaret om denna kunskap åberopas från deras sida.

Per har inte någon större erfarenhet av ärenden där loggar utgör en del av bevisningen mot en misstänkt person. Han erinrade sig tre fall där han ur minnet kunde berätta att loggar förekommit i förundersökningen/huvudförhandlingen och att det i ett fall var diskussion om loggens äkthet. För närmare information om dessa ärenden hänvisar han till förundersökning och dom. Två av ärendena härrör från polisens nät medan det tredje utgörs av ett ärende där en man påstods ha lagrat barnpornografiskt material på sin dators hårddisk.

När det gäller de två ärenden som avser poliser nät, så avser dessa två ärenden personer som påstods ha överträtt sina befogenheter. I det ena fallet var det en kvinna där loggen visade att denna slagit i olika register på grannar och på sonens vänner. Kvinnan förnekade att hon utfört dessa slagningar, men dömdes för tjänstefel i Tingsrätten. Man ifrågasatte inte från något håll riktigheten i de loggutdrag som visade kvinnans aktiviteter i aktuella system utan kvinnan dömdes mot sitt nekande.

Det andra ärendet är en manlig kommissarie som slagit i olika polisiära system som allmänna spaningsregistret (ASP) och misstankeregistret. Den här mannen misstänktes för att ha slagit i systemen av rent privat intressen i syfte att smutskasta en annan person, men som själv hävdade att slagningarna var motiverade ur ett tjänsteperspektiv. Den mannen friades från misstankar om tjänstefel.

I ärendet med kommissarien användes aldrig loggen som något bevis i och med att det inte fanns någon anledning att ifrågasätta loggen, då mannen medgav att han utfört aktuella slagningar.

Det tredje ärendet bör vara intressant för intervjuarnas frågeställningar. Det utgjordes av en man som i Tingsrätt och Hovrätt påstod av ICQ-loggar och säkrad e-post från hans dator var manipulerade.

I och med att mannen hade den åsikten gjordes en närmare utredning där man från försvarets sida anlitade expertkunskap. Detta blev dyrt men var nödvändigt i och med den åtalades inställning.

Brott som barnpornografi innebär att den misstänkte tilldelas en offentlig försvarare, och förutsättningarna för att kunna göra egna efterforskningar, trots ökade kostnader, ökar väsentligt i och med att stora delar av kostnaderna därmed faller på staten i stället för på den enskilde. I det här fallet anlitade försvaret en egen expert inom aktuellt område.

I Tingsrätten, där domaren var en yngre man, framkom det att denne förstod resonemanget från försvarets sida, och bland annat återspeglade det sig i domen från Tingsrätten där mannen friades från delar av den del som avsåg barnpornografiska bilderna på datorns hårddisk.

I Hovrätten var domaren äldre, och det framstol här lika tydligt att domaren inte förstod den diskussion som parterna förde i rättssalen. Bland annat vittnade en polisman vid man Jim från Länskriminalens strategiska avdelning, och det blev en diskussion om loggar och säkrat material mellan parterna som var mycket svår att förstå. Per beskrev den tekniska diskussionen mellan åklagarens expertis och föresvarets egen som en diskussion som fördes ovanför domstolarnas och advokatsidans horisont. I Hovrätten dömdes mannen för de åtalade brotten.

Detta får exemplifiera det snabba genomslag som IT-tekniken har fått i dagens samhälle. I dag krävs det specialkunskaper för att kunna hantera sådana här mål. Normalt vill man kunna förstå den bevisning som åberopas, även om den inte har tagits fram av en själv. När det gäller sådana här ärenden är det besvärande då man inte behärskar sina vapen, i det här fallen själva tekniken.

Ett fingeravtryck är lättare att förstå, det har avsatts av en individ och säkrats med en beskriven och erfaren metod, för att sedan ha blivit identifierad av en specialutbildad tekniker. I slutändan kan utlåtandet kontrolleras i och med att det finns ett säkrat och jämförelseavtryck att jämföra med. Hela händelsekedjan är känd och dokumenterad sedan långt tidigare, och metodens svagheter kan ifrågasättas eftersom de är tämligen lätta att förstå. När det gäller IT-relaterad bevisning är varken kedjan eller tekniken känd, och för att kunna ifrågasätta den krävs en kompetens som normalt inte finns bland dagens aktörer i en domstol. Ett problem i det här fallet är att brott som olaga dataintrång normalt innebär att den åtalade inte tilldelas en offentlig försvarare, varför den åtalade många gånger står ensam, eller i bästa fall med ett eget juridiskt ombud i en rättegång.

När vi gick in på frågor som om det händer att man frågar vilken form av autenticeringsteknik som använts för de system som loggarna avser så svarade Per nej. För egen del känner han inte till de olika teknikerna för hur en användare kan bevisa att denne är den som han/hon utger sig för att vara, vilket är ett måste för att kunna ställa en sådan fråga.

Per har heller inte varit med om att man någon gång från någon sida (åklagare, domare eller advokat) ställt frågor om informationens väg när det gäller loggen som bevisning eller underlag för en utredning eller huvudförhandling. Sådana frågor ställs i dag inte beroende på att datorkunskapen är så rudimentär hos alla befattningshavare som i dag arbetar i rättskedjan. Man vet inte hur man skall ifrågasätta ett sådant skriftligt bevis som en logg. Det är ungefär som med DNA, men vet inte hur man skall ifrågasätta det heller. Man kan angripa var DNA har hittats, men inte tekniken för hur DNA pekar ut en viss individ.

Intervjun slut klockan 14.20

Bilaga D

Intervjuer: Informationssäkerhetsområdet

Intervju

Person: **André Richardsson, IT-säkerhets konsult**
Plats: **Ekelöw Infosecurity, Rökubbsgatan 6, Stockholm**
Tidpunkt: **6 Maj, 2004 Klockan 10.00 – 11.45**

André Richardsson arbetar som senior informationssäkerhetskonsult vid Ekelöw Infosecurity AB som har sitt huvudkontor på Rökubbsgatan 6 i Stockholm. I sitt arbete har André kommit i kontakt med många utredningar där företag och organisationer anlitat extern hjälp eftersom de misstänkt att deras system blivit hackade eller på annat sätt manipulerade.

Intervjun med André inleddes med en kort koncis fråga. Kan man lita på en logg? Svaret på den frågan blev från Andrés sida blev ett tveklöst nej. När vi bad honom precisera sig och berätta varför man inte med automatik kan lita på en logg gav han följande förklaring.

Sett ur ett tekniskt perspektiv lagras loggar i allmänhet på en hårddisk på en server. I allmänhet är det även så att systemet som genererar loggarna körs på samma server. För att detta skall vara möjligt krävs det att det finns minst en person som har fullständig behörighet att kunna göra allt på maskinen, nämligen administratören.

En administratör kan göra allt på en server. Det innefattar åtkomst till loggfiler som ligger lagrade på servern. Även om dessa till en del skyddas av operativsystemet när det är i gång, så finns det mängder av mjukvara tillgänglig på Internet som går under ”rootkit” som gör att man kan komma åt och förändra eller förstöra informationen i loggfilerna. En administratör kan med dessa rootkits göra precis allt som har med påverkan av loggar att göra.

Om någon gör ett intrång i på en server hör det till att man döljer sitt intrång genom att manipulera med systemets loggfiler. Det finns ofta ingenting som skyddar loggfilerna, utan de lagras på servern i klartext. I bästa fall kan de vara skyddade med CRC32, vilket medför integritetsskydd av filen, men sällan mer än så. Däremot finns det tredjeparts verktyg på marknaden som skyddar loggfilerna bättre. Om dessa används kan man ge loggfilerna ett bättre integritetsskydd.

André säger under intervjun att det är omöjligt att garantera en loggs äkthet om loggen lagras på samma hårddisk som systemet körs på. För att ha en chans att skydda loggen måste den transporteras till en annan dator där administratören för systemet som genererat loggen inte har åtkomst till systemet som lagrar loggen och tvärt om. Om loggarna ligger lokalt i det system som kan attackeras så kan man inte lita på dem. Däremot kvarstår dock problemet med den administratör som administrerar servern med loggarna. Även den administratören kan använda sig av rootkits eller sin behörighet för att ändra och manipulera bland loggarna. Både de som genereras av serverns operativsystem, och de loggar som servern lagrar för andra system.

Eftersom det alltid går att komma åt och manipulera en logg av den eller de som har legal eller illegal åtkomst till servern som lagrar loggarna så kan man inte utan vidare lita på att dessa är korrekta. Av den anledningen måste därför maskinen skyddas rent fysiskt. Loggarna kan dock även kommas åt via nätverket om det finns möjligheter att göra det på grund av att servern har vissa åtkomliga tjänster. För att skydda servern som lagrar loggarna via nätverket måste man bygga upp ett skydd som gör att det inte går att ta sig in den vägen. Det kan ske med traditionell brandväggsteknik eller om man kan bygga in en lösning som innebär att trafiken är enkelriktad, t.ex. överföring av loggar i ett switchat nät med transportprotokollet UDP som inte kräver ”ackar”.

De verktyg som André inledningsvis talar om är så kallade rootkit. Ett rootkit utgörs av färdigskrivna program eller script som tagits fram för att dölja ett intrång på en maskin så att man kan behålla access till maskinen i fråga utan att upptäckas. Dessa finns för både Windows- och Linuxvärden. Exempel på saker man kan göra med rootkits är dölja processer, dölja inloggade användare, tcp / udp connections, kataloger / filer osv. Möjligheterna är oändliga.

Ett rootkit innehåller vanligtvis nätverkssniffers, verktyg för att radera loggen, trojaner och utbytbara systemverktyg som netstat, ifconfig, ps och killall. Genom att t.ex. byta ut netstat mot en egenskriven döljs pågående processer och aktiva portar eftersom den utbygga netstat inte kommer att visa annat än en del av de aktiviteter som pågår i datorn. Valde delar döljs.

En förutsättning för att kunna installera dessa rootkits är att angriparen först lyckats ta kontroll över en dator. För administratören är detta naturligtvis ingen konst i och med att denne redan har tillträde till servern. Andra som inte är innehavare av adminbehörigheter måste först göra sig till administratör. För detta finns det andra verktyg som t.ex. Peter Nordahls bootbara programvara som gör att man kan boota om en Windowsmaskin och därefter byta ut adminlösenordet. [84] Rootkits finns för de flesta OS, vanligast förekommer de dock för Unixbaserade system, men de finns även för Windows. Exempel på rootkits är:

- Knark (rootkit för Windows)
- SucKIT
- slapper

För att exemplifiera vad man kan göra med ett rootkit återgav André en utredning som han för en tid varit med om och som slutade med att man hos ett företag hittade ett antal rootkits installerade i en av företagets servrar. Av allt att döma hade dessa rootkits installerats av någon administratör eller någon annan som haft fysiskt tillgång till servern.

En ond administratör kan installera ett rootkit direkt på maskinen utan att det upptäcks. De processer som man sedan vill köra på serven kan köras lokalt eller via nätverket eftersom en del av verktygen som följer med vid en installation medger remote access till maskinen, något som inte en syns om man kör en netstat fråga på servern.

Man kan inte utan vidare upptäcka att en server som är ”rootad”, dvs en server som är installerad med rootkit. För att upptäcka någonting sådant krävs för vissa rootkits att hårddisken först speglas för att därefter undersökas från en annan dator.

[84] http://home.eunet.no/pnordahl/ntpasswd/

En fråga som André ställer sig är hur det kan komma sig att man som administratör oftast ses som en helt oantastlig människa. En administratör ges behörigheten att kunna göra precis allt på en dator, oftast utan att man ifrågasätter det eller bygger in andra kontrollåtgärder för att övervaka dennes aktiviteter. Eftersom en administratör, eller en person som gör sig till administratör på en dator, kan göra precisa allt så talar logiken för att en logg därmed inte med automatik kan vara någonting som man kan lita på. För att höja tillförlitligheten till en logg måste man därför utföra en rad åtgärder.

Loggservern skall ligga på ett separat nät som är skilt från it-enheten och dess administratörer som skapar dem. Det skall aldrig vara samma administratör som hanterar loggar i den delen av nätet som lagrar loggarna och de system som skall övervakas och tvärtom. Loggskötarna skall ses som revisorer och skall ej ha behörighet över de system som loggarna genereras ur och tvärtom.

Ett bra loggsystem krävs externa loggservrar. Dessa skall vara konfigurerade så att de inte skall kunna kommunicera ut på nätet. UDP skulle kunna användas i och med att man i ett switchat nätverk endast har marginella kollisioner. Vidare måste loggarna kunna skyddas under transporten i nätverket mot manipulation. Det finns verktyg som signerar och krypterar alla loggposter, men den process som styr detta kan stängas av utav den som äger maskinen, dvs administratören. Det gamla talesättet ”skit in och skit ut” är en verklighet även här.

För att försvåra, och därmed höja sannolikheten att en logg är riktig, för behöriga eller obehöriga att kunna påverka loggarna är det en lämplig åtgärd att låsa in dessa i ett låst utrymme. Detta skulle kunna vara någon form av bur som i sin tur videoövervakas. Åtkomsten till buren med servern/servrarna skulle kunna vara kopplat till samma säkerhet som smartkortsinloggnig eller liknande. Tillsammans med manuella rutiner som tvåhandsfattning och drifthandböcker ger ytterligare kontroll över vem som gör vad och varför på någon av dessa servrar. Med tvåhandsfattning avses minst två administratörer som endast känner till halva delen av ett admin lösenord.

Ett sätt att minska loggarnas tilltro, eller till och med göra dem värdelösa, vore att manipulera med systemtiden. Genom att ändra systemtiden i loggenererande system blir det näst intill omöjligt att ”mappa” ihop loggarna om man har behov av att följa en användares aktiviteter i olika system.

Det finns speciell programvara som är framtagen för att kontrollera om en server är ”rootad”. Dessa programvaror kommer inte att kunna upptäcka alla rootkits, men det finns framtaget för upptäckt av vissa. Ett annat sätt man kan göra för att vara säker på att vitala systemfiler inte blivit utbytta i samband med installation av något rootkit, är att man i samband med en riktig installation beräkna kryptografiska checksummor av dessa filer och därefter lagra dessa på ett säkert ställe, t.ex. på en CE-skiva som låses in i ett kassaskåp. Med jämna mellanrum, eller i samband med misstänkta intrång, skullem men med en sådan åtgärd ganska lätt kunna säkerställa att vissa vitala systemfiler inte bytts ut. Man får då åter komma ihåg att det är en administratör som skall utföra detta arbete, och om det skall gå att lita på dennes utsaga att servern inte är manipulerad så måste man även kunna lita på administratören.

Enda sättet att vara riktigt säker på att man fått bort alla rootkit, om något sådant skulle upptäckas, är att göra en riktig ominstallation från ursprunglig originalmedia.

André ser inte loggen som ett bevis, utan något som indikerar att någonting har hänt. Bevisen måste man därför hämta från den dator varifrån trafiken genererats. Genom att undersöka den datorns hårddisk kan man hitta sådana spår på hårddisken som styrker det som loggarna påstår. Därmed har man information från två olika håll som styrker varandra. Fortfarande har man dock inte med automatik pekat ut en enskild människa, utan i detta fall den aktuella datorn varifrån trafiken genererats. Andra utredningar får sedan styrka vem som nyttjat datorn för aktuellt ändamål. Ledning för detta kan man då finna i t.ex. inpasseringssystem, om sådant finns, för att påvisa om aktuell person befann sig på arbetet denna dag eller ej.

Kan man inte styrka loggen med spår från användarens dator ser André inte att en logg kan användas för att bevisa en enskild användares aktiviteter eftersom dessa lika gärna kan vara genererade eller editerade av en administratör eller annan person som har tillgång till loggfilerna. Man får heller inte glömma bort att ett papper som utgör en utskrift av en logg i sin tur kan skrivas av, och i samband med det få sitt ursprungliga innehåll förändrat.

När man talar om administratörens möjlighet att förändra loggarna, eller andras möjlighet att göra det via rootkit, så spelar själva autenticeringsbiten ingen större roll. Om en användare loggat in i ett system med användarnamn och lösenord eller om denne loggat in med hjälp av ett smart kort och en challenge – responsmetod, så kvarstår fortfarande administratörens eller den som tagit över maskinerna möjlighet att manipulera loggarna. Sett i perspektiv utan hänsyn till administratörer eller de som tagit sig åtkomst till servrarna via rootkit, så är naturligtvis en logg som bygger på användarnamn och lösenord svagare än en som bygger på starkare autenticering, men frågan om man kan lita på en logg måste ses ur ett helhetsperspektiv, och då får dessa metoder mindre betydelse om man inte säkrat upp loggarnas transport och förvaring på ett säkrare sätt.

André ställde frågan om alla loggsystem i sig är felfria. Kan man alltid lita på att en logg genererats korrekt? Kan man garantera att systemen inte har buggar som visar sig i vissa sällsynta fall? André berättade om en tvist mellan en bankkund och en bank som skulle avgöras i rätten i ett annat land. Banken hävdade att deras system var säkert varpå kunden begärde att få ta del av den säkerhetsgranskning som måste ha gjorts för att kunna påstå någonting sådant. Detta vägrade banken att lämna ut vilket medförde att banken förlorade. Något att tänka på.

André har haft utredningar där man kommit fram till att det av allt att döma varit en viss administratör som orsakat en loggad aktivitet i ett system, och inte den användare som loggen pekade ut som varande den som förorsakat trafiken. Det gick aldrig att leda i bevis, men vad det hela gick ut på var att administratören bytte ut lösenordet för en användare till ett som denne skrev in. När det var gjort, vilket var möjligt då administratören kan göra detta, så gick administratören in med användarens identitet. I loggarna såg det då ut som om det var användaren som gjort aktuell slagning, men i själva verket var det någon annan som använde sig av användarens identitet. I det här fallet en administratör som bytt ut det gamla lösenordet till ett nytt. Kontot var därmed övertaget av administratören och loggarnas betydelse var helt satt ur spel. Även om det inte gick att leda i bevis vem det var som gjort denna förändring så visar den ganska klart på att sådana saker händer, och i och med att de har hänt så kommer de att hända igen, och därför kan man med automatik inte lita på en logg.

Kan man då inte skapa en säker logg? André säger att man i dag knappast kan göra det. I grund och botten är processarkitekturen i en dator felkonstruerad för detta. Det är fel att övervara processerna i en maskin och samtidigt lagra loggarna i samma maskin. Allt exekverar i samma system, och det finns inget skyddat minnesutrymme. En lösning vore att skapa multipla servrar där användarna bara tillåts prata med så kallade front ends servrar där användarnas program exekveras, och aldrig direkt med bakomvarande servar där loggarna lagras. Kvar finns dock problemet med administratörerna.

En annan lösning är att sprida ut arkitekturen så att man ha en autenticeringsserver, en server för åtkomst och en annan för loggning. Gör att sopa igen spåren efter sig vid ett intrång måste man därför ge sig på flera servrar, vilket skulle försvåra.

Därmed blir systemen mindre sårbara för dessa aktiviteter genom att komplexiteten i systemen kommer att medföra att en elak administratör eller obehörig därmed kommer att få det svårare att dölja sina aktiviteter. En logg som styrks av en annan logg är också någonting som ökar loggens tilltro. Loggarna skulle på så sätt stödja varandra.

Det går inte att föra en sådan här diskussion om man inte tar upp ämnet trojaner. En installerad trojan skulle kunna ligga och köra på användarens dator utan att denne är medveten om det. Trojanen skulle kunna vara skriven på så sätt att den gör det möjlig för någon att via nätverket accessa användarens klient, för att på så sätt låta inkräktaren utföra slagningar i olika målsystem, vilka därmed skulle loggas på användaren. Loggarna kommer tveklöst att peka ut användaren, utan att det är användarens om gjort slagningen. Det kommer att kunna bevisas att denne var på arbetet, satt vid sin dator, och varför skulle användaren därmed inte ha utfört dessa slagningar? Där ser man var en logg skulle kunna vara värd. I och med att detta är möjligt måste det kontrolleras om det funnits en trojan på användarens klient för att loggen skall ha någon som helst tillförlitlighet.

Att ta sig in i system med hjälp av trojaner är det i särklass vanligaste sättet i dag. Trojanen öppnar vägen genom brandväggen genom att trafiken initieras inifrån och kanske bundlat till ett protokoll som SMTP och port 25 eller HTTP och port80.

André avslutade intervjun med att berätta att han under sitt arbete som konsult kommit i kontakt med olyckliga informationssäkerhetschefer som inte fått gehör för de faror de identifierat inom sina organisationer. För att konkretisera det hela har de initierat ett angrepp för att göra hoten synliga, och därmed själva fått sparken. Ett exempel är Sveriges Riksdag där en ansvarig person varnat för mailsystemet som byggde på SMTP. Den kräver ingen autenticering för att skapa ett mail, men ingen lyssnade. Till slut skrev han ett mail till Thorbjörn Fälldin i en annan Riskdagsledamots namn med ett innehåll som avsåg Öresundsbron. Det blev ett oerhört liv och personen som skrev mailet fick sparken.

Intervjun slut klockan 11.45

Intervju

Person: **Mats Söderholm & Mattias Olsson, FKC AB, IT-säkerhets konsulter**
Plats: **Polhemsgatan 32, Stockholm**
Tidpunkt: **12 Maj 2004 Klockan 13.15 – 16.20**

Mats och Mattias arbetar som säkerhetskonsulter och har under många år arbetat med frågor som bland annat handlar om hur man skall skapa så säkra och trovärdig loggar som möjligt. Tillsammans driver de det egna företaget FKC AB. Det är bland annat i samband med uppdrag åt försvaret som de har engagerats i frågor som berör säker logghantering.

Intervjun inleddes med att Mats och Mattias tillfrågades om man kan lita på en logg. Båda svarade inledande med att man inte utan vidare kan göra det. På frågan varför berättade de följande.

För loggar som skapas av operativsystem som har en högre klassificering enligt ”The Orange Book”, som C-2 system, så skyddas dessa loggar av operativsystemet. Kravet på dessa operativsystem är att loggarnas integritet skall vara garanterad till en viss nivå. Dessa loggar måste förr eller senare överföras till ett annat lagringsmedia. Annars kommer loggarna till slut att skrivas över. Ett grundläggande krav i samband med denna överflyttning är att skydda loggarnas integritet, dvs att i samband med denna överflyttning skydda dem mot förändring eller att man kan skriva extra loggar eller att radera vissa av dem.

Oavsett hur det går till nr dessa loggar överförs till ett annat lagringsmedia så måste man ställa sig frågan vad det är som gör att man kan garantera att samtliga loggar förts över och att inte vissa av dem försvunnit under denna hantering. Vidare måste man ställa sig frågan hur dessa loggar skyddas i nätverket under överflyttningen till sin nya lagringsplats. Om loggarna skrivs in i en databas kan de t.ex. manipuleras med SQL-kommandon som ”update” och ”delete”.

Vad som också påverkar trovärdigheten av loggarnas innehåll är hur autenticeringen av användarna har gått till. En logg visar vad som skett, inte vilken fysisk människa som gjort vad. Kan man verkligen lita på att det är användare A som loggat in i systemet eller kan det vara som så att någon utgivit sig för att ha varit användare A. Kan användare A ha lånat ut sin identitet eller inloggningsutrustning (smarta kort) till någon annan eller kan någon annan ha ”snappat” åt sig lösenordet vida nätverk eller genom att kika över axeln när användare A loggat in, för att sedan använda sig av dessa uppgifter och logga i med A:s lösenord eller annan inloggningsutrustning. Kan man angripa trovärdigheten hos en logg beroende av för svag autenticering spelar det ingen roll hur starkt skydd man byggt in i servrar och vilka administrativa säkerhetslösningar man tagit fram för att kompensera administratörernas potentiella hot. Kan man inte lita på inloggningsmekanismerna eller att autenticeringen är för svag (lösenord) kommer loggen att kunna ifrågasättas även om det som loggats är helt korrekt.

Vidar måste man ställa sig frågan vad man har för säkerhet i nätet? Går det att koppla in ny hård- och mjukvara i nätet och lyssna av trafiken och går trafiken i klartext eller är den krypterad. Ofta kan man lita på en BKS, men vad är det som har skett innan en användare kommer dit.

Hos vissa operativsystem är loggarna till en början alltid skapade i binära format. Så är fallet t.ex. hos Solaris och NT. Olika organisationer har krav på att lagra loggarna i olika lång tid. För försvaret finns ett krav på loggarna skall lagras och vara läsbara i 25 år. Det innebär att man som regel konverterar bidnära loggar till textformat så att man kan garantera att dessa är läsbara för eventuella framtida bruk. Om man inte gör denna konvertering måste man lita på att man har kvar sådan programvara som i dag kan läsa binära loggar även i framtiden. Det är inte utan vidare en självklarhet att man har kvar applikationer som kan läsa alla binära loggformat om 20 till 25 år.

Vissa loggar som systemloggar genereras som regel i textformat, och att loggar har olika format är något som försvårar för vidare logganalyser. Till detta tillkommer att en användare kan ha olika identiteter i olika system. Det skulle kunna vara en självklarhet att kräva att användarnamn alltid skall vara ett och samma värde, som personnummer eller ett annat unikt värde, men vissa operativsystem som t.ex Unix klarar inte av användarnamn som börjar med en siffra.

När vissa loggar genereras med IP som användarnamn, andra med personnummer och ytterligare andre med annat prefix blir analysen svår. Ofta kan det vara en nödvändighet att korsköra loggar från olika system, och då måste man kunna binda en användare till olika användaridentiteter. Här blir systemklockan en viktig del eftersom en systemklockan som inte är gemensam kommer att ytterligare försvåra eller tillintetgöra möjligheten till att visa eller fastställa en viss användares rörelser i olika system. Vissa system loggar tidsangivelsen ner till hundratusendels sekund. Frågan som uppkommer är hur stor tidsskillnad som en organisation kan acceptera för att loggarna skall kunna användas för det som de är till för.

System som var för sig genererar sina loggar bör samlas in centralt för att kunna hanteras i en central loggdatabas. För att dessa loggar skall kunna hanteras krävs en gemensam systemklocka. Hur säkrar man att tiden distribueras till samtliga system.

Det är ingen skillnad mellan loggar och annan information som lagras i ett system. Båda typerna av information måste kunna skyddas med samma styrka. I sig är en logg inte speciellt hemlig eftersom den som regel inte innehåller något som visar vilken information som behandlats när loggen skapades. Däremot är loggens integritet viktig att skydda.

En viktig fråga som man måste ställa sig är om man loggar rätt saker. Vad som är rätt information att logga varierar naturligtvis från system till system, men frågan är viktig eftersom det är lätt att ”drunkna” i för mycket information. En logg kan även tillmätas mindre värde beroende på att man valt att logga fel saker.

För att en logg skall kunna tillmätas någon form av betydelse gäller det att man kan lita på autenticeringen. Den måste vara tillräckligt stark och står i förhållande till det som systemet skall skydda. I vissa fall, där informationens klassificering är tillräckligt låg, kan det vara befogat att endast använda sig av användarnamn och lösenord.

Ett sätt att skydda loggarna är att använda sig av tekniker som signering, kryptering, administrativa rutiner som tvåhandsfattning, att skriva direkt till media som inte går att radera, att använda sig av transportprotokollet UDP så lite som möjligt, att fysiskt skydda servrarna som lagrar loggarna och att begränsa administratörsrättigheterna.
Om loggarna överförs till ett annat lagringsmedia så kan detta ske antingen i realtid eller vid vissa fastställda tillfällen. Dessa kan ske efter viss tid eller när en viss loggmängd genererats. När man skickar över loggarna till sin nya lagringsmedia måste det till någon form av mekanism som skickar en kvittens som säger att mottagarsystemet tagit emot loggen och att den kommit fram oförändrad. Först därefter kan loggen i det system som skickat den raderas.

Det gäller att man kan lita på denna mekanism, och att man kan hantera den eller de som har rättigheter att stänga av denna mekanism. Här gäller det även att kunna garantera att systemet som skickar loggarna skickar till rätt mottagarsystem, och att systemet som tar emot loggarna vet att loggarna kommer från ett system som har rätt att skicka loggar. Det krävs med andra ord en ömsesidig autenticering mellan dessa två system.

Man måste skydda överföringen mellan systemen som skickar loggarna och mottagarsystemet. Loggposter kan bytas ut under transport i nätverket. Man kan skapa falska loggposter som skjuts in i målsystemet för att uppnå vissa önskade effekter, något som skulle kunna skjuta hela trovärdigheten i det centrala loggsystemet i sank. Sådana aktiviteter kan ske om det är möjligt att koppla in otillåten mjuk-och hårdvara i nätet mellan sändande och mottagande system.

En lösning på kravet att skydda loggarnas integritet är att signera dessa. Frågan som uppkommer är om varje enskild loggpost måste signeras eller om det är möjligt att samla ihop flera loggar och skicka iväg dessa vid ett och samma tillfälle och skapa signaturen då denna informationsmängd i stället för på varje logg. Om loggarna skall skjutas iväg i så nära realtid som möjligt uppkommer frågan hur nära denna realtid är. Organisationen som genererar dessa loggar måste själva ta ställning till dessa frågor.

En viktig sak som berör administratörerna är separering av administratörsrollerna. Ingen skall tillåtas vara administratör på allt. En uppdelning som innebär att en administratör administrerar säkloggen, en annan behörigheter och en tredje driftrelaterade händelser ökar säkerheten eftersom dessa då endast har åtkomst och kontroll inom sina områden. Det skall vidare vara skilda roller mellan dem som sköter systemen och nätverken och de som har till uppgift att hantera och analysera loggarna. Anledningen är naturligtvis att man vanligtvis vill dölja ett intrång i systemmiljön genom att radera loggarna. Är dessa skilde åt rent fysiskt och administratörsmässigt blir det mycket svårare att göra dessa förändringar bland loggarna.

Vidare kan man kräva förstärkta inloggningsskydd för administratörer som skall logga in på servrarna som utöver något som administratören kan även innehåller något som administratören har. T.ex. smarta kort med tillhörande PIN-kod.

Till administratörerna kan man koppla många administrativa regelverk som t.ex. tvåhandsfattning som innebär att en administratör endast känner till halva delen av ett lösenord. Vidare kan man kräva att administratörerna för manuella driftloggar där man skall ange syfte med vad man gjort, och naturligtvis vad man gjort. Enskilda maskiner kan låsas in i burar och burarna kan övervakas. Endast vissa skall ha åtkomst till dessa, och när så sker skall detta bevakas t.ex. via video från en övervakningsenhet.

Genom att bygga upp denna kedja av tekniska och administrativa regelverk kan man på ett mer genomtänkt sätt säkra upp vad det är som administratörerna kan göra. Allt som dessa gör skall sedan loggas på ett sätt att var och en av dessa inte har åtkomst till, eller möjlighet till att manipulera med de loggar som de genererar.

Vissa operativsystem ger stöd för en uppdelning och begränsning av administratörernas rättigheter där en grundtanke är att ingen skall vara total administratör och på detta sätt ha tillgång till allt. Exempel på sådana operativsystem är Trusted Solaris, HP som har en egen variant av ”trusted system”. AEX (IBM) och SE Linux som tagits fram av NSA. Det har börjat komma fram fler tillverkare som säljer ”säkrare” operativsystem där man lagt viss del av fokus på administratörsrollerna.

När man gör denna uppdelning kommer detta naturligtvis i strid med termer och verklighet som budget. Det kostar att ha flera administratörer än en, och i vissa fall kan man tänka sig att de olika administratörsrollerna går att kombinera så att en har flera roller.

Ytterligare en form av begränsning är att styra så att det endast är möjligt att logga in på vissa servrar från annat än vissa IP-segment. Utöver detta kan man konfigurera switchar och routrar så att dessa inte släpper igenom t.ex. FTP och det inte är som så att FTP är något som behövs.

Det är väldigt viktigt att en server konfigureras på rätt sätt. En felaktigt konfigurerad server kan medföra oerhörda säkerhetsluckor. Av den anledningen kan det vara klokt att inte släppa in en server i driftnätet förrän dess konfiguration noggrant testats i ett testnät. Detta kräver att man har ett testnät skilt från driftnätet. I vissa fall kan det till och med vara nödvändigt att ha ett mellanliggande nät som i sig är skilt från både drift och testnät. Där kan mer omfattande tester ske för att validera att den hård-och mjukvara som skall installeras i driftnätet är rätt konfigurerad. En del av konfigureringen går naturligt vis ut på att tjänster som inte skall användas inte skall finnas installerade, och att de som skall användas är rätt konfigurerade. En riktigt kontrollerad konfiguration innebär en checksummekontroll av varje binär för att säkerställa att endast rätt programvara installeras.

Både Mats och Mattias är överens om att den som rent fysiskt har tillgång till en dator i regel kan göra vad som helst. Man kan då byta diskar, ta en image av en disk för att i lugn och ro analysera den och sedan återkomma och utnyttja de svagheter man hittat. Om man kan boota om maskinen med annan bootbar programvara, och på så sätt gå runt det skydd som operativsystemet i normala fall utgör, kan man göra inställningar som påverkar säkerhetsinställningar samt installera främmande programvara. Med rätt programvara kan man även manipulera maskinen så att man kan logga in som root, med allt som detta innebär. Med andra ord så kan en angripare göra i stort sett vad som helst bara denne har fysisk åtkomst till maskinen.

Det är ur detta perspektiv man måste betrakta administratörerna. Dessa har samtliga fysisk tillgång till ett antal maskiner, och av den anledningen måste man även begränsa deras fysiska till gång till att endast omfatta de maskiner som ligger inom deras ansvarsområde. Därför är det administratörerna som utgör det största säkerhetsrelaterade hotet i och med att de i sitt arbete som regel har fysisk åtkomst till en stor del av maskinvarorna som loggarna passerar eller ingår i.

Genom att fysisk åtkomst till maskinvaran sätter flertalet skyddsåtgärder ur spel så ingår det som en del att skydda maskinvaran rent fysiskt på så sätt som tidigare anförts i denna intervju.

Intervjuarna ställde frågan om det är möjligt att skapa en hundraprocentigt säker logg. Svaret på frågan blev nej och en motfråga med innehållet om det är nödvändigt att ha ett sådant krav.

Anledningen till Mats och Mattias svar att det inte går att skapa en hundraprocentigt säker logg är att det alltid kommer att krävas mänsklig inblandning i logghanteringen som administratörer och användare som slarvar med sina lösenord eller sin inloggningsutrustning. Det går alltid att manipulera den programvara som någonstans kommer att hantera loggarna. Likaså är det svårt att förhindra fysisk åtkomst till datorer som är bärare av applikationer eller databaser.

En helt säker logg bygger vidare på det faktum att ett operativsystem som t.ex. Unix installerats helt enligt installationsanvisningar och fastställd konfigurering. För att garantera detta skulle man vara tvungen att ha kontrollerat varje binär med checksummor så som tidigare angivits. Den pålitliga maskinen skall då kopplas till nätet, men frågan är då vad som finns i nätet.

Om man flyttar fokus från loggarna till själva logganalysen så blir frågan vad som skall loggas en viktig fråga. Den frågan skall besvaras utifrån vad det är man vill veta och något som skall anpassas för system till system. Strävan är att logga ner på individnivå, vilket kräver mer än endast lösenord. En förstärkt inloggning som bygger på någonting som användaren kan och har innebär som regel PIN-kod och smart kort. För att komma längre än så krävs någon form av övervakning som kan ge spårbarhet att det inte endast var användarens smarta kort som loggat in i systemet, utan även att någon kan intyga att en unik person låg bakom inloggningen tillsammans med kort eller lösenord. Detta kan ske med videoövervakning eller tvåhandsfattning.

Med stora mängder loggar är det inte svårt att ta fram vad N.N har gjort. Svårigheten med att ta fram information i en miljö med stora mängder loggar är däremot att ta reda på vad användarna gjort i systemet med utgångspunkt att man söker den eller de som överträdd sina befogenheter eller på annat sätt gjort otillåtna slagningar. För att klara av det kan det vara en idé att ta med sig lite annan kunskap in i analysförfarandet. Både Mats och Mattias har ett förflutet med Data Ware housing teknik. Dvs teknik som bygger på möjligheten att ta fram statistik och annan information från affärssystem.

Så kallade Data Mining verktyg är verktyg som man med denna teknik kan ta fram som bygger på statistiska avvikelser i systemen som avviker från det som kan anses som normalt. Ett exempel på denna teknik är kortföretagen som kan kontakta en kund med en förfrågan om det stämmer att han ett visst datum gjort ett uttag i ett annat land. Detta sedan systemen upptäckt att denna kund normalt inte reser i detta land. Något som systemen lagrar information om i samband med kundens normala användande av kortet. Ett annat exempel är att ett vanligt beteende för att testa om ett kort är stulet är att man prövar det i en miljö där man inte behöver möta en människa. Att tanka två liter bensin i en automat skulle kunna utgöra ett sådant test. Sedan bär det iväg till en juvelerare där större inköp görs. Enligt Mats och Mattias är detta ett skarpt exempel på hur ett beteende med stulna kontokort kunnat identifierats.

Studier av polismäns beteende i systemen skulle kunna bygga på mönster som att man vanligtvis först söker personnummer för att med detta gå in i andra system och söka information. Vidare skulle antalet slagningar i olika system kunna tas fram som en form av Gaus klocka där ett visst normalt antal slagningar troligen skulle fånga den stora massan av användarna medan några få skulle stå för oerhört stora mängder slagningar och några få för väldigt få antal slagningar. På liknande sätt skulle man kunna bygga upp en statistisk bild av hur vissa användare använder sig av systemen, för att sedan med olika verktyg upptäcka avvikelser från dessa.

Vissa saker kommer alltid att kunna vara möjliga att göra i ett nätverk eller inom ett system. Det finns då en möjlighet att förbjuda användarna från dessa möjlighet och sätta in periodiska eller ständiga kontroller för att se om någon bryter mot dessa regelverk.

Man får inte glömma att det ofta finns loggar att hämta hos andra komponenter i ett nätverk än bara hos klienten och målsystemen. Ett exempel på detta är DHCP servern som kan ställas in att logga vilka MAC-adresser som ropat efter en tilldelad IP-adress. Vidare skulle man denna väg kunna få information om var någonstans en person satt i nätet när inloggningen skedde. Ju fler loggar man har som styrker varandra, desto starkare blir loggarnas budskap.

Genom att samla in loggar från många olika ställen kan man bygga upp en bild som säger mer än bara en logg från ett ställe.

Man kan sammanfatta frågan om trovärdiga och pålitliga loggar med att säga att hela kedjan måste vara säker. För en klient innebär det att klienten inte är bärare av okänd programvara. Av nätet krävs det en arkitektur och en teknisk lösning som innebär att man inte utan vidare kan sniffa nätverkstrafiken utan att nya komponenter i nätverket måste kunna upptäckas eller göra omöjliga att koppla in. Vidare måste man kunna säkerställa att loggarnas integritet kan skyddas i samband med överföring mellan olika lagringsmedier samt att man kan garantera att vissa loggar inte försvinner under transporten. Vidare så måste analysprocessen vara så dokumenterad att om man gör om den skall man kunna garantera att den ger samma utfall.

Flera källor styrker varandra och minskar risken att vissa delar av systemen skull kunna vara påverkade. Autenticeringen skall vara dubbelriktad för att förhindra att användare eller målsystem talar med fel partner. Vidare måste man använda sig av förstärkta inloggning för att styrka utpekandet av att en viss person utfört en viss aktivitet. För att detta skall vara till någon nytta måste man dessutom möta hotet från administratörerna på ett sådant sätt som tidigare diskuterats under denna intervju. Vidare så förekommer det vid all logganalys att materialet på något sätt hanteras manuellt. Det gäller då att man kan beräkna hashsummor på de filer som skall hanteras så att man kan garantera att dessa inte förändrats under hanteringen.

Andra frågor som berördes under intervjun var vem som skall kontrollera den som kontrollerar loggarna och vilka regler som skall styra vad vilken information som logganalytikern skall få ta del av. Ett exempel är om man loggar mailtrafiken, skall då logganalytikern tillåtas ta del av mailets innehåll och eventuella bifogade filer, eller hur skall man lösa den biten.

Intervjun slut klockan 16.20

Bilaga E

Intervjumanual

Intervju manual

- **Hur ser man på bevisvärdet av en logg?**
- **Hur används en logg under förundersökningen, skillnad fu och huvudförhandling?**
- **Har bevisvärdet i en logg någonsin ifrågasatts?**
- **Referens till domar där loggar har använts som bevis eller stödbevis?**
- **Har det ifrågasatts ett diskuterats hur en loggfil har hanterats innan den hamnar hos utredande personal, t.ex. kommer loggarna till polisen på en CD/ROM, hur har loggarna hanterats innan och efter (Lagrats skyddad o.s.v.)?**
- **Om den misstänkte nekar, hur ställer man sig då till en loggs värde. Litar man på den, om inte varför?**
- **Känner du till något fall där en misstänkts fällts mot sitt nekande enbart på loggar?**
- **Har man ifrågasatt värdet av en logg när den lämnas in av annan, t.ex. tekniker på ett företag eller kommun. D.v.s. fall där det inte är polisen själva som tar fram loggmaterialet?**
- **Har man någonsin diskuterat vilken betydelse administratörer har vad gällande äktheten i en logg. T.ex. kan någon annan ha skapat loggen i den utpekades namn?**
- **Hanterar man en loggs värde olika beroende på hur användaren har loggat in i systemet (smarta kort/användarnamn lösenord)?**

Bilaga F

Matris över rättsfall – Interna dataintrång inom polisen

Diarie-nummer	Påföljd			Inställning till delgiven brottsmisstanke			Inställning till logg	
K/B/Al-nummer	Fälld	Friad	Föreläggande	Erkänner	Förnekar	Medger omständigheter	Bestrider	Medger
K 247500-98	X					X		X
K 87667-00			X	X				X
K 239806-96	X					X	X	
K23751-96	X				X		X	
Al 79393000	X					X		X
K 115759-95	X					X		X
K 101663-94		X				X		X
K 107454-94	X					X		X
K 126559-98			X	X				X
Al 79314096	X					X		X
K 106595-97		X			X		X	
K 164344-99	X					X		X
K 238441-00	X			X				X
K 101674-94	X			X				X
B 890-94	X			X				X
K 143209-01		X				X		X
K 268119-02	X					X		X
K162463-02	X					X		X
K156035-00			X	X				X
K 63397-03			X	X				X