

Dit artikel is de eerste in een reeks van vier, die ingaat op een aantal verschillende cryptografische producten en methodieken, waarbij er onder andere naar de werking en de praktische toepasbaarheid wordt gekeken.

In deze aflevering wordt gestart met het bestands- en folderencryptieproduct PGP (voorheen Pretty Good Privacy).

Het tweede artikel behandelt de twee e-mail encryptiestandaarden OpenPGP en S/MIME.

In de derde aflevering wordt het Encrypted File System (EFS), wederom bestands- en folderencryptie,

van Microsoft Windows 2000 behandeld.

In een afsluitend artikel worden de genoemde bestands- en folderencryptieproducten met elkaar vergeleken.

PGP

onder de loep

Leon Kuunders

lijk beheer, eindgebruiker, implementatie, integratie, profiel van de fabrikant en techniek. Deze bijlage wordt via het internet gepubliceerd¹.

Wat is PGP?

Pretty Good Privacy is het product dat in 1991 door de uitvinder Phil Zimmerman als freeware ter beschikking werd gesteld aan iedereen die e-mail verkeer wilde coderen.

Het product is in de loop der jaren uitgegroeid tot het meest populaire e-mail encryptiesoftware ter wereld. In 1997 werd zijn bedrijf PGP Inc. door Network Associates International overgenomen. Sindsdien is de software in hoog tempo uitgebreid met modules voor Distributed Firewall-, Personal Intrusion Detection-, VPN- en File & Folder Encryption.

In dit artikel wordt alleen aandacht besteed aan de mogelijkheden voor het coderen en decoderen van bestanden en folders middels de File & folder Encryption module PGP-disk versie 7.0.

Hoe werkt PGP?

Voor het automatisch coderen van bestanden maakt PGP gebruik van de module PGP-disk. PGP-disk ondersteunt Windows95/98/ME/NT4/2000 en Apple MacOS. Een PGP-disk wordt gemaakt als een bestand van minimaal enkele megabytes groot, dat wordt geactiveerd (gemount) als extra schijf (zichtbaar in de Explorer) of als een folder (alleen op Windows 2000 NTFS). Bestanden die worden geplaatst in zo'n folder of schijf worden gecodeerd en zijn alleen leesbaar voor personen die hiertoe gemachtigd zijn.

Een PGP-disk wordt aangemaakt als een collectie blokken van 512 bytes. Blokken die aan het begin van het PGP-volume staan worden gebruikt voor het vastleggen van administratieve data zoals de file allocation table. De gecodeerde gegevens worden in het midden van het bestand geplaatst (de data-area). De PGP-disk driver vertaalt alle gegevens die het bestandssysteem wil lezen van of schrijven naar het volume, naar het lezen of schrijven van individuele datablokken (sectoren). Het coderen en decoderen van de gegevens gebeurt on-the-fly, per sector. PGP-disk weet dus niet wat voor bestanden er op een PGP-volume staan, zodat het mogelijk is om een PGP-disk te formatteren in elk formaat dat door het besturingssysteem wordt herkend.

...Het adequaat omgaan met een digitale sleutel gaat veel gebruikers al te ver...

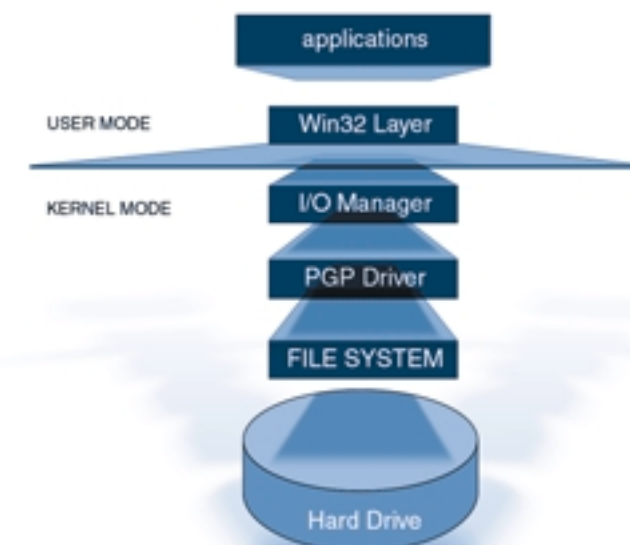
PGP-disk kan voor het coderen en decoderen van gegevens gebruik maken van een 128-bit versie van het symmetrische CAST algoritme of een 256-bit versie van het Twofish algoritme. Tijdens het aanmaken van een PGP-disk wordt een hoeveelheid willekeurige data van de gebruiker verzameld waarmee de 128-bit sessie sleutel wordt gegenereerd. Deze sessiesleutel wordt gecombineerd met 64-bits 'ruis', om een dictionary attack op de wachtzin onmogelijk te maken. Vervolgens wordt de aldus gemaakte sleutel gebruikt om de PGP-disk aan te maken en te coderen.

Een PGP-disk heeft één beheerderswachtzin of publieke sleutel en kan naast een zevental extra wachtzinnen een ongelimiteerd aantal extra publieke sleutels bevatten waarmee toegang tot de PGP-disk kan worden verkregen. Om problemen met de PGP-disk, ontstaan door slechte sectoren op de harde schijf, te verkleinen, wordt de gecodeerde sessiesleutel in de eerste en de laatste blokken van de PGP-disk opgeslagen.

De wachtzinnen die gebruikt worden om de PGP-disk te kunnen laden worden door PGP in een tijdelijke geheugen opslagplaats bewaard. Op deze manier wordt voorkomen dat een wachtzin in het swap-bestand terecht komt. Zelfs tijdens het invoeren van de wachtzin wordt deze beschermd en als onleesbare tekst in het geheugen geplaatst.

De PGP-diskdriver is het hart van PGP-disk. Deze driver maakt het mogelijk om rechtstreeks met de PGP-disk te communiceren. Het formatteren van de PGP-disk en het mounten ervan is zonder de driver niet mogelijk. Op Windows NT en Windows 2000 wordt de driver voor PGP-disk geïnstalleerd in kernel-mode (zie figuur 1.).

Door het gebruik van de driver bestaat de mogelijkheid om geheugenblokken te reserveren voor de PGP-disk. Dit maakt de bescherming van de wachtzin mogelijk.



figuur 1: Integratie van PGP-disk met NT.

Zodra een gebruiker een PGP-disk wil activeren, zal door de PGP-diskapplicatie gevraagd worden om een wachtzin. De wachtzin wordt gebruikt om de sessiesleutel waarmee de PGP-disk is gecodeerd te decoderen. Vervolgens wordt aan de PGP-diskdriver deze sessiesleutel samen met het pad naar het PGP-disk bestand en de gewenste schijf doorgegeven. De driver zorgt er vervolgens voor dat er door het besturingssysteem een nieuw volume wordt aangemaakt met de gewenste driveletter. Nadat het volume is geladen, controleert het besturingssysteem wat voor formaat het nieuwe volume heeft. Als de systeemdriever het nieuwe volume heeft herkend, wordt het volume beschikbaar gesteld aan de gebruiker en kan ervan worden gelezen en/of naar worden geschreven.

De praktijk

Om op een veilige en betrouwbare manier cryptografische producten in te kunnen zetten, is het noodzakelijk dat een oplossing wordt gevonden voor vraagstukken die voornamelijk te maken hebben met het sleutelbeheer, zoals 'Wat is de geldigheidsduur van een sleutel?', 'Wie kan een sleutel van een medewerker intrekken indien deze het bedrijf verlaat?', 'Hoe worden sleutels uitgedeeld aan medewerkers?' en 'Hoe wordt een sleutel verkregen indien een medewerker daar niet aan wil- of kan meewerken?'. (Bij een justitieel onderzoek naar het bedrijf of de medewerker, zal het bedrijf in staat moeten zijn de informatie te ontsleutelen zonder afhankelijk te zijn van de bereidwilligheid van de medewerker.) Antwoorden hierop zijn sterk afhankelijk van zowel de technische als de organisatorische omgeving waarin het product wordt ingezet. Kijkt men naar de randvoorwaarde van de cryptografie, namelijk de eis dat het op een

...Controle op de naleving van het vastgestelde cryptografiebeleid is essentieel...

Cryptografische producten maken gebruik van wiskundige algoritmes die berichten of bestanden op een dusdanige manier te versleutelen, dat het terugrekenen van het originele bestand alleen maar binnen afzienbare tijd kan worden gedaan indien de gebruikte sleutel bekend is. De gebruikte wiskundige algoritmes zijn te verdelen in public-key⁵ en secret-key⁶ systemen. Bij public-key systemen (asymmetrische systemen) wordt er gebruik gemaakt van een privé en een publieke (openbare) sleutel, terwijl in secret-key systemen (symmetrische systemen) slechts één sleutel in gebruik is. Een secret-key systeem is vanwege het

gebruikte algoritme vele malen sneller dan een public-key systeem. Tevens moet een privé sleutel in een public-key systeem langer zijn dan een geheime sleutel uit een secret-key systeem, omdat het in een public-key systeem eenvoudiger en dus sneller is om de privé sleutel terug te rekenen (factoring) dan deze te gokken (brute-force) door alle mogelijke combinaties te proberen. De meeste producten werken met een combinatie van beide technieken, door informatie te coderen met

een symmetrische techniek, en de daarvoor gebruikte (willekeurig gekozen) sleutel te coderen met behulp van een asymmetrische techniek. Hiermee wordt de snelheid van een symmetrisch systeem gecombineerd met de veiligheid van een asymmetrisch systeem. Om te kunnen zien hoe veilig een gebruikt cryptografisch systeem is, moet men echter niet alleen kijken naar de gebruikte sleutellengte, maar tevens naar de implementatie van de verschillende technieken.

CRYPTOGRAFISCHE ALGORITHMES

betrouwbare manier ingezet móet worden, dan is de controle op naleving van het vastgestelde beleid essentieel.

Een succesvolle implementatie van PGP-disk steunt behoorlijk op de definitie van duidelijke en werkbare richtlijnen met betrekking tot het sleutelbeheer. De meest eenvoudige implementatie gaat uit van een grote mate van verantwoordelijkheid voor de eindgebruiker. Daarbij wordt met een zogenaamde additionele decryptie-sleutel (ADK), die bijvoorbeeld door de directe lijnverantwoordelijke in de organisatie wordt beheerd, de beschikbaarheid van de gecodeerde gegevens gegarandeerd. Dit is nodig indien de gebruiker zijn eigen privésleutel verliest, zijn wachttin is vergeten of geen medewerking wil of kan verlenen.

Werken met een PGP-disk is eenvoudig, niet alleen voor de eindgebruiker, maar zeker ook voor de beheerder. Met behulp van de 'PGP Administrator Setup' kan een beheerder alle opties die voor PGP-disk gebruikt mogen worden definiëren en vastleggen in een installatiepakket dat zonder verdere gebruikersinterventie kan worden geïnstalleerd op een

desktop of laptop. Ook het implementeren van een ADK is vast te leggen in deze setup. Na installatie kan de gebruiker desgewenst zelf niets meer veranderen aan de instellingen die zijn vastgelegd, waardoor de controle op het gebruik van de versleuteling wordt vergroot.

...Veilig en betrouwbaar cryptografische producten inzetten staat of valt met sleutelbeheer...

Sleutelbeheer

Het gebruik van cryptografische producten is in grote mate afhankelijk van het op een juiste wijze opzetten van het sleutelbeheer. Immers, met het uitdelen van sleutels wordt het vertrouwen tussen verschillende partijen bekrachtigd. Een groot aantal partijen wijst erop dat Pretty Good Privacy, vanwege het eindgebruikers karakter van het product en de mogelijkheid om naast een hiërarchische certificatenstructuur zoals deze in x.509 wordt gebruikt tevens andere vertrouwensrelaties te creëren (het zogenaamde 'web-of-trust' model), niet geschikt zou zijn voor het op grote schaal inzetten van de techniek. De problematiek blijft echter voor beide technieken (zowel PGP als x.509, zie²) hetzelfde. Het succesvol opzetten van een public-key-infrastructuur kan alleen indien duidelijke procedures worden vastgelegd rondom het sleutelbeheer. Het ontbreken van duidelijke richtlijnen en werkinstructies zal de implementatie van ieder encryptieproduct tot een mislukking maken.

Het merendeel van de initiatieven die door marktpartijen en de overheid³ worden ontplooid op het gebied van PKI en encryptie, richten zich op de formele x.509 standaard. Kijkt men naar de kosten en de hoeveelheid tijd die het opzetten van zo'n formele structuur met zich meebrengt, dan is voor het bedrijfsleven het opzetten van een PGP infrastructuur op dit moment het meest aantrekkelijk, zeker voor het MKB+.

IN HET NIEUWS

Informatiebeveiliging op nationale agenda VS

Op 22 mei 1998 werd in de VS het Presidential Decision Directive (PDD) nummer 63 gepubliceerd. Dit presidentieel besluit deed het onderwerp 'informatiebeveiliging' op de nationale agenda van de VS belanden. Onder president Bush wordt daar nu door National Security Advisor Condoleezza Rice verder opvolging aan gegeven. Zij heeft op 23 maart aangekondigd dat deze zomer het nieuwe 'National Plan for Critical Infrastructure Assurance' zal worden gelanceerd. Dit plan is geschreven door zowel overheid als bedrijfsleven en is de eerste stap op weg naar het ineenslaan van de handen van beide om de bescherming van de kritische infrastructuur van de VS te garanderen. Het plan speelt zich af op federaal en nationaal niveau en beslaat meerdere sectoren van de economie.

<bron>

www.newsbytes.com

Voor meer informatie zie ook

www.ciao.gov

www.nipc.gov

VN stellen wereldwijde e-security strategie op

In de week van 26 maart vond in New York een conferentie plaats van gedelegeerden van alle lidstaten van de Verenigde Naties en de Amerikaanse high-tech industrie. Doel van de conferentie was nieuwe strategieën te vinden voor het omgaan met internetcriminaliteit en wereldwijde e-commerce beveiligingsvraagstukken. De Informatica werkgroep van de VN (Working Group on Informatics) stelt zich ten doel diploma ten gevoelig te maken voor de implicaties van IT. De werkgroep

EU zet vaart achter harmonisatie telecomwetgeving

De Europese Unie wil de telecom-regelgeving zo snel mogelijk dit jaar hebben aangenomen. Dit is de uitkomst van de Europese top in Stockholm van eind maart. De Europese Commissie zal samenwerken met de Raad van Europa bij het totstandbrengen van de randvoorwaarden voor een 'draadloos Europa'. Hoogwaardig onderzoek naar toekomstige draadloze technologieën zal worden gestimuleerd, de uitrol van de nieuwe generatie internet (Ipv6) zal worden aangemoedigd en er zal zorg worden gedragen voor de

hoog niveau van beveiliging worden behaald alwaar het het beschermen van vertrouwelijke gegevens betreft.

De juridische aspecten rondom digitale handtekeningen ('Hoever gaat de aansprakelijkheid van een organisatie die de sleutels beheert?') en digitale certificaten zijn bewust buiten het artikel gehouden. Nadere informatie hierover is onder andere bij ECP.NL te vinden⁴.

PGP wordt wereldwijd door miljoenen mensen gebruikt en het aantal informatiebronnen over deze technologie op het internet is dan ook zeer uitgebreid. De belangrijkste en meest bruikbare informatiebronnen zijn voor u verzameld op <http://www.nedsecure.nl/pgp/index.htm>.

<over de auteur>

Leon Kuunders is als security consultant en

managing partner werkzaam bij NedSecure Consulting.

leon.kuunders@nedsecure.nl

is echter slechts een adviesorgaan voor VN-organisaties en kan derhalve alleen aanbevelingen doen over welke stappen deze organisaties zouden moeten ondernemen. Tijdens de conferentie komen onderwerpen aan bod zoals het opstellen van een gemeenschappelijk juridisch raamwerk voor het omgaan met internetcriminaliteit en hoe om te gaan met privacy-issues op het internet.

<bron>

www.computerworld.com

juiste condities voor het ontwikkelen van veelalige content voor draadloze diensten. Tevens zullen de EC en de Raad van Europa samenwerken aan een samenhangende Europese strategie voor de beveiliging van computernetwerken en de implementatie daarvan. In juni zal deze strategie door de regeringsleiders worden gepresenteerd tijdens de Europese top in Göteborg, juni dit jaar.

<bron>

www.automatiseringsgids.nl