Sleutelen aan versleutelen

Organisatorische aspecten rond cryptografie

M.W. Baurichter

De noodzaak om informatie beveiligd op te slaan of beveiligd te verzenden neemt sterk toe nu netwerken steeds 'opener' worden. Thans zijn vele encryptieapplicaties op de markt beschikbaar die ieder specifieke functionele en technische voor- en nadelen bezitten. In dit artikel wordt uiteengezet welke voordelen en risico's samenhangen met het gebruik van dit soort applicaties in het algemeen en welke kritieke succesfactoren hieruit volgen. Vervolgens worden enkele willekeurig geselecteerde applicaties beschouwd en ten slotte worden enkele (audit)aspecten opgesomd die door de IT-auditor gedurende een onderzoek ten minste dienen te worden beoordeeld.

Inleiding

Virtuele netwerken, Internet-koppelingen, Remote Access Servers, websites met koppelingen aan mirrored databases en overige informatietechnische toepassingen zijn al niet meer weg te denken uit de infrastructuur van menige organisatie. Het beoogde resultaat voor de eindgebruiker is transparante toegang tot beveiligde data. Om dit resultaat te bereiken worden organisaties aangespoord tot het nemen van allerhande beveiligingsmaatregelen om deze netwerken, en de data die zich op deze netwerken bevinden, te beschermen tegen en af te schermen van ongeautoriseerde gebruikers. Echter, organisaties lopen met het nemen van beveiligingsmaatregelen veelal achter op deze nieuwe toepassingen. Het is niet ongebruikelijk voor een organisatie op verschillende afdelingen parallel ICT-projecten te ontwikkelen die ieder een specifieke impact hebben op de informatiebeveiliging, met wellicht lokale optimalisatie maar organisatiebreed vaak slechts suboptimalisatie tot gevolg.

Een andere vorm van 'beschikbaarheid van data' is de snelle toename van laptops en notebooks. Delen van databases worden opgeslagen op de harddisk en zodoende buiten de fysieke beveiliging van een organisatie gebracht. Met de diefstal van een laptop gaat er veelal méér verloren dan de kosten van de aanschaf van de hardware. Actuele kopieën van bedrijfsgegevens zijn immers in handen gekomen van ongeautoriseerde personen en kunnen ten laste van de rechtmatige eigenaar te gelde worden gemaakt, bijvoorbeeld door verkoop aan een concurrent, door 'terugverkoop' aan de eigenaar, of door verkoop aan de pers. De opkomst van de Personal Digital Assistants (PalmPilots en dergelijke) zal de tendens van het exporteren van bedrijfsgegevens alleen maar versterken en evenzeer de reeds genoemde risico's die hiermee samenhangen.

Tevens kan hier nog worden stilgestaan bij de veiligheid van het communiceren via e-mail. Iedere dag worden vele miljoenen e-mails verzonden. De ervaring leert dat vertrouwelijke en onvertrouwelijke informatie in de meeste gevallen zonder enige vorm van beveiliging (plaintext) via het Internet wordt verzonden. Onderschepte berichten en berichten abusievelijk verzonden aan de verkeerde personen zijn dan gewoon leesbaar (zie ook kadertekst 2).

Bovenstaande toepassingen maken enigszins duidelijk dat het beschermen van de gegevens zelf, op het meest inhoudelijke niveau, steeds belangrijker is geworden. Cryptografie, het versleutelen van gegevens, doet hier haar intrede.

In dit artikel wordt beschreven met welke organisatorische en technische aspecten rekening dient te worden gehouden bij het toepassen van cryptografie binnen een organisatie. Het artikel behandelt primair de versleuteling van gegevens en niet de cryptografische technieken zoals deze aanwezig zijn in smartcards, firewalls, routers, etc. Eerst wordt beschreven wat cryptografie (technisch) inhoudt en welke soorten cryptografische toepassingen beschikbaar zijn. Vervolgens worden risico's van het gebruik van cryptografie opgesomd, alsmede de kritieke succesfactoren voor een succesvolle implementatie en gebruik van cryptografie. Enkele encryptieapplicaties worden kort besproken en het artikel wordt besloten met een beschrijving van de aspecten die voor een succesvolle implementatie noodzakelijk zijn en waarmee tijdens een audit rekening dient te worden gehouden.

Cryptografie: methoden en technieken

Een artikel over cryptografie zou niet compleet zijn zonder de basics van cryptografie aan te halen.

Cryptografie betekent de leer van het versleutelen. Deze wel erg brede afbakening wordt in dit artikel verkleind tot het versleutelen van (elektronische) gegevens. Dit proces staat globaal weergegeven in figuur 1.

Hierbij kan worden opgemerkt dat plaintext de leesbare tekst betreft en ciphertekst de versleutelde, onleesbare tekst. Het versleutelen (encrypten) vindt plaats met behulp van een algoritme en een sleutel, het 'ontsleutelen' (decrypten) vindt eveneens plaats met behulp van het algoritme en een sleutel. In principe kan cryptografie plaatsvinden volgens twee methoden[1], te weten:

* symmetric key encryption;
* asymmetric key encryption.

1) Een derde soort cryptografisch algoritme bestaat erin dat, gebaseerd op een asymmetrisch algoritme, alleen digitale handtekeningen kunnen worden geplaatst, bijvoorbeeld het Digital Signature Algorithm.

Symmetric key encryption (ook wel conventional encryption of secret key encryption genaamd) maakt gebruik van een algoritme dat met een sleutel de tekst kan encrypten en met behulp van dezelfde sleutel de tekst tevens kan decrypten. Zoals in figuur 2 wordt getoond, is voor beide transformaties dus slechts één sleutel nodig.

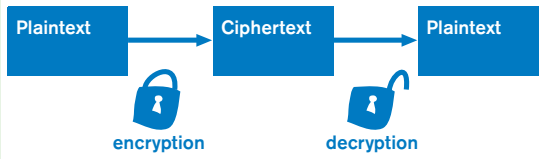
Dit soort versleuteling is geschikt voor het snel versleutelen van data die niet verzonden hoeven te worden maar op een lokale harddisk of server worden opgeslagen. Het verzenden van versleutelde data (volgens symmetric key encryption) kán natuurlijk wel, maar dan dient de geheime sleutel ook te worden verzonden, wil de ontvanger de tekst kunnen decrypten om de data te kunnen lezen. Wanneer deze sleutel in handen van de verkeerde persoon valt, is de ketting van geheimhouding doorbroken en kan er niet meer van worden uitgegaan dat teksten vertrouwelijk zijn. Tevens zou het gebruik van symmetric encryption voor vertrouwelijke communicatie vereisen dat voor iedere persoon met wie gecommuniceerd wordt, een aparte sleutel dient te worden aangemaakt en (veilig) bewaard; een chaotische situatie. Algoritmen die gebaseerd zijn op symmetric key encryption zijn onder andere DES, IDEA en RC5. In kadertekst 3 worden twee algoritmen uitgebreider besproken.

Een oplossing voor de sleutelproblematiek is de asymmetric key encryption (ook wel public key encryption genaamd). Hierbij wordt namelijk gebruikgemaakt van een paar (twee) sleutels die één op één bij elkaar horen. Zo is het bij asymmetric key encryption mogelijk met één van deze sleutels de tekst te encrypten (public key) en met de andere sleutel deze ciphertext te decrypten (private key of secret key). Deze vorm van encryptie is weergegeven in figuur 3.

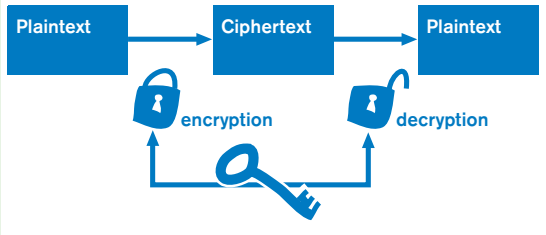
De public key kan aan iedereen worden verstrekt, dit terwijl de secret key goed 'geheim' dient te worden gehouden voor anderen. Voor het encrypten en verzenden van een bericht aan persoon A wordt de (openbare) public key van A gebruikt. Alleen persoon A kan vervolgens met zijn secret key de tekst decrypten.

Een andere veelgebruikte toepassing die met behulp van asymmetric key encryption kan worden toegepast, is de digitale handtekening. Een bericht kan worden ondertekend door gebruik te maken van de secret key en de hashwaarde[2] van het bericht, de ontvanger kan de handtekening verifiëren door gebruik te maken van de bijbehorende public key. Door zogenaamde timestamps toe te passen is de handtekening uniek en tijdgebonden.

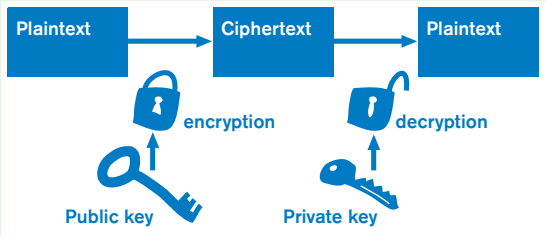
Uit het bovenstaande blijkt duidelijk dat het beheren van de secret key essentieel is. Het algoritme is namelijk openbaar maar de sleutel is persoonlijk en die bepaalt *hoe* een tekst wordt versleuteld. Het gebruik van een secret key is veelal beveiligd door middel van een wachtwoord. In de toekomst kan het wachtwoord wellicht worden vervangen door een persoonlijk biometrisch 'wachtwoord' (zie het artikel van Van der Vlugt in deze Compact).



Figuur 1. Encryptieproces.



Figuur 2. Symmetric key encryption.



Figuur 3. Asymmetric key encryption.

Kenmerken en toepassingen encryptie

Encryptie kan overal waar (elektronische) informatie zich bevindt, worden toegepast. En encryptie wordt ook al toegepast zonder dat wij ons dit nu direct realiseren. Zo zijn bijvoorbeeld encryptietechnieken geïmplementeerd in de geldautomaten, de Chipknip en de Chipper, Internet-browsers en mobiele telefoons alsmede in decoders voor bijvoorbeeld kabelleverancier Canal+. Ook maken diverse besturingssystemen gebruik van encryptie om wachtwoorden beveiligd op te slaan.

Een globale onderverdeling van encryptie zou kunnen zijn:
* encryptie van gegevens tijdens transport;
* encryptie van gegevens in opslag.

Encryptie van gegevens tijdens transport

Het gebruik van encryptie bij datacommunicatie richt zich op een veilige informatieoverdracht van zender naar ontvanger via een 'kwetsbaar' communicatiekanaal. Dit kanaal kan onder andere een intern netwerk zijn, een huurlijn of het Internet. Juist het beveiligen van de communicatie over het kanaal is bij dit soort encryptie essentieel. Doordat relatief weinig gegevens worden verzonden, en dus worden versleuteld, kan worden gekozen voor zowel asymmetrische als symmetrische versleuteling. Asymmetrische encryptie heeft vanwege de betere sleuteldistributiemogelijkheden de voorkeur bij encryptie van gegevens tijdens transport.
Enkele toepassingen voor encryptie van gegevens onderweg:

Cisco routers
Cisco routers (en equivalenten) met IOS versie vanaf 11.2 beschikken over de mogelijkheid om de te routeren data op IP-niveau tussen 'trusted' routers te versleutelen.

2) Over een variabele invoering (bijvoorbeeld een document) wordt een waarde berekend (hashwaarde of checksum). Hiermee wordt een zogenaamde fingerprint van het document gegenereerd die veelal korter is dan het document zelf. Een wijziging van het document kan met behulp van de hashwaarde worden achterhaald.

Deze techniek staat ook wel bekend als Cisco Encryption Technology (CET).

PPTP (Point to Point Tunneling Protocol)
Een (softwarematig) protocol dat ontworpen is om tussen twee of meer servers een versleutelde tunnel over al dan niet verschillende netwerkprotocollen (TCP/IP, Netbeui, etc.) te creëren.

PGP (Pretty Good Privacy)
Encryptieapplicatie die (voornamelijk) ontworpen is om e-mail te verzenden nadat deze is versleuteld. Hierbij vindt het versleutelen van gegevens dus bij en door de eindgebruikers plaats, evenals het ontsleutelen.

Encryptie van gegevens in opslag

Een aparte tak van sport binnen cryptografie zijn de applicaties die encryptiefaciliteiten voor opslag bieden. Deze encryptie omvat vaak veel gegevens (delen van de harddisk) die dus snel dienen te worden verwerkt; hiertoe wordt veelal symmetrische encryptie toegepast. Symmetrische encryptie is namelijk naar rato duizend maal (!) sneller dan asymmetrische encryptie.
Enkele aspecten die op encryptiefaciliteiten voor opslag van toepassing zijn:

On-the-fly encryption
Bestanden bevinden zich altijd in versleutelde fase en worden, wanneer ze worden aangeroepen door een applicatie of een gebruiker, automatisch gedecrypt. Wanneer deze bestanden (tussentijds) worden opgeslagen, gebeurt dat in geëncrypte vorm. Bij uitval van een besturingssysteem is het originele bestand altijd versleuteld opgeslagen.

Partiële en volledige encryptie
Bij partiële encryptie worden in de encryptieapplicatie partities, folders en bestanden vooraf aangemerkt als te versleutelen; overige delen van de harddisk worden derhalve cleartext opgeslagen. Bij volledige encryptie wordt de gehele inhoud van de harddisk geëncrypt opgeslagen, vaak inclusief Master Boot Records en dergelijke technische informatie. Het opstarten van de encryptieapplicatie vindt plaats vanaf de bootsector; de benodigde bestanden die versleuteld zijn opgeslagen, worden *on-the-fly* gedecrypt.

Bootprotectie
Wanneer een encryptieapplicatie beschikt over bootprotectie kunnen gebruikers niet de encryptie omzeilen door bijvoorbeeld met een Linux bootflop de harde schijf te benaderen. Het (d)e(n)crypten vindt plaats nadat een gebruiker zich door middel van een script, dat zich op de bootsector bevindt, heeft geauthenticeerd. Gedurende de periode dat deze gebruiker is ingelogd, worden bestanden automatisch ver- en ontsleuteld.

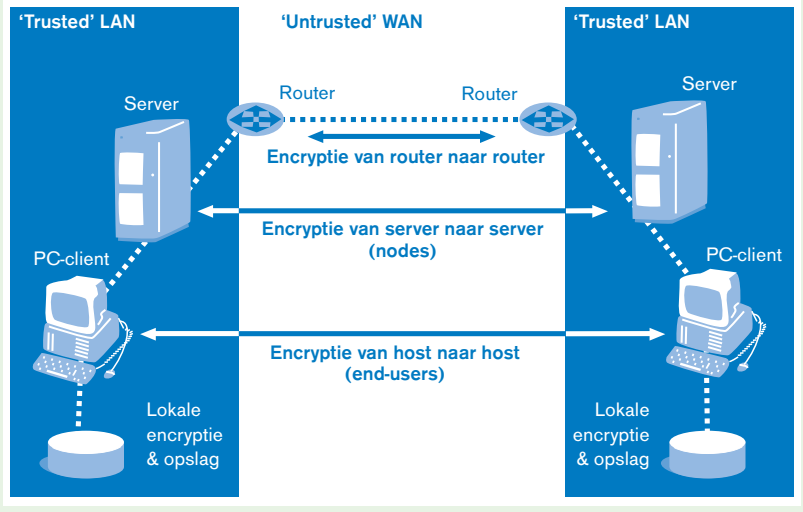
Secure-wipe of secure-delete
Een 'achterdeur' bij encryptie is het originele plaintextbestand. Wat gebeurt er met dit bestand nadat dit is versleuteld of wordt verwijderd door de gebruiker? Veelal staan deze bestanden ongealloceerd op de harddisk en kunnen zij relatief makkelijk worden teruggehaald. Derhalve is de functionaliteit secure-wipe/secure-delete ontworpen. Een bestand dat de gebruiker wil verwijderen, wordt in dit geval met binaire nullen overschreven en vervolgens verwijderd.

Hulpmiddelen voor encryptie van opgeslagen gegevens worden verderop in dit artikel besproken.

Wanneer we bovenstaande verdeling van encryptie schematisch weergeven, krijgen we het beeld zoals dat wordt gepresenteerd in figuur 4. Hierbij dient te worden opgemerkt dat varianten van deze soorten ook mogelijk zijn. Zo kunnen PC-clients ook deel uitmaken van een Virtual Private Network (VPN) door een versleutelde tunnel met een server op te zetten; dan ontstaat een variant met encryptie van client naar server (hetgeen overigens al met een SSL-sessie wordt gerealiseerd).

In figuur 4 komt duidelijk naar voren dat het soort encryptie dat wordt geïmplementeerd consequenties heeft voor het traject dat wordt versleuteld. Zo wordt bij encryptie van server naar server een langer traject versleuteld dan bij versleuteling tussen routers. In beide gevallen wordt echter een stuk traject onversleuteld afgelegd, namelijk over het 'vertrouwde' LAN. Cleartextcommunicatie op dit laatste traject kan nog gewoon worden onderschept en afgeluisterd.

Figuur 4.
Verdeling van soorten encryptie.



Doelen van encryptie

Met behulp van cryptografie kunnen de volgende doelen worden gerealiseerd:
* het verhinderen van modificatie van informatie; waarborgen van de integriteit (integriteit);
* het bewaren van de vertrouwelijkheid van elektronisch opgeslagen en verzonden informatie (vertrouwelijkheid en beschikbaarheid);
* het verhinderen van succesvol namaken van elektronische transacties (reconciliatie);
* het vaststellen van de identiteit van afzender(s) (authenticiteit en non-repudiation).

Het verhinderen van modificatie van informatie; waarborgen van de integriteit
Dit wil zeggen het versleutelen van informatie opdat niemand wijzigingen kan aanbrengen, ofwel om de integriteit van informatie te waarborgen. Dit wil niet zeggen dat versleutelde bestanden niet kunnen worden gewijzigd, dit kan wel maar heeft tot gevolg dat de bestanden verminkt en/of onleesbaar worden. De inhoud van de tekst kan niet *ongemerkt* worden gewijzigd.

Een voorbeeld van een toepassing die het bovenstaande realiseert, is de functionaliteit van het Secure Socket Layer (SSL)-protocol in browsers en/of andere applicaties.

Het bewaren van de vertrouwelijkheid van elektronisch opgeslagen en verzonden informatie
Het klassieke doel van cryptografie is het waarborgen dat een tekst geheim blijft en alleen leesbaar is door diegene die wordt vertrouwd. Dit streven kan worden bereikt zowel met symmetrische als met asymmetrische versleuteling. De beschikbaarheid van data wordt hierbij in principe tegengegaan, in feite het tegenovergestelde doel van wat normaliter met beschikbaarheid wordt bedoeld.

Toepassingen die het bovenstaande aspect kunnen waarborgen, zijn bijvoorbeeld encryptie van e-mail (bijvoorbeeld PGP) en het SSL-protocol in browsers.

Het verhinderen van succesvol namaken van elektronische transacties
Met cryptografie kan ook worden bereikt dat een elektronische transactie niet meermalen wordt verzonden (reconciliatie). Deze techniek wordt toegepast op het gebied van transacties bij electronic commerce, zoals het SET-protocol.

Zoals reeds aangehaald is een toepassing hiervan het SET-protocol. Soortgelijke aspecten worden nagestreefd in toepassingen als SWIFT en bij applicaties voor elektronisch bankieren.

Het vaststellen van de identiteit van afzender(s)
Met behulp van (asymmetrische) encryptie is het mogelijk de authenticiteit van een zender vast te stellen door een digitale handtekening te plaatsen met behulp van de private key. Voorwaarde is wel dat er in het verleden overeenstemming is bereikt tussen de zender en de ontvanger over de validiteit van de publieke sleutel. Hierin kan een Trusted Third Party een belangrijke rol spelen. Tevens kan non-repudiation worden bereikt: een gebruiker kan niet ontkennen een bericht te hebben verzonden doordat gebruik is gemaakt van een unieke handtekening.

Enige toepassingen zijn wederom SWIFT en PGP.

Bovenstaande toelichting maakt duidelijk dat er vele doelen van cryptografische toepassingen zijn. Door slim gebruik te maken van cryptografie kunnen in één slag de kwaliteitsbegrippen vertrouwelijkheid, (met opzet on)beschikbaarheid, integriteit, authenticatie en non-repudiation worden geregeld.

Risico's

Het versleutelen van gegevens heeft natuurlijk niet alleen maar voordelen maar kent ook zijn risico's. Wil een organisatie een weloverwogen beslissing kunnen nemen over het introduceren van cryptografie, dan dient eerst duidelijk te worden welke risico's hiermee samenhangen en welke maatregelen dienen te worden genomen om de risico's te voorkomen dan wel deze tot een acceptabel niveau terug te brengen. Een gestructureerde aanpak is derhalve een vereiste teneinde alle risico's in kaart te brengen om ze vervolgens te kunnen adresseren.

Hieronder zijn enkele generieke bedreigingen en risico's opgesomd die kunnen optreden bij het gebruik van cryptografie. De risico's kunnen liggen op de volgende vlakken: risico's met betrekking tot de cryptografische toepassing (applicatie) zelf, risico's met betrekking tot het beheer van de applicatie (en alles wat hiermee samenhangt) en risico's tijdens het gebruik van de cryptografische toepassing. Per bedreigingen en risico's zijn enkele maatregelen vermeld.

Bedreigingen en risico's cryptografische applicatie

1. Het in de applicatie gehanteerde algoritme is zwak.
Het risico dat hier kan optreden, is dat een zogenaamde brute-force attack[3] een serieuze kans van slagen heeft. Stel bij het selecteren van de applicatie daarom de eis dat een algoritme is gehanteerd dat 'volwassen' is en als een sterk algoritme wordt beschouwd.

2. In de applicatie treedt een storing op waardoor reeds versleutelde gegevens niet meer zijn te decrypten.
Het verlies van gegevens is hierbij het evidente risico dat kan optreden. Een maatregel hiertegen is het inrichten van adequate back-upprocedures voor gebruikers en de gebruikers attenderen op het belang van naleven van de back-upprocedures.

3. Het genereren van de sleutel vindt plaats door middel van enkele bekende en (achteraf) te herleiden factoren.
Het wordt hierdoor mogelijk de (private) keys met redelijk gemak te reproduceren. Derhalve dient vooraf, gedurende de selectie van de applicatie, te worden vastgesteld dat de sleutel afhankelijk is van vele verschillende factoren die niet herleidbaar en/of reproduceerbaar zijn.

4. Andere software (antivirussoftware, defragmentatiesoftware) werkt niet goed samen met de versleutelingssoftware.
Een risico dat hierdoor kan optreden, is dat de gegevens worden verminkt en derhalve niet meer zijn op te vragen. Vooraf dient dus goed te worden vastgesteld of de versleutelingssoftware niet conflicteert met overige toepassingen.

5. Het besturingssysteem van de PC crasht waardoor de applicatie de gegevens niet versleuteld opslaat.
Vertrouwelijke gegevens staan onbeveiligd (niet versleuteld) op de harddisk van de PC. Stel derhalve bij het selecteren van de applicatie vast of de functionaliteit van on-the-fly encryption onder alle omstandigheden ge-

3) Een aanval op een versleutelde tekst (teneinde de tekst te kunnen lezen) door systematisch alle mogelijke sleutels te hanteren tot een leesbaar eindresultaat wordt gevonden.

handhaafd blijft. Reguliere identificatie- en authenticatiemaatregelen op het niveau van het besturingssysteem dienen aanwezig te zijn.

6. Een gebruiker versleutelt een bestand en verwijdert het originele (plaintext-)bestand. De verwijdering is echter niet definitief [4].
De verwijderde gegevens (al dan niet vertrouwelijk) staan onbeveiligd op de harddisk en de vertrouwelijkheid is niet meer gewaarborgd. Daarom dient bij het selecteren van de applicatie te worden vastgesteld of de 'secure-wipe'-functionaliteit aanwezig is.

4) Risico alleen bij partiële encryptie.

7. De temp-directory, waar het besturingssysteem alle 'geopende' bestanden in opslaat, wordt bij afsluiting van de PC niet automatisch en niet definitief geleegd[4].
Het risico van deze bedreiging is eveneens dat vertrouwelijke gegevens onbeveiligd op de harddisk blijven staan. Stel derhalve bij het selecteren van de applicatie vast of de temp-directory automatisch en definitief wordt geleegd bij het afsluiten van het besturingssysteem of selecteer een applicatie die volledige encryptie van de harddisk biedt.

8. Het besturingssysteem heeft voor het gebruik van virtual memory een swap-file (of pages) op de harddisk staan, die door iemand met fysieke toegang kan worden gekopieerd[4].
Vertrouwelijke gegevens staan onbeveiligd op de harddisk. Stel bij het selecteren van de applicatie vast of de swap-file automatisch en definitief wordt verwijderd bij het afsluiten van het besturingssysteem en stel vast dat een pagefile in gebruik niet kan worden gekopieerd.

Samenvatting risico's en maatregelen applicatie
Uit voorgaande risico's komt duidelijk naar voren dat de risico's die (inherent) aanwezig zijn bij de applicatie eigenlijk alleen kunnen worden voorkomen door het selecteren van een goed product. Deze toch wel eenvoudige conclusie komt voort uit het feit dat de meeste applicaties standaardpakketten zijn waarin geen modificaties kunnen worden aangebracht. Het vooraf onderkennen van de voor- en nadelen van een applicatie is dus noodzakelijk.

Beheerders moeten voorafgaand aan de implementatie van een cryptografische toepassing procedurele en operationele maatregelen hebben getroffen.

Bedreigingen en risico's beheer van cryptografische applicatie

1. De beheerafdeling heeft geen adequate koppeling gelegd tussen de gebruiker en zijn/haar persoonlijke sleutel.
Het risico dat hierbij kan optreden, is dat gegevens van een gebruiker bij verlies van het wachtwoord niet meer kunnen worden gedecrypt. Derhalve dient een beheerprocedure te worden ontwikkeld die een adequate koppeling tussen iedere gebruiker en diens persoonlijke sleutel afdwingt.

2. De beheerafdeling heeft bewust geen back-ups van de sleuteldatabase gemaakt (beveiliging), zodat bij een crash van de harddisk de database niet meer voorhanden is.
De gegevens van een gebruiker kunnen bij verlies van het wachtwoord niet meer worden gedecrypt. Derhalve dient een beheerprocedure te worden ontwikkeld zodat zeer frequent (na iedere mutatie) een back-up van de sleuteldatabase wordt gemaakt. Deze back-up dient beveiligd te worden opgeslagen en alleen geautoriseerde beheerders dienen toegang tot deze database te bezitten.

3. De beheerafdeling heeft de sleuteldatabase niet adequaat beschermd tegen ongeautoriseerde toegang.
De integriteit van de sleutels is niet meer gewaarborgd en daarmee impliciet de vertrouwelijkheid, beschikbaarheid en integriteit van de versleutelde gegevens. De database met unieke sleutels dient op een fysiek onbereikbare stand-alone PC, ten minste beschermd door een wachtwoord, te worden opgeslagen.

4. Kennis voor het effectief verhelpen van storingen als gevolg van de cryptografische software is niet voorhanden.
Een risico hiervan is dat de beschikbaarheid van versleutelde gegevens in gevaar kan komen als een storing niet adequaat wordt verholpen. De beheerafdeling dient derhalve te beschikken over een knowledgedatabase van reeds opgetreden incidenten, de beheerders dienen specifieke cursussen te volgen van de leverancier en een supportovereenkomst (SLA) dient met de leverancier te worden afgesloten voor het verlenen van ondersteuning.

Samenvatting risico's en maatregelen beheer
Het implementeren van cryptografische toepassingen in een organisatie betekent dat zwaar moet worden gesteund op de beheerorganisatie. Beheerders moeten voorafgaand aan de implementatie al procedurele en operationele maatregelen hebben getroffen en daar consequent de hand aan houden.

Bedreigingen en risico's gebruik van cryptografische toepassingen

1. Er is gekozen voor een zeer lange sleutellengte zodat een zware versleuteling plaatsvindt.
Hierdoor treedt het risico op dat de performance van applicaties zijn weerslag heeft op de productiviteit van de gebruiker. Met andere woorden, het feit dat de processor zware berekeningen uitvoert om gegevens te versleutelen, gaat ten koste van de performance van de operationele processen. Met het oog hierop dient een sleutellengte (en algoritme) te worden geselecteerd waarbij performance en beveiliging adequaat zijn.

2. De organisatie die het gebruik van de applicatie verplicht stelt, is aanwezig in landen waar al of niet stringente restricties met betrekking tot encryptie door de overheid worden opgelegd.
Een volledige uitrol van encryptieapplicaties wordt hierdoor niet (legaal) mogelijk. Derhalve dient een toepas-

sing te worden geselecteerd die in elk land waar de organisatie aanwezig is, is toegestaan.

3. De gebruikers maken back-ups van de versleutelde gegevens die via het back-upprogramma cleartext op de server worden opgeslagen.
De vertrouwelijkheid van gegevens komt in gevaar doordat niet overal encryptie wordt toegepast op gegevens waarvoor dat nodig is. Selecteer hiervoor een applicatie die versleutelde back-ups kan uitvoeren en implementeer een pakket dat versleuteling op fileservers kan handhaven.

4. Geïnstalleerde trojans (BackOrifice, Netbus) worden door de antivirussoftware niet gedetecteerd.
Het risico dat hierbij kan optreden, is dat gegevens van de harde schijf via het netwerk worden opgevraagd (en ontsleuteld) en vervolgens worden geëxporteerd, waardoor de vertrouwelijkheid en de beschikbaarheid van de gegevens worden aangetast. Om dit te voorkomen dienen antivirussoftware en actuele updates op de clients te worden geïnstalleerd. Tevens dient de firewall te zijn beschermd tegen externe, niet vertrouwde netwerken.

5. De gebruiker schrijft het wachtwoord van de (private/secret) key ergens op.
Ongeautoriseerde gebruikers kunnen daardoor in de positie komen om versleutelde gegevens te decrypten. Attendeer de gebruikers op de noodzaak van het waarborgen van de vertrouwelijkheid van het wachtwoord.

6. De gebruiker verifieert niet of de public key van de afzender daadwerkelijk hoort bij de afzender. Met andere woorden, de gebruiker stelt de authenticiteit van een derde niet succesvol vast[5].
Een gebruiker communiceert abusievelijk met iemand die zich uitgeeft voor de bedoelde wederpartij. Attendeer de gebruikers op de noodzaak van het verifiëren van de publieke sleutel op juistheid en richt een Public Key Infrastructure (PKI) in.

7. De gebruiker maakt gedurende een langere periode gebruik van dezelfde sleutel.
Doordat een gebruiker gedurende langere tijd dezelfde sleutel hanteert krijgt een eventuele aanvaller de kans om voldoende ciphertextvoorbeelden te verzamelen en aldus de kans de sleutel te herleiden. Hiertoe dienen de gebruikers te worden geattendeerd op de noodzaak van het frequent genereren van een nieuwe sleutel. Dit dient eveneens procedureel te worden afgedwongen.

Samenvatting risico's en maatregelen gebruik
Het gebruik van encryptieapplicaties is pas dan succesvol wanneer reguliere beheertechnische processen (backups uitvoeren, doorvoeren antivirussoftware, etc.) adequaat plaatsvinden. Het is niet een kwestie van een keuze maar van een combinatie.

Kritieke succesfactoren

Uit het voorgaande blijkt dat enerzijds vele risico's kunnen optreden bij het gebruik en beheer van encryptieapplicaties (alsmede dat er de intrinsieke risico's van een specifieke encryptieapplicatie zijn), maar dat dergelijke applicaties anderzijds vele voordelen bieden. Het is van belang om hiermee vooraf bij selectie, implementatie en inrichting van de beheerorganisatie rekening te houden, zodat de risico's kunnen worden geminimaliseerd en de voordelen kunnen worden gemaximaliseerd. Dit vindt zijn neerslag in de kritieke succesfactoren.

1. Selecteer een applicatie die beschikt over een sterk en volwassen (bewezen) cryptografisch algoritme.
Men kan er pas zeker van zijn dat een algoritme sterk is, wanneer dit is bewezen. In de praktijk kost dit bewijzen erg veel tijd. Het is derhalve van belang dat een algoritme reeds enige tijd bestaat en dus volwassen is en enige bekendheid heeft verkregen, zodat men de tijd heeft gehad om het algoritme te bestuderen en te beoordelen. Algoritmen die nieuw zijn – of erger: die niet openbaar worden gemaakt – hebben deze beoordeling (nog) niet gehad en dienen dus bij voorbaat als onbetrouwbaar te worden beschouwd. Bruce Schneier, een expert op het gebied van cryptografie, is zelfs nog stelliger: 'Many published algorithms are insecure and almost all unpublished algorithms are insecure'.

2. Hanteer een sleutellengte waarbij optimalisatie van veilige versleuteling en minimaal verlies van performance worden bereikt.
In de regel geldt dat het kraken van een versleuteld bericht door middel van een brute-force attack bij een langere sleutellengte meer tijd kost dan bij een kortere sleutellengte[6]. Men zou dus geneigd zijn een zo lang mogelijke sleutellengte te selecteren. Echter, in die gevallen waarbij het proces van versleutelen merkbaar performanceverlies oplevert, dient overwogen te worden een kortere sleutel te selecteren of de rekenkracht van het systeem uit te breiden. Eveneens kan voor een sleutellengte worden gekozen die lang genoeg vertragend werkt: zo hoeft een elektronische transactie die slechts een paar minuten geheim dient te zijn, niet zo sterk te zijn dat zij weerstand kan bieden tegen een brute-force attack die enkele maanden in beslag neemt.

3. Selecteer een applicatie die volledige encryptie in plaats van partiële encryptie biedt.
Partiële encryptie heeft als voordeel dat (systeem)bestanden die niet versleuteld zijn, sneller worden opgevraagd; dit komt de performance ten goede. Echter, tijdelijke bestanden in de temp-folder, slecht verwijderde bestanden en in verkeerde folders geplaatste bestanden (in folders die niet worden versleuteld) zijn bij diefstal van een laptop gewoon opvraagbaar en leesbaar.

4. Zorg ervoor dat de beheerorganisatie beschikt over voldoende kennis en kunde met betrekking tot de encryptieapplicatie en mogelijke problemen.
Een encryptiepakket is niet een product dat kan worden geïnstalleerd en op zichzelf staat. Gebruikers vergeten na hun vakantie wachtwoorden en harddisks krijgen corrupte sectors waardoor bestanden niet meer zijn te openen. De beheerafdeling dient hier vooraf rekening mee te houden om adequaat problemen te kunnen oplossen. De praktijk leert dat organisaties hier veelal te licht over denken en het niet zo nauw nemen met rigoureuze beheermaatregelen; voor een gebruiker is het formatteren van de harde schijf echter géén oplossing.

5) Risico alleen bij encryptie voor communicatiepakketten (PGP).
6) Hierbij dient wel te worden opgemerkt dat de sleutellengten van symmetrische en asymmetrische algoritmen niet zonder meer vergelijkbaar zijn. Zo is een symmetrische sleutellengte van 128 bits ongeveer even kwetsbaar voor een succesvolle brute-force attack als een asymmetrische sleutellengte van 2304 bits.

5. Zorg ervoor dat de beheerorganisatie sleutelbeheer (vooraf) adequaat heeft ingericht.
Het is reeds meermalen gezegd: het succes van een cryptografische toepassing staat of valt met de wijze waarop sleutelbeheer is ingericht. Sleutels zijn te gemakkelijk beschikbaar of sleutels zijn helemaal niet beschikbaar; twee uitersten die met adequaat sleutelbeheer dienen te worden voorkomen. Het lijkt zo makkelijk te realiseren maar helaas wijst de dagelijkse praktijk anders uit.

Het succes van een cryptografische toepassing staat of valt met de wijze waarop sleutelbeheer is ingericht.

6. Attendeer de gebruikers vooraf op de risico's van het gebruik van encryptie en controleer periodiek op naleving van procedures.
Het gebruik van encryptie heeft pas zin wanneer gebruikers zich realiseren wat er precies plaatsvindt en wat het uiteindelijke doel is. Organisaties verzuimen vaak de belangrijkste partij voor te lichten, namelijk diegenen die er dagelijks mee moeten werken. Neem hen dan eens kwalijk dat ze er (zo) ook naar gaan handelen, en overgaan tot plaintext back-ups, wachtwoorden op post-it plakkers, etc.

7. Zorg ervoor dat 'overige' beveiligingsmaatregelen adequaat zijn ingericht.
Het gebruik van een encryptie is geen vervanging, maar een toevoeging op de veelal reeds ingevoerde beveiligingsmaatregelen. Trojans, virussen en keybordrecorders zijn potentiële bedreigingen voor data. Zijn deze maatregelen niet adequaat ingericht, dan zal encryptie geen wezenlijke verbetering bieden op het gebied van beveiliging. De reeds eerder geciteerde Bruce Schneier spreekt ons wederom met zijn wijsheid toe: 'It can be impossible to build a secure application on top of an insecure computing platform'.

De implementatie van cryptografie

Organisaties die besluiten om encryptiepakketten voor PC's, of ruimer cryptografische technieken, te gaan gebruiken en direct overgaan tot het selecteren van een applicatie en vervolgens tot implementatie van deze cryptografische toepassing, worden vroeg of laat geconfronteerd met de gevolgen hiervan zoals die in dit artikel reeds zijn aangehaald. Het is daarom van belang dat een organisatie, voorafgaand aan de daadwerkelijke selectie en implementatie, een gestructureerd proces doorloopt. Dit proces (A framework for using cryptography) is door het European Security Forum ([ESF97]) beschreven en wordt hieronder sterk verkort weergegeven.

Dit proces bestaat uit drie fasen die evaluatief en continu worden doorlopen. Dit betekent dat de stappen parallel kunnen worden doorlopen en dat het bijstellen naar aanleiding van de bevindingen (door optredende veranderingen in de organisatie) non-stop zal blijven plaatsvinden. De onderkende fasen zijn:

1. inventarisatie;
2. ontwikkelen van een beleid;
3. opstellen van normen.

1. Inventarisatie

In deze fase wordt in kaart gebracht welke cryptografische toepassingen reeds aanwezig zijn binnen een organisatie en wat de specifieke eigenschappen hiervan zijn (algoritmen, sleutellengte, etc.). Deze inventarisatie is van belang omdat de te selecteren applicaties mogelijk kunnen worden beïnvloed door de reeds aanwezige cryptografische toepassingen. Tevens wordt geïnventariseerd welke procedures op het gebied van cryptografie reeds operationeel zijn en welke (beheerders)rollen en verantwoordelijkheden zijn vastgesteld, denk hierbij bijvoorbeeld ook aan SLA's voor ondersteuning door leveranciers. Ten slotte dient te worden geïnventariseerd of de organisatie reeds een beleid heeft voor het gebruik van cryptografie en welke (operationele) voorschriften voor eindgebruikers hieruit zijn afgeleid.

De deliverables uit deze fase zijn dus:
* een overzicht van gehanteerde cryptografische toepassingen;
* een overzicht van gehanteerde algoritmen en sleutellengten;
* een overzicht van aanwezige beheerprocedures met betrekking tot cryptografie;
* een overzicht van beleidsuitgangspunten van de organisatie betreffende cryptografie;
* een overzicht van aanwezige en vereiste (beheerders)rollen en verantwoordelijkheden betreffende cryptografische toepassingen.

In principe wordt deze inventarisatiefase binnen een organisatie maar één keer uitgevoerd. Het is vervolgens wel van belang de opgeleverde deliverables van deze fase in de toekomst bij te houden en eventuele nieuwe ontwikkelingen te verwerken.

2. Ontwikkelen van een beleid

Om binnen een organisatie eenduidig, gestructureerd en dus gecontroleerd gebruik te gaan maken van cryptografie is top-downsturing een vereiste. Derhalve dient een beleid te worden opgesteld waarin wordt uiteengezet op welke gegevens en waar cryptografie zal worden toegepast. Tevens wordt in het beleid vastgelegd welke randvoorwaarden gelden voor het gebruik van cryptografie (soort algoritmen en minimale en maximale sleutellengten), alsmede de te vervullen taken betreffende het beheer van cryptografie.

Het beleid dient, gebaseerd op het resultaat van voorgaande fase, te worden opgesteld en zal voor een langere periode (vijf jaar) als leidraad dienen voor nieuwe ontwikkelingen.

De deliverable van deze fase is een beleidsdocument met hierin richtlijnen betreffende:
* de filosofie over het gebruik van cryptografie;
* een classificatie van te versleutelen gegevens;
* rollen en verantwoordelijkheden van beheerders;

* te hanteren cryptografische algoritmen en sleutellengten;
* in te richten beheerprocedures.

3. Opstellen van normen

Het voorgaande dient te worden vertaald in operationele normen waaraan de te selecteren cryptografische toepassingen dienen te voldoen. Deze normen kunnen direct worden toegepast in projecten waarin (zijdelings) cryptografische toepassingen worden ingezet. Op het gebied van techniek, gebruik, beheer en organisatie worden normen opgesteld. In specifieke gevallen dienen additionele normen te worden geformuleerd, omdat deze niet voorhanden zijn. Deze normen moeten echter wel uit het beleidsdocument worden geëxtraheerd.

Wanneer het beleidsdocument verandert, dienen de normen overeenkomstig te worden aangepast. Idealiter wordt getoetst in hoeverre de reeds uitgerolde projecten nog voldoen aan het vernieuwde beleid en de nieuwe normen.

De deliverables van deze fase:
* technische normen (waaronder de benoeming van het algoritme en de sleutellengte);
* normen die aanwijzen aan welke onderdelen van een organisatie cryptografie is toegestaan of voor welke dit verplicht is;
* normen die als randvoorwaarden fungeren voor het sleutelbeheer en het algemene beheer;
* normen die indicatief zijn voor de verantwoordelijkheden en taken die dienen te worden toegewezen.

Deze fasen hebben tot doel om binnen een organisatie top-downsturing te geven aan het gebruik van cryptografie. Wanneer deze fasen zijn doorlopen, kan een afdeling bovengenoemde stukken hanteren voor het selecteren en implementeren van een cryptografische toepassing.

Encryptieapplicaties

In deze paragraaf passeren enkele (willekeurig gekozen) encryptieapplicaties de revue. Aangezien het beoordelen van deze applicaties beperkt is gebleven tot het bestuderen van voorhanden zijnd marketingmateriaal en tot het nalezen van enkele artikelen, wordt ten aanzien van de geprezen eigenschappen een slag om de arm gehouden.

Windows NT Encryption File System

In Windows NT 2000, de opvolger van de huidige NT versie 4.0, is één van de nieuwe toepassingen het Encryption File System (EFS). Deze toepassing kan niet als een pur sang applicatie worden beschouwd aangezien zij geïntegreerd is in het besturingssysteem. Echter, gezien de toenemende inzet van Windows NT kan redelijkerwijs worden aangenomen dat geïntegreerde onderdelen, zoals het EFS, ook veelvuldig zullen worden gebruikt.

Het reguliere bestandssysteem van Windows NT (NTFS) biedt van zichzelf de mogelijkheid om bestanden te beveiligen en toegang te verlenen aan specifieke groepen en/of gebruikers. Echter, met programma's zoals NTFS-DOS en NTFS-bootflop voor Linux kan de beveiliging van NTFS onbelemmerd worden omzeild (mits fysieke toegang tot het systeem wordt verkregen). Reden voor Microsoft om de opvolger van Windows NT te voorzien van een geïntegreerde encryptiefaciliteit in het bestandssysteem (en daarmee weer in het besturingssysteem van Windows NT).

Vanuit de reeds bekende Explorer kunnen folders en bestanden door gebruikers worden aangemerkt als te encrypten; het betreft hier dus partiële encryptie. EFS doorloopt dan het volgende proces.

Door EFS wordt een unieke sleutel gegenereerd waarmee het bestand wordt versleuteld; deze sleutel wordt de File Encryption Key genoemd (FEK). De versleuteling vindt plaats door middel van het DESX-algoritme (een sterkere variant van DES) en de unieke sleutel (FEK). Vervolgens neemt de EFS de publieke sleutel van de gebruiker en/of groep die de versleuteling 'initieerde', en versleutelt met behulp van CryptoAPI de unieke FEK hiermee. De versleutelde FEK wordt vervolgens bij het versleutelde bestand (of folder) opgeslagen. Dit proces is hierna ter verduidelijking gestructureerd weergegeven:

1. Een bestand/folder wordt door de gebruiker getypeerd als te versleutelen.
2. Encryption File System genereert een unieke sleutel (File Encryption Key).
4. Bestand/folder wordt met behulp van het DESX-algoritme en de sleutel geëncrypt.
5. De sleutel wordt met de publieke sleutel van de gebruiker/groep geëncrypt en samen met het versleutelde bestand opgeslagen.

In feite wordt dus gebruikgemaakt van twee soorten encryptie, asymmetric en symmetric encryption; asymmetric encryption voor het versleutelen van de FEK en symmetric encryption voor het versleutelen van het bestand.

Wanneer een applicatie of gebruiker aan NTFS het verzoek doet om een versleuteld bestand op te vragen, geeft NTFS intern de call door aan EFS. EFS zoekt vervolgens de secret key van de gebruiker/groep op en decrypt de FEK. Met behulp van de FEK kan het bestand worden gedecrypt.

Beide processen zijn transparant voor de gebruikers. Lezen en opslaan, decrypten en encrypten, vindt on-the-fly plaats.

Een belangrijk punt van EFS is het gegeven dat een share versleuteld kan worden aangeboden en dat meerdere gebruikers (of een groep) die beschikken over de secret key (behorend bij de public key waarmee de FEK is versleuteld), de share kunnen benaderen en lezen.

Applicaties die niet via EFS een call (kunnen) uitbrengen, krijgen een versleuteld bestand (ciphertext) ter beschikking. Dit is gunstig voor bijvoorbeeld het uitvoeren van back-ups aangezien deze dan beveiligd zijn opgeslagen.

Een belangrijk negatief punt is dat de secret key van de gebruiker/groep op een 'beveiligd' deel binnen het bestu-

EFS	
Algoritme	DESX (versleutelen bestand) CryptoAPI (versleutelen FEK)
Sleutellengte	128 bits (56 bits voor non-US-versie)
Soort encryptie	Partiële encryptie van gegevens in opslag
Bootprotectie	Nee
On-the-fly	Ja

Tabel 1. Feiten Encryption File System.

ringssysteem wordt opgeslagen. Met andere woorden, iemand die fysieke toegang tot het Windows NT-systeem heeft, kan de secret key van het systeem afhalen. Microsoft onderkent dit risico en wil op korte termijn de EFS-technologie uitbreiden met smartcardreaders waarop de secret key kan worden geplaatst.

Een ander negatief punt van EFS, dat trouwens geldt voor elke encryptieapplicatie die on-the-fly encryption faciliteert, is het feit dat trojans ook als reguliere applicaties worden gezien. Trojans draaien immers onder het account van de gebruiker. Maar de besturingssystemen Windows NT en 95 in het bijzonder worden de laatste tijd geplaagd door trojans als BackOrifice (2000) en Netbus, waarmee onder andere bestanden via een netwerk van de harddisk opgehaald kunnen worden. Als de trojan draait als applicatie van een reguliere gebruikersaccount, worden de bestanden eerst on-the-fly gedecrypt alvorens ze worden verstuurd.

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is een applicatie die in vele versies, commercieel en freeware, beschikbaar is. Het primaire doel van deze applicatie is het versleutelen van e-mail; secundair kunnen met PGP bestanden op de harddisk worden versleuteld. Aangezien PGP gebruikmaakt van asymmetrische algoritmen is het eigenlijk ongeschikt om grote hoeveelheden data on-the-fly te versleutelen.

Een generiek[7] procesverloop van het gebruik van PGP is als volgt:

Voor het gebruik van PGP dienen gebruikers te beschikken over een paar sleutels, te weten een secret key en een public key. Dit paar kan met behulp van de PGP-applicatie worden gecreëerd. De public key kan aan eenieder worden verstrekt om veilig te communiceren. De ontvangers van de public key dienen te verifiëren of de public key daadwerkelijk afkomstig is van de zender (zie ook de eerste subparagraaf onder 'Risico's'). De gebruiker dient de secret key geheim te houden.

Een gebruiker (de zender) geeft vanuit een mailprogramma aan dat de e-mail dient te worden versleuteld. Voor veel mailprogramma's (o.a. Eudora, Exchange en Outlook) zijn zogenaamde plug-in's gemaakt zodat de PGP-applicatie is geïntegreerd in het mailprogramma. Als de e-mail wordt verzonden, 'herkent' PGP automatisch de naam van de geadresseerde en selecteert de bijbehorende public key. Wil de zender de tekst achteraf ook nog kunnen lezen dan dient hij zijn eigen public key eveneens toe te voegen. PGP versleutelt automatisch de tekst (inclusief de eventuele attachments), zodat de inhoud van de e-mail bestaat uit ciphertext en niet leesbaar is (zie figuur 5).

PGP	
Algoritme	Diffie-Hellman (RSA mag nu niet meer worden gebruikt, maar komt nog voor bij oudere versies)
Sleutellengte	768 tot 4096 bits
Soort encryptie	Partiële encryptie van gegevens in transport
Bootprotectie	Nee
On-the-fly	Nee, actief encrypten/ decrypten van bestanden

Tabel 2. Feiten Pretty Good Privacy

Tevens kan de zender ervoor kiezen een digitale handtekening aan de inhoud van de e-mail toe te voegen. Hiertoe wordt met behulp van de secret key een digitale handtekening gegenereerd.

De ontvanger van de e-mail kan de e-mail lezen door de ciphertext met de secret key te decrypten. Hiertoe dient de ontvanger te beschikken over de secret key en het wachtwoord dat toegang tot de secret key geeft. Tevens kan de ontvanger met de public key van de zender de handtekening verifiëren; de ontvanger is er nu van verzekerd dat de e-mail van de betreffende zender afkomstig is.

Een belangrijk voordeel van PGP is het gegeven dat gebruikers bijna autonoom een PGP-applicatie kunnen gebruiken. Organisatiebrede of -overstijgende maatregelen zoals Certificate Authorities zijn hierbij niet nodig.

Figuur 5. Ciphertext gegenereerd door PGP.

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.0 for non-commercial use
<http://www.pgp.com>

qANQR1DBwU4DnK6mCaDOFoEQB/9QAzjtW03emk
q7k3acMQbXe8W2nmUgYQaveqVp
LjNoMtQm3uq/KEa1IrObuFSdHyuGfB+apj1a+fRc+9af
HTprf2ncRcR+aVWSUdbX
OemdBeJlaijk1VsOOU801S5wvJpYDbBEirDMf23Hp9
BqMjoOOH78z2gk/hz++u7+
xx8HfmfQyWs3MzSKwkisbqixSzuvKbFiUjtjOjlUWicNnE
vJ3jtOStCpaORhddM4
83ZAR4mgMob5AFDQAW9n5uomql3KpWQi9Ks325it
qo7Cn/301zH4SgmS6ajHYuxK
kvD1+1vVJ/EhK8eRuYGXnlluhg===cgAT
-----END PGP MESSAGE----
```

7) Hierbij is van een PGP-applicatie voor Windows 95 uitgegaan. Unix-versies zijn veelal commando-georiënteerd.
8) Het patent op het Rivest-Shamir-Adelman cryptografische algoritme loopt in de Verenigde Staten per 20 september af; hierna kan het algoritme vrijelijk worden gebruikt.

Safeboot

Safeboot PC encryption is een encryptieapplicatie die beschikbaar is voor de besturingssystemen Windows 95/98 en NT. De nieuwste versie (3.3) wordt hier beschreven.

De functionaliteit van Safeboot is als volgt. Bij de installatie van Safeboot op een PC wordt een unieke sleutel (secret key) aangemaakt die vervolgens gedurende de periode dat Safeboot geïnstalleerd is, wordt gehanteerd voor het versleutelen. Vervolgens worden alle bestanden die zich op de harddisk bevinden met deze sleutel en het RC5-algoritme versleuteld. Bestanden die (achteraf) worden toegevoegd, worden ook met deze sleutel en dit algoritme versleuteld. Het resultaat is een volledig versleutelde harddisk (volledige encryptie).

Op de bootsector van de harddisk is een string geplaatst die normaliter de bootsequence van het geïnstalleerde besturingssysteem initieert. Bij een geïnstalleerde Safeboot-applicatie verwijst de initiatiestring echter naar de Safeboot-shell die zich met een inlogscherm presenteert aan de gebruiker. De gebruiker dient vervolgens zijn account en wachtwoord in te voeren (beide geldig) teneinde de PC succesvol te laten opstarten. Safeboot decrypt door middel van dit wachtwoord de secret key die 'ergens' op de harddisk is opgeslagen. Deze secret key en een zogenaamde Safeboot-shell worden vervolgens in het externe geheugen geplaatst en zullen, zolang de PC aanstaat, hier aanwezig blijven. Alle bestanden die worden opgevraagd en worden opgeslagen, bijvoorbeeld gedurende het gebruik van een Word-applicatie, worden vervolgens on-the-fly gedecrypt en geëncrypt in het externe geheugen van de computer.

Een alternatief op bovenstaand proces is dat de gebruikers de unieke sleutel op een hardware token bij zich dragen. Hiervoor wordt de sleutel op een PCMCIA-card of met behulp van een seriële/parallelle smartcardreader en smartcard aangeleverd. Een wachtwoord is dan nog steeds noodzakelijk maar om succesvol gebruik te kunnen maken van de PC dient de gebruiker te beschikken over een kenniskenmerk én een bezitskenmerk.

Een belangrijk voordeel van Safeboot is het gegeven dat de harddisk in zijn geheel wordt versleuteld. Hierdoor zijn databestanden die zich in de temp-directory, pagefiles, etc. bevinden automatisch ook versleuteld. Een nadeel hiervan is dat niet-vertrouwelijke bestanden, zoals systeembestanden en applicaties, ook versleuteld dienen te worden in het externe geheugen, hetgeen altijd een mate van performanceverlies oplevert. De meningen over de exacte mate van performanceverlies lopen nogal uiteen tussen de leverancier/fabrikant en de gebruikers van het product Safeboot.

Safeboot	
Algoritme	RSA RC5 (ondersteunt ook aangepaste of propriety-algoritmen)
Sleutellengte	1024 bits
Soort encryptie	Volledige encryptie van gegevens in opslag (partieel is mogelijk)
Bootprotectie	Ja
On-the-fly	Ja

Tabel 3. Feiten Safeboot.

Met Safeboot is het ook mogelijk wachtwoordinstellingen te configureren. Hierbij kan worden gedacht aan de geldigheidsduur van een wachtwoord, het wel of niet tonen van de laatst ingelogde account, screensaver met wachtwoordbeveiliging, etc. Tevens bezit Safeboot een auditfunctie waarmee de beheerder specifieke activiteiten kan herleiden. Een andere optie die Safeboot ondersteunt is (voor Windows NT-omgevingen) single sign-on. Met het aanloggen op Safeboot kan de gebruiker transparant doorloggen op een Windows NT-domein, de gebruiker voert derhalve nog maar één keer zijn wachtwoord in. Een nadelig puntje hiervan is dat dit wachtwoord (de hash) gecached wordt opgeslagen in de registry van de client-PC (met alle risico's die hiermee samenhangen).

De fabrikant van Safeboot heeft, als één van de weinige, het belang van adequaat beheer van encryptieapplicaties onderkend. Zo levert Safeboot onder andere de volgende faciliteiten:
* recovery information betreffende Safeboot via netwerk te ontvangen/verzenden (in plaats van diskette);
* corporate database voor gecentraliseerd beheer van de sleutels, smartcards, etc.

Voor adequaat beheer een stap in de goede richting, maar alleen niet voldoende.

Auditaspecten cryptografie-implementatie en -beheer

Bij een audit naar opzet, bestaan en werking van maatregelen en de effectiviteit van gebruikte hulpmiddelen in een organisatie worden de volgende 'objecten' onderscheiden en beoordeeld:
* de opzet van de cryptografische toepassing(en);
* de functionaliteit van de cryptografische toepassing(en);
* het beheer van de cryptografische toepassing(en).

In drie tabellen wordt een overzicht gepresenteerd naar de aspecten die per object worden beoordeeld. Het overzicht wordt gevormd door het aspect, de norm of eis van de organisatie, de te stellen vragen alsmede een toelichting op de auditvraag. De tabellen hebben de vorm van een controleprogramma.

De opzet van de cryptografische toepassing(en)

Auditaspect	Norm/eis	Te onderzoeken (auditvraag)	Opmerkingen
Noodzaak voor cryptografie	* De organisatie dient (beleidsmatig) te hebben vastgesteld of cryptografie dient te worden toegepast.	* Is op beleidsniveau de noodzaak voor het gebruik van cryptografie vastgesteld? * Welke voordelen/kwaliteitsaspecten denkt de organisatie met cryptografie te realiseren?	* Wil een organisatie gestructureerd gebruik gaan maken van cryptografie, dan dient zij top-down in plaats van bottom-up te worden geïmplementeerd. * Een organisatie dient eerst in kaart te hebben gebracht waarom zij denkt cryptografie nodig te hebben en welke voordelen hiermee worden bereikt.
Geclassificeerde data	* Het dient te zijn vastgesteld welke gegevens geclassificeerd zijn voor cryptografie.	* Heeft de organisatie een classificatie uitgevoerd van al of niet te versleutelen gegevens?	* Encryptie heeft pas zin wanneer een organisatie onderkent welke gegevens hiervoor zijn genomineerd.
Inventarisatie cryptografische toepassingen	* Een actuele inventarisatie van de reeds aanwezige cryptografische toepassingen dient te zijn uitgevoerd.	* Welke cryptografische toepassingen (inclusief algoritmen, etc.) zijn thans aanwezig binnen de organisatie?	* Om compatibiliteit tussen overige applicaties en toepassingen te handhaven/realiseren dient zicht op de reeds aanwezige cryptografische toepassingen te worden verkregen.
Toepasbaarheid cryptografie	* Het dient te zijn vastgesteld of de organisatie legaal gebruik kan maken van cryptografie.	* In welke landen wil de organisatie de cryptografische toepassing(en) gaan uitrollen? Welke restricties met betrekking tot cryptografie gelden in deze landen? * Welke juridische consequenties treden op bij gebruik van encryptie?	* Cryptografie is, evenals de ICT, grensoverschrijdend. Nationale wetten dienen geen belemmering te vormen. * Is de organisatie in landen aanwezig waar key-escrow door de overheid wordt verplicht?
Uitvoeren van risicoanalyse	* Een risicoanalyse dient te zijn uitgevoerd waaruit de noodzaak voor het gebruik van encryptie moet blijken.	* Welke risico's loopt de organisatie wanneer geen gebruik wordt gemaakt van cryptografie? * Welke maatregelen dienen te worden genomen om de risico's weg te nemen? * Welke kosten zijn gemoeid met het gebruik van cryptografie? * Ondervinden de primaire processen geen last van het gebruik van cryptografie?	* Een risicoanalyse dient voor een organisatie duidelijk te maken welke voor- en nadelen met behulp van cryptografie worden bereikt.
Vastleggen rollen	* De verschillende te onderkennen rollen met betrekking tot cryptografie dienen te zijn benoemd.	* Welke functionarissen spelen een (operationele) rol met betrekking tot cryptografie? * Zijn de verantwoordelijkheden toegekend?	* Het gebruik van cryptografie dient te worden begeleid. Hiervoor dienen in de organisatie verantwoordelijkheden te zijn belegd.

Functionaliteit van de cryptografische toepassing(en)

Auditaspect	Norm/eis	Te onderzoeken (auditvraag)	Opmerkingen
Ondersteunde besturingssystemen	* Het pakket dient door zoveel mogelijk besturingssystemen te worden ondersteund.	* Welke besturingssystemen worden ondersteund door het pakket? * Welke besturingssystemen zijn aanwezig? * Heeft de organisatie plannen om op (korte) termijn te migreren naar een ander platform (bijvoorbeeld van Windows 95 naar Windows NT)?	* Mede gezien de toekomstvastheid van het gebruik van een encryptieapplicatie is het aan te bevelen een applicatie te kiezen die op meerdere besturingssystemen draait.
Installatiegemak	* Het pakket dient in een overzichtelijk installatieproces te kunnen worden geïmplementeerd.	* Hoe (op welke wijze) vindt de installatie van het pakket plaats? * Hoe ervaart de beheerafdeling de installatie? * Hoe wordt een uniforme installatie gerealiseerd?	* Omdat het uit het oogpunt van uniformiteit gewenst is dat iedere PC met dezelfde instellingen wordt uitgeleverd, dient het installatieproces bij voorkeur door middel van een overzichtelijk menu en wellicht met een installatiescript te worden uitgevoerd.
Gehanteerd cryptografisch algoritme	* Het encryptiepakket dient een veilig cryptografisch algoritme te gebruiken.	* Welk algoritme wordt gehanteerd, hoeveel bits vercijfering vindt plaats?	* Hoewel dit één van de belangrijkste auditaspecten zou moeten zijn, blijft de rol van een auditor hier veelal beperkt tot het waarnemen welk algoritme wordt gebruikt en hoe veilig dit algoritme en de sleutellengte in de vakliteratuur worden getypeerd (zie kadertekst 1).
Genereren sleutel	* Per gebruiker dient een unieke sleutel te worden gegenereerd die achteraf onherleidbaar dient te zijn. De sleutels dienen periodiek te worden vervangen.	* Op welke wijze wordt een sleutel gegenereerd? * Van welke factoren (variabelen) is het genereren van een sleutel afhankelijk? * Maakt het genereren van een unieke sleutel deel uit van het installatieproces? * Is de geldigheid van een sleutel gelimiteerd?	* Voor de beheerafdeling zal het gebruik van één enkele sleutel gemakkelijker zijn dan het beheren van honderden verschillende sleutels (elk beschermd door het persoonlijk gebruikerswachtwoord). Uit oogpunt van beveiliging is dit natuurlijk onacceptabel. * Het gebruik van dezelfde sleutel voor langere perioden is een risico dat voorkomen dient te worden.
Identificatie en authenticatie	* Toegang tot versleutelde bestanden dient plaats te vinden op basis van ten minste een unieke gebruikersnaam en wachtwoord. * Het vaststellen van de authenticiteit dient te geschieden op basis van bezits- en kenniskenmerk (token en wachtwoord).	* Dient de gebruiker zich te identificeren? * Identificeert en authenticeert de gebruiker zich door middel van een wachtwoord? * Ondersteunt het pakket het gebruik van hardwaretokens zoals smartcardreaders en PCMCIA-cards?	* Toegang tot versleutelde bestanden op basis van gebruikersnaam en wachtwoord heeft uit oogpunt van beveiliging de voorkeur boven het vaststellen van de authenticiteit op basis van alleen een wachtwoord. * Een additionele laag van beveiliging wordt gecreëerd door het gebruik van encryptieapplicaties die hardwaretokens ondersteunen, zoals een PCMCIA-card.
Accountpolicies	* Het dient mogelijk te zijn flexibel parameters te bepalen betreffende: – lengte en samenstelling wachtwoord; – aantal toegestane inlogpogingen; – periodiciteit van lock-out; – geldigheidsduur wachtwoord; – historie van aantal wachtwoorden; – toestaan van wijzigen wachtwoord; – inlogtijden; – etc.	* Is het mogelijk accountpolicies te bepalen? * Welke accountpolicies (met welke waarden) zijn ingesteld? * Op basis waarvan zijn de accountpolicies vastgesteld?	* Het vaststellen van de waarden voor accountpolicies zou, best practice, dienen te geschieden op basis van het reeds aanwezige informatiebeveiligingsbeleid. * Bij het beoordelen van de ingestelde waarden dient rekening te worden gehouden met het feit dat praktische ondersteuning door de beheerafdeling veelal alleen mogelijk is wanneer men fysiek over de PC kan beschikken (geen telefonische en/of remote support). Een mix dient te worden gevonden tussen een adequate beveiliging en een voor gebruiker en beheerder werkbare situatie.

vervolg op pagina 38

vervolg van pagina 37

Auditaspect	Norm/eis	Te onderzoeken (auditvraag)	Opmerkingen
Audit trail	* De applicatie dient te beschikken over logfunctionaliteiten.	* Beschikt de applicatie over de mogelijkheid om specifieke voorvallen te registreren? * Stel vast welke gegevens worden gelogd. * Stel vast door wie de loggegevens kunnen worden uitgelezen en op welke wijze de integriteit van de loggegevens kan worden vastgesteld.	* Een audit trail in een encryptieapplicatie kan informatie verschaffen over mogelijke inbraakpogingen en de bron van problemen in de applicatie verklaren.
Bootprotectie	* Ongeacht het bootmedium (hard- of floppydisk) dienen alleen geautoriseerde gebruikers toegang tot de harddisk te kunnen krijgen (totale encryptie).	* Wat is de status van de bestanden (versleuteld of niet) als de PC onverwacht uitvalt? * Vindt on-the-fly decryptie en encryptie plaats?	* Aspecten die veelal in de handleiding van de applicatie zijn beschreven.
Objectaccess	* Het dient mogelijk te zijn specifiek aan te geven welke folders en/of bestanden versleuteld worden (bij partiële encryptie). * Volledige encryptie verdient de voorkeur.	* Bestaat de mogelijkheid om partities, folders en bestanden te versleutelen? * Vindt on-the-fly decryptie plaats? * Wordt gebruikgemaakt van single sign-on techniek? * Wat is de status van de bestanden (versleuteld of niet) als de PC onverwacht uitvalt?	* Het gebruik van partiële encryptie verwacht van de gebruiker een dosis discipline aangezien de gebruiker nieuwe bestanden in de te versleutelen folders moet opslaan. * Bij partiële encryptie dient de applicatie te beschikken over de functionaliteit om bij afsluiten van de PC de inhoud van de temp-directory definitief te verwijderen.
Fail-restore mogelijkheden	* Het pakket dient de mogelijkheid te bezitten om bij een storing (verlies wachtwoord, corrupte sectors harddisk, corrupte bootsector) toch nog bestanden te decrypten.	* Welke fail-restore procedures zijn aanwezig? * Beschikt de beheerafdeling over een masterkey? * Welke garanties worden door de leverancier afgegeven? * Wat is de impact op de bestanden (versleuteld of niet) als de PC onverwacht uitvalt?	* De auteur van dit stuk heeft als gebruiker helaas slechte ervaringen op dit gebied.
Efficiency en performance	* De werking van de applicatie dient de functionaliteit niet te verstoren.	* Treedt merkbare performance-achteruitgang op na installatie van het pakket?	* Een sterk algoritme (veilig?) met een grote sleutellengte kan mogelijk een negatieve impact hebben op de performance en daarmee op de gebruikersacceptatie.

Samenvatting

Door het gebruik van cryptografie, bijvoorbeeld door het gebruik van encryptieapplicaties (waarop in dit artikel specifiek is ingegaan), wordt men in staat gesteld kwaliteitskenmerken zoals integriteit, vertrouwelijkheid en authenticiteit van gegevens in één keer te waarborgen. In een tijdperk waarin steeds meer gebruik wordt gemaakt van transparante netwerken, shared databases en remote toegang tot corporate netwerken, wordt het belang van het waarborgen van deze kwaliteitsaspecten alsmaar groter. Dit artikel beschrijft de organisatorische aspecten omtrent het gebruik van cryptografische toepassingen in een organisatie en de risico's die met het gebruik van cryptografie samenhangen.

Het selecteren, implementeren en beheren van cryptografische toepassingen is geen sinecure. Men dient voordat tot selectie en implementatie van cryptografische toepassingen wordt overgegaan goed in kaart te hebben gebracht welke cryptografische toepassingen reeds aanwezig zijn en welke gegevens dienen te worden beschermd. Hiertoe is in het artikel een verkorte variant van een framework van het European Security Forum beschreven alsmede is een opsomming opgenomen van kritieke succesfactoren. Hieruit blijkt dat men uitgangspunten dient te hanteren die voor de lange termijn en organisatiebreed kunnen worden ingezet, teneinde synergie tussen meerdere cryptografische toepassingen binnen een organisatie te bewerkstelligen.

Aan het gebruik van encryptieapplicaties zijn enkele risico's verbonden die men met maatregelen dient tegen te gaan teneinde een adequaat gebruik van dit soort applicaties te waarborgen. De risico's zijn verdeeld in de aspecten applicatie, beheer en gebruik. In het artikel zijn deze risico's uitgebreid aan bod gekomen en zijn enige maatregelen opgesomd. Tevens wordt benadrukt dat 'reguliere' informatiebeveiligingsmaatregelen niet komen te vervallen door het gebruik van encryptieapplicaties, maar gewoon aanwezig dienen te zijn om adequaat gebruik van dit soort applicaties te waarborgen.

Beheer van de cryptografische toepassing(en)

Auditaspect	Norm/eis	Te onderzoeken (auditvraag)	Opmerkingen
Genereren sleutels	* Sleutels dienen uniek en door geautoriseerde medewerkers te worden gegenereerd.	* Welke normen heeft de organisatie gesteld aan de samenstelling van de sleutels (lengte, 'houdbaarheid', etc.)? * Hoe worden de sleutels gegenereerd? * Welke medewerkers zijn geautoriseerd om sleutels te genereren?	* De uniciteit van een sleutel maakt het beheer complexer voor een beheerorganisatie.
Beheer sleuteldatabase	* Adequate beheerprocedures met betrekking tot de sleuteldatabase dienen aanwezig te zijn.	* Hoe worden de volledigheid en de integriteit van de database gewaarborgd? * Met welke procedures worden sleutels toegevoegd in en verwijderd uit de database? * Worden sleutels definitief verwijderd? * Welke medewerkers hebben het recht de sleuteldatabase in te zien, te migreren en/of er back-ups van te maken? * Waar en hoe is de sleuteldatabase opgeslagen? – logische toegangsbeveiliging; – fysieke toegangsbeveiliging. * Hoe wordt de continue beschikbaarheid van de database gewaarborgd?	* Het verwijderen van oude sleutels kan op een later tijdstip tot gefrustreerde gebruikers leiden. * Het is duidelijk dat (het beheer van) de sleuteldatabase de achilleshiel van een succesvolle implementatie van cryptografie is.
Koppeling sleutels uit database met de objecten	* De (unieke) sleutels dienen onvoorwaardelijk gekoppeld te zijn aan het juiste object (PC, personeelsnummer).	* Op welke wijze worden de sleutels thans gekoppeld aan de objecten? * Is wijziging van hardware van de eigenaar funest voor de koppeling van de sleutels?	* Wanneer een organisatie meer dan, zeg, honderd sleutels bezit wordt het adequaat koppelen van sleutels aan objecten zeer belangrijk om een en ander beheersbaar te houden.
Kennis en kunde beheerafdeling	* De beheerafdeling dient capabel te zijn om adequaat beheer te voeren.	* Beschikt de beheerafdeling over voldoende kennis en kunde om ondersteuning te kunnen leveren? * Hebben de beheerders cursussen gevolgd van de leverancier?	* Beheerafdelingen dienen ervaring met de applicatie in werkinstructies en knowledgedatabase te hebben vastgelegd.
Uitgifte standaardconfiguratie	* Binnen de organisatie dienen zo weinig mogelijk verschillende cryptografische applicaties en versies te worden gebruikt.	* Hoe gaat de beheerafdeling om met nieuwe versies? * Is vastgelegd welke versie standaard is?	* Het implementeren van verschillende standaarden kan tot problemen leiden bij migratie, ondersteuning, etc.
Ondersteuning leverancier	* Een overeenkomst dient te zijn afgesloten waarin wordt vastgelegd welke vorm van ondersteuning wordt geleverd.	* Stel vast op welke wijze ondersteuning wordt geleverd.	* In principe zou, zoals bij een regulier applicatieselectietraject, de continuïteit van een leverancier mede aandachtspunt dienen te zijn.

Drie encryptieapplicaties worden in dit artikel behandeld, zodat de lezer een indruk krijgt van enkele applicaties die momenteel beschikbaar zijn. Tevens wordt hiermee gepresenteerd welke specifieke functionaliteit door een applicatie kan worden geboden.

Ten slotte zijn in het artikel aspecten genoemd waarmee gedurende een beoordeling van een cryptografische toepassing rekening dient te worden gehouden. Hierbij is ruim aandacht besteed aan het beheer van deze toepassingen.

Literatuur

Boeken, whitepapers

[ESF97]
European Security Forum, *A framework for using cryptography*, 1997.

[Micr98]
Microsoft Corporation/(Windows NT Server), *Encrypting File System for Windows NT version 5.0*, whitepaper, 1998, www.microsoft.com.

[Moon98]
R. Moonen, *Oplossingen voor veilige electronic commerce over Internet*, Compact 1998/4.

[Netw98]
Network Associates, *An Introduction to cryptography*, 1998.

[RSA99]
RSA Laboratories, *Frequently Asked Questions About Today's Cryptography*, 4th version, www.rsa.com.
[Schn96]
Bruce Schneier, *Applied Cryptography protocols, algorithms, and source code in C*, second edition, Wiley, 1996.
[WNT99]
Windows NT Magazine, *Inside EFS part I*, june 1999.
[WNT99]
Windows NT Magazine, *Inside EFS part II*, july 1999.

Websites

www.certicom.com
Elliptic Curve Cryptosystem Whitepapers
www.controlbreak.nl
Control Break Europe
www.counterpane.com
Counterpane Homepage
www.jya.com/crypto.htm
Cryptome
www.rsa.com
RSA Data Security, Inc.
www.sonic.net/~bear/rsa.htm
The RSA Algorithm

Kaderteksten

ntsecurity-digest Tuesday, May 18 1999 Volume 03: Number 491

Date: Mon, 17 May 1999 07:16:57 -0400 (EDT)
From: Jeff Barber <jeffb@issl.atl.hp.com>
Subject: Re: [NTSEC] Keeping Admins out of sensitive data

> Encryption doesn't buy you security, it only buys you time.

Strictly speaking, that's true of course, but with plenty of bits and a good cipher, it buys you time on a cosmologic scale. Here's the analysis of 128-bit IDEA (the symmetric cipher used in PGP) from Appendix II of the comp.security.pgp FAQ:

Keylength

The length of the key used to encrypt data always puts an upper limit on the security of an algorithm. In principle, one could try all possible keys, and see which one correctly decrypts the data. This is called a 'brute-force attack'. The number of possible keys should be large enough to make this impossible. For IDEA, there are 2^{128} keys, or about 3×10^{38}. If we had a computer capable of trying one billion keys per second (10^9/s) (this is beyond the capability of existing supercomputers) how long would it take to find one IDEA key?

There are $60 \times 60 \times 24 \times 365 = 3.15 \times 10^7$ seconds in a year.

With 10^{38} keys, it would take this hypothetical computer $3 \times 1038/(10^9 \times 3 \times 10^7) = 10^{22}$ years to find one key.

If every person on earth had one such computer, it would 'only' take $10^{22} / 5 \times 10^9 = 2 \times 10^{12}$ years. This is hundreds of times longer than the age of the earth (4.5×10^9 years). So we can conclude that IDEA is quite safe from a brute-force attack.

Kadertekst 1. Encryption doesn't buy you security, it only buys you time.

M.W. Baurichter
is werkzaam bij KPMG EDP Auditors in de business unit Technology & Assurance. Zijn werkzaamheden richten zich voornamelijk op het uitvoeren van audits van Unix- en Windows NT-omgevingen. Tevens houdt hij zich bezig met Internet-gerelateerde activiteiten zoals firewall-certificering en het opstellen van Internet-beveiligingsbeleid voor diverse organisaties. Daarnaast participeert hij in de productontwikkelgroepen Open Omgevingen en Electronic Commerce.

In de inleiding is kort toegelicht wat de toenemende noodzaak voor cryptografie is. Zowel particulieren als bedrijven maken steeds meer gebruik van het Internet en mobiele telefoons. Echter, niet alleen bonafide partijen maken gebruik van de informatie- en communicatietechnologie, ook criminele organisaties maken gretig gebruik van deze technieken waarmee zij activiteiten ontplooien die het daglicht niet kunnen verdragen. Onderstaande toelichting maakt duidelijk dat de Europese Commissie op supranationaal niveau hiertegen iets wil doen. Hierbij kan de vraag worden gesteld wie nu daadwerkelijk wordt 'aangepakt'.

ENFOPOL 19
Het Europees Parlement heeft medio 1999 besloten over een nieuwe Europese richtlijn op het gebied van de telecommunicatie. Deze richtlijn, genaamd ENFOPOL 19, maakt het mogelijk dat officiële instanties nieuwe telecommunicatiediensten kunnen aftappen.

Internet en mobiele telefonie, waaronder het Iridium, zouden bij goedkeuring door de overheden worden (mis)(ge)bruikt om informatie te verzamelen. Ook het gebruik van cryptografie zou aan banden worden gelegd (door middel van escrow-procedures), dit alles om criminele activiteiten tegen te gaan.

Voor bonafide bedrijven en particulieren zou het illegaal worden om zich te wapenen tegen bedrijfsspionage en privacy-inbreuk, voor criminele organisaties zou het natuurlijk ook illegaal zijn maar het is hoogst onwaarschijnlijk dat zij zich spontaan zullen conformeren aan de(ze) wet.

http://www.heise.de/tp/english/special/enfo/6397/1.html

Kadertekst 2.
De noodzaak voor cryptografie.

De beveiliging van versleutelde data (ciphertext) is gebaseerd op de sterkte van het algoritme en de geheimhouding van de sleutel. De geheimhouding van de sleutel is, nadat deze op een willekeurige wijze is gegenereerd, te realiseren door adequaat sleutelbeheer. De sterkte van het algoritme is intrinsiek en kan 'achteraf' door maatregelen niet meer worden beïnvloed, hierbij aanpassingen op de (source)code van algoritmen buiten beschouwing latend. Hieronder volgt een korte uiteenzetting over twee algoritmen waarvan de eerste als zwak algoritme en de tweede als sterk algoritme wordt beschouwd.

DES
Sleutellengte: 64-bit invoer (56-bit effectieve sleutellengte)

DES is in 1970 oorspronkelijk door IBM ontwikkeld en in 1976 door het National Institute of Standards and Technology (NIST) als standaardalgoritme voor encryptie van niet-geclassificeerde data aangenomen. (Deze standaard is sinds 1997 overigens niet meer officieel van kracht.)

Tot op heden is het DES-algoritme niet gekraakt anders dan door het uitputtend berekenen van mogelijke sleutels (brute-force attack). Berekend is dat een computer ter waarde van 1 miljoen dollar het DES-algoritme door middel van een brute-force attack binnen anderhalve dag kan kraken, later is dit bijgesteld tot 35 minuten bij eenzelfde uitgave. Duidelijk is dat het DES-algoritme onveiliger wordt naarmate de rekenkracht van computers verder toeneemt.

Het is Amerikaanse overheidsinstanties verboden nog gebruik te maken van het DES-algoritme. Als tijdelijk alternatief is het Triple-DES-algoritme aanbevolen, dat tot nu toe véél langer bescherming blijft bieden. Thans zijn door de Amerikaanse overheid vijf algoritmen geselecteerd waarvan één algoritme de definitieve opvolger van het DES-algoritme zal gaan worden. Het betreft de algoritmen MARS (IBM), RC6 (RSA), Rijndael (J. Daemen en V. Rijmen), Serpent (R. Anderson e.a.) en Twofish (B. Schneier e.a.). Het uiteindelijk geselecteerde algoritme zal worden beschouwd als de Advanced Encryption Standard (AES).

Blowfish
Sleutellengte: Block cipher 64-bit block invoer (variabele sleutellengte van 32 tot 448 bit)

Het Blowfish-algoritme is oorspronkelijk ontwikkeld door Bruce Schneier (Applied Cryptography) in 1993. Het algoritme is vele malen sneller dan het DES-algoritme wanneer het draait op een Pentium-computer. Het algoritme is niet gepatenteerd en is vrij te gebruiken in applicaties. Daar Blowfish beschikt over een variabele sleutellengte, is het mogelijk kortere sleutellengten te gebruiken en zo exportrestricties te omzeilen, waardoor het algoritme in meerdere landen kan worden gebruikt.

Blowfish wordt als een sterk algoritme beschouwd en is tot op heden niet gekraakt, terwijl het algoritme al vele malen is getest. Het algoritme wordt meer en meer in (commerciële) applicaties toegepast (PGPfone, Nttrust, SSH voor Unix en in het besturingssysteem OpenBSD).

Kadertekst 3.
Zwakke en sterke algoritmen.