



VEILIGHEIDSMAAATREGELEN IN EN MET SOFTWARE (2)

DERRICK GOSSELIN

Refererend aan het veiligheidsmodel (zie A&B 85/7) noemen we beveiliging met software die maatregelen die vallen binnen het gebied van de accesscontrole. Dit betekent enerzijds de actieve accesscontroles en anderzijds de cryptografie.

VEILIGHEIDSMAAATREGELEN MET SOFTWARE

De actieve accesscontroles

Actieve accesscontrole software wordt gerealiseerd door een groep programma's die op basis van een op voorhand opgestelde toegangsautorisatie, toegang verlenen tot specifieke gegevensobjecten, bestanden, programma's,....

Het voorwerp van bescherming kan worden genomen op het niveau van records, files of bestanden; op het niveau van programma's of op het niveau van de periferie-apparatuur zoals terminals, printers,...

Het onderwerp dat toegang kan krijgen omvat zowel personen, programma's als periferieapparatuur.

Het belangrijkste kenmerk waaraan accesscontrole software moet voldoen is beperkte toegang verlenen aan een combinatie van parameters. Zo moet beveiliging mogelijk zijn: per onderwerp dat toegang kan krijgen vanaf een specifieke plaats waar het onderwerp dat toegang vraagt zich bevindt; voor een specifieke functie van dit onderwerp en dit gedurende een welbepaalde tijd.

Het grootste probleem bij de accesscontrolesoftware is het feit dat deze hoofdzakelijk afhankelijk is van de constructeur en als dusdanig integraal deel uitmaakt van de

computerarchitectuur. Gezien een computer niet geselecteerd wordt op basis van accesscontrolesoftware moet men zich meestal tevreden stellen met wat de constructeur levert.

De mogelijkheid bestaat natuurlijk om zogenaamde security software pakketten aan te kopen, maar ook hier is men beperkt tot deze welke compatibel zijn met het bestaande systeem.

De meest gekende onder deze security software pakketten zijn RACF (Resource Access Control Facility) van IBM en ACF2 (Access Control Facility) van de Cambridge system group. Beide pakketten zijn geschreven om gebruikt te worden op IBM machines.

Gemeenschappelijk bij alle accesscontrole software is het uitvoeren van enerzijds de accesscontrole en anderzijds de access auditing.

De accesscontrole functie controleert de toegangscontrole tot de systeemgegevens en data bases op basis van toegangsregels die vooraf zijn vastgelegd.

Pogingen om toegang te krijgen tot het systeem worden onderschept, gecontroleerd op hun correctheid, toegangsautorisatie, ... Op basis van deze controles wordt er al dan niet toegang verleent tot de gevraagde informatie. De password protectie speelt hierbij een belangrijke rol.

De systeemauditingfunctie zal alle pogingen tot het overtreden van de vooropgestelde toegangsregels rapporteren. Bovendien worden ook alle toegangen en toegangspogingen geregistreerd en alle wijzigingen of pogingen tot het aanbrenge van wijzigingen aan systeeminformatie.

Problemen bij password protectie

De eigenschappen van een pass-

word zijn dat ze enerzijds moeilijk moeten te decoderen zijn (door het proberen van karaktercombinaties) en anderzijds voldoende kunnen worden herinnerd zonder ze te moeten neerschrijven. Het is evident dat beide vereisten in tegenstelling staan tot elkaar. Studies hieromtrent hebben uitgewezen dat het meest efficiënte formaat van een password bestaat uit een combinatie van vier tot vijf alfanumerieke karakters (9).

Een ander probleem in verband met passwords is de toekenning ervan. In principe is het zo dat enkel de computer en de gebruiker het password mogen kennen. Deze benadering heeft echter een aantal fundamentele nadelen. Vooreerst zal de gebruiker een password kiezen dat voor hem enige betekenis heeft (zoals zijn geboortedatum, naamafkortingen, enz...). Dit betekent dat iedere persoon die het individu wat kent reeds veel kans heeft om zijn password te ontcijferen. Bovendien is het zo dat, wil men een efficiënte beveiliging hebben met een password, men dit regelmatig moet veranderen. Indien de keuze van een password bij de gebruiker blijft, zal hij het meestal niet veranderen. Laatste probleem: het feit dat een gebruiker zijn password kan vergeten. Dit is des te meer het geval als men niet continu met het systeem werkt.

Teneinde deze nadelen op te vangen kan men het kiezen van een password overlaten aan een centrale administratie, die de passwords genereert, verdeelt en onderhoudt.

De behoefte om een password regelmatig te veranderen werd onderzocht door professor Lance Hoffman. Hij ontwikkelde terzake een formule die bepaalt om de hoeveel tijd een password dient te worden veranderd wil het als veilig worden beschouwd (10): ▶

$$T = \frac{A^s \times R \times E}{2}$$

T = de veiligheidsperiode van het password.

A = de grootte van het alfabet waaruit de karakters van het password gekozen kunnen worden.

s = de lengte van het password.

R = de transmissiesnelheid van de communicatielijns.

E = het aantal karakteruitwisselingen bij de log-in procedure.

De formule van Hoffman, opgesteld vanuit het standpunt van een vrijwillige poging om een password te breken, geeft duidelijk aan dat de beschermtijd van een password T zeer snel toeneemt met de grootte van het alfabet A en met de lengte van het password s zelf. Bovendien wordt de beschermtijd sterk verminderd bij trage transmissie R en bij weinig informatie-uitwisselingen E bij het inloggen.

In de praktijk gaat men meestal de Hoffman beschermtijd T van een password halveren omdat naast opzettelijke pogingen om een password te breken, er ook toevallige oorzaken kunnen zijn waardoor een password bekend kan worden. We nemen dus aan dat beide oorzaken een gelijke kans van optreden hebben. Indien dus de formule een periode van 14 maand oplevert waarbinnen een password moet worden veranderd, zal het password om de 7 maanden moeten worden gewijzigd.

De cryptografie

De veiligheidsbarrières op het laagste niveau, namelijk op het niveau van de gegevens zelf, wordt gerealiseerd door de cryptografie. De cryptografische technieken worden toegepast teneinde enerzijds bij communicatie of informatie - overdracht erop toe te zien dat

de informatie-inhoud bij eventuele aftapping niet bruikbaar is voor derden en dat bovendien de authenticiteit van de berichten gewaarborgd kan worden. Immers, de toegang tot een informatiesysteem is niet beperkt tot de periferie-apparatuur. Het is evident dat wanneer men informatie overstuurt langs elektromagnetische weg (kabel of straalverbinding) men kans loopt op aftakking.

Anderzijds zorgen deze cryptografische software pakketten ervoor dat wanneer een faling zou optreden van de accesscontrole software en een niet-geautoriseerde gebruiker toch toegang krijgt tot het systeem de gegevens in zo'n vorm zijn opgeslagen dat ze onbruikbaar zijn. De cryptografie bestaat essentieel uit twee bewerkingen: encryptie of het omzetten van de oorspronkelijke tekst in een geheimschrift en decryptie, de omgekeerde bewerking.

Het principe van de cryptografie steunt op een aantal algemene gekende wiskundige operaties (algoritmen) in combinatie met een geheime sleutel (11,12,13). Deze algoritmen kunnen zowel in hardware als in software worden uitgevoerd. De keuze hieromtrent is afhankelijk van de transmissiesnelheid. Hoge transmissiesnelheden vereisen cryptografische methoden uitgevoerd in hardware, als men niet noemenswaardig lang wil wachten. (14)

Momenteel bestaat er geen enkel industrieel algoritme dat tergelijktijd praktisch is en waarvan de veiligheid bewezen is (15).

Het is evenwel zo dat de relatieve veiligheid of de minimumtijd om een boodschap te breken in relatie staat met de lengte van de encryptiesleutel. Hoe korter deze sleutel des te kleiner is de veiligheid. De meeste industriële systemen verei-

sen slechts een relatieve veiligheid van enkele dagen tot enkele jaren, uitzonderingen achterwege gelaten, zoals b.v. de medische wereld waar men een relatieve veiligheid vereist van minimum 70 jaar! Twee types van cryptografische pakketten zijn momenteel op de markt beschikbaar: de symmetrische en de asymmetrische of publieke sleutel-systemen.

De meeste van deze symmetrische pakketten zijn gesteund op de DES standaard (Data Encryption Standard) (16). Ze worden symmetrisch genoemd omdat zowel de encryptie als de decryptie met een unieke sleutel gebeurt. Dit systeem heeft het nadeel dat de sleutel bewaard wordt door het systeem.

De nieuwste ontwikkelingen op het vlak van de encryptie-technieken maken gebruik van de zogenaamde publieke sleutels. Dit systeem maakt gebruik van twee sleutels per gebruiker. De eerste sleutel wordt gebruikt voor de encryptie, de andere voor decryptie. De encryptiesleutel wordt gedeponereerd in een publiek toegankelijke databank, terwijl de ander privé wordt gehouden. Wanneer twee gebruikers met elkaar willen communiceren zal de eerste gebruiker zijn boodschap encrypteren met de publieke encryptiesleutel van de andere. De ontvanger zal het bericht dan decrypteren met zijn privé-sleutel. Dit systeem biedt een zeer hoge betrouwbaarheid omdat het systeem enkel nog de encryptiesleutel bevat die toch publiek gekend is.

De meest gekende publieke sleutel - algoritme is dat van Rivest-Shamir-Adleman of het RSA algoritme (17).

Te nemen maatregelen bij cryptografie

De invoering van cryptografie

moet sterk worden overwogen. De risicoanalyse kan hier zeker een antwoord op geven.

Vooreerst kunnen er instabiliteitsproblemen optreden bij het gebruik van cryptografie.

Veiligheidsmaatregelen moeten worden genomen tegen het uitstralen van informatie die in ongecodeerde vorm verstuurd wordt langs elektromagnetische weg. Het afschermen van de toestellen is dus aangeraden.

De geheime decryptiesleutel moet veilig worden bewaard en beschermd tegen ongeautoriseerde kennisname. Bovendien moet de plaats waar de oorspronkelijke gegevens zich bevinden sterk worden bewaakt en alle data moeten zo snel mogelijk worden gecodeerd. Het principe is hier dat de encryptie zo dicht mogelijk bij de bron moet gebeuren.

Men moet ermee rekening houden dat encryptie zeer tijdrovend is en bijgevolg duur. Het encrypteren van grote volumes van data is momenteel financieel onhaalbaar indien het algoritme in software is uitgevoerd.

Het laten lopen van een RSA-algoritme op een IBM 370 machine vraagt een CPU tijd van ongeveer (18):

$$T = BL \times KL \times 0.005$$

Hierin is T de CPU tijd in seconden, BL totale te coderen tekst in bytes en KL lengte van de encryptiesleutel.

Nemen we een sleutel van 100 getallen of 42 bytes en een tekst van drie A4 pagina's (zijnde 6000 bytes) dan wordt de nodige CPU tijd bij benadering geschat op 21 minuten! Nemen we een kost van 1.000 BF per minuut CPU tijd, dan kost de encryptie van drie pagina's tekst ons niet minder dan 21.000 BF!

VEILIGHEIDSMATREGELEN BIJ HET GEBRUIK VAN MICROCOMPUTERS

Als gevolg van de inschakeling van microcomputers en de verbinding van microcomputers met mainframe computers, kan een organisatie niet langer meer alleen steunen op de procedures uitgewerkt om de veiligheid van grote centrale systemen te waarborgen.

Het toenemend gebruik van microcomputers resulteert in de meeste organisaties in een waaier van verschillende apparatuur, software, programmatie-activiteiten en gedecentraliseerde gegevens en software opslag.

De mogelijkheden om gegevens op te vragen, te stockeren en te wijzigen komen meer en meer in handen van de gebruiker. De organisatie als geheel heeft dan ook de neiging om hierover de controle te verliezen. De kwetsbaarheid van de organisatie neemt toe en deze is vele malen groter bij een veelvuldig ongecontroleerd gebruik van microcomputers dan bij de klassieke gecentraliseerde informatiesystemen.

Redenen voor deze verhoogde kwetsbaarheid zijn te vinden in de wijziging die het informatiebeheer ondergaat t.g.v. de microcomputer. In een mainframe-omgeving is er een duidelijke functiescheiding tussen programmeurs, systeemanalisten,... omwille van interne controles.

Bij het gebruik van microcomputers verdwijnt meestal dit onderscheid omdat de gebruiker zelf veelal deze functie uitoefent. Een microcomputer-gebruiker zal nu meestal niet dezelfde discipline vertonen en procedures volgen zoals dit gebeurt bij grotere systemen.

Meestal is er een gebrek aan systeemdocumentatie, worden geen sterke controles uitgevoerd bij het wijzigen van programma's, backup en recovery procedures bestaan meestal niet,...

Naast deze problemen van organisatorische en methodologische aard heeft men bovendien het probleem dat de operatingsystemen op microcomputers te zwak zijn om voldoende toegangsbeveiliging en bescherming te bieden wat de gegevens en de programmatuur betreft. Omwille van het feit dat de technische kennis om een microcomputer te bedienen veel kleiner is dan voor een mainframe systeem kunnen ook meer personen toegang krijgen tot het systeem.

Te nemen veiligheidsmaatregelen: Bij het gebruik van microcomputers moet men er vooreerst voor zorgen dat er backup- en recovery-procedures aanwezig zijn. Men moet ervoor zorgen dat er steeds een kopie is van de bestanden die men opgebouwd heeft.

Deze backups zijn zeer belangrijk vermits door het indrukken van een verkeerde toets, of door het morsen van koffie op een diskette, of door het uitvallen van de stroom maanden werk kunnen worden vernietigd. Het probleem is des te acuter wanneer een microcomputer door meer gebruikers gedeeld wordt en de gegevens op een gemeenschappelijke disk staan. Verkeerde manipulatie door een van de gebruikers kan de hele harddisk uitvegen.

Men mag niet vergeten dat de operatingsystemen te zwak zijn uitgebouwd om u te beschermen tegen dergelijke zaken. Het is nodig dat een backup wordt genomen van alle bestanden en dat deze wekelijks wordt hernieuwd, terwijl dagelijks een backup wordt genomen van

het werk dat gedurende de dag is gepresteerd. Het regelmatig 'saven' van de werkzaamheden dient tevens te gebeuren (om de tien minuten in een werkomgeving als beveiliging tegen stroomuitval).

De totale backup dient minimaal zes weken te worden bewaard en moet worden ondergebracht in een brandvrije kluis.

Het belang van backup bij microcomputers is evenredig met de kracht van deze microcomputer.

Een tweede belangrijk punt bij het werken met microcomputers is het verzorgen van de documentatie. Een nauwkeurige beschrijving van de programma's en gegevens moet hier gebeuren zodat bij afwezigheid van de hoofdgebruiker zijn werk niet volledig nutteloos wordt voor anderen.

Niet alleen de eigen documentatie is van belang maar ook dient men toe te zien op de kwaliteit van de verstrekte documentatie bij aan-

koop van software pakketten. Deze documentatie kan sterk in kwaliteit verschillen van softwarehuis tot softwarehuis. Gezien de sterke concurrentiemarkt waarop deze softwarehuizen werken moet men er tevens rekening mee houden dat vele van deze huizen binnen afzienbare tijd zullen verdwijnen.

Een derde belangrijk punt bij het gebruik van microcomputers is de beveiliging van de hard- en software.

Men dient erop toe te zien dat alle disketten write-protected zijn wanneer ze gedurende een zekere tijd niet meer gebruikt zullen worden. Dit dient in ieder geval te gebeuren met de backup-disketten.

Wegens de niet voldoende uitgebouwde operating-systemen en bijgevolg het gebrek aan access controle software moeten alle gegevens met een confidentieel karakter op disketten bewaard worden en nooit worden achtergelaten

op het massageheugen (harddisk). Indien men dit wel doet is deze informatie niet meer beschermd tegen wijziging, kopiëren of kennisname door niet geautoriseerde gebruikers.

De toegangsbeveiliging van microcomputers kan evenwel gebeuren door het aanbrengen van speciale sloten die bv. met een fysieke sleutel de spanning afgrendelen enz... (19)

Ook kan men speciale software pakketten installeren die password protectie leveren, beveiliging tegen het kopiëren van bestanden, toegangsbeveiliging tot harddisk en cryptografie (DES en RSA).

De meeste van deze software pakketten werken onder MSDOS operating systeem en vragen een geheugencapaciteit van 48 tot 128 Kbyte. Hun prijs varieert tussen de 5.000 BF en de 20.000 BF (20).

Referenties

- O'Gardy, C. en Ross, S., 'Passwords, Frequency of change and its Impact on Data Security', *Computer Security*, N.9 (1977).
- Hoffman, L., *Modern Methodes of Computer Security and Privacy*, Englewood Cliffs N.J., Prentice-Hall, 1977.
- Helleman, M., 'Mathematics of Public key Cryptography', *Scientific American*, Vol.241, N.2.
- Pritchard, J.A.T., *Data Encryption*, N.C.C. Publications, The National Computing Centre Limited, Manchester, 1980.
- Knuth, D., *Seminumerical algorithms*, Vol.2, Readings M.A., Addison-Wesley, 1981.
- Mokhoff, N., 'Communication I.C.'s', *IEEE Spectrum*, jaarg.19, N.1 (1982), pag. 41-42.
- Desmedt, Y., Govaerts, R., Vandewalle, J., 'Industriële Cryptografie : Noodzakelijke bescherming van informatie tegen misbruik en vervalsing', *Het Ingenieursblad*, jaarg.52, nr.1 (1983), pag. 17-23.
- Diffie, W. en Hellman, M.E., 'Exhaustive cryptanalysis of the N.B.S. Data Encryption Standaard', *Computer*, jaarg.10, nr.6 (1977), pag. 74-84.
- Rivest, R., Shamir, A. en Adleman, L., 'Method for obtaining digital Signatures and Public-key Cryptosystems', *Communications of the A.C.M.*, Vol.21, nr.2, Feb. 1978.
- The inner circle*, Vol.1, nr.3, Publikatie van de Circle Software Corp.
- Rhodes, B., 'Micro Security that makes sense', *Computer Decisions*, mei 1985, pag. 72-85.
- Reel, N., 'Data Security : Can Your Computer Keep a Secret ?' *Computing for Business*, April 1985, pag. 32-35.