Skydd av data på bärbara datorer

En kartläggning av olika lösningar för att förhindra att värdefull information blir stulen[1]

Frida Bergman
Carl Hagström

Institutionen för data- och systemvetenskap
Stockholms universitet / Kungliga Tekniska Högskolan

Juni 2005

[1] Uppsatsen motsvarar 20 poäng för vardera författare

Abstract

Mobile devices are considered to be one of the biggest challenges for IT and information security personnel to manage. Use of their devices is seldom limited to within the office and their connection to the corporate network is sporadic. Laptops have decreased in price and at the same time computing power has increased. This has made them popular to use as the primary work unit. At the same time theft of laptops increases daily. Often these laptops contain secret information. The value of the stolen information often exceeds that of the hardware. That is why methods to protect this information are needed.

The purpose of this thesis is to identify important factors that can influence the choice of one method over another when it comes to protecting information on laptops. This is done through a survey of these methods.

In the thesis a number of strategies for risk reduction, encryption and authentication are discussed. Risk reduction strategies include policies, security standards, user education, alarms and restrictions. Authentication is needed in order to control that the right person has access to the unit and that the person is who he says. This can be done through passwords, smart cards, USB-tokens, one-time passwords and biometrics. Encryption protects the information by making it unreadable to unauthorized users. This can be done through tactic and strategic encryption.

A system is only as secure as its weakest link. Therefore one must see the system as a whole. It is not enough to only use strong authentication and encryption. One should make security thinking a part of the daily routine that must be integrated into every part of the organization.

Sammanfattning

Mobila enheter är en av de största utmaningarna för IT- och informationssäkerhetspersonal att hantera. Dessa enheter är sällan på kontoren och deras uppkoppling mot företagets nätverk är sporadisk. Bärbara datorer har sjunkit i pris samtidigt som datakraften har ökat, det har medfört att de blivit allt mer populära att använda som primära arbetsdatorer. Samtidigt ökar antalet stölder av bärbara datorer dagligen. Ofta innehåller dessa bärbara datorer hemlig information. Värdet på den stulna informationen överstiger ofta värdet på den stulna hårdvaran mångfalt. Därför behöver man skydda denna information från obehöriga. För detta ändamål finns det ett flertal metoder.

Syftet med uppsatsen är att identifiera viktiga faktorer som kan påverka valet av en metod över en annan att skydda data på bärbara datorer med. Detta har gjorts genom en kartläggning av dessa metoder.

I uppsatsen behandlas ett flertal metoder för riskreduceringsstrategier, kryptering samt autentisering. Riskreduceringsstrategier inkluderar policy, säkerhetsstandarder, användarutbildning, alarm och restriktioner. En metod behövs för att kontrollera att rätt personer har åtkomst till enheten och att personen ifråga verkligen är den han utger sig för att vara. Detta kan göras med lösenord, USB-token, aktiva kort, engångslösenord eller biometri. Kryptering skyddar informationen på datorn genom att göra den oläsbar för obehöriga. Detta kan göras med taktisk eller strategisk kryptering.

Ett system är bara så säker som dess svagaste länk. Därför måste man se helheten i systemet. Det räcker inte att enbart satsa på stark autentisering eller kryptering, man bör göra säkerhetstänkandet till en del av vardagen som måste integreras i alla delar av organisationen.

1 Inledning

Detta kapitel ämnar ge läsaren förståelse för problemet och bakgrund i ämnet. Vidare beskrivs syfte, mål samt avgränsningar. I metoddelen redogör författarna hur de skall gå tillväga för att uppnå syftet.

1.1 Bakgrund

Att upprätthålla data och informationssäkerhet är en komplex uppgift som varje organisation måste betänka i dagens affärsmiljö. Stöld av utrustning, misskötsamma anställda, industrispionage och även cyberterrorism händer i en allt mer ökad omfattning [Gordon et al, 2004]. Därför behöver organisationer definiera och implementera policys, procedurer och verktyg som skyddar känslig information från otillåten åtkomst [Symantec, 2004]. Som alla riskhanteringsstrategier måste organisationer väga kostnaderna för säkerhet mot riskerna. Det är den svåraste delen av processen och många företag inser inte hur omfattande och farliga hoten är. Företagen vill hålla kostnaderna nere samtidigt som de vill ha säkra system. Därför försöker informationssäkerhetspersonal att spara pengar åt organisationen genom att implementera säkerhet till lägsta möjliga kostnad [Absolute Software, 2003].

Mobila enheter innebär kanske den största utmaningen för IT - och informationssäkerhets-personal att hantera. Dessa enheter är sällan på kontoren och deras uppkoppling mot företagets nätverk är sporadisk. Bärbara datorer har sjunkit i pris samtidigt som datakraften har ökat, det har medfört att de blivit allt mer populära att använda som primära arbetsdatorer [Spooner, 2003]. Antalet stölder av bärbara datorer ökar dagligen och omsätter idag ca: 7,5 miljarder kronor över hela världen [Utimaco, 2004]. Ofta innehåller dessa bärbara datorer hemlig information [Dean, 2001][Bedell, 2002]. Värdet på den stulna informationen överstiger ofta värdet av den stulna hårdvaran mångfalt [Utimaco, 2004].

En anledning till att intresset för att skydda information på datorer har ökat är lagar och bestämmelser. I USA finns en lag som säger att organisationer som blir av med utrustning som innehåller kunddata måste informera kunderna om vilka uppgifter som hamnat på villovägar. Men om informationen är krypterad slipper organisationerna informera kunderna. [Byttner, 2004]

Företag och organisationer behöver säkerhetslösningar som kan skydda deras information på bärbara datorer. Säkerhetssystemen på de bärbara datorerna måste kunna fungera utan tillgång till det primära säkerhetssystemet och utan tillgång till nätverket. Det är viktigt att man kan identifiera och autentisera användaren även när det inte finns något nätverk tillgängligt. Det är även viktigt att systemet som skyddar datorn är säkert, för att när datorn blivit stulen har angriparen ingen tidsbegränsning för att bryta sig in i systemet. En tredje viktig faktor är att systemet är så transparant som möjligt för användaren och skall ej stå i vägen för användaren när den skall använda datorn - säkerhetssystem är bara så bra som de är funktionella. [Utimaco, 2004]

En kartläggning av olika alternativa lösningar för att skydda data på bärbara datorer behövs för att kunna jämföra deras styrkor och svagheter. I dags dato finns ingen sådan kartläggning och därför har vi fått i uppdrag av Rikspolisstyrelsens informationssäkerhetsavdelning att göra en sådan.

1.2 Syfte

Syftet med uppsatsen är att identifiera viktiga faktorer som kan påverka valet av en metod över en annan för att skydda information på bärbara datorer med. Detta skall göras genom en kartläggning av dessa metoder.

1.3 Mål

Det långsiktiga målet med uppsatsen är att den skall kunna ligga till grund för beslut av säkerhetslösning för bärbara datorer hos företag och organisationer.

1.4 Avgränsning

Vi avgränsar oss till att undersöka lösningar för Windows XP. Detta då vår uppdragsgivare använder Windows XP som primär plattform. Författarna exkluderar hur man skyddar information via nätverket samt skydd av hårdvaran. Detta på grund av att uppsatsen annars skulle bli allt för omfattande.

1.5 Metod

Här redogör författarna för uppsatsens arbetsmetod. Arbetet kan delas in i tre olika faser: litteraturstudie, kvalitativa intervjuer och sammanställning av material.

1.5.1 Metodval

En hermeneutisk forskningsansats har använts vid undersökningen inför denna uppsats. Med det innebär att det är tolkningen av informationen författarna samlat in som har varit det centrala i arbetet. Hermeneutik innebär att man medvetet använder sina värderingar i forskningsprocessen. Den erfarenhet och kunskap forskaren har, väger in när han tolkar sina resultat. Detta skiljer sig från den positivistiska inriktningen där man gärna vill tro på absolut kunskap [Thurén, 2003]. Författarna har hållit sig objektiva till de metoder som skall kartläggas, dock kommer deras förförståelse att inverka då de skall avgöra hur pass väl de fungerar. Förförståelsen kommer mest att influera kriterierna för urvalsramen.

Angreppssättet för denna uppsatts är induktivt, det vill säga upptäcktens väg [Holme, Solvang, 1997]. Detta angreppssätt valdes på grund av att författarna ej hade några föraningar om det framtida resultat och därmed ej kunde fastställa någon hypotes. Den induktiva analysen används, till skillnad från deduktiv analys (bevisandes väg), när man inte har någon klar hypotes att gå efter. Istället bildar man sig en uppfattning av det studerade problemets verklighet under arbetets gång och genom generaliseringar nås i slutändan en helhetsbild, det slutliga resultatet (en teori). [Patton, 1988]

1.5.2 Validitet

Validitet innebär att man verkligen har undersökt det man vill undersöka och ingenting annat [Thurén, 2003]. I uppsatsen brukar författarna begreppet validitet i frågan om de undersöker rätt tekniker. Genom att sätta upp kriterier skiljer vi ut tekniker vi anser väsentliga för

uppsatsen. Författarna har sedan genom förmedlade kontakter tillförsäkrat att de tekniker vi undersökt är aktuella och relevanta.

1.5.3 Datainsamling

För att tillförsäkra oss om att hitta så många potentiella metoder som möjligt till vår urvalsram har vi använt följande tillvägagångssätt. Författarna har sökt i artiklar, facklitteratur, böcker samt rapporter för att hitta metoder som har nyttjats, testats och granskats i förhållandevis stor utsträckning. För att försäkra oss om att vi har hittat de mest relevanta källorna har vi använt oss av sökmotorer så som Google och Citeseer samt sökt efter litteratur på nationella bibliotekssystemet Libris.

Författarna har använt sig av ett flertal sökord både på engelska och svenska därav:
Pre-boot autentisering, autentisering, hårddisk kryptering, kryptering, stöld av bärbara datorer, bootsekvens, skydd av bärbara datorer, säkerhet för bärbara datorer, aktiva kort, USB-token, biometri, engångslösenord, filkryptering, mappkryptering, virtuell hårddiskkryptering, EFS, lösenord, BIOS-lösenord, kabellås, säkerhetspolicy, bootskydd, Master Boot Record med flera.

Författarna beslutade sig även för att komplettera datainsamlingen med en intervju för att få rekommendationer om ytterligare information.

1.5.4 Urvalskriterier

De kriterier författarna använt sig av för att styra urvalet av metoder är följande:

- Metoden skall vara väldokumenterad samt presenterad på engelska eller svenska.
- Informationen skall vara tillgänglig för allmänheten.
- Metoden skall vara väl beprövad och använd i dags dato.

Ytterligare ett kriterium som vi utgått ifrån är att metoden ej skall vara produktspecifik. Vi har valt att skriva om tekniken bakom produkten och ej produkten i sig.

1.5.5 Kvalitativa intervjuer

Syftet med kvalitativa intervjuer är att öka informationsvärdet och skapa en grund för en djupare och mer fullständig uppfattning om det fenomen som studeras [Holme, Solvang, 1997]. Vi valde att kontakta utvecklare och produktägare på ett säkerhetsledande företag både i och utanför Sverige. Det företag som kontaktades var Utimaco. Författarna försökte även att kontakta andra företag men utan resultat. Trots ett flertal försök till kontakt både via e-mail och via telefon, lyckades vi ej få till stånd fler intervjuer. Detta berodde i stor del på att företagen vi kontaktade, ej ville dela med sig av för produkten specifika hemligheter. Dessa experter inom området förmedlades av vår uppdragsgivare.

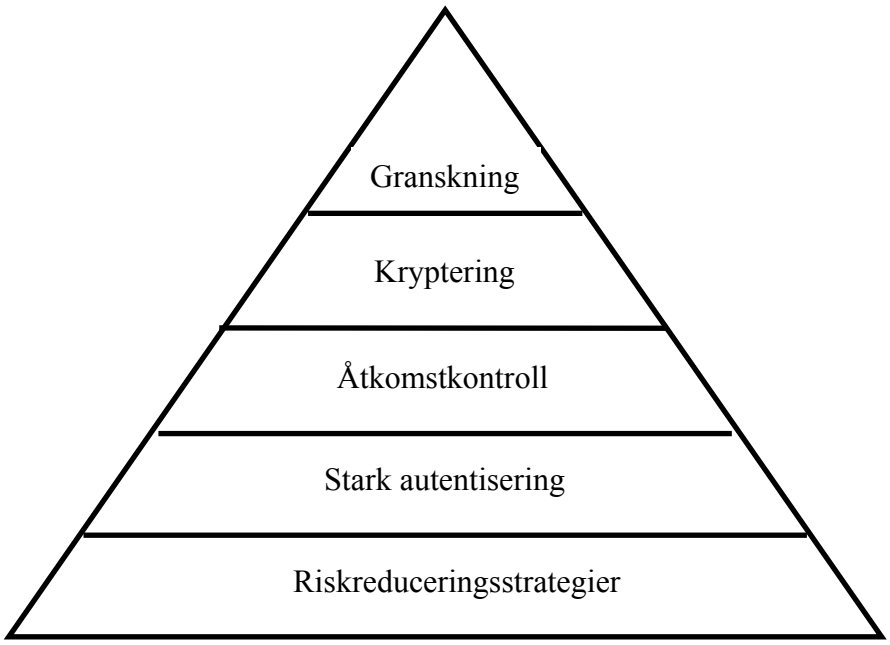
1.6 Målgrupp

Uppsatsen riktar sig till säkerhetsansvariga på organisationer och företag som önskar få fördjupad kunskap om skydd av data på bärbara datorer. Den riktar sig även till IT-studerande och övriga som är intresserade av ämnet.

1.7 Disposition

Uppsatsen är uppbyggd efter denna modell av Mark Lobel kallad säkerhetspyramiden. Säkerhetspyramiden (se figur 1) visar de delar som behövs för att skapa en säker miljö för datorer [Lobel, 2000]. Lobel motiverar pyramidens syfte och användning nedan (översatt till svenska av författarna):

”Att skydda sina tillgångar har alla i tider varit en viktig del i vårat samhälle, inte minst av militära, privata och ekonomiska anledningar. Autentisering är konceptet för att tillåta användning av dessa resurser. Autentisering kan idag dock inte existera i ett vakuum, det måste existera i en del av en säkerhetsram för att helt kunna säkra organisationers tillgångar. Denna säkerhetspyramid ger organisationen ett lager med multipla skydd mot inkräktare.” [Lobel, 2000, s.3,]



Figur 1, Säkerhetspyramiden

Riskreduceringsstrategier

Först och främst måste man ha riskreduceringsstrategier vilket inkluderar säkerhetspolicy, användarutbildning, alarm och restriktioner. Detta för att minska risken att värdefull information skall komma i orätta händer.

Stark autentisering

Stark autentisering behövs för att kontrollera att rätt personer har åtkomst till enheten och att personen ifråga verkligen är den han utger sig för att vara.

Åtkomstkontroll

Åtkomstkontroll används för att förhindra obehörig eller oavsiktlig förändring av information samt obehörigt avslöjande av information och svarar alltså mot aspekterna sekretess och riktighet inom datasäkerhet (se s.7).

Kryptering

Kryptering skyddar informationen på datorn genom att göra den oläsbar för obehöriga.

Granskning

Slutligen bör man granska systemet för att försäkra sig om dess effektivitet. Om någon av de lägre nivåerna inte uppnås kan ej de efterföljande stegen realiseras.

Vår uppsats är indelad i åtta kapitel. Kapitel två innehåller en utökad bakgrund för att ge en fördjupad bild av problemet. Tredje kapitlet handlar om riskreduceringsstrategier samt fysiskt skydd. I kapitel fyra beskrivs autentisering och olika autentiseringsmetoder. Kapitel fem beskriver hårddiskkryptering, både strategisk och taktisk samt åtkomstkontroll. Åtkomst-kontroll är en del av detta kapitel på grund av att många krypteringsapplikationer inkluderar åtkomstkontroll. Kapitel sex beskriver granskning. Kapitel sju innehåller vår analys. Uppsatsen avslutas med en diskussion i kapitel åtta.

2 Utökad bakgrund

I detta kapitel beskriver vi mer utförligt vad som är orsakerna till förlust och stöld av bärbara datorer samt vilka problem som det kan medföra.

2.1 Ökad användning av bärbara datorer

I Sverige såldes 296 050 datorer under tredje kvartalet år 2004, elva procent mer än vid tredje kvartalet 2003. Största ökningen står bärbara datorer för [Byttner, 2004]. Där låg ökningen på 33 procent och totalt såldes 109 820 bärbara datorer. I och med den senaste boomen står bärbara datorer för 37 procent, vilket är den högsta andelen hittills [Byttner, 2004].

Allt mer av arbetet sker utanför kontoret, visar en undersökning från Economist Intelligence. Kontorsanställda jobbar i genomsnitt 35 procent av sin arbetstid utanför kontoret. För två år sedan var siffran 25 procent. Om två år beräknas 42 procent av arbetstiden tillbringas utanför kontoret. Vanligaste stället att jobba på distans är från hemmet, vilket sker i 57 procent av fallen. I 16 procent sker distansjobbet på resa. Den mest förekommande sysselsättningen är att kommunicera med affärskontakter, vilket sker i 67 procent av fallen, följt av möten. Många skriver eller förbereder rapporter eller presentationer, ägnar sig åt strategiskt tänkande, läser e-post eller att hantera projekt och administration. Största barriären mot att jobba utanför kontoret är säkerheten. Det uppger 27 procent av de undersökta som ett allvarligt hinder. Undersökningen avsåg 600 medarbetare på olika chefspositioner i Europa och Mellanöstern. [Wallström, 2004]

I takt med att våra arbetsvanor blir alltmer flexibla och mobila ökar också möjligheterna. Enligt undersökningsföretaget IDC förväntas antalet personer som arbetar via mobila system att stiga med nära 13 miljoner fram till år 2005 [HP, 2004].

2.2 Stöld av bärbara datorer

Bärbara datorer löper större risk att bli stulna än stationära datorer. Stationära datorer är ofta inlåsta i säkra lokaler med god fysisk kontroll av människor medan bärbara datorer vanligtvis befinner sig utanför en organisations säkerhetskontroller [Sadlier, 2003]. En bärbar dator är liten, lätt och kan enkelt stjälas från en ouppmärksam ägare. Vem som helst kan förlora en bärbar dator vilket exemplifieras i följande anekdot översatt från engelska av författarna.

”Omedveten om att han skull bli en fotnot i industrispionagehistoria, skakade Irwin Jacobs hand med personer som gratulerade honom efter hans tal. Klockan var 13.00 den 16: e september 2000 vid Society of American Business Editors and Writers i Hyatt Regency i Irvine, California. I rummets ena ände stod Jacobs, en före detta professor vid MIT som grundade företaget Qualcomm 1985 och drev företaget till vinster på 3,9 miljarder dollar per år. Några meter ifrån honom låg hans bärbara dator, vilken han hade använt under sin presentation. Efter att ha pratat med journalister ett par minuter upptäckte Jacobs att hans dator var borta. Reportrar frågade vad som fanns lagrat på datorn. Jacobs svarade ”allting”. Ekonomiska rapporter, hemlig företagsinformation, åratal av e-mail, bilder på barnbarnen – allt fanns på hans dator. ”Vart jag än går har jag med mig den” sade han. ”Den har varit med mig jorden runt ett flertal tillfällen.” [Mann, 2001, s. 1]

När en bärbar dator blir stulen eller förlorad måste en organisation hantera ett flertal problem. Kostnaden av att ersätta hårdvaran är oftast försvinnande liten i jämförelse med den potentiella kostnaden som framgår av följande punkter:

- **Sekretess**

  Detta avser att informationen endast är tillgänglig för dem som har behörighet. Informationen lagrad på användarens enhet kan bli tillgänglig för en tredje part. I händelse att enheten innehåller konfidentiell information kan detta medföra stora risker för organisationen [Mitrovic, 2004].

- **Riktighet**

  Avser skydd och behandlingsmetoder så att informationen förblir korrekt och fullständig [Mitrovic, 2004]. Om enheten innehåller mjuka certifikat för åtkomst till organisationens nätverk är det möjligt att enheten kan användas för att få otillåten åtkomst till företagets resurser [Sadlier, 2003].

- **Tillgänglighet**

  Definieras av att den behöriga användaren alltid har tillgång till informationen vid behov [Mitrovic, 2004]. Om användaren förlorar sin enhet och informationen sparad på denna kan detta innebära att användaren blir oförmögen att utföra sina arbetsuppgifter innan enheten har ersatts [Sadlier, 2003].

Att avgöra antalet stulna datorer i en organisation är en utmaning. På företagsmarknaden är många organisationer oförmögna att noggrant spåra sina datorer, och inte minst varför de gått förlorade. En objektiv källa för information är datorleasingföretag som spårar med hög precision antalet maskiner som skickas ut vid start av uthyrning mot hur många som returneras i slutet. När man räknade ihop antalet saknade datorer i slutet av en tvåårig uthyrningscykel, saknades upp till 20 % av det totala antalet. Då detta gällde datorer generellt var antagligen andelen förlorade bärbara datorer mycket större [Absolute Software, 2003] [Gordon et al, 2004]. I en Sifoundersökning från september 2000 uppger vart sjätte bolag på Stockholmsbörsen att de drabbats av förlust eller stöld av bärbara datorer [Protectdata, 2000].

När man jämför hur de olika datorerna gått förlorade märker man att intern förlust är större än alla andra källor till stöld. Enligt Absolute Software är de stora orsakerna för förlust av bärbara datorer:

- Intern förlust – uppskattningsvis 60 %
- Intern stöld – uppskattningsvis 30 %
- Extern stöld – uppskattningsvis 10 %

Intern förlust

Den största orsaken till förlust av datorer inom företag är ej rapporterade förluster och ej rapporterade stölder. Det inkluderar också datorer som flyttar från anställd till anställd utan att skrivas upp. [Absolute Software, 2003]

Intern stöld

Intern stöld kan omfatta sparkade anställda som vägrar lämna tillbaka sina datorer, organiserad stöld inom företaget samt tjuvaktiga anställda. En undersökning visar att 40 % av alla stölder sker medan någon befinner sig inne på kontoret samtidigt som stölden pågår [Korzeniowski, 2001].

Extern stöld

Extern stöld är den minsta kategorin för förlust av bärbara datorer. Den kan enligt [Absolute Software, 2003] delas in i olika subklasser:

- Opportunistisk stöld
    - Oansvarighet: Trots värdet på enheten och informationen lagrad på den är oansvarighet och ouppmärksamhet en av de ledande orsakerna till extern stöld.
    - ”Smash and grab”: I den typiska ”smash and grab” stölden stjäls bärbara datorn från ägarens bil eller hem.
    - Kontorsstöld av icke-anställda: Den här typen av stöld kan vara allt ifrån tjuvar som kör genom fönstret och stjäl så många datorer som möjligt under en tvåminutersperiod, till tjuvar som klär ut sig till anställda och samlar ihop bärbara datorer och lämnar kontoret obemärkta.

- Stöld för företagsspionerі
    - Detta är ovanligt men ett växande problem, där en specifik användare som har känslig information på sin dator är målet för stöld. Detta står inte för en stor del av antalet stölder, men när det händer, slår det hårt mot organisationen. Chefer med konfidentiell finansiell information, interna strategidokument, källkod, kundlistor, vetenskapliga formler, affärshemligheter och annan konfidentiell information är alla potentiella offer.

3 Riskreduceringsstrategier

I det här kapitlet beskrivs första nivån i säkerhetspyramiden, hur man kan reducera riskerna för att information blir stulen. Flera strategier finns tillgängliga för att reducera risken för förlust och stöld. Dessa strategier har olika grad av effektivitet, användbarhet samt användningskostnad. För att avgöra vilka risker och säkerhetsbehov en organisation har kan man genomföra en riskanalys. En riskanalys är en analys av hur stor risken är att man skall konfronteras med att hot omsätts i handling. Detta tas upp i Appendix D. [RMT-gruppen, 1999]

Figur 2, Säkerhetspyramiden - Riskreduceringsstrategier

Det finns tre olika tillvägagångssätt för att skydda en bärbar dator: fysisk säkerhet innan stöld, accesskontroll för att skydda känslig information efter stöld samt spårningsteknologi för att underlätta spårning av enheterna efter stöld [Ryder, 2001].

3.1 Fysisk säkerhet

Att undvika stöld är en av de mest effektiva metoderna för riskreducering [Ryder, 2001]. Man måste dock tänka på att ej förstöra fördelarna som bärbara datorer medför. Författarna delar in förhindrande åtgärder i tre kategorier: användarutbildning, säkerhetspolicy samt alarm och restriktioner. Det finns allmänna riskreduceringsmetoder som hamnar utanför denna uppsats ramar. Exempel på detta är avskräckande metoder för att förebygga stölder.

3.1.1 Användarutbildning

En mycket användbar metod för att undvika stöld är genom att utbilda användarna. Användare brukar ej uppskatta metoder som inskränker deras produktivitet eller minskar bekvämligheten. Genom att undervisa användarna om riskerna vid förlust och stöld, metoder för att reducera riskerna samt innebörden av förlust av konfidentiell information för organisationen, kan man minska antalet förlorade enheter. [Sadlier, 2003]

Användare bör lära sig att hålla sin dator under uppsikt när de befinner sig utanför kontoret. De får aldrig lämna datorn utan tillsyn och ej heller visa att de bär på värdefull utrustning. Att bära sin dator i en dyrbar datorväska kan vara ett stort misstag. Dölj istället datorn i en annan typ av väska exempelvis en ryggsäck eller större väska som inte ser ut att innehålla en bärbar dator. Många användare är omedvetna om grundläggande metoder för att förhindra stöld. Därför bör information om detta ingå i företagets program om säkerhetsmedvetande. [LaptopsGuide, 2004] [Microsoft 2, 2004]

3.1.2 Säkerhetspolicy

Om metoder för att förhindra stöld ej är tillräckligt är den enklaste lösningen att förhindra användaren från att lagra känslig information på enheten. En sådan policy är svår att upprätthålla men i samverkan med god användarutbildning kan den vara effektiv.

Informationsklassifikationspolicys bör klart definiera vilken sorts data som är tillåten att lagra på bärbara enheter. Om man saknar andra skydd är det den bästa lösningen för att förhindra förlust av känslig information på högriskenheter. En organisation bör ha en klar policy för hur man skall agera vid stöld eller förlust av en bärbar dator. Det bör finnas en metod för ägaren att snabbt rapportera förlusten. För att minska risken att enheten används för att få otillåten åtkomst till organisationens nätverk bör ägarens certifikat revokeras och nya utges samt notifiera de parter som kan beröras av händelsen. Organisationen bör även ha ett klart budskap till användarna. Det är viktigt att användare rapporterar stöld eller förlust av en enhet snabbast möjligt. Om användarna är rädda för disciplinära åtgärder, finns risken att de ej kommer rapportera stölden eller ljuga om konfidentiell information lagrad på enheten. [Sadlier, 2003]

Enligt en undersökning på 600 IT-chefer, utförd av IDC 2004, har 20 % av företagen i Norge och Sverige inga planer på att skapa en säkerhetspolicy, då främst små bolag. Förklaringen till detta är att de upplever att de kan hantera problemställningarna utan att skriva ner dem. Det är dock viktigt att formulera en policy då det tvingar de ansvariga att tänka på ett strukturerat sätt. Det finns stora behov av att hjälpa bolag att analysera sin säkerhetspolicy mot dagens hotbild. Den största utmaningen kommer när policyn är utformad och ska förklaras för användarna. [Wallström B, 2004]

3.1.3 Alarm och restriktioner

Det existerar många produkter för att fysiskt skydda bärbara datorer. Vi kommer att ta upp de vanligast förekommande.

Enligt [Sadlier, 2003] finns olika typer av lås för att skydda datorn från stöld när man är ute och reser. Genom att låsa fast datorn med en kedja förhindrar man enkelt stöld. Dock används de ogärna av användarna och lämnas ofta hemma på grund av dess otymplighet. Dessa lås liknar lås som används på cyklar och består av en stålkabel som man kan vira runt ett fastsatt objekt. Kabellåset sätts in i den bärbara datorns Universal Security Slot (USS) vilken återfinns på 80 % av alla bärbara datorer och nästan alla datorer som produceras i dag har sådana. De två ändarna på kabeln säkras med ett hänglås. Dessa är billiga och enkla att använda men kan lätt klippas av med rätt verktyg [LaptopsGuide, 2004]. Kabellås är mest effektiva när de används på kontoret eller hemma men de måste användas för att ha någon inverkan. Tjuvar brukar ofta slå till vid konferenser och mässor på grund av att ägarna känner sig säkra i en grupp av kollegor, speciellt när man använder samma konferensrum i två till tre dagar. Även om det finns bra ställen att använda kabellåset på, tenderar användaren att nyttja låset mindre och mindre desto längre de stannar på ett och samma ställe. Det är ofta då tjuvarna slår till. Det är viktigt att få användaren att låsa sin dator att bli en rutin, precis som man startar datorn och stoppar i kontakten [Korzeniowski, 2001].

En annan lösning är att använda sig av alarmsystem. De är konstruerade så att de utlöser ett larm i händelse att enheten blir stulen eller kvarglömd. Det vanligaste systemet för detta är en avståndssensor som sätts fast på enheten. Användaren bär på en mottagare, om denna kommer på ett visst avstånd från datorn utlöses alarmet [Sadlier, 2003]. Mer avancerade versioner finns tillgängliga som förstör informationen på enheten. En nackdel är enligt [Korzeniowski, 2001] att alarmet utlöses om användaren glömmer att stänga av det när han lämnar enheten på jobbet, i bilen eller i hemmet. Detta kommer att göra användaren mindre benägen att använda alarmet.

Det finns även produkter som kombinerar larm och kabellås exempelvis ett lås som består av fiberoptiskkabel. Det går ständigt ljussignaler genom kabeln och om signalen avbryts ljuder ett alarm. [Hildreth, 2001]

3.2 BIOS-lösenord och hårddisklösenord

BIOS kan på de flesta datorer konfigureras så att man kan kräva lösenord av användaren innan datorn laddar operativsystemet. Det hindrar enligt [Absolute Software, 2003; Sadlier, 2003] datorn från att starta, om lösenordet är inkorrekt. Detta kan låta som en bra strategi som motverkar stöld och skyddar data från att bli stulen. Denna lösning kan dock ge en falsk känsla av säkerhet då BIOS-lösenord inte ger något riktigt säkerhetsskydd. För att förstå anledningen till detta måste man se vad som egentligen är implementerat. När man använder sig av BIOS-lösenord lägger man till ett steg i bootprocessen, som kräver användar-autentisering innan den fortsätter att starta operativ systemet [Absolute Software, 2003; LaptopsGuide, 2004]. Appendix A beskriver datorns bootsekvens mer utförligt.

Det är större chans att en förlorad bärbar dator lämnas tillbaka om den som hittat den ej kan starta den. Detta för att kunna få eventuell hittelön eller beröm. BIOS lösenord skyddar dock bara datorn i sig själv och ej data på hårddisken, vilken enkelt kan tas bort och läsas på en annan dator [Sadlier, 2003]. För att förhindra detta har vissa bärbara datorer hårddisklösenord. Hårddisklösenord gör så att den ej aktiveras om ej korrekt lösenord skrivs in. Detta skydd kan man dock komma förbi med rätt färdigheter och utrustning [Sadlier, 2003]. BIOS-lösenord hindrar datorn från att starta men skyddar inte data på hårddisken. Dessutom kan man radera BIOS-lösenordet från de flesta datorer genom att ta bort CMOS-batteriet en kort tid. Detta återställer CMOS inställningarna till sina ursprungsinställningar. Det är ingen trivial uppgift men det är inte svårt för en teknisk kunnig person. Om en dator med BIOS-lösenord blir stulen är chansen stor att den slängs bort. Om personen är enträgen kommer han att ta bort hårddisken för att få tillgång till informationen, eller återställa BIOS genom att ta bort CMOS-batteriet, för att sedan kunna sälja datorn. I vilket fall som helst kan värdefull data exponeras [Absolute Software, 2003].

BIOS-lösenord, antingen system eller hårddiskbaserat, är en utmaning för en organisation. Om en användare byter lösenord på sin enhet och sen glömmer bort det, är det svårt att få tillbaka lösenordet. Många tillverkare stöder administrationslösenord som kan användas för att återfå förlorade BIOS-lösenord. [Sadlier, 2003]

De flesta bärbara datorer kan sättas i viloläge för att spara batterikraft när de ej används. Detta tillför möjligheten att snabbt återställa datorn som man lämnade den. Detta innebär att många användare hellre sätter datorn i viloläge än stänger av den. Det är viktigt att enheten är konfigurerad att autentisera användaren både på BIOS- och på operativsystems- nivå. Om autentisering inte krävs efter det att datorn kommer ur viloläge innebär det att en tjuv enkelt kan få tillgång till en enhet stulen i viloläge. Detta därför att den ej frågar efter BIOS-lösenordet då den ej behöver gå igenom datorns startsekvens. [Sadlier, 2003]

3.3 Avlägsna identifieringsmärken

Om en bärbar dator har märken som berättar vilken organisation den tillhör är det större risk att den som tagit datorn intresserar sig för innehållet, istället för att bara formatera hårddisken och sälja datorn. Sådan identifiering kan upplysa en professionell tjuv om potentiella köpare,

exempelvis organisationens konkurrenter. Avsaknad av märkning i samband med BIOS-lösenord och hårddisklösenord ökar chansen att en förlorad enhet returneras eller slängs bort istället för att den känsliga informationen extraheras. Dessa råd gäller enbart om avsikten är att skydda informationen och ej hårdvaran. [Sadlier, 2003]

[Sadlier, 2003] delar upp identifieringsmärkning i följande kategorier:

- **Ägarinformation:** Skall vara generisk och ej identifiera organisationen som enheten tillhör.
- **”Returnera till ägaren” information:** Bör tillhandahållas av en tilltrodd tredje part, exempelvis tillverkaren om den tillhandahåller en sådan tjänst.
- **Supportinformation:** Dessa påminner användaren vilket nummer de skall ringa om de har problem med sin dator. Det innebär dock att tjuven kan ringa detta nummer för att identifiera organisationen till vilken enheten tillhör.

Att ta bort identifieringsmärken är ett av de mest kostnadseffektiva stegen för att reducera risken för att känslig information stjäls.

3.4 Spårning

Spårningsteknologi i form av gömda applikationer på hårddisken finns för att hjälpa till vid återfinnandet av en stulen enhet. När en stulen enhet med spårningsteknologi kopplas in i telenätet eller ett nätverk försöker applikationen kontakta en central övervakningsstation som rapporterar dess position. Principen liknar GPS (Global Positioning System) baserade system. [LaptopsGuide, 2004]

4 Autentisering

Detta kapitel innehåller information om nivå två i säkerhetspyramiden, autentisering. Autentisering är sättet att verifiera identiteten på en person/enhet [Pagina, 2004]. Det kan också användas för att verifiera att information och data som sänds är samma som ursprungligen sändes och att det är samma sändare. Nära associerat med autentisering är användarrättigheter, vilket avgör vilka rättigheter och privilegier som är tillgängliga för den autentiserade personen. Att knyta samman autentisering och användarrättigheter är identitetshantering. Identitetshantering omfattar många lösningar och applikationer tillhandahåller varierande nivåer av säkerhet och användarhantering. [Kolodgy, 2003]

Figur 3, Säkerhetspyramiden - Stark autentisering

4.1 Användarnamn och lösenord

Den primära autentiseringsmetoden för datorsystem är specifika användarnamn och lösenord för olika system. Detta innebär att för varje applikation eller system som kräver åtkomst finns det ett specifikt användarnamn och lösenord skapat för användaren [Ahuja, 1996]. Applikationen har sin egen databas med åtkomsträttigheter och de är vanligtvis inte delade mellan applikationer. Det är bra när en användare bara måste använda en handfull applikationer, men när antalet applikationer och användare ökar, ökar också säkerhets- och hanteringsproblemen. [Kolodgy, 2003]

Vad många företag nu upplever är överbelastning av lösenord. Användare har många fler lösenord än vad de kan komma ihåg. Användare inom ett företag har ofta ett flertal olika lösenord. För att öka på förvirringen så är lösenordsformaten annorlunda för varje applikation, vissa lösenord måste bytas periodiskt och andra räcker för evigt. Överbelastning av lösenord har blivit ett stort problem för IT - och nätverkssäkerhets- administratörer. [Kolodgy, 2003]

4.1.1 Vad är problemen med användandet av lösenord?

Vanligtvis placerar man ansvaret för att skapa lösenord hos användaren. Användaren är tillbedd att skapa ett lösenord som de kan komma ihåg, men andra inte kan gissa. Därmed utvecklas en paradox, användaren glömmer bort sitt lösenord i sin uppgift att skapa ett lösenord som inte går att gissa. Det leder mer ofta än sällan till likgiltighet hos användaren. Detta är den ledande faktorn mot styrkan och effektiviteten i dagens autentiseringssystem. Lösenordshanteringssystem slutade för många år sedan att skapa lösenord till användarna. Att låta användarna bestämma sina egna lösenord leder nästan alltid till att svaga lösenord väljs. När man tvingar användarna att använda starka lösenord, blir lösenord på post-it lappar allt vanligare. Om vi betraktar dagens autentisering och lösenordssystem är det lätt att avgöra att vissa svagheter kan spåras till specifika komponenter inom autentiseringssytemet [VeriSign, 2004].

Följande diskussion framhäver svagheterna i dagens autentiseringssystem enligt [VeriSign, 2004]:

- Inmatning av lösenord

  I många fall kan säkerheten vid inskrivningen av lösenord lätt äventyras genom att man helt enkelt tittar över någons axel och läser av tangentbordstryckningar. Avancerade program skrivs för att producera listor av lösenord från möjliga bokstavskombinationer och placeringen av händerna på tangentbordet. Tangentbordsavläsningsprogram har funnits lika länge som tangentbordet. De tillhandahåller ett utmärkt sätt att stjäla lösenord och användarnamn. I vissa fall kommer mjukvaran ihåg lösenordet och applikationen får lösenord och användarnamn från applikationen själv och ej från individen.

- Lösenordstransport

  När en användare skriver in sitt lösenord blir överföringen till autentiseringsenheten ofta osäker. Många gånger frågas man efter lösenord på en webbsida då browsern inte är i säkert läge. Det är vanligt att tillverkare använder krypterad transport som är svag eller har andra begräsningar, exempelvis storlek. Transporten av lösenord är ett av det mest förbisedda problemen i moderna autentiseringssytem.

- Lagring av lösenord

  Hur lagras lösenorden i systemet? Det finns fyra olika nivåer av lagring – i klartext, krypterad, gömd – i klartext, gömd - krypterad. Många applikationer har historiskt sett valt dåliga lagringslösningar och vissa använder svag kryptering som enkelt kan forceras med råstyrka. Om en dator blir stulen kan angriparen leta upp dessa lösenordslistor för att få tillgång till ett privat nätverk, exempelvis ägarens företag.

Lösenord är den största risken inom autentiseringssystem. Om användare fortsätter att välja svaga lösenord spelar det ingen roll hur stark transport, lagring, verifiering och inmatning man har [VeriSign, 2004]. Samtidigt som lösenord kräver mycket underhåll så tillhandahåller de en lägstanivå av säkerhet och ger ingen säker identifikation av användaren. Användandet av enbart lösenord äventyrar den övergripande säkerheten av en organisations nätverk av följande anledningar enlig [Kolodgy, 2003] och [Fryksten, 2002]:

- De kan skrivas ner och läggas där de lätt kan hittas.
- De kan delas utan svårighet – trots att man håller fast vid obligatoriska lösenordsbyten och hårda lösenordsregler så hindrar det inte att man delar och skriver ner dem.
- Många skapar lösenord som är enkla att komma ihåg t.ex. födelsedagar, namn och platser. Maskingenererade lösenord eller lösenordsvalskriterier eliminerar detta men leder i de flesta fall till att lösenordet skrivs ner.
- Användare väljer vanligen samma lösenord till flera applikationer så att det blir enkelt att komma ihåg. Det innebär att om man har lyckats gissa ett lösenord så är det ofta det första man försöker med på nästa applikation.
- Många användare behöver byta lösenord med hjälp av supporten för att de glömmer dem.

Många problem associerade med lösenord gör att det inte längre accepteras av många företag. Att förlita sig på enbart lösenord tillhandahåller inte en säker, kostnadseffektiv eller lätthanterbarlösning. Många företag behöver andra autentiseringsmetoder. [Kolodgy, 2003]

4.1.2 Lösenords statistik

Lösenord kan skrivas från fyra teckenuppsättningar vilket visas i tabell 1.

Teckenuppsättningar	Antal tecken
Numeriska	10
Alfabetiska	26
Versaler/gemener	52
Tangentbord/utökat	33
Maximalt antal tecken	95

Tabell 1, Antal tecken per teckenuppsättning (ASCII).

För att hitta det totala antalet potentiella kombinationer av tecken till ett lösenord med bestämd längd, kan man ta totala antalet möjliga tecken (x) upphöjt med antalet tecken i lösenordet (y). Ett sex tecken långt lösenord som använder alla versaler har totala antalet kombinationer av 26^6=308 915 776.

Det totala antalet potentiella teckenkombinationer i ett lösenord med variabellängd hittas genom att ta antalet tillgängliga tecken (x), upphöjt med det lägsta antalet fält (y), adderat inkrementerat till digniteten av högsta antal fält (z). Om du har ett 1-6 tecken långt lösenord som endast består av gemener blir resultatet: X^y +…+ X^z vilket är 26^1+…+26^6= 321 272 406.

1-6 tecken långa lösenord ger följande möjligheter:

Teckenuppsättning	Antal kombinationer
Alfabetiska	321 272 406
Versaler/gemener	20 158 268 676
Numeriska	1 111 110
Versaler/gemener + numeriska	57 731 386 986
Utökad	1 108 378 656
Versaler/gemener + numeriska + utökad	742 912 017 120

Tabell 2, Antalet kombinationer med 1-6 tecken.

1-8 tecken långa lösenord ger följande möjligheter:

Teckenuppsättning	Antal kombinationer
Alfabetiska	217 180 147 158
Versaler/gemener	54 507 958 502 660
Numeriska	111 111 110
Versaler/gemener + numeriska	221 919 451 578 090
Utökad	1 134 979 744 800
Versaler/gemener + numeriska + utökad	6 704 780 954 517 120

Tabell 3, Antalet kombinationer med 1-8 tecken.

Enligt en undersökning av 3289 lösenord gjord av Robert Morris och Ken Thompson refererad av [VeriSign, 2004] kom de fram till dessa resultat:

- 54 % av alla lösenord var mellan 3-6 tecken långa. I dag bör man helst använda lösenord som är minst åtta tecken långt för att kunna motstå råstyrkeattacker och ordboksattacker. Ordboksattack innebär att man provar alla ord i en ordbok för att försöka ta sig in i systemet.

- De flesta lösenord i undersökningen innehöll stora delar gemener. För att försvåra för en angripare bör man använda en blandning av versaler, gemener och nummer.
- Om uppskattningsvis 20 år har längden på lösenord bara ökat med två tecken, medan datorkapaciteten har ökat mångfalt. Detta innebär att det blir lättare för en angripare att ta sig in med råstyrka, när datorkraften angriparen har tillgång till ökar.
- För var tjugonde lösenord man hittar är det en stor chans att av lösenorden även kommer att väljas av en annan användare. Detta innebär att användare tenderar att använda likartade lösenord vilket underlättar för angriparen. Dessa duplicerade lösenord tenderar att falla i enkelt gissbara kategorier, så som uppslagsord och namn. För att undvika detta bör man välja lösenord som ej återfinns i en ordbok. Genom att använda ordlistor kunde undersökarna hitta 999 lösenord, 31,6 % av lösenorden.
- Lösenordslängden kommer inte att öka om det ej krävs av operativsystemet eller autentiseringssystemet. Användare har en viss tendens att behålla samma lösenord om ett byte ej krävs.
- Användare nyttjar samma lösenord på olika system. Detta underlättar för angriparen att få tillgång till olika resurser på systemet om han får tillgång till ett lösenord.

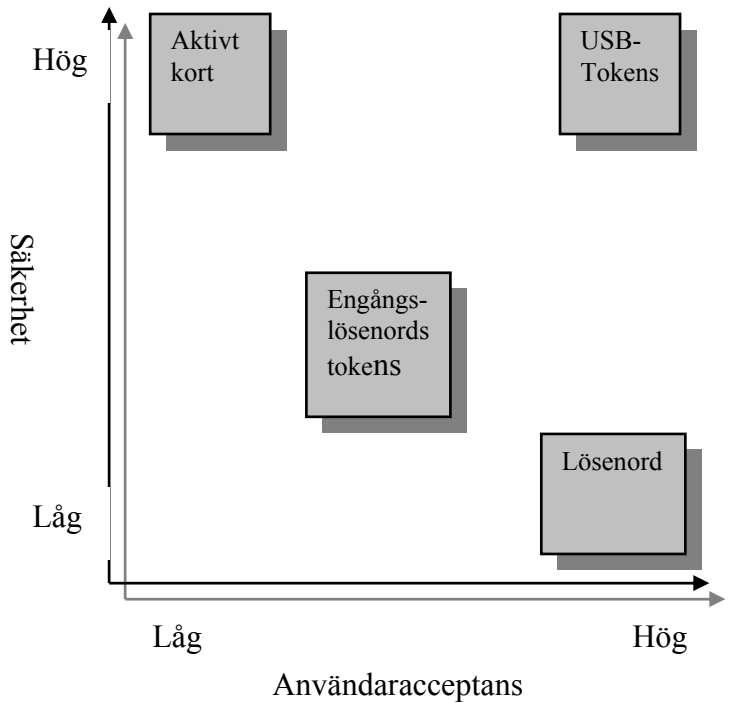
För att förbättra säkerheten i lösenordssystem föreslår VeriSign [VeriSign, 2004] följande:

- Öka kraven på lösenordslängd.
- Kontrollera att inte användarnamnet används som lösenord.
- Inför tidsperiodiska lösenordsbyten.
- Stäng konton efter X antal felaktiga inloggningsförsök.

4.2 Tvåfaktorig användarautentisering

Bättre användarhantering och säkerhet kan ges med autentiseringsmetoder som använder hårdvarukomponenter, någonting du har, med ett lösenordssystem, någonting du vet, eller med biometrisk autentisering, någonting du är [Gleeson, 2004]. Hårdvarukomponenter kan inkludera aktivt kort, engångslösenordstoken och USB-tokens [Gleeson, 2004]. För att bli autentiserad måste användaren ha hårdvaran och kunna lösenordet. Alla dessa komponenter måste överensstämma med autentiseringssystemet som används av alla ingångar till ett givet system [Kolodgy, 2003].

Användandet av två faktorig eller tre faktorig autentisering ökar kraftigt säkerheten av autentiseringssystemet. Utan den extra faktorn är tillgång till applikationen eller nätverket ej möjlig. Skulle hårdvarukomponenten tappas bort eller bli stulen, upptäcks det fort av användaren. Om ett lösenord blir stulet är det ingen som upptäcker det innan någon bryter sig in i systemet. Med en personlig token eller aktivt kort elimineras möjligheten att flera användare använder samma lösenord. [Kolodgy, 2003]



Figur 4, En jämförelse av metoder för autentisering utifrån användaracceptans och säkerhet. [Kolodgy, 2003]

Autentiseringsmetoder använda av företag måste kunna utföra sina primära funktioner på ett säkert sätt. De måste även kunna hantera olika miljöer och överensstämma med företagspolicy. Önskan att minska kostnaderna, öka nätverkseffektiviteten samt erbjuda användarvänliga metoder är också faktorer som tas i beaktande av företag. En vanlig orsak till varför företag inte byter till starkare autentiseringsmetoder är att många tror att lösenordsystem är gratis och om de inte tvingas att byta till säkrare system kommer de ej att byta till starkare autentiseringssystem. Lösenord är dock inte gratis om man beaktar hanteringen och utställandet av lösenord och kostnaden för telefonsamtal till supporten då lösenord har glömts. [Kolodgy, 2003]

4.3 Aktiva kort

Ett aktivt kort är ett plastkort i samma storlek som ett kontokort med ett inbäddat datorchip. Chippet kan antingen vara en mikroprocessor med internt minne eller ett minneschip med ej programmerbar logik. Chippets koppling kan vara antingen genom direkt fysiskt kontakt eller också via avlägsen kontakt genom ett elektromagnetiskt interface [Cagliostro, 1999].

Kortet tillhandahåller inte enbart minneskapacitet, utan har också beräkningsförmåga. Det aktiva kortets självstyre gör det resistent mot attacker eftersom det inte behöver vara beroende av potentiella sårbara externa resurser. På grund av detta karaktärsdrag, så kan aktiva kort användas av olika applikationer som kräver ett starkt säkerhetsskydd [Chan, 1997].

Aktiva kort används sällan till bärbara datorer, vissa enheter har dock en inbyggd kortläsare. Det finns även portabla aktiva kort läsare som kan kopplas in i enheterna. [Korzeniowski, 2001]

4.3.1 Historia

Teknologin har sitt ursprung från 1970-talet då uppfinnare i Tyskland, Japan och Frankrike patenterade kortet. Det var dock inte förrän på mitten av 1980-talet som det började användas i stor omfattning. Sen dess har industrin vuxit oerhört, och idag beräknas det att det tillverkas ca en miljard (1 000 000 000) kort per år (från år 1998) [Cagliostro, 1999].

4.3.2 Teknologi

Det finns två generella kategorier av aktiva kort: kontakt och kontaktlösa aktiva kort. Ett kontaktaktivt kort kräver insättning i en kortläsare med en direkt koppling till mikromodulen på kortets yta (vanligtvis guldfärgad). Det är genom denna fysiska kontakt som överföringen av kommandon, data och kortets aktuella status görs. Ett kontaktlöst aktivt kort kräver bara närhet till en kortläsare. Både kortet och läsaren har antenner och det är via denna kontaktlösa länk som de två kommunicerar. De flesta kontaktlösa kort erhåller också kraften till det interna chippet från denna elektromagnetiska signal. [Cagliostro, 1999]

Det finns även en kombination av dessa två olika sorters kort, det så kallade kombikortet, då med ett chip för både kontakt och kontaktlösa interface [Cagliostro, 1999]. Chippen som används i alla dessa kort kan delas in i två kategorier: mikroprocessorchip och minneschip. Ett minneschip kan ses som en liten floppydisk med valbar säkerhet. Minnes kort kan lagra från 103 bits till 16 000 bits data. De är billigare än mikroprocessorkort men med en motsvarande reduktion av handhavandet av datasäkerhet, eftersom den måste lita på kortläsaren för att säkra data på kortet [Cagliostro, 1999]. Minneskort tenderar man att använda i miljöer med lägre säkerhetskrav på grund av sin oförmåga att genomföra krypterade algoritmer [Rainbow Technologies, 2002].

Ett mikroprocessorchip kan lägga till, ta bort och på annat sätt manipulera informationen på sitt eget minne. Den kan ses som en miniatyrdator med en input/output-port, operativsystem och ett sekundärminne. De finns tillgängliga i 8, 16 eller 32 bit arkitektur. Deras dataminneskapacitet sträcker sig från 300 bytes till 32 000 bytes [Cagliostro, 1999]. Kortet erbjuder i sig själv säkerhet, oberoende av kortläsaren, detta gör att kortet blir idealt för applikationer som kräver hög säkerhet. Med mikroprocessorkort är användarens privata nyckel alltid säkert sparad på kortet och lämnar därefter aldrig kortet. Genom att använda kortets egen processor stannar alla kryptografiska funktioner, inkluderat signaturer och dekryptering av sessionsnycklar, inuti kortet [Rainbow Technologies, 2002].

Filstrukturen hos det aktiva kortets operativsystem liknar till stor del andra vanliga operativ-system så som UNIX och MS-DOS. För att tillhandahålla en bättre säkerhetskontroll, intensifieras attributen hos varje fil med tillägg av accessbegränsningar och filstatusfält i huvudet (eng. header). Även fillåsning används för att skydda filen från access. Dessa säkerhetsmekanismer och algoritmer tillhandahåller logiskt skydd hos det aktiva kortet. [Chan, 1997]

Nu för tiden hävdar företag och kryptografer att de har förmågan att attackera och knäcka det aktiva kortet. Vissa utför fysiska attacker medan andra bara bevisar sin framgång med matematiska satser. De flesta attacker idag, är klassificerade som klass 3 attacker, med vilket menas att kostnaden associerad till att knäcka systemet är mycket högre än kostanden av själva systemet, eller så krävs det flera hundra års datorkraft att bryta sig in i en endaste transaktion. Samtidigt som teknologin gör snabba framsteg, uppdaterar och förbättrar

tillverkarna sina produkter konstant. Aktiva kort anses i grunden vara en säker enhet. Det är en säker plats att lagra värdefull information så som privata nycklar, kontonummer och värdefull personlig data, så som biometrisk information. Kortet är också en säker plats att utföra off-line processer, exempelvis publik- eller privat nyckelkryptering och dekryptering på.[Chan, 1997]

4.4 USB-tokens

En autentiseringsmetod som ökar i popularitet är USB-tokens som fungerar som en nyckel. En kryptografisk algoritm är lagrad i en enhet som stoppas in i USB kontakten. Dessa token är populära eftersom de är kompatibla med de flesta datorer. USB-tokens har ofta digitala certifikat lagrade i dem och de kan vanligtvis användas som lagringsenheter för att spara valfri data.

USB-token innehåller ett litet datorchip för att säkert kunna lagra information. Den är tekniskt sett identiska med aktiva kort, med undantaget från deras form och interface. USB-token är för det mesta mindre än en husnyckel och är designad att interagera med Universal Serial Bus (USB) porten [Rainbow Technologies, 2002]. USB porten kom 1995 och återfinns idag på i stort sätt alla datorer som tillverkas [Paulsen, 2004]. Precis som aktiva kort finns dessa token tillgängliga i både minnes och mikroprocessor variationer.

USB-baserade tokens tillhandahåller unika fördelar i kooperativa IT miljöer. Kortläsare behövs inte eftersom USB-tokens istället enkelt pluggas in i USB-porten som finnes på de flesta datorer. De flesta nya populära operativsystem har USB-drivrutiner inbyggda som utnyttjar plug-and-play teknik för att ladda de drivrutiner som krävs för USB-token. [Rainbow Technologies, 2002]

USB-token kan vara mycket snabbare än de vanliga portkopplade aktiva kortläsarna, detta tack vare den höga farten hos USB i jämförelse med de äldre seriella portarna. USB-tokens är lätta att använda och designade för att passa på en nyckelkedja. Studier som gjorts, visar att vid erbjudandet av att få välja mellan antingen ett aktivt kort eller en USB-token svarade 95 % att de föredrog token. [Rainbow Technologies, 2002]

4.5 Engångslösenord

Engångångslösenordstokens är en teknik som funnits mer än 20 år. Från säkerhetssynpunkt är det en teknologi som fortsätter att vara framgångsrik därför att den kombinerar tvåfaktorig autentisering med engångslösenord. Två faktorer erbjuder en hög grad av säkerhet att användaren verkligen är den han/hon utger sig för att vara. Engångångslösenordstokens lyckas genom att försäkra att lösenordet genererat av token är unikt, oförutsägbart och annorlunda varje gång det används. [CryptoCard, 2003]

I traditionella lösenordsautentiseringssystem använder man samma lösenord gång efter gång, detta kan utnyttjas av någon som vill göra intrång. Ett engångslösenordsautentiseringssystem eliminerar detta problem genom att kräva olika lösenord varje gång användaren loggar in på systemet. Efter det att lösenordets används är det inte längre giltigt och kan ej användas för att få åtkomst till systemet. Två typer av engångslösenordssystem är vanliga i dag (enligt Microsoft, 2003):

- **Lösenordslista**. En lista med lösenord varav varje kan användas en gång för att logga in i systemet. Lösenordets godkänns används och slängs. Denna process upprepas vid varje inloggning tills det ej finns några lösenord kvar på listan. En ny lista måste då genereras åt användaren. Många lösenordslistor distribueras i pappersformat och bärs runt av användaren.

  Engångslösenordssystemet förhindrar återspelningsattacker, men för att vara synkroniserad med systemet krävs det att användaren stryker ett lösenord på listan varje gång det används. Detta kan skapa en administrativ börda, på grund av att listan måste genereras, distribueras och sedan hanteras av användarna.

- **Lösenordstoken.** Mjukvara eller hårdvara som innehåller en lösenordsgenerator som kan synkroniseras med en autentiseringsserver. En token binds till en användares konto och lösenord genereras periodiskt, bara serverns mjukvara kan avgöra vilket lösenord som är giltigt för användaren vid det givna tillfället. På grund av att lösenordet byts periodiskt är det i stort sett omöjligt för en illvillig användare att spela in lösenordet och återanvända det senare.

4.6 Biometri

Biometri är vetenskapen om mätningar av fysiska kännetecken. Biometri används ofta för att skydda lokaler med potentiellt värdefull information och värdefulla enheter. Biometri tillhandahåller ytterligare ett sätt att förhindra otillåten åtkomst genom att endast tillåta användare som autentiserar sig med sina fysiska egenskaper, exempelvis fingeravtryck, röstigenkänning, ansiktsigenkänning och iris-scan. Alla biometriska system arbetar i stort sett likadant, en användare skannar sin identifieringsegenskap i en avläsningsenhet. Denna sparar mönstret i en databas [Korzeniowski, 2001]. Bilderna översätts sedan till en unik signatur som beräknats från ett flertal unika punkter som utvunnits från bilden, vanligtvis mellan 8 och 17 punkter vid fingeravtryckskläsning [Symantec B, 2004]. För att få åtkomst till datorn måste användaren autentisera sig med sin identifieringsegenskap, denne får åtkomst om mönstren överensstämmer [Korzeniowski, 2001]. De mer avancerade produkterna av den här typen lägger till andra mätningar exempelvis fingrets ledningsförmåga, elektrisk stabilitet och så vidare. Detta för att säkerställa att det ej är ett fabricerat eller avhugget finger. Fördelen med biometri är att de kännetecken som används ej kan stjälas eller lånas [Symantec B, 2004].

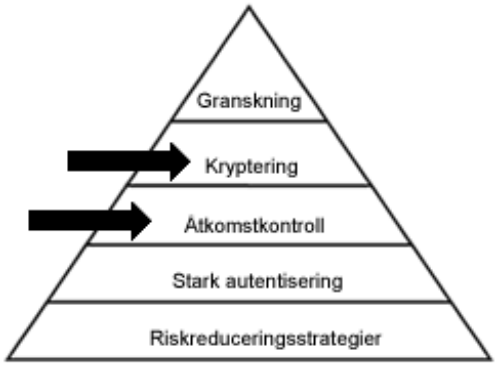
De första biometriska enheterna var dyra och designades i första hand för stationära datorer. Den expanderande säkerhetsmarknaden och förbättrad teknik har dock gjort teknologin mer kostnadseffektiv för portabla enheter. Det finns exempelvis skanners som kopplas in i USB-porten, inbyggda mikrofoner, kameror, finger-, ansikts- samt röstigenkänningsenheter för bärbara datorer. Det finns produkter som kombinerar olika biometriska identifierings-egenskaper exempelvis röstigenkänning tillsammans med fingeravtryck. Andra system kombinerar en biometrisk egenskap tillsamman med en hårdvarukomponent exempelvis USB-token och aktivt kort. Detta ger trefaktorig användarautentisering. [Korzeniowski, 2001]

Dock har ett flertal tester, utförda av datortidningar, av biometriska verktyg som finns tillhanda för bärbara datorer varit negativa. Endast ett fåtal verktyg fick godkänt. Exempelvis utgick många verktyg från färre än åtta mätpunkter för digitala fingeravtryck, trots att åtta är minimum. Många verktyg fungerade inte tillräckligt bra för att kunna användas. Det behövdes nästan en halvtimme för att få ett fingeravtryck igenkänt, och produkten innehöll även

programdrivrutiner som fick datorn att starta om och dessa var de slutliga versionerna av produkten. En japansk student lyckades lura 80 % av verktygen med hjälp av ett falskt finger gjort av ett slags fast gelé. [Symantec B, 2004]

5 Hårddiskkryptering och Åtkomstkontroll

Medan kabellås och alarm kan förhindra stöld av bärbara datorer, behöver man fortfarande skydd för att göra informationen på datorn oåtkomlig utifall att enheten skulle bli stulen. Därför skriver författarna i detta kapitel om nivå tre och fyra i säkerhetspyramiden, olika metoder för att kryptera data på hårddiskar och åtkomstkontroll. Åtkomst-kontroll är en del av detta kapitel då åtkomst-kontroll ofta är integrerat med krypterings-applikationerna eller Windows XP. Kapitlet börjar med en generell beskrivning av kryptering och går sedan in på olika kryptografiska tekniker. Kryptering av data tillhandahåller det bästa skyddet mot spridning av hemlig information från förlorade datorer. Information skyddad av en stark, välimplementerad kryptografisk teknik kan göra den oanvändbar för en tjuv. [Sadlier, 2003]



Figur 5, Säkerhetspyramiden – Åtkomstkontroll och Kryptering

5.1 Kryptering

En metod för kryptering och dekryptering kallas för chiffer. Alla moderna algoritmer använder en nyckel för att kontrollera kryptering och dekryptering, en nyckel kan bara dekrypteras om nyckeln överensstämmer med krypteringsnyckeln. Det finns två olika klasser av nyckelbaserade algoritmer; symmetriska och asymmetriska. Skillnaden är att symmetriska algoritmer använder samma nyckel för kryptering och dekryptering medan asymmetriska algoritmer använder olika nycklar för kryptering och dekryptering. Appendix C beskriver kryptering och algoritmer mer utförligt. [Kessler, 2004]

Nyckelns längd

En fråga som ofta ställs i dessa sammanhang är hur långa krypteringsnycklar som krävs för att uppnå en rimlig säkerhet. Algoritmer har skiftande drag, och det är ingen idé att jämföra nyckelns längd mellan olika krypteringssystem. Normalt behöver asymmetriska krypteringsalgoritmer betydligt längre nycklar för att nå samma säkerhetsnivå som symmetriska algoritmer. Som exempel kan ges om svårigheten att knäcka en symmetrisk kryptering med 56-bitars nyckel. Det tar cirka 38 år med en snabb persondator, men cirka.12 sekunder med en superdator. Att göra nycklarna längre har vissa nackdelar. Antingen blir krypteringen eller dekrypteringen långsam beroende på använd metod. [Kessler, 2004]

Om man antar att man bygger en dator som kan knäcka en 56-bitars DES nyckel på en sekund, skulle det innebära att det tar 149 triljoner år att knäcka en 128-bitars AES nyckel med samma dator. Som jämförelse kan nämnas att universum antas vara mindre än 20 miljarder år gammalt. Därav anses 128-bitars symetriska nycklar omöjliga att knäcka om det ej finns någon svaghet i algoritmen. [NIST, 2002]

Nyckelkvalitet

Nycklar räknas fram genom att en programvara tar fram slumptal, detta kallas pseudo-slumptalsgenerering. Slumptalen från en pseudoslumptalsgenerator är inte riktiga slumptal de har bara likartade egenskaper från riktiga slumptal [Wikipedia 3, 2004]. Mycket noggrann matematisk analys krävs för att försäkra att de genererade numren är tillräckligt slumpartade. Ett slumptal läggs sedan in i en matematiskformel, vilken räknar fram en nyckel. Slumptal är mycket svårt för en dator att generera. För att skapa många nycklar krävs bra slumptalsgeneratorer. Ingen nyckel får vara den andra lik, så att man ej kan se ett mönster [PKI-forum, 2004].

Råstyrkeattack

En råstyrkeattack är i dagens läge det enda sättet att knäcka välgjord kryptering. Det innebär att man prövar alla möjliga krypteringsnycklar. Desto längre krypteringsnyckel man har desto längre tid tar det att knäcka krypteringen. För varje bit som läggs till i nyckellängden fördubblas antalet möjliga nycklar. [Kommunikationsverket, 2004]

5.1.1 Taktisk kryptering

Det finns två tillvägagångssätt vid kryptering av data på bärbara datorer [WinMagic, 2003]:

- **Taktiska system:** krypterar enbart markerade filer eller kataloger
- **Strategiska system:** krypterar all data på enheten, sektor för sektor.

Med taktisk kryptering menas att användaren själv får välja vilka kataloger och filer som skall vara krypterade. Detta ställer större krav på den enskilde användaren. Prestanda-implikationerna blir inte lika omfattande vid taktisk kryptering då systemfiler och liknande ej behöver krypteras.

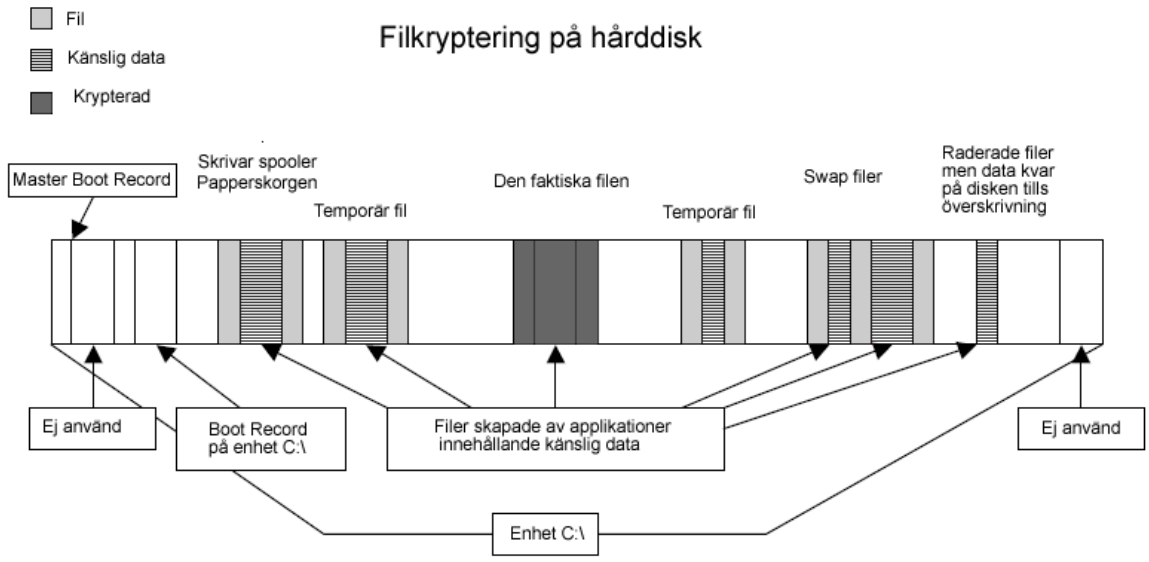
Taktiska system kan exponera hemlig information då känslig information kan finnas utanför filen den är lagrad i. Det är exempelvis möjligt att temporära filer som skapas medan ett dokument editeras innehåller klartext från dokumentet. I händelse att datorn kraschar eller stängs av på ett felaktigt sätt samtidigt som känsliga dokument är öppna, kan systemfilerna komma att innehålla klartext från dessa dokument. Dessa filer kan lämna spår av klartext på hårddisken och kan återfås genom avancerade tekniker för återskapning av data.

5.1.1.1 Manuell filkryptering

Manuell filkryptering innebär att användaren väljer vilka filer han vill kryptera för att skydda dem från att läsas av andra. Denna form av kryptering kräver ej att man går djupt in i operativsystemet för att använda. [WinMagic, 2003]

Filkryptering används vanligen för att skicka filer över Internet. En användare krypterar manuellt de filer han vill skydda från att läsas av obehöriga [WinMagic, 2003]. Denna metod är dock långsam, speciellt när det involverar stora mängder data att kryptera. Manuell filkryptering krypterar bara själva filen, temporära filer och swapfiler är ej krypterade, vilket man kan se i figur 6, och kan återfinnas i klartext [PCPlus, 2000]. Saknaden av transparens är även det ett problem [WinMagic, 2003]. En användare kan glömma att kryptera en fil och

lämnar den därmed oskyddad. Filkrypteringsapplikationer är därmed acceptabla för att skicka filer från dator till dator via exempelvis e-mail, men kan ej skydda lagrad data effektivt eller komplett.



Figur 6, Filkryptering på hårddisk (översatt och bearbetad från engelska av författarna). [Winmagic, 2003, s. 6]

5.1.1.2 Mappkryptering

Mappkryptering innebär att användare kan välja mappar vars innehåll krypteras automatiskt när filer sparas i dem. Mappkryptering är mer transparant för användaren än filkryptering, då han ej behöver välja manuellt vilka filer som skall krypteras i applikationen, utan bara behöver spara dem i en av de krypterade mapparna. Båda är däremot filbaserade vilket betyder att de bara krypterar de valda filerna/mapparna. Mappkryptering kräver att man går djupare in i operativsystemet då applikationen måste genskjuta operativsystemets filaccess. Detta därför att krypteringsapplikationen måste hålla reda på om en fil blir flyttad till eller från en krypterad mapp och därefter genomföra antingen kryptering eller dekryptering. [WinMagic, 2003]

Mappkryptering tillhandahåller inte skydd av temporära filer, swapfiler, gömda partitioner, raderade filer eller ledigt hårddiskutrymme, vilket illustreras i figur 7 [PCPlus, 2000]. Mappkryptering kräver mycket resurser av processorn för att kontrollera filaccess och gör även att filerna tar upp mer utrymme på hårddisken [WinMagic, 2003]. Detta gör mappkrypteringsapplikationer långsamma att använda.

5.1.1.3 Virtuell diskkryptering

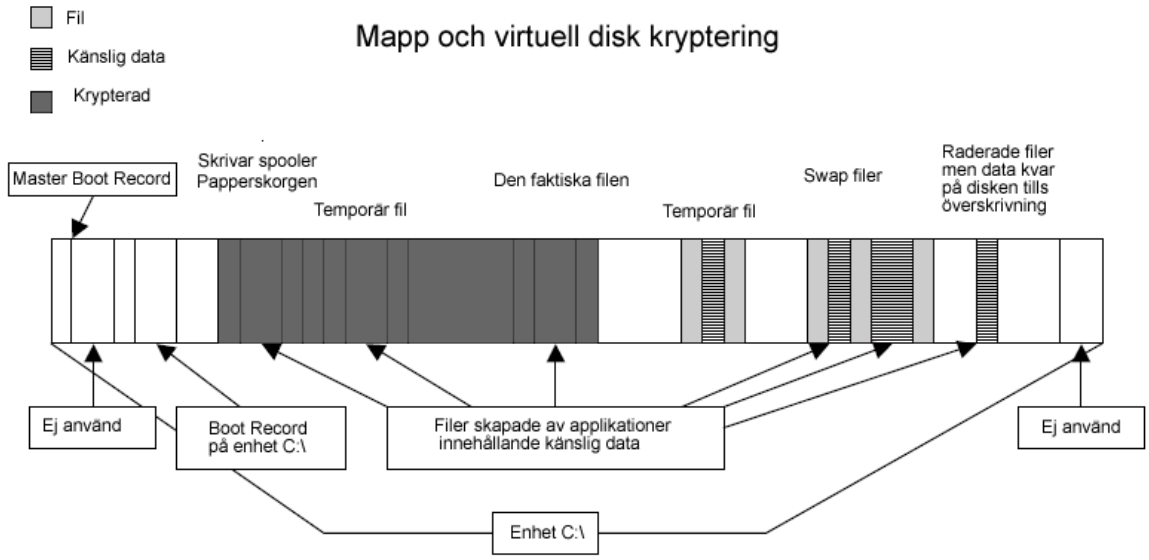
Virtuella diskkrypteringsapplikationer skapar en stor, gömd fil som den organiserar och presenterar inför operativsystemet som en ny logisk enhet, exempelvis x:\. [DeMaria, 2002]

All data placerad på den virtuella disken blir krypterad. Krypteringsapplikationen behöver ej kryptera var fil för sig, utan filerna krypteras automatiskt när de skrivs eller läses.

Krypteringsprocessen sker på nivån där data hanteras som sektorer, vanligtvis delar om 512 bytes, vilket gör att metoden är sektorbaserad istället för filbaserad. [WinMagic, 2003]

Virtuell diskkryptering har dock enligt [WinMagic, 2003] och [DeMaria, 2002] ett antal nackdelar:

- Virtuell diskkryptering använder mer resurser på grund av att den måste omdirigera diskaccess till en annan fysisk fil. Detta gör därmed systemet långsammare.
- Operativsystemet känner inte igen en virtuell disk som en verklig fysisk disk vilket innebär att operativsystemet vägrar att skapa temporära filer och swapfiler på en virtuell hårddisk.
- Virtuelldiskkryptering skyddar ej temporära filer eller swapfiler vilket illustreras i figur 7.
- Faktumet att en virtuell hårddisk i verkligheten är en fil gör den känslig för radering av andra applikationer eller användaren. Om en annan applikation skriver över denna fil eller skadar den innebär det att all information lagrad på den virtuella enheten kan förstöras.



Figur 7, Mapp- och virtuell diskkryptering (översatt från engelska och bearbetad av författarna) [Winmagic, 2003, s. 6]

5.1.1.4 Säkerhetssystemet i Windows XP

I den här sektionen beskrivs åtkomstkontrollen och krypteringssystemet i Windows XP.

Säkerhet via integritet

Windows XP har ett säkerhetssystem som använder sig av integritet för att uppnå säkerhet. Det betyder att alla systemresurser såsom skrivare och filer har en ägare som kan bestämma över rättigheterna för filen eller resursen, exempelvis vilka användare som har åtkomst till en given fil. Resursen ägs vanligtvis av den som skapade den, du äger till exempel som standard en fil du skapat. Användare som är systemadministratörer kan dock ta över ägarskapet av resurser de ej skapat själva. [Bott, Siechert, 2002]

NTFS

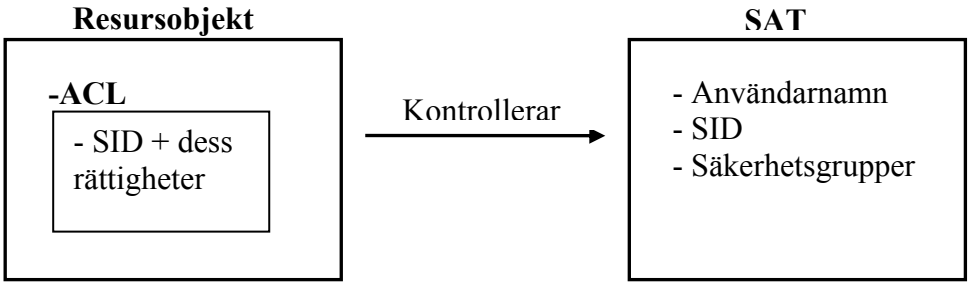
Filsystemen är en viktig del av säkerhet i ett operativsystem. Den här sektionen beskriver de filsystem som är tillgängliga i Windows XP, New Technology File System (NTFS), File Allocation Table 16 (FAT16), och FAT32, samt förklarar varför NTFS bör användas. [Souppaya, Johnson et al, 2004]

När det gäller säkerhet är NTFS överlägset de andra filsystemen som Windows XP tillhandahåller, FAT16 och FAT32, vilka Windows XP stödjer av kompabilitetsskäl. Dessa används av MS-DOS, Windows 95, Windows 98 och Windows Me. FAT16 och FAT32 konstruerades dock ej med säkerhet i åtanke. Varken FAT16 eller FAT32 har funktioner för åtkomst kontroll av filer eller kryptering av filer. Windows XP använder NTFS version 3.1. [Bott, Siechert, 2002; Souppaya, Johnson et al, 2004]

Åtkomstkontroll

Windows XP tilldelar alla användarkonton ett säkerhets-ID (SID) för att kunna avgöra vilka användare som har åtkomst till en resurs. Ditt SID är ett stort tal som är garanterat unikt inom nätverket och följer dig överallt i Windows XP. När du loggar in kontrollerar Windows först ditt användarnamn och lösenord. Efter det skapas ett System Access Token (SAT). Det innehåller ditt användarnamn och SID, samt information om eventuella säkerhetsgrupper som ditt konto tillhör. Alla program som startas får en kopia av dit SAT. [Bott, Siechert, 2002]

När man sedan försöker komma åt en resurs, exempelvis en skrivare, kontrollerar operativsystemet ditt SAT och avgör huruvida du har rättighet att använda skrivaren eller ej. För att bestämma detta tittar Windows på resursens access control list (ACL). Resursens ACL är en lista med SID:ar och med de åtkomsträttigheter som gäller för vart och ett. Alla resursobjekt har en ACL. [Bott, Siechert, 2002]



Figur 8, Åtkomstkontroll i Windows XP.

Behörigheter och rättigheter

Windows skiljer mellan två olika typer av åtkomsträttigheter. Dessa är behörigheter och rättigheter. En behörighet är möjligheten att komma åt ett objekt på ett definierat sätt, exempelvis att kunna skriva till en fil eller att kunna radera en fil. En rättighet är möjligheten att kunna utföra en åtgärd som gäller hela systemet, t. ex att logga in eller att ställa om klockan. [Bott, Siechert, 2002]

Ägaren av en resurs eller en systemadministratör är den som hanterar åtkomsten till resursen. Äger du t. ex en skrivare eller är administratör kan du hindra någon från att använda en specifik skrivare. [Bott, Siechert, 2002]

Encrypted File System

I Windows 2000 introducerade Microsoft Encrypted File System (EFS). EFS är ett krypteringsverktyg inbyggt i operativsystemet som, om det används, höjer säkerheten för filer som tidigare bara skyddats via Access Control Lists (ACL). Största anledningen till denna funktion är att Windows XP:s säkerhetssystem enkelt kan tas förbi av en angripare med fysisk tillgång till datorn. Ett antal lättåtkomliga applikationer kan användas för att tillhandahålla läs- och skrivaccess till data lagrad på NTFS-volymer genom att kringgå operativsystemets säkerhetsskydd. När en dator startar från en CD, diskett eller USB-minne med drivrutiner för NTFS, blir hårddisken och all dess data enkelt åtkomlig. Genom att använda EFS kan man hemlighålla data även om angriparen har fysisk åtkomst till den. [McIntosh, 2001]

EFS använder ett publikt-privat nyckelpar och en nyckel per fil för att kryptera och dekryptera data. När en användare krypterar en fil, genereras en filkrypteringsnyckel (FEK) som används för att kryptera data. Denna nyckel krypteras sedan med användarens publika nyckel och den krypterade nyckeln blir lagrad med filen. När filen sedan skall dekrypteras används först användarens privata nyckel för att dekryptera filkrypteringsnyckeln och sedan filkrypterings-nyckeln för att dekryptera data. På så sätt finns informationen lagrad på hårddisken men i krypterat format och kan ej läsas utan tillgång till den privata nyckeln. [Microsoft, 2004; Souppaya, Johnson et al, 2004]

Kryptera fil
1. Generera FEK 2. Kryptera filen med FEK 3. FEK krypteras med användarens publika nyckel 4. Krypterad FEK lagras med filen
Dekryptera fil
1. Dekryptera filens FEK med användarens privata nyckel 2. Dekryptera filen med FEK

Tabell 4, Kryptering och dekryptering med EFS.

Nackdelar med EFS

Med EFS måste man välja vilka filer eller mappar som skall krypteras manuellt. Detta kan innebära problem, då många program använder sig av temporära filer och säkerhetskopior som kan ha lagrats i en mapp vilken du ej har valt att kryptera. När man valt vilka mappar som skall krypteras görs kryptering och dekrypteringsprocessen i bakgrunden. Det betyder att du arbetar med krypterade filer på samma sätt som du gör med ej krypterade filer. När Windows upptäcker att en krypterad fil öppnas letar systemet reda på ditt certifikat och

använder dess privata nyckel för att dekryptera data allt eftersom den läses från disken. [Bott, Siechert, 2002]

Trots att EFS krypterar filer finns det fortfarande inget bootskydd. Det innebär att vem som helst kan starta datorn från CD-ROM, USB-minne eller diskett. [Utimaco EFS, 2004] [Souppaya, Johnson et al, 2004]

EFS finns endast tillgänglig för NTFS5 volymer. FAT-16, FAT-32, NTFS 4 och HPFS (High Performance File System) volymer kan ej krypteras med hjälp av EFS. Detta medför att filer på CD-ROM skivor och disketter ej går att kryptera med EFS. [Utimaco EFS, 2004] [Souppaya, Johnson et al, 2004]

EFS blir först tillgänglig efter Windows loginskärm, Graphical Identification and Authorization(GINA). Det innebär att alla filer som behövs för uppstart av datorn, innan loginskärmen, ej kan krypteras. Flera av dessa filer kan innehålla känslig information, exempelvis swapfilen, systemfiler och boot.ini. [Utimaco EFS, 2004]

EFS använder den symmetriska krypteringsalgoritmen DESX med 40-bitars nycklar i den internationella versionen och 128-bitars 3DES nycklar i USA och Kanada. 40-bitars nycklar kan numera enkelt knäckas och anses idag inte längre vara säkra mot angrepp [Utimaco EFS, 2004]. Windows XP uppgraderat med Service Pack 1 använder sig av Advanced Encryption Standard (AES) som algoritm vid kryptering [Souppaya, Johnson et al, 2004]. Nyckellängden är valbar av användaren och kan vara 128, 192 eller 256 bitar lång. Man kan även välja kryptering med 3DES, då är nyckellängden antingen 112 eller 168 bitar [Microsoft 3, 2004].

EFS är ett krypteringsverktyg för användaren. Detta innebär att användaren själv ansvarar för vilka filer och kataloger som skall vara krypterade. Det är därför omöjligt för t. ex ett företag att veta om konfidentiella filer verkligen är krypterade. Det är omöjligt att kryptera ett helt system med EFS. Om man väljer att kryptera alla kataloger på datorn lagras ändå all data som sparas i roten av en volym eller i en ny mapp, i klartext. [Utimaco EFS, 2004]

Under EFS krypteringsprocess lagras en kopia av filen i klartext för att den ej skall raderas utifall att processen misslyckas. De här kopiorna raderas, men ligger kvar på hårddisken tills de skrivs över av ny data. [Utimaco EFS, 2004]

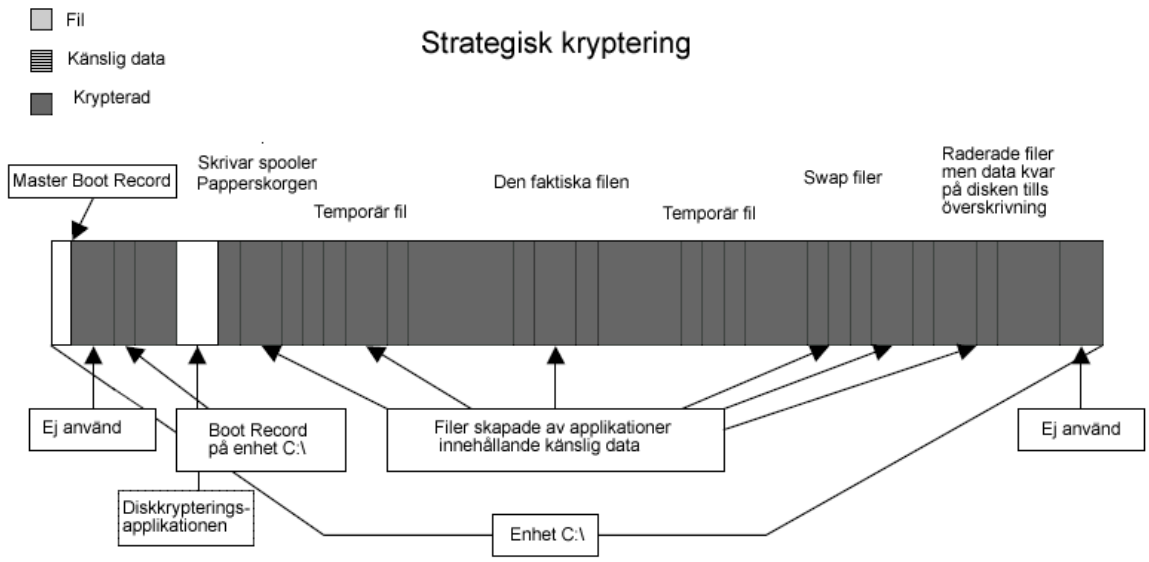
Inga varningar utfärdas när krypterade filer sparas eller transporteras i klartext. Om en fil sparas på en CD-ROM meddelas ej användaren om att den sparas i klartext. När en krypterad fil skickas över nätverket till en annan NTFS5 partition, krypteras den när den kommer fram men skickas i klartext (förutom när Web Distributed Authoring and Versioning (WebDAV) används, vilken sänder filer krypterade över nätverket). Detta innebär att användare måste skicka sina filer genom ett separat krypteringsprotokoll, t. ex SSL/TLS eller IPsec. [Utimaco EFS, 2004; Souppaya, Johnson et al, 2004]

5.1.2 Strategisk kryptering

Nackdelen med taktisk kryptering är att den krypterade filen kan återfinnas på någon annan plats inom hårddisken, exempelvis swapfilen, temporära filer skrivar-spoolern etc. För att skydda även dessa filer krävs att man krypterar hela hårddisken, förutom Master Boot Record och diskkrypteringsapplikationen. Detta illustreras nedan i figur 9. Eftersom hela hårddisken

krypteras, inklusive operativsystemet, måste krypteringsapplikationen startas före operativsystemet. För att åstadkomma detta byter programmet ut bootloadern som vanligtvis startar operativsystemet. Denna startar efter bytet istället krypteringsprogrammet som börjar med att autentisera användaren (pre-boot autentisering). Detta kan göras med användarnamn och lösenord samt stark autentisering med någon form av token. [DeMaria, 2002]

Med strategisk kryptering menas att hela hårddisken krypteras, sektor för sektor. Det betyder att användaren inte behöver besluta vilken information som skall krypteras eller ej. Detta är dock mer prestanda krävande då hela operativsystemet är krypterat. Kritiskt för lösningen är krypteringsnycklarna, hur de lagras och hur de räknas fram. [Utimaco, 2004]



Figur 9, Strategisk kryptering (översatt och bearbetad av författarna). [Winmagic, 2003, s. 8]

5.1.2.1 Datorns startsekvens

När datorn slås på finns det inget operativsystem i minnet, datorns hårdvara kan inte utföra de komplicerade funktionerna som ett operativsystem kan, exempelvis som att starta ett program från hårddisken. Därav skapas en paradox: för att ladda operativsystemet i minnet måste det redan finnas ett operativsystem. Appendix A beskriver datorns bootsekvens mer utförligt.

Bootloader

Lösningen på denna paradox ges genom att använda ett litet program, kallad bootloader eller BIOS (Basic Input/output System). Detta program har ej samma funktionaliteter som ett operativsystem men är skräddarsytt för att starta tillräckligt med funktioner för att operativsystemet skall starta. Ofta används bootloaders i flera steg där ett flertal små program kallar på varandra tills de sista av dem startar operativsystemet. Processen börjar med att datorns processor exekverar mjukvara i en ROM (Read Only Memory) på en fördefinierad adress. Denna mjukvara innehåller grundläggande funktioner för att söka efter enheter lämpade att delta i startprocessen. Ett litet program laddas från en speciell sektion av den bäst lämpade enheten exempelvis en hårddisk på datorn. Den första delen av bootloadern kallas Master Boot Record (MBR) och är alltid 512 bytes lång. Denna slutar med ett värde som

lyder AA55h, vilken BIOS söker efter för att försäkra sig om att det är en korrekt bootloader. [Russinovich, 1998]

MBR är alltid lokaliserad på cylinder 0, huvud 0 och sektor 1, vilket är den första sektorn på disken. Det är den fasta startpunkten som hårddisken alltid använder [Bott, Siechert, 2001]. Om denna sektor hittas laddas den in i minnet och testas för en godkänd signatur. Saknas en MBR eller en godkänd signatur stoppas bootsekvensen med ett meddelande som kan se ut på följande sätt: NO ROM BASIC - SYSTEM HALTED. När BIOS startar maskinen, letar den här efter instruktioner och information om hur den skall starta hårddisken och ladda operativsystemet. MBR innehåller Master Partition Table. Denna tabell innehåller beskrivningar om partitionerna som finns på hårddisken. Det finns bara plats i tabellen för information om fyra partitioner då den är väldigt liten. Därför kan en hårddisk bara ha fyra riktiga partitioner även kallade primära partitioner. En av partitionerna är markerad som aktiv partition vilket indikerar att det är den datorn ska använda vid bootprocessen. [Mossywell, 2003] [Kozierok, 2001]

MBR innehåller Master Boot Code vilken BIOS laddar och exekverar för att starta bootsekvensen. Detta program överför sedan kontrollen till boot-programmet lagrat på den partition som används för att starta datorn. Processen att installera multipla operativsystem på en dator involverar vanligen att byta ut original Master Boot Code mot en kod som tillåter användaren att välja en specifik partition att ladda i nästa steg av processen. På grund av att informationen lagrad i MBR är så viktig, skulle en skada innebära stor förlust av data. Eftersom Master Boot Code är det första program som exekveras när du sätter på din dator, är det en vanligt förekommande angreppspunkt för virus och andra attacker. [Kozierok, 2001] [Bott, Siechert, 2001]

Bootloader steg två

Efter den första bootloadern startas nästa bootloader. Denna startar sedan det riktiga operativsystemet. I Windows XP heter denna Ntldr. Denna laddar bl. a. drivrutiner och andra applikationer som krävs för att starta operativsystemet. Startprocessen anses färdig när datorn kan svara på kommandon från användaren. [Russinovich, 1998]

När man använder en strategisk krypteringsapplikation byter man ut MBR så att denna startar krypteringsapplikationen. Detta innebär att fas 1 av startprocessen ej kan krypteras, det vill säga datorns MBR. Den andra fasen krypteras dock i och med att krypteringsprocessen startas direkt efter inläsning av MBR. Det gör den ej vid användande av taktiska krypteringsapplikationer. Taktiska krypteringsapplikationer kan endast startas efter det att operativsystemet startats. Detta gör dem oförmögna att kryptera någon av startfaserna.

5.1.2.2 Pre-boot Autentisering (PBA)

Alla strategiska hårddiskkrypteringsapplikationer börjar med att användaren får autentisera sig innan operativsystemet startats. Pre-boot autentiseringsapplikationer brukar bestå av tre olika säkerhetsprocesser enligt [Utimaco, 2004]:

- Pre-boot Autentisering
- Bootskydd
- Kryptering

Pre-boot autentiseringen gör så att ingen kan komma åt information på datorn som inte är behörig. Användaren måste logga in med användar-id och lösenord, eller annan metod för att kunna starta operativsystemet och komma åt information på hårddisken. Inga uppgifter om lösenord och användar-id sparas på hårddisken, därför kan man vara säker på att bara autentiserade personer kan starta upp datorn. Ett potentiellt angreppssätt är att använda råstyrka, vilket går ut på att prova alla lösenord tills man hittat det rätta. För att skydda sig mot detta använder sig applikationerna av olika tekniker, exempelvis en teknik som gör att för varje felaktig lösenord, fördubblas tiden man måste vänta för att slå in nästa, eller att man bara har ett givet antal försök innan kontot spärras. [Utimaco, 2004]

5.1.2.3 Bootskydd

Under bootsekvensen är operativsystemet ännu inte aktivt. Därför är operativsystemets säkerhetsmekanismer ej heller fungerande, exempelvis MBR som sköter den pågående bootsekvensen skyddas ej av operativsystemet. MBR attackeras ofta av en vanlig form av datavirus - bootsektorvirus. Dessa sprider sig genom att kopiera sig själva till alla boot-sektorer på alla lagringsenheter som används. Dessa virus kan blockera, manipulera och radera filer och enheter. [Utimaco, 2004]:

Bootskydd medför två saker enligt [Krause, 2002; Reichert, 2004; Utimaco, 2004]:

- Tvingar uppstart från hårddisk

  Bootskydd hindrar datorn från att starta upp från lagringsenheter andra än den lokala hårddisken. Detta är viktigt därför att användandet av andra lagringsenheter kan medföra att uppstart av operativsystem kan undvikas och att attackeraren skulle kunna ge sig själv administratörrättigheter på datorn. Detta skulle medföra att han fick tillgång till alla filer. Pre-boot autentiseringsapplikationer medför att bara autentiserade användare kan starta från hårddisken.

- Master Boot Record Skydd

  Master Boot Record är väl skyddat. Om applikationen upptäcker att MBR har blivit manipulerad eller modifierad på något sätt av exempelvis virus, tvingar den datorn att använda original MBR. Första gången applikationen installeras görs en kopia av original MBR. På så sätt skyddar applikationen mot bootsektorvirus.

5.1.3 Autentiseringsprocessen vid strategiskkryptering

Centrala funktioner i PBA applikationen måste exekveras innan operativsystemet startas eftersom operativsystemet är krypterat. Vid den här tidpunkten finns det ingen support tillgänglig från operativsystemet. Mängden programkod som krävs innan boot av OS är mellan 64-128 kb av exekverbar kod. Denna kod är lagrad på hårddisken som en fil. Innan boot laddas denna kod av en loader som har ersatt den traditionella MBR record. Platsen som koden är lagrad på hårddisken är beskriven som ett logiskt sektornummer vilken lagras i en tabell på sektor två. Denna information ligger i en MBR tabell. Tabellen innehåller kodlängden samt lagringsplatsen för användar-login dialogen. Original MBR, som fanns innan PBA applikationen installerades, är lagrad på två oanvända sektorer på hårddisk spår 0.

Denna sektor behövs när PBA applikationen ska avinstalleras. Den nya MBR efter det att PBA applikationen installerades, vilket är en loader för PBA applikationens huvudmodul, är också kopierad och lagrad på hårddisk spår 0. Därför kan ett system med en skadad sektor enkelt repareras. [Krause, 2002; Reichert, 2004]

Vid boot finns det ingen USB-support tillgänglig. Detta betyder att en av uppgifterna som PBA applikationens huvudmodul har, är att aktivera USB-gränssnittet. När USB-gränssnittet är aktiverat söker PBA:n efter aktiva kortläsare eller USB-token inkopplade i USB-porten. När det är gjort utförs en första kontroll för att se om användaren har stoppat in det korrekta kortet/token. Innan man får åtkomst till data på kortet måste användarautentiseringen vara gjord. Nu implementeras en bakgrundsmekanism som kommer att upptäcka om kortet/token tas bort innan inloggningsprocessen är färdig. [Krause, 2002]:

Användarautententisering är en process som är integrerat i operativsystemet i det aktiva kortet/USB-token. Innan datafilerna på kortet blir tillgängliga måste lösenordsdialogen framträda. Lösenordet som skrivs in av användaren krypteras och används som pinkod för att få tillgång till den första filen på det aktiva kortet, den så kallade lösenordsfilen. Om användaren skriver fel lösenord får man ingen åtkomst till filen över huvudtaget. Efter ett antal felaktiga försök blir åtkomsten till lösenordsfilen låst. Om man skriver in korrekt lösenord får man tillgång till lösenordsfilen som läses av PBA applikationens huvudmodul. Information från lösenordsfilen avgör strategin för lösenordsbyte och andra policys som krävs av inloggningsprocessen. [Krause, 2002]

5.2 Prestanda implikationer

När man använder en krypteringslösning måste man tänka på prestandakostnaderna. Det kan vara opassande att använda en sådan lösning om prestandakostnaderna blir för höga. Alla kryptosystem kommer att ta prestanda från processorn om man inte har en dedikerad kryptoprocessor, vilket dock är ovanligt i mobila enheter. [Sadlier, 2003]

5.3 Nyckelhantering

Nyckelhantering är en viktig fråga när man använder kryptografiska system. Organisationen måste kunna bevara möjligheten att upprätthålla sin säkerhetspolicy. Främst måste det enligt [Sadlier, 2003] vara möjligt att:

- Upprätthålla säkerhetskrav i form av krypteringsalgoritm, nyckel och lösenordsstyrka.
- Återställa data från mobila enheter utan ägarens inblandning exempelvis om användaren glömmer sitt lösenord, blir otillgänglig eller vägrar att samarbeta.
- Integrering med organisationens Public Key Infrastructure (PKI) kan vara ett kraftigt verktyg vid nyckelhantering i stora organisationer.

När nycklarna genereras måste det ske centralt, antingen med organisationens Additional Decryption Key (ADK) eller med en metod där man bevarar nyckeln och lagrar den säkert. Detta på grund av att det ej får vara möjligt att generera en krypteringsnyckel som hemlighålls för organisationen. Informationen måste kunna dekrypteras om användaren förolyckas eller försvinner. [Sadlier, 2003]

5.4 Vanliga problem för hårddiskkrypteringsapplikationer

I den här sektionen beskrivs vanliga problem för hårddiskkrypteringsapplikationer och vad det kan medföra.

5.4.1 Temporära filer

Temporära filer skapas av många mjukvaror för att spara data medan en fil är öppen, många gånger för att spara en kopia av filen i fall att något oväntat skulle ske med datorn, exempelvis strömavbrott. Temporära filer används även av webbläsare, e-mailklienter samt allehanda Windowsfunktioner. Windows låter dig bestämma var dina temporära filer skall lagras men många applikationer väljer att lagra dem på andra ställen. Dessa filer är viktiga men skapar en säkerhetsrisk om de ej krypteras när de skapas. [Protectdata, 1999]

5.4.2 Sidväxling

Sidväxling används frekvent i moderna operativsystem. När sidväxling sker innebär det att Windows skriver data på hårddisken från primärminnet, i minnessidor, utifall att primärminnet tar slut. Detta innebär att datorn tror att den har mer minne än den verkligen har. När data som skrivits på hårddisken behövs igen läser operativsystemet in den i primärminnet och flyttar ut data från primärminnet till hårddisken. Det betyder att operativsystemet kan lagra vilken data som helst på hårddisken, inklusive känslig data man som användare tror är skyddad, i klartext. [WinMagic, 2003]

5.4.3 Papperskorgen

När en fil raderas flyttas den till papperskorgen. Användaren kan sedan återställa de raderade filerna ända till det han väljer att tömma papperskorgen. Även om man har tömt papperskorgen finns filerna kvar fysiskt på hårddisken, och kan enkelt återskapas med hjälp av program gjorda för detta ändamål. De raderade filerna kan återskapas ända tills de skrivs över av andra filer. [WinMagic, 2003]

5.4.4 Viloläge

Viloläge används ofta på bärbara datorer för att spara på batterierna då den är på men ej används. När datorn går in i viloläge sparar den all data från primärminnet till hårddisken. Detta gör att datorn kan återgå till exakt samma läge den var i innan viloläget. Det innebär att känslig information kan sparas på hårddisken från primärminnet, inklusive krypterings-nyckeln som används av hårddiskkrypteringsprogrammet. Många krypteringsprogram kan ej hantera data säkert på en dator med viloläge. Detta innebär ett stort problem för datorer med viloläge då många användare tror att datorn är avstängd när den gått in i det läget. [Utimaco, 2004]

5.4.5 Gömda partitioner

En gömd partition är en del av hårddisken som operativsystem såsom Windows ej kan upptäcka. Vissa applikationer använder dessa partitioner för att spara data på. Vissa applikationer sparar data kontinuerligt på en gömd partition istället för i en fil på en normal

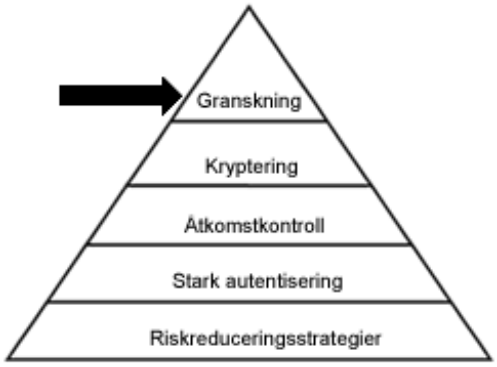
partition när datorn går in i viloläge. Detta innebär att information sparas i klartext på dessa partitioner, utan skydd. [WinMagic, 2003]

5.4.6 Ledigt utrymme och utrymme mellan partitioner

Sektorer i slutet på diskar som inte tillhör någon partition kan visas som ledigt utrymme. Andra oanvända sektorer hittas mellan partitioner och utvidgade partitionstabeller. Vissa applikationer och virusprogram använder detta utrymme för att spara data på. Även när en hårddisk formateras förblir data på dessa sektorer orörd och kan återställas. [WinMagic, 2003]

6 Granskning

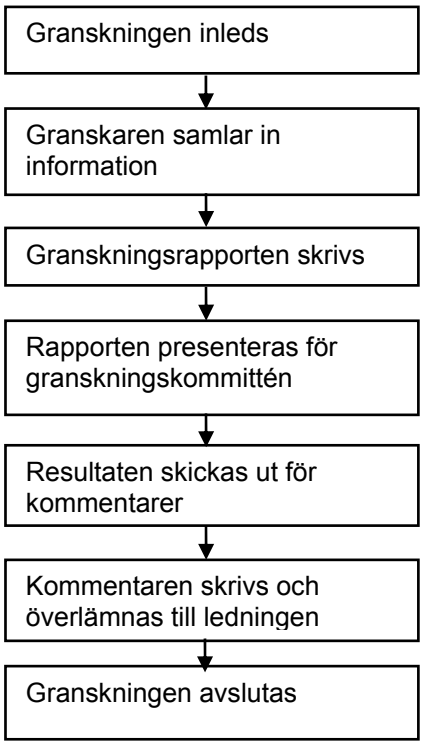
Granskning är en process som skall genomföras regelbundet. Granskning är en viktig del för att upptäcka intrång i systemet och för att avgöra vad som hände och hur. Detta innebär att ett effektivt subsystem för granskning är en viktig del i alla säkerhetssystem. [Bishop, 2003]



Figur 10, Säkerhetspyramiden - Granskning

Informationssystemets säkerhet för bärbara datorer bör kontrolleras regelbundet. Sådana kontroller bör ske mot tillgängliga säkerhets-riktlinjer. [SIS, 2002]

Granskning är ett mycket välstrukturerat sätt att undersöka ett system eller en arbetsmetod. I allmänhet krävs andra färdigheter än dem som krävs för analyser, även om det är möjligt att hitta folk som både kan känna på sig var fara finns och granska att system efterlever regler. Säkerhetsavdelningen behöver ibland granska efterlevnaden av policy och standarder. En person som har kunskaper i granskningstekniker måste kunna peka ut områden där efterlevnaden inte är fullgod och överräcka sina resultat till företagsenheterna och andra medlemmar av säkerhetsavdelningen. Granskningsprocessen exemplifieras i figur 11. [Maiwald, Sieglein, 2002]



Figur 11, Granskningsprocessen. [Maiwald, Sieglein, 2002, s. 84]

7 Analys

Syftet med uppsatsen var att identifiera viktiga faktorer som kan påverka valet av en metod över en annan, för att skydda data på bärbara datorer med. Författarna har i uppsatsen presenterat ett flertal metoder för att skydda data och delat in dessa metoder i riskreduceringsstrategier, autentisering samt kryptering. Nedan följer resultatet av denna kartläggning stegvis presenterad i enlighet med säkerhetstriangeln.

7.1 Riskreduceringsstrategier

I alla delar av en organisations säkerhetsprogram är det viktigt att först analysera och förstå riskerna innan man bestämmer en strategi för riskreducering. När det gäller mobila enheter, bör en organisation först samla in information om antalet enheter som används, hur de används och vilken data som lagras på dem. Detta för att kunna avgöra vilken typ av säkerhet som krävs och vad som är ekonomiskt försvarbart.

Figur 12, Säkerhetspyramiden - Riskreduceringsstrategier

7.1.1 Utbildning och säkerhetspolicy

Det är viktigt att ha en tydlig policy och utbildning för att minska riskerna för att värdefull information blir stulen. Att förhindra stöld är den mest effektiva tekniken men man måste även ha policys i fall att förlusten blir ett faktum, exempel på detta är informations-klassifikationspolicys som definierar vilken typ av data som får lagras på bärbara enheter samt var. En organisation bör även ha en policy som beskriver hur användaren skall gå till väga vid förlust.

7.1.2 Alarm och kabellås

Det finns många produkter för att fysiskt skydda bärbara datorer, exempelvis kabellås, alarm med avståndssensor samt kombinationer av alarm och kabellås. Det är dock viktigt att användaren använder dessa och gör det till en rutin på samma sätt som han startar datorn och stoppar kontakten i väggen.

7.1.3 BIOS-lösenord & hårddiskslösenord

Accesskontroll med hjälp av BIOS-lösenord och hårddisklösenord kan vara ett sätt att skydda informationen på datorn. Problemet är att en tekniskt kunnig person enkelt kan ta sig förbi denna form av accesskontroll vilket riskerar att känslig information exponeras.

7.1.4 Avlägsna identifieringsmärkning

Genom att avlägsna identifieringsmärken minskar man intresset för informationen inuti datorn och gör att tjuven kanske bara formaterar hårddisken och säljer den. Annars finns risken att tjuven söker upp potentiella köpare av informationen, exempelvis företagets konkurrenter. Ytterligare ett steg att minska uppmärksamhet från din dator är att ej förvara den i en väska avsedd för en bärbar dator då dessa enkelt kan kännas igen av en tjuv.

7.1.5 Spårningsteknologi

Utifall att en bärbar enhet blir stulen finns det metoder att spåra den. Spårningsteknologi i form av en gömd applikation på hårddisken är en. Den försöker kontakta en central övervakningsstation, via telenätet eller Internet, och sedan rapportera sin position.

En riskreduceringsmetod utesluter ej en annan, och kan i de flesta fall kombineras. Flera av dessa strategier ger tillsammans en synergieffekt vilket leder till ökad säkerhet. Som exempel kan ges policy och utbildning. Om ett företag har en informationssäkerhetspolicy men ingen utbildning kring den, är risken stor att många anställda ej vet hur policyn skall efterlevas. Kombinerar man dock dessa blir resultatet ökad säkerhet och förståelse för riskerna och skyddsmetoderna.

Kartläggningen har resulterat i en uppdelning av riskreduceringsstrategierna i tre olika säkerhetskategorier. Dessa sammanställs i nedanstående tabell.

	Utbildning	Säkerhetspolicy	Alarm & kabellås	BIOS-lösenord & hårddiskslösenord	Spårnings-teknologi	Avlägsna id-märkning
Säkerhetsfaktorer						
Fysisk säkerhet	X	X	X			X
Accesskontroll innan OS				X		
Spårning					X	

X = JA

Tabell 5, Riskreduceringsmetoder

- Fysisk säkerhet

Faktor för att fysiskt skydda sin dator innan stöld. Här placeras utbildning, säkerhets-policy, alarm och kabellås samt avlägsna identifieringsmärkning.

- Accesskontroll innan OS

Förhindra åtkomst för obehöriga före operativsystemets uppstart.

- Spårning

Teknologi för att spåra en dator efter stöld.

7.2 Autentisering

Stark autentisering med två faktorer är idag viktigt för att hålla säkerheten på en god nivå. Att bara använda användarnamn och lösenord innebär många problem. Användare tenderar att skriva upp lösenord om de är för svåra att minnas och när de får skapa lösenorden själva blir de ofta svaga lösenord som kan återfinnas i en ordbok. Att förlita sig på enbart lösenord tillhandahåller ej en säker, lätthanterbar eller kostnadseffektiv lösning. Många företag behöver andra autentiseringsmetoder.

Figur 13, Säkerhetspyramiden - Stark autentisering

Bättre användarhantering och säkerhet kan ges med autentiseringsmetoder som använder hårdvaru-

komponenter, någonting du har, med ett lösenordssystem, någonting du vet eller med biometrisk identifiering, någonting du är. Författarna har kartlagt fem olika metoder för autentisering. Dessa är: lösenord, aktiva kort, USB-token, engångslösenord samt biometrisk identifiering. Författarna har jämfört olika säkerhetsfaktorer hos de utvalda metoderna. Resultatet av denna kartläggning redovisas nedan.

Kartläggningen har resulterat i en uppdelning av autentiseringsmetoderna i fem olika säkerhetsfaktorer. Dessa skiljer metoderna från varandra och kan påverka valet av en metod över en annan. Nedan följer en sammanställning av faktorerna:

- Tvåfaktorig
  Användandet av enbart lösenord anses idag ej vara en tillräckligt säkert, kostnadseffektivt och lätthanterbar lösning. Därför anser vi att det väldigt viktigt att autentiseringsmetoden möjliggör två faktorig autentisering.

- Användarvänlig
  En produkt måste vara användarvänlig om man vill att användarna skall använda dem på rätt sätt. Om det är krångligt att använda produkten ignorerar många användare de regler som är uppsatta kring produktens användning. Därav anser vi att det är en viktig faktor att beakta.

- Funktionellt lämplig på mobila enheter
  Vissa produkter lämpar sig bättre än andra för användandet till mobila enheter. Det är viktigt att produkten är liten och portabel och helst ej kräver extra utrustning.

- Skyddar mot råstyrkeattacker
  Om en bärbar dator kommer i orätta händer, har förövaren gott om tid att attackera systemet med råstyrka. Därför är detta en viktig faktor att tänka på gällande just bärbara datorer.

- Kan ej förloras
  Om datorn blir stulen tillsammans med den andra faktorn, exempelvis användarens USB-token, innebär det att bara lösenordet återstår för förövaren att ta sig förbi. Om den andra faktorn ej går att stjäla är det en stor fördel.

I tabell 6 följer en sammanställning av dessa fem faktorer relaterat till de autentiserings-metoder som tagits upp i kartläggningen.

	Lösenord	**Aktiva kort**	**USB-token**	**Engångslösenord**	**Biometri**
Säkerhetsfaktorer					
Två faktorig		**X**	**X**	**X**	**X***
Användarvänlig	**X**		**X**		**X****
Funktionellt lämplig på mobila enheter	**X**		**X**		**X*****
Skyddar mot råstyrkeattacker		**X**	**X**	**X**	**X**
Kan ej förloras					**X**

X = JA

* Kan kombineras med aktiva kort, USB-token eller engångslösenord för att få trefaktorig autentisering. ** Lider fortfarande av igenkänningsproblem. *** Funktionellt lämpligt endast om skannern är inbyggd i enheten.

Tabell 6, Autentiseringsmetoder.

7.2.1 Säkerhetsfaktorer

- Tvåfaktorig: Aktiva kort, USB-token, engångslösenord och biometri kan med fördel kombineras med ett lösenordssystem för att erhålla tvåfaktorig autentisering.

- Användarvänlig: USB-token är små och får plats på en nyckelring, aktiva kort kräver att man har en kortläsare, detta gäller även biometri som kräver en skanner. Engångslösenord kräver mycket administration med distribuering. Därav är USB-token att föredra för bärbara datorer ur användarvänligt syfte. Även lösenord anses användarvänligt i den mån användaren kommer ihåg sitt lösenord.

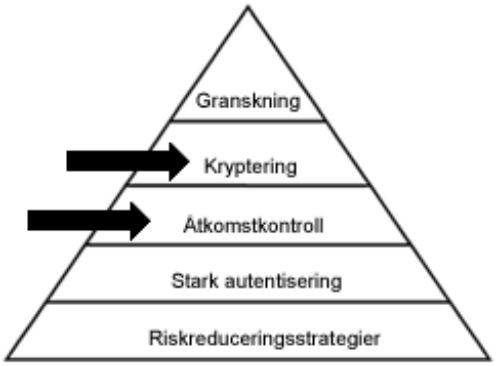
- Funktionellt lämplig på mobila enheter: Aktiva kort kräver kortläsare, biometri kräver skanner, engångslösenord kräver distribution. Därav lämpar sig lösenord och USB-token sig bäst på bärbara enheter.

- Skyddar mot råstyrkeattacker: Lösenord går att attackera med råstyrkeattacker, det innebär att man prövar alla tillgängliga kombinationer av lösenord. Det går ej att göra med aktiva kort, USB-token, engångslösenord eller biometri.

- Kan ej förloras: Vid biometrisk autentisering avläses ett personligt kännetecken exempelvis fingeravtryck eller irismönster. Detta gör dem i princip omöjliga att förlora till skillnad mot de övriga som lätt kan tappas bort eller bli stulna.

7.3 Kryptering

Ovan metoder kan förhindra stöld av bärbara datorer och autentiserar användaren, men man behöver även skydd för att göra informationen på enheten oåtkomlig för obehöriga. Åtkomstkontroll är en del av detta stycke då åtkomstkontroll ofta är integrerat med krypteringsapplikationerna eller Windows XP. För att åstadkomma detta behöver man hårddiskkryptering. Det finns många olika produkter för hårddiskkryptering men två olika distinkta tillvägagångssätt, taktisk och strategisk. Taktiska system krypterar enbart markerade filer och kataloger medan strategiska system krypterar hela hårddisken sektor för sektor. När man använder en krypteringslösning måste man tänka på prestanda kostnaderna. Det kan vara opassande att använda en sådan lösning om prestanda kostnaderna blir för höga.



Figur 14, Säkerhetspyramiden - Åtkomstkontroll och Kryptering

Författarna har studerat fem olika krypteringsmetoder: filkryptering, mappkryptering, virtuell diskkryptering, EFS samt strategisk kryptering. De fyra förstnämnda metoderna är alla varianter av taktiska krypteringssystem. Kartläggningen har resulterat i elva faktorer som skiljer metoderna från varandra. Nedan följer dessa faktorer:

- Skyddar individuella filer
  Innebär att metoden kan kryptera filer.

- Skyddar innehållet i en mapp
  Innebär att man kryptera allt innehåll i en mapp. Detta underlättar användandet av krypteringsapplikationen.

- Skyddar temporära filer
  Innebär att information som skrivits på hårddisken i form av en temporär fil skyddas av krypteringsapplikationen. Viktigt då nyligen använd information kan vara enkelt åtkomligt för en förövare om ej detta skydd finns.

- Skyddar raderade filer
  När man raderar en fil i Windows XP försvinner ej informationen förrän den skrivs över av annan information. Därav kan raderade filer återskapas och läsas om skydd mot detta ej finns.

- Skyddar filnamn
  Ibland räcker det med bara filnamnet för att känslig information skall komma ut. Om filnamnen ej kan läsas av en obehörig försvinner detta hot.

- Skyddar hela operativsystemet
  Operativsystemet består av en rad känsliga filer. Om dessa ej skyddas kan förövaren manipulera systemet och få tillgång till konfidentiell information.

- Tillhandahåller bootskydd
  Innebär att operativsystemets säkerhetssystem ej kan kringgås med hjälp av drivrutiner via CD-ROM, diskett eller USB-minne.

- Tillhandahåller pre-boot autentisering
  Innebär att autentisering sker innan operativsystemet startats. Detta medför att hela operativsystemet kan krypteras och det innebär ett extra autentiseringsskydd.

- Realtidskryptering/Realtidsdekryptering
  Innebär att krypteringen/dekrypteringen inte är märkbar för användaren. Detta medför att användaren ej behöver interagera med krypteringsapplikationen.

- Användaren behöver ej välja vad som ska krypteras
  Om användaren själv väljer vad som skall krypteras krävs att han/hon vet vilken information som är konfidentiell. Detta lägger ansvaret helt på användaren att använda krypteringsfunktionen.

I tabell 7 följer en sammanställning av dessa faktorer relaterat till de krypteringsmetoder som tagits upp i kartläggningen.

	Taktisk kryptering				Strategisk kryptering
	Fil-kryptering	Mapp-kryptering	Virtuell disk-kryptering	EFS	
Säkerhetsfaktorer					
Skyddar individuella filer	X	X	X	X	X
Skyddar innehållet i en mapp		X	X	X	X
Skyddar temporära filer					X
Skyddar raderade filer			X		X
Skyddar filnamn			X		X
Skyddar hela operativ-systemet					X
Tillhandahåller bootskydd					X
Tillhandahåller pre-boot autentisering					X
Transparensfaktorer					
Realtids kryptering		X	X	X	X
Realtids dekryptering		X	X	X	X
Användaren behöver ej välja vad som ska krypteras					X

X = JA

Tabell 7, Krypteringsskydd.

7.3.1 Krypteringsskydd

- Skyddar individuella filer: samtliga metoder har denna funktion
- Skyddar innehållet i en mapp: Endast filkryptering saknar denna funktion.
- Skyddar temporära filer: Då olika applikationer skapar temporära filer på för användaren okända positioner på hårddisken är det omöjligt för taktiska system att kryptera alla dessa filer. Enda sättet att säkert skydda temporära filer är genom att använda strategisk kryptering.
- Skyddar raderade filer: Då raderade filer inte verkligen raderas förrän de skrivs över av ny data innebär det att de kan återskapas. För att skydda dessa filer krävs antingen virtuell diskkryptering eller strategisk kryptering.
- Skyddar filnamn: Enbart ett filnamn kan ge mycket information till en hackare. Den berättar ofta om innehållet i filen. För att skydda denna information fordras virtuell diskkryptering eller strategisk kryptering.
- Skyddar hela operativsystemet. För att skydda hela operativsystemet krävs strategisk kryptering. Viktiga filer går ej att kryptera med de andra metoderna. Exempel på detta är filer som krävs för att starta Windows.

- Tillhandahåller bootskydd: Bootskydd innebär att datorn ej kan startas med en annan enhet, exempelvis CD-skiva, USB-minne eller diskett, för att ta sig förbi säkerhetssystemet på hårddisken. Enda metoden som tillhandahåller detta är strategisk kryptering.

- Tillhandahåller pre-boot autentisering: Med pre-boot autentisering menas att användaren autentiseras innan operativsystemet startas. Detta gör det möjligt att kryptera de filer som krävs av Windows startprocess. Endast strategisk kryptering erbjuder denna funktion.

- Realtidskryptering: Med realtidskryptering innebär att krypteringsprocessen sker automatiskt i bakgrunden och tillåter användaren att jobba med datorn som vanligt under tiden. Endast filkryptering saknar denna funktion.

- Realtidsdekryptering: Med realtidsdekryptering innebär att dekrypteringsprocessen sker automatiskt i bakgrunden och tillåter användaren att jobba med datorn som vanligt under tiden. Endast filkryptering saknar denna funktion.

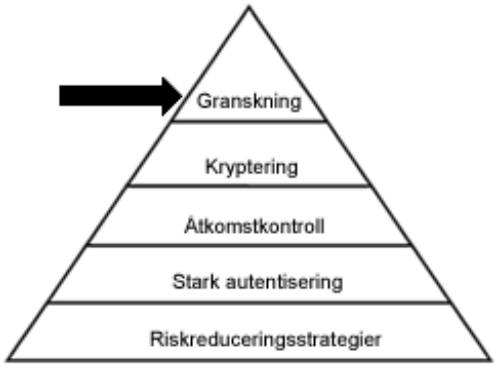
- Användaren behöver ej välja vad som ska krypteras: Detta innebär att användaren ej behöver ta eget ansvar över vilka filer som ska krypteras. Samtliga filer krypteras. Detta tillhandahålls enbart av strategisk kryptering

Det är omöjligt att helt eliminera risken att krypterad data blir åskådliggjord för obehöriga användare. Kryptering försvårar processen men gör det inte omöjligt. Risken kan reduceras till en acceptabel nivå men den kan inte bli helt eliminerad.

Även om det tar tusentals år att lösa ett krypto är det ändå en tidsfråga. Desto starkare nycklar som används desto längre tid tar det att lösa kryptot. Starkare nycklar kräver emellertid mer datorkraft och använder mer processor resurser.

Det är nästan alltid enklare för en obehörig användare att knäcka användarens lösenord med råstyrka än att knäcka krypteringsnycklarna. Därav är det viktigt att använda stark kryptering med lika stark autentisering - en tjuv behöver inte slå sönder fönstret om dörren är olåst.

Krypteringsstyrkan som en organisation använder för att skydda sina bärbara enheter måste kalkyleras baserat på en balans mellan kostnad, prestanda, hur lång tid organisationen behöver hålla informationen säker samt produktens autentiseringsstyrka.



Figur 15, Säkerhetspyramiden - Granskning

7.4 Granskning

Sista steget är att granska säkerhetssystemet det vill säga de övriga delarna i säkerhets-pyramiden. Om ett intrång har skett är det viktigt att ta reda på hur detta skett så att man kan förbättra systemet.

7.5 Scenariobeskrivning

I detta stycke redovisas hur resultaten är tillämpbara i praktiken genom att de appliceras på några välvalda scenarier. Dessa scenarier representerar olika behov av informationsskydd och visar vilken lösning som är bäst lämpad i varje enskilt fall.

Faktorer vi har tagit hänsyn till vid framställandet av dessa scenarier är:

- Storleken på organisationen: Om man har många användare av mobila enheter ökar risken att hemlig information hamnar i orätta händer. Stora organisationer har ofta större möjlighet att administrera utfärdandet av nycklar och lösenord samt större säkerhetsbudget.

- Grad av hemlig information: Om informationen anses mycket hemlig bör man vidta alla möjliga åtgärder för att förhindra stöld av information. Detta innefattar allt från företagshemligheter till personuppgifter. Exponering av viss information kan vara olaglig eller vara kritisk för människors liv och hälsa.

- Grad av mobilitet: Om organisationen har hög grad av mobilitet innebär det att risken ökar för en mobil enhet kan bli stulen eller borttappad. Organisationer med hög grad av mobilitet använder sina mobila enheter både under och efter arbetstid och på olika platser; exempelvis i hemmet, på tåget och under presentationer.

- Grad av datorkunskap: Om organisationen ifråga har anställda med stor datorkunskap, kan mer ansvar läggas på dem. Detta innebär att de anställda får ansvara för att hemlig information är krypterad. En aspekt är om datasäkerhetskunskapen är mycket stor kan det innebära att internt anställda vet hur man tillförskaffar sig hemlig information. Om detta är fallet och att man bedömer att risk finns för intern stöld, bör man använda sig av starkast möjliga skydd.

- Kostnader: En aspekt att tänka på är kostnaden av säkerhetssystemet. Som med alla riskhanteringsstrategier måste organisationer väga kostnaderna för säkerhet mot riskerna. Om den hemliga informationen ej anses vara alltför värdefull är det möjligt att organisationen ej behöver det starkaste och dyraste säkerhetssystemet. En stor kostnad är även hanteringen och utfärdandet av nycklar och lösenord.

Scenario 1: En stor organisation med mycket hemlig information och hög grad av mobilitet, exempelvis Polisen.

Mycket av det polisen arbetar med skyddas av sekretesslagen, och att glömma en dator med skyddsvärd information innebär med andra ord ofta brott mot sekrettesslagens bestämmelser. En glömd dator sker knappas uppsåtligen varför man inte dömer personer för uppsåtligt brott, men deras interna bestämmelser är hårdare. Där anges att skyddsvärda uppgifter skall vara under bevakning eller skyddas av en godkänd kryptering om informationen tas ut från skalskyddade områden. [Lindblom, 2005]

Exempel på vad förlorad information skulle innebära för Polisen är många och har ofta allvarliga konsekvenser. Om en bärbar dator skulle förloras under en pågående brotts-utredning kan det innebära att den misstänkte kan förbereda sig inför ett kommande förhör. Detta betyder att han kan anpassa sin berättelse efter informationen efter vad vittnen sagt. Även namngivna uppgiftslämnare finns dokumenterade på enheten. Dessa riskerar att dödas, skadas, hotas eller mutas om informationen hamnar i orätta händer.

Information av denna typ bör skyddas av strategisk kryptering eftersom hoten är många och konsekvenserna ödesdigra vid förlust. Här går en skiljelinje när hoten är allvarliga och attackerarnas resurser är stora. I detta scenario måste man förbereda sig för alla tänkbara attacker. Bara fragment av klartext kan få allvarliga konsekvenser. Tänk dig att man hittar ett namn i en swapfil på en dator stulen under en pågående rättegång mot en kriminell organisation. Det skulle inte krävas mycket för organisationen att ta reda på om namnet i fråga är namnet på en uppgiftslämnare eller annan person med tillgång till viktig information som kan påverka rättegångens utfall. På grund av detta, i enlighet med tabell 7, anser vi att strategiskkryptering är den bästa metoden för att skydda information på. Detta diskuteras mer ingående i kapitel 5. Enligt resultatet i tabell 6 bör krypteringen kombineras med stark autentisering, förslagsvis USB-token. Man kan även använda aktiva kort men då krävs även att det finns en kortläsare vilket gör de mindre lämpade för användning till mobila enheter, se tabell 6. Vi anser att lösenord inte ger ett tillräckligt starkt skydd i detta fall då systemets skydd ändå aldrig är starkare än lösenordet. Lyckas man knäcka lösenordet spelar det ingen roll vilken typ av kryptering man använder. För att ytterligare minimera risken att denna typ av information ska komma på villovägar rekommenderar vi stark användandet av kabellås utanför skalskyddade områden, i överensstämmelse med analysen av riskreduceringsstrategier under stycke 7. Det är även av yttersta vikt att användarna instrueras i hur de skall förvara USB-nyckeln och datorn. Inget av dessa skydd har någon som helst betydelse om datorn lämnas med USB-nyckeln sittandes kvar i USB-porten. Detta hanteras genom att man i ett tidigt skede måste klargöra innebörden av vad som kan hända om information av den här typen går förlorad och utforma klara policys om hur datorn och USB-nyckeln skall förvara samt vilken typ av information som överhuvudtaget bör lagras på en bärbar enhet. Detta redovisas i analysen av riskreduceringsstrategier under stycke 7. En sammanställning av ovanstående råd återfinns i tabellerna nedan:

Riskreducering

	Utbildning	Säkerhetspolicy	Alarm & kabellås	BIOS-lösenord & hårddisklösenord	Spårnings-teknologi	Avlägsna id-märkning
Säkerhetsfaktorer						
Fysisk säkerhet	X	X	X			
Accesskontroll innan OS						
Spårning						

Tabell 8, Riskreduceringsmetoder - Scenario 1

Autentisering

	Lösenord	Aktiva kort	USB-token	Engångslösenord	Biometri
Säkerhetsfaktorer					
Två faktorig		X	X		
Användarvänlig			X		
Funktionellt lämplig på mobila enheter			X		
Skyddar mot råstyrkeattacker		X	X		
Kan ej förloras					

Tabell 9, Autentiseringsmetoder - Scenario 1

Kryptering

	Taktisk kryptering				Strategisk kryptering
	Fil-kryptering	Mapp-kryptering	Virtuell disk-kryptering	EFS	
Säkerhetsfaktorer					
Skyddar individuella filer					X
Skyddar innehållet i en mapp					X
Skyddar temporära filer					X
Skyddar raderade filer					X
Skyddar filnamn					X
Skyddar hela operativsystemet					X
Tillhandahåller bootskydd					X
Tillhandahåller pre-boot autentisering					X
Transparensfaktorer					
Realtids kryptering					X
Realtids dekryptering					X
Användaren behöver ej välja vad som ska krypteras					X

Tabell 10, Krypteringsmetoder - Scenario1

Scenario 2: En stor organisation med viss hemlig information och hög grad av mobilitet, exempelvis Institutionen för Data- och Systemvetenskap (DSV) på Stockholms Universitet.

Vissa lärare vill ha eget ansvar över sina datorer och inga bestämmelser om vad som får installeras. Samtidigt vill de ha friheten att ta med datorn hem samt kunna ta med sig den till undervisningen. De anser sig inte ha tid för säkerhet, även om en del kan mycket om säkerhet i teorin har de svårt att tillämpa säkerheten i praktiken. Lärarna har register över studenterna med bedömning av deras prestationer lagrade på de bärbara datorerna. Även tentamensfrågor samt forskningsresultat är känslig information som ej bör exponeras för obehöriga.

Vi rekommenderar att de använder någon form av taktisk kryptering för att skydda känslig information, förslagsvis EFS. Eftersom EFS ingår i Windows XP innebär det ej heller någon kostnad för organisationen. Anledningen till att vi rekommenderar EFS i det här scenariot är att vi inte anser att hotet är tillräckligt stort för att strategisk kryptering behöver tillämpas. Detta i enlighet med resultaten som visas i tabell 8. Vi rekommenderar dock att kabellås används vid användande av datorerna utanför kontoret, framförallt i undervisningssalar för att undvika att datorn blir stulen under rast eller liknande situation. Detta redovisas i analysen av riskreduceringsstrategier under stycke 7. På grund av de faktorer som diskuteras i kapitel fyra och de resultat som framkommer i tabell 6, angående problem vid användandet av lösenord rekommenderar vi någon form av stark autentisering, förslagsvis USB-tokens. Lärarna borde utbildas i vad de har för ansvar för att skydda information gentemot Datalagen och Personuppgiftslagen (PUL). När man använder ett taktiskt krypteringssystem som EFS innebär det att användarna själva ansvarar för att kryptera de filer som innehåller känslig information. Därför är det viktigt att de undervisas i de lagar som råder och vilka filer som kan tänkas innehålla känslig information. Användarna borde även utbildas i praktiskt säkerhetstänkande för att kunna motsvara de krav som Datalagen och PUL specificerar. Detta i enlighet med riskreduceringsstrategianalysen i stycke 7. En sammanställning av ovanstående råd återfinns i tabellerna nedan:

Riskreducering

	Utbildning	Säkerhetspolicy	Alarm & kabellås	BIOS-lösenord & hårddisklösenord	Spårnings-teknologi	Avlägsna id-märkning
Säkerhetsfaktorer						
Fysisk säkerhet	X		X			
Accesskontroll innan OS						
Spårning						

Tabell 11, Riskreduceringsmetoder – Scenario 2

Autentisering

	Lösenord	Aktiva kort	USB-token	Engångslösenord	Biometri
Säkerhetsfaktorer					
Två faktorig			X		
Användarvänlig			X		
Funktionellt lämplig på mobila enheter			X		
Skyddar mot råstyrkeattacker			X		
Kan ej förloras					

Tabell 12, Autentiseringsmetoder – Scenario2

Kryptering

	Taktisk kryptering				Strategisk kryptering
	Fil-kryptering	Mapp-kryptering	Virtuell disk-kryptering	EFS	
Säkerhetsfaktorer					
Skyddar individuella filer				X	
Skyddar innehållet i en mapp				X	
Skyddar temporära filer					
Skyddar raderade filer					
Skyddar filnamn					
Skyddar hela operativsystemet					

Tillhandahåller bootskydd					
Tillhandahåller pre-boot autentisering					
Transparensfaktorer					
Realtids kryptering				X	
Realtids dekryptering				X	
Användaren behöver ej välja vad som ska krypteras					

Tabell 13, Krypteringsmetoder – Scenario 2

Scenario 3: En liten organisation, med mindre hemlig information och hög grad av mobilitet, exempelvis en rekryteringsbyrå.

Denna rekryteringsbyrå har ca 10 anställda. Tidigare hade de stationära datorer men har nu bytt ut dem mot bärbara datorer. Detta för att de skall kunna arbeta hemifrån och göra företagspresentationer med hjälp av dem. Denna rekryteringsbyrå lagrade alla sina kandidater och kunder i en databas som lagrades lokalt på datorerna. Om en av dessa filer skulle hamna i fel händer skulle det få allvarliga konsekvenser för företaget. Hela företagets verksamhet är baserat på detta register. I dagsläget har företaget inget skydd förutom svaga lösenord som användarna själva har valt.

Det här är ett svårt scenario där man måste beakta ett flertal faktorer. För det första måste man tänka på vad det finns för möjliga hot. Ett möjligt hot är företagsspionerі där en någon annan organisation försöker få tillgång till deras kandidatregister. En andra faktor är kostnaden. Om organisationen anser att informationen är så pass dyrbar att det berättigar införskaffandet av en produkt som använder sig av strategisk kryptering ska de göra det. Denna kostnad kan dock anses för hög och man an argumentera för att denna typ av organisation inte behöver använda strategisk kryptering. Detta eftersom licenserna är dyra och kräver administratör av nyckelgenerering och utförandet av lösenord. På grund av hög mobilitet rekommenderas dock användandet av kabellås (se stycke 7) för att minska risken för stöld, och minst taktisk kryptering med förslagsvis EFS (se tabell 7). EFS ingår i Windows XP och på så sätt tillkommer inga kostnader för organisationen. Organisationens datoradministratör kan enkelt skapa en mapp till användarna där de ombeds spara alla hemliga filer. De bör givetvis kryptera kundregistret och göra den åtkomlig endast för de anställda som behöver ha tillgång till den. Kundregistret måste även skyddas gentemot Datalagen och PUL. Vidare rekommenderas användning av stark autentisering med USB-token då systemet aldrig blir säkrare än den säkerhet autentiseringssystemet tillhandahåller. Detta påvisas i resultatet i tabell 6. Det är även viktigt att utbilda de anställda i hur man skyddar den hemliga informationen och använder tekniken. Detta i enlighet med analysen av riskreduceringsstrategier i stycke 7. En sammanställning av ovanstående råd återfinns i tabellerna nedan:

Riskreducering

	Utbildning	Säkerhetspolicy	Alarm & kabellås	BIOS-lösenord & hårddisklösenord	Spårnings-teknologi	Avlägsna id-märkning
Säkerhetsfaktorer						
Fysisk säkerhet	X					
Accesskontroll innan OS						
Spårning						

Tabell 14, Riskreduceringsmetoder – Scenario 3

Autentisering

	Lösenord	Aktiva kort	USB-token	Engångslösenord	Biometri
Säkerhetsfaktorer					
Två faktorig			X		
Användarvänlig			X		
Funktionellt lämplig på mobila enheter			X		
Skyddar mot råstyrkeattacker			X		
Kan ej förloras					

Tabell 15, Autentiseringsmetoder – Scenario 3

Kryptering

	Taktisk kryptering				Strategisk kryptering
	Fil-kryptering	Mapp-kryptering	Virtuell disk-kryptering	EFS	
Säkerhetsfaktorer					
Skyddar individuella filer				X	
Skyddar innehållet i en mapp				X	
Skyddar temporära filer					
Skyddar raderade filer					
Skyddar filnamn					
Skyddar hela operativsystemet					
Tillhandahåller bootskydd					
Tillhandahåller pre-boot autentisering					
Transparensfaktorer					
Realtids kryptering				X	
Realtids dekryptering				X	
Användaren behöver ej välja vad som ska krypteras					

Tabell 16, Krypteringsmetoder – Scenario 3

Scenario 4: Privatperson med hemlig information och hög grad av mobilitet.

Peter har köpt en bärbar dator att använda för privat bruk. Peter förvarar sina familjebilder, och personliga brev på datorn. Peter har alltid med sig datorn när han är ute och reser och använder den flitigt. Peter vill inte att hans brev eller bilder skall komma i fel händer, då han är en offentlig person, och söker därför en billig metod att skydda sin information med. Han har inte heller några särskilda tekniska färdigheter utan föredrar en enkel lösning för sin känsliga information.

Vi rekommenderar att Peter använder taktisk kryptering, förslagsvis EFS (se tabell 7). Detta för att vi ej anser att hotet mot Peters information eller konsekvenserna av exponering av denna, kan anses särskilt stort. Med EFS kan han, utan att det kostar honom något extra, kryptera all känslig information som han vill skydda från läsning av obehöriga. EFS anser vi även vara enkelt att använda, och kräver inga speciella färdigheter vilket beskrivits i kapitel fem. Peter kan även använda sig av ett starkt lösenord att autentisera sig med i enlighet med kapitel fyra. Som enskild privatperson anser vi det inte nödvändigt med någon form av tvåfaktorig autentisering (se tabell 6), då kostnaderna för detta inte känns motiverat i förhållande till riskerna. Eftersom Peter är en person som ofta är på resande fot, rekommenderar vi användandet av kabellås, detta för att reducera risken för stöld i enlighet med analysen av riskreduceringsstrategier i stycke 7. En sammanställning av ovanstående råd återfinns i tabellerna nedan:

Riskreducering

	Utbildning	Säkerhetspolicy	Alarm & kabellås	BIOS-lösenord & hårddisklösenord	Spårnings-teknologi	Avlägsna id-märkning
Säkerhetsfaktorer						
Fysisk säkerhet			X			
Accesskontroll innan OS						
Spårning						

Tabell 17, Riskreduceringsmetoder – Scenario 4

Autentisering

	Lösenord	Aktiva kort	USB-token	Engångslösenord	Biometri
Säkerhetsfaktorer					
Två faktorig					
Användarvänlig	X				
Funktionellt lämplig på mobila enheter	X				
Skyddar mot råstyrkeattacker					
Kan ej förloras					

Tabell 18, Autentiseringsmetoder – Scenario 4

Kryptering

	Taktisk kryptering				Strategisk kryptering
	Fil-kryptering	Mapp-kryptering	Virtuell disk-kryptering	EFS	
Säkerhetsfaktorer					
Skyddar individuella filer				X	
Skyddar innehållet i en mapp				X	
Skyddar temporära filer					
Skyddar raderade filer					
Skyddar filnamn					
Skyddar hela operativsystemet					
Tillhandahåller bootskydd					
Tillhandahåller pre-boot autentisering					
Transparensfaktorer					
Realtids kryptering				X	
Realtids dekryptering				X	
Användaren behöver ej välja vad som ska krypteras					

Tabell 19, Krypteringsmetoder – Scenario 4

8 Diskussion

Denna uppsats klargör skillnaderna mellan olika säkerhetslösningar gällande för bärbara datorer. Målet med uppsatsen var att den ska ligga till grund för beslut av säkerhetslösning för bärbara datorer hos företag, organisationer och privatpersoner. Vi anser att vår kartläggning tillsammans med våra utarbetade tillämpningsscenarier ger en bra grund för en förståelse av metoderna, och att uppsatsen därför ger tillräcklig insikt i ämnet för att läsaren skall kunna välja en metod över en annan. Detta är ett område där tekniken går snabbt framåt. Många av de metoder vi har kartlagt kan kombineras med varandra. Det går aldrig att få ett 100 % säkert system men många av metoderna gör det mycket svårt även för de tekniskt skickligaste att komma åt informationen lagrad på en bärbar enhet. Ett system är bara så säker som dess svagaste länk. De metoder som låter användaren avgöra vilka filer som skall krypteras kräver att användaren är väl medveten om de hot som finns och hur enkelt det är att få åtkoms till en dator utan stark autentisering. Därför anser författarna att användarutbildning bör finnas för att upplysa användarna om hur de på bästa sätt kan undvika att känslig information exponeras. Vikten av utbildning är enligt oss stor och måste ingå vid införskaffning av ett nytt säkerhetssystem. Om användarna inte vet hur de skall använda systemet så att säkerheten upprätthålls har tekniken inget syfte.

I uppsatsen har vi valt att inte skriva om produktspecifika metoder, vi gjorde dock ett undantag med EFS. Detta gjorde vi på grund av att uppsatsen är avgränsad till att behandla Windows XP. Eftersom EFS är en del av Windows XP ansåg vi det nödvändigt att skriva om denna produktspecifika metod. Vi har även avgränsat oss från att skriva om skydd av själva hårdvaran och fokuserat enbart på skyddet av information. Detta innebär att det finns andra lösningar för riskreduceringsmetoder som är bättre lämpade för skydd av hårdvara. Ett exempel är att avlägsna identifieringsmärkning. Om skydd av hårdvaran är viktigare än skydd av informationen ska man ej tillämpa denna metod utan då istället märka sina enheter permanent. Det finns allmänna riskreduceringsmetoder som hamnar utanför denna uppsats ramar. Exempel på detta är avskräckande metoder för att förebygga stölder.

Under tiden författarna har skrivit uppsatsen har det kommit nya produkter som integrerar kryptering i hårdvaran. En av dem består av en hårddisk som krypteras direkt via inbyggd hårdvara. Det innebär att allt på hårddisken krypteras, inklusive bootsektorn utan någon som helst inverkan på prestanda [Thales, 2004]. Några av dessa lösningar nyttjar kontaktlösa aktiva kort där det räcker att man drar det aktiva kortet över enheten och knappar in ett lösenord för att logga in på enheten. Kryptering med hjälp av hårdvara ökar även säkerheten då det innebär att man ej behöver ha nyckeln i minnet. Vi ser inga problem med denna nya metod gällande vår struktur för uppsatsen. Metoden skulle placeras in i strukturen, på nivå fyra, kryptering, i uppsatsens säkerhetspyramid. Vi tror att kryptering med hjälp av hårdvara är något som kommer att vara på stark fram marsch i framtiden. Denna teknik är dock fortfarande väldigt dyr och används först och främst av regeringar och försvarsmakter.

Då information i dokument och filer kan lagras på många olika ställen på hårddisken anser författarna att man bör använda strategisk kryptering om man vill vara helt säker på att all känslig information verkligen är krypterad. Strategisk kryptering tillsammans med stark autentisering med USB-token är den lösning författarna förespråkar och anser vara den säkraste samt användarvänligaste lösningen för användning på bärbara enheter. Biometriska autentiseringsmetoder lider fortfarande av problem vid mönsterigenkänning. I framtiden kan

detta dock bli ett säkert alternativ till USB-tokens. Målet med uppsatsen är dock att läsaren själv skall kunna avgöra vilken säkerhetsmetod som lämpar sig bäst för läsarens behov.

9 Referenslista

Böcker & Tidsskrifter

[Ahuja, 1996] Ahuja, Vijay, *Network & Internet Security*, Boston AP Proffesional, 1996

[Bishop, 2003] Bishop, Matt, *Computer Security art and Science*, Addison-Wesley, 2003

[Bott, Siechert, 2002] Bott, Ed, Carl, Siechert, *Microsoft Windows XP Utan och Innan*, Pagina, 2002

[Fryksten, 2002] Fryksten, Mikael, DatorMagazin nr. 4, *Konsten att knäcka ett lösenord*, 2002

[Gollmann, 1999] Gollmann, Dieter, *Computer Security*, Pagina förlags AB, 1999

[Holme, Solvang, 1997] Holme, Idar Magne, Solvang, Bernt Krohn, *Forskningsmetodik: Om Kvalitativa Och Kvantitativa Metoder*, Studentlitteratur AB, 1997

[Maiwald, Sieglein, 2002] Maiwald, Eric, Sieglein, William, *Datasäkerhet i Praktiken*, Pagaina, 2002

[Mitrovic, 2004] Mitrovic, Pedrag, Nätmagazin nr. 5, *Common Criteria*, Medströms dataförlag AB, 2004

[Patton, 1988] Patton, Michael Quinn, *How to Use Qualitative Methods in Evaluation*, Sage Pubns, 1988

[SIS, 2002] Swedish Standards Institute, *Handbok i Informationssäkerhetsarbete*, SIS Förlag AB, 2002

[Thurén, 2003] Thurén, Torsten, *Vetenskapsteori för nybörjare*, Liber, 2003

Dokument

[CryptoCard, 2003] CryptoCard whitepaper, *Universal Authenticated Logon,* 2003

[Gordon et al, 2004] Gordon, Lawrence A., Loeb, Martin P., Lucyshyn William, Richardson Robert, *2004 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2004

[Kolodgy, 2003] Kolodgy, Charles J, *Identity Management in a Virtual World,* IDC, 2003

[Korzeniowski, 2001] Korzeniowski, Paul, *Locking down the Laptop*, Information Security Magazine, 2001

[Krause, 2002] Krause, Georg, *Architecture of the Integrated Security System*, CE-Infosys Pte Ltd, 2002

[Russinovich, 1998] Russinovich, Mark, *Inside the Boot Process Part 1*, Windows 2000 & .NetMagazin, Penton Media, Inc, 1998

[Russinovich, 1999] Russinovich, Mark, *Inside the Boot Process Part 2*, Windows 2000 & .NetMagazin,Penton Media, Inc, 1999

[Sadlier, 2003] Sadlier, George, *Mobile Computing Security*, INS Whitepaper, 2003

[Souppaya, Johnson et al, 2004] Souppaya Murugiah, Johnson Paul M., Kent Karen, Harris Anthony, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, National Institute of Standards and Technology, 2004

[Utimaco, 2004] Utimaco Safeware AG, *SafeGuard Easy – The electronic fortress, Access Protection and encryption for data on Notebooks and Workstations,* Whitepaper 2004

[Utimaco EFS, 2004] Utimaco Safeware AG, *Comparison of SafeGuard Easy Disk Encryption and Win2000 Encrypted File System (EFS)*, Whitepaper 2004

Internet

[Absolute Software, 2003] Absolute Software Corporation*,* Whitepaper, *Pre-boot Authentication and Computer Security*, 2003, http://www.absolute.com/public/computraceplus/whitepaper.asp#, Datum: 2004-09-23

[Bedell, 2002] Bedell, Doug, *Lock Your Laptops,* 2002, The Dallas morning news, http://www.dougbedell.com/laptopsecurity.html, Datum: 2004-09-23

[Byttner, 2004] Byttner, Karl-Johan, *Pointsec erövrar USAs myndigheter*, Computer Sweden http://computersweden.idg.se/ArticlePages/200411/12/20041112175356_CS292/20041112175356_CS292.dbp.asp, Datum: 2004-12-17

[Cagliostro, 1999] Cagliostro, Charles, *Smart Cards Primer,* 1999, Smart Card Alliance, http://www.smartcardalliance.org/industry_info/smart_cards_primer.cfm, Datum: 2004-09-07

[Chan, 1997] Chan, Siu-cheung Charles, *An Overview of Smart Card Security,* 1997, http://home.hkstar.com/~alanchan/papers/smartCardSecurity/index.html, Datum: 2004-09-07

[DeMaria, 2002] DeMaria, Mike, *Gone In 6.0 Seconds*, 2002, CMP Media LLC, http://www.networkcomputing.com/1320/1320f4.html, Datum: 2004-10-18

[Dean, 2001] Dean, Joshua. "Lost Laptops Compromise Secrets, 2001, Govexec, http://www.govexec.com/features/1001/1001managetech2.htm, Datum: 2004-09-23

[Gleeson, 2004] Gleeson, Julie, Protocom SecureLogin, *Advanced Authenticaton: the future of network authentication*, 2004 , Whitepaper, http://www.protocom.com/whitepapers/pslaa_whitepaper.pdf, Datum: 2004-09-07

[Hildreth, 2001] Hildreth, Stephen, Protect your laptop!, 2001, Hildreth Enterprises L.L.C http://www.powerbookcentral.com/features/locks.shtml, Datum: 2004-10-12

[HP, 2004] HP, *Njut av hur enkelt och praktiskt det är att skriva ut trådlöst*, http://www.hp.se/om/publikationer/nyhetsbrev/0403a.html, Datum: 2005-01-17

[Kessler, 2004] Kessler, Gary, *An overview of cryptography*, Whitepaper, http://www.garykessler.net/library/crypto.html#aes Datum: 2004-10-13

[Kommunikationsverket, 2004] Kommunikationsverket, *Kommunikationssäkerhet (COMSEC),*

http://www.ficora.fi/ruotsi/tietoturva/tietoliikenne.htm, Datum: 2004-09-07

[Kozierok, 2001] Kozierok, Charles M, *Major Disk Structures and the Boot Process*, 2001, The PC Guide, http://www.pcguide.com/ref/hdd/file/struct_MBR.htm, Datum: 2004-05-27

[LaptopsGuide, 2004] Laptops Guide, *Laptop security*, http://www.laptops-guide.com/laptop-security.html, Datum: 2004-10-12

[Lobel, 2000] Lobel, Mark, *Case for Strong User Autentication,* 2000, Pricewaterhousecooper http://www.pwcglobal.com/extweb/manissue.nsf/2e7e9636c6b92859852565e00073d2fd/728d168e9e5cce04852566fd00665839/$FILE/case_for_strong(pwc)_wp.pdf, Datum: 2004-10-12

[Mann, 2001] Mann, Charles C., *Where the Hell is My Laptop?*, Business 2.0 Media Inc, http://www.business2.com/b2/web/articles/0,17863,513164,00.html Datum: 2005-01-07

[McIntosh, 2001] McIntosh, Robert, *Windows 2000's Encrypting File System*, 2001, Penton Media, Inc, http://www.windowsitpro.com/Article/ArticleID/19721/19721.html, Datum: 2004-09-07

[Microsoft, 2003] Microsoft, *Secure User Authentication for the Next-Generation Secure Computing Base,* Whitepaper, http://www.microsoft.com/resources/ngscb/documents/ngscb_authentication.doc, Datum: 2004-10-11

[Microsoft, 2004] Microsoft, *Encrypting File System overview,* http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt_overview.mspx, Datum: 2004-09-07

[Microsoft 2, 2004] Microsoft, *7 ways to protect your laptop on the road*, http://www.microsoft.com/athome/security/onthego/ontheroad.mspx, Datum: 2004-10-12

[Microsoft 3, 2004] Microsoft, *AES Provider Algorithms*, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/seccrypto/security/aes_provider_algorithms.asp, Datum: 2004-12-02

[Mossywell, 2003] Mossywell, *Computer Boot Sequence*, 2003, http://www.mossywell.com/boot-sequence/#The_Master_Boot_Record, Datum: 2004-05-27

[NIST, 2002] National Institute of Standards and Technology, *Advanced Encryption Standard,* 2002, http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html, Datum: 2005-01-17

[Pagina, 2004] Pagina IT-ordbok, http://www.pagina.se/itord/default.asp?SokOrd=autentisering. Datum: 2004-09-07

[Paulsen, 2004] Paulsen, Karl, *The Evolution of the Universal Serial Bus* http://www.tvtechnology.com/features/Media-Server-Tech/Feature_Paulsen.shtml, Datum: 2004-12-02

[PC Guide, 2004] PC Guide, *Master Boot Record (MBR),* http://www.pcguide.com/ref/hdd/file/structMBR-c.html, Datum: 2004-10-27

[PCPlus, 2000] PC Plus, *Open Secrets*, 2000, Future Publishing http://www.pcplus.co.uk/tips/default.asp?pagetypeid=2&articleid=4581&subsectionid=390, Datum: 2004-10-19

[PKI-Forum, 2004] PKI-Forum, *Introduktion till kryptering* http://www.pki-forum.com/intro/krypto.shtml, Datum: 2004-09-07

[Protectdata, 1999] Protectdata, Protect 19, http://www.protectdata.com/common/upl/files/file7478.pdf, Datum: 2004-12-06

[Protectdata, 2000] Protectdata, Årsredovisning 2000, http://www.protectdata.com/common/upl/files/file47843.pdf, Datum: 2004-10-11

[Rainbow Technologies, 2002] Rainbow Technologies ,*Two-Factor Authentication – Making Sense of all the Options,* 2002, Whitepaper, http://www.safenet-inc.com/insights/whitePDF/2FACTOR-V52.pdf, Datum: 2004-09-07

[RMT-gruppen, 1999] RMT-gruppen, *Riktlinjer för riskhantering i samhälle och näringsliv,* 1999, http://www.sff.a.se/branding/rmriktl.pdf, Datum: 2005-01-09

[Ryder, 2001] Ryder, Josh, *Laptop Security, Part One: Preventing Laptop Theft*, SecurityFocus, http://www.securityfocus.com/infocus/1186, Datum: 2005-01-07

[Schneiner, 2004] Schneier, Bruce, *The Blowfish Encryption algorithm*, http://www.schneier.com/blowfish.html, Datum: 2004-10-13

[Spooner, 2003] Spooner, John G, *Notebook Sales Hit New Highs*, 2003, CNET Networks, Inc. http://zdnet.com.com/2100-1103_2-1022905.html, Datum: 2004-09-23

[Symantec, 2004] Symantec, *Att bygga en effektiv säkerhetspolicy*, 2004, http://www.symantec.se/region/se/corporate/building_securitypolicy.html, Datum: 2004-09-23

[Symantec B, 2004] Symantec, *Biometri: börjar vi närma oss en ny era inom säkerhetsteknologin?,* http://www.symantec.com/region/se/resources/biometrics.html, Datum: 2005-01-17

[Thales, 2004] Thales, *Guardisk – Secure Hard Disk Encryption*, http://www.thales-esecurity.com/ProductsServices/documents/Guardisk04.pdf, Datum: 2005-01-25

[VeriSign, 2004] VeriSign, *The Security Risk of Using Passwords,* Whitepaper, http://www.safescrypt.com/resources/PasswordWhitePaper.pdf, Datum: 2004-09-07

[Wallström, 2004] Wallström, Martin, Distansjobb hett för affärsfolket, ComputerSweden, http://computersweden.idg.se/a/20040521080103_CS866, Datum: 2005-01-07

[Wallström B, 2004] Wallström, Martin, *Vadå säkerhetspolicy?*, Computer Sweden, http://computersweden.idg.se/ArticlePages/200408/26/20040826170144_CS558/20040826170144_CS558.dbp.asp, Datum: 2005-06-07

[Webopedia, 2004] Webopedia, *BIOS*, http://www.webopedia.com/TERM/B/BIOS.html, Datum: 2004-10-13

[Wikipedia, 2004] Wikipedia, *International Data Encryption Algorithm* http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm, Datum: 2004-10-13

[Wikipedia 3, 2004] Wikipedia, *Pseudorandom number generator* http://en.wikipedia.org/wiki/Pseudo-random_number_generator, Datum: 2004-12-02

[WinMagic, 2003] WinMagic Inc., *Disk Encryption Products*, 2003, Whitepaper, http://www.winmagic.com/whitepaper.pdf, Datum: 2004-09-07

Intervju

[Lindblom, 2005] Lindblom, Roger, Riskpolisstyrelsenssäkerhetsenhet, Datum: 2005-01-24, Rikspolisstyrelsen, Stockholm

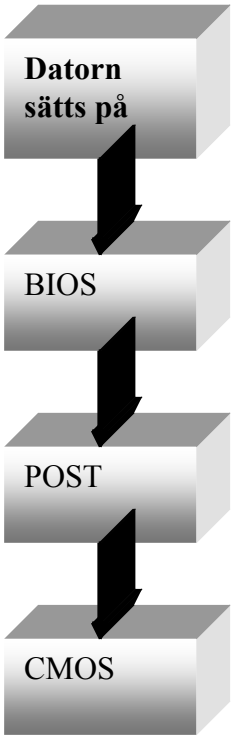
[Reichert, 2004] Reichert, Tomas, Utvecklingschef, Utimaco Safeware AG, Datum: 2004-03-24, Rikspolisstyrelsen, Stockholm

Appendix A, Bootsekvens

I det här kapitlet beskriver processen som datorn går igenom från att strömmen slås på till det att operativsystemet har startat. Detta kallas bootsekvensen. Förståelse av bootsekvensen är viktig för att kunna få en inblick i hur pre-boot autentisering möjliggörs samt för att se vilken information som blir tillgänglig innan inloggning i XP sker. Följande rubriker följer bootsekvensordningen och beskriver vad som händer under processen.

Datorn startas

Strömförsörjningen genomför ett självtest. När spänningen och strömstyrkan är acceptabel indikerar strömförsörjningen att elkraften är stabil och skickar en ”Power Good” signal till processorn. Tiden det tar från att man slår på datorn tills ”Power Good” skickas, är vanligen mellan 0,1–0,5 sekunder. Mikroprocessorns timerchip tar emot ”Power Good” signalen. När ”Power Good” signalen tas emot slutar timerchippet att skicka omstartssignaler till processorn vilket medför att den kan börja exekvera. [Russinovich, 1998]



Figur 16, Bootsekvens del 1

BIOS

Efter det börjar processorn exekvera BIOS-kod. BIOS står för Basic Input/Output System. BIOS är inbyggd mjukvara som avgör vad en dator kan göra utan att starta någon applikation. På en PC innehåller BIOS all kod som krävs för att kontrollera tangentbordet, visa grafik, diskenheter, seriell kommunikation och ett antal andra funktioner. [Webopedia, 2004]

Processorn laddar BIOS och utför sedan ett test av central hårdvara för att verifiera grundläggande funktionalitet. Alla fel som uppstår vid den här tidpunkten i bootsekvensen rapporteras med hjälp av ”beep-koder” på grund av att video subsystemet ej har initialiserats. BIOS söker sedan efter de enheter som behöver ladda sina egna BIOS-rutiner. [Russinovich, 1998]

Kall eller varm start

BIOS kontrollerar om det är en ”kall-start”[2] eller en ”varm-start”[3]. För att avgöra huruvida det är en varm-start eller en kall-start kollar BIOS-uppstartsrutiner värdet på två bytes. Alla värden förutom 1234h indikerar att det är en ”kall-start”. Om det är en ”kall-start” exekverar BIOS hela POST (Power On Self Test). Om det istället är en ”varm-start” görs inget minnestest. [Russinovich, 1998] [Bott, Siechert, 2001]

POST

POST kan brytas ner i tre komponenter:

[2] Kall start betyder att man startar datorn från att varit avstängd [Webopedia]
[3] Varm start betyder att man startar om en dator som redan är påslagen via operativsystemet[Webopedia]

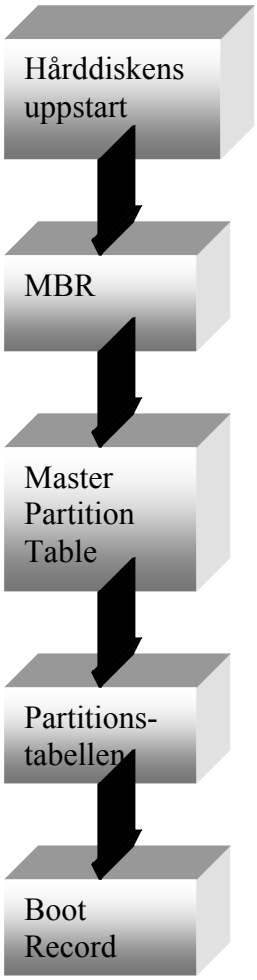
- Videotestet initialiserar grafikkortet, testar grafikkortet och dess minne. Slutligen visas konfigurationsinformation och felmeddelande.
- BIOS identifikationen visar BIOS versionen, tillverkare och datum.
- Minnestestet testar RAM minnet och visar hur mycket minne som är installerat.

Fel som uppstår under POST kan enkelt klassificeras som fatala eller ej fatala. Ett ej fatalt fel genererar vanligen ett felmeddelande på skärmen och tillåter systemet att fortsätta bootsekvensen. Ett fatalt fel, stoppar bootsekvensen och signalerar vanligen fel med en serie av ”beep-koder”. [Russinovich, 1998]

CMOS

BIOS lokaliserar och läser konfigurationsinformationen lagrad i CMOS. CMOS (vilket står för Complementary Metal-Oxide Semiconductor) är en liten del av minnet (64 bytes) som drivs av ett litet batteri på moderkortet. Det viktigaste BIOS-uppstartsrutin för CMOS gör, är att indikera i vilken ordning diskarna skall undersökas för att hitta operativsystem t. ex diskett, CD eller hårddisk. [Russinovich, 1998]

Hårddiskens uppstart



Figur 17, Bootsekvens del 2

När man sätter på datorn börjar processorn jobba. I det här läget är systemets minne tomt och processorn har ingenting att exekvera. För att försäkra sig om att datorn alltid kan starta oavsett vilken BIOS som finns eller vilken tillverkare som har gjort den börjar den alltid exekvera på samma plats, FFFF0h. På liknande sätt måste varje hårddisk ha en fast “startpunkt” där nyckelinformation är lagrad om hårddisken, exempelvis hur många partitioner den har och vilken typ av partitioner de är etc. Någonstans behöver BIOS starta det initiala boot-programmet som startar laddningsprocessen av operativsystemet. Platsen där denna information är lagrad kallas Master Boot Record (MBR). [PC Guide, 2004]

Master Boot Record

MBR är alltid lokaliserad på cylinder 0, huvud 0 och sektor 1, vilket är den första sektorn på disken. Det är den fasta startpunkten som hårddisken alltid använder [Bott, Siechert, 2001]. Om denna sektor hittas laddas den in i minnet och testas för en godkänd signatur. Saknas en MBR eller en godkänd signatur stoppas bootsekvensen med ett meddelande som kan se ut på följande sätt: NO ROM BASIC - SYSTEM HALTED. När BIOS startar maskinen, kollar den här efter instruktioner och information om hur den skall starta hårddisken och ladda operativsystemet. MBR innehåller följande strukturer: [PC Guide, 2004]

- Master Partition Table: Denna tabell innehåller beskrivningar om partitionerna som finns på hårddisken. Det finns bara plats i tabellen för information om fyra partitioner då den är väldigt liten. Därför kan en

hårddisk bara ha fyra riktiga partitioner även kallade primära partitioner. En av partitonerna är markerad som aktiv partition vilket indikerar att det är den datorn ska använda vid bootprocessen. [PC Guide, 2004]

MBR innehåller det initiala boot-programmet, Master Boot Code, som BIOS laddar och exekverar för att starta bootsekvensen. Detta program överför sedan kontrollen till boot-programmet lagrat på den partition som används för att starta datorn. Processen att installera multipla operativ system på en dator involverar vanligen att byta ut original Master Boot Code mot en kod som tillåter användaren att välja en specifik hårddisk att ladda i nästa steg av processen. [PC Guide, 2004] [Bott, Siechert, 2001]

På grund av att informationen lagrad i MBR är så viktig skulle en skada innebära stor förlust av data. Eftersom Master Boot Code är det första program som exekveras när du sätter på din dator, är det en favoritplats för virus och andra angrepp. [PC Guide, 2004]

Offset	Längd	Innehåll
0	446	Master Boot Code. Denna kod ansvarar för att lokalisera partitionen att starta från och instruera processorn att fortsätta exekvera från File System Boot Sector's början. Den här koden innehåller felmeddelanden, exempelvis "Fel vid uppstart av operativ system" och "Saknar operativ system".
446	16	Första partitionens beskrivning
462	16	Andra partitionens beskrivning
478	16	Tredje partitionens beskrivning
494	16	Fjärde partitionens beskrivning
510	2	55 AA

Tabell 10, Master Boot Record [Mossywell, 2004]

Partitionstabellen

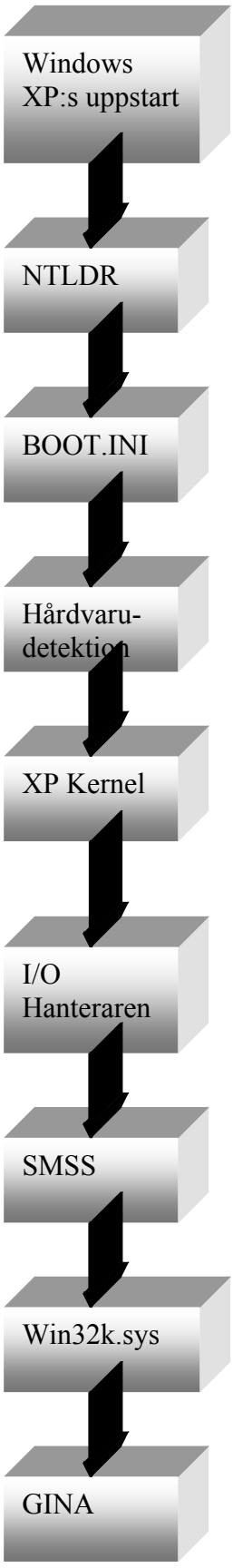
Partitionsladdaren undersöker partitionstabellen för en partition markerad som aktiv. Partitionsladdaren söker sedan den första sektorn av den partitionen för att hitta Boot Record. Boot Record är också 512 bytes stor och innehåller en tabell som beskriver det som är utmärkande för partitionen (antalet bytes per sektor, antalet sektorer per kluster etc.) och innehåller även jump kod för att lokalisera den första av operativsystemets systemfiler (IO.SYS i DOS). [Russinovich, 1998]

Operativsystemets uppstart

Boot Record

Den aktiva partitionens Boot Record letar efter en godkänd bootsignatur och om den hittas exekveras bootsektorkoden som ett program. Uppstarten av Windows XP kontrolleras av filen NTLDR vilken är en gömd systemfil som finns i systempartitionens rootkatalog [Bott, Siechert, 2001]. NTLDR (NT Loader) startar XP i fyra steg: [Russinovich, 1998]

1. Initiala bootladdningsfasen
2. Val av operativsystem
3. Hårdvarudetektion
4. Konfigurationsval



Figur 18, Bootsekvens del 3

NTLDR initiala fasen

Under den initiala fasen växlar NTLDR processen från realläge till skyddat läge. Detta placerar processen i 32-bitars minnesläge och startar minnessidväxling. Efter det laddar den passande drivrutiner för ett minifilsystem som tillåter NTLDR att ladda filer från en partition formaterad med något av de filsytem som stöds av Windows XP. Windows XP stöder partitioner formaterade med antingen FAT-16, FAT-32 eller NTFS filsystem. [Russinovich, 1998]

BOOT.INI

Om filen BOOT.INI är lokaliserad i root katalogen kommer NTLDR läsa in dess innehåll i minnet [Bott, Siechert, 2001].Om BOOT.INI innehåller information om mer än ett operativsystem så kommer NTLDR stoppa bootsekvensen och visa menyalternativ där användaren får välja operativsystem. Om filen BOOT.INI inte hittas i rootkatalogen kommer NTLDR att fortsätta bootsekvensen och försöka ladda Windows XP från den första partitionen på den första disken, vanligtvis C:\. [Russinovich, 1998]

Bootval med F8

Om man antar att operativsystemet som laddas är Windows NT, 2000 eller XP kan man trycka på F8 för att visa olika bootval, exempelvis skyddat läge och sista fungerande konfiguration. Efter varje lyckad bootsekvens gör operativsystemet en kopia av den nuvarande kombination av drivrutiner och systeminställningar och lagrar den som sista fungerande konfiguration. Denna samling av inställningar kan användas för att boota systemet i det fall att installation av en ny enhet orsakat fel vid bootning av operativsystemet. [Russinovich, 1998]

Hårdvarudetektion

Om valt operativ system är XP kommer NTLDR fortsätta bootprocessen genom att lokalisera och ladda det DOS-baserade programmet NTDETECT.COM för att utföra hårdvarudetektion. NTDETECT.COM samlar en lista på installerade hådvarukomponenter och returnerar denna lista för senare inkludering i registret under HKEY_LOCAL_MACHINE\HARDWARE nyckeln. [Russinovich, 1998]

Hårdvaruprofiler

Om datorn har mer än en definierad hårdvaruprofil kommer NTLDR programmet att stanna och visa en meny med hårdvaruprofiler och konfigurationsåterställning. Saknas mer än en hårdvaruprofil kommer NTLDR hoppa över detta steg och inte visa någonmeny.[Russinovich,1998]

Start av XP kernel

Efter val av hårdvarukonfiguration börjar NTLDR att ladda XP kerneln (NTOSKRNL.EXE). Kerneln är den centrala delen i ett operativsystem. Det är den del av operativsystemet som startas först och stannar kvar i huvudminnet. På grund av att den stannar kvar i minnet är det viktigt att den är så liten som möjligt medan den fortfarande tillhandahåller alla nödvändiga tjänster som krävs av andra delar av operativsystemet och applikationer. Vanligen är kerneln ansvarig för minnes-, process-, tjänst- samt diskhantering. [Webopedia]

Under laddning av kernel kommer NTLDR att behålla kontroll över datorn. Skärmen töms och en serie av vita rektanglar åker över botten av skärmen [Russinovich, 1998] . Samtidigt laddar NTLDR även hårdvaruabstraktionslagret HAL.DLL vilket kommer skydda kerneln från hårdvaran. Båda filerna är lokaliserade i katalogen <winnt>\system32. [Bott, Siechert, 2001]

Drivrutiner för bootenheter

NTLDR laddar sedan drivrutiner till enheter som är markerade som bootenheter. Vid laddning av dessa drivrutiner lämnar NTLDR sin kontroll över datorn. Alla drivrutiner har en subnyckel i registret under HKEY_LOCAL_MACHINE\SYSTEM\services. Alla drivrutiner som har startvärdet SERVICE_BOOT_START anses vara en enhet som ska starta vid bootning. För varje laddad fil skrivs en punkt ut på skärmen, om inte /SOS alternativet är påslaget, då skrivs filnamnen ut istället. [Russinovich, 1998]

Initialisering av XP kernel

NTOSKRNL går igenom två faser i sin bootprocess, fas 0 och fas 1. Fas 0 initialiserar precis tillräckligt av kerneln och verkställande subsystem för att grundläggande tjänster som krävs för slutförandet av initieringen blir tillgängliga [Bott, Siechert, 2001]. Vid denna punkt visar systemet en grafisk statusrad som indikerar laddningsstatus. XP avaktiverar avbrottssignaler under fas 0 och aktiverar dem före fas 1. HAL kallas för att förbereda avbrottshanteraren, minneshanteraren, objekthanteraren, säkerhetsreferensmonitorn och processhanteraren för initialisering. Fas 1 börjar när HAL kallas för att förbereda systemet att acceptera avbrottssignaler från enheter. Om det finns mer än en processor initialiseras den nu. [Russinovich, 1999]

I/O hanteraren

Initialisering av I/O hanteraren börjar med processen att ladda alla systemets drivrutiner. Den börjar där NTLDR slutade med att först slutföra laddning av bootenheterna. Sedan sammanför den en lista av drivrutiner i prioritetsordning och försöker ladda var och en i turordning. Misslyckas laddning av en drivrutin kan operativsystemet bli åtsagt att starta om datorn med sista kända fungerande konfiguration. [Russinovich, 1999]

SMSS

Den sista uppgiften för fas 1's initialisering av kerneln är att starta Session Manager Subsystem (SMSS). SMSS är ansvarig för skapandet av användargränssnittet. SMSS körs i användarläge men olikt andra användarlägesapplikationer anses SMSS som en tilltrodd del av

operativsystemet och använder bara kärnfunktioner. Dessa två funktioner tillåter SMSS att starta upp det grafiska subsystemet och inloggningsprcessen. [Russinovich, 1999]

Win32k.sys

SMSS laddar enhetsdrivrutinen win32k.sys vilken implementerar det grafiska subsystemet win32. Kort efter win32k.sys startats växlar skärmen till grafiskt läge. Tjänstsubsystemet startar nu alla tjänster markerade för autostart. När alla enheter och tjänster är uppstartade anses bootsekvensen vara lyckad och konfigurationen sparas som sista lyckade konfiguration. [Russinovich, 1999]

Inloggning

XP bootsekvensen anses inte vara färdig innan det att en användare lyckats logga in i systemet. Processen börjar med att filen WINLOGON.EXE visar inloggningsrutan GINA, Graphical Identification and Authorization.[Bott, Siechert, 2001]. Denna dialogruta dyker upp under tiden som subsystemet för tjänster startar nätverkstjänsten. [Russinovich, 1999]

Appendix B, Ordlista

FAT, FAT-16, FAT-32

På engelska File Allocation Table, förkortas FAT, en tabell som operativsystemet använder för att hitta filer på en disk. Genom fragmentering kan en fil delas upp i många små delar som sprids på disken. Det är FAT som håller reda på alla dessa små delar. I DOS-system lagras FAT i dolda filer, FAT-filer.

Systemet för äldre versioner av DOS och Windows 95 hette FAT16 och i de nyare versionerna, efter Windows 95, version OSR2, heter det VFAT eller FAT32. I Windows 2000 (och även i Windows NT) finns dock även NTFS vilket rekommenderas av Microsoft.

FAT är en del av filkatalogen. Om den skadas går det inte att utan vidare läsa in filer från disken.

HAL

Hardware Abstraction Layer, en virtuell dator som operativsystemet skapar i den befintliga hårdvaran, dvs. moderkortet. HAL är således en slags drivrutin för moderkortet som anpassar det till operativsystemet.

Microsoft kan alltså anpassa Windows till vilken processor som helst genom att skriva ett annat HAL och kompilera om operativsystemet för denna processor.

Minnessidväxling

Överföring av datasidor (minnessidor) från primärminne till sekundärminne eller tvärtom. Förekommer vid användning av virtuellt minne.

MS-DOS

Förkortning för Microsoft Disk Operating System, operativsystem för 16-bitarsdatorer (med processorerna i 80-serien) som bl.a. medger trädstrukturerade filkataloger. IBM använder en variant av MS-DOS i persondatorn IBM PC. MS-DOS har hämtat många drag från operativsystemet UNIX. MS-DOS torde vara världens mest använda och spridda operativ-system men har ersatts av Windows 95 och senare versioner.

NTFS

New Technology File System, ett filhanteringssystem, en filtilldelningstabell, som används i Windows NT och även i Windows 2000 och senare versioner. Det kan hantera långa filnamn, har inbyggd säkerhet, kan hantera mycket stora lagringsmedia m.m. Det stöder objektorienterade tillämpningar genom att filerna hanteras som objekt med användar- eller systemdefinierade attribut.

Plug and play

Refererar till ett datorsystems förmåga att automatiskt konfigurera expansionskort och andra enheter. Du skall kunna plugga in en enhet och använda den utan att oroa dig över olika inställningar.

Reelltläge

Real mode, det läge i vilket processorerna 80286 och 80386 kör ett program i taget, dvs utan att kunna använda multikörning. Kallas även "DOS-läge" eller reellt läge.

Skyddat läge

Det läge i vilket processorer efter 80286 kan köra flera program samtidigt. Skyddet syftar på att de olika programkörningarna är skyddade mot påverkan av varandra. Kallas även OS-läge.

Spooler

Mellanlagrare, ett program som tar hand om data som adresserats till en yttre enhet och lagrar dessa data i minnet. Data överförs till den yttre enheten när de kan bearbetas. När data har mellanlagrats är processorn fri och kan fortsätta själva bearbetningen medan den yttre enheten styrs av det som mellanlagrats. Denna typ av mellanlagring används oftast vid utskrifter.

Appendix C, Krypteringsalgoritmer

Det finns två olika klasser av nyckelbaserade algoritmer, symmetriska och asymmetriska. Skillnaden är att symmetriska algoritmer använder samma nyckel för kryptering och dekryptering medan asymmetriska algoritmer använder olika nycklar för kryptering och dekryptering. [Kessler, 2004]

Symetriska algoritmer kan delas in i ström chiffer och block chiffer. Ström chiffer kan kryptera en enda bit av klartext åt gången, medan block chiffer kan ta ett antal bitar (vanligtvis 64 bitar i moderna chiffer), och kryptera dem på en gång. [Kessler, 2004]

Asymmetriska chiffer tillåter krypteringsnyckeln att vara publik vilket tillåter vem som helst att kryptera med den nyckeln. Dock kan bara den som har dekrypteringsnyckeln dekryptera meddelandet med den. Krypteringsnyckeln kallas även för publik nyckel och dekrypteringsnyckeln kallas för privat eller hemlig nyckel. [PKI-forum, 2004]

Generellt är symmetriska algoritmer mycket snabbare att använda på en dator än asymmetriska. I praktiken används de ofta tillsammans, så att en publik nyckelalgoritm används för att kryptera en slumpmässigt genererad krypteringsnyckel, och den slumpmässiga nyckeln används för att kryptera själva meddelandet med en symmetrisk algoritm. Detta kallas ibland för hybrid kryptering. [Kommunikationsverket, 2004]

DES

DES är en algoritm som utvecklades I mitten av 70-talet. DES betyder Data Encryption Standard och gjordes till en standard av Amerikanska National Institute of Standards and Technology (NIST). [Gollmann, 1999] [Kessler, 2004]

DES är ett block chiffer med 64 bitars block storlek. DES använder 56 bitars nycklar, vilket idag är för svagt för att använda. Moderna datorer kan knäcka dessa nycklar genom att prova alla möjliga kombinationer (råstyrka). [Gollmann, 1999]

En variant på DES är 3DES och är baserad på att använda DES tre gånger. 3DES är starkare än DES men anses vara långsamt jämfört med ett flertal nya block chiffer. [Kessler, 2004]

AES

Som svar till attackerna mot DES, började NIST sökandet efter en algoritm som kunde möta 2000-talets säkerhetsbehov. Efterträdaren skulle komma att kallas Advanced Encryption Standard AES men hette från början Rijndael. AES skapades av två belgiska kryptografer Joan Daemen och Vincent Rijmen. AES stöder 128, 192 och 256 bitars nycklar. NIST valde Rijndael som efterträdare till DES på grund av att den presterar mycket bra i både hård- och mjukvara, i många olika miljöer och lägen. [Kessler, 2004]

Blowfish

Blowfish utvecklades år 1993 av Bruce Schneier. Algoritmen var tänkt som en kostnadsfri och licensfri konkurrent till DES och IDEA. Blowfishnycklar har variabel längd, 32 till 448 bitar (4 till 56 tecken). Algoritmen är mycket snabbare än både DES och IDEA och används i över 150 produkter. [Schneier, 2004]

IDEA

International Data Encryption Algorithm, IDEA, utvecklades under 1991 vid ETHZ. IDEA använder sig av en nyckel på 128 bitar (16 tecken). Algoritmen använder sig av 17 "rundor" för att kryptera data. [Wikipedia, 2004]

Twofish

Twofish är baserad på Blowfish och är utvecklad av Counterpane Labs. Algoritmen använder en nyckel på 256 bitar (32 tecken) och var även den kandidat till AES. [Schneier, 2004].

Appendix D, Riskanalys

Vid granskning av bärbara datorers säkerhetssystem är det viktigt att undersöka vilka möjliga hot som kan vara riktade mot organisationen samt vilka hot som blivit realiserade. För att klargöra hotbilden behöver man göra en riskanalys. Ett hot kan definieras som en risk att någon kommer att skada en person, eller stjäla alternativt skada egendom avsiktligt. En hotbild utgör summan av de olika risker en person eller en verksamhet är exponerad för. En riskanalys är en analys av hur stor risken är att man skall konfronteras med att hot omsätts i handling. [RMT-gruppen, 1999]

Riskstyrningsprocessen

Enligt SIS [SIS, 2002] hade Riskstyrning (risk management) sin födelse i 1700-talets upplysningstid. Då utforskade man det okända i jakten på kunskap. Riskstyrning är i dag en generell process för att hantera riskerna. Om konsekvensen av en risk är acceptabel anses risken vara löst. I riskstyrningsprocessen ingår två huvuddelar:

- Riskanalys använder vi för att definiera riskerna. Riskanalysen är en sökande och upptäckande process för att finna hoten och dess källor. Efter riskanalysen kan man sedan dra slutsatser som hjälper till att bedöma hotets allvarlighetsgrad, vem eller vilka förövare kan förväntas, vad är de kapabla till, hur kommer dessa att gå tillväga och hur skyddar man sig på bästa sätt.

- Riskkontroll är den andra delen och är ett sätt att kontrollera riskerna och sedan reducera dem. Processen gör det möjligt att sedan ta fram en åtgärdsplan, kontrollera riskstatus, införa åtgärder och korrigera eventuella avsteg från planen. En riskanalys är inte en engångsföreteelse, utan en pågående process där nya analyser genomförs löpande för att säkerställa att säkerhetsåtgärderna anpassas kontinuerligt till förändringar i hotbilden.

Organisationer brukar i början av riskstyrningsprocessen ha oklara tankar om vad som kan drabba dem. Det finns många okända faktorer att överväga. Tanken med riskstyrnings-processen är att omvandla osäkerheterna till ett mer acceptabelt och beräkningsbart risktagande. Det innebär också att man måste förstå vilka komponenter som måste beaktas i de beslut som fattas. När risker ska identifieras och analyseras inleds också arbetet med att undersöka sannolikheten för att risken ska inträffa och vad som kan bli konsekvensen. [RMT-gruppen, 1999]

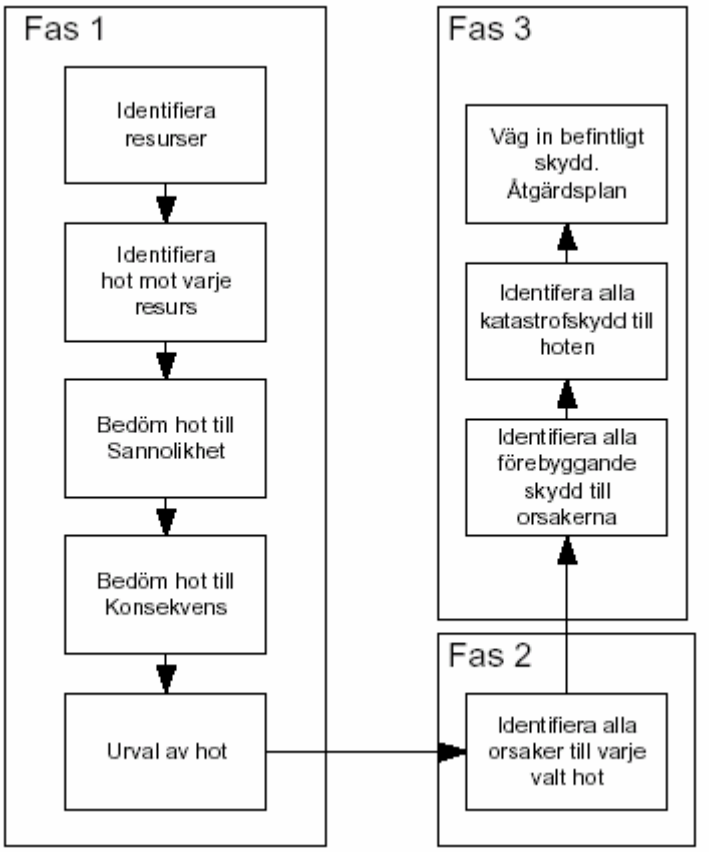
Enligt SIS [SIS, 2004] ökar hoten mot verksamheten tillsammans med befintliga säkerhetshål, verksamhetens sårbarhet. En risk existerar även om ingen har lyckats identifiera den. Exempelvis om lösenord används, är risken stor för att någon kommer att ta sig in i den mobila enheten trots att det ej har inträffat tidigare. Konsekvensen av risken beror inte på om den har bedömts som viktig eller ej. Det är endast de åtgärder som utförts för att komma till rätta med risken – förebyggande eller skadereducerande – som hindrar att den blir ett problem. Oberoende av hur risken en gång uppskattats kan den ändra sin betydelse med tiden. Som exempel kan man nämna att samtidigt som processorkraften ökar i datorer krävs det att man använder längre lösenord för att kunna motstå råstyrkeattacker. Detta gäller också nyckellängden i krypteringssystem. På grund av att riskerna förändras med tiden, innebär det att riskanalysen som arbetssätt ej är en engångsföreteelse utan en upprepad process som bör

göras minst en gång per år eller när ändringar sker i processer eller på andra sätt. Åtgärderna minskar riskerna och motverkar hoten. En viktig del inom riskanalysområdet är att väga kostnaden för åtgärderna mot de risker som finns. En åtgärd mot en viss risk ska inte vara starkare än tvunget, men ej för kostsam i förhållandet till vad skadan hade kostat om den faktiskt inträffat. För att förenkla och standardisera besluten som organisationerna måste fattas i samband med riskanalysen kan olika typer av beslutsmatriser byggas upp.

Enligt en rapport hämtad från Brottsförebyggande rådets analys 2000 över skadekostnader i samband med dataintrång är medelkostnaden för ett dataintrång 356 000 kronor. Om verksamheten utsätts för ett intrång måste en verksamhet med 4 procents vinstmarginal sälja för nästan 9 miljoner kronor innan förlusten är täckt. [SIS, 2002]

Översiktlig modell för riskanalys

I det här stycket presenteras en modell för riskanalys i praktiken. Analysmodellen är indelad i tre faser. Viktigt är att man under dessa faser ej beaktar de befintliga skyddsåtgärderna på grund av att det är mycket svårt att avgöra hur effektiva dessa åtgärder är. Den första fasen kallas ”brainstorming session”. I den andra fasen identifierar man alla orsaker till varje hot och i den tredje identifierar man alla förebyggande skydd till orsakerna. Detta illustreras i figur 8.



Figur 19, Översiktig modell för riskanalys. [SIS, 2002]

Exempel på resultat efter riskanalys av bärbara datorer

Författarna har i tabell 22 arbetat fram ett exempel på hur ett resultat efter en riskanalys av bärbara datorer i en organisation kan se ut. För att kunna utföra en riskanalys måste man dock

först framställa en tabell som visar hur stor sannolikheten är att hoten realiseras och allvarlighetsgraden av hotets konsekvens. En sådan kan enligt SIS utformas enligt följande tabell.

Sannolikhet (S)	Konsekvens (K)
Nivå 0 = Osannolik, inträffar om 30 år	Betydelselös
Nivå 3 = Mindre sannolik, inträffar om 5 år	Låg, kan påverka trovärdighet, viss ekonomisk påverkan, gränslandet mellan vad som är lagligt, lite påverkan på människors liv och hälsa.
Nivå 5 = Möjlig, kan inträffa under året.	Hög, Är avgörande för trovärdighet, har stor ekonomisk påverkan, gråzonen för vad som är lagligt, stor påverkan på människors liv och hälsa.
Nivå 8 = Sannolik, inträffar flera gånger per. år	Mycket hög, kan hota företagets trovärdighet, mycket stor ekonomisk påverkan, är olagligt, mycket stor påverkan på människors liv och hälsa.

Tabell 21, Tabell över sannolikhet och konsekvens för hot. [SIS, 2002, kapitel 2- s. 5]

Efter det kan man utföra riskanalysen på organisationens mobila enheter där man sammanställer hot, sannolikhet, konsekvens och orsak. Därefter kan man ta fram förebyggande skydd och skadebegränsande lösningar. Dessa skydd och lösningar skall vara dimensionerade för att klara av att stå emot de hot man vet finns mot verksamheten.

Resurs	Hot	S	K	Orsak	Förebyggande skydd (mot orsak)	Katastrof skydd (mot hot)
Bärbara datorer	Obehörig tillskansar sig konfidentiell information	5	8	Lättillgänglig dator ej fysiskt Skyddad	Tillse att obehöriga inte kan komma åt datorerna (fysiskt)	Kryptera konfidentiell information
					Förvara inte konfidentiell information på lättillgängliga datorer	
					Använda kabellås eller alarm	
					Använd stark autentisering med exempelvis aktivt kort, biometri, engångslösenord eller USB-token	
				Lämnad oövervakad och inloggad	Inför automatisk utloggning/låsning av dator inom viss tidsrymd	
					Information och utbildning	
	Stöld	5	5	Bärbar dator förvaras i bil	Information och utbildning	
					Förvara ej bärbara datorer i bilen	
				Datorn står lättillgänglig	Flytta datorn till en plats som ej är lättillgänglig	
					Lås fast datorn	
				Industri-spionage	Kryptera informationen	
					Spara ingen hemlig information på bärbara enheter	

Tabell 22, Resultat efter riskanalys av bärbara datorer.