Bestands– en schijfencryptie

Een onderzoek naar de toepasbaarheid binnen SURFnet bv.

Marya Steenman & Thijs van den Berg

4 juli 2005

Masteropleiding Systeem- en Netwerkbeheer
Universiteit van Amsterdam

In opdracht van SURFnet

SURFnet

Samenvatting

Steeds meer mensen maken gebruik van laptops en PDA's voor hun werk. Op laptops en PDA's is hierdoor steeds vaker vertrouwelijke bedrijfsinformatie aanwezig. Daar het aantal diefstallen van laptops en PDA's nog steeds stijgt is het risico groot voor een bedrijf dat vertrouwelijk informatie in verkeerde handen valt. Encyptie kan de schade van diefstal beperken door de informatie te versleutelen en daarmee onleesbaar te maken voor onbevoegden. Ook vanuit de overheid is aandacht besteed aan het toepassen van encryptie. Tot nu toe is het gebruik ervan toegestaan, mits wanneer gevraagd de data toegankelijk gemaakt kan worden.

Globaal kunnen er drie vormen van encryptie onderscheiden worden:

Bestandsencryptie Hierbij worden lossen bestanden versleuteld.

Filesysteemencryptie Hierbij wordt een filesysteem geïmplementeerd die encyptie levert.

Schijfencryptie Hierbij wordt de hele harde schijf of partities versleuteld. Dit kan zowel software- als hardwarematig gedaan worden.

Er moet rekening worden gehouden met het feit dat het gebruik van encryptie ook risico's met zich meebrengt en dat encryptie niet altijd zo veilig is als het lijkt. Risico's als het verlies van sleutels moeten onderkend worden en een key-management infrastructuur is daarom gewenst. Bij het implementeren van een encryptie methoden moeten aan aspecten als schaalbaarheid en performance gedacht worden.

Om de praktische toepasbaarheid van bestands- en schijfencryptie voor SURFnet te onderzoeken zijn zes encryptieproducten onderzocht. De volgende aspecten van elk product zijn onderzocht:

- Gebruikersgemak
- Recovery
- Veiligheid
- Performance
- Praktisch aspecten

Uit alle onderzoeken blijkt dat er geen standaard oplossing is. Het te gebruiken product hangt af van de situatie waarin het gebruikt gaat worden.

Gezien de mate van vertrouwelijke informatie die bij SURFnet in omloop is, is het gebruik van schijfencrytpie (CompuSec) en bestandsencrytpie (AxCrypt) de beste oplossing om de vertrouwelijkheid van gegevens te waarborgen. Er moet voor het verloop van medewerkers wel een key-management infrastructuur opgezet worden op basis van self-escrowing. Hiervoor ligt de expertise bij SURFnet die al geruime tijd ervaring heeft als CA en leverancier van PKI diensten.

Inhoudsopgave

Hoofdstuk 1

Inleiding

1.1 Probleemstelling

Steeds meer mensen krijgen een laptop en PDA van het bedrijf. Dit is makkelijk want nu kan er overal gewerkt worden, zelfs thuis. Deze trend brengt echter wel een risico met zich mee voor het bedrijf. Laptops en PDAs zijn erg gevoelig voor diefstal maar ook systemen op kantoor of thuis kunnen gestolen worden. Als een systeem gestolen wordt kan vertrouwelijke bedrijfsinformatie in handen vallen van personen waarvoor het niet bestemd is. Wie herinnert zich niet het incident met de PC van Officier van Justitie Joost Tonino?

Tegen diefstal of verlies is helaas niet veel te doen maar om de schade na de diefstal te beperken wel. Bestanden op de laptop/PDA kunnen versleuteld worden. Op deze manier blijft vertrouwelijke informatie uit handen van mensen waarvoor het niet bestemd is.

1.2 Doel

Het doel van het project is het uitvoeren van een gedegen onderzoek naar de verschillende manieren van bestands– en diskencryptie die er momenteel voor desktops/ laptops/ PDAs beschikbaar zijn. Daarbij wordt de nodige aandacht gegeven aan de theoretische grondslag van de bescherming die de diverse methoden bieden en aanvallen die daarop geboden worden. Verder richt het onderzoek zich op de praktische uitwerking van de theorie en de uitrol aspecten van de onderzochte manieren voor in ieder geval voor 1 scenario: het SURFnet kantoor. Daarnaast wordt er eventueel ook gekeken naar wat er zou gebeuren als je één en ander zou opschalen, bijvoorbeeld voor een universiteit of hogeschool.

Uit het onderzoek komt een aanbeveling en checklist die SURFnet en/ of haar klanten kan helpen bij het kiezen van de juiste encryptie methoden en product.

1.3 Leeswijzer

Globaal is het rapport in twee stukken verdeeld: een theoretisch stuk en een praktisch stuk. Het theoretische stuk begint met achtergrondinformatie over cryptografie en geeft weer wat de kwetsbaarheden en risico's zijn van cryptografie. Vervolgens worden de verschillende vormen van bestands– en diskencryptie in kaart gebracht en worden de kenmerken van elke vorm onderzocht.

Het praktische gedeelte begint met het in kaart brengen van de doelgroep en platformen die gebruik zouden moeten gaan maken van bestands– en diskencryptie. Aan de hand hiervan en aan de hand van het theoretisch onderzoek wordt een pakketselectie gemaakt. Deze pakketten worden op verschillende punten onderzocht. Aan het eind van het onderzoek wordt een eisenpakket opgesteld waaraan bestands- en diskencryptie software zou moeten voldoen. Dit eisenpakket kan door verschillende partijen gebruikt worden als leidraad bij de keuze van een eigen oplossing.

Ten slotte wordt er een conclusie gegeven en worden enkele aanbevelingen gedaan.

1.4 Relevantie

Dit rapport is bedoeld om SURFnet bv van een concreet advies te voorzien, op basis van theoretische en praktische onderbouwing, op basis waarvan zij bestands- of diskencryptie kunnen implementeren in hun eigen omgeving. Hierbij wordt waar mogelijk een herbruikbare uitwerking van de praktisch tests geleverd. Daarnaast wordt voor de afdeling "Community support" van SURFnet een advies geleverd voor het gebruik van bestands- en diskencryptie bij klanten van SURFnet.

Theoretisch onderzoek

Hoofdstuk 2

Cryptografie

In dit rapport zal vaak gesproken worden over begrippen als *cryptografie*, *encryptie*, *decryptie* en *cryptografisch algoritmen*. In dit hoofdstuk wordt een korte inleiding tot deze begrippen gegeven.

2.1 Inleiding

Cryptografie is afgeleid van twee Griekse woorden welke zoiets als "geheim" en "schrijven" betekenen. Cryptografie betekent dan ook ongeveer "geheimschrijven". Cryptografie kan daarmee gedefinieerd worden als de wetenschap die zich bezighoudt met het versleutelen en ontcijferen van al dan niet versleutelde informatie.

Het versleutelen of vercijferen van informatie is het zodanig veranderen van een begrijpbaar bericht dat het moeilijk is om te herleiden wat het oorspronkelijke bericht was. Dit hele proces staat over het algemeen bekend als *encryptie*. Het omgekeerde proces, het ontcijferen van het versleutelde bericht staat bekend als *decryptie*.

Voor het uitvoeren van deze processen is een encryptie algoritme nodig. Een algoritme is een systematisch stelsel voor het uitvoeren van wiskundige functies en de volgorde daarvan. Er kan onderscheid gemaakt worden tussen twee soorten encryptie algoritmen:

Restricted algoritmen Deze algoritmen werken op basis van geheimhouding van het algoritme. Deze manier van bescherming staat ook wel bekend als *security through obscurity*. Mocht de werking van een dergelijk algoritme ooit bekend worden dan is iedereen in staat om alle met dat algoritme gecodeerde berichten te decrypten.

Algoritmen met sleutels De meeste algoritmen maken gebruiken van sleutels. Hierbij wordt niet een algoritme gebruikt als geheimhoudingsfactor voor de encryptie maar wordt daar een sleutel voor gebruikt. Door het algoritme te voorzien van een sleutel is het niet mogelijk het encrypte bericht te achterhalen wanneer de werking van het algoritme bekend wordt. De werking van het algoritme wordt juist vaak bewust bekend gemaakt om andere de mogelijkheid te geven het algoritme te testen op veiligheid.

Naast het bovenstaande onderscheid kan er nog een verder onderscheid gemaakt worden. Er zijn twee duidelijke vormen te onderscheiden van encryptie algoritmen die werken met sleutels:

Symmetrische algoritmen Bij deze algoritmen wordt dezelfde sleutel gebruikt voor vercijfering en ontcijfering. Deze algoritmen staan ook bekend als "secret key" algoritmen.

Asymmetrische algoritmen Bij asymmetrische algoritmen wordt gebruikt gemaakt van twee verschillende sleutels; een privé sleutel die alleen bekend is bij de eigenaar van de sleutel en een sleutel die publiek bekend is. Eén sleutel wordt gebruikt voor het encrypten van het bericht en de andere sleutel voor het decrypten. Deze algoritmen staan ook bekend als "public key" algoritmen.

Een belangrijk verschil tussen deze twee algoritmen is dat symmetrische encryptie minder rekenintensief is en daardoor sneller dan asymmetrische cryptografie. Symmetrische encryptie heeft ook vaak de voorkeur voor grote bestanden of hoge datasnelheden[14].

Naast alle encryptie algoritmen is er nog een aparte groep cryptografisch algoritmen. Dit zijn de zogenaamde *hash algoritmen*. Hash algoritmen zijn functies die een bericht van onbepaalde lengte kunnen omzetten in een onbegrijpbaar bericht van een vaste lengte. Dit bericht wordt een "hash"genoemd. Hash algoritmen zijn functies die maar één kant op werken, vanuit de hash kan niet het originele bericht weer gecreëerd worden. Deze cryptografiche algoritmen zijn dan ook geen encryptie algortimen. Een voorbeeld van het gebruik van hash algoritmen is het veilig opslaan van wachtwoorden. In plaats van het wachtwoord wordt de hash van het wachtwoord opgeslagen.
In de loop van de jaren zijn er vele soorten restricted, symmetrische en asymetrische cryptografische algoritmen ontwikkeld. In deze paragraaf worden de belangrijkste cryptografisch algoritmen besproken.

2.2 Encryptie algoritmen

AES / Rijndael

AES staat voor "Advanced Encryption Standard". AES zelf is geen algoritme maar een standaard die het gebruik van een bepaald algoritme specificeert. Het algoritme gebruikt voor AES is voortgekomen uit een wedstrijd uitgeschreven door het Amerikaans Nationaal Instituut voor Standaardisatie en Technologie. Het gekozen algoritme is het Rijndael algoritme ontwikkeld door Joan Daemen en Vincent Rijmen. Dit is een symmetrisch algoritme welke een sleutellengte ondersteunt van 128, 192 of 256 bits.

DES

DES staat voor "Data Encryption Standard" en is ontwikkeld in de jaren 70. DES is een zeer bekend en veel gebruikt symmetrisch algoritme. Een nadeel van DES is de erg beperkte sleutellengte van 56 bits.

3DES

De opvolger van DES staat bekend als 3DES. 3DES is bedoeld om de sleutellengte en de veiligheid van DES te vergroten. Bij 3DES zijn drie DES bewerkingen achter elkaar geschakeld. Dit kan op twee verschillende manieren:

- Twee sleutels van 56 bits waarbij de eerste en derde bewerking met dezelfde sleutel worden uitgevoerd en waarbij effectief een sleutel van 112 bits ontstaat.
- Drie onafhankelijke sleutels van 56 bits waarbij effectief een sleutel van 168 bits ontstaat.

IDEA

IDEA staat voor "International Data Encryption Algorithm" en is ontwikkeld in de jaren 90 in Zwitserland. Het algoritme zelf lijkt erg op DES. Het manipuleren van bits gebeurd echter op een veel complexere manier en tevens wordt een grotere sleutel gebruikt van 128 bits. IDEA is in een aantal landen gepatenteerd maar wel in elke land te gebruiken voor niet-commercieel gebruik. Veel producten ondersteunen IDEA maar wel maar bieden een functie om IDEA aan of uit te zetten. Afhankelijk van het land zal IDEA dus gebruikt kunnen worden of niet.

RC2, RC4, RC5, RC6

RC staat voor "Rivest Cipher". RC2, RC4 en RC5 zijn symmetrische algoritmen ontwikkeld door Ron Rivest voor het bedrijf RSA Data Security. RC6 is afgeleid van RC5 en is ontwikkeld door Ron Rivest, Matt Robshaw, Ray Sidney en Yiqun Lisa Yin.

RC5 en RC6 ondersteunen beide sleutellengten tot 2048 bits. Voor RC5 wordt echter een sleutellengte aanbevolen van 128 bits en voor RC6 een sleutellengte van 128, 192 of 256 bits.

Blowfish

Blowfish is ontwikkeld door Bruce Schneider en is gepubliceerd in 1994. Blowfisch wordt als relatief snel symmetrisch algoritme beschouwd. Blowfish ondersteund een sleutellengte van 32 tot 448 bits.

RSA

RSA is een afkorting van de namen van de bedenkers; Ron Rivest, Adi Shamir en Leonard Adleman. Zij ontwikkelden dit algoritme in 1977. Ondanks dat RSA dus alweer een aantal jaren oud is, is het nog steeds een veel gebruikt algoritme voor asymmetrische encryptie. RSA ondersteund een sleutellengte van 330 tot 2048 bits.

Diffie-Helmann

Diffie-Helmann is ontwikkeld door Whitfield Diffie en Martin Helmann in 1976. Diffie-Helmann is geen encryptie algoritmen maar een manier voor twee partijen om een gedeeld geheim vast te stellen. Dit gedeelde geheim kan vervolgens gebruikt worden om er een key van te maken die gebruikt kan worden als input voor een symmetrisch encryptie-algoritme.

2.3 Hash algoritmen

MD2, MD4 en MD5

MD staat voor "Message Digest". De MD-algoritmen zijn one-way hash functies ontwikkeld door Ron Rivest. De laatse versie, MD5, creëert een 128 bits hash waarde.

SHA, SHA-1, SHA-2

SHA staat voor "Secure Hash Algorithm". Dit algoritme is ontwikkeld door het Amerikaans Nationaal Instituut voor Standaardisatie en Technologie in samenwerking met het Amerikaanse National Security Agency. Inmiddels zijn er van SHA verschillende varianten beschikbaar met verschillende hashwaarden en kleine verschillen in ontwerp. SHA-1 creëert een hash waarde van 160 bits. SHA-2 is

een verzamelnaam voor versies met een verschillende grotere hash waarden. Er is een 224, 256, 385 en 512 bits versie.

2.4 Kwetsbaarheden

Encryptie lijkt ideaal om er voor te zorgen dat informatie uit handen blijft van onbevoegde personen. Het gebruik van encryptie leidt soms echter tot een vals gevoel van veiligheid. Encryptie kan namelijk gekraakt worden, het kraken van encryptie staat bekend als cryptoanalyse. Een bekende aanval om encryptie te kraken is de zogenaamde *brute force* aanval. Een brute force aanval is een methode om encryptie te kraken door het proberen van alle mogelijkheden; bijvoorbeeld door het proberen van alle mogelijke wachtwoorden of sleutels.

Om encryptie zo betrouwbaar mogelijk te maken zijn een paar factoren van essentieel belang:

Het gebruik van een sleutel of niet. Algoritmen die zonder sleutel werken, de zogenaamde "restricted algoritmen", waarbij de betrouwbaarheid gebaseerd is op geheimhouding van het algoritme zijn in eerste instantie betrouwbaar. Er kan alleen niet vanuit gegaan worden dat de werking van het algoritme geheim blijft. Mocht de werking van een dergelijk algoritme bekend worden dan is iedereen in staat om alle met dat algoritme gecodeerde informatie te decrypten. Het gebruik van een sleutel is dan ook essentieel voor de betrouwbaarheid van een algoritme.

De lengte van de sleutel. Het gebruik van een sleutel brengt niet gelijk extra betrouwbaarheid met zich mee. Het is van belang dat de gebruikte sleutel lang genoeg is. Hoe langer een sleutel is, hoe langer het duurt om een brute force aanval te laten slagen. Sinds 1995 staat DES met een sleutellengte van 56 bits bekend als onbetrouwbaar en onveilig door de beperkte lengte van de sleutel.

Bescherming van de sleutel Data kan met een goed algoritme en een sleutel van voldoende lengte versleuteld worden, als de sleutel echter in verkeerde handen valt dan is de encryptie waardeloos geworden. Bij het gebruik van sleutels dient dus de nodige aandacht gegeven te worden aan de bescherming en opslag van de sleutels.

Hoofdstuk 3

Code voor Informatie Beveiliging

3.1 Inleiding

De code voor informatiebeveiliging is een voorschrift over hoe informatiebeveiliging geïmplementeerd zou moeten worden binnen een organisatie. Het voorschrift doet een aantal aanbevelingen over verschillende aspecten die te maken hebben met informatiebeveiliging.

De code schrijft voor dat voor het bewaken van vertrouwelijkheid, integriteit en authenticiteit cryptografische systemen gebruikt moeten worden om vertrouwelijke gegevens te beveiligen. Het cryptografisch systeem dat gebruikt gaat worden moet voldoen aan de eisen die gesteld worden aan het beveiligingsniveau dat nodig is voor de informatie.

Belangrijke punten zijn verder:

- Er moet rekening gehouden worden met de regels die de overheid gesteld heeft aan het gebruik van cryptografische systemen en het encrypten van informatie.
- Key management; hoe wordt omgegaan met het verlies of beschadiging van sleutels, wie hebben de beschikking over sleutels etc.

3.2 Nederlandse wetgeving

Rond 1995 [3, 4, 5] is er binnen de overheid discussie ontstaan over het gebruik van encryptie en met name de regulatie ervan.
In een wetsvoorstel is een voorstel gedaan tot verbod op encryptie en een vergunningsstelsel die gereguleerd gebruik van encryptie mogelijk maakt.

Reden voor de inhoud van dit voorstel was de mogelijkheid voor criminelen encryptie te gebruiken waardoor bewijsmateriaal onbruikbaar zou worden. Uit reacties gegeven op het wetsvoorstel bleek dat het op dat moment technisch en juridisch niet mogelijk was zo'n structuur op te zetten.

In 1998 is in de "Wet Computercriminaliteit" opgenomen dat van de verdachte decryptie geëist kan worden.

Na 11 september 2001 is de discussie sterker op gang gekomen. Voor de bestrijding van terrorisme is het noodzakelijk inzage te kunnen hebben in informatie wanneer dit gewenst is.

De huidige wetgeving zegt dat je opgedragen kan worden informatie vrij te geven en dus te decrypten. Er wordt (nog) niets gezegd over de manier waarop de sleutel beheerd moet worden zoals dat bij voorbeeld bij key–escrowing gebeurt[1]

3.3 Key management

Hoewel de wet niets zegt over het in bewaring geven van encryptie sleutels [6, 7] is dit voor bedrijven zelf wel van belang. Alleen de eigenaar van de sleutel weet het wachtwoord en alleen de eigenaar kan dus informatie leesbaar maken. Binnen bedrijven betekent dit dat hier rekening mee gehouden moet worden bij verloop van medewerkers. De informatie van de medewerkers moet wel bruikbaar blijven voor het bedrijf. Er zijn twee veel besproken manieren om er voor te zorgen dat ook na het wegvallen van medewerkers de informatie toegankelijk blijft.

Escrow Escrowing is het in bewaring geven van de privé sleutel bij een derde partij een zogenaamde TTP (Trusted Third Party)

Self -Escrow Bedrijven (met name grote) zijn huiverig tegenover het onderbrengen van de privé sleutel bij een TTP en gaan over tot self-escrowing. Dit betekent dat binnen een bedrijf de verschillende prive sleutels op een of andere manier bewaard worden.

[1] Het bij een vertrouwde derde partij in bewaring brengen van de encryptiesleutel

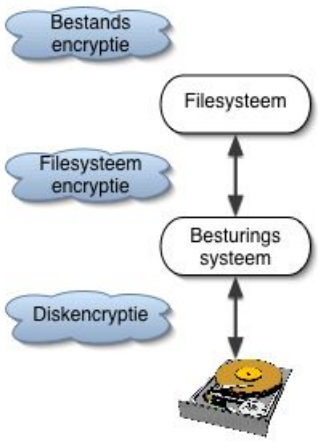
Hoofdstuk 4

Vormen van bestands- en schijfencryptie

Encryptie kan gebruikt worden voor het beschermen van vele soorten gegevens en informatie. In dit onderzoek wordt alleen gekeken naar encryptie van gegevens en informatie op desktops, laptops en PDAs. Dit soort encryptie staat ook wel bekend als bestands en schijfencryptie. Er wordt dus niet gekeken naar encryptie van bijvoorbeeld email of andere soorten dataverkeer.

Voor het encrypten van gegevens en bestanden zijn verschillende manieren beschikbaar. In het artikel van Poul-Henning Kamp [2] worden globaal de volgende klassen onderscheiden:

- Bestandsencryptie
- filesysteemencryptie
- Schijfencryptie



Figuur 4.1: Plaats van bestands–, filesysteem– en schijfencryptie t.o.v. systeem

4.1 Bestandsencryptie

Bestandsencryptie [1] is encryptie op applicatieniveau. Dit betekent dat elk bestand, directory, etc. afzonderlijk van het andere versleuteld wordt, al dan niet met dezelfde key. Het encrypten gebeurt in principe altijd doormiddel van een applicatie. Een gebruiker wordt geacht zelf de juiste bestanden te encrypten en decrypten.

4.2 Filesysteemencryptie

Bij deze manier wordt een apart filesysteem gebruikt om gegevens en bestanden te kunnen encrypten. Er zijn verschillende manieren waarop filesysteemencryptie kan werken[8]:

Block-based systemen Block-based systemen werken tussen het fysieke apparaat en het filesysteem in. Encryptie gebeurt per schijfblok, wat als voordeel heeft dat er geen kennis nodig is van het bovenliggende filesysteem en zou daarom ook gebruikt kunnen worden voor swappartities. Verder is een eigenschap van block-based systemen dat ze de informatie over bestanden (eigenaar en dergelijke) en de directory structuur ook niet bekend maken.

Disk based systemen Bevinden zich op een hoger niveau dan een block-based systeem en zijn daarom in staat complexere acties met betrekking tot autorisatie en authenticatie uit te voeren. Op dit niveau wordt niet van schijfblokken gesproken, maar over bestanden en mappen en de layout daarvan op de harde schijf. Verder kunnen ze ook meta-data verborgen houden, hoewel dit vaak niet toegepast wordt om de opbouw van het filesysteem duidelijk te houden voor het besturingssysteem. EFS van Microsoft is een voorbeeld van een disk based systeem.

Network loopback based systemen Deze manier van filesysteem encryptie bevindt zich weer op een hoger niveau dan het disk based systeem en ze functioneren bovenop het echte filesysteem en werken via het netwerk. Het feit dat ze bovenop het gewone filesysteem werken heeft tot gevolg dat ze geen ivloed hebben op de layout van het filesysteem op de harde schijf, een network loopback based systeem maakt gebruik van het onderliggende standaard filesysteem. Het nadeel van dit systeem als gekeken wordt naar de encryptie en prestatie is dat alles via het netwerk verloopt. Bij de beveiliging gaat ook de veiligheid van het onderliggende protocol een rol spelen.

Stackable file systemen Stackable file systems valt tussen het disk based systeem en het network loopback file systeem, en werkt bovenop het normale filesysteem maar acties hoeven niet via het netwerk of de user kernel te lopen.

Als een gebruiker inlogt op het besturingssysteem zijn bestanden direct na het inloggen beschikbaar. Als andere personen dus inloggen met het account van deze gebruiker dan hebben zij ook toegang tot de bestanden en gegevens op het filesysteem.

4.3 Schijfencryptie

Bij deze manier wordt de hele schijf[1] geëncrypt[1] en is een sleutel nodig voor het encrypten en decrypten. De twee eerder genoemde manieren werken onder het besturingssysteem, terwijl schijfencryptie onafhankelijk tracht te zijn van het besturingssysteem. Installatie van schijfencryptie kan echter niet onafhankelijk van het besturingssysteem plaatsvinden en het vooraf decrypten van de schijf zou te veel tijd in beslag nemen. De oplossing die schijfencryptie-implementaties hiervoor

[1] Wanneer van schijfencryptie gesproken wordt kunnen ook alle partities op een schijf bedoeld worden.

bieden is het vooraf unlocken van de schijf waardoor de data van het besturingssysteem gedecyrpt en geladen kan worden.

Wanneer ingelogd wordt onder het besturingssysteem, worden aangesproken bestanden automatisch versleuteld en ontsleutelt zonder dat de gebruiker dit merkt. Elke read en write actie op de harde schijf wordt het encryptie proces aangesproken.

Het voordeel van schijfencryptie is dat de hele schijf voorzien is van encryptie, en dus ook de tijdelijke bestanden en mappen en de swap partities. Schijfencryptie is op twee manieren te realiseren:

Software Doormiddel van speciale software die de encryptie en decryptie voor zijn rekening neemt.

Hardware Door het gebruik van hardeschijven met ingebouwde encryptie. Een voorbeeld hiervan zijn de schijven van Seagate[13].

Hoofdstuk 5

Bestands- en schijfencryptie in de praktijk

In dit hoofdstuk zullen we een aantal aspecten van bestands- en schijfencryptie bespreken die bij de implementatie ervan een rol spelen.

5.1 Risico's

5.1.1 Encryptie sleutels

Encryptie maakt vaak gebruik van sleutels, en dit brengt risico's met zich mee: Wat als een sleutel verloren gaat? Er zijn verschillende oorzaken te bedenken waardoor dit kan gebeuren:

- Een persoon kan plotseling overlijden en zodoende zijn sleutel(s) mee het graf in nemen.
- Een persoon kan ontslag krijgen/nemen en zijn sleutel(s) opzettelijk meenemen of vernietigen.
- Een persoon kan zijn sleutel(s) kwijt raken.

Het verlies van een sleutel heeft zeer ernstige gevolgen. Bij het verlies van een sleutel is in principe alle informatie die met deze sleutel encrypt is onbereikbaar geworden. Mocht een persoon overlijden of ontslag nemen/krijgen en zijn sleutel vernietigen dan is al zijn gedane werk verloren gegaan. Een eventuele opvolger en collega's kunnen niet meer bij het gedane werk van deze persoon komen.

Het risico van het verliezen van een sleutel kan beperkt worden door goed sleutelbeheer. Bij sleutelbeheer worden sleutels op een centrale veilige plek opgeslagen (zie hoofdstuk 3).

5.1.2 Verantwoordelijkheid

Bij bestandsencryptie is de gebruiker verantwoordelijk voor het encrypten en decrypten van de verschillende bestanden. Bij filesysteemencryptie is dit ook zo wanneer bestanden niet standaard naar een map voorzien van encryptie worden weggeschreven. Bij schijfencryptie is dit transparant voor de gebruiker, omdat dit automatisch gebeurt. Dit laatste heeft als voordeel dat altijd in ieder geval de meest belangrijke informatie geëncrypt is, terwijl dit bij bestands- en filesysteemencryptie nog maar de vraag is.

5.1.3 Wachtwoord

Bij bestandsencryptie kunnen wachtwoorden[1] gebruikt worden die de gebruikers zelf maken. Het risico hiervan is dat gebruikers vaak wachtwoorden kiezen die makkelijk via verschillende manieren te achterhalen zijn (via bijvoorbeeld een brute-force aanval of social-engineering).

Bij filesysteemencryptie is ongeveer hetzelfde van invloed, omdat dit afhankelijk is van het wachtwoord dat gebruikt wordt bij inloggen op het systeem. Wanneer niet afgedwongen wordt een sterk wachtwoord te gebruiken is ook het filesysteemencryptie principe niet voorzien van een sterk wachtwoord.

Bij schijfencryptie kan een apart wachtwoord gebruikt worden voor het toegankelijk maken van de schijf, het risico hiervan is dat ook dit wachtwoord zwak gekozen kan worden.

Wanneer wachtwoorden gebruikt worden is het systeem zo sterk als het wachtwoord is. In alle gevallen (ook bij gebruik van Single-Sign-On) is het van groot belang dat een sterk wachtwoord gekozen wordt. Het wachtwoord dient bij voorkeur ongelijk te zijn die van het gebruikers account. Dit om een extra laag van veiligheid in te bouwen.

5.1.4 Tijdelijke bestanden

Bij bestandsencryptie worden tijdelijke bestanden en swappartities niet geëncrypt, waardoor er toch vertrouwelijke informatie beschikbaar kan blijven.

Ook voor filesysteemencryptie geldt dat de encryptie zich beperkt tot die data die bewust wordt aangemerkt voor encryptie. Dit betekent dat tijdelijke bestanden en data in bijvoorbeeld swap ruimte niet voorzien is van encryptie en dus beschikbaar is voor anderen.

5.1.5 Beschikbaarheid

Als gebruik wordt gemaakt van bestandsencryptie moet voor het openen van bestanden of mappen een wachtwoord opgegeven worden. Bij filesysteem- en schijfencryptie is dit niet het geval. Eenmaal ingelogd zijn alle bestanden beschikbaar voor de gebruiker en na uitloggen niet meer.

Schijfencryptie beschermt de gegevens wanneer de schijf in verkeerde handen valt (bijvoorbeeld bij diefstal). Wanneer ingelogd is op het systeem zijn wel alle gegevens beschikbaar en dus leesbaar.

Het feit dat na inloggen alle gegeven beschikbaar zijn, betekent ook dat bestanden op de normale manier door programma's gebruikt worden. Wanneer bestanden overgedragen worden op een ander (via bijvoorbeeld email) zijn deze niet langer versleuteld.

Bij filesysteemencryptie geldt dit niet, bestanden blijven versleuteld. Wanneer een bestand naar het geheugen geschreven moet worden (bijvoorbeeld na het openen ervan) wordt het gedecrypt. Wanneer bestanden van een geëncrypt filesysteem uitgewisseld worden, worden deze bestanden onversleuteld uitgewisseld.

Alleen bij bestandsencryptie is het mogelijk bestanden geëncrypt uit te wisselen.

[1] In plaats van wachtwoorden kunnen natuurlijk ook technieken als smartcard en tokens gebruikt worden

5.1.6 Keyloggers

Zowel software- als hardwarematig zijn keyloggers te gebruiken om aangeslagen toetsen te registeren en zo wachtwoorden en dergelijke te achterhalen. Niet alleen kan zo het gebruikerswachtwoord achterhaald worden, maar ook de wachtwoorden die gebruikt worden voor het encryptie mechanisme.

5.2 Schaalbaarheid

Bestandsencryptie is onafhankelijk van het besturingssysteem en wordt gerealiseerd door door een applicatie. Alleen de gebruiker heeft controle op het encryptie- en decryptieproces. Hierdoor kunnen verschillende systemen (gebruikers) op dezelfde manier gebruik maken van bestandsencryptie. De uitwisseling van bestanden is om dezelfde reden gemakkelijk voor de gebruikers. Verder kan deze manier van versleutelen ook gebruikt worden om andere media als USB sticks te voorzien van encryptie. Omdat voor encryptie/decryptie alleen een applicatie nodig is wordt de schaalbaarheid afhankelijk van hoe een organisatie omgaat met het uitrollen van applicaties. Indien dit uitrollen centraal gebeurd is bestandsencryptie erg schaalbaar.
Alle standaard filesystemen van de meest gebruikte besturingssystemen ondersteunen geen encryptie. Er zal dus uitgeweken moeten worden naar een alternatief filesysteem dat wel overweg kan met encryptie. Deze filsystemen zijn vaak besturingssysteemafhankelijk. Zo biedt Microsoft EFS(Encrypted File System) aan maar alleen voor Windows 2000 en Windows XP Professional. Zolang door een organisatie het zelfde besturingssystemen gebruikt wordt voor alle werkplekken dan is filesysteemencryptie goed schaalbaar. Wordt niet een standaard besturingssysteem gebruikt dan zal voor elke besturingssysteem een apart filesysteem gezocht en geïmplementeerd moeten worden en is de schaalbaarheid dus erg laag.
Schijfencryptie wordt ook vaak gerealiseerd door software. Hierbij geldt net als bij bestandsencryptie dat de manier van uitrollen van de applicatie invloed heeft op de schaalbaarheid. Het uitrollen bij schijfencryptie is wel een stuk lastiger omdat voor het eerste gebruik de hele hardeschijf versleuteld moet worden.

5.3 Performance

Zoals eerder gezegd werkt bestandsencryptie onafhankelijk van het besturingssysteem, dus op dit gebied (zoals bijvoorbeeld bij het opstarten van het systeem) vindt geen performance verlies plaats. Het enige moment waarop theoretisch performance verlies bemerkt zou kunnen worden is wanneer een bestand geëncrypt of gedecrypt moet worden.

De performance van filesystemencryptie is min of meer hetzelfde als voor bestandsencryptie. Data wordt op het moment van toegang gedecrypt en daarom zal alleen op dat moment performanceverlies merkbaar zijn. In tegenstelling tot bestandsencryptie worden alle bestanden in het filesysteem automatisch geëncrypt en hoeft dit niet zoals bij bestandsencryptie expliciet aangegeven te worden.

Bij schijfencryptie is ook bijna geen performance verlies, maar alleen bij het openen en afsluiten van bestanden. Wanneer het systeem eenmaal opgestart is zijn alle bestanden beschikbaar en worden alleen bij gebruik geëncrypt en gedecrypt.

5.4 Praktische aspecten

In deze paragraaf worden enkele praktische aspecten besproken waarmee rekening gehouden moet worden wanneer gekozen wordt van een vorm van encryptie.

- Backup
- Schijfbeheer
- Gebruikersprofielen
- Implementatie

5.4.1 Backup

Data die door middel van bestandsencryptie versleuteld is, wordt door het besturingssysteem en andere applicaties nog steeds als losse files gezien. Bij het maken van een backup blijven deze bestanden dan ook voorzien van versleuteling.

Bij filesysteem– en schijfencryptie is dit niet het geval. Zodra bestanden benaderd worden, worden ze ontsleutelt. Wanneer van deze bestanden een backup gemaakt wordt, worden ze onversleuteld opgeslagen op het backup medium tenzij hiervoor ook encryptie voorzieningen bestaan. Wanneer een kopie van de hele schijf gemaakt wordt (in geval van een image of raid schijf) blijft de encryptie wel bestaan.

5.4.2 Schijfbeheer

Bij het gebruik van schijfencryptie kan onderhoud aan de schijf (zoals defragmentatie) effect hebben op de versleutelde data. Bij bijvoorbeeld defragmentatie heeft het verplaatsen van data negatieve gevolgen. Verder kan de toegang tot de PC geheel blokkeren als het encryptie mechanisme niet meer goed werkt.

Het gebruik van partitioneringsprogramma's kunnen er ook voor zorgen dat data niet meer te decrypten is. Als een gedeelte van een versleutelde partitie geformatteerd wordt mist het encryptie mechanisme een gedeelte van de data.

5.4.3 Gebruikersprofielen

Bij veel bedrijven wordt gewerkt via gebruikersprofielen waarbij gebruikersdata op een netwerkserver opgeslagen wordt. Als de systemen van de gebruikers worden voorzien van schijfencryptie, maar er wordt gewerkt via gebruikersprofielen wordt de data niet voorzien van versleuteling omdat de data niet lokaal opgeslagen wordt.

Het is belangrijk na te gaan waar bepaalde data zich bevindt en af te wegen of schijfversleuteling wel de oplossing is.

5.4.4 Implementatie

Het implementeren van een encryptie methode hangt af van de gekozen methode en de situatie binnen het bedrijf. Hoe wordt bestandsencytpie in de organisatie uitgerold, hoe voorzien we alle schijven van encryptie? Dit soort vragen moeten beantwoord worden voordat de implementatie plaatsvindt.

Het uitrollen van een encryptiemethode zou in de ideale situatie zo veel mogelijk geautomatiseerd moeten plaatsvinden. Met bestandsencryptie en filesysteemencryptie is dit goed te doen, bijvoorbeeld door gebruik te maken van een installatie-image. Bij schijfencryptie wordt dit een stuk lastiger, omdat dit per schijf moet gebeuren.

Hoofdstuk 6

Conclusie theorie

Het gebruik van encryptie is een veel besproken onderwerp. Duidelijk is wel dat het gebruik ervan onmisbaar is om vertrouwelijke informatie uit handen te houden van personen waarvoor deze informatie niet bestemd is. In de "Code voor Informatiebeveiliging"wordt het gebruik van encryptie aanbevolen. Wel moet opgemerkt worden dat encryptie een vals gevoel van veiligheid kan geven, omdat sleutels en algoritmen gekraakt zouden kunnen worden.

Zoals in hoofdstuk 2 beschreven wordt zijn er vele verschillende soorten algoritmen elk met verschillende sleutellengtes te gebruiken voor het versleutelen van informatie. Het mag duidelijk zijn dat bij gebruik van encryptie de keuze voor een algoritme en de lengte van de sleutel belangrijk is. AES met 128 bits sleutel wordt tegenwoordig als veelgebruikt en veilig algoritme beschouwd voor beveiliging op langere termijn. Indien een grotere sleutel mogelijk is voor encryptie heeft dit altijd de voorkeur.

Voor het versleutelen van informatie op laptops, desktops en PDAs is een keuze mogelijk tussen bestands-, filesysteem- en schijfencryptie. De veiligheid die een encryptie methode biedt hangt onder andere af van het onderliggende algoritme en de manier waarop wachtwoorden en sleutels gebruikt worden. Wanneer mensenlijk handelen een grote rol gaat spelen heeft dit ook een grote invloed op hoe sterk de veiligheid kan zijn. Wel kan geconcludeerd worden dat encryptie in meer of mindere mate leidt tot prestatieverlies.

Case SURFnet / praktisch onderzoek

Hoofdstuk 7

Bedrijfsanalyse

In dit hoofdstuk wordt een analyse gemaakt van SURFnet bv. Hierbij word gekeken naar de aanwezige gebruikersgroepen, de mate waarin vertrouwelijke informatie aanwezig is en welke platformen gebruikt worden.

7.1 Gebruikersgroepen

Binnen het SURFnet kantoor zijn twee verschillende gebruikersgroepen te onderscheiden. Er is gekozen voor het maken van onderscheid op basis van technische achtergrond, omdat op andere punten (als het werken met vertrouwelijke informatie of rechten) niet van toepassing is wanneer een vorm van encryptie gebruikt gaat worden.

- Technische gebruikers
- Niet- technische gebruikers

Het aantal niet technische gebruikers is belangrijk in het maken van een keuze voor een product. Wanneer er veel niet technische gebruikers zijn is het niet verstandig een product te kiezen dat ingewikkeld is in het gebruik. Zeker wanneer gebruik gemaakt zou gaan worden van bestandsencryptie belemmert de moeilijkheid van een product het consequente gebruik van bestandsencryptie.

Binnen het SURFnet kantoor ligt het aantal niet- technische gebruikers erg laag.

7.2 Vetrouwelijke gegevens

Het gebruik van encryptie en het soort encryptie hangt af van het feit of er vertrouwelijke gegevens aanwezig zijn. Binnen het SURFnet kantoor kan de volgende informatie als vertrouwelijk aangemerkt worden:

- data-dragers (bestanden, documenten, emails) met wachtwoorden
- data-dragers met betrekking tot serieuzere incidenten bij SURFnet-CERT
- data-dragers met betrekking tot personeelsgegevens.
- data-dragers met betrekking tot aanbestedingen.

SURFnet is een organisatie met een groot aantal klanten. Er is een actief contact tussen SURFnet en haar klanten en daarmee gaat er ook vertrouwelijke informatie over en weer.

7.3 Platformen

Het onderzoek naar bestands- en schijfencryptie richt zich alleen tot gebruikersplatformen die gebruikt worden binnen het SURFnet kantoor. Tijdens het onderzoek wordt niet gekeken naar de serverplatformen binnen SURFnet of platformen bij klanten van SURFnet.
Alle gebruikersplatformen binnen SURFnet zijn gestandaardiseerd. Er zijn drie soorten standaard gebruikersplatformen te onderscheiden:

PC's met Windows XP Professional Deze vormen de vaste werkplekken van alle medewerkers binnen SURFnet.

Laptops met Windows XP Professional Deze vormen de mobiele werkplekken van medewerkers en zijn onder andere bedoeld als thuiswerkplek.

PDA's met Windows CE Deze worden door medewerker gebruikt voor onder andere het opslaan van adresgegevens.

7.3.1 VIA project

Intern is SURFnet bezig met het VIA project (Vernieuwde Interne Automatisering). Tijdens dit project worden alle werknemers van onder andere nieuwe werkplekken en laptops voorzien.

Een ander onderdeel van het project is een DVD die de werkplek kan installeren of herstellen. Deze DVD gaat uit van een bepaald gebruik en indeling van de schijf, namelijk 4 partities waarvan c: de systeem partitie is. Wanneer er behoefte is aan het herstellen van de werkplek kan voor verschillende opties gekozen worden:

- Partitioneren en formatteren van de gehele harde schijf
- Herpartitioneren en formatteren van de c:-partitie
- Installeren van de standaard SURFnet werkplek
- Terugzetten van een Ghost image.

7.4 Eisen en Wensen

In de volgende paragrafen worden de eisen en wensen van SURFnet bv met betrekking tot bestands– en schijfencryptie op een rij gezet.

7.4.1 Eisen

Besturingsysteem Het standaard platform gebruikt bij SURFnet bv is een desktop/ laptop met Windows XP Professional. Er moet dus minimaal ondersteuning zijn voor Windows XP Professional.

Hibernation Er wordt veel gebruik gemaakt van laptops. Met name laptops zijn gevoelig voor diefstal. Bij gebruik van hibernation wordt de actieve (al dan niet gevoelige) data naar de harde schijf geschreven. Het product moet hibernation ondersteunen en deze data versleuteld bewaren.

Gebruikergemak Het product moet zo min mogelijk handelingen van de gebruikers vereisen.

7.4.2 Wensen

Platform ondersteuning Bij SURFnet bv wordt door verschillende werknemers ook gebruik gemaakt van een tweede besturingssysteem. Ondersteuning van meerdere besturingssytemen is gewenst.

Platform Gewenst is ook het gebruik van het pakket voor PDA's.

Partitionering Partitionering wordt (onder andere voor een tweede besturingssysteem) bij surfnet veel gebruikt en de mogelijkheid dit toe te kunnen blijven passen is een wens.

RAID ondersteuning Steeds vaker zijn werkstations uitgerust met RAID, dus de voorkeur gaat uit naar ondersteuning voor RAID.

Hoofdstuk 8

Productselectie

Om de praktische aspecten van bestands- en diskencryptie te onderzoeken worden een aantal producten geselecteerd en onderzocht. Er zijn op het gebied van encryptie vele tientallen producten te krijgen vinden. In dit onderzoek zijn in het totaal zes producten aan een onderzoek onderworpen.

Aan de keuze voor deze producten ligt een aantal eisen en wensen ten grondslag:

- Alle producten dienden te werken onder Windows XP Professional vanwege het gebruik hiervan binnen SURFnet bv.
- De producten dienden niet allen dezelfde vorm van encryptie toe te passen. Om deze reden is gekozen voor drie bestandsencryptie producten, één encrypted filesyteem en twee schijfencryptie producten.
- De producten dienden niet allen commerciële of allen open source producten te zijn maar een mix hiervan. Open-source pakketten hebben namelijk als voordeel dat de volledige specificatie van het product beschikbaar is. Daarnaast wordt gekeken naar onderlinge verschillen in onder andere prestatie tussen commerciële en open-source pakketten.
- De producten dienen een zekere mate van volwassenheid bereikt te hebben.
- De producten dienen gebruik te maken van de hedendaagse standaarden op het gebied van encryptie,

In de volgende paragrafen zullen alle gekozen producten kort besproken worden. De keuze voor de producten is gemaakt op basis van de eisenlijsten hiervoor genoemd en die van SURFnet.

8.1 TrueCrypt

TrueCrypt(http://www.truecrypt.org) is een open-source bestandsencryptie programma. Het voordeel van het gebruik van opensource programma's is dat alles van het product bekend gemaakt mag worden, dit geldt dus ook voor TrueCrypt en zowel de broncode als een uitgebreide beschrijving van de interne werking van het product zijn voorhanden.

De reden dat gekozen is voor TrueCrypt is:

- Bestandsencryptie op basis van containers(zie hst 10.1)
- Ondersteuning voor Windows XP

- Ondersteuning voor USB-sticks.
- Gratis
- Veel gebruikt open-source pakket

8.1.1 Specificaties

De huidige productversie van TrueCrypt is 3.1a. De verschillende encryptie algoritmen die TrueCrypt gebruikt zijn:

- AES-256
- Blowfish 448-bit key
- CAST5
- Serpent 256-bit key
- Triple DES
- Twofish 256-bit key

8.2 AxCrypt

AxCrypt is een opensource bestandsencryptie programma. Het programma is beschikbaar onder de GNU General Public License en is ontwikkeld door de zweed Svante Seleborg .

De reden dat gekozen is voor AxCrypt is:

- Bestandsencryptie
- Ondersteuning voor Windows XP
- Gratis
- Veel gebruikt open-source pakket
- Onderdeel van de SURFkit[17]

8.2.1 Specificaties

De huidige productversie van Axcrypt is 1.6.1 en dateert van 16-03-2005. Het encryptie algoritme dat AxCrypt gebruikt is AES-128 en als hash algoritme wordt gebruik gemaakt van SHA-1.

8.3 PGP Desktop

PGP Desktop is een pakket dat zowel bestandsversleuteling als schijf versleuteling ondersteunt. De achtergrond van het pakket is PGP (Pretty Good Privacy) een veel gebruikt computerprogramma voor cryptografie en authenticatie.

De reden dat gekozen is voor PGP Desktop is:

- Bestandsencryptie

- Gehele schijfencryptie
- Ondersteuning voor Windows XP
- Ondersteuning voor randapparatuur
- Open-source van de onderliggende techniek (PGP)
- Veel gebruikt techniek (PGP)
- Wordt al binnen SURFnet gebruikt voor onder andere encryptie en signering van mail

8.3.1 Specificaties

De huidige product versie van PGP Desktop is 9.0. PGP Desktop maakt gebruik van de volgende encryptie en hash algoritmen:

- AES
- CAST
- IDEA
- Triple DES
- Twofish
- RSA
- Diffie-helman
- SHA1 en SHA2
- MD5 en RIPEMD

8.4 EFS

EFS(http://www.microsoft.com) is het ingebouwde filesysteem (behoeft dus geen extra installatie) encryptie systeem van Windows 2000 en Windows XP Professional en daarom ook interessant om bij het onderzoek te betrekken.

De reden dat gekozen is voor EFS is:

- Filesysteem encryptie
- Geïntegreerd met Windows XP
- Vanuit SURFnet gevraagd

8.4.1 Specificaties

De werking van EFS is gebaseerd op de cryptografische ondersteuning die geïntroduceerd werd met Windows NT[15].

Binnen EFS wordt gebruik gemaakt van twee algoritmen:

- DESX
- RSA-1024

8.5 CompuSec

CompuSec is een schijfencryptie programma ontwikkeld door het bedrijf CE-Infosys (www.ce-infosys.com). CE-Infosys is een internationaal bedrijf gespecialiseerd in data en netwerk beveiligingssystemen. De basis versie van CompuSec is gratis beschikbaar. Tegen betaling levert CE-Infosyst geavanceerde toevoegingen voor CompuSec als vingerafdruklezers of een centraal management systeem.

De reden dat gekozen is voor CompuSec is:

- Gehele schijf versleuteling
- Bestands versleuteling
- Ondersteuning voor Windows XP
- Ondersteuning voor hibernation
- Ondersteuning voor randapparatuur
- Gratis in de basisversie

8.5.1 Specificaties

De huidige productversie van CompuSec is 4.18.1 en dateert van 22-02-2005 Voor het encrypten van data wordt gebruik gemaakt van AES-128. In combinatie met het betaalde product GlobalAdmin kan ook gebruik gemaakt worden van AES-256 of DESX.

8.6 DriveCrypt Plus Pack (DCPP)

DCPP is een schijfencryptie programma ontwikkeld door het bedrijf SecurStar Computer security.(http://www.securstar.com)

Van DCPP is een 30 dagen testversie onderzocht. Deze testversie bevatte wel alle functionaliteiten die ook in het volledige programma aanwezig zijn.

De reden dat gekozen is voor DCPP is:

- Schijfencryptie op basis van partities
- Ondersteuning voor Windows XP
- Ondersteuning voor randapparatuur

8.6.1 Specificaties

De huidige versie van DCPP is 3.0G en dit pakket maakt gebruik van het AES-256 algoritme om data te encrypten.

Hoofdstuk 9

Productonderzoek

In dit hoofdstuk wordt het onderzoek naar de geselecteerde producten beschreven.

9.1 Testopstelling

Voor het onderzoek zijn drie Intel Pentium III 1.00 GHz systemen met 256 MB RAM gebruikt. Op elke systeem is Windows XP geïnstalleerd met de laatste patches(20 juni). Elke systeem bevatte een 20 GB harde schijf verdeeld in twee partities; 5 GB NTFS testpartitie en 15 GB NTFS partitie.

Voor het testen van encryptie en decryptie is gebruik gemaakt van vier standaard bestanden (met random data) van de volgende grootte:

- 1 MB
- 10 MB
- 100 MB
- 1000 MB

9.2 Onderzoek

In de volgende paragrafen wordt precies beschreven welke aspecten van elk product onderzocht zijn. Bij het onderzoek naar de geselecteerde producten is er vooral voor gekozen om te kijken naar wat voor praktisch aspecten het gebruik van deze producten met zich mee brengt. Daarnaast is ook extra aandacht besteed aan de veiligheid en betrouwbaarheid van een product op basis van wat de theorie hierover zegt.

De producten verschillen onderling op punten als: installatie, werking, recovery, etc. Dit maakt het niet mogelijk eenduidige tests toe te passen om deze aspecten te onderzoeken. Er wordt per aspect beschreven wat het doel van het onderzoek is. Daar waar mogelijk (bijvoorbeeld de performance test) wordt beschreven welke stappen genomen moeten worden om dezelfde vergelijkbare resultaten te krijgen.

9.2.1 Gebruiksgemak

Bij veel vormen van encryptie, vooral bestandsencryptie, is de gebruiker zelf verantwoordelijk voor de beslissing of hij/zij bestanden encrypt en voor het uitvoeren van het encryptieproces. Gebruikers zullen dus overtuigd moeten worden van het belang van encryptie. Zelfs als gebruikers overtuigd zijn van het belang laten gebruikers het gebruik van een product vaak afhangen van het gebruiksgemak. Indien de gebruikers te veel handelingen moeten verrichten is de kans groot dat zij het product links zullen laten liggen.

Gebruiksgemak beoordelen wij op:

GUI Hoe ziet de interface van het product eruit, werkt het goed, is het overzichtelijk.

Installatie Is de installatie eenvoudig, of zijn er veel onduidelijke functies aanwezig.

Windows look-and-feel Werkt het zoals mensen gewend zijn dat applicaties werken onder Windows. Hierbij kan gedacht worden aan de opbouw van menu's, het overspringen naar velden met de tab-toets, etc.

Bruikbaarheid zonder handleiding Wijst het programma zich vanzelf voor gebruikers met enige achtergrond met Windows, of is het voor iedere stap nodig de handleiding te raadplegen.

Gebruiksondersteuning Hoe is de gebruikers ondersteuning? Is er een handleiding, FAQ, hulpfunctie, (web)fora en support van de leverancier beschikbaar voor het beantwoorden van vragen.

9.2.2 Recovery

Het risico van het kwijtraken van een wachtwoord of sleutel is al eerder besproken in hoofdstuk 5. Zonder het wachtwoord of key is het bijna onmogelijk geworden het decryptieproces uit te voeren. In het onderzoek wordt daarom gekeken naar de volgende punten:

Wachtwoord en key recovery Is het mogelijk om bij het kwijtraken van een wachtwoord of key nog steeds bij data te kunnen komen. Zo ja, hoe wordt dit toegepast en is het praktisch bruikbaar.

9.2.3 Veiligheid

Encryptie kan op vele manieren toegepast worden en biedt niet altijd de veiligheid die het lijkt te bieden. Van elk product is de veiligheid op de volgende punten onderzocht:

Tijdelijke bestanden Hoe gaat het product om met tijdelijk bestanden? worden deze goed verwijderd?

Schijven omwisselen Wat gebeurt er als een harde schijf, die compleet versleuteld is of waarvan delen versleuteld zijn, als secondary schijf in een ander testsysteem wordt geplaatst. Dit is getest op de volgende manier; De harde schijf is met een product compleet versleuteld. Deze harde schijf is vervolgens in een andere testsysteem gezet als secondary schijf. Vanuit het besturingssysteem is nu gekeken of de tweede versleutelde schijf benaderbaar was en wat voor informatie deze toonde.

Opslag van keys en wachtwoorden Hoe en waar slaan producten keys en wachtwoorden op.

9.2.4 Performance

Encryptie en decryptie kost altijd een geringe tijd door de complexiteit en vele handelingen die het encryptie algoritme uitvoert. De hoeveelheid tijd is voor elk encryptie algoritme weer verschillend.

Bij de bestandsencryptie producten is onderzocht hoe lang het duurt of verschillende bestanden te encrypten of te decrypten en of met deze waarden het nog steeds goed werkbaar is. Bij de schijfencryptie producten is onderzocht hoe lang het duurt om de complete harde schijf te versleutelen en ontsleutelen. Daarnaast is ook gekeken naar de invloed van de schijfencryptie op de read en write speed van de harde schijf. Hiervoor is gebruik gemaakt van het programma *Fresh Diagnose*[12].

Bestandsencryptie Meten van de duur van de encryptie en decryptie van de in paragraaf 9.1 genoemde bestandsgroottes. Verschillen tussen de producten in encryptie en decryptie snelheid zegt iets over het verschil in performance.

Filesysteem encryptie Hoe lang duurt het om een bestand naar een geëncrypt filesysteem te schrijven. Hierbij zijn twee tijden te onderscheiden, namelijk de kopieer tijd en de encryptie tijd. De kopieertijd is korter dan de encryptie tijd, de toegankelijkheid van een bestand geeft in dit geval aan dat de encryptie tijd ook verlopen is.

schijfencryptie Bij partitie en schijf versleuteling worden de gemiddelde read en write tijden vergeleken met de gemiddelde read en write tijden van de niet versleutelde versie van deze partities en schijven.

9.2.5 Praktische aspecten

Met het gebruik van een encryptie product komen een aantal dingen kijken. Zo kan het delen van bestanden met collega's onmogelijk worden of kunnen bestanden misschien niet meer gebackup worden.

Van elk product zullen de volgende praktische aspecten bekeken worden:

Hibernation Hoe gaat het product om met hibernation?

Partitionering Hoe gaan producten om met partitionering. Is dit nog mogelijk na het gebruik van encryptie?

Backup Wat voor invloed heeft het maken van een backup voor de encryptie van bestanden en mappen?

9.3 Checklist

Alle punten uit de hiervoor genoemde paragrafen vormen de basis van een checklist waarin per product wordt aangegeven hoe ze voor de verschillende punten beoordeeld zijn. Deze checklist is te vinden in bijlage A.

Hoofdstuk 10

Resultaten

In dit hoofdstuk wordt het resultaat weergegeven van het uitgevoerde onderzoek naar encryptieproducten.

10.1 TrueCrypt

TrueCrypt werkt op basis van containers. Een bestand wordt geëncrypt en is vervolgens een container waarin andere bestanden opgeslagen en dus geëncrypt worden. Deze containers kunnen standaard en hidden zijn. Een hidden container is een container binnen een standaardcontainer en wordt na opgeven van een ander wachtwoord zichtbaar. Dit heeft als voordeel dat wanneer het wachtwoord van de standaard container bekend gemaakt moet worden niet de gegevens in de hidden container zichtbaar worden.

Containers worden bruikbaar gemaakt door ze te mounten in het Windows filesysteem, hierna zijn de containers aan te spreken als partities zoals dit ook mogelijk is voor bijvoorbeeld de c:- partitie.

10.1.1 Werking

Sleutels

Master key Wordt gebruikt om de container te encrypten en decrypten. De masterkey wordt bewaard in de TrueCrypt header in een versleutelde vorm door een random number generator die gebruik maakt van een hash algoritme (HMAC-SHA-1 of HMAC-RIPEMD-160).

User key De user key wordt gebruikt om de TrueCrypt header te decrypten (deze header bevat de masterkey). De user key wordt geconstrueerd aan de hand van het gebruikers wachtwoord wordt een key afgeleid.

Samengevat wordt de master key opgeslagen in de header van de versleutelde container en die wordt gedecrypt aan de hand van de user key die afgeleid wordt van een wachtwoord dat alleen de gebruiker van de container weet.

Encryptie werking

Wanneer een container gemount wordt gebeurt globaal het volgende [9]:

1. De header wordt in RAM gelezen.

2. TrueCrypt probeert de header te decrypten. Om dit te kunnen doen is de juiste combinatie van onder andere hash functies en encryptie functies[1]. Deze informatie is niet in de header opgenomen, zo is een container niet te identificeren. De juiste combinatie van parameters wordt on-te-fly geprobeerd.
3. Decryptie wordt als succesvol beschouwd wanneer de eerste 4 bytes van de gedecrypte data de ASCII string "TRUE"bevat, en de CRC-32 van de header klopt. Hierna wordt ervan uit gegaan dat het juiste wachtwoord (en overige parameters) gebruikt is en wordt alleen nog bepaald of de juiste versie van het programma gebruikt wordt.
4. Uit de gedecrypte header worden de Master keys en IV's[2] opgenomen en deze kan gebruikt worden om sectoren van de container te decrypten

10.1.2 Gebruiksgemak

TrueCrypt heeft geen integratie met Windows, het is een apart op te starten programma waarmee alles gedaan wordt. Het programma wijst zich vanzelf, maar heeft geen Windows look-and-feel. Het aanmaken van containers vereist een aparte denkslag, omdat eerst een file aangemaakt moet worden waarvan vervolgens een container gemaakt wordt. Dit is gelijk ook een van de nadelen van dit systeem (bestandsencryptie op basis van containers), want als het container bestand verwijderd wordt zijn ook alle daarin opgenomen bestanden verdwenen. Daarnaast brengt het container bestand wel de mogelijkheid het te verplaatsen naar een andere locatie.

Containers die aangemaakt worden kunnen vervolgens als schijf (al dan niet automatisch) gemount worden.

Installatie

De installatie van TrueCrypt is eenvoudig. Er zijn een zestal opties aanwezig, waaronder installatie directory en ïnstall for all users". Voor het testen van het product zijn alle opties aangezet en geïnstalleerd in c: \Program Files\TrueCrypt. Tijdens de installatie is te volgen welke stappen het systeem uitvoert en welke bestanden naar de schijf geschreven worden.

Gebruikersondersteuning

TrueCrypt heeft een uitgebreide gebruikersondersteuning in de vorm van:

- Handleiding
- Forum
- Website
- Helpfunctie
- FAQ

10.1.3 Recovery

Er is geen recovery procedure voorhanden. Extra gevoelig is dit systeem (zoals al eerder genoemd) voor het weggooien van het container bestand.

[1] Overige parameters zijn: Number of ciphers, Mode of operation, Block size, Key size.

[2] IV's (intitialization vector) zijn een (random) blok van bits die gecombineerd wordt met het eerste blok van de data wanneer voor elk bestand dezelfde sleutel gebruikt wordt.

10.1.4 Veiligheid

Naar de volgende aspecten is gekeken om te beoordelen hoe TrueCrypt omgaat met verschillende aspecten die de beveiliging zouden kunnen aantasten.

Swap file Een swapfile wordt onder Windows gebruikt voor data die niet meer in het geheugen past. Deze file bevindt zich op de harde schijf. Data die zich in het geheugen bevindt kan bij gebrek aan geheugenruimte naar de schijf (swap file) geschreven worden. In het geval van TrueCrypt betekent dit dat data die gebruikt wordt zich gedecrypt in het geheugen bevindt en wanneer de page file gebruikt wordt gedecrypt naar de harde schijf geschreven wordt.

Het schrijven van data naar swap files geldt niet voor wachtwoorden, sleutels en IV's.
De makers van TrueCrypt raden aan geen gebruik te maken van de swapfile wanneer met gevoelige informatie gewerkt wordt.

Data corruptie Verschillende oorzaken (bv. hardware fouten) kunnen ervoor zorgen dat de bestanden die geëncrypt zijn corrupt raken. Wanneer het geëncrypte bestand om een of andere reden verandert is decryptie niet meer mogelijk.

Meerdere gebruikers Wanneer meerdere gebruikers gebruik maken van een systeem en de TrueCrypt volumes worden gemount dan zijn deze ook zichtbaar voor de andere gebruikers van het systeem. Alleen wanneer het systeem opnieuw opgestart wordt worden de volumes ge- unmount. De verschillende containers kunnen in FAT of NTFS formaat gemaakt worden, maar het feit dat een container het NTFS formaat heeft, heeft geen invloed op de rechten voor de gebruiker, en iedereen die de bestanden in de container kan zien, kan er ook gebruik van maken.

Opslag sleutels en wachtwoorden TrueCrypt slaat geen wachtwoorden en sleutels op op de harde schijf. Al deze gegevens worden versleuteld opgeslagen en uiteindelijk afgeleid van een gebruikerswachtwoord die opgegeven wordt door de gebruiker.

10.1.5 Performance

Voor het gebruik van TrueCrypt moet een container gecreëerd worden. Voor de testen is een container gecreerd van 1,2 GB container. Dit nam 116 sec in beslag.

Bij TrueCrypt is de performance getest door elk van de vier standaard bestanden te kopiëren naar de versleutelde container en de tijdsduur van het kopiëren te meten. De resultaten van de test zijn in bijlage D terug te vinden. Voor de bestanden van 1 en 10 MB is de tijd van kopiëren dermate klein dat dit voor een gebruiker haast niet merkbaar is. Bij het kopiëren van grote bestanden naar de container duurt het opslaan echter wel langer dan het opslaan van dezelfde bestanden op een gewone partitie of schijf. Het performance verlies is pas goed merkbaar bij bestanden groter dan 1 GB.

10.1.6 Praktische aspecten

Er kan een hidden container gemaakt worden in een bestaande container. Op basis van het wachtwoord wordt bepaald of de hidden of de niet hidden container gemount wordt. Dit heeft als voordeel dat je het wachtwoord van de gewone container uit handen kan geven, maar dat de hidden container dan niet zichtbaar wordt.

Bij bestandsuitwisseling worden bestanden niet geëncrypt verstuurd omdat de container als gewone schijf benaderd wordt. De container zelf kan wel verstuurd worden. Daarbij is er een traveler optie

die bijvoorbeeld usb-stick-containers kan encrypten en automounten.

TrueCrypt biedt ook de optie om partities en schijven te encrypten. Dit werkt ook op de container manier en de nieuwe schijf moet gemount worden om te kunnen gebruiken en is voorzien van een wachtwoord. De geëncrypte schijf is in eerste instantie dus niet te zien onder Windows en ook niet onder Partition Magic.

Hibernation

Hibernation is een optie voor Windows om je systeem tijdelijk inactief te maken, waarna hij weer snel opstart in de situatie waarin hij voor het laatst actief was. Wanneer er hibernation wordt gebruikt, wordt net als bij de swap file de openstaande bestanden naar de harde schijf geschreven. TrueCrypt kan niet voorkomen dat geopende bestanden met vertrouwelijke informatie onversleuteld naar de schijf worden geschreven waneer het systeem in hibernation gaat.

Backup

Het backuppen van bestanden versleuteld met TrueCrypt is geen probleem, de bestanden worden ook na encryptie als bestanden gezien en worden ook zo door het besturingssysteem aangesproken.

10.2 AxCrypt

10.2.1 Werking

AxCrypt biedt alleen de functie om bestanden te encrypten en decrypten. Er kunnen geen hele partities of directories geëncrypt worden. Bij selecteren van een directory worden wel automatisch alle bestanden in die map geëncrypt met het zelfde wachtwoord of key.

10.2.2 Gebruikersgemak

AxCrypt kan niet opgestart worden als apart programma. In plaats daarvan wordt AxCrypt geïntegreerd in Windows explorer. In het menu, dat verschijnt door in Windows met de rechtermuisknop op een bestand te klikken, zijn de functies van AxCrypt te vinden. Hierdoor is het product erg goed bruikbaar voor één ieder die met Windows kan werken. Tevens vraagt het product een beperkt aantal handelingen voor het encrypten en decrypten van bestanden. Over het algemeen is het gebruikersgemak van AxCrypt zeer goed te noemen en heeft AxCrypt een zeer lage leercurve.

Installatie

De installatie van AxCrypt is erg simpel. Er wordt een taal gevraagd en een installatie directory. Tegen het einde van de installatie wil het installatieprogramma gegevens naar de ontwikkelaar zenden. Dit klinkt enigsinds verdacht, maar dit kan wel gewoon geweigerd worden. Het hele programma is maar 1.5 MB groot. Het programma dient geïnstalleerd te worden onder administrator rechten, gebruikers zelf kunnen het programma niet installeren.

Gebruikersondersteuning

Op de website van AxCrypt(http://axcrypt.sourceforge.net) is uitgebreide documentatie te vinden over de werking, installatie en mogelijkheden van AxCrypt. Support van de leverancier is niet mogelijk omdat het product door één persoon gemaakt is.

10.2.3 Recovery

AxCrypt biedt geen recovery mogelijkheden. In het geval een key of wachtwoord verloren gaat is alle data die met deze key of wachtwoord is geëncrypt ook verloren.

Als een bestand met encryptie corrupt raakt of veranderd wordt is het niet meer mogelijk dit bestand te decrypten. Ondanks dat dus een kleine stukje van het encrypte bestand corrupt kan zijn is alle origenele data verloren.

10.2.4 Veiligheid

Axcrypt gebruikt het AES algoritme met een 128 bits key voor het encrypten van bestanden. AES met een 128 bits sleutel kan op dit moment nog als veilig beschouwd worden. Essentieel voor de veiligheid is wel een goede random sleutel. AxCrypt biedt standaard een fuctie om zo'n sleutel te genereren.

Alle bestanden die geëncrypt worden met AxCrypt krijgen de extensie .axx . Hierdoor weet een eventueel kwaadwillig persoon die een bestand in handen krijgt met welk product het bestand geëncrypt is. Deze persoon kan nu bijvoorbeeld AxCrypt zelf gebruiken om het bestand proberen te decrypten. Daarnaast zouden ook de specificaties van het product gebruikt kunnen worden om het makelijker te maken het bestand te decrypten via een andere weg. Het is op zich geen reël gevaar, maar het is in ieder geval al een stuk dichterbij de data dan wanneer deze gegevens niet bekend zouden zijn.

Tijdelijke bestanden

Als een geëncrypt bestand geopend wordt dan wordt een tijdelijke gedecrypte kopie van het bestand gemaakt in de map

```
c:\Document and Settings\Administrator\Local Settings\Temp\axcrypt
```

Zodra het bestand wordt afgesloten wordt deze kopie geëncrypt en wordt het orginele bestand overschreven. Indien AxCrypt niet goed afgesloten wordt of een systeem crasht zou het mogelijk kunnen zijn dat deze tijdelijke bestanden blijven bestaan. Dit is tijdens het onderzoek niet bewezen maar is theoretisch wel mogelijk.

10.2.5 Performance

Bij AxCrypt is de performance getest door elk van de vier standaard bestanden te encrypten en decrypten en de tijdsduur van de encryptie te meten. De resultaten van de bestanden van 100 en 1000 MB zijn in bijlage D.2 terug te vinden. Voor de bestanden van 1 en 10 MB was de encryptie en decryptie tijd dermate klein dat dit voor een gebruiker haast niet merkbaar. In de praktijk wordt door gebruikers veelal gewerkt met bestanden tussen de 1 en 10 MB en heeft het performanceverlies niet echt invloed.

10.2.6 Praktische aspecten

Hibernation

AxCrypt ondersteund geen hibernation. Indien een geëncrypt bestand open staat en het systeem in hibernation mode gaat wordt data die in het geheugen staat onversleuteld op de harde schijf opgeslagen.

backup

Het maken van backups van bestanden die geëncrypt zijn met AxCrypt gaat altijd goed. geëncrypte bestanden zijn filesysteem onafhankelijk en kunnen dus opgeslagen worden op cd-rom, DVD of USB-stick

10.3 PGP Desktop

10.3.1 Werking

De werking van PGP Desktop berust op PGP. Bij PGP kan gebruik gemaakt worden van asymmetrisch encryptie wat werkt met een wachtwoord of asymmetrische encryptie in de vorm van publieke en privé sleutels.

10.3.2 Gebruikersgemak

PGP Desktop biedt twee mogelijkheden om het programma te gebruiken, geïntergreerd via Windows explorer of door het programma zelf te starten. De eerste mogelijkheid biedt vooral de basis functies zoals het en- en decrypten van bestanden. Het programma zelf is erg uitgebreid en wat moeilijker in gebruik. Vooral aspecten als het genereren van sleutels vergt eigenlijk een basiskennis van PGP.

Hoewel PGP Desktop in dit onderzoek bekeken wordt als bestandsencryptie product is het veel meer dan dat. Zo beschikt PGP Desktop ook over de mogelijkheden om:

- Virtual schijven aanmaken
- Hele harde schijf encrypten

Het maken van virtule schijven of het encrypten van de hele harde schijf werkt erg gemakkelijk onder PGP Desktop.

Installatie

De installatie van PGP Desktop is gemakkelijk, snel en eigenlijk vergelijkbaar met het installeren van elk ander programma.

10.3.3 Recovery

PGP Desktop biedt standaard geen recovery mogelijkheden. Bij het gebruik van sleutels zullen van privé sleutels zelf veilig backups gemaakt moeten worden.

10.3.4 Veiligheid

PGP Deskop biedt voor encryptie een hoeveelheid aan beschikbare algoritmen waaronder de huidige standaarden als AES en RSA. Bij PGP Desktop kan ook gekozen worden voor grotere sleutels dan vaak in andere programma's mogelijk is. Grotere sleutels gebruiken dan standaard lijkt soms overbodig maar biedt voor veiligheid op langere termijn wel betere bescherming.

Tijdelijke bestanden

Bij het encrypten van bestanden wordt er een kopie gemaakt. Het originele bestand blijft dus bestaan. Deze bestanden dienen zelf veilig verwijderd te worden. PGP Desktop biedt voor het veilig verwijderen wel een zogenaanmde "shred"functie.

10.3.5 Performance

Bij PGP Desktop is gekeken naar performance van bestandsencryptie en van schijfencryptie.

Schijfencryptie

Het initieel compleet encrypten van de harde schijf nam op het testsysteem(20 GB hd) 1 uur en 30 min in beslag. Het compleet decrypten nam 1 uur en 57 min in beslag. De duur van encryptie tijdens het werken in het besturingssysteem is niet te testen omdat het encryptie en decryptie proces op de achtergrond plaatsvind. In plaats daarvan is een read/ write performance test op de partitie gedaan, waarvan de resultaten in bijlage D.3 te vinden zijn. Zoals de tabel laat zien is er wel performance verlies te zien, met name in read acties is dit duidelijk.

Bestandsencryptie

Invloed van bestandsencryptie op performance is getest door elk van de vier standaard bestanden te encrypten/decrypten en de tijdsduur van de encryptie/decryptie te meten. De resultaten van de bestanden van 100 en 1000 MB zijn in bijlage D.4 terug te vinden. Voor de bestanden van 1 en 10 MB was de encryptie en decryptie tijd dermate klein dat dit voor een gebruiker haast niet merkbaar is. In de praktijk wordt door gebruikers veelal gewerkt met bestanden tussen de 1 en 10 MB en hebben gebruikers dus bijna geen last van het encrypten en decrypten van bestanden.

10.3.6 Praktische aspecten

backup

Bij het gebruik van de bestandsencryptie functie is het mogelijk bestanden geëncrypt te backuppen omdat de encryptie onafhankelijk is van het filesysteem. Bij alleen het gebruik van de schijfencryptie is dit niet het geval en zal dus nog apart bestandsencryptie gebruikt moeten worden.

10.4 EFS

EFS wordt standaard meegeleverd met Windows 2000 en XP Professional en werkt op bestanden en mappen, niet op partities en schijven. Door EFS toe te passen op mappen als "My Documents"worden de bestanden in die map automatisch ge-encyrpt en gedecrypt wanneer dit nodig is. Bestanden en mappen die voorzien zijn van encryptie worden gemerkt (naam veranderd van kleur), dit kan via mapopties veranderd worden.

10.4.1 Werking

Wanneer er voor het eerst een bestand geëncrypt wordt, wordt er een public en private key gegenereerd. Wanneer een bestand ge-encyrpt wordt genereerd EFS een willekeurig nummer die geassocieerd wordt met het bestand, het FEK (File Encryption Key)[15]. De FEK wordt gebruikt om de inhoud van het bestand te encrypten met het DESX algoritme. De FEK wordt met het bestand bewaard en geëncrypt met de EFS public key met behulp van het RSA-128 algoritme.

DESX is een symmetrisch algoritme die vaak als eigenschap hebben dat ze snel zijn en dus handig om grote hoeveelheden data te encrypten. Een symmetrisch algoritme maakt gebruik van één sleutel, dit is een zwak punt, want als eenmaal de sleutel bekend is kan je bij alle data. RSA is een asymmetrisch algoritme die als kenmerk hebben langzamer te zijn dan symmetrische algoritmen, maar er wordt gebruik gemaakt van 2 sleutels. De combinatie van de twee zorgt voor snelle encryptie van de data

en vervolgens wordt de symmetrische sleutel met een asymmetrische sleutel geencytp waardoor deze moeilijker te achterhalen wordt.

De combinatie van a- en symmetrische algoritmen maken het delen van bestanden moeilijk, omdat kennis van sleutels nodig is en dat is niet gewenst. Windows en EFS zorgen door het managen van public keys dat bestands uitwisseling wel mogelijk is en zo veel mogelijk transparant voor de gebruiker.

10.4.2 Gebruiksgemak

EFS is geïntegreerd in Windows en het gebruik ervan spreekt behoorlijk voor zich. Het enige nadeel is dat het handmatig moet gebeuren en dat de optie voor het encrypten redelijk verscholen is. Eenmaal geëncrypt werkt het allemaal transparant, dit is vooral waar voor mappen.

Het encrypten gebeurt door een finkje aan te zetten, en decrypten door hetzelfde finkje weer uit te zetten.

Installatie

EFS is onderdeel van het Windows besturingssysteem en hoeft niet apart geïnstalleerd of geactiveerd te worden.

Gebruikersondersteuning

EFS heeft een goede gebruikersondersteuning in de vorm van:

- Microsoft Technet Website
- Helpfunctie
- FAQ

Daarnaast is er op het Internet ook veel informatie te vinden over EFS.

10.4.3 Recovery

Er is een recovery mechaniek aanwezig om bestanden als dan niet in active directory te recoveren. Er worden gebruikers (hoeft niet perse de administrator te zijn) aangemaakt die als recovery agent kunnen dienen. Wanneer een private key verloren is gegaan kan de te decrypten informatie naar de recovery agent gestuurd worden om te recoveren. Dit recoveren werkt alleen voor systemen die dezelfde recovery policy hebben als de recovery agent.

10.4.4 Veiligheid

EFS is voor dagelijks gebruik een goed alternatief, maar toch zitten er een aantal zwakheden en onvolkomen heden aan:

Gebruikerswachtwoord

De sleutels gebruikt voor EFS worden geëncrypt met de gebruikers wachtwoord als input. Wanneer de wachtwoord policy van de organisatie het afdwingt van tijd tot tijd de wachtwoorden te veranderen zijn de bestanden geëncrypt met EFS niet langer te decrypten. Microsoft onderkent dit probleem en in een volgend service pack zou dit probleem opgelost moeten zijn[11].

Encryptie algoritme

EFS gebruikt DESX wat niet het sterkst beschikbare symmetrische algoritme is dat beschikbaar is.

Tijdelijke bestanden

EFS bestanden die in het geheugen geladen worden hebben de kans naar de harde schijf geschreven te worden wanneer bijvoorbeeld de swap-file gebruikt wordt. EFS voorkomt niet dat deze data onversleuteld naar de schijf wordt geschreven.

Opslag van keys en wachtwoorden

EFS slaat de publieke en privé sleutel van de gebruiker apart van het FEK op. Beide sleutels worden wel opgeslagen op het systeem en iemand met voldoende rechten kan ook gebruik maken van deze sleutel.

10.4.5 Performance

Het verschil in performance tussen het schrijven naar een EFS directory en een niet EFS directory is te vinden in bijlage D.4. Zoals uit de tabel blijkt is de performance van bestanden van 100 MB al merkbaar, maar waarschijnlijk niet storend. Storend wordt het wel wanneer bestanden groter dan 1 GB naar EFS geschreven worden. Dit is ook goed merkbaar wanneer het systeem "Not Respondingäangeeft als het grote bestanden moet wegschrijven naar EFS.

10.4.6 Praktische aspecten

Het encrypten van bestanden en mappen heeft bij het verplaatsen van deze bestanden en mappen (en bestanden in de mappen) binnen Windows geen effect op de encryptie ervan, ze blijven geëncrypt.

Het is mogelijk om de gebruikte keys en certificaten te exporteren en op een andere plek op te slaan wanneer ze verloren gaan op de machine waarop ze gebruikt worden. Bij EFS is standaard een recovery mechanisme aanwezig, namelijk de administrator is de recovery agent die altijd in staat is om de geëncrypte data te decrypten.

Encryptie algoritme

Het gebruikte encryptie algoritme van EFS staat in de registry aangegeven onder

`HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS`

Door deze entry aan te passen kan een tweede/ ander algoritme gebruikt worden[10].

Backup

Bij het backuppen van bestanden geëncrypt met EFS verliezen deze hun encryptie, omdat het medium waarnaar ze gebackupped worden (waarschijnlijk) geen EFS ondersteunt.

10.5 CompuSec

10.5.1 Werking

CompuSec werkt op de achtergrond in het besturingssysteem en onderschept alle lees en schrijf acties en past zo on-the-fly encryptie en decryptie toe.

10.5.2 Gebruikersgemak

CompuSec werkt na de installatie compleet transparant voor de gebruiker. Er moet alleen voor het laden van het besturingssysteem een username en wachtwoord worden ingevoerd. Deze username en wachtwoord zijn onafhankelijk van de username en het wachtwoord van het besturingssysteem. CompuSec biedt wel de mogelijkheid om Windows accounts te koppelen aan een CompuSec account. Hierdoor ontstaat een zogenoemde single sign-on situatie en hoeven alleen nog de CompuSec username en wachtwoord ingevoerd te worden.

Installatie

CompuSec is redelijk simpel te installeren. Tijdens de installatie kan gekozen worden uit een paar opties als: single sign-on en een optie om ook losse bestandsencryptie mogelijk te maken.

10.5.3 Recovery

Er wordt in CompuSec twee manieren recovery mogelijkheden geboden—:

Resetcode Indien een wachtwoord van een willekeurig CompuSec account vergeten wordt is er de mogelijk om het wachtwoord te resetten met behulp van de wachtwoord resetcode.

Recovery hulpprogramma Indien door een fout het besturingssysteem niet geladen kan worden is het niet mogelijk om de harde schijf te decrypten. Alle data zou nu verloren zijn. Met behulp van een bootable floppy met het recovery hulpprogramma kan de harde schijf ge-decrypt worden buiten het besturingssysteem om. Hiervoor is wel een username en wachtwoord nodig.

10.5.4 Veiligheid

Bij het installeren van CompuSec wordt ook een backup bestand aangemaakt. Dit backup bestand dient goed bewaard te worden want dit bestand is vereist om CompuSec te deïnstalleren. Tijdens het openen van dit bestand in Notepad was een username en het wachtwoord van de resetcode gewoon in plaintext terug te vinden.

Tijdelijke bestanden

Het probleem van tijdelijke bestanden dat speelt bij bestandsencrypie is hier niet van toepassing. Het grote voordeel van de manier waarop CompuSec werkt is dat werkelijke alle data geëncrypt wordt.

Schijven omwisselen

Bij deze test is een met CompuSec geëncrypte harde schijf in een andere testsysteem geplaatst als tweede harde schijf. Bij het opstarten van het besturingssysteem(Windows XP Professional) wordt de schijf zelf wel herkent maar geeft Windows aan dat de schijf ongeformateerd is. Er is geen data terug te vinden.

10.5.5 Performance

Nadat CompuSec geïnstaleerd is moet initieel de hele hardeschijf geëncrypt worden. Het compleet encrypten van de harde schijf nam op het testsysteem(20 GB hd) ongeveer 75 min in beslag. CompuSec geeft in de handleiding een tijd aan van twee en een half uur voor een 40 GB harde schijf.

De duur van encryptie tijdens het werken op het systeem is niet te testen, omdat het encryptie en decryptie proces op de achtergrond plaatsvindt. In plaats daarvan is een read/ write performance test op de partitie gedaan, waarvan de resultaten in bijlage D.5 te vinden zijn.

10.5.6 Praktische aspecten

Extra's

Compusec wordt, indien bij de installatie ervoor gekozen is, geleverd met twee extra programma's; Een apart programma voor het encrypten van removable media en een apart programma genaamd Datacrypt voor het encrypten van losse bestanden. Dit werkt met public en private keys.

Hibernation

CompuSec biedt ook ondersteuning voor hibernation. Als een systeem in hibernation mode gaat wordt de data die vanuit het RAM naar de harde schijf net als andere data gewoon geëncrypt.

Partitionering

Bij het gebruik van CompuSec blijft partitionering gewoon mogelijk.

10.6 DriveCrypt Plus Pack(DCPP)

10.6.1 Werking

DCPP werkt als volgt[**?**]; Wanneer data op de schijf aangesproken wordt, wordt het door DCPP gedecrypt voordat het in het geheugen geladen wordt. Andersom gebeurd ongeveer hetzelfde, wanneer data klaar is om terug geschreven te worden naar de schijf wordt het eerst door DCPP geëncrypt. Beide processen gebeuren transparant voor de gebruiker en applicaties.

Data wordt wanneer het in het geheugen geladen wordt sector voor sector gedecrypt, en er is dus nooit sprake van een volledige decryptie van een bestand, alleen de benodigde sectoren worden gedecrypt.

10.6.2 Gebruiksgemak

Het programma werkt gemakkelijk, maar het wijst zich niet helemaal vanzelf. Bij de makers was dit waarschijnlijk ook duidelijk en er is een quick-user-guide meegeleverd die alles prima stap voor stap beschrijft.

Installatie

De installatie van DCPP is gemakkelijk en snel. Er wordt om wat opties gevraagd, zoals preboot authentication.

Gebruikersondersteuning

DCPP heeft een goede gebruikersondersteuning in de vorm van:

- Website
- Knowledge Base

- FAQ
- Support

Daarnaast is er op het Internet ook veel informatie te vinden over EFS.

10.6.3 Recovery

MBR

Wanneer het preboot authenticatie systeem geinstalleerd wordt is ondersteuning van VESA compatibiliteit vereist. Wanneer je niet zeker bent van de ondersteuning kan je gewoon de verschillende opties proberen. Mocht het niet werken dan kan je de MBR van het systeem herstellen met fdisk/mbr.

ER disk

Er kan een ER (Emergency Repair) disk gemaakt worden. Deze disk kan gebruikt worden bij harddisk problemen. Er kan op 3 verschillende manieren een ER disk gemaakt worden.

Floppy Booten en schijf decrypten vanaf floppy

Image file Voor het maken van een ER schijf op cd-rom

Old style Bootauth (het pre boot authenticatie systeem) wordt op floppy geïnstalleerd.

10.6.4 Veiligheid

Wanneer een partitie of schijf geëncrypt met DCPP onder een ander besturingssysteem wordt bekeken is geen data of meta data zichtbaar. Er is geen informatie te krijgen over bestanden en folders.

10.6.5 Performance

De duur van encryptie is in het geval van DCPP niet te testen, omdat het encryptie en decryptie proces op de achtergrond plaatsvindt. Om toch de invloed van encryptie aan te kunnen tonen is een read/ write performance test op de partitie gedaan, waarvan de resultaten in bijlage D.6 te vinden zijn. Zoals de tabel laat zien is er wel performance verlies te zien, met name in read acties is dit duidelijk.

10.6.6 Praktische aspecten

Keystores

DCPP maakt gebruik van zogenaamde keystores. Elke gebruiker heeft voor het encrypten en gebruik maken van geëncrypte schijven een keystore nodig waarin de verschillende sleutels opgeslagen worden. De keystore maakt ook het importeren van sleutels van andere gebruikers mogelijk, zodat verschillende mensen een geëncrypte partitie voor elkaar toegankelijk kunnen maken.

Pre-boot authenticatie en Single-Sign-On

DCPP kan ook preboot authenticatie verzorgen, welke er voor zorgt dat de schijven vooraf geunlocked moeten worden en booting mogelijk wordt. In combinatie met pre-boot authenticatie (welke op basis van de keystore wachtwoorden is) kan ook Single-Sign-On gebruikt worden waarna de gebruiker direct ingelogd wordt onder zijn gebruikers account. Het nadeel aan het gebruik van

Single sign-on is dat wanneer verbinding gemaakt wordt vanaf een willekeurige pc met remote desktop er automatisch ingelogd wordt zonder het opgeven van een gebruikersnaam of wachtwoord.

Bij preboot authentication kunnen ook verschillende opties meegegeven worden, zo kan bijvoorbeeld een nep foutmelding gegeven worden waarna wel ingelogd kan worden.

Encryptie

DCPP is een schijfencryptie tool die partities en hele schijven (op basis van partities) kan encrypten. Het encryptie proces kan gebeuren terwijl gebruik gemaakt wordt van het systeem.

Wanneer een gebruiker een schijf geëncrypt heeft en een ander gebruiker logt in dan is deze schijf/ partitie niet bruikbaar. De onbruikbaarheid van de schijf wordt gegeven als een melding dat de partitie nog niet geformatteerd is. Wanneer de rechten van de gebruiker het mogelijk maken deze partitie te formateren gaat de data van de schijf (die in feite een geëncrypte schijf is) verloren.

Hibernation

DCPP ondersteunt geen hibernation.

10.7 Checklists

Als samenvatting van het onderzoek naar de encryptieproducten zijn twee checklisten gecreëerd. Deze checklisten, die te vinden zijn in bijlage B en C, kunnen gebruikt worden als leidraad bij het kiezen voor encryptie. De eerste checklist dient als leidraad bij het kiezen van een vorm van encryptie. De tweede checklist dient als leidraad voor het kiezen van een product die encryptie moet gaan verzorgen.

Hoofdstuk 11

Conclusie en aanbevelingen

In de vorige hoofdstukken zijn verschillende onderwerpen met betrekking tot bestands- en schijfencryptie aan bod gekomen. Hieruit blijkt dat er niet één oplossing altijd de goede is. De juiste oplossing hangt af van de situatie en de mate van vertrouwelijkheid van de informatie.

De producten die onderzocht zijn hebben allemaal sterke en minder sterke punten en elk product kan in bepaalde situaties meer voordelen bieden dan andere pakketten.
Zo is bestandsencryptie erg simpel in gebruik en zeer geschikt voor het encrypten van een gering aantal gebruikers en in een organisatie waar gebruikers de verantwoordelijkheid nemen voor het zelf encrypten van data.
Schijfencryptie biedt twee grote voordelen ten opzichte van de andere twee manieren. Ten eerste is het hele proces van encryptie en decryptie transparant voor de gebruiker en ten tweede wordt echt alle data geëncrypt.

11.1 Aanbevelingen

Een onderdeel van het project was te kijken naar welke vorm van bestands- en/ of disk encryptie het best te gebruiken zou zijn voor SURFnet kantoor. Om hier een aanbeveling over te kunnen doen is gekeken naar de organisatie zelf en naar de theoretische achtergrond van de verschillende manieren om data te beveiligen.

De uiteindelijke aanbeveling voor SURFnet bv is om schijfencryptie te gebruiken in combinatie met bestandsencryptie.

Gezien de mate van vertrouwelijke informatie zullen bestands- en filesysteem encryptie alleen niet voldoende beveiliging bieden. Dit komt voornamelijk doordat er van medewerkers verwacht wordt zelf bestanden te versleutelen of op de juiste plaats op te slaan. De meest gebruikers binnen SURFnet zijn technisch genoeg om dit te doen. In het begin zal dit goed gaan, maar de ervaring leert dat de discipline vaak afzwakt. Ook het veelvuldig gebruik van laptops maakt schijfencryptie het beste alternatief, omdat indien deze gestolen worden een dief niets kan omdat alle data geëncrypt is.

Mocht er besloten worden inderdaad schijfencryptie te implementeren zal wel rekening gehouden moeten worden met de situatie binnen SURFnet. Een goed voorbeeld hiervan is de installatie en herstel DVD van het VIA project. Wanneer de hele harde schijf versleuteld wordt, zijn in sommige gevallen de partities niet meer te onderscheiden, behalve wanneer toestemming is om de schijf te

ontsleutelen. Dit betekent dat de installatie en herstel DVD niet in staat is de C: partitie opnieuw te formatteren. CompuSec biedt wel hele schijf encryptie waarbij de partitie tabel nog toegankelijk is. Een ander voorbeeld is dat enkele medewerkers binnen SURFnet op de vrije partities een ander besturingssysteem installeren waardoor zich mogelijk op deze partities ook vertrouwelijke informatie bevindt.

Bestanden die via email of het netwerk de werkplek verlaten verliezen hun versleuteling. Daarom is schijfencryptie met aanvulling van bestandsencryptie de beste oplossing. Vanuit de ervaring opgedaan tijdens het onderzoek wordt aangeraden CompuSec te gebruiken als schijfencryptie product en daarbij gebruik te maken van AxCrypt als bestandsencryptie product.

Er is op dit moment ook veel ontwikkeling gaande op het gebied van ingebouwde encryptie in harde schijven. Wellicht is dit een oplossing die nog veiliger is en betere performance biedt. Hier is echter geen concreet onderzoek naar gedaan.

11.2 Key-management

Zoals in paragraaf 3.3 aangegeven is, is er een zeker vorm van key-management nodig om sleutels te kunnen beheren. Er is een keuze mogelijk tussen het in bewaring geven van een key door een TTP (escrow) of het zelf in bewaring nemen van de verschillende sleutels.

SURFnet is een CA (Certification Authority) en heeft een eigen PKI omgeving. Daarmee beschikt SURFnet zelf over voldoende expertise om key-management op te zetten. Om deze reden is self-escrowing voor SURFnet de manier om keys te beheren.

Bibliografie

[1] Nedsecure; http://www.nedsecure.nl/index.html?products/Encryptie/encr.html NSCcenter

[2] Kamp Poal-henning; *GBDE-GEOM Based Disk Encryption*; http://phk.freebsd.dk/pubs/bsdcon-03.gbde.paper.pdf

[3] Koops, Bert-Jaap;*Encryptie: sleutel tot informatiemaatschappij of tot criminaliteit*; http://rechten.uvt.nl/koops/NGI-VISI.HTM

[4] Kuunders, Leon; *Reguleren sterke cryptografie? Niet doen!*; http://leon.kuunders.info/regulerencrypto.html#1

[5] Branders, Ben; *Encryptie*; http://branders.name/schrijfsels/encryptie/

[6] Koops, Bert-Jaap;*Notaris, ik houd mijn sleutels liever zelf*; http://rechten.uvt.nl/koops/KNB-W8FF.HTM

[7] Koops, Bert-Jaap de Jong, Huub; *De risico's van data recovery voor overheid en gebruikers*; http://rechten.uvt.nl/koops/PUB/ttp-risk.htm

[8] Wright Charles P. , Dave Jay, Zadok Erez; *Cryptographic File Systems Performance: What You Don't Know Can Hurt You*; http://www.filesystems.org/docs/nc-perf/index.html

[9] TrueCrypt; *TrueCrypt User Guide*; www.truecrypt.org

[10] O'Reilly; *Windows Encrypted File System: Replace DESX algorithm with 3DES*; http://hacks.oreilly.com/pub/h/2134

[11] Microsoft TechNet; *You cannot access EFS files after you change the user password to a new password on a Windows XP Service Pack 2-based computer*; http://support.microsoft.com/?kbid=890951&SD=tech

[12] Fresh Diagnose; http://www.freshdiagnose.com/

[13] Kallender Paul; *Seagate Preps Hard-disk Encryption Technology. Your laptop's data would be automatically encrypted as it was written to the disk.*; http://www.pcworld.com/resource/article/0,aid,121522,pg,1,RSS,RSS,00.asp

[14] Charles Kaufman en Radia Perlman(2002) *Network Security*, Prentice Hall PTR

[15] Russinovich Mark; *Inside Encrypting File System*; http://www.windowsitpro.com/Article/ArticleID/5387/5387.html

[16] *Overview to Security and Anonymity*; http://computersandjunk.com/Guides-and-Tutorials/Computer-Security/Security-and-Encryption-FAQ-2.html

[17] SURFnet; *SURFkit*; http://www.surfkit.nl

Bijlage A

Checklist

Prooduct	#1	#2	#3	#4	#5	#6
Encryptievorm						
Bestandsencryptie						
Filesyteemencryptie						
Schijfencryptie						
Besturingssysteem ondersteuning						
Windows XP						
Linux						
Mac OS X						
Authenticatie methoden						
Password						
Keys						
Token						
Single sign-on met Windows						
Pre-boot						
Recovery mogelijkheden						
Password en key recovery						
Bestanden recovery						
Overige aspecten						
Gratis						
Open source						
Hibernate ondersteuning						
Werkt ook met RAID						
PDA ondersteuning						
Meerdere gebruikers						
Partitionering						
Verwijderbare media						
Gebruikersgemak						
Handleiding						
Volwassenheid						
Documentatie						
Leverancier support						

Tabel A.1: Checklist

Bijlage B

Checklist vorm

Eisen	**Bestandsencryptie**	**Filesysteemencryptie**	**Schijfencryptie**
Performanceverlies	Minimaal	Minimaal	Minimaal
Volledige data encryptie	Nee	Nee	Ja
Schijf partitionering mogelijk	Ja	Ja	Nee
Transparantie voor gebruiker	Nee	Gemiddeld	Ja
Encryptie bij bestandsuitwisseling	Ja	Nee	Nee
Gebruikersprofielen	Lokaal Server	Lokaal	Lokaal
Bakcup	.	.	.
Schaalbaarheid	Gemiddeld	Gemiddeld	Gemiddeld

Tabel B.1: Checklist vorm encryptie

Bijlage C

Checklist product

\+ Goed

+/- Gemiddeld

\- Minder

X Ja/ Aanwezig

	DCPP	**CompuSec**	**EFS**	**AxCrypt**	**PGP desktop**	**TrueCrypt**
Encryptievorm						
Bestandsencryptie				X	X	X
Filesyteemencryptie			X			
Schijfencryptie	X	X			X	
Besturingssysteem ondersteuning						
Windows XP	X	X	X	X	X	X
Linux		X				
Mac OS X				X		
Authenticatie methoden						
Password	X	X		X	X	X
Keys	X		X	X	X	X
Token	X					
Single sign-on met Windows	X	X	X			
Pre-boot	X	X			X	
Recovery mogelijkheden						
Password en key recovery	X	X	X			
Bestanden recovery	X	X	X			
Overige aspecten						
Gratis		X	X	X		X
Open source				X		X
Hibernate ondersteuning		X				
Werkt ook met RAID			X	X	X	X
PDA ondersteuning						
Meerdere gebruikers	X	X	X		X	X
Partitionering	X	X	X			X
Verwijderbare media	X	X	X	X	X	X
Gebruikersgemak	+/-	+	+	+	+/-	+/-
Handleiding	+	+	+	+	+/-	+
Volwassenheid	X	X	X	X	X	X
Documentatie	+/-	+	+	+	+/-	+
Leverancier support	X	X	X		X	

Tabel C.1: Checklist

Bijlage D

Performance onderzoeks resultaten

D.1 TrueCrypt

Bestandsgrootte	**Schrijven naar partitie zonder encryptie**	**Schrijven naar container**
1 MB	$<$ 1 sec	$<$ 1 sec
10 MB	1 sec	$<$ 1 sec
100 MB	8 sec	11 sec
1000 MB	1 min 22 sec	1 min 48 sec

Tabel D.1: TrueCrypt performance

D.2 AxCrypt

Bestandsgrootte	**Encryptie/ decryptie**	**Tijd**
100 MB	encryptie	1 min 2 sec
100 MB	encryptie	1 min 3 sec
100 MB	encryptie	1 min 6 sec
Gemiddeld	**encryptie**	**1 min 4 sec**
100 MB	decryptie	38 sec
100 MB	decryptie	36 sec
100 MB	decryptie	43 sec
Gemiddeld	**decryptie**	**39 sec**
1000 MB	encryptie	12 min
1000 MB	encryptie	12 min 17 sec
1000 MB	encryptie	12 min 10 sec
Gemiddeld	**encryptie**	**12 min 9 sec**
1000 MB	decryptie	7 min 40 sec
1000 MB	decryptie	7 min 43 sec
1000 MB	decryptie	7 min 45 sec
Gemiddeld	**decryptie**	**7 min 43 sec**

Tabel D.2: AxCrypt performance

D.3 PGP Desktop

Partitie groote	**Read/ Write (MB/s)**	**Partitie met encryptie**	**Partitie zonder encryptie**
20 GB	Write	5,64	5,41
20 GB	Write	5,74	5,30
20 GB	Write	5,76	5,84
Gemiddeld	**Write**	**5,71**	**5,52**
20 GB	Read	7,33	10,05
20 GB	Read	7,27	10,66
20 GB	Read	7,24	10,69
Gemiddeld	**Read**	**7,28**	**10,47**

Tabel D.3: Read/ Write performance PGP Desktop

Bestandsgrootte	**Encryptie/ decryptie**	**Tijd**
100 MB	sym. encryptie	1 min 35 sec
100 MB	sym. encryptie	1 min 40 sec
100 MB	sym. encryptie	1 min 32 sec
Gemiddeld	**sym. encryptie**	**1 min 36 sec**
100 MB	sym. decryptie	1 min 30 sec
100 MB	sym. decryptie	1 min 25 sec
100 MB	sym. decryptie	1 min 29 sec
Gemiddeld	**sym. decryptie**	**1min 28 sec**
100 MB	asym. encryptie	45 sec
100 MB	asym. encryptie	47 sec
100 MB	asym. encryptie	43 sec
Gemiddeld	**asym. encryptie**	**45 sec**
100 MB	asym. decryptie	30 sec
100 MB	asym. decryptie	26 sec
100 MB	asym. decryptie	27 sec
Gemiddeld	**asym. decryptie**	**28 sec**
1000 MB	sym. encryptie	7 min 15 sec
1000 MB	sym. encryptie	7 min 40 sec
1000 MB	sym. encryptie	7 min 18 sec
Gemiddeld	**sym. encryptie**	**7 min 24 sec**
1000 MB	sym. decryptie	6 min 5 sec
1000 MB	sym. decryptie	6 min 20 sec
1000 MB	sym. decryptie	6 min 11 sec
Gemiddeld	**sym. decryptie**	**6 min 12 sec**
1000 MB	asym. encryptie	8 min 6 sec
1000 MB	asym. encryptie	8 min 15 sec
1000 MB	asym. encryptie	7 min 59 sec
Gemiddeld	**asym. encryptie**	**8 min 7 sec**
1000 MB	asym. decryptie	5 min 55 sec
1000 MB	asym. decryptie	5 min 10 sec
1000 MB	asym. decryptie	5 min 33 sec
Gemiddeld	**asym. decryptie**	**5 min 43 sec**

Tabel D.4: Bestandsencryptie PGP Desktop

D.4 EFS

Bestandsgrootte	**Schrijven naar paritie met encryptie**	**Schrijven naar partitie zonder encryptie**
1 MB	1 sec	$<$ 1 sec
10 MB	2 sec	$<$ 1 sec
100 MB	42 sec	1 sec
1000 MB	10 min 2 sec	1 sec

Tabel D.5: EFS performance

D.5 CompuSec

Partitie grootte	**Read/ Write (MB/s)**	**Partitie met encryptie**	**Partitie zonder encryptie**
1,84 GB	Write	4,83	5,42
1,84 GB	Write	4,83	4,9
1,84 GB	Write	5,13	4,88
Gemiddeld	**Write**	**4,93**	**5,06**
1,84 GB	Read	8,79	10,87
1,84 GB	Read	9.07	10,46
1,84 GB	Read	9,16	9,16
Gemiddeld	**Read**	**9,00**	**10,16**

Tabel D.6: Read/ Write performance CompuSec

D.6 DCPP

Partitie groote	**Read/ Write (MB/s)**	**Partitie met encryptie**	**Partitie zonder encryptie**
1,84 GB	Write	4,36	5,42
1,84 GB	Write	4,22	4,9
1,84 GB	Write	4,58	4,88
Gemiddeld	**Write**	**4,38**	**5,06**
1,84 GB	Read	6,66	10,87
1,84 GB	Read	6,62	10,46
1,84 GB	Read	6,88	9,16
Gemiddeld	**Read**	**6,72**	**10,2**

Tabel D.7: Read/ Write performance DCPP