UNIVERSITY OF JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

- NonCommercial — You may not use the material for commercial purposes.

- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

Surname, Initial(s). (2012) Title of the thesis or dissertation. PhD. (Chemistry)/ M.Sc. (Physics)/ M.A. (Philosophy)/M.Com. (Finance) etc. [Unpublished]: University of Johannesburg. Retrieved from: https://ujdigispace.uj.ac.za (Accessed: Date).

NEL

NETWERKSEKERHEID.

deur

ABRAHAM JACOBUS NEL

verhandeling

voorgelê ter vervulling van die

vereistes vir die graad

MAGISTER IN DIE EKONOMIESE EN BESTUURSWETENSKAPPE

in

INFORMATIKA

aan die

RANDSE AFRIKAANSE UNIVERSITEIT.

STUDIELEIER : PROF. J.H.P. ELOFF.

FEBRUARIE 1991.

TITLE : NETWORK SECURITY.

AUTHOR : A.J. NEL.

SUPERVISOR : PROF J.H.P. ELOFF.

DEGREE : M.COM.

DEPARTMENT : COMPUTER SCIENCE.

LANGUAGE : AFRIKAANS.

SUMMARY.

Networks and data communications are two fields of the computer industry that show the biggest growth in terms of new technology and software. Organizations and other users of computers and computer equipment want to have access to their information at all times and from where ever they are. The only way to achieve this, is to interconnect computers with the use of networks and telecommunication.

This increased use of networks and data communications by the public sector leads to the need for better security measures to protect the data and information on the networks . Although there are some aspects of general computer security and network security that apply to both fields, there are also a lot of problems that are unique to network and communications security. One of the main problems in the development of security measures for networks is the different standards and architectures that are used by manufacturers of computer and network equipment. Because of this the need arises for the development of universally accepted standards for the manufacturing of computer and network equipment as well as standards for software development.

The aim of this dissertation was to study the unique features, security problems and security measures of computer networks and data communications.

The following is a synopsis of the the chapters in the dissertation :

Chapter 1 forms an introduction and gives an overview of problems in the general computer security and network security fields. Definitions for networks and network security are developed for use in the rest of the dissertation. Finally a possible framework for the rest of the study is set defined.

In **chapter 2** an overview is given of the Open System Interconnection(OSI) model of the International Standards Organization(ISO). Special attention is given to the Security Addendum, as well as the use of security perimeters.

Chapter 3 deals with interconnection between networks. An overview is given on existing interconnection technology and methods like bridges, routers and gateways and the impact they have on network security.

Chapter 4 addresses issues on management and control of network and inter-network rights. The Access control list and Access control matrix is discussed as well as the Path-context-model as a possible new approach to be used in network security.

In **chapter 5** an overview is given of communications media. A wide range is discussed from twisted pair cable, to optical fibre and the use of cellular telephone technology in computer networks. The different media are evaluated on general as well as security related characteristics.

Chapter 6 deals with access control. The different ways of identifying users when they attempt to log onto the network are discussed. More traditional approaches like passwords are discussed as well as new developments in biometric identification methods such as speech and retina pattern recognition. Finally Access port protection is discussed as well as the use of modems in a network.

In **chapter 7** an overview of cryptography is given. The discussion consists of a short overview of the Data Encrytion Standard(DES) and Public Key Cryptography. Next the placement of encryption in the network is discussed, as well as the problem of Key management. Finally the evaluation of cryptographic equipment is discussed.

Chapter 8 deals with the development of a methodological approach to the implementation of network security. The RS-methodology developed at the Rand Afrikaans University is discussed and extensions are made to the existing methodology. These extensions addresses issues regarding the development and implementation of network and communications security measures in an organization.

In **chapter 9** topics for future study are addressed.

INHOUDSOPGAWE.

HOOFSTUK 1.

INLEIDING.

1.1 Inleiding.

Netwerke en datakommunikasie is van die velde wat die vinnigste ontwikkel in die rekenaarbedryf. Die probleem is dat die tegnologiese ontwikkeling besig is om die sekerheid en bestuursaspekte van netwerke en datakommunikasie agter te laat. 'n Voorbeeld wat hier genoem kan word, is die gebruik van sateliet- en radioverbindings as kommunikasiekanale. Die probleem hier is dat die kommunikasiekanale oop is en baie maklik onderskep kan word.[9] Dit is maar een van die baie probleme wat veroorsaak word deur die beskikbaarstelling van nuwe tegnologiese ontwikkelings in die netwerk en datakommunikasieveld.

Die probleem word heelwat vererger deur die gebruik van Lokaleareanetwerke(LANs) en Wyeareanetwerke(WANs). Dit stel die gebruiker in staat om met feitlik enige rekenaar toegang tot 'n netwerk te verkry. Verder word verskeie van die netwerke aanmekaar gekoppel wat gewone rekenaarsekerheidsmaatreëls baie meer ingewikkeld maak.

Dus is ons besig om as gevolg van tegnologiese ontwikkeling te beweeg vanaf die huidige toestand na 'n tegnologies meer gevorderde toestand in die toekoms. Die veranderings in tegnologie beïnvloed die netwerksekerheids- en netwerkbestuursomgewing op verskillende maniere. Die invloed word nie altyd deeglik besef nie, en word baie min bestudeer. So byvoorbeeld, wat is die impak van "Electronic Data Interchange" op netwerksekerheid?

Die doel van hierdie verhandeling is om juis die invloed van nuwe tegnologie in die netwerkomgewing te bestudeer. Deur bestudering van bestaande sekerheidsmaatreëls en meganismes, kan bepaal word watter addisionele stappe geneem kan word indien bestaande stappe nie voldoende is nie. Om die invloed te bestudeer, moet daar eers gekyk word na die bestaande probleme in die netwerksekerheidsveld, bestaande netwerktegnologie, en die invloed wat bestaande tegnologie daarop het.

Hoofstuk een bestaan verder uit die volgende paragrawe :

1.2 Rekenaarsekerheidsprobleem.
1.3 Benaderings tot netwerksekerheid.
1.4 Terminologie.
1.5 Doelwit van studie.

1.2 REKENAARSEKERHEIDSPROBLEEM.

Om 'n beter perspektief te kry van netwerksekerheid, kan gekyk word na probleme wat in die algemene rekenaarsekerheidsveld geïdentifiseer is. Laasgenoemde is geïdentifiseer deur middel van onderhoude met sekere ondernemings in Suid-Afrika wat baie van netwerke en datakommunikasie gebruik maak.[12][13]

- Virusse.

  Dit is 'n bedreiging wat al hoe ernstiger afmetings begin aaneem. Die probleem is dat die virusse al hoe meer gesofistikeerd en gevaarliker raak. Nuwe virusse word gewoonlik so ontwikkel om bestaande teenmaatrëels te omseil. Dus kan daar in die meeste gevalle eers iets gedoen word na die virus reeds die rekenaar besmet het.

  Gelukkig is die virusprobleem in Suid-Afrika beperk tot relatief skadelose soorte en kom dit feitlik sonder uitsonderings net op individuele rekenaars voor en nie op netwerke nie. In ander lande soos die V.S.A. is daar egter verskeie gevalle waar virusse netwerke aangeval het en groot skade aangerig het.[4] Dit dui daarop dat die probleem in SA in die toekoms baie sal vererger en dit het uit die gesprekke in [12] duidelik geword dat daar vroegtydig voorsorg geneem sal moet word.

- Netwerkargitektuur.

  'n Belangrike aspek van netwerksekerheid wat feitlik altyd buite rekening gelaat word, is die invloed wat netwerkargitektuur daarop het. Netwerkargitektuur dui op die spesifieke topologie soos byvoorbeeld 'n ster- of ringkonfigurasie. Die belangrikste kriteria wat 'n onderneming gewoonlik gebruik as hy tussen argitekture moet besluit, is die koste. Dit is egter belangrik dat hulle ook moet kyk na die invloed wat die argitekture op bestaande en beoogde sekerheid sal hê.

  Vir sekere argitekture is dit makliker om sekerheidsmaatreëls op te stel as vir ander. Byvoorbeeld 'n ster-argitektuur het 'n sentrale rekenaar wat kommunikasie tussen nodes beheer. Dus kan die sentrale rekenaar kontroleer of kommunikasie tussen die twee nodes mag plaasvind.

- Netwerk- en Internetwerkregte.

  In die meeste gevalle voorsien die bepaalde netwerkbedryfstelsel, bv NOVELL [94], reeds die fasiliteite om regte aan gebruikers toe te ken. Daar is egter in sommige gevalle addisionele maatreëls nodig om die regte te bestuur. Die belangrikste probleem ontstaan by internetwerkregte. In die meeste gevalle is daar verskillende netwerke wat aanmekaar gekoppel is. Daar moet 'n manier wees om regte tot individuele netwerke te beperk, maar in baie gevalle moet die regte ook tussen die netwerke oorgedra kan word.

- Aktiwiteitboekhouding.

  Dit is in die meeste gevalle nie genoeg om slegs gewone toegangsbeheer op netwerke toe te pas nie. Uit meeste van die gespekke, wat gevoer is met ondernemings waar netwerke gebruik word, het dit duidelik geword dat daar 'n metode moet bestaan waarvolgens al die aktiwiteite van die gebruiker tydens 'n sessie aangeteken kan word.[12]

  'n Sessie is al die aktiwiteite vandat die gebruiker aangeteken het totdat hy uitgeteken het. Al hierdie aktiwiteite behoort met soveel detail as moontlik in 'n boekhouding opgeneem te word wat dan deur die netwerksekerheidsadministrateur ondersoek kan word.

  Dit bring egter ander probleme mee. 'n Gebruiker moet nou baie duidelik gëidentifiseer en gewaarmerk word. Inligting wat in so 'n boekhoudingsfasiliteit opgeneem kan word, sluit in :
  - Pogings deur gebruiker om aan te teken.
  - Watter lêers en hulpbronne die gebruiker gebruik.
  - Watter ongemagtigde aksies hy probeer uitvoer.

  'n Belangrike vereiste is egter dat die stelsel so min as moontlik invloed op die reaksietyd van die netwerk moet hê en ook so min as moontlik van die netwerk se hulpbronne in beslag moet neem.

- Toegangstabelle/toegangsmatrikse.

  Die meeste sekerheidstelsels maak gebruik van toegangstabelle wat die regte tussen subjekte en objekte in die stelsel aandui. Objekte is byvoorbeeld lêers, programme en hulpbronne soos drukkers.

In netwerke en hoofraamstelsels is die tabelle geneig om egter onbeheerbaar groot te word, en moet daar na alternatiewe oplossings gesoek word.

- Fisiese sekerheid.

  Die beskerming van apparatuur is steeds 'n belangrike probleem by netwerke en ook ander stelsels. Hier kan ook ingesluit word die beskerming van media soos skyfpakke, drukstukke en rugsteun kopieë van data. Hier is fisiese toegangsbeheer van gebruikers tot die apparatuur en media nodig. Nog 'n belangrike aspek is die fisiese beskerming van kommunikasieverbindings.

- Inligtingsbestuur.

  Probleme wat hier ondervind word, is die neem van rugsteuning en rampherstel. Die beskerming van die rugsteuning en rampherstelprosedures is ook hier van toepassing.

- Poortbeskerming.

  Netwerke beskik oor verskeie verbindings met die buitewêreld deur middel van deurgangspoorte met ander netwerke en ook modems. 'n Deurgangspoort is die koppelvlak tussen twee netwerke. Die belangrikste probleem is egter modems en hoe om die gebruiker aan die anderkant positief te identifiseer. Die probleem met deurgangspoorte is om regte tussen die twee netwerke te kontroleer en oor te dra.

- Kommunikasieverbindings.

  Die kommunikasieverbindings in 'n netwerk is die mees kwesbaarste punt in 'n netwerk. Elke soort skakel beskik oor sekere voordele en nadele en oefen 'n baie groot invloed op die sekerheid van die netwerk uit. Tegnologie in die gebied ontwikkel vinnig en 'n studie van die tegnologieë en die invloed daarvan op netwerksekerheid is in die meeste gevalle in gesprekke genoem.

- Beskerming van data.

  Op netwerke, en veral LANs, beweeg daar groot hoeveelhede belangrike inligting wat beskerm moet word. Die voordeel van hoofraam netwerkstelsels is dat, as gevolg van massas data wat daar rondbeweeg, dit vir 'n indringer moeilik is om tussen bruikbare en waardelose inligting te onderskei.

LANs aan die anderkant, vervoer minder data en die inligting is ook meer verstaanbaar, soos bv bestuursverslae. Veral met die toenemende belangrikheid van "Electronic Data Interchange" of EDI, is die beskerming van data deur die hele netwerk van groot belang. Dit sluit in die geheimhouding, waarmerking en behoud van integriteit van die data.

- Risiko-ontleding en -bestuur.

  Risiko-ontleding en -bestuur vir individuele rekenaars en hoofraamrekenaars is reeds in baie gevalle bestudeer.[10] Die meeste ondernemings maak van die ontledings- en bestuurspraktyke gebruik vir netwerke. Daar is egter weer sekere kenmerke aan netwerke wat veroorsaak dat daar spesiale aandag aan spesifiek netwerke gegee moet word. Om maar net 'n paar probleme te noem:
  - Hoe betroubaar is die kommunikasieskakels wat deur die poskantoor voorsien word?
  - Watter moontlikheid is daar van rugsteunskakels soos mikrogolf- en satelietskakels?

- Rampherstel.

  Alhoewel rampherstel reeds baie bestudeer is, en rampherstelprodedures reeds ontwikkel is, is die probleem dat die prosedures gewoonlik vir 'n spesifieke geval of onderneming ontwikkel is. Daar is 'n behoefte aan die ontwikkeling van meer algemene rampherstelprosedures, wat ook netwerke insluit. Rampherstel sluit al die prosedures in wat nodig is om in die geval van enige ramp of beskadiging aan rekenaarstelsel en/of netwerk, die stelsel te herstel tot 'n vlak so na as moontlik aan die toestand voor die ramp.

Om 'n beter perspektief te kry van netwerksekerheid in die praktyk, het die gesprekke wat gevoer is in [12], gehandel oor rekenaarsekerheid in die algemeen. Die rede waarom die gesprekke oor algemene sekerheids probleme gehandel het, was omdat die skrywer wou bepaal wat die verband tussen probleme in algemene rekenaarsekerheid en netwerksekerheid is. So kan ook bepaal word in watter van die twee velde die meeste probleme lê, sonder om die gesprek spesifiek op netwerksekerheid toe te spits. Feitlik al die punte wat bespreek is, kan onder netwerksekerheid geklassifiseer word, en dus sal die res van die studie op netwerksekerheid toegespits word.

Voor daar voortgegaan word met die bestudering van netwerksekerheid, word daar eers gekyk na die volgende punte:

1.2.1 Wat is 'n netwerk?
1.2.2 Voordele van die gebruik van netwerke.
1.2.3 Rekenaarsekerheidsverwante probleme in netwerke.

1.2.1 Wat is 'n netwerk?

In die literatuur wat bestudeer is, is daar min ooreenstemming oor presies wat 'n netwerk is. Vervolgens sal 'n paar van die definisies kortliks bestudeer word, en dan sal 'n definisie, wat vir die res van die verhandeling sal geld, opgestel word.

Volgens AMSEL [1], is 'n netwerk 'n onderverbinding van stelsels en toestelle vir inligtingkommunikasie. Verder word die terme telekommunikasienetwerk en netwerk as ekwivalente terms beskou. Volgens hierdie definisie word telefoonkommunikasie en datakommunikasie omvat deur die enkele term telekommunikasie.

Volgens LOOMES [2], is 'n netwerk 'n reeks punte wat deur kommunikasiekanale gekoppel is.

LONG [3] beskou 'n netwerk en datakommunikasie as afstandsrekenaarapparatuur-toestelle, wat deur kommunikasiekanale verbind word.

Die ooreenkoms tussen die drie definisies is die verbinding van toestelle deur middel van kommunikasiekanale.

Vir verdere doeleindes, beskou die skrywer 'n netwerk as 'n versameling nodes wat deur middel van kommunikasiekanale aanmekaar verbind is in so 'n mate dat oordrag van inligting tussen die nodes kan plaasvind. Die verbinding moet van so 'n aard wees dat hulpbronne, soos byvoorbeeld databasisse en drukkers gesamentlik deur die nodes benut kan word. 'n Node kan enige rekenaarapparatuurtoestel wees en kan selfs 'n ander netwerk soos 'n lokaleareanetwerk (LAN) of wyeareanetwerk (WAN) wees.

1.2.2 Voordele en nadele van die gebruik van netwerke.

Daar bestaan verskeie voor- en nadele in die gebruik van netwerke, nl : [4][[2][3]

Die belangrikste voordele in die gebruik van netwerke is :

- Die deel van hulpbronne tussen nodes, soos databasisse, drukkers ens.
- Verhoogde betroubaarheid aangesien as een node faal, is daar nog ander wat werk.
- Werklas word versprei.
- Baie makliker om netwerk uit te brei deur net 'n nuwe node in die netwerk by te voeg.

In die literatuur wat bestudeer is, word daar in baie min gevalle van die nadele van die gebruik van netwerke gepraat. Vir die skrywer is daar egter 'n paar baie duidelike nadele waarvan die belangrikste die degradering van die algemene sekerheidsgraad van die rekenaarstelsels is. Spesiale netwerkprogrammatuur en -apparatuur is nodig. Die programmatuur en apparatuur is baie ingewikkeld en duur. 'n Netwerk het verder onderhoud nodig, en gebruikers moet opleiding ontvang om dit te gebruik. Dus is bedryfskoste van netwerke hoog.

1.2.3 Rekenaarsekerheids verwante probleme in netwerke.

Netwerke beskik oor spesiale kenmerke wat veroorsaak dat sekerheid op spesiale maniere beïvloed word. Dit is nodig om die kenmerke en die invloed daarvan op sekerheid kortliks te bestudeer. 'n Beknopte opsomming volg.[7][10][11]

- Deling van hulpbronne veroorsaak dat baie gebruikers potensieel toegang kan verkry op plekke waar toegang nie wenslik is nie. Dus is spesiale maatreëls nodig.
- Stelsel is baie kompleks en sekerheidsmaatreëls moet dus ook kompleks wees.
- Netwerke kan ook aan mekaar gekoppel word en dit is moeilik om te bepaal wat die invloed van sekerheid van een netwerk op ander sal hê.
- Op 'n netwerk is daar baie punte wat aangeval kan word, byvoorbeeld nodes en skakels.
- Daar kan baie roetes van een gasheer na 'n ander wees en elke roete lewer addisionele probleme op.
- As gevolg van die toenemende gebruik van netwerke om afstandstoegang tot rekenaarfasiliteite te gebruik, is dit vir indringers 'n makliker en aantrekliker teiken. Die hoeveelheid en waarde van die inligting wat verkry kan word as 'n netwerk binnegedring kan word, neem ook toe.

- Ontwikkeling van netwerktegnologie maak sekere aanvalle moontlik, bv monitor van radio- en satelietverbindings.

Literatuur bestudeer [10][11][61] dui aan dat potensiële netwerksekerheidsoortredings in drie hoofgroepe verdeel kan word :

- Ongemagtigde vrystelling van inligting:
  Byvoorbeeld toegang deur ongemagtigde gebruikers tot lêers.
- Ongemagtigde verandering van inligting:
  Byvoorbeeld bywerking van lêers deur ongemagtigde gebruikers.
- Ongemagtigde weerhouding van gebruik van hulpbronne:
  Byvoorbeeld die oorbelading van netwerk deur onbelangrike boodskappe.

1.3 BENADERING TOT NETWERKSEKERHEID.

Nadat netwerke in die algemeen, sowel as rekenaarsekerheidsverwante probleme in die netwerkomgewing kortliks bespreek is, word netwerksekerheid vir doeleindes van die studie as volg gedefinieer.

Netwerksekerheid bestaan basies uit twee dele, nl fisiese en logiese sekerheid.

- Fisiese sekerheid is die aksies wat fisiese beskadiging of binnedringing van die netwerk se hulpbronne verhoed, soos beskerming van verbindingspanele.
- Logiese sekerheid beskerm die data en ander inligting wat in die netwerk voorkom, soos weerhouding van toegang tot 'n program deur 'n ongemagtigde gebruiker. Verder sluit logiese aspekte ook in datakommunikasieaspekte, soos beskerming van die integriteit, weerhouding en ongemagtigde verandering van die inligting tydens transmissie.

  Logiese sekerheid beheer ook die toegang tot en tussen verskillende programme. Dit sluit in programme wat in geheel op een enkele terminaal of rekenaar uitgevoer word sowel as verspreide programme waar dele van 'n program tussen verskillende rekenaars of terminale versprei is.

Om kommunikasie in 'n netwerk veilig te maak en te beskerm, kan die volgende basiese doelwitte aan netwerksekerheid gestel word:

- Voorkoming van vrystelling van boodskap se inligting deur byvoorbeeld die boodskap te enkripteer.
- Voorkoming van verkeerontleding deur byvoorbeeld opvulling wanneer geen boodskappe deur netwerk gestuur word nie.

- Voorkoming van boodskapstroomontleding deur enkripsie van hele boodskapstroom.
- Opspoor van weerhouding van boodskapdiens deur byvoorbeeld reaksietyd van sekere transaksies te monitor.
- Opspoor van vals verbindingsopstelling deur byvoorbeeld identiteit van gebruiker gereeld te kontroleer.
- Voorkoming van terugtrekking van gestuurde of ontvangde boodskappe deur byvoorbeeld waarmerking en erkenning van ontvangs.

Een van die belangrikste benaderings tot netwerksekerheid, word beskryf in die netwerksekerheidsbylaag en die netwerkbestuursbylaag tot die "Open Systems Interconnection"(OSI) model van die "International Standards Organisation"(ISO). Die twee bylaes hierbo genoem, doen aanbevelings oor die insluiting van sekerheid en bestuurmaatreëls ten opsigte van netwerke in die OSI-model. [4] 'n Bespreking van die OSI-verwysingsmodel sowel as die sekerheids- en netwerkbestuursarigtekture sal in hoofstuk 2 gegee word.[61]

1.4 TERMINOLOGIE.

Vervolgens word daar 'n bespreking gegee van terminologie soos verder in die verhandeling gebruik :

- Elektroniese dataoordrag.

  Die Engelse term is "Electronic Data Interchange" (EDI). Die afkorting, EDI, sal verder gebruik word.

  EDI is 'n proses waarmee die uitruil van inligting, wat gewoonlik deur middel van handelsdokumente gedoen is, geoutomatiseer word. Die handelsdokumente sluit in onder andere administratiewe vorms, fakture , pryslyste, ensovoorts.

- Veselverspreide datakoppelvlak.

  Die engelse term is "Fiber Distributed Data Interface" (FDDI). Die afkorting, FDDI, sal verder gebruik word.

  FDDI is 'n standaard opgestel deur die Amerikaanse Nasionale Standaarde Instituut(ANSI), en handel oor die gebruik van optieseveseltegnologie vir die opstelling van 'n hoëspoednetwerk. FDDI is die standaard vir 'n 100MB/s optiesevesel "token-ring" netwerk.

- Geïntegreerdedienste digitalenetwerk.

  Die Engelse term is "Integrated Services Digital Network" (ISDN).Die afkorting, ISDN, sal verder gebruik word.

  ISDN is 'n beplande wêreldwye telekommunikasienetwerk wat 'n digitale diens sal verskaf vir funksies soos onder andere stem, data, faksimilee ens.

1.5 DOELWIT VAN STUDIE.

Die doel van hierdie verhandeling word saamgevat in die volgende drie punte :

- Netwerksekerheid en die invloed van nuwe tegnologiese ontwikkeling op netwerksekerheid. Aandag sal ten opsigte van sekerheidsaspekte van die volgende geskenk word :
  - Sekerheidsstandaarde
  - Internetwerkskakeling.
  - Kommunikasieverbindings
  - Poortbeskerming.
  - Kriptografie
- Deur die bestudering van bestaande sekerheidsmaatreëls en meganismes te bepaal watter addisionele stappe geneem kan word om bestaande sekerheid te verbeter, indien bestaande stappe onvoldoende is.
- Bestudering van netwerksekerheidsmetodologië vir die implimentasie van netwerksekerheid.

Die studie sal hom in hoofsaak bepaal by 'n literatuurstudie wat 'n oorsig gee van huidige tegnologie en prosedures in die veld van rekenaarsekerheid met besondere verwysing na netwerksekerheid en netwerkbestuur.

1.6 BEKNOPTE OORSIG VAN MOONTLIKE PUNTE IN DIE STUDIE.

Die volgende paragraaf bestaan uit 'n moontlike raamwerk en 'n beknopte oorsig van die moontlike beoogde inhoud van die studie. Daar sal gepoog word om soveel van die volgende punte as moontlik te dek.

1. OSI-standaarde.

   Die International Standards Organization (ISO), het die Open Systems Interconnection(OSI) model vir netwerkskakeling ontwikkel. Die ISO het die raamwerk uitgebrei deur bylaes te publiseer tot die OSI-standaard wat sekerheid en netwerkbestuur in netwerke in aanmerking neem. Volgens die bylae word sekerheidsdienste deur die netwerksekerheidsargitektuur verskaf. Die Netwerkbestuurs- argitektuur, as deel van sy funksionele model, skryf hulpmiddels vir die ondersteuning van sekerheidsdienste en meganismes voor.

   Hier sal die OSI verwysingmodel sowel as die sekerheidsargitektur bestudeer word.

2. Fisiese sekerheid.

   Hier kan gekyk word na die verskillende dele van 'n netwerk wat deur fisiese sekerheid beskerm kan word. Dit is 'n deel van sekerheid wat nie veel aandag geniet nie.

3. Kommunikasieverbindings.

   Bepreking van verskillende transmissiemediums wat as kommunikasieverbindings gebruik kan word. Elke soort verbinding het sekere eienskappe wat 'n invloed op netwerksekerheid kan hê. Dit is hierdie eienskappe wat hier bestudeer sal word. Bv :
   - Koaksialekabels.
   - Data-over-voice kommunikasiekanale.
   - Radioverbindings.
   - Digitaleverbindings.
   - Optiesevesels.
   - Mikrogolfverbindings.
   - Satelietverbindings.

4. Netwerkargitektuur.

Die verskillende netwerkargitekture wat bestaan sal hier bespreek word. Wat veral belangrik sal wees om te kyk na wat die kenmerke van die argitekture is, en wat die invloed van die bepaalde argitektuur op bestaande en beplande sekerheidsmaatrëels is. Daar sal verder in van die ander afdelings die moontlikheid van die gebruik van 'n sentrale toegewyde sekerheidsrekenaar genoem word. Die netwerkargitektuur kan 'n groot invloed hê op die plasing van so 'n rekenaar. Aandag sal veral aan die verskillende LAN-argitekture soos die ster, ring en bus gegee word.

5. Internetwerkregte.

Daar word al meer gebruik gemaak van skakelings tussen netwerke. Baie netwerke bestaan reeds uit 'n versameling van verskillede kleiner netwerke soos Lokalearea netwerke. Die probleem wat hier ontstaan, is gebruikers wat van een netwerk na 'n ander wil beweeg. Dit is moeilik om die gebruiker se aksies in 'n opeenvolgende netwerk te monitor. Verder bestaan daar probleme insake die geldigheid van 'n gebruiker se regte tussen die netwerke.

'n Oplossing wat hier bestudeer kan word, is die gebruik van 'n sentrale, toegewyde sekerheidsrekenaar, waardeur enige internetwerktransaksies uitgevoer moet word. Verder sal ondersoek ook gedoen word na die voorstel soos gedoen deur W.H. Boshoff en S.H. Von Solms[64]."Gateways" en ander metodes van internetwerkskakeling kan ook hier bespreek word, sowel as die gebruik van 'n internetwerkregte aktiwiteit boekhoudingsfasiliteit.

6. Aktiwiteitboekhoudingsfasiliteit

Hier sal die moontlike ontwikkeling van 'n aktiwiteitboekhoudingsfasiliteit bestudeer word. Daar sal bepaal word watter soortgelyke fasiliteite reeds bestaan, en hoe effektief dit is. Laastens sal 'n raamwerk vir 'n moontlike boekhoudingsfasiliteitstelsel opgestel word.

7. Poortbeskerming.

Die bespreking van verskillende metodes wat gebruik kan word om toegangspoorte te beskerm.. Wat van spesifieke belang is, is die bestudering van die verskillende soorte modemtegnologieë wat gebruik kan word. Bv :

- Inskakeltoegang.
- Terug-skakelmodems.

Verder sal daar ook gekyk word na koppelvlakke tussen netwerke soos bv :

- Toegangspoorte("gateways").
- Roeteerders.
- "Bridges"

8. Enkripsie

Enkripsie word vir verskillende dienste in sekerheid gebruik. Die volgende punte sal oorsigtelik bespreek word:

- skakelenkripsie.
- punt-tot-puntenkripsie.
- simmetriese enkripsie.
- assimmetriese enkripsie.
- kriptografiese "checkfunction"
- sleutelbestuur

9. Elektroniese handtekeninge.

Wat hier bestudeer kan word, is die hele beginsel van elektroniese handtekeninge. Die studie kan insluit die berekening van die handtekening, die verifiëring en uitruiling van die handtekeninge. 'n Belangrike aspek wat ook bestudeer kan word, is die koppeling van die handtekening met die boodskap of dokument.

10. Toegangsbeheer.

Hier sal metodes bespreek word wat gebruik kan word om gebruikers positief te identifiseer. Die doel is nie om in diepte in elke metode in te gaan nie, maar slegs om die voordele, nadele en betroubaarheid daarvan te bepaal.

11. Data-integriteit.

Hier kan metodes bespreek word wat gebruik kan word om te bepaal of daar op enige manier met boodskappe ingemeng is.

- "checksums"
- ordening en/of tydstempels

12. Voorkoming van verkeerontleding.

Hier sal metodes bestudeer word om te verseker dat die verkeer wat op die dataverbindings voorkom nie ontleed kan word nie. In sommige gevalle is boodskappe geënkripteer, maar kan deur ontleding van die protokol, datapakkie en verkeer , sekere afleidings gemaak word, byvoorbeeld :

- Verkeeropvulling.
- Enkripsie.

13. Roete-beheer.

Hier kan metodes bestudeer word om te verseker dat boodskappe met goedgekeurde roetes van oorsprong na bestemming beweeg.

14. Aantekening.

Hier word die roete wat die boodskap deur die netwerk beweeg aangeteken. In samewerking met roetebeheer, kan die boekhouding gebruik word om roetes te kontroleer en roetes wat problemé lewer, geïdentifiseer word.

15. Netwerkbestuur.

Hier sal netwerkbestuur kortliks bepreek word. Daar sal spesifiek gekyk word na die OSI se bylaag oor netwerkbestuur en daar sal dan veral aandag geskenk word aan die sekerheidsaspekte van netwerkbestuur en die invloed wat netwerkbestuur op netwerksekerheid het.

Die meeste aandag sal geskenk word aan die funksionele model wat deur die OSI voorgeskryf word. Die twee spesifieke areas van die model wat bestudeer sal word, is samestellingsbestuur en sekerheidsbestuur.

16. Netwerkrisikobestuur en ontleding.

Hier sal na die ontwikkeling van 'n algemene risikobestuurs en ontledingsprosedures vir rekenaarstelsels en netwerke gekyk word.

17. Netwerkrampherstel.

Netwerkrampherstelprosedures vir 'n onderneming wat van netwerke gebruik maak, is van die uiterste belang vir die doeltreffende voortbestaan van die onderneming. Hier sal die ontwikkeling van algemene rampherstelprosedures vir rekenaarstelsels en netwerke binne 'n onderneming gekyk word.

HOOFSTUK 2.

NETWERKSTANDAARDE.

2.1. INLEIDING.

As gevolg van die aanhoudende verlaging in pryse van rekenaartoerusting, die toenemende kragtigheid van die toerusting en die verbetering van mens-masjienkoppelvlakke, neem die gebruik van rekenaartoerusting baie vinnig toe. Dit veroorsaak 'n vinnige groei in die vervaardiging van verskillende rekenaar- en inligtingverwante toerusting. Die meeste van die vervaardigers van die toerusting maak van totaal uiteenlopende argitekture en protokolle gebruik. Met die toenemende gebruik van netwerke, wil die gebruiker al meer en meer van die heterogene toerusting aan 'n netwerk koppel. In baie gevalle maak selfs produkte wat deur dieselfde vervaardiger ontwikkel word, nie van dieselfde data-uitruilingskonfensies en datavoorstellings gebruik nie.

Die enigste oplossing vir die probleem is die daarstelling van 'n gemeenskaplike stel reëls waaraan al die vervaardigers van toerusting moet voldoen. Daar bestaan reeds verskillende sulke standaarde waaraan vervaardigers in meerdere en mindere mate gehoor gee. Twee van die mees bekendste standaarde is die "Open Systems Interconnection" (OSI) -verwysingsmodel van die "International Standards Organisation"(ISO), en die "Systems Network Architecture"(SNA) van die IBM-korporasie. [22][61] Die OSI-standaarde begin internasionaal al hoe meer aandag geniet, en verder sal slegs aan die OSI-standaarde gegee word.

Die probleem is dat die standaarde aan die begin nie vir sekerheid voorsiening gemaak het nie, en later in die vorm van bylae bygevoeg moes word, soos byvoorbeeld die sekerheidsargitektuurbylaag tot die OSI-argitektuur[61]. Voor daar verder gegaan word met die bespreking van die sekerheidsaspekte van die standaarde, sal daar eers gekyk word na die basiese OSI-verwysingsmodel. Die doel is nie hier om 'n volledige bestudering van die model te doen nie, maar slegs om die vlakke te identifiseer, te bepaal wat elke vlak se doel is, en te bepaal watter ISO-standaard vir die vlak ontwikkel is.

2.2. OSI-VERWYSINGSMODEL.

In 1978 het ISO begin werk aan die opstel van 'n nuwe argitektuur en familie van protokolle wat spesifiek ontwikkel word vir die gebruik in die verspreide inligting- en telekommunikasieveld. Die nuwe konsep staan bekend as die "Open Systems Interconnection" of OSI-model, en dien wêreldwyd as die hoeksteen van die rekenaarkommunikasieindustrie.[23]

OSI definieer 'n basiese stel van funksies wat in alle verspreide inligting en telekommunikasiestelselprodukte ingesluit moet word om te verseker dat die produkte met mekaar kan kommunikeer. Sedert 1978 is sekere van die OSI familie van standaarde reeds voltooi, terwyl ander voltooiing nader. Die belangrikste voltooide standaard is die OSI-Basiese Verwysingsmodel of ISO 7498.[24][61] Die model verdeel kommunikasiedienste in sewe vlakke, en definieer die koppelvlakke tussen die verskillende vlakke. Deur die standardisasie van die koppelvlakke tussen die vlakke, kan die vervaardigers van produkte verseker dat daar aanpasbaarheid bestaan tussen hulle en ander vervaardigers se produkte, wat aan dieselfde standaarde voldoen.[11][23]

Die OSI-model definieer die rëels en konfensies waaraan die dienste wat in elke vlak voorkom, sowel as die verwantskappe tussen die funksies, moet voldoen. Aangesien die OSI-verwysingsmodel slegs 'n model is, gee dit nie enige detail oor die implimentasie van die dienste of die intervlakkoppelvlakke nie. Dit dien net as 'n raamwerk vir die standaarde wat by elke vlak geïmplimenteer kan word.

Elke vlak het sekere dienste om te verrig. Die boodskap ontstaan op vlak 7 en word afgestuur deur die ander vlakke tot dit vlak 1 bereik. Deur die fisiese medium wat gewoonlik vlak 1 is, bereik die boodskap die ontvanger en beweeg die boodskap weer op in die vlakke tot by vlak 7.

Die sewe vlakke is as volg :

- Vlak een of fisiese skakelvlak.

  Die vlak het te doen met die transmissie van 'n ongestruktureerde bisstroom oor 'n fisiese skakel soos byvoorbeeld 'n elektriese kabel. Die vlak hanteer die meganiese en elektriese karakteristieke nodig vir die opstelling, instandhouding en afskakeling van die fisiese skakel. 'n Baie bekende fisiese vlakstandaard is die RS-232c standaard en IEEE standaarde IEEE 802.3 tot 802.5 en IS 2593. [24][25].

- Vlak twee of dataskakelvlak.

  Voorsien die betroubare oordrag van data oor die fisiese skakel. Versend blokke data of rame. Die belangrikste diens wat die vlak lewer is sinkronisasie, foutbeheer en vloeibeheer. 'n Belangrike dataskakelvlakstandaard is die HDLC- standaard. Die ISO-standaard vir die vlak is IS 8802. [24][25]

- Vlak drie of netwerkvlak.

  Voorsien boonste vlakke met onafhanklikheid van data-transmissie en skakelingstegnologieë wat gebruik word om stelsels te koppel. Die vlak is verantwoordelik vir die opstelling, behoud en onderbreking van koppelings tussen nodi in 'n netwerk. Die vlak hanteer dus die oordrag van inligting tussen rekenaars deur middel van 'n netwerk. Die X.25-standaard is 'n standaard wat vlak 1 tot vlak 3 saamvat in een standaard.[24][25]

- Vlak vier of transportvlak.

  Die vlak voorsien 'n betroubare meganisme vir die oordrag van data tussen twee rekenaars. Voorsien deursigtige en betroubare oordrag van data tussen eindpunte. Voorsien end-tot-end foutherstel en vloeibeheer. Die vlak is ook verantwoordelik vir die versekering dat die datapakkies in volgorde en sonder duplikasie of weglating die eindpunt bereik.

  Die grote en kompleksiteit van die transportprotokol hang af van die betroubaarheid van die onderliggende netwerk en netwerkvlakdienste. ISO het 'n familie van vyf transportprotokolstandaarde ontwikkel. Die standaard is ISO- standaard IS 8073. Elk van die vyf standaarde is ontwikkel vir 'n ander vlak van betroubaarheid. Klas 5 is vir die mees onbetroubare netwerke, en Klas 1 is vir die mees betroubaarste netwerke. [24][25]

- Vlak vyf of sessievlak.

  Voorsien die beheerstruktuur vir kommunikasie tussen toepassings. Beheer dus die dialoog tussen twee endstelsels. Verseker opstelling, behoud en onderbreking van koppelings(sessies) tussen samewerkende toepassings. Die dienste wat hier voorsien word is :
  Dialoogdissipline wat bepaal watter een van die endstelsels op 'n bepaalde oomblik data kan stuur. Groepering wat 'n boodskap opdeel in datablokke of pakkies. Herstel wat 'n kontrolepuntmeganisme voorsien vir herstel na 'n faling tussen twee kontrolepunte. Die twee ISO-standaarde vir die sessievlak is DIS 8326 en DIS 8327. [14][25]

- Vlak ses of voorstellingsvlak.

  Definieer die formaat van die data wat uitgeruil word tussen toepassings en voorsien 'n stel data omskakelingsdienste. Die vlak ontvang data vanaf die toepassingsvlak en skakel dit om na 'n standaardformaat van die data. 'n Voorbeeld is die aantal bisse wat gebruik word om 'n heelgetal voor te stel, kan verskil tussen programmeertale en die omskakeling van ASCII na EBCDIC. Die ISO-standaarde vir die vlak DIS 8822 en DIS 8823. [24][25]

- Vlak sewe of toepassingsvlak.

  Die toepassingsprogramme loop op die vlak.Die vlak voorsien ook die funksies wat die toepassingsprogramme benodig om die OSI-omgewing te kan bereik. Verder kom die algemenedoel toepassings soos lêeroordrag en elektroniese pos in die vlak voor.[25]

Figuur 2.1 is 'n diagrammatiese voorstelling van die sewe vlakke van die basiese OSI-verwysingsmodel.[23]

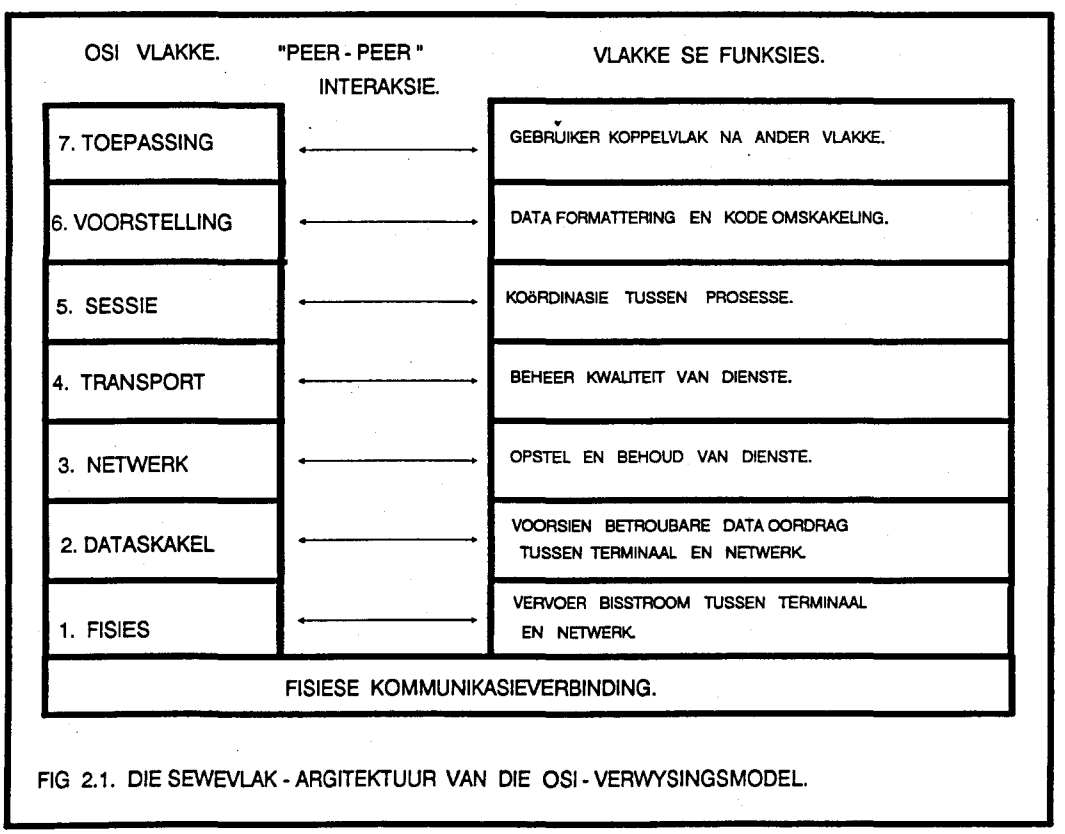


FIG 2.1. DIE SEWEVLAK - ARGITEKTUUR VAN DIE OSI - VERWYSINGSMODEL.

Die basiese OSI-verwyingsmodel het aan die begin nie voorsiening gemaak vir sekerheid nie. Dit het egter gou duidelik geword dat sekerheids- en netwerkbestuursaspekte ook in die standaarde opgeneem sal moet word. Dit het gelei tot die ontwikkeling van die ISO-Sekerheidsargitektuur, en die ISO-Netwerk bestuursargitektuur. In die res van die hoofstuk sal daar 'n kort bespreking van die twee argitekture gegee word.

2.3. OSI-SEKERHEIDSBUITELYNE.

Vir die beplanning, implementering en gebruik van sekerheid in 'n netwerk, kan gekyk word na die begip sekerheidsbuitelyne ("security perimeter"). Die sekerheidsbuitelyn is 'n logiese struktuur in 'n netwerk wat vergelyk kan word met 'n fisiese struktuur in 'n veilige gebou, soos byvoorbeeld 'n kluis in 'n bank. Die sekerheidsbuitelyn word getrek om 'n veilige gedeelte van die netwerk waar sekerheid verseker word deur middel van betroubare personeel of betroubare stelsels. Die oorhoofse doel van OSI-sekerheid, is om data te beskerm sodra dit buite die sekerheidsbuitelyne beweeg. Verlies van sekerheid binne 'n buitelyn word nie hier bespreek nie.[8][129]

Daar bestaan drie basiese sekerheidsbuitelyne wat elk verder bespreek sal word naamlik [8] :

- Sekerheidsbuitelyn om hele netwerk.
- Sekerheidsbuitelyn om elke gebruikersproses.
- Sekerheidsbuitelyn om boonste vlakke van OSI-model.

2.3.1. Sekerheidsbuitelyn om hele netwerk.

Hier word die sekerheidsbuitelyn om die hele netwerk getrek. Daar kan drie redes wees waarom die benadering gevolg word :

- Geen waardevolle of sensitiewe data in die netwerk.
- Geen bedryging bestaan in netwerk nie.
- Sekerheid word deur middel van nie-OSI metodes verseker.

Die benadering kan slegs gevolg word as al die persone en toerusting in die netwerk betroubaar("trusted") is. "Betroubaar" beteken dat geen beplande of onbeplande gebeurlikheid sal plaasvind wat die ongewensde openbaarmaking, modifikasie of verlies van data sal meebring nie.

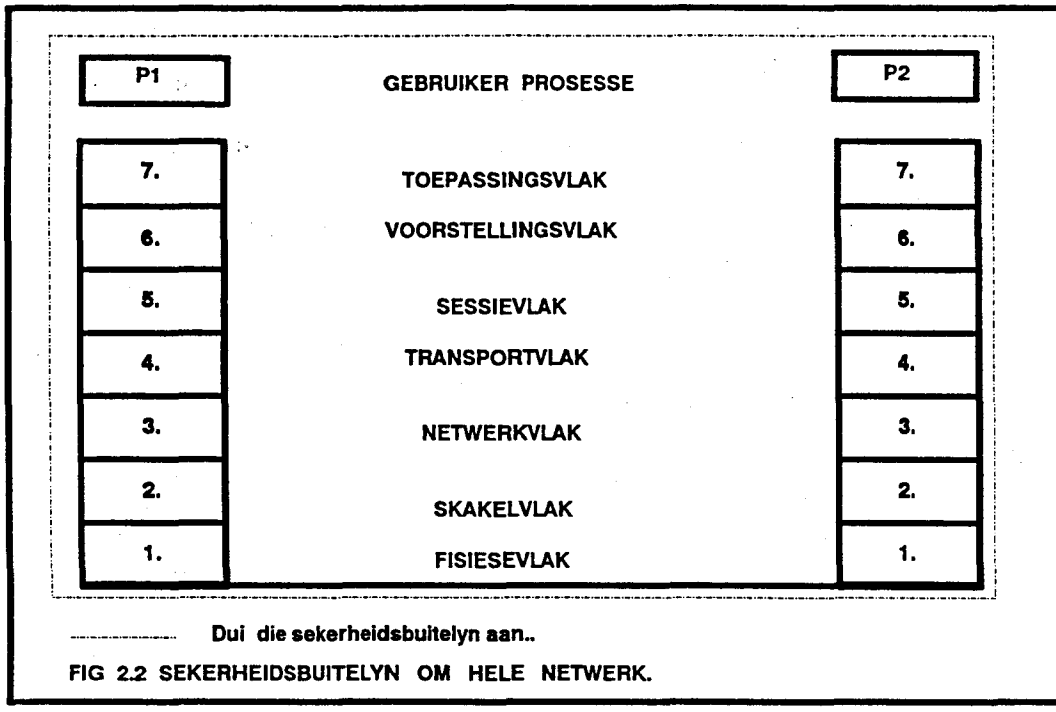


FIG 2.2 SEKERHEIDSBUITELYN OM HELE NETWERK.

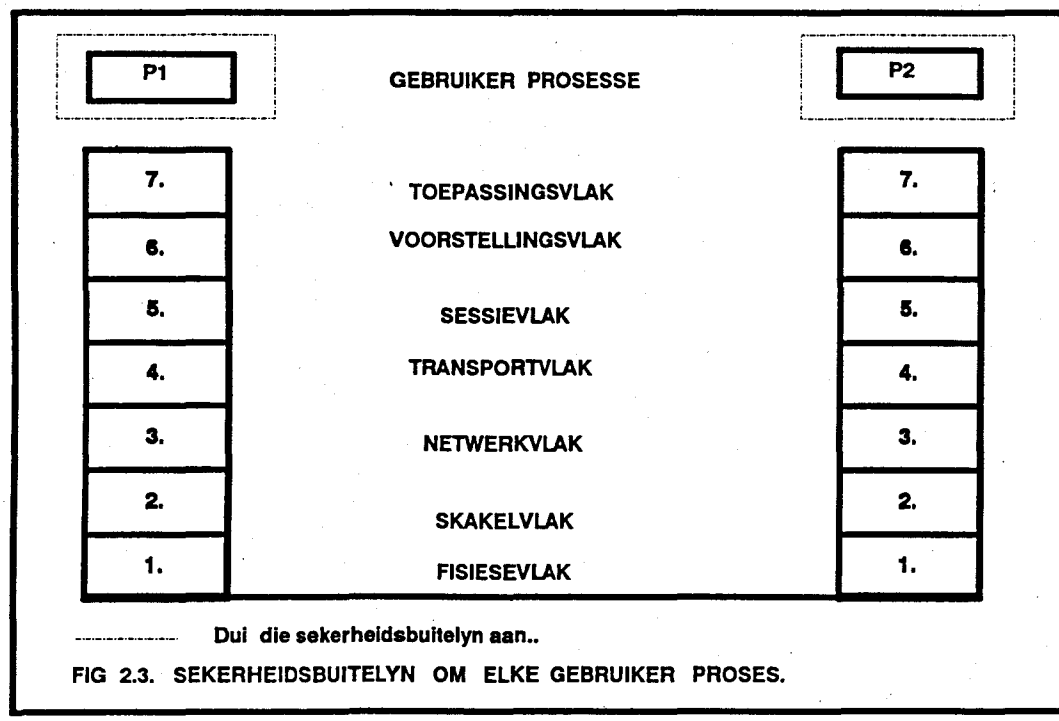


FIG 2.3. SEKERHEIDSBUITELYN OM ELKE GEBRUIKER PROSES.

Betroubaarheid kom in die praktyk op verskillende vlakke voor, byvoorbeeld die databasis is hoogs betroubaar, terwyl die kommunikasieskakels minder betroubaar is. In hierdie bespreking sal betroubaarheid slegs op twee vlakke aanvaar word as betroubaar of nie betroubaar nie. Sien Figuur 2.2 vir 'n diagrammatiese voorstelling.

2.3.2. Sekerheidsbuitelyn om elke gebruikersproses.

Hier word 'n sekerheidsbuitelyn om elke gebruikerproses getrek. Dit veroorsaak 'n hoë graad van afsondering aangesien elke proses sy eie beskerming voorsien, en die proses glad nie die OSI argitektuur moet vertrou nie. Die benadering bring egter mee, dat elke proses of program 'n volledige stel sekerheidsdienste moet implimenteer. Dit is wel moontlik om dit te doen, maar is teenstrydig met die idee van die OSI wat aanbeveel dat dienste in die verskillende vlakke van die argitektuur geplaas moet word, en nie in individuele prosesse nie. Sien Figuur 2.3 vir 'n diagrammatiese voorstelling.

2.3.3. Sekerheidsbuitelyn om boonste vlakke van OSI model.

In die laaste benadering word 'n middeweg tussen die twee vorige benaderings gevolg deur die buitelyn om die boonste vlakke van die OSI argitektuur te trek. Hier word die buitelyn by die Transportvlak (vlak vier), getrek. Sien figuur 2.4 vir 'n diagrammatiese voorstelling.

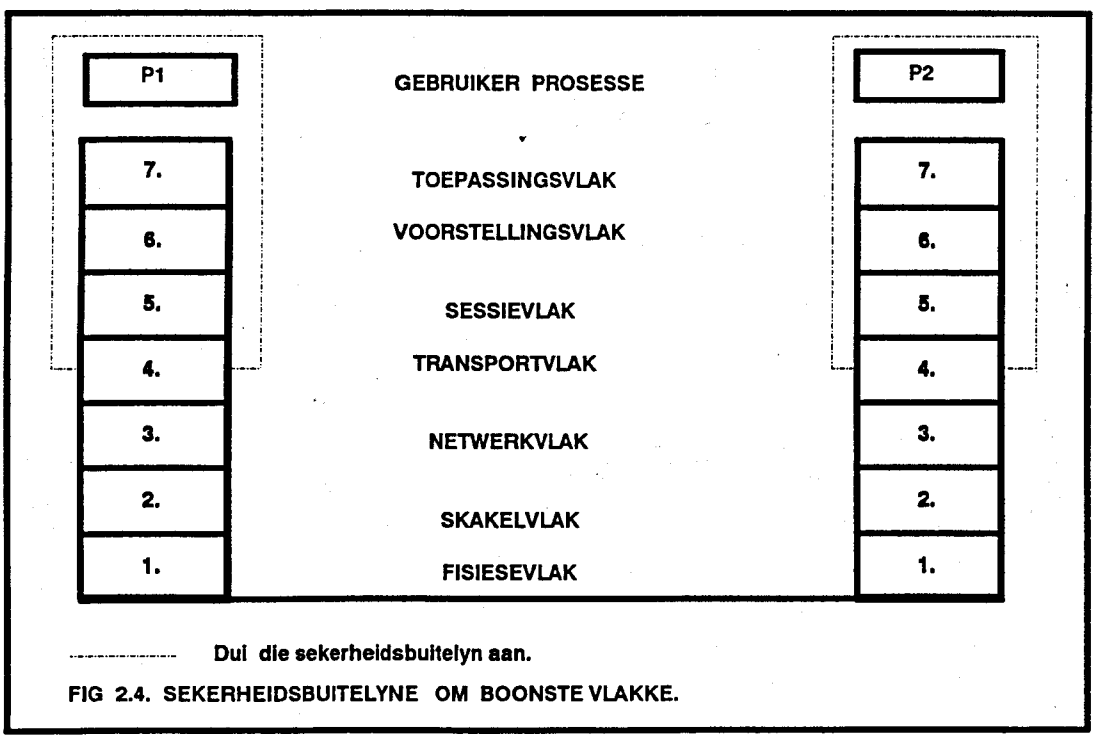


FIG 2.4. SEKERHEIDSBUITELYNE OM BOONSTE VLAKKE.

2.3.4. Onderhandelde sekerheid.

'n Doelwit wat aanbeveel word vir die implementering van sekerheidsdienste is dat die gebruikers soveel buigsaamheid as moontlik moet kry. Dit beteken dat 'n implimentasie die moontlikheid van onderhandeling tussen gebruikers moet voorsien, sodat die gebruikers saam 'n optimum stel sekerheidsdienste moet kan kies.

Die probleem wat egter hier ontstaan is dat sekere ondernemings 'n minimum vlak van sekerheid vereis, wat net deur sekere van die dienste bevredig kan word. Die minimum vereiste veroorsaak dat die ondernemings nie wil onderhandel oor sekere van die sekerheidsdienste nie. 'n Ander uiterste is dat ander ondernemings weer alle sekerheidsdienste wegonderhandel as die dienste die werking van die netwerk nadelig beïnvloed. So byvoorbeeld kan die afname aan reaksietyd wat die gebruik van die sekerheidsdienste veroorsaak, onaanvaarbaar wees. Die gebruikers kan dan besluit om van geen sekerheidsdienste gebruik te maak nie.

Die bruikbaarste oplossing is om van 'n uitbreibare argitektuur gebruik te maak wat die spesiale dienste insluit. Die argitektuur moet egter nie onaanvaarbare, oorhoofse koste veroorsaak vir die prosesse wat nie van die dienste wil gebruik maak nie.

2.4. OSI Sekerheids argitektuur.

In 1982 is 'n voorstel aan die ISO-komitee ISO/TC97/SC16/WG1 gedoen wat die komitee versoek het om 'n Sekerheidsbylaag tot die OSI-Verwysingsmodel te ontwikkel. In November is die voorlopige weergawe gepubliseer as ISO DP 7498/2 wat ook bekend staan as deel 2 van ISO 7498. In die meeste literatuur word die twee terms sekerheidsbylaag en sekerheidsargitektuur beide gebruik om dieselfde onderwerp te beskryf. [7][8][24] [26][28][61]

Die bylaag voorsien 'n algemene beskrywing van die sekerheidsdienste wat met die sewe vlakke van die ISO-verwysingsmodel geassosieer kan word. Verder word ook die meganismes om die dienste mee te implimenteer in die bylaag beskryf.

Volgens die bylaag is die dienste en meganismes ontwikkel om sekere bedreigings in die netwerkomgewing teen te werk. Die bedreigings kan in vier groepe opgedeel word, nl:

- Onbeplande bedreigings wat privaatheid, integriteit en geldigheid van inligting skend.

- Beplande bedreigings wat die doelbewuste insameling van inligting of die doelbewuste inmenging met data insluit.
- Passiewe bedreigings is die versamel of bestudering van data sonder dat die data in enige manier beïnvloed word.
- Aktiewe bedreigings veroorsaak die verandering van data of die werking van die stelsel.

Meganismes kan afsonderlik of in groepe gebruik word om die die dienste wat bedreigings teenwerk, te implimenteer. Die diens van data-integriteit kan byvoorbeeld deur die meganismes enkripsie en digitale handtekeninge verkry word. Die twee meganismes kan afsonderlik of in kombinasie gebruik word.

Vervolgens sal die die volgende punte bespreek word:

2.4.1] Sekerheidsdienste.
2.4.2] Sekerheidsmeganismes.
2.4.3] Toekenning van dienste aan OSI-vlakke.
2.4.4] Sekerheidsbuitelyne en plasing van dienste.
2.4.5] Implimentasie van dienste deur meganismes.
2.4.6] Primitiewe sekerheidsfunksies.

2.4.1. Sekerheidsdienste.

Volgens die bylaag oor netwerksekerheid, word die volgende sekerheidsdienste aanbeveel, en sal nou kortliks bespreek word.[7][8][[23][24][28][61]

- Gelyke entiteite moet geïdentifiseer word.'n Entiteit is 'n gebruiker of program waarmee gekommunikeer word. Alle protokoldataeenheid- (PDU) toegang moet volgens die identifikasie en klasse van inligting beoordeel word. 'n PDU is die kleinste eenheid of pakkie waarin lang boodskappe opgedeel word. Hier moet met sekerheid kan bepaal word dat die regte twee entiteite met mekaar kommunikeer.

- Toegangsbeheer deur middel van 'n stel reëls om entiteit se toegang tot netwerk se hulpbronne te beheer. Die toegangsbeheer word opgedeel in verpligte en diskresionêre toegangsbeheer.
- Verpligte toegangsbeheer is die beheer van toegang tot hulpbronne, in terme van sensitiwiteit van inligting in die hulpbronne. OSI noem dit die reël-gebaseerde sekerheidsbeleid.

- Diskresionêre toegangsbeheer is die beheer van toegang ten opsigte van entiteite se identiteit of groepe waaraan hulle behoort. Volgens OSI is dit 'n identiteitgebaseerde sekerheidsbeleid.

- Datageheimhouding wat deur aktiewe of passiewe aanvalle in gevaar gestel word. Passiewe aanvalle kan wees vrystelling van inligting of verkeerontleding. Aktiewe aanvalle is die verandering, vertraging of herordening van PDUs. Die probleem kan opgelos word deur die gebruik van enkripsie. Volgens OSI het geheim- houding die volgende kenmerke:

- Kommunikasieintegriteit moet verseker word. Hier is dit van belang om die inmenging tydens kommunikasie te kan identifiseer en nie om dit te voorkom nie. Dit kan gedoen word deur middel van waarmerking en enkripsie.

- Verseker diensbeskikbaarheid deur voorkoming van weerhouding van dienste. Netwerke moet minimum vlak van dienslewering verseker deur onder andere die identifisering van toestande wat dienslewering beïnvloed, byvoorbeeld die monitering van reaksietyd van dienste en optredes in geval van faling van apparatuur.

- Verantwoordelikheid. Geheime insameling en beskerming van ouditinligting van entiteite se aksies in 'n boekhoudingsfasiliteit.

- Weerhouding van ontkenning van ontvangs van boodskap deur ontvanger. Weerhouding van terugtrekking van boodskap deur afsender na ontvangs deur ontvanger.

- Verkeersvloeiintegriteit wat verseker dat karakteristieke van data vloei nie ontleed kan word nie en dat gebruikers nie uit die vloei geïdentifiseer kan word nie.

2.4.2 Sekerheidsmeganismes.

Die netwerksekerheidsargitektuur spesifiseer watter meganismes voorsien moet word om die sekerheidsdienste mee te implimenteer. Die netwerksekerheidsbylaag skryf 'n hele aantal meganismes voor om die dienste wat reeds beskryf is mee te voorsien.

Daar kan van verskillende meganismes gebruik gemaak word om 'n bepaalde diens te lewer, en daar kan ook van samevoegings van die meganismes gebruik gemaak word, byvoorbeeld die voorkoming van verkeersontleding kan verkry word deur enkripsie en/of verkeeropvulling.

Sekere meganismes word in die bylaag van die OSI gespesifiseer. Hier sal slegs 'n lys van die meganismes gegee word, aangesien dit breedvoeriger in latere hoofstukke bespreek sal word. Vervolgens 'n beknopte bespreking van 'n paar van die meganismes. [7][8][[23][24][28][61]

- Enkripsie.

  Enkripsie is 'n bewerking op die leesbare inhoud van 'n lêer of boodskap om die inhoud onleesbaar te maak totdat dit weer gedekripteer is.

- Elektroniese handtekeninge.

  Dit is 'n bewerking wat op 'n boodskap gedoen word deur middel van 'n sleutel wat onweerlegbaar aan 'n bepaalde gebruiker verbind kan word. Die handtekening kan byvoorbeeld deur 'n kriptografiese bewerking verkry word.

- Entiteitwaarmerking.

  Dit is die positiewe identifisering van 'n entiteit. Hier moet bewys kan word dat die entiteit eg is, en nie 'n indringer wat 'n wettige entiteit namaak nie.

- Wagwoorde.

  Wagwoorde kan gebruik word om 'n entiteit te identifiseer vir doeleindes van toegangsbeheer en waarmerking.

- Verkeeropvulling.

  Dit behels byvoorbeeld die byvoeging van oortollige, betekenislose data of boodskappe op die netwerk om te voorkom dat tye wat netwerk baie inligting vervoer geïdentifiseer kan word.

- Roeteringsbeheer.

  Hier word die fasiliteit geskep om 'n pakkie of boodskap te verplig om 'n vooraf-bepaalde roete deur die netwerk te volg.

- Notarisasie.
  Hier voorsien 'n betroubare derde party die versekering dat die boodskap veilig vervoer sal word.

2.4.3 Toekenning van dienste aan OSI vlakke.

Figuur 2.5 dui die verskillende dienste aan en die vlakke wat die OSI aanbeveel om die dienste in te plaas.[23][11][24][61] Die literatuur wat bestudeer is, stem nie ooreen met die plasing van die dienste in sekere vlakke nie. Die dienste aangedui met ,'*', kom in al drie bronne voor, terwyl dienste met ,'?', nie in al drie voorkom nie.

Die OSI-sekerheidsbylaag bevat ook 'n stel reëls wat die toekenning van dienste aan die vlakke van die OSI-model voorskryf. Die reëls is as volg.[24][61]

- Die aantal alternatiewe maniere om 'n diens te bereik, moet geminimeer word.
- Veilige stelsels mag van dienste gebruik maak wat vanaf verskillende vlakke in die model kom.
- Bestaande OSI-funksies moet so min as moontlik gedupliseer word om addisionele sekerheidsfunksies te voorsien.
- Vlakonafhanklikheid moet sover as moontlik gerespekteer word.
- Die graad van betroubare funksionaliteit moet sover as moontlik geminimeer word.
- Indien 'n sekerheidsfunksie op een vlak afhanklik is van meganismes op laer vlakke, moet tussen vlakke ontwikkel word om enige sekerheidsverbrekings te voorkom.
- Sekerheidsfunksies moet sover moontlik so ontwikkel word dat die funksies as selfonderhoudende en "add-on" -modules geïmplimenteer kan word.
- Die advies in die bylaag verwys na volledige sewe-vlak eindstelsel implimentasies, en herleistelsels.

SEKERHEIDSDIENSTE.	OSI VLAKKE.						
	1	2	3	4	5	6	7
GELYKE ENTITEITWAARMERKING.			*	*		?	?
TOEGANGSBEHEER.			*	*		?	*
SKAKEL VERTROULIKHEID.	*	*	*	*		*	?
ONGESKAKELDE VERTROULIKHEID.		*	*	*		*	?
SELEKTIEWE VELDVERTROULIKHEID.						*	?
VERKEERSVLOEISEKERHEID.	*		*				*
SKAKEL INTEGRITEIT MET HERSTEL.				*			?
SKAKEL INTEGRITEIT SONDER HERSTEL			*	*		?	?
SELEKTIEWE VELD ONGESKAKELDE INTEGRITEIT.						?	?
DATAOORSPRONG WAARMERKING.			*	*		?	?
NIE-TERUGTREKKING DEUR OORSPRONG						?	?
NIE-TERUGTREKKING DEUR ONTVANGER						?	?

FIGUUR 2.5. VOORSIENING VAN SEKERHEIDSDIENSTE IN DIE VLAKKE VAN DIE OSI - VERWYSINGSMODEL.

2.4.4. Kommentaar oor die gebruik van die OSI- reëls t.o.v. plasing van Dienste.

Die grootste probleem wat kan ontstaan by die gebruik van die reëls wat in 2.4.3 genoem word, is die mate waartoe die toepassings aan die sewe-vlakke van die OSI-model voldoen. Soos die laaste van die reëls in punt 2.4.3 aandui, is die advies gerig op volle implimentasie van die sewe vlakke. Daar bestaan egter baie min produkte en toepassings wat ten volle van al sewe vlakke gebruik maak.

Die belangrikste voordeel verbonde aan die gebruik van die reëls is die minimering van bokoste wat sekerheidsdienste in 'n toepassing sal meebring. Dienste sal met die minimum aantal meganismes geïmplimenteer word. Daar sal so min vlakke as moontlik by die dienste betrek word.

Die implimentasie van dienste as selfonderhoudende "add-on" modules bring die voordeel mee dat as 'n bepaalde diens nie doeltreffend of aanvaarbaar verrig word nie, kan 'n ander implimentasie van die diens vervang kan word.

2.4.5. Sekerheidsbuitelyne en die plasing van dienste.

Die besluit oor die plasing van die dienste in sekere vlakke van die OSI- verwysingsmodel, word sterk beïnvloed deur die keuse van 'n sekerheidsbuitelyn, soos in punt 2.3 bespreek, wat in die toepassing benodig word.

Om te verseker dat enige van die drie buitelyne gebruik kan word, is die maklikste uitweg om te volg die toekenning van al die dienste aan al die vlakke. Die uitweg is wel prakties moontlik, maar sal baie tyd in beslag neem, en sal ook die ingewikkeldheid en prestasie van die netwerk nadelig beïnvloed. Verder strook die benadering ook nie met die van die OSI nie wat aandring op die plasing van die dienste op ander vlakke nie.

As besluit word om die buitelyn om die hele netwerk te trek, is die toepassing ten volle van die netwerk se dienste afhanklik vir die behoud van sekerheid. Die voordeel van die benadering is dat die dienste aan enige vlak toegeken kan word, aangesien die buitelyn nie enige van die vlakke uitsluit nie. Die nadeel is dat daar, soos in punt 3.2.1 genoem is, aangeneem word dat die netwerk in geheel betroubaar is of dat geen sensitiewe inligting in die netwerk voorkom nie. Die aanname is egter onaanvaarbaar in die praktyk, aangesien daar uiters min netwerke is wat aan die aanname voldoen.

As daar besluit word om van die buitelyn om elke gebruikerproses te trek, word daar van geen van die dienste gebruik gemaak nie. Dit bring egter mee dat al die dienste in die toepassing self geïmplimenteer moet word. Die voordeel van die benadering is dat die proses self sy eie sekerheid verseker en glad nie op die netwerk staatmaak vir enige hulp nie. Die nadeel is egter weer dat die toepassing baie ingewikkeld is, en dat die toepassing nie met ander toepassings wat van ander OSI-dienste gebruik maak, kan kommunikeer nie.

SEKERHEIDSDIENSTE.	SEKERHEIDSMEGANISMES.							
	ENKRIPSIE	SYFERHANDTEKENINGE	TOEGANGSBEHEER	DATAINTEGRITEIT	WAARMERKING	VERKEEROPVULLING	ROETEBEHEER	NOTARISASIE
GELYKE ENTITEITWAARMERKING.	*	*			*			
TOEGANGSBEHEER.			*					
SKAKEL VERTROULIKHEID.	*							
ONGESKAKELDE VERTROULIKHEID.	*							
SELEKTIEWE VELDVERTROULIKHEID.	*							
VERKEERSVLOEI SEKERHEID.	*							
SKAKEL INTEGRITEIT MET HERSTEL.	*			*				
SKAKEL INTEGRITEIT SONDER HERSTEL	*			*				
SELEKTIEWE VELD ONGESKAKELDE INTEGRITEIT.	*	*		*				
DATAOORSPRONG WAARMERKING.	*	*						
NIE-TERUGTREKKING DEUR OORSPRONG		*		*				*
NIE-TERUGTREKKING DEUR ONTVANGER		*		*				*

FIG 2.6. MEGANISMES WAT ALLEEN OF IN KOMBINASIE GEBRUIK KAN WORD OM SEKERHEIDSDIENSTE MEE TE IMPLIMENTEER.

Die twee benaderings is die twee uiterstes wat gevolg kan word en het elk sy voordele en nadele. Om te verseker dat 'n boodskap in 'n netwerk veilig is, moet daar op so min van die OSI-vlakke vertrou word as moontlik, maar kan ook nie van geen van die vlakke gebruik gemaak word nie. Die enigste ander benadering is om 'n buitelyn om die boonste vlakke van die OSI-model gebruik te maak. In hierdie benadering word al die dienste aan vlak vier tot vlak sewe toegeken. As na figuur 5 gekyk word, sal gesien word dat die toekenning volgens hierdie benadering wel moontlik is.

Die voordeel van die benadering van buitelyn om die boonste vlakke is dat toepassings wat van die ander twee benaderings gebruik maak, ook hier gebruik sal kan word. Verder voorsien die aanbeveling van die OSI ook die moontlikheid van die toekenning van die dienste aan meer as een vlak. Daar word ook nie op die eerste drie vlakke staatgemaak nie.

2.4.6. Implimentasie van dienste deur middel van meganismes.

Figuur 2.6 dui aan watter meganismes gebruik kan word om 'n bepaalde sekerheidsdiens mee te implimenteer. [11] Die sekerheidsdienste is die dienste wat in afdeling 2.4.1 kortliks bespreek is.

2.4.7. Primitiewe sekerheidsfunksies.

Volgens BARNSTAD [8], kan OSI-sekerheidsdienste geïmplimenteer word deur die ontwikkeling van 'n stel funksies wat geroep kan word om die sekerheidsdienste te verrig. Voorbeelde van die funksies volg hieronder. Die funksies sal geroep word met 'n stel parameters wat tussen die hakkies [] voorkom, en lewer as terugvoer resultate tussen hakkies {}.

1. WAARMERK [ID; WAARMERKER] {RESULTAAT; STATUS }
   Bepaal of WAARMERKER ooreenstem met die beweerde ID deur 'n Betroubare Bestuursinligtingsdatabasis te deursoek. Terugvoer word voorsien in RESULTAAT en STATUS.

2. MAGTIGING [ID; TIPE; HULPBRON] { RESULTAAT; STATUS }
   Bepaal of ID oor magtiging van TIPE beskik tot HULPBRON. En voorsien terugvoer in RESULTAAT en STATUS.

3. ENKRIPTEER [PT; LENGTE; SLEUTELNAAM] { CT; LENGTE; STATUS}
   Enkripteer skoonteks PT van LENGTE met SLEUTELNAAM as sleutel, na syferteks CT van LENGTE.

4. DEKRIPTEER [CT; LENGTE; SLEUTELNAAM] { PT; LENGTE; STATUS}
   Dekripteer syferteks CT van LENGTE met sleutel SLEUTELNAAM na skoonteks PT van LENGTE.

5. BEREKENBWK [DATA; LENGTE; SLEUTELNAAM] { BWK; STATUS }
   Bereken 'n Boodskap Waarmerkings Kode(BWK) van DATA van LENGTE met behulp van sleutel SLEUTELNAAM, en lewer as uitvoer die BWK en STATUS.

6. KONTROLEERBWK [DATA; LENGTE; SLEUTEL; BWK] { RESULTAAT }
   Bereken 'n toets-BWK vir DATA van LENGTE met behulp van sleutel SLEUTELNAAM en vergelyk met BWK, met RESULTAAT as uitvoer.

7. TEKEN [DATA; LENGTE; GEBRUIKERID; SLEUTELNAAM] {
   HANDTEKENING; STATUS }
   Bereken 'n HANDTEKENING vir DATA van LENGTE met behulp van die sleutel SLEUTELNAAM vir gebruiker GEBRUIKERID.

8] KONTROLEERHANDTEKENING [DATA; LENGTE; GEBRUIKERID;
   SLEUTELNAAM; HANDTEKENING] { RESULTAAT; STATUS }
   Bereken 'n toetshandtekening vir DATA van LENGTE met behulp van SLEUTELNAAM vir gebruiker GEBRUIKERID en kontroleer die toetshandtekening met HANDTEKENING.

2.5. OSI-Netwerkbestuursargitektuur.[4][5][6]

Die OSI-netwerkbestuursargitektuur, kan beskryf word as 'n netwerkbestuursomgewing wat bestaan uit hulpmiddels en dienste wat gebruik kan word vir die beheer en bestuur van die netwerk. Ons kyk hier na netwerkbestuur, aangesien daar in die netwerkbestuursargitektuur ook melding gemaak word van sekerheid, en hier word ook 'n aantal meganismes vir sekerheidsbestuur beskryf.[4][5][6]

Saam met die ontwikkeling van die sekerheidsargitektuur in 1978 is ook begin met die ontwikkeling van 'n Netwerkbestuursargitektuur. Vroeg in 1985 is die volgende drie voorlopige standaarde gepubliseer deur die OSI : [24]

- Bylaag 4 tot IS 7498 of IS 7498/4
- DP 9595.
- DP 9596.

Daar word drie verskillende modelle vir die implimentasie van die netwerkbestuursargitektuur deur die OSI ondersoek. Elke model benader die netwerkbestuurstaak vanaf 'n ander oogpunt. Die drie modelle is :

- Organisasiemodel, wat die verspreiding van bestuur deur die netwerk beskryf. Die verspreiding is van so 'n aard dat die bestuur van 'n sekere gedeelte van 'n netwerk so naby as moontlik aan die gedeelte plaasvind.[5]
- Inligtingsmodel, wat die bestuur van inligting, objekte en hulle verwantskappe beskryf.[5]
- Funksionelemodel, wat die "management functional areas" (MFA) en hulle verwantskappe met mekaar bespreek. Die netwerkbestuurstaak word hier opgedeel in vyf areas wat die MFA genoem word.[5]

Die model wat van belang is vir ons doeleindes, is die sogenaamde Funksionelemodel soos bevat in die OSI-standaarde. 'n Beknopte beskrywing volg.

Volgens die OSI bestaan daar vyf funksionele areas wat fasiliteite vir die bestuur van netwerke verskaf. Die vyf areas is :

- Foutbestuur, wat fasiliteite verskaf om foute in die netwerk op te spoor en reg te stel. So byvoorbeeld kan foutbestuur deur middel van foutrapportering bepaal watter dele van die netwerk buite werking is.
- Samestellingbestuur versamel inligting oor die samestelling van die netwerk soos watter tipes terminale gebruik word en presies waar in die netwerk hulle voorkom.
- Prestasiebestuur versamel en verwerk inligting vir prestasiemeting om byvoorbeeld te bepaal of daar op sekere dele van die netwerk oorlading van hulpbronne plaasvind, al dan nie.
- Boekhoudingbestuur. Versamel en verwerk inligting nodig vir kosteverhaling vir gebruik van netwerkhulpbronne.
- Sekerheidbestuur verskaf bestuursfasiliteite vir die bestuur van sekerheidsdienste. Soos byvoorbeeld sleutelbestuur.

Vir doeleindes van netwerksekerheid is slegs die samestellingsbestuur en die sekerheidsbestuurareas van belang. Daar sal nou net 'n kort bespreking van die twee velde gegee word.

- <u>Samestellingsbestuur.</u>

  Die area word in die literatuur [5][6] slegs gebruik om inligting oor die samestelling van die netwerk te versamel en te verwerk. Die inligting word gebruik om die fisiese samestelling van die netwerk te bepaal en foute in die netwerk te identifiseer.

In [4] word 'n netwerkbestuursstelsel genaamd NETMAN bespreek wat van die funksionele model gebruik maak. 'n Belangrike aspek van NETMAN is dat die samestellingsbestuur van die pakket van 'n grafiese voorstellingsfasiliteit gebruik maak om die inligting wat versamel is, te vertoon.

'n Verdere aanwending van samestellingsbestuur wat as moontlike uitbreiding in hierdie studie bestudeer wil word, is die gebruik hiervan vir sekerheidsdoeleindes. 'n Voorbeeld daarvan is die grafiese voorstelling van punte waar die netwerk binnegedring is. Laasgenoemde kan identifikasie en opsporing van indringers baie vergemaklik.

- Sekerheidsbestuur.

Sekerheidsbestuurfasiliteite verleen aan die netwerkbestuurder hulpmiddels om die dienste te bestuur wat toegang tot die kommunikasiehulpbronne beskerm. Die hulpmiddels is:

- Waarmerkingsfasiliteite.
- Toegangsbeheer.
- Enkripsie en sleutelbestuur.
- Waarmerking.
- Bestuur en manipulasie van sekerheids- en aktiwiteitboekhoudings.

Die bestudering van netwerkbestuur lê buite die veld wat in hierdie verhandeling gedek sal word. Die bydrae wat netwerkbestuur tot sekerheid in 'n netwerkomgewing kan lewer is egter belangrik, en daarom is netwerkbestuur kortliks bepreek. 'n Meer indiepte bestudering van die sekerheidsaspekte van netwerkbestuur word oorweeg vir verdere studie in die toekoms.

2.6. SAMEVATTING.

Dit is belangrik dat die bestuur van enige onderneming moet besluit watter standaarde gevolg gaan word by die implimentering van netwerke en netwerksekerheid in die onderneming. Die twee van die belangrikste netwerkstandaarde wat bestaan is die ISO se OSI-verwysingsmodel en sekerheidsbylae en IBM se SNA standaard. Alhoewel die SNA standaard baie wyd in gebruik is, begin die ISO standaarde meer gewild raak, en sal in die toekoms moontlik die mees gewilde standaard wees.[18]

Die voordeel van die ISO-standaarde is dat die standaarde dit vir 3e-party vervaardigers moontlik maak om netwerk- en netwerksekerheidsprodukte te ontwikkel. Die SNA-standaarde word meer deur IBM beskerm, en dit is moeiliker om produkte te ontwikkel wat aan die SNA-standaard voldoen. Die skrywer is van mening dat ISO-standaarde in die toekoms baie gewild sal wees en het dus besluit om in die verhandeling slegs op OSI-standaard te konsentreer.

HOOFSTUK 3.

INTERNETWERKSKAKELING.

INTERNETWERKSKAKELING.

3.1. INLEIDING.

As gevolg van die vinnige groei in die gebruik van persoonlike rekenaars in die kantooromgewing, het die gebruik van Lokaleareanetwerke (LAN) en Wyeareanetwerke (WAN) ook begin toeneem. Die toename in gebruik van netwerke het ontstaan uit die behoefte van gebruikers om gesamentlike hulpbronne te deel. Die gebruik van netwerke het egter so algemeen begin word dat die gebruik van een netwerk in baie gevalle nie voldoende is nie. In sommige gevalle wil gebruikers van hulpbronne gebruik maak wat op ander netwerke as hulle eie voorkom. Dit het veroorsaak dat daar begin is om netwerke aanmekaar te koppel.

Die interkonneksie kan plaasvind tussen netwerke van dieselfde soort en netwerke van verskillende soorte. Internetwerkskakeling bring vir sekerheid in die netwerk, en veral subnetwerke groot probleme mee. Daar bestaan verskillende metodes om netwerke aanmekaar te koppel. Die verskillende metodes kan in drie hoofgroepe ingedeel word nl, brug, roeteerder of deurgang, elk met sy eie unieke karakteristieke wat 'n impak het op netwerksekerheid.

Literatuur verskil baie oor veral die definisie van 'n roeteerder. In die meeste verwysings word 'n roeteerder nie as 'n metode van internetwerkskakeling aangegee nie, maar wel as 'n funksie wat deur 'n brug of 'n deurgang verrig kan word.[26][35] [36] In ander verwysings word 'n roeteerder weer as 'n afsonderlike metode van internetwerkskakeling saam met 'n brug en 'n deurgang beskryf.[18][25] Vir die res van die bespreking sal van die standpunt uitgegaan word dat 'n roeteerder wel 'n afsonderlike metode van internetwerkskakeling is.

Elk van die drie metodes het 'n invloed op die subnetwerke sowel as die internet se sekerheid. Dit is dus belangrik om die werking en kenmerke van elk van die drie metodes deeglik te bestudeer om die probleme wat dit vir sekerheid kan veroorsaak, te identifiseer.

Die res van die hoofstuk is as volg georden :

- 3.2] Internetwerkterminologie.
- 3.3] Redes vir gebruik van internetwerke.
- 3.4] Metodes van netwerkskakeling.
- 3.5] Brug.
- 3.6] Roeteerder.
- 3.7] Deurgang.
- 3.8] Internetstandaarde.
- 3.8.1] ISO-IP.
- 3.8.2] TCP/IP.
- 3.9] Tegnologieë se invloed op netwerksekerheid.
- 3.10] Toekoms.

3.2. INTERNETWERKTERMINOLOGIE.

Eers kyk ons na 'n aantal van die belangrike terme wat in die bespreking gebruik gaan word.[25]

Lokaleareanetwerk(LAN) : Dit is 'n kommunikasienetwerk wat skakeling verskaf tussen 'n verskeidenheid datakommunikasietoestelle in 'n klein geografiese area. Die netwerk maak gebruik van 'n gedeelde transmissiemedium. Data word deur middel van pakkieuitsending deur die netwerk versprei. Data word in pakkies opgedeel wat dan op die netwerk geplaas word deur 'n stasie. Die pakkie kan dan deur al die ander stasies van die netwerk ontvang word.

Internet : Dit is 'n versameling van kommunikasienetwerke wat deur middel van 'n brug, roeteerder of deurgang aanmekaar gekoppel is.[25]

Subnetwerk : Dit verwys na een van die kleiner netwerke wat deel van 'n totale internet uitmaak.

Brug("bridge") : Dit is 'n toestel wat gebruik word om twee LANS wat van identiese LAN-protokolle gebruik maak, aan mekaar te koppel.[18][25]

Roeteerder(router) : Dit is 'n toestel wat gebruik word om twee LANS wat van identiese of verskillende LAN-protokolle gebruik maak te koppel. Die roeteerder maak gebruik van 'n internetprotokol wat in elke roeteerder en gasheer in die netwerk voorkom.[18][26]

Deurgang(gateway) : Dit is 'n toestel wat twee netwerke wat van twee totaal verskillende argitekture gebruik maak, aanmekaar te koppel.[18][25][26]

3.3. REDES VIR DIE GEBRUIK VAN INTERNETWERKE.[18][36]

Dit is soms nie moontlik om 'n netwerk aanhoudend uit te brei of om bestaande netwerke in een groot netwerk saam te voeg nie. Daar bestaan verskeie redes hiervoor en vervolgens sal die belangrikstes hiervan kortliks bespreek word.[18]

- Verskillende soorte rekenaars en apparatuur kom in die meeste ondernemings voor. Dit is nie altyd moontlik om die verskeidenheid apparatuur aan een netwerk te koppel nie aangesien die protokolle en argitekture onderling baie kan verskil. In so 'n geval, word apparatuur van dieselfde soort saam gegroepeer en elke groep kan dan 'n afsonderlike netwerk vorm.

- Sekere rekenaars en verbindings se transmissiespoed verskil van ander. Dit is in so 'n geval beter om die vinnige toerusting in afsonderlike netwerke te plaas van stadige toerusting. So beïnvloed die toerusting mekaar nie nadelig nie. Die twee netwerke kan aanmekaar geskakel word sodat rekenaars wat op die verskillende netwerke voorkom wel met mekaar kan kommunikeer as dit nodig is.

- Die organisasie van die onderneming kan van so 'n aard wees dat 'n afsonderlike netwerk vir elke departement of vloer in die gebou nodig is.

- Die geografiese verspreiding van die onderneming se kantore en netwerke kan van so 'n aard wees dat van meer as een netwerk gebruik gemaak moet word.

- Verskillende ondernemings, met elk sy eie netwerk, moet soms met mekaar kan skakel vir gemeenskaplike sake. So is die interskakeling van netwerke 'n vereiste by die gebruik van "Electronic Data Interchange" of EDI tussen twee ondernemings. EDI is 'n proses waar die uitruiling van inligting wat tradisioneel deur middel van handelsdokumente verrig is, geoutomatiseer word deur middel van rekenaars en netwerke. Sulke handelsdokumente sluit onder andere in bestellings, pryslyste, betalings, rekenings en ontvangserkennings.[45]

Betroubaarheid van verskillende kleiner netwerke is beter en kan beter in stand gehou word. As 'n gedeelte van een groot netwerk buite werking raak, kan dit die hele netwerk laat faal, byvoorbeeld as 'n kabelverbinding onderbreek word, kan die hele netwerk faal.

As dit in een van 'n aantal kleiner netwerke voorkom, is slegs die een netwerk buite aksie.

- Dit is soms vanuit 'n sekerheidsoogpunt vir 'n onderneming beter om van afsonderlike LANS gebruik te maak as van een groot netwerk. So kan kritiese of onveilige gedeeltes van 'n onderneming geïsoleer word van ander dele, byvoorbeeld by 'n universiteit is dit beter om die studentenetwerk van die universiteit se hoofnetwerk af te sonder. Sodoende word verseker dat studente nie ongemagtigde toegang tot sensitiewe inligting op die hoofnetwerk kan kry nie.

- Hoe groter 'n netwerk word, hoe meer word die prestasie van die netwerk beïnvloed. As die netwerk te groot word, kan die prestasie van die netwerk onaanvaarbaar laag daal as gevolg van die oorbenutting van sekere hulpbronne of bottelnekke. In so 'n geval is dit beter om die netwerk in 'n aantal kleiner LANs te verdeel.

- 'n Enkele netwerk kan so groot word dat dit die netwerk se argitektuurbeperkings oorskry, so byvoorbeeld kan die adressering van die netwerk oorskry word, of die netwerk kan te groot raak om effektief te bestuur.

- In die bankwese word daar toenemend gebruik gemaak van Outomatiese tellermasjiene of ook genoem Outobanke. Die Outobanke is gewoonlik deur middel van netwerke aan die bankinstellings se sentrale rekenaars gekoppel. In baie gevalle maak die verskillende bankinstellings nie van dieselfde netwerke gebruik nie. So byvoorbeeld bestaan daar in Suid-Afrika twee groot finansiële netwerke naamlik SASWTICH en MULTINET. Druk van gebruikers om vanaf enige Outobank met sy eie bank te kan kommunikeer, het veroorsaak dat die netwerke ook met mekaar gekoppel moet word.

Sulke internetwerking kan plaasvind binne 'n enkele gebou tot so groot as koppeling tussen netwerke op verskillende vastelande. Die netwerke word gebruik vir take soos onder andere elektroniese pos (e-mail) en toegang tot hulpbronne. Die koppeling tussen die netwerke moet vir die gebruiker so deursigtig as moontlik wees. Die doelwit is om die koppeling van so 'n aard te kry, dat dit vir die gebruiker voel dat hy op een groot netwerk werk in plaas van op 'n internet.

3.4. METODES VAN INTERNETWERKSKAKELING.

Internettegnologie het gelei tot die ontwikkeling van drie tipes koppelingsmetodes, naamlik bruê, roeteerders en deurgange. Daar bestaan verskillende maniere om tussen die drie te onderskei, en daar bestaan ook nie volle ooreenstemming hieroor in die literatuur nie.[18][25][56][59][60][96] Die belangrikste ooreenstemming wat in die meeste literatuur voorkom is die mate waarin die protokolle en argitekture van die twee geskakelde netwerke van mekaar verskil.

Die basiese argitektuur van internetskakelingstegnolgie word deur figuur 3.1 aangedui : [56]

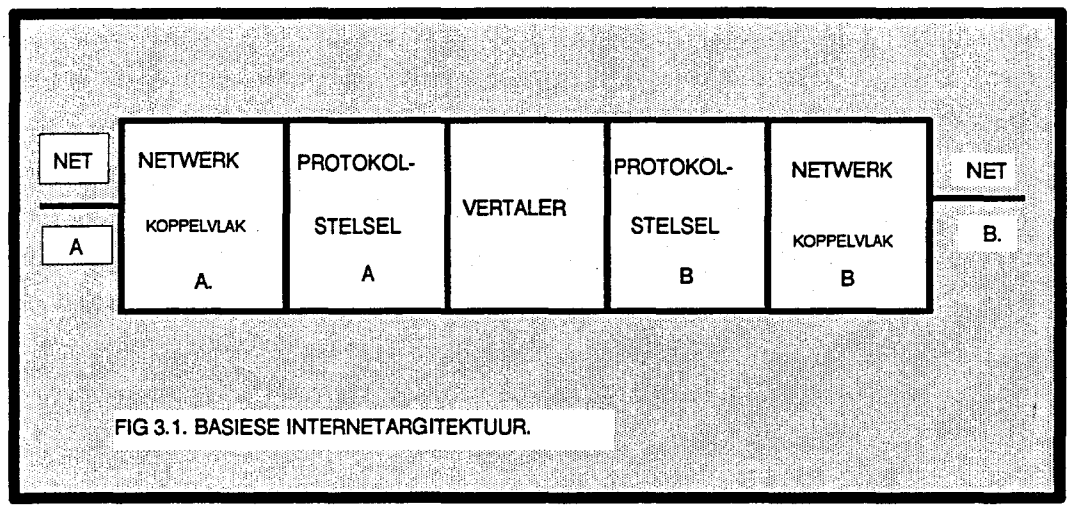


FIG 3.1. BASIESE INTERNETARGITEKTUUR.

Die netwerkkoppelvlakmodules implimenteer gewoonlik die ekwivalent van vlakke 1 en 2 van die OSI-verwysingsmodel. Die modules hang sterk af van die fisiese koppelvlakbehoeftes van die netwerk en wissel van hoë-spoed, enkelkanaal LANs tot multiskakel, satelietgebaseerde, langafstandnetwerke.[56]

Die protokolverwerkingsmodules deel dieselfde algemene apparatuurkarakteristieke, onafhanklik van die tipe protokol wat uitgevoer word. Dit is gewoonlik ekwivalent aan vlak 3 en hoër van die OSI-verwysings model.[56]

Die kompleksiteit en presiese omvang van elke modules word bepaal deur die toepassing van die internetskakeling, of dit 'n brug, roeteerder of deurgang is.[56]

Die argitektuur bestaan uit die volgende vyf modules nl :

- Netwerkkoppelvlak A : Dit is die koppelvlak tussen Netwerk A en die internet skakeling.
- Protokolstelsel A : Protokolstelsel module van netwerk A.
- Vertalermodule : Vertaler wat die oorskakeling en verwerking van die internet- kommunikasie van protokol A na protokol B, of andersom, hanteer.
- Protokol stelsel B : Protokolstelselmodule van netwerk B.
- Netwerkkoppelvlak A : Dit is die koppelvlak tussen die internetskakeling en Netwerk A.

Volgens die basiese argitektuur sal tussen bruê, roeteerders en deurgange onderskei kan word na aanleiding van die kenmerke van die twee protokolstelsels en die vertalermodules soos onderskeidelik aangedui in bostaande diagram. Dus sal ons vir verdere bespreking onderskei tussen die drie tegnologieë op grond van die verskil in argitektuur en protokolle. So sal twee netwerke met identiese argitekture en protokolle met 'n brug verbind word. Twee netwerke waarvan die protokolle nie 100% ooreenkom nie, sal met 'n roeteerder vebind word. Twee netwerke met twee totaal verskillende argitekture en protokolle sal deur middel van 'n deurgang aanmekaar gekoppel word. Om verdere verskille tussen die tegnologieë te toon, sal verdere bespreking sover moontlik in terme van die vlakke van die OSI-model gedoen word.

'n Kort bespreking van elk van die drie metodes volg.[18][25]

3.5. BRUG.

'n Brug word gebruik as die twee netwerke van presies dieselfde protokolle gebruik maak. Byvoorbeeld 2 NOVELL-netwerke.Die brug dra inligting oor op vlak 2 van die OSI verwysingsmodel, nl, die datavlak. Sien figuur 3.2.

Die brug is die eenvoudigste van die drie internetkoppelingsmetodes. Die intelligensie van brug is minimaal aangesien feitlik geen verwerking hier nodig is nie. Die brug verander niks aan die inhoud van die datapakkie nie, en voeg ook niks aan die pakkie by nie. Verder is die brug baie maklik om te gebruik.[18][56][25]

Die brug kan gesien word as 'n adresfilter wat pakkies op een netwerk herken wat vir 'n ander netwerk bedoel is. Die brug kan dan pakkies filteer na aanleiding van sekere adresse of adresreekse.Die pakkies word dan aan die ander netwerk oorgedra. Die brug moet dus oor genoeg intelligensie beskik om te kan bepaal of 'n datapakkie se bestemmingsadres op die huidige netwerk is of nie.

Sien figuur 3.3. vir 'n voorstelling van die gebruik van 'n brug.[56] Die figuur is nie in [56] bespreek nie. Die bespreking wat volg is die mening van die skrywer.

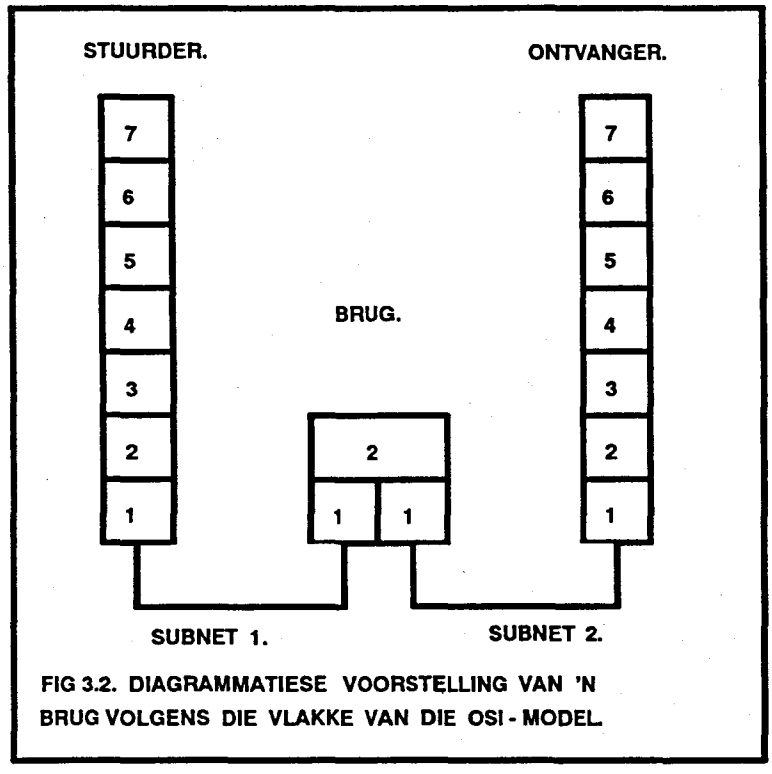


FIG 3.2. DIAGRAMMATIESE VOORSTELLING VAN 'N BRUG VOLGENS DIE VLAKKE VAN DIE OSI - MODEL.

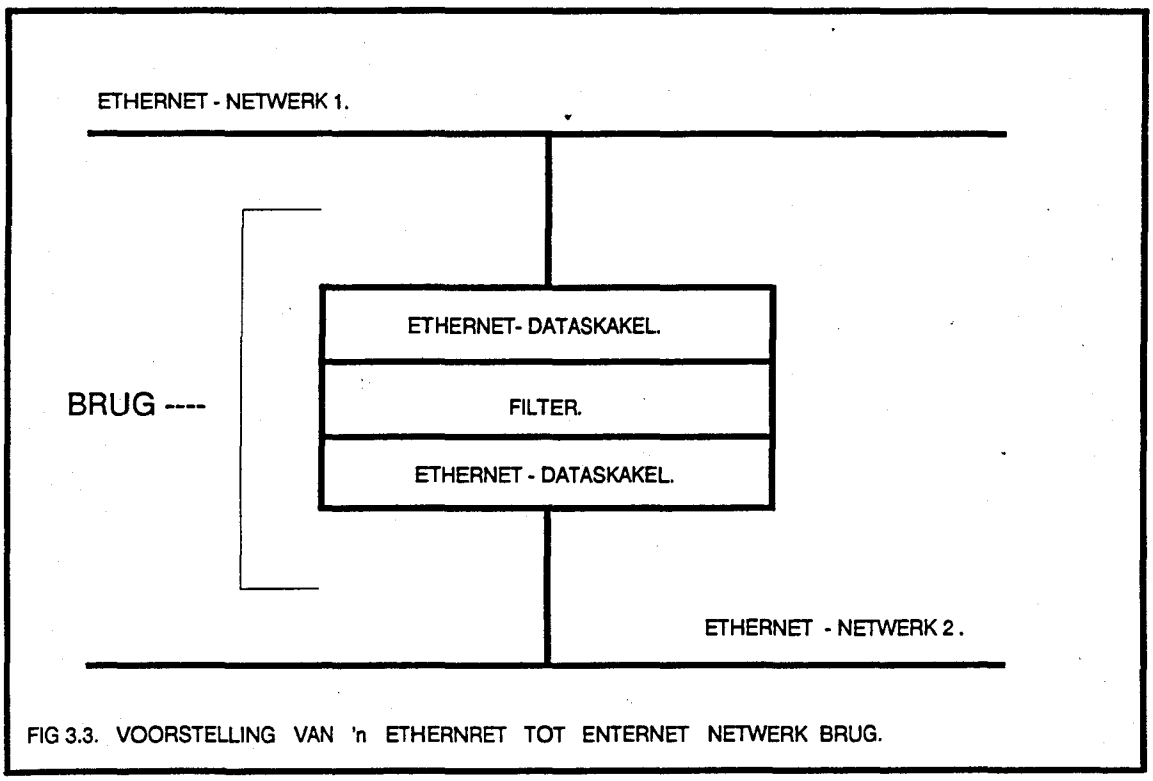


FIG 3.3. VOORSTELLING VAN 'n ETHERNRET TOT ENTERNET NETWERK BRUG.

In figuur 3.3, betaan die netwerkkoppelvlakmodules uit Ethernet-Dataskakelvlak van die Ethernet-netwerk. Aangesien die twee netwerke beide Ethernet netwerke is, is daar geen protokolstelselmodules nodig nie. Die vertalermodule bestaan slegs uit 'n adresfilter wat die pakkies wat vir adresse op die ander netwerk bestem is, identifiseer en deurlaat.

3.6. ROETEERDER.

'n Roeteerder word gebruik as die twee netwerke se LAN-protokolle nie presies met mekaar ooreenstem nie, maar nog steeds aan dieselfde argitektuur, soos die OSI model, voldoen. Hier word inligting op die 3e vlak van die OSI-model, die netwerkvlak, uitgeruil. Sien figuur 3.4.

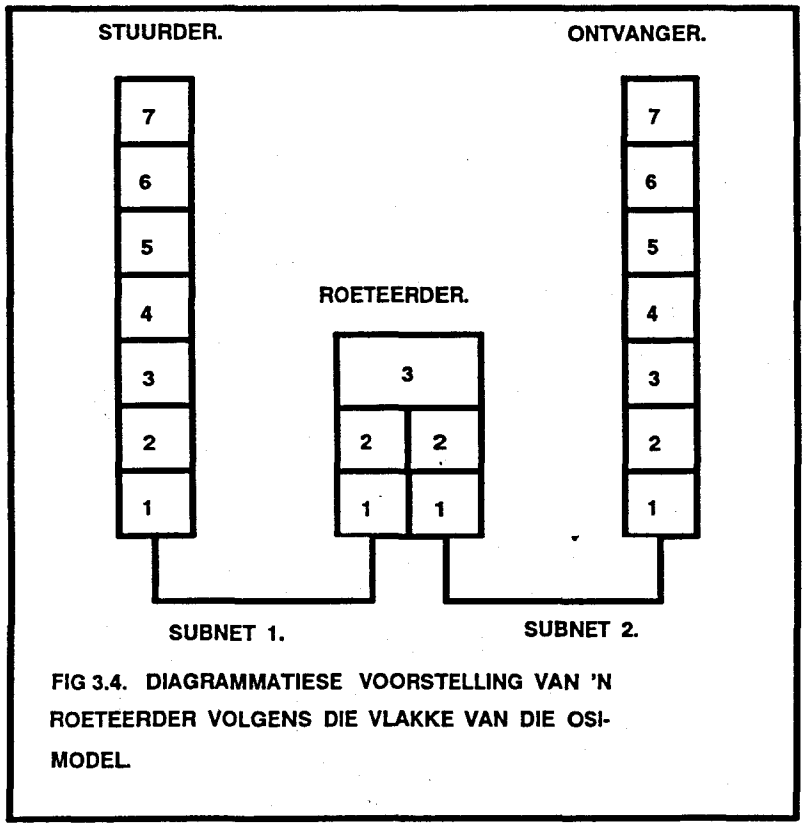


FIG 3.4. DIAGRAMMATIESE VOORSTELLING VAN 'N ROETEERDER VOLGENS DIE VLAKKE VAN DIE OSI-MODEL.

Die roeteerder moet intelligent genoeg wees om die volgende verskille tussen die twee netwerke te kan hanteer :[18][25][56]

- Die twee netwerke kan van verskillende adresseringskemas gebruik maak. 'n Voorbeeld is IEEE 802 LAN protokol maak van 16 of 18 bis adresse gebruik, terwyl X.25 protokol van 12 bis adresse gebruik maak.[18][25] Die roeteerder moet dus oor 'n tipe van globale adresseringsskema beskik sowel as 'n adresgids.

- Maksimum pakkie grote van die twee netwerke kan ook verskil. 'n Pakkie van een netwerk sal byvoorbeeld deur middel van segmentasie opgebreek moet word in kleiner pakkies en dan weer op die volgende netwerk herversend moet word.

- Verskillende apparatuur en programmatuurkoppelvlakke kan op die netwerke bestaan. Die roeteerder moet sover moontlik onafhanklik van die verskille wees.

- Verskillende netwerkdienste voorsien verskillende grade van betroubaarheid. Die roeteerder moet so min as moontlik op die dienste staatmaak.

Sien figuur 3.5 vir 'n voorstelling van die gebruik van 'n roeteerder.[56] Die figuur is nie in [56] bespreek nie. Die bespreking wat volg is die mening van die skrywer.

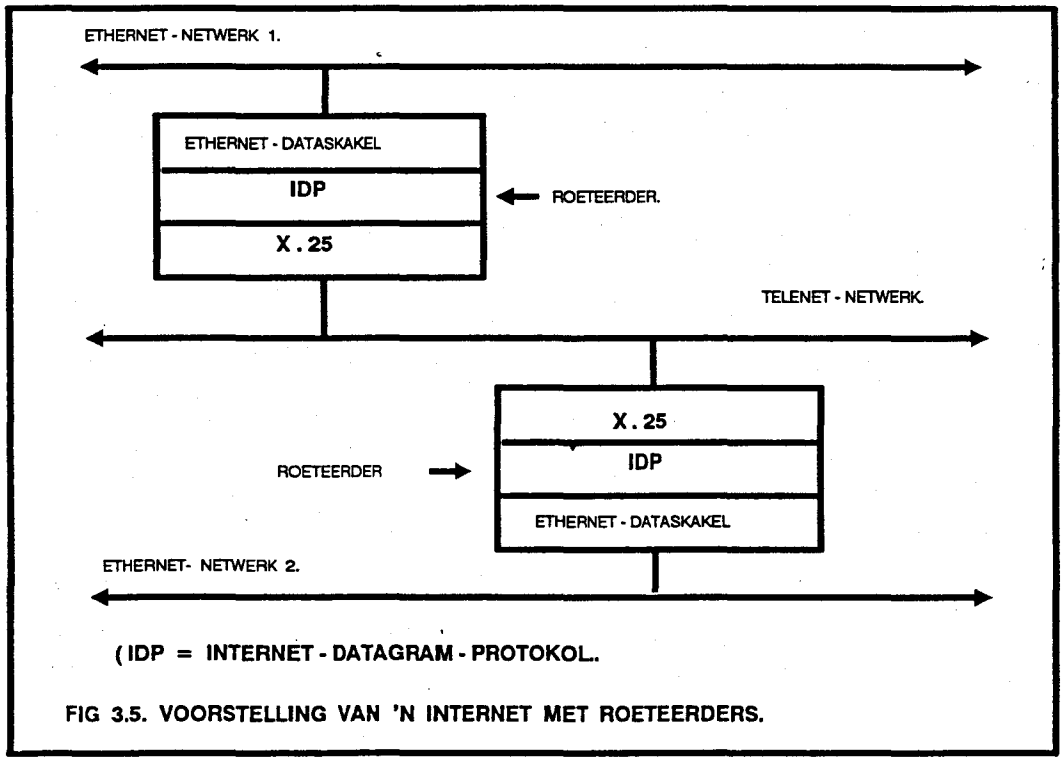


FIG 3.5. VOORSTELLING VAN 'N INTERNET MET ROETEERDERS.

In figuur 3.5 word van roeteerders gebruik gemaak vir kommunikasie tussen twee Ethernet netwerke, deur 'n TELENET-netwerk, wat van die X.25-protokol gebruik maak. Die protokol wat deur die Ethernet-netwerk gebruik word, en die X.25 protokol se boonste vlakke stem ooreen. Daar word van die Internet-Datagram-Protokol (IDP) gebruik gemaak om die oordrag tussen die twee netwerke te verrig.[56]

3.6.1. Werking van roeteerder.[18]

Dit is belangrik dat ons hier in meer detail na die werking van die roeteerder kyk, aangesien die roeteerder die meeste van die drie metodes gebruik word. Verder beskik die roeteerder oor spesiale kenmerke wat 'n invloed op sekerheid van die netwerke kan uitoefen.

Die roeteerder maak gebruik van 'n internetprotokol(IP) wat op vlak 3 van die OSI-model voorkom. Die netwerke moet dieselfde IP hê sowel as dieselfde protokol bo die IP.(Van vlak 4 tot vlak 7). Voorbeelde van sulke protokolle is OSI se transport protokol(TP) of die Amerikaanse Departement van Verdediging(DoD) se transmissie-beheer protokol(TCP/IP). [18]

Hier word daar wel aan die pakkie verander. Die IP lees die datablok en voeg 'n kop wat onder andere die globale netwerkadres in het by. Die globale netwerkadres bestaan uit die netwerk identifiseerder sowel as die versender se adres. Die hele pakkie word 'n datagram genoem. As die IP sien dat die adres op 'n ander netwerk is, gaan die pakkie na die LAN-protokol wat die pakkie voltooi deur die roeteerder se adres in 'n nuwe kop aan die datagram te heg, en die pakkie aan die roeteerder afgee.

Die roeteerder verwyder en ontleed die kop, en bepaal die doelwit van die pakkie. Hier kan twee moontlikhede wees. Die ontvanger is op die netwerk aan die roeteerder gekoppel, of die pakkie moet deur nog 'n roeteerder gaan. In geval 1 word die pakkie op die netwerk geplaas en dit bereik die ontvanger. In geval 2 voeg die roeteerder 'n LAN-protokolkop aan die datagram met die nuwe roeteerder se adres op. Dit gaan voort tot die pakkie 'n roeteerder bereik wat aan 'n netwerk gekoppel is met die bestemming ook daaraan gekoppel.

Dit is soms vir die roeteerder nodig om die pakkie te segmenteer. Dit beteken dat die twee netwerke nie van dieselfde pakkielengtes gebruikmaak nie. Die pakkie word opgedeel en 'n nuwe laervlakpakkie word vir die bepaalde netwerkprotokol saamgestel. Die roeteerder het soms 'n beperkte aantal pakkies wat hy kan hou terwyl hy aan 'n ander pakkie werk. In so 'n geval word die nuwe pakkies weggegooi.

As die pakkie sy doelwit bereik word die IP-pakkie ontbind en die boodskap blokke aanmekaar gekoppel en aan die ontvanger gegee. Die roeteerder waarborg nie die volledigheid van die boodskap of die volgorde van die pakkies nie. Dit is die hoër vlakke van die protokol se probleem om die foute uit te stryk.

Die roetering word verrig deur tabelle in die gasheerrekenaar en roeteerders aan te hou, wat roetes en roeteerders identifiseer. Die tabelle kan staties of dinamies wees. Die voordeel van dinamiese tabelle is dat as 'n roeteerder faal, die tabel verander kan word om 'n nuwe roete sonder die foutiewe roeteerder te kan aandui. Vir sekerheidsdoeleindes, kan sekere roetes spesiaal beskerm word deur byvoorbeeld van hoër kwaliteit transmissiemedia gebruik te maak, of om spesiale enkripsietoestelle op sekere roetes te gebruik. Die roetes kan dan in die tabelle aangedui word om gebruik te word in noodsaaklike gevalle. Die tabelle kan verder ook soms die adresse van sekere roeteerders en stasies aandui wat nie vanuit die bepaalde netwerk bereik mag word nie.[18][26]

3.7. DEURGANG.

'n Deurgang word gebruik waar daar twee netwerke van verskillende argitekture(soos OSI en SNA) aan mekaar gekoppel word. A.g.v. reeds bestaande netwerke is dit soms nie moontlik om te standaardiseer op een soort netwerk nie. Hier word oordrag op die 7e vlak, die toepassingsvlak, van die OSI-model gedoen. Hier is 'n spesifieke toepassingsprogram, genoem die deurgangtoepassing, nodig om die oordrag van een argitektuur na die ander te doen. Sien figuur 3.6.[18][25]

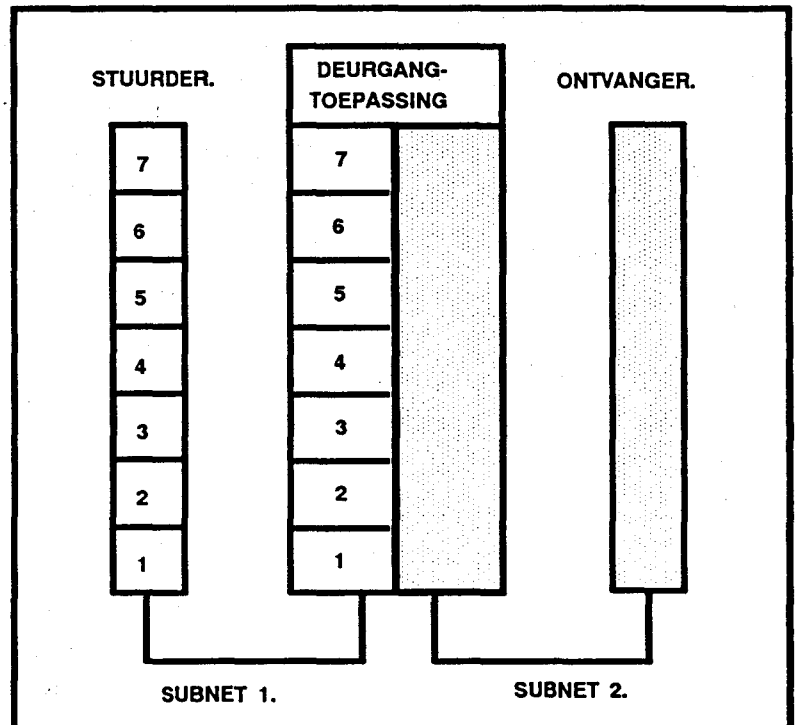


FIG 3.6. DIAGRAMMATIESE VOORSTELLING VAN 'N DEURGANG VOLGENS DIE VLAKKE VAN DIE OSI-MODEL.

Die deurgang is die mees ingewikkeldste van die 3 toestelle. Die brug moet al 7 vlakke van die OSI-model implimenteer sowel as al die vlakke van die ander argitektuur. Die deurgang kommunikeer met elke netwerk in die netwerk se eie "taal", en neem ook die vertaling tussen die twee protokolle waar. Die oorgang word gewoonlik in twee stadiums gedoen.

- Vertaal pakkie vanaf bestaande protokol na 'n interne protokol.
- Vertaal pakkie van interne protokol na doelwitprotokol.

Van die mees algemene vertalings wat hier verkry word, sluit in : [56]

- terminaalprotokolle,
- dokumentformate,
- lêerformate,
- enkripsiemetodes.

Daar bestaan verskillende nadele in die gebruik van 'n deurgang.

- Deurgange is baie ingewikkeld en moeilik om te gebruik.
- Deurgange is potensiële bottelnekke, aangesien die vertaling van die datapakkie van een argitektuur na die ander tyd neem en pakkies dan in die deurgang kan ophoop. Dit kan verder veroorsaak dat die reaksietyd van die netwerk kan verlaag.
- Spesiale kenmerke van bepaalde argitektuur gaan verlore soos byvoorbeeld sekerkeidsmaatreëls, soos enkripsie..
- Die belangrikste probleem met deurgange is dat die deurgang vir die koppeling van twee spesifieke netwerkargitekture ontwikkel is. Dit beteken dat in 'n internet wat van baie verskillende soorte netwerkargitekture gebruik maak, vir elke koppelvlak 'n aparte deurgang ontwikkel moet word.

Sien figuur 3.7 vir 'n voorstelling van internetwerkskakeling deur middel van 'n deurgang.[56] Die figuur is nie in [56] bespreek nie. Die bespreking wat volg is die mening van die skrywer.

In figuur 3.7 word van 'n deurgang gebruik gemaak om 'n ETHERNET-netwerk en 'n LOCALNET-netwerk aanmekaar te koppel. Die twee netwerke maak van twee totaal verskillende protokolle gebruik. Die netwerkkoppelvlakke van die twee netwerke bestaan onderskeidelik uit die ETHERNET-dataskakel, en die LOCALNET-dataskakel. Die protokolstelsels is onderskeidelik ETHERNET XNS-protokol en die LOCALNET-protokol. Die vertalermodule moet hier 'n algehele oorskakeling van een protokol na die ander protokol waarneem.

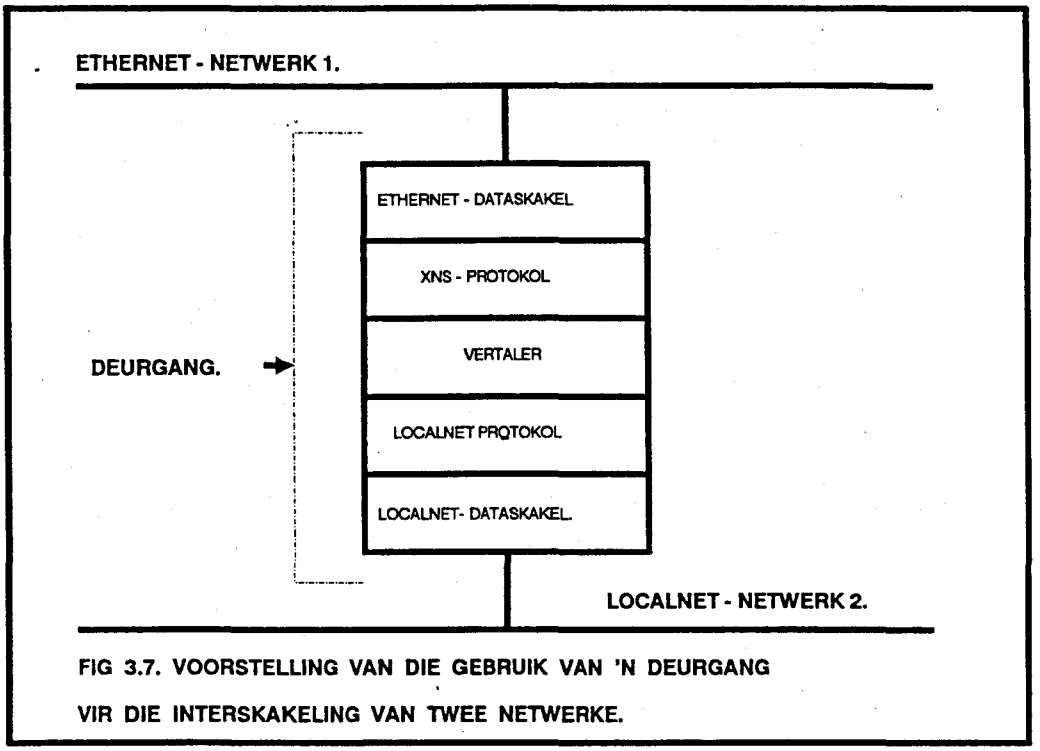


FIG 3.7. VOORSTELLING VAN DIE GEBRUIK VAN 'N DEURGANG VIR DIE INTERSKAKELING VAN TWEE NETWERKE.

3.8. INTERNETWERKPROTOKOL(IP)-STANDAARDE.

Daar bestaan huidiglik 'n baie groot behoefte aan verdere navorsing ten opsigte van InternetProtokolle (IP). Daar bestaan reeds twee IP standaarde wat baie gebruik word nl OSI-IP en die TCP/IP van die Amerikaanse Departement Van Verdediging (DoD).[18][26]

3.8.1. ISO-IP. [18]

Protokol vir voorsiening van die skakellose-modus netwerk diens. (IS 8473) of ISO-IP. Om 'n idee van die protokol te kry, kan gekyk word na die inligting wat in die protokol pakkie se kop voorkom.[18][24]

Die kop bestaan uit 'n vaste en 'n opsionele gedeelte. Die vaste gedeelte bevat inligting soos onder andere die protokolidentifiseerder, weergawe van protokol, leeftyd van die pakkie, ontvanger en stuurderadresinligting.

Die opsionele gedeelte van die kop kan deur die gebruiker aangewend word om die protokol effens aan te pas vir sy eie doeleindes.

Die opsionele gedeelte van die pakkie sluit verskillende opsies in wat aan die gebruiker geleentheid verskaf om die sekerheid en integriteit van die netwerk te verbeter.

- Die roete wat die pakkie deur die internet neem, kan vooraf gespesifiseer word. Dit gee die geleentheid om sekere roetes, wat betroubaar is, te gebruik en probleemareas in die netwerke te vermy.
- Aantekening van die roete wat die pakkie volg. Die inligting kan later ontleed word om te bepaal of daar enige afwykings in die voorgeskrewe roete is. 'n Ander moontlike gebruik is om die roete te bepaal wat pakkies gevolg het waarmee ingemeng is. So kan swakplekke in die netwerk se sekerheid opgespoor word.
- Inligting oor enkripsie wat die ontvanger benodig, kan hier aangeteken word.

3.8.2. TCP/IP of US DoD- standaard

Gebaseer op die V.S.A. se Departement van Verdediging (US DoD) se navorsing oor netwerkprotokolle vir die ARPANET-netwerk, het 'n reeks van vyf protokolle, ook genoem "TCP\IP Protokol Suite", of TCP/IP ontstaan. Die vyf protokolle is :[18][25]

- Internetprotokol (IP),
- Transmissiebeheerprotokol (TCP),
- Lêeroordragprotokol (FTP),
- Eenvoudige posoordragprotokol (SMTP),
- TELNET.

Alhoewel die protokolle ontwikkel is vir gebruik deur die V.S.A. se Departement van Verdediging, het dit gou in die res van die wêreld groot aanhang begin kry.[26]

Die TCP\IP-argitektuur bestaan uit vier vlakke soos aangedui in figuur 3.8.

Die verskillende vlakke verrig die volgende take :

- Die Netwerktoegangsvlak bevat die protokolle wat nodig is vir toegang tot 'n netwerk. Die protokolle is vir kommunikasie tussen die kommunikasienode en die gekoppelde gasheer. TCP\IP beskik hier nie oor 'n unieke protokol nie, maar maak gebruik van protokolle benodig vir 'n spesifieke netwerk, byvoorbeeld Ethernet, X802 of X.25.

- Die Internetvlak bevat prosedures wat die beweging van data oor verskillende netwerke moontlik maak. Die vlak verrig dus 'n roeteringsfunksie. Die protokol in die vlak word die Internetprotokol of IP genoem.

- Die transportvlak verseker die betroubare oordrag van data tussen twee gashere. Die vlak is ook verantwoordelik vir die oorhandiging van die data aan die regte toepassing.

- Die toepassingsvlak bevat die protokolle vir die spesifieke gebruikertoepassings soos byvoorbeeld lêeroordrag(FTP) en elektroniese pos (SMTP).

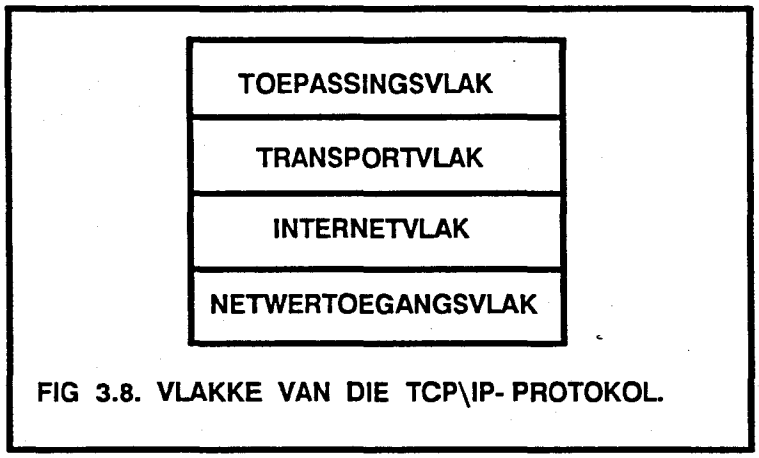


FIG 3.8. VLAKKE VAN DIE TCP\IP- PROTOKOL.

3.9. SEKERHEIDSASPEKTE VAN INTERNETWERKSKAKELING.

Baie min literatuur kan opgespoor word wat aandag gee aan die sekerheidsaspekte van internetwerkskakeling. Daar moet dus na die werking van die Internetwerkskakelings-tegnologieë gekyk word, en daaruit afleidings oor die sekerheidsaspekte gemaak word. Uit die bestudering van die drie tegnologieë vir netwerkskakeling wat in die hoofstuk gedoen is, kan daar 'n aantal interessante opmerkings gemaak word wat met sekerheid te doen het.

In die eerste plek kan Internetwerkskakeling as 'n bedreiging sowel as 'n hulpmiddel vir netwerksekerheid gesien word. Die onoordeelkundige interskakeling van netwerke kan veroorsaak dat ongemagtigde toegang tot hulpbronne op een netwerk verkry kan word vanuit 'n ander netwerk. Groot netwerke kan egter ook opgedeel word in kleiner netwerke. So kan kwesbare dele van 'n netwerk afgesonder word in 'n subnetwerk, en kan toegang tot ander netwerke streng beheer word by die punt van interskakeling.
Afsonderlike netwerke kan ook gebruik word om geheime en sensitiewe werk op te doen. Weer eens kan dit moontlik wees om die netwerk te skakel met ander netwerke, en kan spesiale maatreëls getref word by die punt van interskakeling om ongemagtigde toegang te voorkom.

Die doel van 'n eenvoudige brug is om netwerke so deursigtig as moontlik aanmekaar te skakel. Dit beteken dat die gebruiker nie moet agterkom dat die ander terminaal of node waarmee hy kommunikeer op 'n ander netwerk is nie. Dus kan goeie sekerheid op een netwerk nadelig beïnvloed word as die netwerk waaraan dit gekoppel is met die brug swak sekerheidsmaatrëels het. Daar is egter ook voordele aan hierdie deursigtigheid. Geënkripteerde verkeer word nie by die brug gedekripteer , en dan weer op die nuwe netwerk geënkripteer nie.

By 'n roeteerder en 'n deurgang, kan die verskil in protokolle so groot wees dat die geënkripteerde kommunikasie hier gedekripteer moet word aan die een kant, en dan aan die anderkant weer geënkripteer moet word. Dit beteken dat die pakkie vir 'n kort tydperk in 'n leesbare vorm is, en hier onderskep kan word. Die gebruik van deurgange en roeteerders kan verder 'n groot las op die netwerke plaas as spesiale prosedures ontwikkel moet word om enkripsiesleutels uit te ruil.

Die roeteringsfunksie en roeteringstabelle kan egter met groot vrug aangewend word om sekerheid tussen netwerke te verbeter. Spesiale maatreëls, soos enkripsie, kan op slegs 'n paar belangrike roetes geplaas word. Die roetes kan dan in die tabelle opgeneem word en slegs gebruik word vir verkeer wat van die maatreëls wil gebruik maak. Dit kan verseker dat verkeer wat nie van die sekerheidsmaatreëls wil gebruik maak nie, van onbeskermde roetes gebruik kan maak. Dit kan tot voordeel wees aangesien die onnodige enkripsie- en dekripsieprosesse die prestasie van die netwerk nadelig kan beïnvloed.

Adresfilters by bruê en roetetabelle by roeteerders en deurgange kan ook gebruik word om adresse aan te dui van nodes of hulpbronne wat nie vanaf sekere punte bereik mag word nie.

3.9.1. Gevallestudie van Internetwerke.

Die skrywer het ter illustrasie van voorafgaande aspekte die volgende scenario ontwikkel ter toeligting.

Figuur 3.9 en meegaande beskrywing dui aan hoe internetskakelingstegnologieë sekerheid positief en negatief kan beïnvloed.

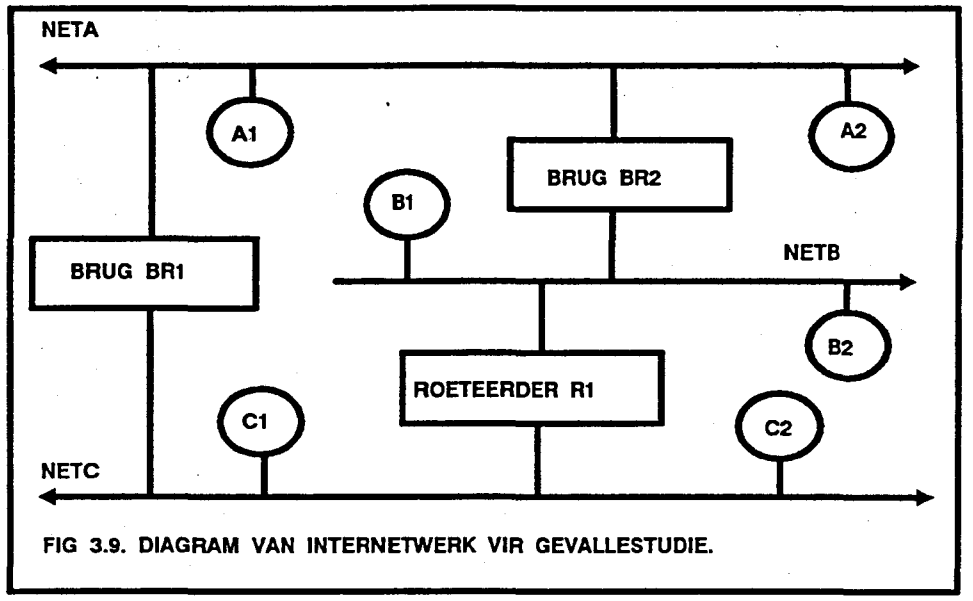


FIG 3.9. DIAGRAM VAN INTERNETWERK VIR GEVALLESTUDIE.

Figuur 3.9 stel drie netwerke voor naamlik :

- NETA met nodes A1 en A2,
- NETB met nodes B1 en B2,
- NETC met nodes C1 en C2.

NETA en NETC is deur middel van brug BR1 gekoppel. NETA en NETB is deur BRUG BR2 gekoppel en NETB en NETC is deur ROETEERDER R1 gekoppel.

NETA en NETC is deur 'n eenvoudige brug BR1 aanmekaar gekoppel wat deursigtige toegang tot mekaar se nodes verleen. Deursigtige toegang beteken dat gebruikers wat van 'n node op een netwerk met 'n node op 'n die ander netwerk wil kommunikeer, nie nodig het om te weet dat die nodes op verskillende netwerke is nie. Dit kom vir die gebruiker voor asof die nodes op dieselfde netwerk is.

Die drukker B2 op netwerk NETB mag slegs deur nodes op NETB en NETA gebruik word. Verder mag nodes C1 en C2 met node B1 kommunikeer. Roeteerder R1 laat slegs verkeer vanaf NETC na NETB toe as dit vir NETA of node B1 bestem is, andersins word kommunikasie vanaf NETC verwerp. Brug BR2 laat egter enige verkeer van NETA toe om NETB, en dus ook node B2, te bereik. C1 en C2 kan ongemagtigde toegang verkry tot B2, deur middel van indirekte toegangskommunikasie met BR1 en BR2, aangesien BR1 alle pakkies van NETC na NETA deurlaat, en BR2 alle pakkies ontvang vanaf NETA aanvaar en na NETB deurstuur.

Die eenvoudige voorbeeld dui aan hoe die sekerheidsmaatrëels op een netwerk deur maatrëels op andèr netwerke, op 'n indirekte wyse kan beïnvloed, as gevolg van die gebruik van internetwerkskakeling. Dit is dus van groot belang dat daar by ontwikkeling en beplanning van sulke internetwerke deeglik gekyk moet word na sulke moontlike, indirekte beïnvloeding tussen netwerke.

'n Moontlike oplossing wat 'n veld vir verdere studie kan uitmaak, is die ontwikkeling van 'n hulpmiddel wat sulke probleme kan identifiseer. Die hulpmiddel kan bestaan uit 'n databasis wat onder andere roeterings tabelle van die netwerke se bruê, roeteerders en deurgange bevat. Verder kan die databasis ook inligting bevat wat aandui wat die toegangsregte van die verskillende nodes op die netwerke op hulle eie netwerke en ook ander netwerke het. 'n Ekspertstelsel kan dan ontwikkel word wat die inligting in die databasis ontleed en moontlike botsings tussen toegangsregte en roeterings kan opspoor.

3.10. SAMEVATTING EN TOEKOMSBLIK.

Internetwerking groei vinnig en die drie tegnologieë nl brug, roeteerder en deurgang, sal in die toekoms baie meer gebruik word. Deurgang kan gesien word as 'n spesiale doel protokol omskakelaar. Die roeteerder is die enigste algemene doel toestel van die genoemde tegnologieë.

Alhoewel die TCP\IP-standaard baie gewild is, kan ander internasionale standaarde soos die ISO-IP gebaseerde LANS in die toekoms meer algemeen word. Roeteerder na roeteerderprotokolle is 'n veld waar daar nog baie sekerheids verwantenavorsing gedoen kan word.[18]

Die ontwikkeling van sogenaamde intelligente bruê, roeteerders en deurgange behoort ook meer aandag te geniet. So ook hulpmiddels soos ekspertstelsels, soos reeds in punt 3.9.1 genoem, om die interaksie tussen die netwerke te bestudeer. So het ekspertstelsels ook 'n bydrae om te lewer by die dinamiese sekerheidsegeoriënteerde herkonfigurasie van netwerke wat nodig mag wees as gevolg van faling van sekere nodes en skakelings.

Sulke falings mag dit nodig maak om bestaande roetetabelle te verander, sodat nuwe roetes daargestel kan word om voortgesette werking van die internet te verseker. Daar moet dus 'n manier gevind word om vinnig die nuwe roetes te identifiseer, en nog belangriker om te verseker dat die nuwe roetes nie bestaande sekerheidsmaatreëls op netwerke omvergooi nie. Indien sekerheid wel nadelig beïnvloed word, moet teenmaatreëls so vinnig as moontlik opgestel word.

HOOFSTUK 4.

NETWERK- EN INTERNETWERKREGTE.

NETWERK- EN INTERNETWERKREGTE.

'n Belangrike deel van enige rekenaar- en netwerksekerheidsstelsel is die beskerming en weerhouding van toegang tot die hulpbronne in die stelsel. Die hoof vraag is **WIE** het die reg om **WATTER** hulpbronne te gebruik en **WAT** mag die spesifieke gebruiker met die hulpbron doen. Vir die bespreking in die res van die hoofstuk moet daar eers onderskei word tussen **SUBJEKTE** en **OBJEKTE**.

'n **SUBJEK** is 'n gebruiker, program of 'n proses wat besig is om een of ander bewerking of taak binne die rekenaar of netwerk te verrig.

'n **OBJEK** is 'n hulpbron wat deur die subjek aangewend word om sy taak te verrig. Die objek kan egter ook 'n ander program, proses, gebruiker of selfs 'n node in 'n netwerk wees.

'n Hulpbron of gebruiker kan nie permanent as 'n objek of subjek geklassifiseer word nie, aangesien die objek in een bewerking weer die subjek in 'n ander bewerking kan wees.

Vir die res van die hoofstuk is die doelwit om metodes te bestudeer om te bepaal wat die **REGTE** is waaroor die bepaalde subjek beskik ten opsigte van 'n bepaalde objek of objekte. Anders gestel, wat mag 'n subjek met 'n bepaalde objek doen. Die bespreking sal veral konsentreer op regte in die netwerk en internetwerkomgewing. In netwerke is die probleem om regte te bepaal en te beheer baie ingewikkeld aangesien daar groot hoeveelde verskillende objekte en subjekte in 'n onveilige omgewing voorkom. By internetwerke is die probleem nog meer gekompliseerd aangesien elke subnet sy eie regte mag hê wat met die ander subnet se regte kan inmeng.

In die hoofstuk sal twee van die algemeenste beskermingsmetodes naamlik Toegangsbeheerlyste en Toegangsbeheermatrikse bespreek word. Laastens sal die sogenaamde Pad-Konteksmodel(PCM) bestudeer word.

Die bespreking sal onder die volgende punte gedoen word naamlik:

- 4.1. Inleiding.
- 4.2. Toegangskontrolelys.
- 4.3. Toegangskontrolematriks.
- 4.4. Pad-Konteksmodel.
- 4.5. Samevatting.

4.1. INLEIDING.

Daar bestaan 'n paar basiese benaderings wat gevolg kan word om objekte in 'n netwerkomgewing te beskerm. Feitlik alle beskermingsmetodes berus op een van die basiese benaderings of selfs kombinasies van die benaderings. Die benaderings is die volgende :[10]

- Kontroleer elke toegang : Dit mag soms nodig wees om 'n subjek se reg tot toegang tot 'n objek terug te trek. As 'n subjek eenmaal toegang tot 'n objek verkry beteken dit nie dat hy die reg permanent verkry het nie. Dit mag soms nodig wees om voortgesette toegangregte terug te trek.

  'n Voorbeeld is die gebruik van 'n leêr op 'n netwerk wat inligting bevat wat periodiek bygewerk word. Gedurende die opdateringsperiode mag geen leesaksies op die leêr uitgevoer word nie. 'n Gebruiker wat leesregte ten opsigte van die leêr het, se leesregte moet dus gedurende die opdateringsperiode herroep word. Vir die redes mag dit nodig wees om elke toegang tot 'n objek te kontroleer.

- Laat minimum voorreg toe : Hier word die objek se regte beperk tot die absolute minimum regte nodig om sy taak te kan verrig. Al is addidionele inligting waardeloos, word sy reg tot die inligting beperk.

  'n Voorbeeld is 'n gebruiker wat skryfregte het na 'n leêr op 'n netwerk. Die netwerk beskik oor verskillende leêrbedieners en die leêr is op een van die bedieners. Die gebruiker mag egter geen inligting ontvang wat hom in staat stel om te bepaal op watter leêrbediener die leêr is nie, al kan hy niks met die inligting doen nie.

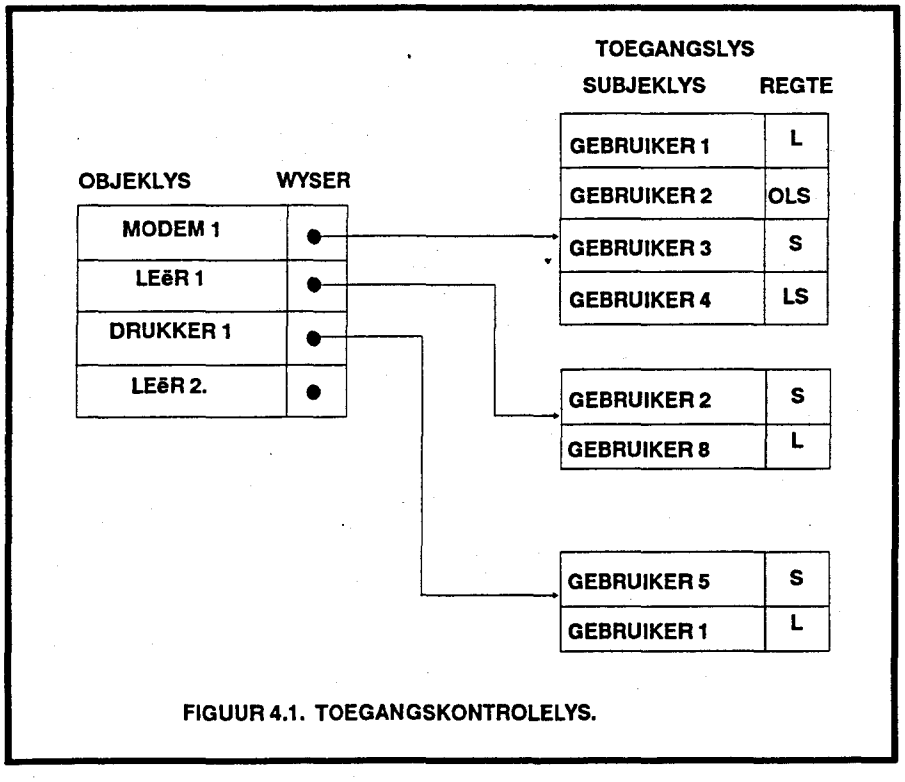
Verifieer aanvaarbare gebruik : Die reg tot toegang is streng 'n JA/NEE besluit. Elke aksie word streng gekontroleer om te bepaal of die aksie wel aanvaarbaar is of nie.

So byvoorbeeld mag die toegelate regte ten opsigte van 'n leêr op 'n netwerk slegs leesregte wees. 'n Gebruiker mag lees, skryf en skep regte op enige deel van die netwerk hê. Alhoewel die gebruiker enige iets in die netwerk mag doen moet sy aksies nog steeds gekontroleer word aangesien hy nie in die leêr mag skryf nie.

4.2. TOEGANGSKONTROLELYS (TKL).

In hierdie metode beskik elke objek oor 'n Toegangskontrolelys(TKL) wat al die subjekte identifiseer wat toegang tot die objek mag verkry[10]. Die TKL bevat die subjek se naam sowel as die regte wat die subjek het in terme van die objek. Figuur 4.1. dui 'n TKL aan waar objek Gebruiker 1 leesregte het tot subjek Modem 1 terwyl objek Gebruiker 4 lees en skryfregte het tot subjek modem 1. Dit beteken dat Gebruiker 1 slegs boodskappe van Modem 1 mag ontvang terwyl Gebruiker 4 boodskappe mag stuur en ontvang.

Sodra 'n subjek toegang tot 'n objek probeer verkry, word die TKL van die bepaalde objek eers gekontroleer om te verseker dat die objek wel in die TKL voorkom voor die toegang verleen word. Vir die bespreking neem ons aan dat objekte G1 en G2 gebruikers is terwyl subjek S1 'n dataleêr is en subjek S2 'n drukker op die netwerk is. As G1 in leêr S1 wil skryf word sy versoek eers met S1 se TKL gekontroleer, G1 is wel in S1 se TKL en toegang word wel tot S1 verleen. As G2 egter 'n drukstuk wil maak met behulp van Drukker S2, sal sy versoek verwerp word aangesien G2 nie in S2 se TKL voorkom nie.



FIGUUR 4.1. TOEGANGSKONTROLELYS.

Die NOVELL netwerkbedryfsstelsel van Netware maak van TKLs gebruik.

4.3. TOEGANGSKONTROLEMATRIKS (TKM).

'n Toegangskontrolematriks (TKM) is 'n matriks waarvan elke ry een subjek voorstel en elke kolom een objek voorstel. Elke inskrywing in die matriks verteenwoordig die **STEL** regte wat die betrokke subjek het ten opsigte van die bepaalde objek. In die oorgrote meerderheid van die gevalle sal die TKM yl wees. Dit beteken dat die meeste subjekte geen toegangsregte tot die meeste objekte sal hê nie.[10][25]

Die gebruik van TKM word baie algemeen gebruik in netwerke en selfs hoofraamomgewings. Die probleem is egter dat die matrikse onbeheerbaar groot en kompleks begin raak. Sodra die TKM metode by internetwerke gebruik word kan die matrikse nog meer kompleks begin raak aangesien drie-dimensionele matrikse dan nodig mag wees om ook aan te dui wat die regte se invloed is in die verskillende netwerke. Figuur 4.2. is 'n voorstelling van 'n TKM in 'n netwerkomgewing.

	OBJEKTE			
SUBJEKTE	MODEM 1	LEêR 1	DRUKKER 1	LEêR 2
GEBRUIKER 1	L		L	
GEBRUIKER 2	OLS	S		
GEBRUIKER 3	S			
GEBRUIKER 4	LS		S	
GEBRUIKER 5				
GEBRUIKER 6				
GEBRUIKER 7				
GEBRUIKER 8		L		

FIG 4.2. TOEGANGSKONTROLE MATRIKS.

In FIG 4.2. word aangedui dat Gebruiker1 leesregte het tot Modem1. Gebruiker 4 het lees en skryfregte tot Modem 1.

4.4. PAD-KONTEKSMODEL (PCM)

Die vorige twee metodes kan beskryf word as die klassieke benadering tot die beheer van regte in 'n rekenaaromgewing wat, later aangepas is om ook in netwerke en internetwerke aangewend te word.

As gevolg van die evolusie in die rekenaar- en netwerkomgewing, begin die gebruik van groot en intergeskakelde netwerke 'n alledaagse verskynsel word. In hierdie meer komplekse omgewing kan die gewone subjek-objek afbeelding van die vorige twee metodes nie meer aan die eise van die omgewing voldoen nie.[64][132] Die grootste probleem van die twee metodes is dat die kontrolelyste en kontrolematrikse baie groot en onbeheerbaar begin word.

4.4.1. INLEIDING TOT DIE PAD-KONTEKSMODEL.

Tradisionele rekenaarstelsels was altyd enkel-domein stelsels met een gasheerrekenaar wat die stelsel beheer het en sekerheid afgedwing het. Die meer algemene gebruik van netwerke en ontwikkelings in die veld van netwerke en verspreide verwerking het veroorsaak dat die nuwe multi-domein stelsels ontstaan. As gevolg van die multi-domain omgewing, het dit nodig geword om 'n nuwe benadering of metode tot netwerksekerheid te ontwikkel. So 'n metode is die sogenaamde Pad-Konteksmodel of "Path Context Model" wat ontwikkel is deur Boshoff en Von Solms by die Randse Afrikaanse Universiteit.[6][126][132]

Figuur 4.3. is 'n voorstelling van 'n multi-domein stelsel vir 'n kort illustrasie van die probleme wat by multi-domein stelsels soos onder andere netwerke voorkom.

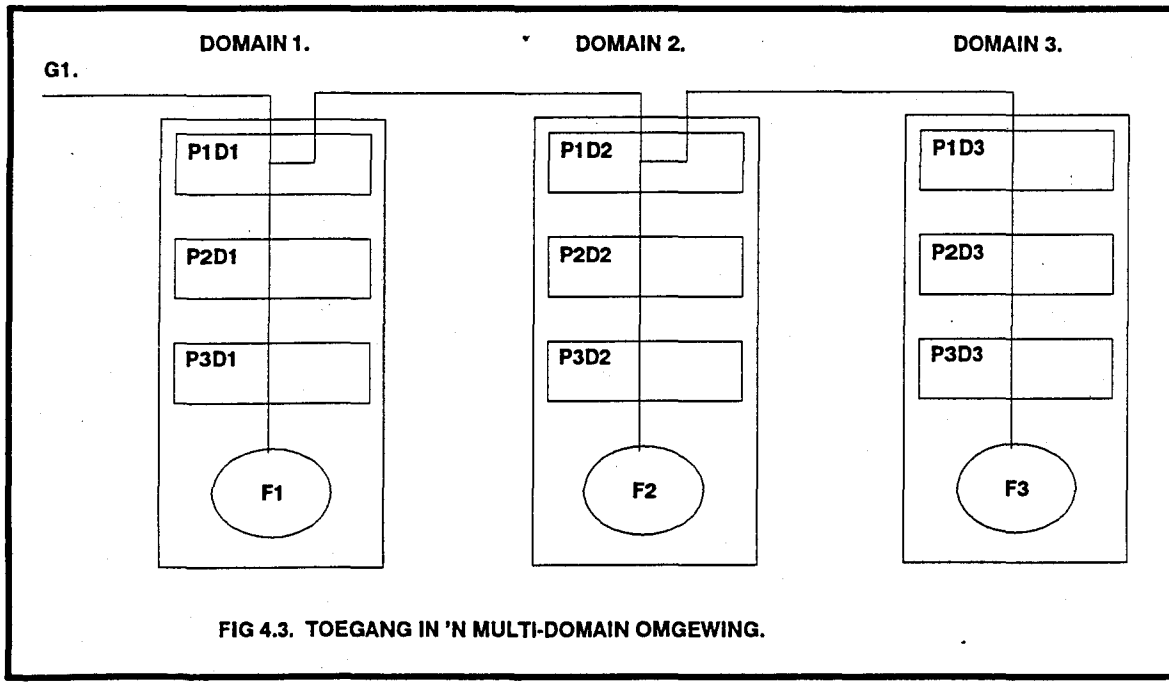


FIG 4.3. TOEGANG IN 'N MULTI-DOMAIN OMGEWING.

Fig 4.3. dui 'n poging aan van 'n gebruiker G1 wat inligting vanaf 'n leêr F3 wil onttrek. Om die inligting te bekom is inligting uit leêrs F1 en F2 ook nodig. Die drie leêrs kom voor in drie verskillende domeine en die gebruiker is nie bewus daarvan dat leers F1 en F2 betrokke is by die proses nie en ook nie van die multi-domein probleem nie.

G1 teken aan in die stelsel deur middel van stelselprogrammatuur P1D1 in domein D1 en versoek inligting uit leêr F3. P1D1 neem beheer oor die hele verwerking oor en sal ook alle verdere verwerking beheer. Om die versoek uit te voer word inligting uit F2 en F3 benodig. P1D1 rig 'n versoek aan P1D2 vir die inligting en P1D2 rig weer 'n verdere versoek aan P1D3 vir die inligting in leêr F3. Die gebruiker mag totaal onbewus wees van die betrokkenheid van P1D2 en P1D3 by die hele proses. En P1D3 mag ook totaal onbewus wees van wie G1 is en wie die oorspronklike versoek gerig het.

Uit voorafgaande bespreking behoort dit duidelik te wees dat die feit dat die ware inisieerder van die versoek en sekere van die prosesse wat die versoek uitvoer totaal onbewus is van mekaar en dat dit vir netwerksekerheid onaanvaarbaar is. Dit is maar 'n baie vereenvoudigde voorstelling van die probleme wat by 'n multi-domein omgewing kan geld.

4.4.2. OORSIG VAN DIE PAD-KONTEKSMODEL.

Enige subjek wat toegang tot 'n objek wil verkry benodig sekere programmatuur en apparatuur om die versoek te kan uitvoer. Voorbeelde van sulke programmatuur en apparatuur is die bedryfsstelsel, kommunikasieprogrammatuur en kommunikasieverbindings. Dit beteken dat daar sekere toegangspaaie is tussen die subjek en die objek. Die PCM benadering berus op die feit dat die aantal toegangspaaie eindig is en dat sekere van die toegangspaaie afgedwing kan word tydens 'n bepaalde versoek.

Indien 'n objek se versoek tot toegang tot enige van die komponente van die toegangspad beheer kan word, kan hy verplig word om 'n spesifieke pad te volg en kan toegang tot die subjek selfs geweier word. Deur elke objek met een of meer toegangspaaie te verbind kan toegang tot die objek beheer word tot slegs versoeke wat die regte pad gebruik.

Die toegangspaaie wat met elke objek verbind word staan bekend as die objek se "Sekerheidsprofiel". Die programmatuur en apparatuur komponente wat die toegangspad uitmaak word die "Bagasie" genoem.

Die PCM hanteer 'n versoek dus as volg :
'n Subjek rig 'n versoek vir toegang tot 'n bepaalde objek. Die versoek word verwerk en bagasie word langs die pad na die objek versamel. Sodra die objek bereik word, word die bagasie met die objek se sekerheidsprofiel vergelyk voor die toegang verwerp of toegelaat word.

Die model is tot dusver nog net op 'n losstaande mikrorekenaaromgewing onder die MS-DOS bedryfstelsel geïmplimenteer. Die volgende fase is om die model ook op netwerke en later selfs internetwerke te implimenteer. Die skrywer is van mening dat die PCM 'n baie belangrike bydra het om te lewer in die netwerksekerheidsomgewing aangesien die verskillende komponente waaruit 'n netwerk bestaan, soos kommunikasieverbindings, modems, leêrbedieners ensovoorts maklik gebruik kan word vir die opstelling van 'n objek se sekerheidsprofiel.

Die ontwikkeling van PCM is nog in die begin stadium en dit is 'n baie relevante veld vir verdere studie.

4.5. SAMEVATTING.

Die beheer van regte in 'n netwerk is 'n belangrike komponent van enige netwerksekerheidsmaatreëls. Die probleem is dat die meerderheid van metodes wat gebruik word om die regte te beheer aanvanklik ontwikkel is vir losstaande rekenaars en enkel-domein stelsels en later aangepas is vir gebruik in netwerke en ander multi-domein stelsels. Hierdie tradisionele metodes soos die Toegangskontrolelyste en Toegangskontrolematrikse kan nie meer aan die eise van die multi-domein omgewings voldoen nie aangesien die lyste en matrikse te groot en ingewikkeld word om effektief verwerk te kan word.

'n Behoefte het begin ontstaan vir die ontwikkeling van 'n nuwe en meer moderne benadering tot die probleem van die bestuur en beheer van regte in die multi-domein omgewing. So 'n metode is die Pad-Konteksmodel(PCM). Die PCM is maar nog in die beginfases van ontwikkeling maar kan moontlik in die toekoms met vrug aangewend word. Die ontwikkeling van nuwe soortgelyke metodes kan 'n baie interessante en relevante veld wees vir verdere studie.

HOOFSTUK 5.

KOMMUNIKASIEVERBINDINGS.

KOMMUNIKASIEVERBINDINGS.

5.1 INLEIDING.

Die kommunikasieverbindings in 'n netwerk is een van die kwesbaarste punte in 'n netwerk.[28] WRIGHT[62] beskryf die onderskepping van elektromagnetiese uitstraling deur die Britse Sekerheidsdiens (MI5), en die Britse Inligtingsdiens(MI6) om kommunikasie van ander lande se Ambassades te onderskep. Die kommunikasieverbindings is baie maklik om te bereik, en onderskepping van kommunikasie kan op enige plek op die verbinding voorkom. Dit is feitlik onmoontlik om die hele verbinding te beskerm. As gevolg van die uitbreiding in gebruik van netwerke, word daar van al hoe meer verskillende soorte kommunikasieverbindings gebruik gemaak. Die kommunikasieverbindings sluit in gewone gedraaidepaar-kabel("twisted pair cable") tot radioverbindings en satelietverbindings.[30]

'n Verdere probleem is die feit dat die meeste navorsing oor ontwikkeling van beskermingsmaatreëls teen onderskepping van inligting deur regeringsinstansies as militêre projekte gedoen word. Die resultate van die navorsing en ander inligting oor die projekte is feitlik hoogs geklassifiseerd en word nie bekend gemaak nie, en indien wel, slegs aan sekere goedgekeurde instansies. 'n Voorbeeld van so 'n projek, is die TEMPEST-projek deur die Nasionale Sekerheidsagentskap(NSA) van die Verenigde State van Amerika.[63] Die TEMPEST-projek handel oor die ontwikkeling van teenmaatreëls vir die beperking van elekrtomagnetiese uitstraling vanaf rekenaartoerusting en kommunikasieverbindings.[63]

Elke soort verbinding beskik oor sekere kenmerke, voordele en nadele en oefen 'n baie groot invloed op die sekerheid van die netwerk uit. Tegnologie op die gebied ontwikkel vinnig en daar word feitlik nooit in die ontwikkeling van die verbindings aandag gegee aan sekerheidsaspekte nie. Dit is 'n ernstige probleem dat die nuwe verbindingstegnologie in die meeste gevalle die ongemagtigde onderskepping van die boodskappe oor die verbinding vergemaklik. [31] 'n Enkele voorbeeld hiervan is die gebruik van satelietverbindings. Enige satellietboodskap kan op enige plek in 'n radius van ongeveer 160 kilometer om die punt waarvoor die boodskap bedoel is, onderskep word.[9]

Buiten probleme met die geheimhouding van die boodskappe op die verbindings, is sekere van die verbindings ook in meerdere en mindere mate bestand teen natuurlike inmenging van buite wat die integriteit van die boodskappe kan beïnvloed. Die inmenging sluit in geruis en verswakking van boodskap as gevolg van uitstraling.

Die res van die hoofstuk sal uit die volgende dele bestaan :

5.2] Terminologie.
'n Kort bespreking van terme wat in die hoofstuk gebruik sal word.

5.3] Bespreking van verskillende verbindings.
Bespreking van die bestaande en toekomstige kommunikasieverbindingstegnologieë. Aandag sal gegee word aan die volgende soorte verbindings:

- Gedraaidepaar-kabels.
- Koaksialekabels.
- Radioverbindings.
- Optieseveselverbindings.
- Mikrogolfverbindings.
- Satellietverbindings.
- Sellulêre telefoonverbindings.

Die kenmerke, voor- en nadele, integriteit en sekerheidsaspekte van die verskillende tipes kommunikasieverbindings sal bespreek word.

5.2 TERMINOLOGIE.

Alvorens daar voortgegaan word met die bespreking van verskillende soorte kommunikasieverbindings, is dit nodig om na 'n paar belangrike terme te kyk.

- 'n Kommunikasieverbinding is die draer van die dataseine tussen twee nodes. 'n Voorbeeld van 'n kommunikasieverbinding is die telefoonkabel tussen twee telefone. Die verbinding maak die eerste vlak (fisiese vlak) van die OSI- verwysingsmodel uit. Ander terme wat ook in die literatuur gebruik word, is : transmissiemedia en kommunikasiemedia. [25][26][[30][32]

- 'n Kommunikasieverbinding kan in verskillende KANALE opgedeel word. Elke kanaal kan gebruik word om 'n sein te stuur. Verskillende seine kan gelyktydig deur die verskillende kanale gestuur word. Elke kanaal bestaan uit 'n sekere bandwydte. [9][26]

- Bandwydte dui die verskil tussen die hoogste en laagste vlak van 'n kanaal se frekwensie aan.[9][26]

- Basisbandtransmissies is die versending van 'n sein oor 'n kanaal, waar die kanaal die hele bandwydte van die verbinding insluit.[9][26]

- Wyebandtransmissie is die versending van seine oor 'n verbinding wat in verskillende kanale opgedeel is.[9][26]

- Kommunikasieverbindings kan in twee groepe verdeel word naamlik : Geleidingsverbindings en Uitstralingsverbindings. [26][34]

- Geleidingsverbindings is verbindings wat gebruik maak van een of ander geleier wat die seine oordra. Daar is dus 'n fisiese koppeling tussen die twee nodes. Voorbeelde is :
  - telefoonkabels,
  - gedraaidepaar-kabels,
  - koaksialekabels,
  - optiesevesels.

- Uitstralingsverbindings maak gebruik van uitstralings oor die lug om seine oor te dra. Hier is daar dus nie 'n fisiese verbinding tussen die twee nodes nie. Voorbeelde is :
  - radioverbindings,
  - satelietverbindings,
  - mikrogolfverbindings,
  - sellulêre telefoonverbindings.

- Bisse-per-sekonde(bps) dui aan hoeveel bisse per sekonde oor 'n verbinding gestuur kan word.

- Aftap.
  Dit is die aksie wat 'n oortreder gebruik om inligting wat oor 'n kommunikasieverbinding beweeg te onderskep. Aftapping word gedoen deur middel van 'n aftapapparaat("wiretap"). Die apparaat kan aan die verbinding gekoppel word deur dit aan die verbinding te heg sonder om dit te beskadig. 'n Ander metode is om die verbinding deur te sny en die aftapapparaat en die twee dele van die verbinding aanmekaar te las.[10][28][29]

5.3. BESPREKINGS VAN VERSKILLENDE SOORTE VERBINDINGS.

In hierdie afdeling sal 'n kort bespreking van die verskillende soorte kommunikasieverbindings volg. Dit is belangrik om hier na die verbindings se kenmerke, voordele, nadele, integriteit en invloed op sekerheid te kyk. In baie gevalle word 'n kommunikasieverbinding nie gekies omdat dit die veiligste is nie, maar wel omdat daar ander voordele soos koste en gemak van installasie is. Wat egter in baie gevalle nie besef word nie, is dat die keuse van 'n goedkoop verbinding baie addisionele kostes kan meebring as gevolg van ekstra maatreëls wat getref moet word om die verbindings te beskerm.

Kommunikasieverbindings kan gesien word as die kwesbaarste plek in 'n netwerk. Die verbinding is gewoonlik maklik om te bereik. In al die literatuur wat die skrywer tot op hede bestudeer het oor kommunikasieverbindings, word daar net in uitsonderlike gevalle, en dan ook net terloops 'n sin of twee oor die sekerheidsaspek gemeld. Feitlik die hele bespreking word bestee aan 'n bespreking van die tegniese aspekte, kostevoordele en die integriteit van die verbindings.[9][10][14][18][25][26][30][34]

In die res van die hoofstuk word daar gepoog om uit die bestaande literatuur soveel as moontlik inligting te bekom oor sekerheid. Waar genoegsame literatuur oor sekerheid nie opgespoor kan word nie, mag dit nodig wees om afleidings in verband met sekerheid te maak vanuit die bespreking van die tegniese aspekte en integriteit van die verbindings.

5.3.1] GEDRAAIDE PAAR-KABELS. [1.]

5.3.1.1] Algemene beskrywing.

'n Gedraaidepaar bestaan uit twee geïsoleerde koperdrade wat in die vorm van 'n spiraal gedraai is. Een kabelpaar vorm een kommunikasieverbinding. Gewoonlik word 'n hele aantal van die kabelpare in 'n enkele kabel saamgevoeg deur dit met 'n beskermende laag te omvou.[32][26]

Gedraaidepaar-kabels kom voor in twee tipes naamlik :

- onbeskermde gedraaidepaar,
- beskermde gedraaidepaar.

1. Verwysings : [2][9][10][25][26][30][32][34][39][41][48]

Onbeskermde gedraaidepaar kabels is die goedkoopste van alle transmissieverbindings. Die kabel word gewoonlik gebruik vir normale telefoonkabels. Die kabel beskik oor minimum isolering, wat veroorsaak dat dit 'n baie hoë vlak van elektromagnetiese uitstraling het. Verder word die kabels ook sterk beïnvloed deur uitstraling van ander bronne. Alhoewel die kabel baie maklik is om te gebruik, is dit baie onbetroubaar.[26][10][30]

Beskermde gedraaidepaar-kabels beskik oor 'n verdere gevlegde metaalomhulsel. Die beskermde kabels is baie beter geïsoleer, en is verder minder vatbaar vir elektromagnetiese uitstraling vanaf ander bronne. Verder is die uitstraling van die kabel self ook baie minder.[26][10][30]

Gedraaidepaar-kabel is die mees algemene verbinding wat in telekommunikasie netwerke gebruik word. In die V.S.A. word gedraaidepaar-kabels volgens die American Wire Gause of AWG stelsel geklassifiseer. Die AWG-klassifikasie dui aan wat die dikte van die kabel is. Hoe dikker die kabel, hoe laer is die AWG nommer. Die belangrikste kabels wat in telekommunikasienetwerke gebruik word, is 22 en 26 AWG-kabels vir kortafstandkabels, en 19 AWG kabels vir langafstande.[32][34]

Die dikte van die kabel is van belang aangesien dit bepaal wat die kapasiteit van die kabel is. Hoe dunner die kabel is, hoe laer is die frekwensie wat die kabel kan dra. Met die gebruik van gedraaidepaar kabels in telekommunikasienetwerke, kan inligting teen 'n spoed van tussen 300 bps tot so hoog soos 19200 bps versend word. Spesiale kabels wat ontwikkel is vir LAN toepassings kan 'n transmissiespoed van tot 10 miljoen bps behaal.[26][34]

5.3.1.2. Sekerheidsaspekte van gedraaidepaar kabels.

Die grootste gevaar by die gebruik van gedraaidepaar-kabels, gesien vanuit 'n netwerksekerheidsoogpunt, is die gevaar van aftapping. Beide aktiewe en passiewe aftappings is baie maklik om te maak. Daar bestaan twee maniere van meeluister. Passiewe meeluister waar die indringer slegs na die kommunikasie luister , en aktiewe meeluister waar die indringer die vloei van die kommuniksie beïnvloed, deur byvoorbeeld addisionele inligting op die verbinding te plaas. [10]

'n Bydraende faktor is die feit dat die kabel van geleiding gebruik maak om seine te vervoer. Dit beteken dat die sein oorgedra word na enige ander geleier wat met die kabel in aanraking kom.[10][26]

Gedraaidepaar-kabel beskik gewoonlik ook oor baie swak isolering wat die fisiese kabel omring. Van die goedkoopste kabels is slegs omring deur papier. Die duurste kabels is omring deur 'n deeglike isolasie van "Polyethelene" of "Polyvinyl-chlorie" en/of 'n metaalomhulsel. Hoe beter die kabel se omhulsel, hoe moeiliker is dit om die kabel te bereik om die aftapping te maak.[32][34]

'n Verdere probleem is die elektromagnetiese uitstraling van die gedraaidepaar-kabels. Die uitstraling van die kabels is van so 'n aard dat dit onderskep en ontleed kan word, sonder om fisies met die kabel in kontak te kom. Hoe beter die isolering van die kabel, hoe minder is die uitstraling van die kabel.[32] [34][9] Swak geïsoleerde kabels se uitstraling kan so hoog wees dat die uitstraling deur 'n gewone sakradio opgevang kan word. Die sein kan dan deur middel van 'n ossiloskoop ontleed word om die inligting te onttrek.[39]

5.3.2. Koaksialekabels.[2.]

5.3.2.1 Algemene beskrywing.

'n Koaksialekabel bestaan uit 'n enkele geleier wat omring is deur verskillende vlakke van isolasiemateriaal, met 'n verdere beskermde omhulsel buite om. Die kabel is baie goed geïsoleer en daar vind feitlik geen elektromagnetiese uitstraling plaas nie. Verder kan feitlik geen bestraling van buite die kabel bereik nie. Dit verseker dat die kabel uiters betroubaar is en dit kan 'n baie hoër dataverkeer dra. In baie gevalle word 'n groep koaksialekabels saam in 'n bondel binne in 'n omhulsel saam gegroepeer om 'n saamgestelde kabel te vorm.[32][26][30]

In baie gevalle word nie al die kabels in die saamgestelde kabel vir kommunikasie gebruik nie. In so 'n saamgestelde kabel word daar gewoonlik 'n paar van die kabels ongebruik gelaat. Die ongebruikte kabels se doel is, om as plaasvervanger te dien as een van werkende kabels beskadig raak. [34][32]

Daar bestaan drie soorte koaksialekabels naamlik basisbandkabel ,wyebandkabel en draerbandkabel.

2. Verwysings : [2][9][10][25][26][30][32][34][39][41][48]

'n Basisbandkabel word gebruik om digitale seine oor te dra. Die hele frekwensiespektrum van die kabel word slegs deur die een sein gedek. Dus kom daar slegs een kanaal op 'n basisbandkabel voor.'n Wyebandkabel maak van analoogseine gebruik. Die kabel kan verskeie kanale dra. Die bandwydte van die kabel verdeel in verskeie kanale, byvoorbeeld 'n kabel met 'n bandwydte van 100 MHz kan opgedeel word in 10 kanale van 10 MHz elk. 'n Draerbandkabel bestaan uit slegs een kanaal, dieselfde as basisband, maar dra analoogseine in plaas van digitale seine.

Koaksialekabels beskik oor 'n groter bandwydte van tot 60 MHz en hoër transmissie spoed as gedraaidepaar kabels. Gewone koaksialekabels kan tot 10800 stem-graad kanale dra. [34]

Daar kan wel van 'n metode genaamd "skin effect" gebruik gemaak word om die kabel se bandwydte bo die 60 MHz grens uit te brei. Hier word van hoë frekwensies gebruik gemaak wat elektromagnetiese velde en uitstraling buite die kabel veroorsaak. Die goeie isolering veroorsaak dat die uitstraling tussen die kabel en die isoleringsmateriaal vasgevang is. Dus kan die verhoogde bandwydte gebruik word vir kommunikasie-doeleindes. [34][32]

5.3.2.2. Sekerheidsaspekte van Koaksialekabels.

Koaksialekabels beskik oor 'n baie beter isolasiemateriaal as wat die geval by gedraaidepaar-kabels is. Die goeie isolering skakel baie van die probleme genoem by gedraaidepaar-kabels uit. Dit is égter nog steeds moontlik om die kabel te tap as die beskermde omhulsel van die kabel oopgesny word.

Die probleem van elektromagnetiese uitstraling is as gevolg van die goeie isolering ook baie beperk. Die probleem is egter dat as die kabel se beskermde omhulsel beskadig word, kan die uitstraling hier ontsnap en beteken die res van die omhulsel niks. Die kwesbaarste plek aan die kabel is die eindpunte van die kabels. Die omhulsel van die kabel moet by die punte afgesny word om die kabel aan die koppelvlakke te heg. As die koppelvlakke nie self geïsoleer is nie, kan die uitstraling hier ontsnap.[39]

Koaksialekabels dra data oor verskillende kanale en teen 'n hoë spoed. Dit maak dit vir die indringer moeilik om die data te onderskep sonder baie ingewikkelde en gevorderde toerusting. Die toerusting moet eerstens tussen die verskillende kanale kan onderskei, en moet verder ook die verhoogde transmissiespoed kan hanteer.[39][10]

Soos reeds genoem, kan die gebruik van die sogenaamde "skin effect" gebruik word om verhoogde bandwydte te verkry.[34][32] Hierdie gebruik kan egter groot sekerheidsprobleme veroorsaak as daar enige swakplekke in die kabel se isolering bestaan. Die elektromagnetiese uitstraling kan dan hier ontsnap en onderskep word.[39]

5.3.3. Optieseveselverbindings.[3.]

5.3.3.1. Algemene beskrywing.

Die kabel wat die seine dra is van dun glasvesel gemaak. Die seine word deur middel van ligpulse deur die vesel gestuur. Die aantal kanale waarin die vesel opgedeel kan word, is baie meer as die aantal kanale op koperdraad. [32][9][26] [30]

Optiesevesels het baie min uitstraling en beïnvloed mekaar nie. Verder is die vesels baie ligter as ander kabeltipes en beskik ook oor beter geleiereienskappe. In die toekoms sal daar al meer van optieseveselkabels gebruik gemaak word om ander kabeltipes te vervang.[9][[26][30]

Optiesevesels beskik oor 'n baie hoë inligtingsoordragkapasiteit. Optiesevesels met 'n bandwydte van 500MHz word reeds gebruik.[34] Eksperimente by die BELL laboratoriums in die V.S.A. het reeds 30000 gelyktydige oproepe op een vesel geplaas.[34] Die AT&T-onderneming in die V.S.A. gebruik optiesevesels wat 95Mbps oor een vesel kan stuur.[32]

'n Verdere kenmerk van optiesevesel is dat die sein wat deur die vesel beweeg nie so vinnig verswak as by ander kabeltipes nie. Dit is dus nie nodig om die sein so baie te versterk nie. Daar is 'n optieseveselkabel van 104KM oor die bodem van die see tussen Tainan, op die Taiwanese hoofeiland, en Makung op die Peng Hu Eilande gelê. Die kabel beskik oor geen herhalers(repeaters) om die seine te versterk nie. Alhoewel daar 'n 60% verswakking in die sein oor die afstand voorkom, bestaan daar nog steeds 'n 40% veiligheidsbuffer voor die sein nie meer opgevang kan word by die bestemming nie. Die kabel is tussen Julie en Augustus 1988 aan 'n reeks toetse onderwerp en in die tydperk is 'n zero bis fouttelling verkry.[42]

3. Verwysings : [2][9][10][25][26][30][32][34][41][42][53][54]

Nuwe ontwikkelings in die optieseveselbedryf laat waarnemers die stelling maak dat herhalerlose kabels van langer as 250km reeds moontlik is.[42]

5.3.3.2 Sekerheidsaspekte.

Optiesevesels beskik oor twee baie belangrike sekerheidsvoordele. Die eerste is die feit dat dit uiters moeilik is om optiesevesels te tap. Om 'n aftapping op 'n optiesevesel te maak moet die vesel fisies deurgesny word. Die probleem is dan om die vesel weer aanmekaar te las. Die lig wat deur die vesel beweeg, word deur enige beskadiging in die vesel beïnvloed. 'n Optiesevesel netwerk moet baie deeglik ingestel word en enige wanbalans in netwerk is maklik merkbaar.

Die tweede voordeel is dat optiesevesels nie van elektrisiteit gebruik maak om seine te vervoer nie, maar wel van lig. Lig het geen elektromagnetiese uitstraling nie, en dus is enige geleidingsaftapping waardeloos op 'n optiesevesel.[10]

Die hoë transmissiespoed en baie verskillende kanale op 'n enkele vesel maak aftapping van die vesel baie moeilik.

As daar gedeeltes van 'n netwerk bestaan waar indringers kan poog om die verbindings te tap, kan hierdie verbindings met optieseveselverbindings vervang word.

Die gebruik van lang herhalerlosekabels, wat vroeër reeds bespreek is,[42] het 'n verdere positiewe invloed op die sekerheid van die kabel. Enige herhaler wat aan 'n optieseveselkabel gelas word, skep 'n geleentheid om die kabel te tap. As daar op enige ander manier 'n tap aan die kabel geheg wil word, moet die kabel fisies beskadig word. Dit sal 'n verlies in seinsterkte veroorsaak wat dadelik by ontvangs van die sein opgemerk sal word.

Alhoewel optiesevesels in die algemeen as uiters bestand teen aftappings beskou word, word daar egter beweer dat dit wel moontlik is om dit te doen. Daar word beweer dat as die omhulsel van die optieseveselkabel oopgesny word, en die kabel effens gebuig word, daar 'n klein hoeveelheid lig kan ontsnap. Solank die kabel nie te ver gebuig word nie, kan die verswakking in die sein nie waargeneem word nie. Dit kan wel moontlik wees om die lig wat ontsnap te ontleed en sodoende die inligting wat oor die kabel vloei te onderskep.[52][53][54]

5.3.4. RADIOVERBINDINGS.[4]

5.3.4.1. Algemene beskrywing.

Radioverbindings maak gebruik van radios en radioseine om inligting tussen twee punte oor te dra. Elke punt, of terminaal, moet oor sy eie versender en ontvanger beskik om seine te versend en te ontvang.

Die gebruik van radioverbindings vir die oordrag van data is nie 'n ou begrip nie, maar as gevolg van verskeie probleme bestaan daar baie min toepassings. Daar sal nog baie navorsing op hierdie gebied gedoen moet word voor die gebruik van radioverbindings algemeen word.

Een van die eerste toepassings van radioverbindings in datakommunikasienetwerke is die ALOHA-netwerk wat deur die Universiteit van Hawaii ontwikkel is. Radioverbindings is gekies aangesien die netwerkterminale op verskillende van die Hawaii-eilande moes verbind. Dit sou baie moeilik en duur wees om al die eilande met behulp van kabels te verbind. Die netwerk het redelik goed gewerk solank daar nie baie terminale aan die netwerk gekoppel was nie. Probleme het begin ontstaan toe die netwerk baie terminale begin bykry het. Te veel terminale het begin meeding vir die beskikbare kanale. Verder het ander radiouitsaaibronne die verbindings nadelig begin beïnvloed.[26][17]

By die PRINCETON Universiteit in die V.S.A. is 'n LAN ontwikkel wat van radioverbindings gebruik maak. Die netwerke staan bekend as "Local Area Wireless Networks" of LAWNS. Die radioseine wat hier gebruik word, maak van die 902 tot 928 MHz frekwensiespektrum gebruik. Die LAWNS maak van die AX.25 protokol gebruik. Die protokol is 'n weergawe van die gewone X.25 protokol wat spesiaal vir radiokommunikasie ontwikkel is.[103]

Volgens Internasionale ooreenkomste word die frekwensiespektrum in verskillende bande opgedeel. Sekere frekwensies word volgens die ooreenkoms gereserveer vir internasionale gebruik soos byvoorbeeld skeepsverkeer. Ander frekwensies kan 'n spesifieke land na eie behoeftes hanteer. In die meeste lande word bepaalde frekwensies vir gebruik in kommunikasienetwerke gereserveer.[47][50][32]

4. Verwysings : [9][10][17][26][34][38][39][52][103]

In Suid-Afrika word die toekenning en registrasie van die frekwensie deur die Suid-Afrikaanse Departement van Pos en Telekommunikasie(SAPT) beheer. Die inligting oor welke frekwensies vir watter doeleindes gebruik word, word as sensitiewe inligting beskou, en word nie aan die publiek bekend gemaak nie.[52]

5.3.4.2. Sekerheidsaskepte van Radioverbindings.

Radioverbindings kan as die kwesbaarste en onbetroubaarste verbindingsmedium beskou word. Aangesien daar van gewone radioseine gebruik gemaak word, kan enige iemand met 'n radio die seine opvang.

In 'n poging om die probleem uit te skakel, word die inligting oor toekenning van frekwensies vir spesifieke doeleindes deur die SAPT as sensitiewe inligting beskou, en word die inligting nie bekend gemaak nie. Die SAPT was nie eers bereid om aan die skrywer inligting oor die frekwensies bekend te maak vir gebruik in die verhandeling nie.[52] Dit is egter nie moeilik om te bepaal watter golflengtes gebruik word nie.

Die LAWNS in die V.S.A. maak van die 902 tot 928 MHz frekwensiespektrum vir kommunikasie gebruik. Die seine is moeilik om te onderskep en word gekombineer met sogenaamde verspreidespektrumtegnologie om sekerheid te verseker. Die verspreide-spektrum ("Spread Spectrum") tegniek het gedurende die 2e Wêreldoorlog ontstaan vir die beskerming van militêrekommunikasie. Die sein word volgens 'n sekere patroon oor die frekwensiespektrum versprei. Die versender en die ontvanger moet beide dieselfde verspreidingspatroon gebruik om te kommunikeer. As iemand probeer om die sein te onderskep sal hy presies moet weet wat die verspreidingspatroon is.[103]

'n Verdere probleem is dat radioverbindings baie beïnvloedbaar is deur steurings vanaf ander bronne. Sulke steurings kan afkomstig wees van ander radio uitsaaibronne of industriële toerusting.[47]

Die enigste veilige manier om inligting te beskerm wat oor radioverbindings gestuur word, is om van enkripsie gebruik te maak.

5.3.5. MIKROGOLFVERBINDINGS.[5.]

5.3.5.1. Algemene beskrywing.

Mikrogolfverbindings maak van baie hoë frekwensie radioseine gebruik. As gevolg van die kort golflengte van die mikrogolfseine, trek die seine in 'n reguit lyn en word vanaf enige obstruksie weerkaats. Dit het tot gevolg dat die seine vanaf spesiale lense weerkaats en gefokus moet word, as die ontvanger nie binne sigafstand van die versender is nie.

Aangesien die mikrogolfseine in 'n reguit lyn beweeg, kan dit nie saam met die aarde se ronding beweeg nie, en moet dus elke paar kilometer opgevang word deur 'n spesiale mikrogolftoring , en weer versend word. Die twee torings moet binne sigafstand van mekaar wees, en daar mag geen versperring tussen hulle wees nie.

In die meeste gevalle word 'n sein deur verskillende torings herlei voor dit sy bestemming bereik.[26][32][34]

5.3.5.2. Sekerheidsaspekte van Mikrogolfverbindings.

Mikrogolfsiene beskik oor dieselfde probleme wat ondervind word met radioseine. Die mikrogolfseine beweeg ook deur die lug en kan deur enige iemand met die regte toerusting onderskep word. Daar bestaan geen manier om die sein te isoleer of af te skerm nie. Dit veroorsaak dat mikrogolwe 'n baie onveilige medium vir dataoordrag is.

'n Verdere probleem, uit 'n sekerheidsoogpunt, is die feit dat daar by mikrogolfseine die probleem van akkurate rig van die seine bestaan. Die ontvanger van die sein moet binne sig van die sender wees, soos reeds genoem. Om egter te verseker dat die sein wel die ontvanger tref, word die sein oor 'n breër pad gestuur. Dit veroorsaak dat die gebied waarin die sein onderskep kan word vergroot, en enige iemand wat tussen twee mikrogolftorings staan, kan die seine onderskep.

5. Verwysing :[2][9][10][25][26][30][32][34][39][41][48]

Een voordeel van mikrogolfseine is dat daar normaalweg 'n hoë volume van verkeer oor een mikrogolfskakel beweeg op dieselfde tyd. Dit is dus moeilik om 'n spesifieke sein te onderskei sonder gespesialiseerde toerusting.[10]

5.3.6. SATELLIETVERBINDINGS.[6.]

5.3.6.1. Algemene beskrywing.

Hier word die kommunikasieseine deur middel van satelliete wat in 'n baan om die aarde beweeg, herlei. Die seine het baie van die karakteristieke van mikrogolfseine. Die frekwensie is ook baie hoog en beweeg in 'n reguitlyn. Die seine word vanaf 'n sender op die aarde na die satelliet gesein. Die sateliet vang die sein op, versterk dit, en stuur dit dan weer na 'n ontvanger op die aarde, of kan die sein ook na 'n ander satelliet stuur as die ontvanger nie binne 'n reguit lyn van die satelliet is nie.[26][32][34]

5.3.6.2 Sekerheidsaspekte.

Die probleem met satellietverbindings is, dat die sein wat teruggestuur word aarde toe, oor 'n baie groot gebied ontvang kan word. Die gebied word die satelliet se voetspoor genoem. Al die ontvangerstasies in die voetspoor kan die seine opvang. In die geval van die INTELSAT-kommunikasiestelsel, dek drie satelliete die hele aarde se oppervlakte. Dit veroorsaak dat elke satelliet se voetspoor ongeveer 33.3% van die aarde se oppervlak dek.[9][32][10]

5.3.7. SELLULÊRE TELEFOONVERBINDINGS.[7.]

5.3.7.1. Algemene beskrywing.

Sellulêre telefoonverbindings is 'n samevoeging van telefoon- en radio-tegnologie. Hier maak die telefoon nie van kabels gebruik om seine na 'n ander telefoon te vervoer nie, maar wel van radioseine. Dit is nodig aangesien daar 'n groot behoefte begin ontstaan het aan draagbare telefone. Die grootste gebruik van die sellulêre telefoon is vir mobiele telefone in voertuie.

6. Verwysings : [2][9][10][25][26][30][32][34][39][41][48]
7. Verwysings : [10][26][31][34][37][38][51]

Aangesien elke oproep van twee kanale gebruik maak, moes 'n metode gevind word om dieselfde frekwensie vir meer as een oproep te kan gebruik. Daarom word 'n geografiese area in verskeie selle opgedeel en elke sel beskik oor 'n laefrekwensiesender. Sodra 'n oproep gemaak word, ken 'n sentrale beheersentrum twee kanale aan die oproep toe. Die telefoon gebruik die frekwensies in sy huidige sel, terwyl 'n ander telefoon dieselfde kanaal in 'n ander sel kan gebruik sonder dat die twee met mekaar inmeng, aangesien die versender/ontvanger in die sel net sterk genoeg is om die sel self te dek.

Sodra die voertuig in 'n ander sel inbeweeg, begin die telefoon die nuwe sel se kanale gebruik. Indien die kanaal reeds in gebruik is, word twee nuwe kanale deur die sentrale beheersentrum aan die oproep toegeken.[34][32][37]

5.3.7.2. Sekerheidsaspekte van Sellulêre telefone.

Sellulêre telefoone maak ook gebruik van radioseine om inligting oor te dra. Die probleem word vererger deur die feit dat die frekwensies wat gebruik word vir die seine maklik deur 'n frekwensieontleder bepaal word. [31]

As gevolg van nuwe ontwikkelings in die model en "LAPTOP"-rekenaarbedryf, kan rekenaars vanuit 'n motor aan 'n netwerk gekoppel word. Dit maak dit moeilik om indringers op te spoor aangesien hulle kan rondbeweeg. Die oordrag van oproepe tussen selle kan gekruisde lyne en tydelike verlies van verbinding tot gevolg hê, wat die sein se integriteit kan beïnvloed.

'n Belangrike probleem by die gebruik van sellulêre telefoonverbindings kom voor by die oorgee van 'n oproep aan 'n ander sel. Die sein verswak hoe nader die voertuig aan die grens van die sel beweeg. Die verswakking in die sein kan die integriteit van die data wat oorgedra word nadelig beïnvloed. Gedurende die oordragprosedure tussen die twee selle, kom daar soms 'n kort onderbreking in die verbinding voor. Al is die onderbreking net 'n breukdeel van 'n sekonde, kan die data se integriteit nog beïnvloed word.

Dit kan ook gebeur dat frekwensies gedurende die oordrag prosedure gekruis raak en vertroulike inligting op verkeerde frekwesies uitgesaai word.

In Europa is daar 'n gesamentlike navorsingprojek genaamd GSM (pan-European Groupe Speciale Mobile) besig om 'n sellulêre televoonverbindingsnetwerk te ontwikkel wat die hele Europa sal insluit. Een van die vereistes wat aan die begin van die projek gestel is, is die enkriptering van die gebruikerdata wat oor die verbindings beweeg.[51]

5.4. Evaluering van geleidingsverbindings.

Tabel 5.1 is deur die skrywer ontwikkel en vergelyk die verskillende geleidingsverbindings wat bestudeer is met mekaar. Daar sal na verskillende faktore gekyk word waarvan die belangrikste die faktore met betrekking tot sekerheid is naamlik : Integriteit en aftapping.

Die faktore wat by die vergelyking in aanmerking kom, is die volgende :

- Koste. Hoe vergelyk die koste van die verskillende verbindings met mekaar? Dit neem slegs die koste van die verbinding self in ag en nie addisionele kostes om die verbinding te beveilig teen aanvalle of uitstraling nie.

- Bandwydte. Hoe vergelyk die verskillende verbindings se bandwydtes met mekaar? Hoe hoër die bandwydte, hoe meer kanale kan daar op die verbinding voorkom, en hoe meer data kan op een slag oor die verbinding vervoer word.

- Isolering. Dit dui aan hoe goed die verbinding geïsoleer word teen bestraling van buite, en hoe goed die uitstraling van die verbinding self beperk word.

- Uitstraling. Dit dui aan hoe sterk die elektromagnetiese uitstraling van die verbinding self is.

- Invloed van buite. Dit dui aan hoe vatbaar die verbinding is vir uitstraling van ander bronne.

- Integriteit. Dit dui aan hoe goed die verbinding die integriteit van die data wat oor die verbinding beweeg, beskerm.

- Gewig. Dit dui aan hoe swaar die fisiese verbinding is.

FIGUUR 5.2. UITSTRALINGSVERBINDINGS.

	RADIO	MIKROGOLF	SATELLIET	SELLULêRE TELEFOON
KOSTE	GOEDKOOP	GEMIDDELD	DUUR	GEMIDDELD
BANDWYDTE	LAAG	GEMIDDELD	BAIE HOOG	GEMIDDELD
UITSTRALING	BAIE HOOG	BAIE HOOG	BAIE HOOG	BAIE HOOG
INVLOED VAN BUITE	BAIE HOOG	HOOG	LAAG	HOOG
INTEGRITEIT	SWAK	GOED	GOED	REDELIK
GEVAAR VAN MEELUISTER	BAIE HOOG	HOOG	HOOG	BAIE HOOG
GEMAK VAN MEELUISTER	BAIE MAKLIG	MOEILIK	MOEILIK	BAIE MAKLIK
UITBREIBAAR-HEID	HOOG	HOOG	HOOG (DUUR)	LAAG (MIN FREKWENSIES)

Die faktore wat by die vergelyking in aanmerking geneem is, is die volgende (slegs die faktore wat verskil van die faktore genoem by geleidingsverbindings word genoem) :

- Uitstraling. Dit dui aan hoe groot die gevaar van onbeheerde uitstraling van die verbinding is.

- Invloed van buite. Dit dui aan hoe groot die gevaar van inmenging van ander bronne, soos byvoorbeeld geraas en steurings is.

- Uitbreibaarheid. Dui aan hoe maklik dit sal wees om die bestaande verbindings uit te brei.

Fig 5.3. is 'n uittreksel uit 'n verslag genaamd "Defending secrets, Sharing data." van die "Office of Technology Assessment"(OTA) van die Kongres van die Verenigde State van Amerika wat in 1988 opgestel is.[53] Die figuur dui aan wat die hulpbronne is wat 'n indringer benodig om 'n bepaalde verbindingstegnologie te tap.

FIGUUR 5.1. GELEIDINGSVERBINDINGS.

	GEDRAAIDE-PAAR. (ONBESKERM)	GEDRAAIDE-PAAR. (BESKERM)	KOAKSIALE-KABEL	OPTIESEVESEL-KABEL
KOSTE	GOEDKOOP	GOEDKOOP	DUUR	BAIE DUUR
BANDWYDTE	LAAG	LAAG	HOOG	BAIE HOOG
ISOLERING	GEEN	SWAK - GOED	GOED	GOED
UITSTRALING	BAIE HOOG	GEMIDDELD	LAAG	GEEN
INVLOED VANBUITE	BAIE HOOG	HOOG (WISSEL)	LAAG	GEEN
INTEGRITEIT	SWAK	SWAK - REDELIK	GOED	BAIE GOED
KABELGEWIG	SWAAR	HOOG	HOOG	LAAG
GEVAAR VAN AFTAPPING	BAIE HOOG	BAIE HOOG	HOOG	BAIE HOOG
GEMAK VAN AFTAPPING	BAIE MAKLIK	MAKLIK	MOEILIK	BAIE MOEILIK
INSTANDHOUD-ING. (PERIODE)	GEREELD	GEREELD	MINDER GEREELD	BAIE MIN

- Gevaar van aftapping. Dit dui aan hoe groot die gevaar is dat die verbinding afgetap kan word.

- Gemak van aftapping. Dit dui aan hoe maklik dit is om die bepaalde verbinding te tap.

- Instandhouding. Dit dui aan hoe gereeld daar aan die verbinding aandag gegee moet word vir instandhoudingsdoeleindes.

5.6. Evaluering van uitstralingsverbindings.

Tabel 5.2 is deur die skrywer ontwikkel en vergelyk die verskillende uitstralingsverbindings wat bestudeer is met mekaar. Daar sal na verskillende faktore gekyk word waarvan die belangrikste die faktore met betrekking tot sekerheid is naamlik : Integriteit en aftapping.

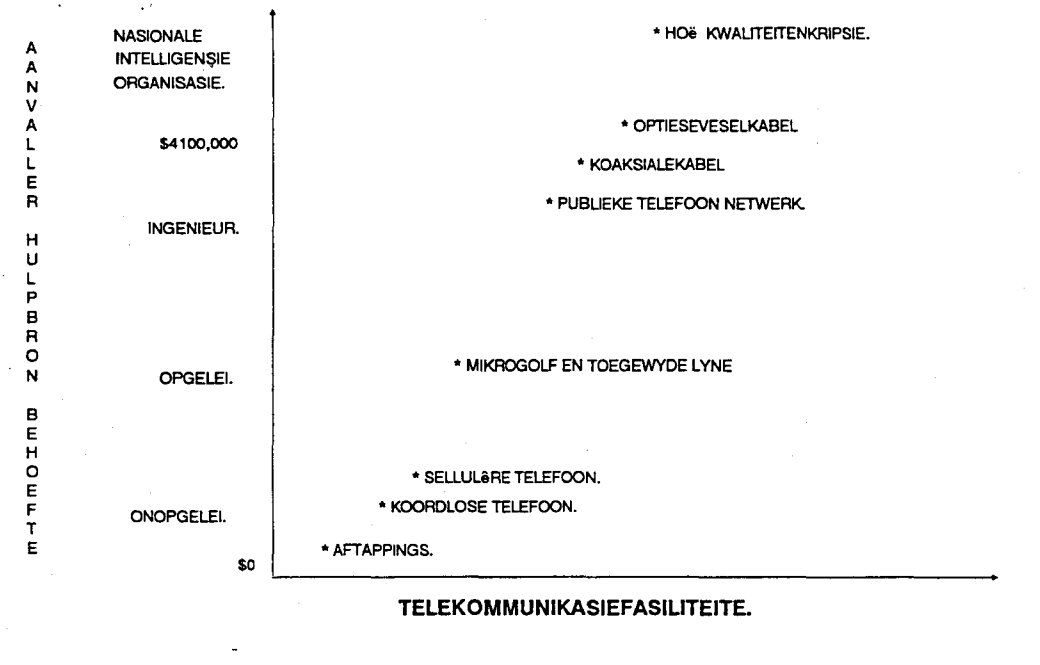


FIG 5.3. SPEKTRUM VAN AANVALLER HULPBRON BENODIGDHEDE VS TEGNOLOGIë.

5.7. SAMEVATTING.

Uit die bestudering van die verskillende kommunikasieverbindings het ons gesien dat daar by die beoordeling van die verbindings na 'n groot verskeidenheid punte gekyk behoort te word. Alhoewel sekere van die verbindings baie goedkoop is, kan daar baie verskuilde kostes wees. So is dit byvoorbeeld baie goedkoop om van gedraaidepaar-kabel gebruik te maak as 'n nuwe netwerk ontwikkel word. Daar kan egter heelwat addisionele koste nodig wees soos om :

- die elektromagnetiese uitstraling te verhoed,
- integriteit van die verbinding te verbeter,
- verbinding te beskerm teen aftappings.

Soos uit die bespreking gesien, is daar geen volkome veilige verbinding nie. Selfs optieseveselverbindings en satelietverbindings kan onderskep word. Die enigste werklike oplossing is om die boodskap self onverstaanbaar te maak vir die onderskepper. Dit bring mee dat die onderskepper niks met die boodskap kan doen as hy dit wel in die hande gekry het nie. Een van die belangrikste metodes om die boodskap wat oor die verbinding beweeg onverstaanbaar te maak, is om van enkripsie gebruik te maak. Enkripsie en ander maatreëls sal in latere hoofstukke aandag geniet.

HOOFSTUK 6.

TOEGANGSBEHEER.

TOEGANGSBEHEER.

In die hoofstuk sal metodes bestudeer word om toegang tot 'n netwerk en die netwerk se hulpbronne te beheer. Netwerke is komplekse stelsels; daar is verskillende komponente, hulpbronne, programme en data wat beskerm moet word. Daar moet dus metodes bestaan om gemagtigde gebruikers te identifiseer. Die metodes sal in afdeling 6.2 bespreek word wat handel oor identiteitverifiëring.

'n Verdere aspek wat in hierdie hoofstuk aandag sal geniet is poortbeskerming. 'n Toegangspoort kan beskou word as 'n toegangspunt of -poort waardeur 'n gebruiker van buite die netwerk, toegang tot die netwerk kan verkry.

6.1. IDENTITEITVERIFIëRING.

Dit is vir enige sekerheidsstelsel van groot belang dat 'n gebruiker wat poog om toegang tot 'n netwerk te verkry, positief geïdentifiseer moet word. Daar bestaan verskeie sulke metodes wat wissel van wagwoorde tot meer moderne metodes soos retina-afdrukherkenning en stemherkenning.

Die metode wat die bekendste is en ook die meeste gebruik word, is wagwoorde.[10] Van die bekendste biometriese metodes is vingerafdrukke en stemherkenning. Die verskillende metodes sal kortliks bespreek word, en meer aandag sal gegee word aan wagwoorde en stemherkenning.

Dit is belangrik om na die verskil tussen die gebruik van bestaande identiteitverifiërings-metodes in die konvensionele hoofraamomgewing, en die netwerkomgewing te kyk.

Hoofraamomgewings is gesentraliseer en kom normaalweg fisies in dieselfde vertrek of gebou voor. Dit beteken dat daar net 'n paar toegangspunte tot die stelsel bestaan en dit dus maklik is om ongemagtigde gebruikers weg te hou van die stelsel. Om die rede, word daar in die meeste gevalle van wagwoorde gebruik gemaak in die hoofraamomgewing.

In die netwerkomgewings is die netwerk se komponente gedesentraliseer en kan die verskillende nodes tussen verskillende geboue en selfs geografies versprei wees. Alhoewel wagwoorde ook hier in die meeste gevalle gebruik word, behoort hier na verbeterde en tegnologies meer gevorderde metodes gekyk te word, soos byvoorbeeld biometriese metodes en ook slimkaarttegnologieë.

6.1.1. FAKTORE WAT 'n INVLOED HET OP DIE KEUSE VAN 'N METODE.

Daar bestaan verskeie metodes om 'n gebruiker te identifiseer. Daar moet egter bepaal word watter van die metodes die geskikste is vir gebruik in 'n netwerk. Dit is belangrik dat die gebruiker, of onderneming wat van die metodes gebruik wil maak, deeglik na die voordele, nadele en kenmerke van die verskillende metodes moet kyk.

Van die belangrikste faktore wat in aanmerking geneem behoort te word tydens die beoordeling van identifikasiemetodes vir netwerkskakeling, is die volgende :[16][65]

- Hoe effektief is die metode?
  Is die betrokke metode werklik in staat om die verlangde vlak van beskerming te lewer? Sekere metodes is baie meer effektief as ander, maar as gevolg van koste oorwegings is dit soms nodig om minder effektiewe metodes te kies omdat meer effektiewe metodes te duur is.

- Hoe aanvaarbaar is die metode vir die gebruiker?
  Sekere metodes sal meer aanvaarbaar wees vir gebruikers as ander metodes. Die gebruik van vingerafdrukke mag byvoorbeeld onaanvaarbaar wees as gevolg van die kriminele konnektasie van vingerafdrukke.

- Praktiese toepasbaarheid.
  'n Metode soos DNA-ontleding is uiters effektief, maar dit is prakties onmoontlik om elke gebruiker in 'n verspreide netwerkomgewing te toets.

- Koste van die metode.
  Die graad van beskerming wat benodig word, sal bepaal hoeveel die aanvaarbare kostes vir die stelsel sal wees. Dit sal byvoorbeeld onnodig wees om 'n Retina-afdruk-metode te gebruik net om 'n drukker te beskerm.

- Tyd wat dit neem vir die identifikasieproses.
  Sekere metodes, soos byvoorbeeld DNA-ontleding, kan 'n paar dae neem om te voltooi. Die identifikasieproses vir gebruik in 'n netwerk moet egter so vinnig as moontlik wees - enkele sekondes, indien moontlik.

6.1.2. KLASSIFIKASIE VAN METODES.

Identifikasiemetodes kan in drie breë kategorieë ingedeel word, alhoewel 'n bepaalde metode elemente uit een of meer kategorieë kan bevat. Die kategorieë is as volg :[10][16]

- Kennis van iets.
  Dit is iets wat die gebruiker weet, byvoorbeeld 'n wagwoord of 'n sleutel. Metodes wat onder die afdeling bespreek sal word, is wagwoorde en kodewoorde.

- Besit van 'n voorwerp.
  Hier moet die gebruiker in besit van een of ander onderskeidende voorwerp wees, byvoorbeeld 'n magneetkaart. Hier sal magneetkaarte en slimkaarte bespreek word.

- Persoonlike eienskap van 'n persoon.
  Hier word een of ander persoonlike, fisiese eienskap van die gebruiker gebruik om hom positief te identifiseer. Hier sal na die sogenaamde biometriese identifikasiemetodes gekyk word, soos onder andere vingermerke, palmafdrukke, retinapatrone, polsaarpatrone, dinamiese handtekeningkarakteristieke en stemherkenning.

6.1.3. VERSKILLENDE METODES VAN IDENTITEITVERIFIKASIE.

6.1.3.1 Kennis van iets.

- Wagwoorde.
  Die gebruik van wagwoorde vir die identifikasie van gemagtigde gebruikers is die mees algemene metode van toegangsbeheer. 'n Wagwoord kan beskryf word as 'n woord bekend aan die gebruiker en die rekenaar. Die basiese idee agter wagwoorde is, dat elke gebruiker oor sy eie geheime wagwoord moet beskik.

  Die gebruiker moet dan elke keer as toegang tot die netwerk verlang word sy wagwoord insleutel. Dit is van groot belang dat die gebruiker sy wagwoord geheim moet hou en ook so 'n woord kies wat ander gebruikers nie sal raai nie.

  Wagwoorde kan deur gebruikers gekies word, of dit kan deur die stelsel aan die gebruiker toegeken word. Beide metodes het voordele en nadele. Gebruikers het die gewoonte om wagwoorde te kies wat maklik is om te onthou, soos motorregistrasienommer of name van familielede. Dit is vir indringers maklik om sulke wagwoorde te bepaal. Die gebruik van stelselgegenereerde wagwoorde skakel die probleem uit, maar het die nadeel dat die wagwoorde moeilik is om te onthou.

Vir meer inligting oor kenmerke van wagwoorde sien [10][16][66][67].

Wagwoorde word literatuurgewys gewoonlik nie bespreek vanuit 'n ISO-model- oogpunt nie. Die skrywer is juis van mening dat wanneer wagwoordstelsels vir netwerktoegangskontrole beskou word, dit uiters noodsaaklik is dat laasgenoemde wel vanuit 'n netwerkmodel (ISO-model) -oogpunt bespreek word.

Wagwoorde word normaalweg op vlak 7, die toepassingsvlak, van die ISO-model geïmplimenteer (sien figuur 2.5 bl 2.15). Dit sal egter meer ideaal wees as dit op vlak 3, netwerkvlak, en vlak 4, die transportvlak, geïmplementeer word. Dit sal beteken dat toegangsbeheer op 'n laer vlak in die netwerk gedoen word, wat toegangsbeheer deur die netwerk sal versprei na die voorpuntverwerkers(FEP) of verkieslik na die verskillende nodes. Dit beteken dat versending van wagwoorde nie oor die transmissieskakels, waar dit onderskep kan word, nodig is nie. Verder sal die benadering ook die werklas van die netwerk verlaag, aangesien kommunikasie tussen node en netwerkbeheerder tot die minimum beperk sal word.

VERSKILLENDE SOORTE WAGWOORDE.

- Groepwagwoorde.
  Hier word dieselfde wagwoord aan 'n groep gebruikers toegeken. Al die gebruikers in 'n bepaalde departement kry byvoorbeeld toegang tot dieselfde programme en data op die netwerk. In die netwerkomgewing kan groepwagwoorde ook die geografiese verspreiding van die verskillende dele van die netwerk reflekteer. So kan elke geografiese gebied oor sy eie groepwagwoord beskik.

  Die probleem is net dat die wagwoord maklik kan uitlek as so baie mense dieselfde wagwoord gebruik.

- 'n Unieke wagwoord.
  Hier moet elke gebruiker oor 'n unieke wagwoord beskik. Dit beteken dat die wagwoord die gebruiker se identiteit bepaal en hom ook waarmerk. In die netwerkomgewing kan 'n unieke wagwoord van groot belang wees aangesien dit gebruik kan word vir aktiwiteitboekhouding by die FEP of die nodes self.

- Nie-unieke wagwoord.
  Hier kan meer as een gebruiker dieselfde wagwoord hê. Die wagwoord kom gewoonlik hier saam met 'n gebruikernaam voor. Die gebruikernaam en die wagwoordkombinasie is uniek. Die gebruikernaam is gewoonlik nie geheim nie, maar die wagwoord wel.

In 'n stelsel wat van nie-unieke wagwoorde gebruik maak, word die gebruiker gewoonlik versoek om sy naam in te sleutel en as die naam wel voorkom in die lys van gebruikers, word die wagwoord versoek.

In die netwerkomgewing is die metode veral van nut aangesien die groot aantal gebruikers wat 'n netwerk gebruik, veroorsaak dat wagwoorde soms ooreenkom.

Die veiligheid van die stelsel kan verhoog word as die stelsel beide die gebruikernaam en wagwoord vra, maar nie aandui watter een van die wagwoord of gebruikernaam verkeerd is as die versoek tot toegang faal nie.[10]

6.1.3.2. In besit van iets.(Token)

- Magneetkaart.[16]
  Hier moet die gebruiker in besit wees van 'n magneetkaart wat sekere inligting bevat wat die gebruiker identifiseer. Die kaart is van plastiek, met die gedrukte inligting op die voorkant en 'n magneetstrook aan die agterkant. Sien figuur 6.1.

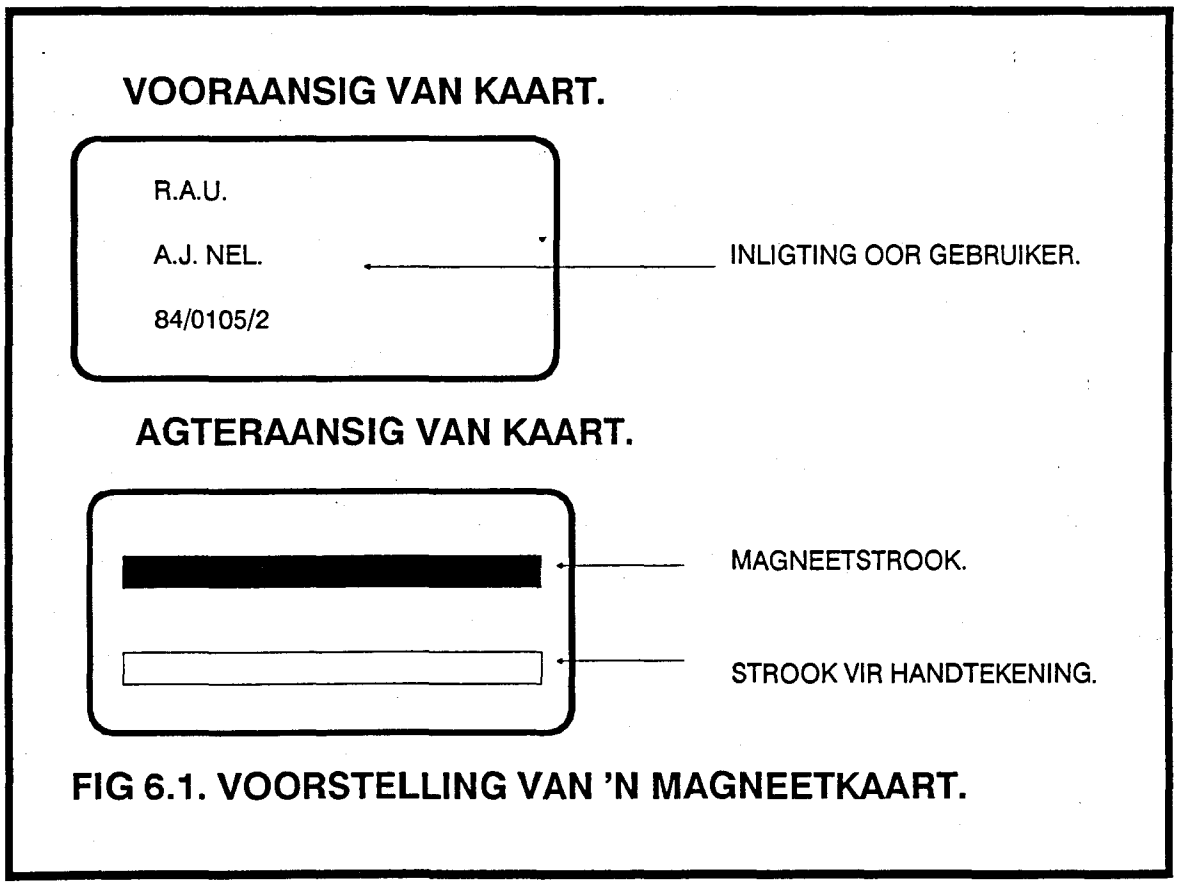


FIG 6.1. VOORSTELLING VAN 'N MAGNEETKAART.

Die tegniek is reeds in gebruik in die Outomatiese TellerMasjienomgewing(ATM) vir identifikasie van gebruikers. Inligting wat die gebruiker identifiseer, word in geënkripteerde vorm op die kaart se magneetstrook gestoor.

In 'n ATM-kaart word 'n geheime persoonlike identifikasie kode of PIN aan die gebruiker toegeken en op die kaart gestoor. Elke keer as die gebruiker toegang tot die ATM verlang, moet hy die kaart in 'n kaartleser plaas en sy PIN op 'n sleutelbord insleutel. Die rekenaar vergelyk die PIN op die kaart, en die PIN wat die gebruiker ingesleutel het.

Afhangende van die hoeveelheid geheue wat op die kaart voorkom, kan meer as een wagwoord, PIN of ander inligting ook op die kaart gestoor word. Baie van die kaarte wat reeds in gebruik is, het 'n foto van die eienaar op. 'n Voorbeeld van so 'n kaart is die studentekaarte van die Universiteit van Stellenbosch.

Die groot nadeel van die metode is die feit dat enigeeen wat oor die kaart beskik en die PIN ken, die kaart kan gebruik. As die kaart dus gesteel word en die oortreder die PIN ken, kan hy die kaart ongemagtig gebruik. Die kaart kan ook maklik verlore raak, en dan kan die gemagtigde gebruiker nie toegang tot die netwerk verkry nie.

In die netwerkomgewing sal elke node, soos byvoorbeeld 'n terminaal, oor 'n kaartleser moet beskik wat die kostes van die metode kan verhoog.

Die koste van die kaarte is ongeveer $15 terwyl die kaartlesers ongeveer $400 kos.[87]

- Die Slimkaart.[16]

'n Meer moderne ontwikkeling is die sogenaamde Slimkaart of "Smartcard". Die kaart lyk dieselfde as die gewone magneetkaart, maar beskik ook oor 'n ingeboude mikroverwerker met addisionele geheue op die kaart. Sien figuur 6.2. Dit beteken dat die kaart se geheue baie groter is as die gewone magneetkaart, en die verwerker kan ook dataverwerkingstake verrig. Baie van die Slimkaarte bevat steeds die magneetstrook op die agterkant van die kaart, en kan ook sonder die verwerker gebruik word as 'n gewone magneetkaart.

Die Slimkaart het die voordeel dat die ekstra geheue aangewend kan word om verskillende wagwoorde en/of ander inligting in te stoor. Soos die tegnologie verbeter, neem die geheuekapasiteit van die Slimkaart toe. Die geheue kan opgedeel word in openbare en geheime areas en verskillende wagwoorde kan aan die areas toegeken word. Die verwerker beheer toegang tot die geheue en kan die inligting op die kaart enkripteer. Die inligting kan verwerk word en verander word. Van die heel nuutste Slimkaarte beskik oor 'n sleutelbord en 'n vertoonvenster wat beteken dat die gebruiker ook sy PIN direk op die kaart kan invoer.[16]

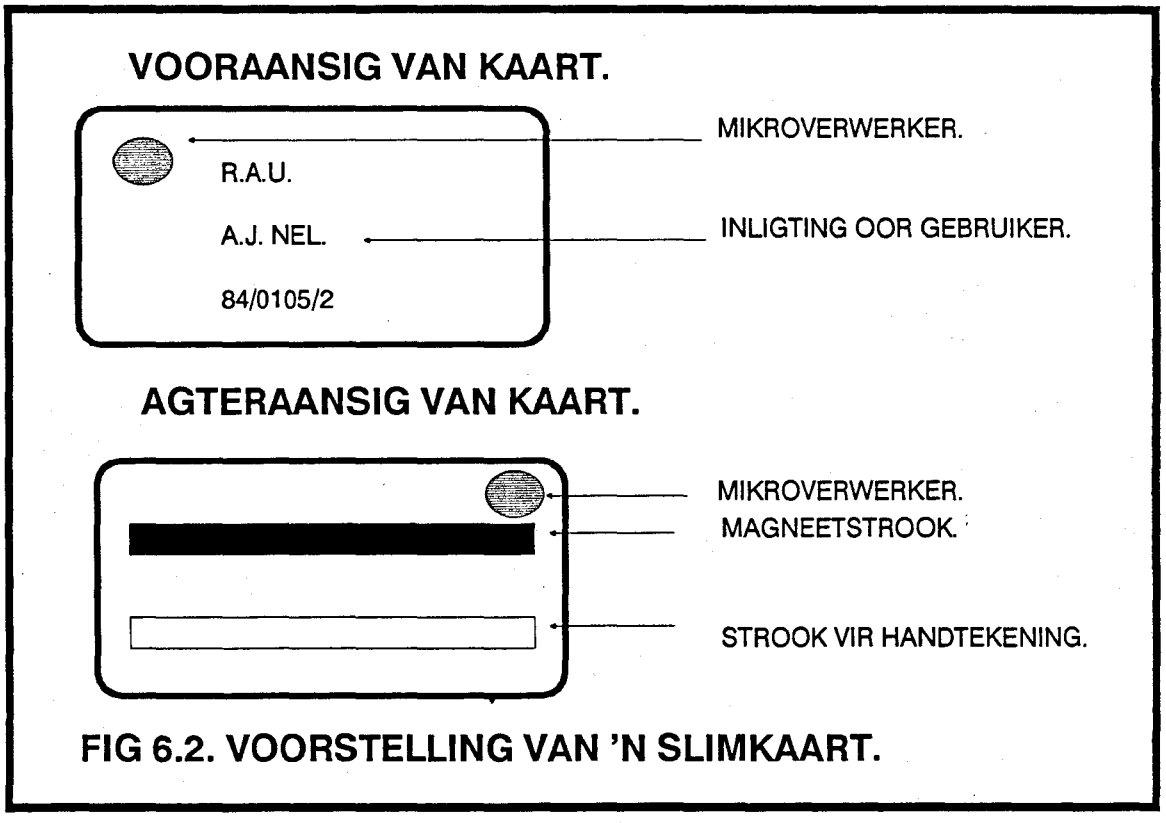


FIG 6.2. VOORSTELLING VAN 'N SLIMKAART.

Die gebruik van Slimkaarte sal in die toekoms toeneem, en die skrywer voel dat die volgende toepassings ondersoek behoort te word. Een belangrike gebruik van die Slimkaart kan wees die aantekening van tye wat die gebruiker toegang tot die netwerk probeer verkry het, en wat hy daar gedoen het. So kan 'n persoonlike aktiwiteitlog op die kaart opgebou word. Die area waarin die inligting gestoor is, kan deur 'n spesiale wagwoord beskerm word wat slegs die netwerkadministrateur toegang daartoe gee.

'n Verdere toepassing wat in 'n later stadium deur die skrywer ondersoek sal word, is die gebruik van die Slimkaart vir die stoor van die gebruiker se foto in die geheue van die kaart. Dit beteken dat die kaart ook gebruik kan word vir fisiese toegangsbeheer waar 'n sekuriteitswag die gebruiker visueel moet identifiseer vir toegang. 'n Losstaande, persoonlike rekenaar met 'n kaartleser kan deur die wag gebruik word om die foto van die gebruiker van die kaart te onttrek en op die rekenaar se skerm te vertoon.

Die toepassing kan later verbeter word sodat die gebruiker deur geslotebaan TV afgeneem word, en die beeld met die foto op die kaart vergelyk kan word. Die toegangsbeheer kan outomaties geskied, en die teenwoordigheid van die sekuriteitswag is dan onnodig. Veral in die netwerkomgewing kan die metode meer aanvaarbaar wees as die metode waar die wag die toegangsbeheer verrig. Die geslotebaan TV-apparaat sal egter die koste verhoog.

'n Verdere voordeel van die metode is dat die foto in die kaart se geheue nie sigbaar is nie. Dus kan die kaart nie gesteel word en die foto dan vervang word met die ongemagtigde gebruiker nie. Die foto kan ook op voorafbepaalde tye outomaties bygewerk word om veranderings soos hare wat groei en veroudering van die gebruiker te weerspieël.

Die kaart is egter heelwat duurder as die gewone magneetkaarte en die kaartleser is ook baie meer ingewikkeld en duurder.

6.1.3.3. Persoonlike eienskap. (Biometriese metodes).

- Vingermerke.

  Dit is al reeds vir 'n baie lang tyd bekend dat vingerafdrukke van individue tot so 'n mate verskil dat dit aangewend kan word vir die positiewe identifikasie van 'n individu. Vingerafdrukke is vir die eerste keer in 1897 deur Sir Edward Henry van die Metropolitaanse polisie in Londen, Engeland gebruik om misdadigers uit te ken.[16]

  Daar is reeds verskeie elektroniese produkte beskikbaar waarmee vingerafdrukke afgeneem en gestoor kan word op band of optiese stoormedia.[65] Die afdrukke kan dan vergelyk word met nuwe afdrukke wat geneem word om sodoende 'n gebruiker te identifiseer.

Probleme kan ondervind word met gebruikeraanvaarding, aangesien vingerafdrukke in die meeste lande in die wêreld deur die polisie gebruik word om misdadigers uit te ken.[16][65] 'n Verdere probleem is die slytasie wat voorkom op die toerusting wat die vingerafdruk afneem. Die gebruiker moet met sy vingers fisies aan die sensor raak. Die aanraking veroorsaak slytasie.[65]

Alhoewel vingerafdrukke 'n baie duidelike identifikasie kan maak, kan beserings aan vingerpunte veroorsaak dat die gebruiker se vingerafdruk verander. Sodra die besering genees het, sal die vingerafdruk egter weer dieselfde wees as voor die besering.[16]

Toerusting vir vingerafdrukverifiëring is baie kompleks en is dus redelik duur. Die kostes van nuwer tegnologie behoort egter te daal en sodra die metode meer gebruik word, sal dit ook help om die kostes laer te maak.[16]

In die netwerkomgewing mag dit nodig wees dat elke node oor 'n vingerafdruktoestel moet beskik. Dit veroorsaak dat die kostes baie hoog sal wees wat die metode nog meer onaanvaarbaar maak.

- Palmafdrukke.
  Net soos vingerafdrukke, is afdrukke van 'n individu se handpalms ook uniek, en kan dus ook vir identifikasie gebruik word. Die basiese werking, voordele en nadele is dieselfde as vir vingerafdrukke. Aangesien die palmafdruk baie groter is as vingerafdrukke, neem die palmafdruk baie meer spasie op en neem die identifikasieproses ook langer. Slytasie van toerusting is hoër en die toerusting sal ook duurder wees.

  Net soos by vingerafdrukke, sal die metode duur wees aangesien identifikasietoestelle by elke node moet voorkom.

- Retina-patrone.
  Hier word die patroon van 'n individu se retina se bloedvate gebruik vir die identifikasieproses. Die gebruiker sal versoek word om in 'n toestel met twee oogstukke te kyk en op 'n kruis te fokus. 'n Afdruk sal dan van die retinas van die oë gemaak word deur middel van 'n lae-intensiteit infrarooi-straal, wat dan met vorige afdrukke vergelyk kan word vir identifikasiedoeleindes. [16]

Die metode is uiters suksesvol en het die verdere voordeel dat die toerusting feitlik geen slytasie opdoen nie. Gebruikers mag egter skrikkerig wees om die metode te aanvaar aangesien daar vrees kan bestaan vir skade aan die oë.[16][65] Die toerusting is egter baie ingewikkeld en duur.

Die EyeDentify-maatskapy van Portland in die V.S.A. bemark die EyeDentify 8.5 retina-identifikasiestelsel teen 'n prys van US$4995. [89]

- Polsaarpatrone.
  Die patrone van die are in 'n individu se polse is ook uniek, en kan gebruik word vir identifikasie. Die metode het egter nog baie min aandag geniet.

- Dinamiese handtekeningkarakteristieke.
  Aangesien handtekeninge reeds baie lank gebruik word om 'n individu te identifiseer en dokumente te onderteken, kan dit beskou word as die mees aanvaarbare biometriese identifikasiemetode.[16][65] Dit is egter baie moeilik om twee handtekeninge met mekaar te vergelyk, en baie navorsing word nog oor die onderwerp gedoen.

  Daar bestaan verskeie kenmerke van die handtekening wat ontleed kan word. Die voltooide handtekening kan ontleed, word sowel as die handtekeningproses. As die voltooide handtekening gebruik word, word die sekere aspekte van die handtekening, soos die vorm van sekere karakters ontleed. Die probleem is dat die handtekeninge feitlik nooit ewe groot is nie. Dit beteken dat daar vir 'n sekere afwyking voorsiening gemaak moet word wat klaar die integriteit van die stelsel begin verlaag.

  As die handtekeningproses ontleed word, moet die gebruiker met 'n spesiale pen wat aan 'n rekenaar gekoppel is, sy handtekening maak. Dan word daar gekyk na karakteristieke soos spoed, ritme en druk wat op die pen geplaas word. Hier moet weer eens vir afwykings voorsiening gemaak word.

  Elektroniese handtekeningontleding sal nog baie bestudeer moet word voor dit werklik aangewend kan word. Alhoewel daar reeds 'n paar produkte beskikbaar is, lewer dit nog nie bevredigende resultate nie.[16][65]

  Ion Track Instruments van Burlington in die V.S.A. bemark die Securosign-stelsel teen US$5000. [89]

- Stemherkenning.
  Die gebruik van stemherkenning vir die identifikasie van persone begin al hoe meer aandag geniet onder navorsers. Hier word die frekwensiepatrone van 'n individu se spraak gebruik vir die identifikasiemetode.[65]

  Die voordele van gebruik van die metode is duidelik. Die opvallendste is die identifikasie van 'n persoon oor 'n telefoon. Dit kan veral vir gebruik in die netwerkomgewing baie nuttig wees.

  Die ideaal is dat die gebruiker dadelik herken kan word as hy begin praat, maak nie saak wat hy sê nie. Dit is egter nie so maklik om enige woord te herken en te ontleed nie. Verder neem die ontledingsproses 'n redelike lang tyd. Die prosedure wat meestal gebruik word, is die volgende. Die gebruiker word versoek om 'n vasgestelde aantal woorde en sinne uit te spreek. Die uitspraak word opgeneem en ontleed om dan 'n profiel van die gebruiker se spraakkarakteristieke te bepaal. Sodra die gebruiker geïdentifiseer moet word, moet hy weer 'n voorafbepaalde sin of paar woorde spreek wat dan met sy spraakprofiel vergelyk word.[16][65] Die groot probleem hier is weereens oor hoeveel afwykings om toe te laat. As 'n mens gespanne is, kan dit jou uitspraak beïnvloed.

  Stemherkenningstelsels bestaan reeds, maar is nog nie ten volle betroubaar nie. Die stelsel is nog baie kompleks en baie duur.

  Stemherkenning se verdere groot nadeel is ook dat elke stemafdruk baie geheue in beslag neem. Dit beteken dat die databasis wat die stempatrone bevat baie groot is, en die opsporing en onttrekking van 'n bepaalde patroon baie tyd in beslag sal neem.

  Ecco Industries van Denver in die V.S.A. bemark die VoiceKey-Toegangsbeheerstelsel teen US$1200. [89]

6.1.4. SAMEVATTING VAN IDENTITEITVERIFIËRING.

Die gebruik van wagwoorde word in die meeste gevalle gekies, aangesien dit die bekendste, en maklikste implimenteerbare metode is. Verskillende studies het egter bewys dat wagwoorde verskeie nadele het waarvan veral swak wagwoordbestuur die belangrikste is.[66][67][69][77] Dit het die vraag na meer effektiewe en moderne metodes verhoog

Kaarttegnologieë begin meer aandag geniet, maar probleme soos die verlies van die kaart maak die metode onaantreklik.

Die gebruik van biometriese metodes kan in die toekoms moontlik die antwoord wees. Die metodes het egter almal dieselfde probleme. Toerusting is duur, en veral in die netwerkomgewing waar die toerusting by elke node gedupliseer moet word, is dit 'n groot faktor. Verder is die metode ook van die nuutste tegnologie, en gebruikers is skrikkerig vir nuwe tegnologie. Daar sal nog heelwat navorsing oor biometriese metodes gedoen moet word voor die publiek dit sal vertrou, en die kostes daarvan sal afneem.

Die skrywer het die volgende tabel 6.3 ontwikkel om die verskillende nie-biometriese identiteitverifiëringsmetodes te vergelyk.

FIG 6.3 KENMERKE VAN NIE-BIOMETRIESE METODES.

	WAGWOORDE	MAGNEETKAART	SLIMKAART
EFFEKTIWITEIT	HOOG	REDELIK	HOOG
PRAKTIESE TOEPAS-BAARHEID	HOOG	HOOG	HOOG
GEBRUIKERAAN-VAARBAARHEID	HOOG	HOOG	HOOG
REAKSIETYD	VINNIG	VINNIG	VINNIG
PRYS	GOEDKOOP	GEMIDDELD	DUUR

Die faktore wat by die vergelyking in aanmerking gekom het, is die volgende :

- Effektiwiteit. Hier word gekyk na hoe effektief die metode is om 'n gebruiker te identifiseer. Die effektiwiteit van 'n Slimkaart vir identifikasie is baie hoër as by magneetkaarte aangesien slimkaarte moeiliker is om te vervals, en besit addisionele kenmerke soos die mikroverwerker om werking te verbeter.

- Praktiese toepasbaarheid. Hoe toepasbaar is die metode in die netwerkomgewing. Sekere metodes is baie effektief, maar nie prakties toepasbaar nie. So is polsaar-herkenning meer effektief as wagwoorde, maar as gevolg van koste en apparatuur-vereistes is polsaarherkenning nie moontlik nie.

- Gebruikeraanvaarbaarheid. Hoe aanvaarbaar sal die metode vir die gebruikers wees? Die gebruik van retinapatroonherkenning mag onaanvaarbaar wees vir gebruikers omdat hulle bang is vir oogbeserings. In Suid-Afrika is dit veral belangrik om te bepaal of die metodes vir alle bevolkingsgroeppe aanvaarbaar sal wees. Die kriminele konnektasie aan vingermerke sal veral in Suid-Afrika probleme veroorsaak.

- Reaksietyd. Hoe vinnig is die identifikasieproses in vergelyking met die ander metodes? In sekere toepassings is dit nodig dat die herkenningsproses baie vinnig moet wees. Die ontleding van palmafdrukke sal byvoorbeeld langer neem as vingermerkafdrukke aangesien die palmafdrukke baie groter is as vingermerke.

- Prys. Wat is die metode se prys in vergelyking met die ander metodes? Veral in netwerkomgewings sal koste van uiterste belang wees, aangesien die apparatuur by elke node gedupliseer moet word. So byvoorbeeld sal daar kaartlesers by elke terminaal aangebring moet word.

Die skrywer het die tabel 6.4 ontwikkel om die verskillende biometriese identiteitverifiëringsmetodes te vergelyk.

Die faktore wat by die vergelyking in aanmerking gekom het, is die volgende (slegs faktore wat nie reeds by nie-biometriese metodes genoem is nie.):

- Koste per eenheid. Koste van die apparatuureenheid wat van die metode gebruik maak. Die pryse is die laagste prys in Dollar in 1989.[87]
- Eenhede verkoop. Totale aantal eenhede verkoop gedurende 1987 en 1988 volgens 'n studie deur "Personal Identification News". [87]

6.2. POORTBESKERMING.

Gebruikers van netwerke begin al hoe meer daarop aandring om toegang tot netwerke te verkry al is hulle nie fisies by die netwerk nie. Dit word meestal gedoen deur die rekenaar deur middel van modems aan die netwerke te koppel. Die punt waardeur die toegang verkry word, word die toegangspoort genoem. Die toegangspoort kan ook die punt wees waar netwerke aanmekaar gekoppel word.

FIG 6.3 KENMERKE VAN NIE-BIOMETRIESE METODES.

	VINGER-MERK	PALM-AFDRUK	RETINA-PATROON	POLSAAR-PATROON	DINAMIESE HANDTEKE-NING	STEM-HERKENN ING
EENHEDE VERKOOP 1987	260	60	125		125	600
EENHEDE VERKOOP 1988	475	130	175		195	625
KOSTE per EENHEID 1989	1800	3000	5000		640	1200
EFFEKTIWI-TEIT	REDELIK	REDELIK	BAIE HOOG	REDELIK	REDELIK TOT HOOG	HOOG
PRAKTIES TOEPAS-BAAR	REDELIK.	REDELIK	HOOG	LAAG	REDELIK	HOOG
GEBRUIKER AANVAAR-BAARHEID	LAAG	LAAG	LAAG - REDELIK	ONBEKEND	HOOG	HOOG
REAKSIE-TYD	VINNIG	STADIG	VINNIG	ONBEKEND	VINNIG	STADIG

Die toegangspoort veroorsaak egter heelwat probleme vir sekerheid in 'n netwerk. Dit is nodig dat die persoon wat die toegang versoek, deeglik geïdentifiseer moet word. Verder is dit ook belangrik dat die inligting wat tussen die gebruiker en die netwerk beweeg, ook beskerm moet word, byvoorbeeld deur enkriptering van die inligting.

Van die kwesbaarste punte in 'n netwerk is die inskakeltoegangspoort. Hier kan die gebruiker toegang tot die netwerk verkry deur die poort met sy telefoon te skakel. Daar bestaan verskeie administratiewe en apparatuurtegnieke wat gebruik kan word om die poort te beskerm. [10]

6.2.1. INSKAKELTOEGANG.

Hier word na gewone inskakeltoegang gekyk. Die gebruiker wil toegang tot die netwerk verkry, en skakel direk met sy telefoon die nommer van die toegangspoort. So verkry sy rekenaar dan toegang tot die netwerk. Die toegangspoort kan moontlik 'n spesiale wagwoord of ander toegangsbeheerprogram aktiveer wat die gebruiker positief identifiseer. In baie gevalle moet die gebruiker slegs oor 'n wagwoord beskik en bestaan daar geen verdere maniere om die gebruiker te identifiseer nie.

Die film "WAR GAMES", wat handel oor 'n jeugdige wat deur middel van 'n persoonlike rekenaar en 'n modem toegang kry tot die V.S.A.-Lugmag se kernmisiellanseerrekenaar, het die moontlike gevaar van inskakeltoegang duidelik gemaak. Volgens die film maak die jeugdige gebruik van 'n werklike program genaamd "DEMON DIALER" gebruik om telefoonnommers te identifiseer wat aan modems en rekenaars gekoppel is.[82] Alhoewel dit slegs 'n storie is en feitlik onmoontlik is om te gebeur, het dit sekerheidsbestuurders in die rekenaar- en netwerkomgewing die potensiële gevaar van inskakel toegang gewys.

6.2.2. OUTOMATIESE TERUGSKAKEL.

Een metode van beskerming van 'n toegangspoort is die sogenaamde outomatiese terugskakelmetode. Hier skakel die gebruiker weereens die toegangspoort en voorsien 'n wagwoord of identifikasiekode. Die gebruiker en die rekenaar onderbreek dan die oproep. Die rekenaar beskik dan oor 'n lys van gemagtigde gebruikers en die gebruikers se telefoonnommers. Die rekenaar skakel dan die gebruiker terug by 'n voorafbepaalde nommer.[16][82]

Die belangrikste probleem met die metode is die feit dat die gebruiker altyd van dieselfde telefoonnommer af toegang tot die netwerk moet probeer verkry.[16][82]

Daar bestaan egter twee metodes waarmee die stelsel mislei kan word.[57] Sekere van die stelsels verwag van die gebruiker om die oproep te kanselleer, en die rekenaar monitor die lyn totdat 'n "Idle"-sein ontvang word, wat aandui dat die oproep onderbreek is, waarna die gebruiker teruggeskakel word. Dit is egter moontlik vir die gebruiker om 'n nagemaakte "Idle"-sein na die toegangspoort te stuur wat die netwerkrekenaar sal mislei. Die teruggeskakelde oproep sal dan oor diesselfde lyn gemaak word en kan dan onderskep word.

Die tweede metode is deur middel van oproepherroetering. Daar bestaan 'n prosedure waar daar met die telefoonmaatskappy(in SA die SAPT) ooreengekom kan word dat oproepe na 'n sekere nommer na 'n ander nommer herlei kan word. Die persoon of rekenaar wat die oproep maak, weet nie van die herroetering nie. Die wettige gebruik van die prosedure word meestal gebruik vir persone wat oproepe by 'n sekere nommer verwag, maar dan by 'n ander nommer sal wees.

6.2.3. GEDIFFERENSIEERDE TOEGANGSREGTE.

Belangrike of sensitiewe inligting kan beskerm word deur toegang te beperk tot 'n paar veilige punte. So kan die toegang slegs toegelaat word as die versoek van veilige en bekende plekke af kom. Minder sensitiewe inligting mag egter van enige plek af bereik word.[16]

6.2.4. STIL MODEMS.

Hierdie metode is ontwikkel om te verseker dat telefoonnommers wat aan modems gekoppel is nie geïdentifiseer kan word nie. Gewoonlik stuur 'n modem 'n draersein("Carrier signal") in die lyn af sodra 'n oproep na die nommer gemaak word. Dit veroorsaak dat nommers met modems maklik opgespoor kan word.

Stil modems wag tot die modem van die rekenaar wat die oproep maak die eerste sein stuur, voor die draersein teruggestuur word. Dus kan slegs seine van modems af die nommer gebruik.[16]

6.2.5. MENSLIK GEKONTROLEERDE TOEGANG.

In die metode is die poort nie aan die begin direk aan die netwerk gekoppel nie. Die gebruiker skakel die poort se nommer, en 'n operateur beantwoord die oproep waarna die gebruiker homself moet identifiseer. As die operateur tevrede is met die identifikasie, word die lyn aan 'n modem en dan aan die netwerk gekoppel.[82]

6.2.5. SAMEVATTING VAN POORTBESKERMING.

Afstandstoegang tot netwerke begin al meer gewild raak, en gebruikers sal in die toekoms ook al hoe meer aandring op afstandstoegangfasiliteite. Pryse van modems het reeds gedaal tot vlakke wat dit bekostigbaar maak vir feitlik enige rekenaargebruiker. Dit veroorsaak dat die toegangspoorte tot netwerke deeglik beskerm sal moet word.

Die soort van poortbeskerming wat gebruik word, sal bepaal word deur die vlak van beskerming wat verwag word. Die ongemagtigde gebruikers wat toegang tot netwerke probeer verkry, word meer gesofistikeerd, en dus sal netwerkbestuurders kennis moet dra van nuwe ontwikkelings in die modem- en poortbeskermingsveld.

6.3. SAMEVATTING.

Beheer van toegang tot enige netwerk, en die netwerk se hulpbronne, steun sterk op die bepaling van die gebruiker se identiteit. Hoe meer versprei die toegangspunte tot die netwerk, hoe moeiliker raak dit om die toegang te beheer, en raak dit ook moeiliker om die gebruiker se identiteit te verifieer. Die keuse van die identiteitverifiëringsmetode vir enige netwerk sal afhang van baie faktore soos koste, en veral van die vlak van beskerming wat verwag word.

Bestaande maatreëls wat gebruik maak van wagwoorde sal in die toekoms vervang word met meer gesofistikeerde metodes wat veral biometriese identifikasiemetodes sal insluit. Baie navorsing is egter nog nodig voor die biometriese metodes effektief, en goedkoop genoeg sal wees vir algemene gebruik. In Suid-Afrika sal daar veral gelet moet word op die gebruikeraanvaarbaarheid van enige stelsel wat beplan word.

HOOFSTUK 7.

KRIPTOGRAFIE.

KRIPTOGRAFIE.

Enkripsie kan beskou word as verreweg die belangrikste hulpmiddel of meganisme wat in netwerk- en kommunikasiesekerheid aangewend kan word vir die beskerming van data en ander inligting. Die literatuur maak in die meeste gevalle van die term enkripsie gebruik om enkripsie, dekripsie en sleutelbestuur in te sluit.[7][10][25] Die korrekte term hier is egter **Kriptografie**, wat beide enkripsie, dekripsie asook sleutelbestuur insluit.[16][61]

In FIG 2.6 in hoofstuk 2 word aangedui dat enkripsie die sekerheidsmeganisme is wat gebruik kan word om feitlik enige sekerheidsdiens mee te implimenteer. Enkripsie word gebruik om die inhoud van 'n boodskap onverstaanbaar te maak vir enige iemand wat nie oor die fasiliteite en regte beskik om die boodskap weer te dekripteer nie. Dekripsie is weer die teenoorgestelde proses, om die geënkripteerde boodskap of data weer terug te verander, of te dekripteer na die oorspronklike, verstaanbare vorm.

In paragraaf 7.1 sal aandag gegee word aan die presiese definisie van enkripsie, dekripsie, kriptografie en ander belangrike terme.

Die doel van hierdie hoofstuk is nie om 'n volledige in diepte bespreking van die tegniese- en teoretiese aspekte van kriptografie te gee nie. Vir die aspekte kan die leser die volgende bronne raadpleeg [10][11][16][25][90][91][92][107][108]. Al die terme wat nodig is vir die hoofstuk kan in paragraaf 7.1 gevind word.

Hoofstuk 7 sal toegespits word op 'n funksionele bestuursbespreking van kriptografie. Wat van belang sal wees in die bespreking is die kenmerke van kriptografie wat van belang is vir die bestuur van 'n onderneming en die persone wat gemoeid is met die beskerming van data en inligting op netwerke. Vir hulle is die tegniese, teoretiese en wiskundige aspekte wat 'n die oorgrote meerderheid van bestaande literatuur voorkom, nie van veel nut nie. Vir hulle is dit van groter belang om te kyk na aspekte soos koste van kriptografiese maatreëls, gemak van implimentasie, maniere om 'n keuse te maak tussen verskillende produkte, ensovoorts.

'n Belangrike aspek van kriptografie wat ook aandag aan gegee sal word, is **Sleutelbestuur.** Die effektiwiteit van enige kriptografiese stelsel rus op die effektiewe verspreiding van sleutels wat gebruik word in die enkripsie en dekripsieprosesse. Vir die doel sal daar 'n kortlikse bespreking wees van verskillende metodes van sleutelverspreiding.

In die res van die hoofstuk sal kriptografie onder die volgende paragrawe bespreek word :

7.1. TERMINOLOGIE.

Hier sal gekyk word na die belangrikste terminologie benodig vir die bespreking van kriptografie.

7.2. BASIESE KONSEPTE.

Hier sal die basiese konsepte nodig vir die bespreking van kriptografie kortliks bespreek word soos onder andere Basiese enkripsie, enkelsleutelenkripsie, en publieke sleutelenkripsie.

7.3. ENKRIPSIETEGNIEKE.

Hier sal die twee belangrikste enkripsietegnieke naamlik blok- en stroomenkripsie bespreek word.

7.4. ENKRIPSIESTELSELS.

Hier sal 'n kort bespreking van die belangrikste enkripsiestelsels gegee word naamlik:

- PUBLIEKE SLEUTEL.
- "DATA ENCRYPTION STANDARD" (DES).

7.5. PLASING VAN ENKRIPSIE IN NETWERKARGITEKTUUR.

Hier sal aandag gegee word aan die plasing van enkripsie en dekripsie in die netwerkargitektuur.

7.6. SLEUTELBESTUUR.

Hier sal 'n oorsigtelike bespreking gegee word van die belangrikste metodes wat aangewend word om enkripsie- en dekripsiesleutels deur 'n netwerk te versprei. Verder sal daar ook 'n kort bespreking gegee word van sleutelbestuur en verspreiding van sleutels in die finansiële netwerkomgewing.

7.7. EVALUERING VAN KRIPTOGRAFIESE APPARATUUR.

Hier sal 'n raamwerk vir die evaluasie van kriptografiese apparatuur in 'n netwerkomgewing opgestel word.

7.1. TERMINOLOGIE.

Voor daar voortgegaan word met die bespreking van kriptografie, moet daar eers na die definisie van sekere terme gekyk word.

- Skoonteks : Die oorspronklike verstaanbare data word skoonteks genoem.

- Syferteks : Dit is die geënkripteerde, onverstaanbare data wat verkry word nadat skoonteks deur middel van enkripsie getransformeer is.

- Kriptografie: Dit is die beginsels, vermoëns en metodes vir die transformasie van data, om die inligtingsinhoud daarvan te verberg, voorkoming van onopgemerkte verandering en/of voorkoming van ongemagtigde gebruik van die data.[61]

- Stuurder : Dit is die persoon, node of proses wat die inligting aan die ontvanger versend.

- Ontvanger : Dit is die wettige persoon, node of proses wat die inligting ontvang wat deur die stuurder aan hom gestuur is.

- Enkripsie : Dit is die kriptografiese transformasie van data met die doel om syferteks te verkry.[61]

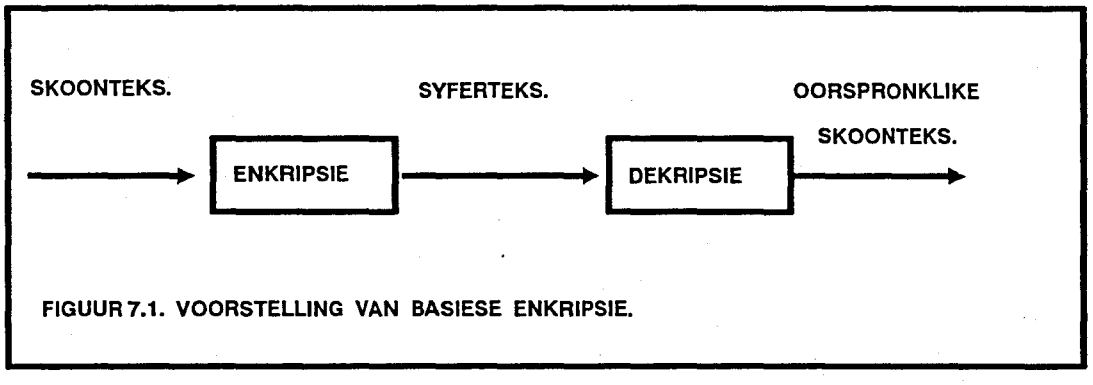
- Dekripsie : Dit is die omgekeerde van enkripsie.[61] Geënkripteerde data ,of syferteks, word gedekripteer om weer verstaanbare, of skoonteks, te verkry.

- Kriptostelsel : Dit is 'n enkripsie- en dekripsiestelsel.[10]

- Sleutel : 'n Sleutel is 'n veranderlike wat saam met die enkripsie- en dekripsie-algoritme gebruik word om die syferteks te genereer. Die algoritme doen, tesame met die sleutel, 'n bewerking op die skoonteks wat dan die syferteks lewer. Die dekripsiealgoritme gebruik weer dieselfde sleutel in die dekripsieproses om weer die skoonteks te lewer.

7.2. BASIESE KONSEPTE.

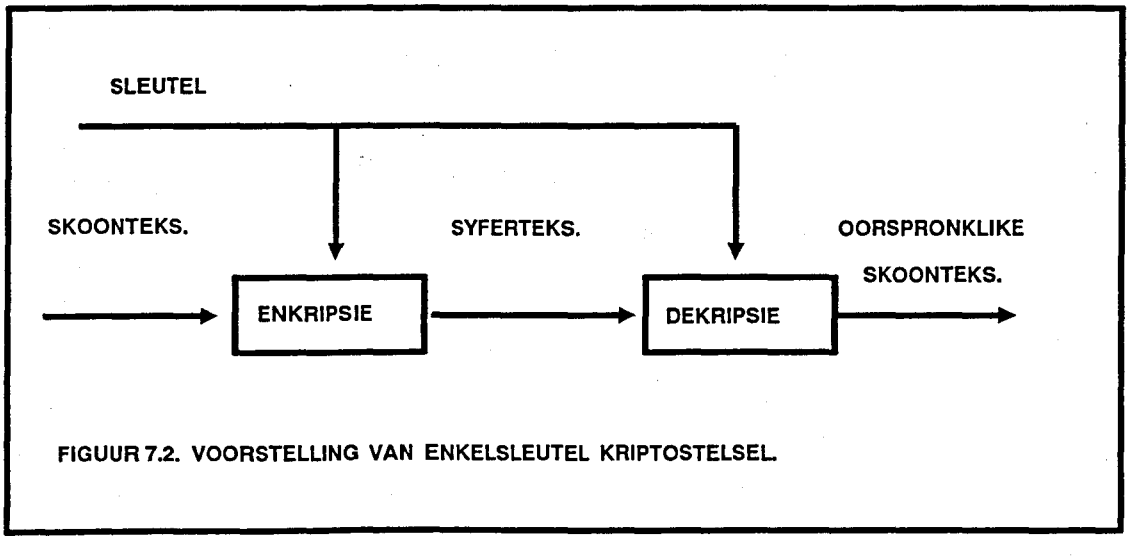
Basiese enkripsiestelsel. Hier bestaan daar 'n vasgestelde enkripsie en dekripsiealgoritme. Skoonteks word deur die enkripsiealgoritme verwerk en lewer syferteks. Die syferteks word dan weer deur middel van die dekripsiealgoritme gedekripteer om weer skoonteks te verkry. Sien figuur 7.1.



FIGUUR 7.1. VOORSTELLING VAN BASIESE ENKRIPSIE.

In die stelsel word nie van 'n sleutel gebruik gemaak nie, en word 'n sleutellose kriptostelsel genoem.[10]

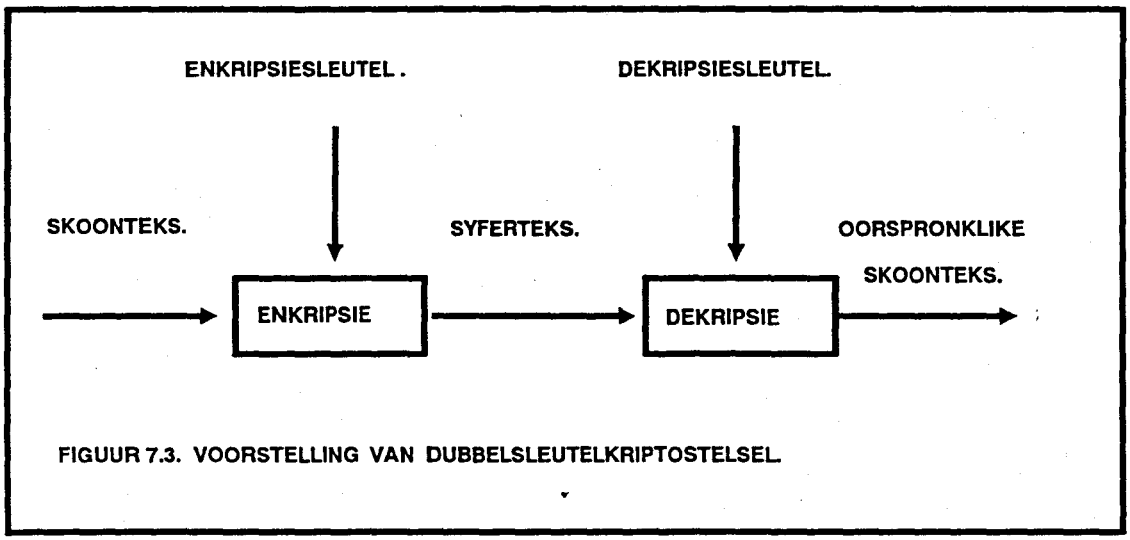
Om die beskerming wat 'n kriptostelsel verleen te verbeter, kan ook van 'n sleutel in die enkripsie- en dekripsieproses gebruik gemaak word. Die enkripsie- en dekripsiealgoritmes het buiten die skoonteks ook 'n sleutel as invoer. Verskillende sleutels genereer verskillende syferteks. Sien figuur 7.2.



FIGUUR 7.2. VOORSTELLING VAN ENKELSLEUTEL KRIPTOSTELSEL.

Figuur 7.2. dui 'n enkelsleutelkriptostelsel aan. Hier word dieselfde sleutel vir enkripsie en dekripsie gebruik. As 'n ander sleutel vir dekripsie gebruik word as wat vir enkripsie gebruik is, sal die uitvoer nie skoonteks wees nie. Die nadeel van so 'n stelsel is die feit dat die sleutel aan die stuurder sowel as die ontvanger bekend moet wees. Die stelsel word ook 'n simmetriese stelsel genoem.[10]

'n Verdere stelsel, genoem 'n asimmetriese stelsel of tweesleutelstelsel, maak gebruik van twee verskillende, maar verwante sleutels. Een sleutel word gebruik vir enkripsie, terwyl die ander sleutel gebruik word vir dekripsie. So 'n kriptostelsel is die Publieke sleutelkriptostelsel, wat later in paragraaf 7.4. bespreek sal word.[16] Sien figuur 7.3. vir 'n voorstelling van 'n assimetriese kriptostelsel.



FIGUUR 7.3. VOORSTELLING VAN DUBBELSLEUTELKRIPTOSTELSEL.

7.3. ENKRIPSIE TEGNIEKE.

Daar bestaan twee hoofklasse van enkripsietegnieke naamlik :

- Bloktegnieke: Hier word die skoonteks in vasgestelde blokke opgedeel en elke blok word dan op sy eie saam met 'n sleutel geënkripteer, en dan later weer gedekripteer. Die sleutel is gewoonlik dieselfde lengte as die blok.
- Stroomtegnieke: Hier word die enkripsie en dekripsieproses karakter vir karakter of selfs bis vir bis gedoen.

7.3.1. BLOK.

As van blokenkripsietegnieke gebruik gemaak word, word die skoonteks in blokke opgedeel wat min of meer ooreenkom met die lengte van die sleutel. Die hele blok word dan geënkripteer waarna na die volgende blok beweeg word. Die dekripsieproses vind op dieselfde wyse plaas. Sien figuur 7.4 vir 'n diagrammatiese voorstelling van blokenkripsie.

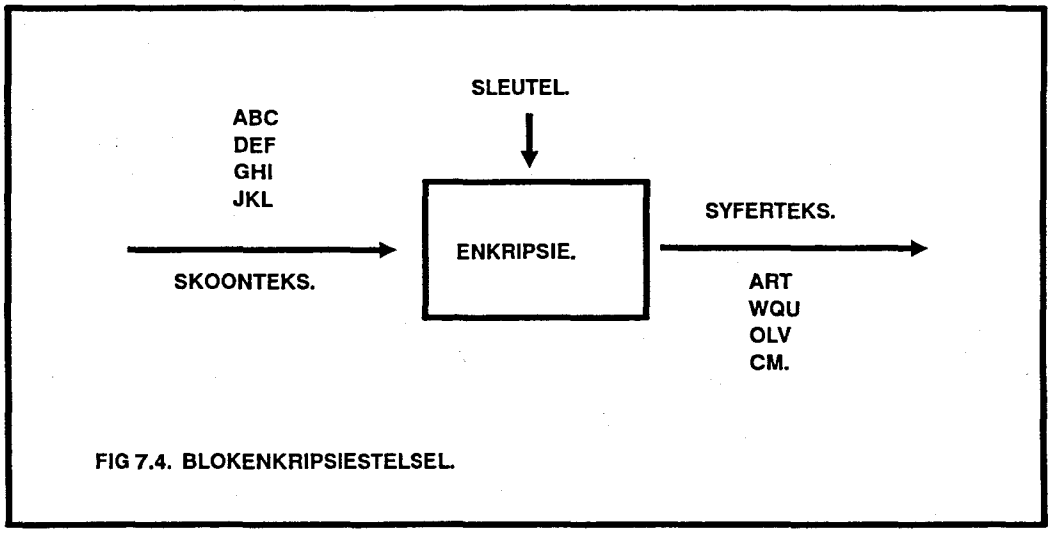


FIG 7.4. BLOKENKRIPSIESTELSEL.

7.3.2. STROOM.

Hier word 'n karakter geënkripteer of gedekripteer sodra dit ontvang word. Die skoonteks of syferteks word dus intyds verwerk soos dit ontvang word. Sien figuur 7.5. vir die diagrammatiese voorstelling van stroomenkripsie.

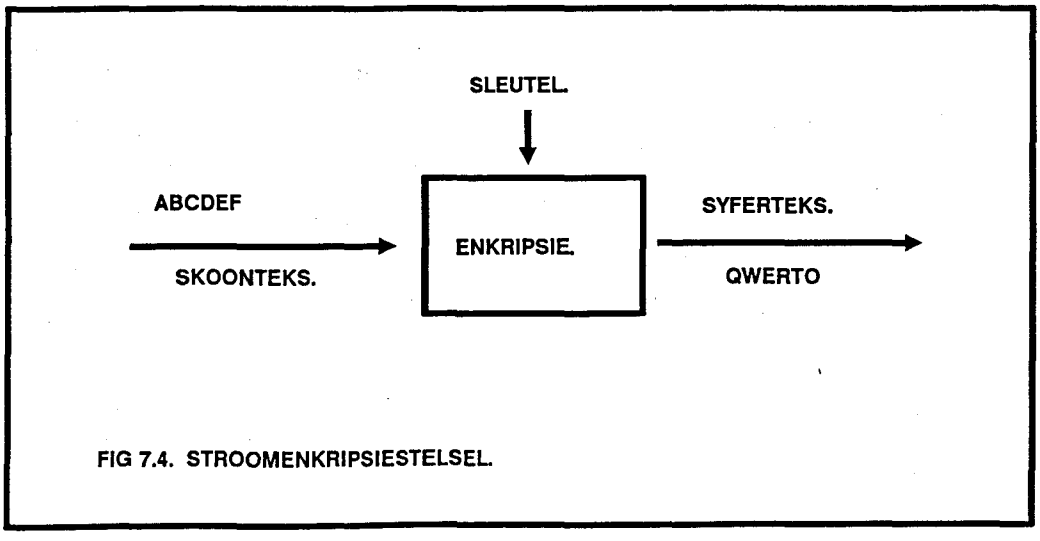


FIG 7.4. STROOMENKRIPSIESTELSEL.

7.3.3. EVALUERING VAN TEGNIEKE.

In 'n netwerksekerheidsomgewing het die gebruik van stroomenkripsie 'n belangrike voorsprong bo blokenkripsie, aangesien die teks of boodskap, soos dit ontvang word, onmiddellik verwerk word. By blokenkripsie moet die hele blok eers ontvang word voor met die verwerking begin kan word. Dit beteken dus dat stroomenkripsie baie vinniger as blokenkripsie sal wees.[16] In 'n netwerk is dit van groot belang dat die enkripsieproses so deursigtig as moontlik moet wees vir die gebruiker. Dus is die spoed van die enkripsie- en dekripsieverwerkings van groot belang.

7.4. ENKRIPSIESTELSELS.

7.4.1. PUBLIEKE SLEUTEL.

In 1976 het Hellman en Diffie 'n nuwe kriptografiese stelsel ontwikkel wat bekend gestaan het as die publieke sleutelenkripsiestelsel.[16][90][91][108]

In die stelsel word gebruik gemaak van twee sleutels wat verskillend, maar wel verwant aan mekaar is. Die een sleutel is 'n publieke sleutel, wat algemeen bekend is, terwyl die tweede sleutel, wat bekend staan as die private sleutel of geheime sleutel, geheim is en slegs aan die eienaar bekend is. Gewoonlik word die publieke sleutel in 'n gids, wat met 'n telefoongids vergelyk kan word, gepubliseer. Die publieke sleutel word gebruik om 'n boodskap te enkripteer, terwyl die privaatsleutel nodig is om die boodskap weer te dekripteer. 'n Geënkripteerde boodskap kan nie weer deur middel van die enkripsiesleutel gedekripteer word nie. Dit staan bekend as eenrigtingenkripsie.[16][90][108]. Slegs die geheime sleutel kan vir die doel gebruik word.

Publieke sleutelenkripsie kan met die volgende voorbeeld verduidelik word. Gebruiker A wil 'n boodskap aan gebruiker B stuur. Gebruiker A soek gebruiker B se publiekesleutel in die gids op, en enkripteer die boodskap daarmee, en stuur die geënkripteerde boodskap aan gebruiker B. Sodra gebruiker B die boodskap ontvang het, dekripteer hy die boodskap met sy privaatsleutel om weer die skoonteksboodskap te kry.

Die voordeel van die stelsel is dat geheime sleutels nie tussen gebruiker uitgeruil moet word nie. As die publieke sleutel in 'n openbare gids gepubliseer word, kan enige iemand 'n geënkripteerde boodskap aan die gebruiker stuur, indien sy publieke sleutel wel in die gids verskyn.

Een van die eerste publieke sleutelenkripsiestelsels wat gepubliseer is, is ontwikkel deur Rivest, Shamir en Adleman, en staan bekend as die RSA-publieke sleutelenkripsiestelsel. Die wiskundige en tegniese aspekte van die RSA-metode word in die volgende bronne bespreek, [16][90][91][92][95][96][99][108][114].

7.4.2. "DATA ENCRYPTION STANDARD" (DES).

Die enkripsiestelsel wat die meeste gebruik word, staan bekend as die "Data Encryption Standard" of slegs DES, wat in 1977 deur die Nasionale Buro van Standaarde (NBS) van die V.S.A. aanvaar is. Die DES-enkripsiestelsel is 'n baie kragtige enkripsiestelsel en die beskrywing van die interne werking van die algoritme is buite die omvang van die verhandeling. 'n Volledige beskrywing van die stelsel kan gevind word in [16].

DES maak gebruik van die blokenkripsietegniek en data word geënkripteer in blokke van 64 bisse met 'n sleutel van 56 bisse. DES maak verder gebruik van substitusie(vervanging) en transposisie(verskuiwing) van bisse. Die kragtigheid van die algoritme ontstaan uit die opeenvolgende, herhalende toepassing van die twee tegnieke vir 'n totaal van 16 siklusse. Daar bestaan reeds stelsels wat van dubbele DES-enkripsie gebruik maak vir versterkte enkripsie.[16][29]

Die dekripsieproses word verkry deur slegs die enkripsieproses om te draai. Sien figuur 7.6. vir 'n voorstelling van DES.

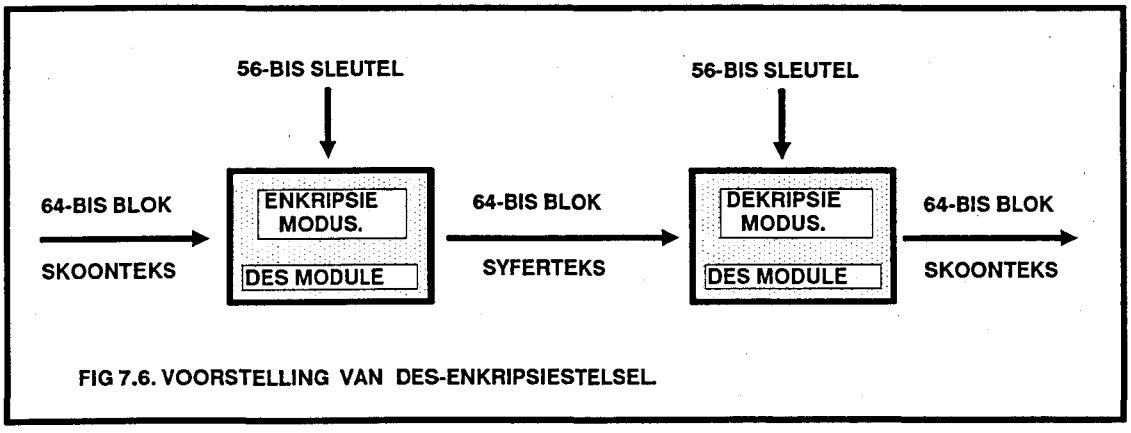


FIG 7.6. VOORSTELLING VAN DES-ENKRIPSIESTELSEL

Alhoewel DES beskou word as van die beste enkripsiestelsels in die wêreld, verskyn daar nog gereeld in die literatuur bewerings oor die kwesbaarheid van die DES-algoritme. [16][95]

Alhoewel die algoritme openbaar is, is die ontwerpskriteria geklassifiseer as geheim deur die NBS. Verder word DES-toestelle deur die V.S.A.-regering as sogenaamde "Auxiliary military equipment" geklassifiseer, en is uitvoerpermitte nodig om dit oor V.S.A.-grense te vervoer. Die uitvoerpermitte is onderworpe aan Amerikaanse Internasionale Verkeer in Wapen Regulasies (ITAR), en kan dus as gevolg van die internasionale wapenboikot teen Suid-Afrika nie ingevoer word uit die V.S.A. nie.[16]

7.5. PLASING VAN ENKRIPSIE IN NETWERKARGITEKTUUR.

Wanneer selfs 'n vereenvoudigde voorstelling van 'n kommunikasienetwerk bestudeer word, sal gemerk word dat daar as gevolg van die kompleksiteit van die stelsel verskeie punte is waar die netwerk aangeval kan word. Figuur 7.7. dui 'n eenvoudige voorstelling van 'n netwerk aan. Die figuur dui aan dat 'n netwerk uit verskeie nodes, terminale en rekenaars kan bestaan. Op die diagram word ook duidelik aangedui waar daar kwesbare punte voorkom.

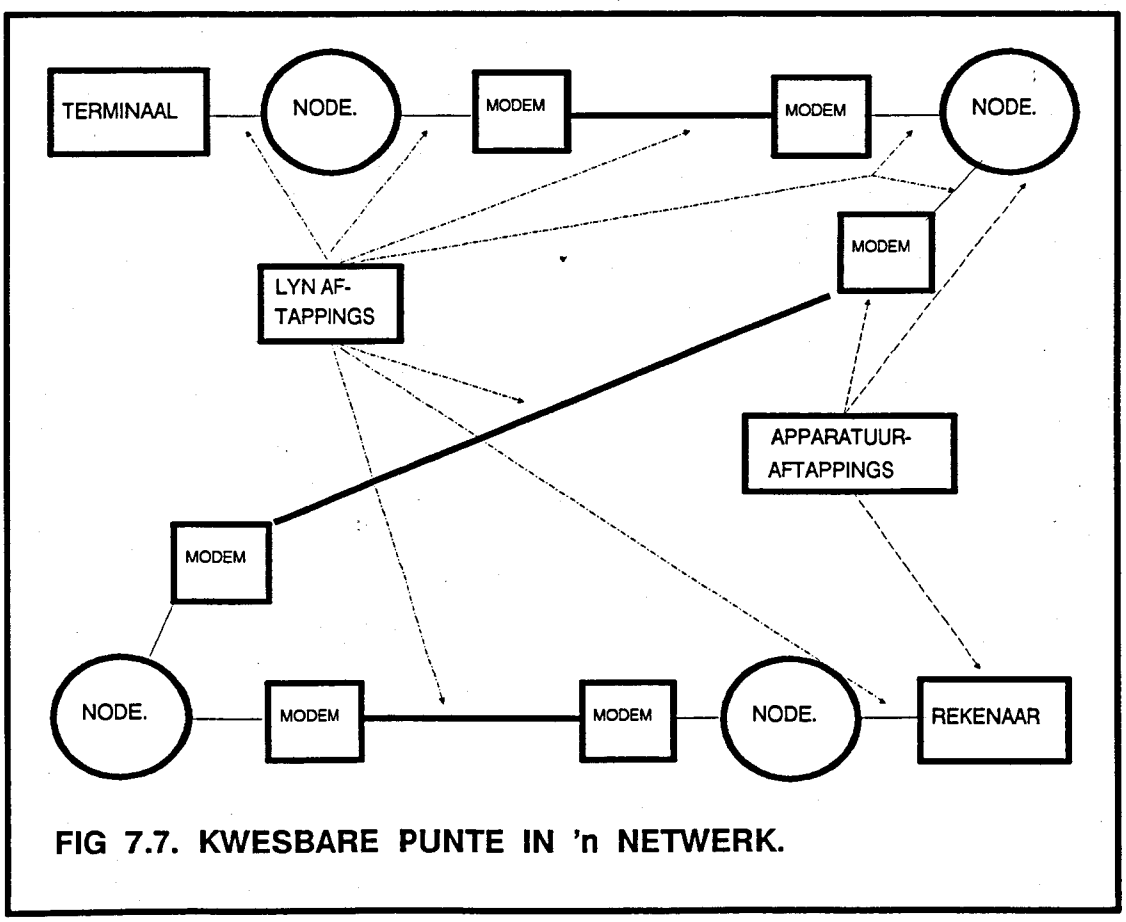


FIG 7.7. KWESBARE PUNTE IN 'n NETWERK.

Die volgende vyf risikopunte kan in 'n netwerk geïdentifiseer word :[29]

- Die terminaal self kan 'n apparatuur- of programmatuuraftapapparaat bevat.
- Die verbinding tussen die terminaal en die node kan 'n aktiewe of passiewe aftapping bevat.
- Enige van die netwerknodes kan 'n aftapapparaat bevat.
- Verbindings tussen verskillende nodes kan afgetap word.
- Rekenaar self kan 'n aftapapparaat bevat.

Om die risikopunte te beskerm, is die plasing van die enkripsieapparatuur van groot belang. Dit is as gevolg van verskillende faktore, soos onder andere koste, nie altyd moontlik om die hele netwerk te beskerm nie. Daar bestaan 3 basiese benaderings tot die plasing van enkripsieapparatuur in die netwerkargitektuur naamlik :

- Skakelenkripsie vir die beskerming van data op die verskillende kommunikasieverbindings.
- Node-vir-Node-enkripsie om data tot binne die node te beskerm.
- End tot end enkripsie om data deur die hele netwerk te beskerm vanaf die versender, tot by die ontvanger.

Elk van die drie benaderings sal nou verder bespreek word.

7.5.1. SKAKELENKRIPSIE.

Die eenvoudigste plasing van dataenkripsie-toerusting in 'n netwerk is op skakelvlak. Skakelenkripsie word aangedui in figuur 7.8.

Op die manier sal die enkripsietoerusting feitlik alle karakters wat deur die toerusting beweeg enkripteer. Sekere van die beheerkarakters sal nie geënkripteer word nie. Die benadering lewer baie goeie beskerming teen die bedreiging van skakelaftappings. Die nadeel van die metode, gesien vanuit 'n netwerksekerheidsoogpunt, is egter dat die enkripsietoerusting buite die nodes geleë is, en dus is die verbinding vanaf die node tot by die enkripsietoestel kwesbaar. Verder is die data binne die node self ook kwesbaar, indien 'n aftaptoestel daar geplaas word.

Die data- of protokoleenhede word in geheel geënkripteer en dus is die protokolkoppe wat die adresse van die versender en die ontvanger bevat, ook geënkripteer. Dus voorsien skakelenkripsie ook verkeervloeisekerheid.

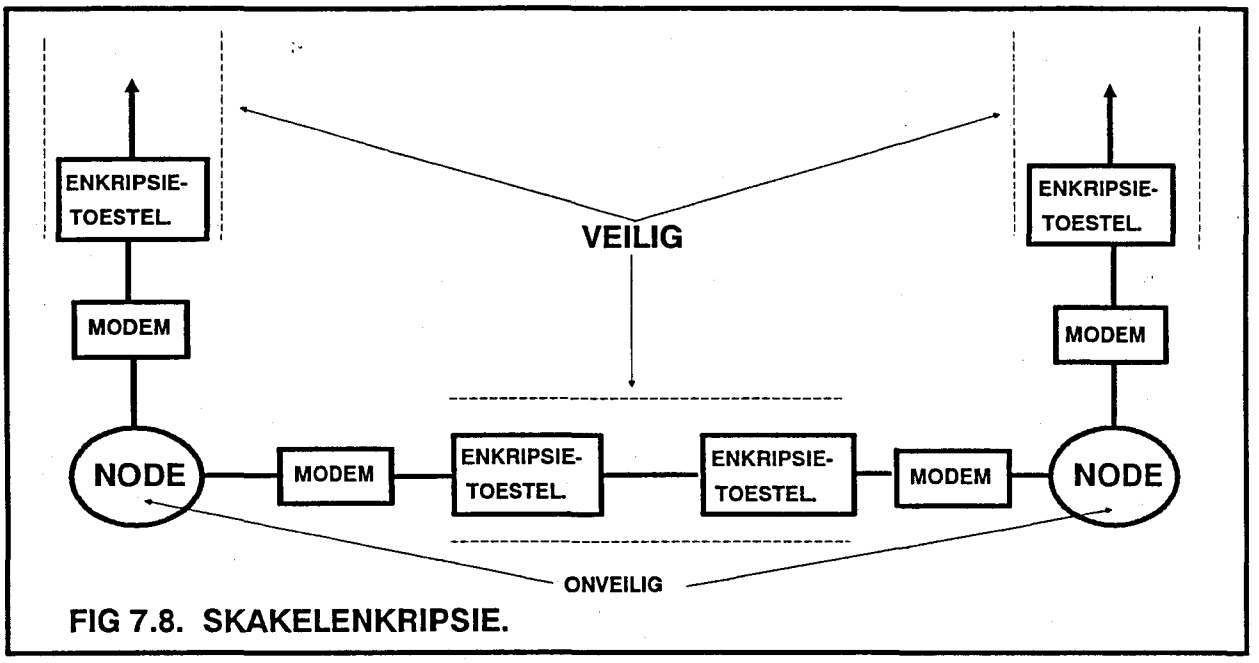


FIG 7.8. SKAKELENKRIPSIE.

7.5.2. NODE VIR NODE ENKRIPSIE.

Een van die belangrikste netwerksekerheidsnadele in skakelenkripsie is die feit dat die data binne die node self en tussen die node en die enkripsietoerusting kwesbaar is. Skakelenkripsie kan egter uitgebrei word tot binne die node, deur die enkripsietoerusting binne die node te plaas. Die benadering word node- vir- node enkripsie genoem, en word voorgestel deur figuur 7.9.

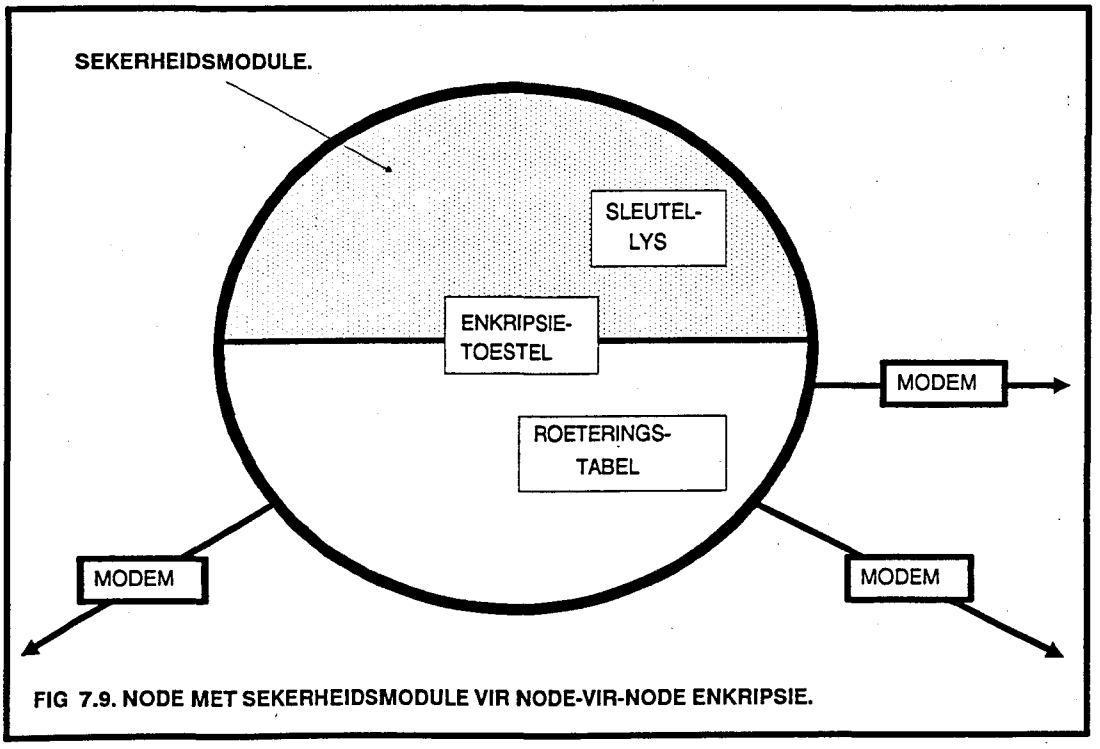


FIG 7.9. NODE MET SEKERHEIDSMODULE VIR NODE-VIR-NODE ENKRIPSIE.

Hier word aangeneem dat die enkripsietoerusting in die vorm van 'n enkripsiemodule binne in die node voorkom. Die enkripsiemodule is 'n geslote "blackbox" wat volkome veilig is, en die inligting en bewerkings in die module kan nie afgetap word nie.'n Datapakkie of protokolpakkie word tussen die twee nodes versend met die koppe in ongeënkripteerde vorm en die res van die pakkie in geënkripteerde vorm. Die metode bring mee dat die node slegs die kop van die pakkie wat hy ontvang, ondersoek om die bestemming te bepaal, en nie nodig het om die pakkie verder te dekripteer nie. Dus is die data nooit binne die node in gedekripteerde vorm nie.

Indien die pakkie wel met 'n nuwe sleutel geënkripteer moet word, word die dekripsie en enkripsie binne die veilige enkripsiemodule in die node gedoen. Die nuwe roeteringsinligting word dan buite die enkripsiemodule weer in die pakkie se kop gelaai. Die groot nadeel vanuit 'n netwerksekerheids oogpunt van die metode is egter die feit dat die pakkie se koppe nie geënkripteer is nie, en kan dus onderskep word, wat bepaling van die oorsprong en die bestemming moontlik maak.

7.5.3. END -TOT- END ENKRIPSIE.

In die derde metode, word die data binne die oorsprongnode geënkripteer, en eers weer by die bestemmingnode gedekripteer. Sien figuur 7.10.

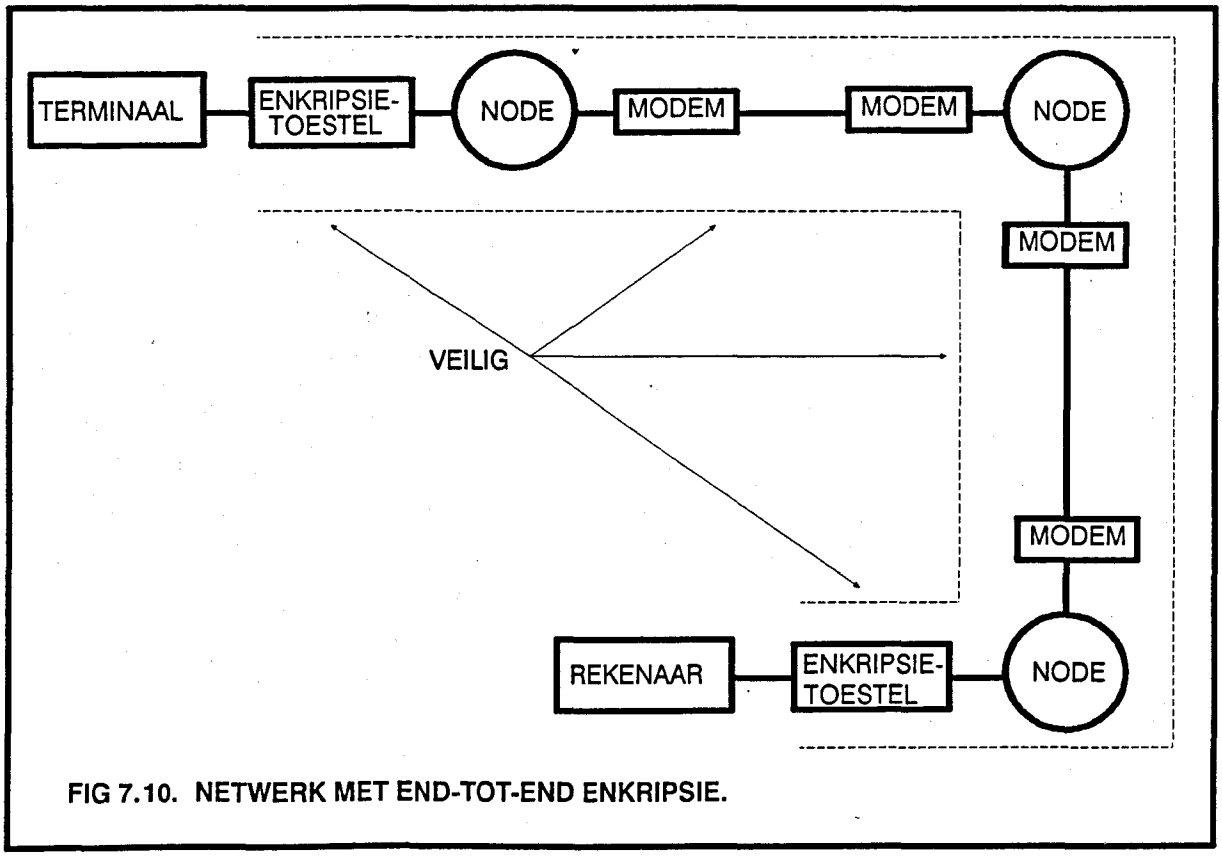


FIG 7.10. NETWERK MET END-TOT-END ENKRIPSIE.

Net soos in die node-vir-node enkripsie, is die pakkie se kop nie geënkripteer nie. Dus bestaan die gevaar van verkeersontleding deur indringers ook by die metode.

7.5.4. BEOORDELING VAN DIE DRIE BENADERINGS VANUIT 'N NETWERKSEKERHEIDSOOGPUNT.

Elk van die drie benaderings beskik oor sekere voordele en nadele. Dit is egter duidelik dat enkripsie die beste beskerming lewer as dit baie hoog, of baie laag in die netwerkargitektuur geplaas word. As so laag as moontlik gekies word, moet dit so na as moontlik aan die fisiese vlak in terme van die OSI-model geplaas word. Vir die ander uiterste is implimentasie in die boonste end-tot-end vlakke die beste. 'n Verdere groot probleem by enkripsie, maak nie saak op watter vlak, watter benadering gebruik word nie, is die probleem van sleutelverspreiding. Die probleem sal later in die hoofstuk bespreek word. Tabel 7.1. dui die belangrikste kenmerke van die drie metodes aan, terwyl tabel 7.2. die mate van beskerming teen verkeerontleding en boodskap- beskerming aandui.

TABEL 7.1. KENMERKE VAN VERSKILLENDE ENKRIPSIEMETODES.

SKAKELENKRIPSIE	NODE-VIR-NODE ENKRIPSIE	END-TOT-END ENKRIPSIE
BOODSKAP SLEGS OP SKAKEL GEëNKRIPTEER.	BOODSKAP TUSSEN NODES GEëNKRIPTEER	BOODSKAP VANAF STUURDER TOT ONTVANGER GEëNKRIPTEER
BOODSKAP ONBESKERM TUSSEN ENKRIPSIETOESTEL EN NODE	BOODSKAP ONBESKERM IN NODE.	BOODSKAP BESKERM DEUR HELE NETWERK
KOPPE ONGEëNKRIPTEER DUS IS VERKEERONTLEDING MOONTLIK	KOPPE ONGEëNKRIPTEER DUS IS VERKEERONTLEDING MOONTLIK	KOPPE GEëNKRIPTEER DUS IS VERKEERONTLEDING ONMOONTLIK
ELKE SKAKEL MOET OOR TWEE KRIPTOGRAFIESE-TOESTELLE BESKIK.	ELKE NODE MOET OOR 'N KRIPTOGRAFIESE TOESTEL BESKIK.	KRIPTOGRAFIESE TOESTELLE SLEGS IN EINDPUNTE NODIG.
VERSPREIDING VAN SLEUTELS SLEGS NODIG TUSSEN TWEE TOESTELLE OP ELKE SKAKEL	VERSPREIDING VAN SLEUTELS NODIG TUSSEN TWEE AANGRENSENDE NODES	VERSPREIDING VAN SLEUTELS NODIG TUSSEN TWEE EINDPUNTE.

TABEL 7.2. BELANGRIKSTE SEKERHEIDSKENMERKE.

	VERKEERONTLEDING	BOODSKAPBESKERMING
SKAKELENKRIPSIE	ONMOONTLIK	SLEGS OP SKAKELS
END-TOT-END ENKRIPSIE	GEEN BESKERMING	HELE NETWERK
NODE-VIR-NODE ENKRIPSIE	GEEN BESKERMING	TUSSEN NODES

7.6. SLEUTELBESTUUR.

'n Baie belangrike aspek in kriptografie is bestuur en beheer van die sleutels wat in die kriptografiese proses gebruik word. Die sukses van enige kriptografiese proses berus op die geheimhouding en beskerming van die enkripsie- en dekripsiesleutels. In die netwerksekerheidsomgewing word die probleem van beskerming van die sleutels baie meer gekompliseerd, aangesien die stuurder en die ontvanger ver uitmekaar kan wees. Die probleem wat op netwerke bestaan dat data ongemagtig onderskep kan word deur indringers, geld ook vir die verspreiding van sleutels. Daar moet dus metodes bestaan wat die veilige vervoer van sleutels deur die netwerk verseker.

Die probleem eindig egter nie met die vervoer van die sleutels nie. Die generering en berging van die sleutels is ook 'n proses wat beskerm moet word, terwyl die vernietiging van sleutels wat nie meer gebruik word nie, 'n aspek is wat in baie gevalle in die literatuur oor die hoof gesien word.

Sleutelbestuur sluit alle aspekte ten opsigte van die hantering van sleutels in die netwerk in, vanaf die generering van die sleutels, tot die uiteindelike vernietiging van die sleutels. Die meeste probleme word ondervind met die verspreiding van die sleutels en die berging daarvan.[15][16][61]

In die res van die afdeling, sal Sleutelbestuur onder die volgende punte bespreek word

- Tipiese lewensiklus van 'n sleutel.
- Generering en toetsing.
- Verspreiding, laai en berging.
- Vernietiging.
- Tipes sleutels en hulle karakteristieke.

7.6.1. Tipiese lewensiklus van 'n sleutel.

Volgens die OSI-sekerheidsbylaag sluit sleutelbestuur die volgende in :

- Generering van nodige sleutels op tye nodig vir die vlak van sekerheid benodig,
- Bepaal volgens toegangsbeheerbehoeftes, watter entiteite 'n kopie van elke sleutel moet kry,
- Beskikbaarstelling en verspreiding van sleutels op 'n veilige manier.

Verder erken die OSI die moontlikheid dat sekere sleutelbestuurstake buite die OSI-omgewing vervul sal word. Dit sluit in die fisiese verspreiding van sleutels op 'n betroubare manier. Die uitruiling van sleutels kan ook gesien word as 'n gewone funksie van die bepaalde vlak deur middel van 'n **Sleutelverspreidingstelsel** of 'n vooraf-verspreiding deur 'n bestuursprotokol.[61]

Die OSI-benadering tot sleutelbestuur ignoreer egter twee belangrike aspekte van sleutelbestuur, naamlik die toetsing van die sleutels en die vernietiging van die sleutels, wat wel in lewensiklusse in ander literatuur voorkom.[15][16].

Die tipiese lewensiklus van 'n sleutel in 'n netwerkkriptografiese stelsel wat vir die res van die hoofstuk gebruik sal word, is die volgende :[15][16]

- Generering en toetsing.
  In die eerste stap word die sleutel gegenereer en getoets.
- Verspreiding, laai en berging.
  In stap twee word die sleutel versprei tussen die verskillende nodes waar dit gelaai en geberg word.
- Vernietiging.
  In die laaste stap word die sleutel wat nie meer in gebruik is nie, vernietig.

Sleutelbestuur is een van die belangrikste afdelings van netwerksekerheid en kan die sukses of mislukking van netwerksekerheid bepaal. Soos veral in hoofstuk 2 bespreek, is enkripsie die enigste werklik bruikbare sekerheidsmeganisme om sekerheid in 'n netwerk te verseker. Die effektiwiteit van enkripsie hang weer af van die sleutels wat gebruik word om die enkripsie mee uit te voer. 'n Netwerkomgewing veroorsaak egter weer verdere probleme as gevolg van die afstande en aantal gebruikers of nodes waarheen die sleutels versprei moet word.

7.6.1. Tipiese lewensiklus van 'n sleutel.

Volgens die OSI-sekerheidsbylaag sluit sleutelbestuur die volgende in :

- Generering van nodige sleutels op tye nodig vir die vlak van sekerheid benodig,
- Bepaal volgens toegangsbeheerbehoeftes, watter entiteite 'n kopie van elke sleutel moet kry,
- Beskikbaarstelling en verspreiding van sleutesl op 'n veilige manier.

Verder erken die OSI die moontlikheid dat sekere sleutelbestuurstake buite die OSI-omgewing vervul sal word. Dit sluit in die fisiese verspreiding van sleutels op 'n betroubare manier. Die uitruiling van sleutels kan ook gesien word as 'n gewone funksie van die bepaalde vlak deur middel van 'n **Sleutelverspreidingstelsel** of 'n vooraf-verspreiding deur 'n bestuursprotokol.[61]

Die OSI-benadering tot sleutelbestuur ignoreer egter twee belangrike aspekte van sleutelbestuur, naamlik die toetsing van die sleutels en die vernietiging van die sleutels, wat wel in lewensklusse in ander literatuur voorkom.[15][16].

Die tipiese lewensiklus van 'n sleutel in 'n netwerkkriptografiese stelsel wat vir die res van die hoofstuk gebruik sal word, is die volgende :[15][16]

- Generering en toetsing.
  In die eerste stap word die sleutel gegenereer en getoets.
- Verspreiding, laai en berging.
  In stap twee word die sleutel versprei tussen die verskillende nodes waar dit gelaai en geberg word.
- Vernietiging.
  In die laaste stap word die sleutel wat nie meer in gebruik is nie, vernietig.

Sleutelbestuur is een van die belangrikste afdelings van netwerksekerheid en kan die sukses of mislukking van netwerksekerheid bepaal. Soos veral in hoofstuk 2 bespreek, is enkripsie die enigste werklik bruikbare sekerheidsmeganisme om sekerheid in 'n netwerk te verseker. Die effektiwiteit van enkripsie hang weer af van die sleutels wat gebruik word om die enkripsie mee uit te voer. 'n Netwerkomgewing veroorsaak egter weer verdere probleme as gevolg van die afstande en aantal gebruikers of nodes waarheen die sleutels versprei moet word.

7.6.2. Generering en toetsing.

Daar bestaan twee basiese metodes van sleutelgenerasie en toetsing, naamlik ongeskakelde("off-line") en geskakelde("on-line") sleutelgenerasie.

- Ongeskakelde generasie.

  Hier word die sleutels deur 'n stelsel gegenereer wat nie direk of intyds met die netwerk gekoppel is nie. Ander terme wat gebruik word vir ongeskakelde sleutelgenerasiestelsels, is betroubarederdepartye(B3P), sleutelgenereringsstasies (SGS) sleutelverspreidingsstasies(SVS) of sleutelbedieners(SB)("Key servers") [15] [90]

  Ongeskakelde generasie van sleutels het die belangrike voordele dat sleutels in grootmaat gegenereer en deeglik getoets kan word. Verder kan die statistieke van die sleutels deeglik beheer word.

  'n Tipiese sleutelgenereringsstasie sal oor die volgende elemente beskik.[15]
  - Rekenaar met sleutelgenererings- en toetsingsprogram
  - Intydse horlosie vir die opdatering en verandering van sleutels in geval van vervaldatums.
  - Willekeurige of pseudo-willekeurige getalgenereerder.
  - Log- of stelselaantekeningsfasiliteit wat rekord hou van inligting soos sleutels gegenereer, sleutels uitgereik, aan wie die sleutels uitgereik is, of geregistreerde gebruikers in 'n netwerk.

  Gegenereerde sleutels moet nou getoets word om te verseker dat die sleutel geldig is. Ongeldige sleutels kan onder andere van die volgende wees : duplikaat sleutels, sleutels wat te kort is, sleutels wat uit dieselfde karakter bestaan ensovoorts. As daar byvoorbeeld van 'n DES-stelsel gebruik gemaak word, is daar sekere sleutels wat as swak of semi-swak sleutels geklassifiseer word. [16][112][115] Sulke sleutels moet hier geïdentifiseer word en met ander sleutels vervang word.

- Geskakelde generasie.

  Hier word die sleutels deur die kriptografiese toerusting self gegenereer en getoets net voor beskermde kommunikasie benodig word.

Geskakelde generasie bring nuwe netwerksekerheidsvoordele, maar ook probleme in 'n netwerk mee. Geskakelde generasie het die voordeel dat die sleutels nie gestoor of versprei moet word nie, en vereenvoudig dus die las van sleutelbestuur op die netwerksekerheidsmaatreëls. Die nadeel is egter dat die generering van die sleutel die reaksietyd van die netwerk kan verlaag. Soos reeds in vorige hoofstukke genoem, verwag gebruikers beskerming, maar nie ten koste van reaksietyd van die netwerk nie. Dus is dit uiters noodsaaklik dat enige netwerksekerheidsmaatreëls, en dus ook enige sleutelbestuursmaatreëls, so deursigtig as moontlik vir die gebruiker moet wees.

Verder is die kriptografiese toerusting meer kompleks, aangesien al die sleutel-genererings- en toetsingsfasiliteite in al die toerusting gedupliseer word. Sulke duplisering van toerusting verhoog die kostes van kriptografiese maatreëls in 'n netwerk, en kan netwerksekerheidsmaatreëls te duur maak.[15]

7.6.3. Verspreiding, laai en berging.

Kriptografiese sleutels kan met die hand of outomaties versprei en gelaai word.

- Handgebaseerde metodes.

Papier.

Die maklikste manier is om die sleutels op papier neer te skryf en dan die papier met die hand of per pos af te lewer. Die metode is veral van nut waar die sleutels kort is en gereeld verander word. Die papier kan maklik vernietig word nadat die sleutels in die terminaal ingevoer is. 'n Nadeel van die metode is dat as die papier nie vernietig is nie, dit in verkeerde hande kan beland.

As die metode deur 'n onderneming gebruik word, is dit noodsaaklik dat deeglike administratiewe prosedures ontwikkel moet word om die handtering en vernietiging van die papier te verseker. Die werknemers van die onderneming moet deeglik op hoogte van die prosedures gebring word.

Permanente geheuemodules.

Die metode voorsien 'n relatiewe goedkoop oplossing in terme van apparatuurkoste. Twee hoof katerorieë bestaan, naamlik inprop- en opvulmodules.

Die **Inpropmodules** word gelaai met die sleutels en dan binne die kriptografiese toerusting verseël vir solank as wat die sleutel in gebruik is. 'n Verdere maatreël wat die skrywer kan aanbeveel is dat die module en die toerusting inmengbestand ("tamper-proof" of "Tamper-resistant") behoort te wees. Dit beteken dat die inligting en die sleutels in die modules vernietig sal word as daar gepoog word om die module te verwyder, of enige ander ongemagtigde aksie op die module uitgevoer word.

Opvulmodules word gelaai met sleutels, en word dan vir 'n kort tyd aan die kriptografiese toerusting gekoppel, waartydens die sleutels in die toerusting gelaai word. Die modules kan dan veilig toegesluit word. Meer as een toestel kan met dieselfde module gelaai word. Dit is belangrik dat die inhoud van die module ook geënkripteer word en ook inmengbestand behoort te wees.

Die modules kan wissel van goedkoop, onintelligente toerusting soos magneetkaarte, tot duurder en intelligente toerusting soos slimkaarte en geheue- skyfies.

Magnetiese- en optiese media.

Dit is soms nodig om sleutels in grootmaat te vervoer, wat verspreidings- media met 'n groot geheuekapasiteit vereis. Hier kan gebruik gemaak word van sagteskywe, hardeskywe, optiese skywe en magneetbande. Optiese media het die nadeel dat baie van die bestaande produkte sogenaamde WORM- geheue("Write- Once-Read-Many-times") is. Dit beteken dat daar net een keer op die media geskryf kan word en dan nie uitgevee kan word nie. Dit veroorsaak dat die skywe of modules na gebruik fisies vernietig moet word om die sleutels te vernietig.

- Outomatiese metodes.

Hier word die sleutels elektronies, en in geënkripteerde vorm oor die netwerk self versprei. Die sleutels word met 'n spesiale sleutelenkripsiesleutel geënkripteer om dit te beskerm tydens die verspreidings- en laaifases.

Tabel 7.3. dui die voor- en nadele van die belangrikste verspreidingsmedia aan.

Tabel 7.3. Voor- en nadele van verskillende verspreidingsmedia.

	VOORDELE	NADELE
EPROM	BAIE BETROUBAAR	MOEILIK OM TE HERPROGRAMMEER EN BEPERKTE KAPASITEIT.
EEPROM (E^2PROM)	ELEKTRIES HERPROGRAMMEERBAAR EN BAIE BETROUBAAR	DUUR
BATTERY GERUGSTEUNDE RAM	VINNIGE ELEKTRIESE HERPROGRAMMERING EN KAN INMENGBESTAND WEES	SLEUTELS KAN UITGEVEE WORD AS BATTERYE FAAL
"FLASH" GEHEUE	GOEDKOPER AS EEPROM	KAN NET IN GROOT EENHEDE UITGEVEE WORD (BLADSY OF ALLES)
SAGTESKYWE	HOë KAPASITEIT, GOED VIR MODULE OF MASSA SLEUTELTOEPASSINGS. BAIE STELSELS HET REEDS SAGTESKYFAANDRYWERS	BESET SAGTESKYFAANDRYWER WAT BENODIG MAG WORD. KWESBAAR VIR ONGEMAGTIGDE KOPIëRING. VIRUSSE.
VERWYDERBARE HARDESKYWE	HOë KAPASITEIT EN VINNIGE TOEGANG.	DUUR EN MOEILIK VIR MASSAUITVEE.
MAGNETIESE BAND	HOë KAPASITEIT, GOEDKOOP, BAIE AANPASBAAR, MASSAUITVEE	STADIG, BEGIN KOSTE IS HOOG
OPTIESE SKYWE	BAIE HOë KAPASITEIT, WORD GOEDKOPER	STADIGE TOEGANG, GEEN MASSAUITVEE.

- Betroubaarheid : Dit dui aan hoe veilig die voorbestaan van die sleutels op die media is, byvoorbeeld die stoor van die sleutels in gewone RAM is onveilig aangesien 'n onderbreking in die kragtoevoer die sleutels sal vernietig.

- Kapasiteit : Dit dui aan of sleutels in groot hoeveelhede op die media gestoor kan word.

- Herprogrammering : Dit dui aan of dit moontlik is om media meer as een keer te gebruik. So kan sagteskywe meer as eenkeer gebruik word, terwyl sommige optiese skywe slegs een keer gebruik kan word.

- Spoed en toegangstye : Om die reaksietyd van enige kriptografiese toerusting te minimeer, moet die toegangstyd tot die media so kort as moontlik wees. So is 'n hardeskyf se toegangstyd baie vinniger as 'n magneetband.

- Massauitvee : Dit dui aan of die sleutels op die medium vinnig uitgevee kan word, en of sleutels selektief uitgevee kan word. Dit is van belang aangesien die vernietiging van ou sleutels nodig mag wees.

7.6.4. Vernietiging.

'n Baie belangrike aspek van sleutelbestuur wat feitlik geen aandag in die literatuur geniet nie is wat om met die sleutels te doen as dit verval, of nadat dit deur nuwe sleutels vervang word. Die skrywer is van mening dat hierdie aspek van uiterste belang is. Ou sleutels wat nie meer gebruik word nie, kan in ongemagtigde hande probleme veroorsaak. As ongemagtigde persone ou sleutels in die hande kan kry, kan dit hulle 'n idee gee oor die proses wat gebruik word om die sleutels te genereer. Daar moet seker gemaak word dat alle ou sleutels vernietig word sodra dit deur nuwe sleutels vervang is, byvoorbeeld deur die verspreidingsmedia en stoorarea skoon te vee sodra die sleutels oorgelaai is of sodra die sleutel se leeftyd verstreke is.

7.6.5. Tipes sleutels en hulle karakteristieke.

Die volgende is 'n oorsigtelike bespreking van die verskillende tipes sleutels wat in 'n kriptografiese stelsel gebruik word.[15][16][90][91][114][115][119][123]

- "One-Time-Pad"(OTP)-sleutels.

  OTP-sleutels word gebruik vir veilige kommunikasie van hoogsgeheime inligting. Die OTP-sleutel het dieselfde lengte as die boodskap wat versend moet word. Aangesien die boodskap en die sleutel dieselfde lengte het, sal herhalende karakters in die boodskap nie herhalende karakters in die geënkripteerde boodskap veroorsaak nie. Die krag van die gebruik van OTP-sleutels berus juis daarin dat daar geen moontlikheid bestaan dat daar herhalende karakters in die geënkripteerde boodskap voorkom wat ontleding van karakterfrekwensies moontlik maak nie.

Dit is belangrik dat die sleutel net een keer gebruik moet word. Die beskerming van OTP-sleutels is baie belangriker as by enige ander sleuteltipe, aangesien die algoritme vir OTP-enkripsie baie eenvoudig is. Die gebruik van OTP-sleutels in die netwerkomgewing is baie ongewild as gevolg van die komplekse generasie, verspreiding en beskermingsfasiliteite wat dit benodig.

Vanuit 'n netwerksekerheidsoogpunt is die gebruik van OTP-sleutels onaantreklik, aangesien dit 'n baie groot las op sekerheidsmaatreëls plaas. OTP-sleutels word gewoonlik net in spesiale gevalle gebruik.

- Gewone geheime sleutels.

Dit is die mees algemene sleutel in gebruik. Die lengte van die sleutels hang af van die bepaalde toepassing, en kan wissel van tien tot honderde bisse. Die grootte van die aantal moontlike sleutels, en die frekwensie van gebruik sal bepaal of die sleutels sekwensieel of willekeurig gegenereer sal word. Gewone geheime sleutels word gewoonlik in sleutelmodules of opvulmodules geberg en versprei.

Die beskerming van die sleutels vanaf generasie tot vernietiging is weereens van uiterste belang alhoewel die betroubaarheid van die stelsel verhoog kan word deur die geheimhouding van die enkripsie- en dekripsiealgoritmes.[15] Vanuit 'n netwerksekerheidsoogpunt beteken dit egter dat die enkripsie- en dekripsie- algoritmes in elke node geïmplimenteer moet word. Verder moet die sleutels na al die nodige nodes versprei word.

- Boodskapsleutels.

'n Boodskapsleutel is 'n nie-geheime sleutel, wat in kombinasie met 'n geheime sleutel gebruik word. Die sleutels word gebruik as daar 'n beperkte aantal geheime sleutels bestaan, en dieselfde geheime sleutel meer as een keer gebruik moet word.

Die geheimesleutel sowel as die boodskapsleutel word saam in die kriptografiese algoritme ingevoer. Dit beteken dat as dieselfde boodskap met dieselfde geheimesleutel geënkripteer word, sal die boodskapsleutel verseker dat die geënkripteerde teks nie dieselfde is nie.

- Sleutelenkripsie- of Meestersleutels.

  Meestersleutels word gebruik om ander sleutels mee te enkripteer tydens die verspreiding van die sleutels of as die sleutels gestoor word. Meestersleutels word in 'n semi-permanente vorm in die kriptografiese toerusting gestoor en beskik oor 'n langer leeftyd as die meeste ander sleutels. Die sleutel bestaan vir 'n beperkte leeftyd binne die enkripsietoerusting, en word aan die einde van die leeftyd vernietig en vervang met 'n nuwe sleutel of stel sleutels.

- Permanente of gebruikersleutels.

  Gebruikersleutels kan beskou word as deel van die kriptografiese algoritme, aangesien die sleutels nie gereeld vervang word nie. Hier kan die enkripsiealgoritme verander word en nie die sleutel nie.

  Gebruikersleutels is gewoonlik 64 bisse of langer in lengte, sodat alle moontlike kombinasies nie deur aanvallers getoets kan word nie. Die sleutels kan willekeurig gegenereer word, aangesien dit nie baie vervang word nie. Slegs een sleutel per kriptografiese toestel in elke netwerk is nodig.

  Uit 'n netwerksekerhedsoogpunt kan hierdie metode probleme veroorsaak aangesien die gevaar van ongemagtigde bloodstelling van die sleutel in enige netwerk bestaan. Dit is 'n moeilike proses om die nuwe sleutels aan die gebruiker toe te ken as sy sleutel in verkeerde hande beland het.

- Sessiesleutels.

  Sessiesleutels word gebruik in rekenaarnetwerke waar 'n kommunikasiesessie opgestel word tussen twee terminale of tussen 'n terminaal en 'n gasheerrekenaar. 'n Sessie kan slegs bestaan uit die versending van een kort boodskap, of dit kan bestaan uit die versending van groot hoeveelhede data oor 'n periode van 'n paar ure.

  Die sessiesleutel kan gekies word uit 'n vooraf verspreide stel sleutels, of kan uitgeruil word aan die begin van die sessie, en word gebruik as 'n gewone enkripsiesleutel vir die duur van die sessie. Daar bestaan gewoonlik 'n sessiesleutel vir beide rigtings van die dataverkeer.

  Sessiesleutels beskik verder oor dieselfde kenmerke as gewone geheimesleutels.

Vir netwerksekerheid hou hierdie metode voordele sowel as nadele in. Kommunikasie word baie goed beskerm, aangesien elke sessie oor nuwe sleutels beskik. Dit maak dit baie moeilik vir enige indringer om genoeg inligting te onderskep om die sleutels te bepaal, veral as die sessies so kort as moontlik gehou word. Verder word slegs een sessie se kommunikasie in gevaar gestel as die sleutels in verkeerde hande val. Die nadeel is dat kort sessies weereens groot sleutelverkeer veroorsaak wat 'n las op die netwerk plaas. Die metode is egter in die meeste netwerke en veral finansiële netwerke in gebruik.

- Wagwoordtipe sleutels.

Wagwoordtipe sleutels kom gewoonlik voor in lêerenkripsie pakette waar die gebruiker 'n wagwoord kies om die data te enkripteer en dieselfde wagwoord weer nodig het om die data te dekripteer. Die sleutel is gewoonlik ses karakters of langer, en word gekombineer met 'n permanente sleutel in die enkripsiealgoritme.

Die metode is nie baie veilig nie, aangesien die sleutel dieselfde probleme as gewone wagwoorde het. Die sleutel is gewoonlik te kort, en kan ook gewoonlik maklik geraai word, aangesien gebruikers die gewoonte het om wagwoorde te kies wat met hulle self verband hou, soos byvoorbeeld adresse en telefoon nommers. Die metode behoort sover moontlik vermy te word, veral in die netwerksekerheidomgewing. [15]

- Publieke sleutels.

Publieke sleutelkriptografie maak gebruik van sleutelpare. Die een sleutel is geheim terwyl die ander een bekend is. Die stelsel staan bekend as 'n asimmetriese stelsel waar die publieke sleutel algemeen bekend is, terwyl die geheime sleutel net aan die eienaar bekend is. Die geheime sleutel kan nie afgelei word van die publiekesleutel en/of die algoritme nie. Beide enkripsie en waarmerking kan deur middel van publiekesleutels verkry word.

Publiekesleutels is gewoonlik tussen 500 en 'n 1000 bisse lank. Die sleutels word gekies uit spesiale priemgetalle wat nie maklik gefaktoriseer kan word nie. Die kragtigheid van die publiekesleutelalgoritme ontstaan uit die feit dat dit uiters moeilik is om groot getalle te faktoriseer.[15][16][108]

Die belangrikste nadeel van publieke sleutelalgoritmes is dat dit as gevolg van die komplekse wiskundige berekenings stadig is. Dus word dit gewoonlik net vir sleuteluitruiling of vir versending van kort boodskappe gebruik. Die vinnigste algoritme aan die begin van 1990 kon 19 killobisse per sekonde hanteer in vergelyking met die Megabisse per sekonde van gewone stelsels.[15]

7.6.6. SLEUTELBESTUUR IN DIE FINANSIëLE BANKOMGEWING.

In die finansiële bankomgewing kom daar twee belangrike stelsels voor waar sleutelbestuur van groot belang is nl :

- Elektroniese fondsoordrag by verkooppunt of EFT-POS ("Electronic funds Transfer at Point of Sale")[16][114][115][119][123]

  In 'n EFT-POS stelsel betaal 'n gebruiker 'n onderneming vir goedere of dienste gelewer deur die onderneming. Die gebruiker betaal deur middel van 'n kaart en identifiseer homself deur sy geheime Persoonlike Identifikasie Nommer(PIN) op 'n spesiale PIN-sleutelbord of PIN-pad in te sleutel. Die terminaal kommunikeer met die gasheerrekenaar in die bank om die gebruiker se PIN en saldo te kontroleer. Die transaksiedata word ook hier vasgelê vir die oordrag van die fondse vanaf die gebruiker se rekening.

- Outomatiese tellermasjiene of ATM ("Automated teller Machines") [16][115][119][122]

  In 'n ATM-stelsel kan 'n gebruiker banktransaksies vanaf enige ATM-terminaal verrig. Hier maak die gebruiker weer eens van 'n kaart gebruik en sleutel ook sy PIN in om homself te identifiseer. Die terminaal kommunikeer hier ook met die gasheerrekenaar in die bank om die gebruiker se PIN en saldo te kontroleer. Die transaksiedata word ook hier vasgelê vir die verdere uitvoering van die transaksie.

Die vernaamste sekerheidsprobleem by die twee stelsels is die feit dat beide die stelsels fondsoordragte in onveilige (publieke) omgewings doen. In beide stelsels kom terminale in publieke areas voor en dus is streng fisiese beskerming van die stelsels nie moontlik nie. Streng veiligheidsmaatreëls is nodig om die transaksieboodskappe tussen die terminale en die gasheerrekenaar te beskerm. Die twee belangrikste maatreëls wat hier gebruik word is die enkripsie van die PIN en transaksiedata en en die byvoeging van 'n boodskap waarmerkingskode of MAC ("Message Authentication Code"). Die enkripsie beskerm die PIN en transaksiedata teen ongemagtigde openbaarmaking, terwyl die MAC gebruik word om die egtheid van die boodskap te bewys.

Beide die enkripsie- en die waarmerkingsprosesse maak normaalweg gebruik van standaard gepubliseerde algoritmes, wat beteken dat die sekerheid van die hele stelsel afhanklik is van die geheimhouding van die sleutels.

Om sekerheid te verbeter word afsonderlike sleutels gebruik vir die enkripsie- en waarmerkingsprosesse. Aangesien die sleutels en die algoritmes in die PIN-pad en die ATM se geheue gestoor word, moet verseker word dat die sleutels nie uit die toestelle onttrek kan word na dit eers in die toestelle ingevoer is nie. Indien dit wel moontlik is, moet die potensiële finansiële skade deur indringers geminimeer word.

Die eerste doelwit is om die PIN-pad en die ATM inmengbestand te maak wat sal verseker dat enige ongemagtigde poging om die sleutels te onttrek die vernietiging van die sleutels tot gevolg sal hê. Die tweede doelwit is om die sleutels gereeld te verander om gevolge van onopgespoorde ongemagtigde openbaarmaking van sleutels te beperk.[115][122]

Daar bestaan twee algemene sleutelbestuursmetodes vir die verandering van die enkripsie- en waarmerkingssleutels naamlik :

- Meester/sessiesleutelstelsels
- Transaksie veranderlikesleutelstelsels.

Vervolgens sal daar 'n kort bespreking van beide metodes, sowel as die sterk- en swakpunte van elke metode gegee word.

MEESTER/SESSIESLEUTELSTELSELS

Die metode is die mees algemene metode wat gebruik word in EFT-POS en ATM stelsels gebruik word.[115][122] Elke PIN-pad en ATM bevat 'n meestersleutel wat min, indien ooit vervang word. Sodra die terminaal aanteken na die gasheerrekenaar, word 'n nuwe enkripsie- en waarmerkingsleutel, wat onder die bepaalde terminaal se meestersleutel geënkripteer is, na die terminaal gestuur. Die sleutels word in die terminaal gedekripteer en dan vir die bepaalde sessie gebruik vir enkripsie en waarmerking van boodskappe gedurende die sessie. 'n Sessie kan verskil van stelsel tot stelsel maar is normaalweg net 'n dag lank.[16][115][122]

Indien die sessiesleutels ongemagtig vrygestel word, word al die transaksies vir die bepaalde sessie in die bepaalde ATM of EFT-POS toestel bedreig.

As die meestelsëutel egter vrygestel word, word alle gewese sowel as toekomstige transaksies in die bepaalde ATM of EFT-POS toestel bedreig. Dit is dan ook die vernaamste swakpunt in die Meester/sessiesleutelstelsel.

Indien aangeneem word dat die gasheerrekenaar veilig is en die Meestersleutel aan die begin op 'n veilige manier gelaai word, bestaan daar twee maniere om die sleutels te bepaal, naamlik : [115]

- **Fisiese- of logieseinmenging met die PIN-pad of die ATM** sodat die sleutels vrygestel word. Op die wyse kan beide die Meester- en die Sessiesleutel vrygestel word. Die sleutels word ook normaalweg gelyktydig vrygestel.

  Om die impak van die vrystelling te bepaal is daar weer twee moontlikhede. Indien die vrystelling **opgemerk** word, kan die sleutels gekanseleer of vervang word. In so 'n geval kan slegs gewese transaksies en sleutels ontsyfer word. Indien die vrystelling egter **onopgemerk** is en die gebruik van die PIN-pad en ATM gaan voort, is beide gewese en toekomstige transaksies en sleutels in gevaar.

- **Ontleding van geënkripteerde data.** In die metode word al die moontlike sleutels gebruik om 'n boodskap te enkripteer. Die resultaat word dan vergelyk met die geënkripteerde data wat onderskep is. Die metode word uitputtende soek genoem. As 'n algoritme soos DES gebruik word, sal die metode lank, duur wees maar teoreties wel moontlik.[115]

  Aangesien die Meestersleutel slegs gebruik word om die Sessiesleutels mee te enkripteer, sal dit eers nodig wees om die Sessiesleutel te bepaal en dan dieselfde proses om weer die Meestersleutel te bepaal. Vanuit die oogpunt is die Meestersleutel dubbel beskerm.[115] As die Sessiesleutel opgespoor word, word dit 'n **enkelbreek** genoem. As die Meestersleutel opgespoor word, word dit 'n **dubbelbreek** genoem.

TRANSAKSIE VERANDERLIKESLEUTELSTELSELS.

Die metode is ontwikkel om die swakpunte in die meester/sessiesleutelstelsels uit te skakel. Hier word veral aandag geskenk aan die gevaar wat die vrystelling van die meestersleutel kan veroorsaak. Daar is met die tyd verskillende transaksie- veranderlikesleutelstelsels ontwikkel, maar die basiese werking van al die stelsels is dieselfde.[115]

In hierdie stelsel is daar geen Meestersleutel nie. Die enkripsie- en waarmerkingssleutels word outomaties na elke transaksie verander. Die opdateringsfunksie is 'n eenrigtingfunksie wat beteken dat as een transaksiesleutel vrygestel word slegs die een transaksie in gevaar is. Daar is in die geval geen bedreiging vir gewese transaksies of sleutels nie. Dit is wel moontlik om toekomstige sleutels te bepaal indien die oorspronklike vrystelling onopgemerk is.

Tabel 7.4. som die impak van die verskillende vrystellings op.

TABEL 7.4. IMPAK VAN VERSKILLENDE VRYSTELLINGS.

		VERSKILLENDE MOONTLIKE VRYSTELLINGS			
BEDRYGING	SLEUTEL STELSEL	ENKELE BREEK	DUBBELE BREEK	VRYSTELLING OPGEMERK	VRYSTELLING ONOPGEMERK
TOEKOMSTIGE TRANSAKSIES	MEESTER/ SESSIE	SESSIE ALLEEN	JA		JA
	TRANSAKSIE VERANDELIK	NEE	NEE		JA
VORIGE TRANSAKSIES	MEESTER/ SESSIE	SESSIE ALLEEN	JA	JA	JA
	TRANSAKSIE VERANDERLIK	NEE	NEE	NEE	NEE

7.7. EVALUERING VAN KRIPTOGRAFIESE APPARATUUR.

Die keuse van kriptografieseprogrammatuur en apparatuur kan vir enige onderneming baie probleme veroorsaak. Baie ondernemings beskik nie oor die fasiliteite en ondervinding om 'n deeglike ondersoek na die produkte te maak nie. Daar is verskillende faktore en eienskappe waarna daar gekyk behoort te word tydens die evaluering van kriptografiese produkte.

Highland bespreek in [89] die evaluering van enkripsieprogrammatuur en -apparatuur vir **mikrorekenaars**. In die bespreking word daar slegs gekonsentreer op losstaande mikrorekenaars en daar word nie aandag geskenk aan netwerke en rekenaars wat aan netwerke gekoppel is nie. Die doel van hierdie afdeling is die proses wat in [89] bespreek word toe te pas op die netwerkomgewing en waar nodig uit te brei om in die netwerkomgewing gebruik te word vir die beoordeling van kriptografiesetoerusting.

Die evaluasie proses bestaan uit ses fase naamlik:

- Fase 1 - Basiese vrae.
- Fase 2 - Evaluasie omgewing.
- Fase 3 - Evaluasie van enkripsie kenmerke.
- Fase 4 - Enkripsie tyd en lêer grote.
- Fase 5 - Sleutel en herwinningskenmerke.
- Fase 6 - Addisionele kenmerke.

7.7.1. Fase 1 - Basiese vrae.

Daar is 'n paar basiese vrae wat beantwoord moet word voordat daar begin word met die evaluering van 'n spesifieke produk. Die vrae is daarop gerig om te bepaal hoe nodig die onderneming die toerusting het.

- Watter vlak van beskerming is nodig?
  Alle ondernemings het nie nodig om om inligting en kommunikasie te beskerm op die vlak nodig vir militêre- en regeringsinstansies nie. Dit is belangrik om te bepaal van wie die inligting beskerm moet word. Voorbeelde hier is ongemagtigde werknemers en mededingers. Verder moet bepaal word wat die kundigheidsvlak van die indringers is. Is die indringers hoogs profesioneel met van die modernste toerusting? Of is die indringers slegs amateurs wat maklik gekeer kan word?

- Is dieselfde algoritme of stelsel nodig vir alle sensitiewe data en boodskappe?
  Hoe meer ingewikkeld die algoritme is, hoe hoër is die koste en hoe langer neem die enkripsie/dekripsie proses. In baie gevalle sal 'n onderneming oor data beskik wat uiters geheim is maar ander data wat baie minder geheim is. Om dus alle data aan die hoogste moontlike vlak van beskerming te onderwerp is onnodig en kan baie tyd in beslag neem. Dit mag dus nodig wees om verskillende algoritmes te gebruik, een vir hoogs geheime inligting en 'n ander vir mindergeheime inligting.

- Watter gedeelte van die onderneming se data moet geënkripteer word?
  Die hoeveelheid data wat geënkripteer moet word is 'n baie belangrike faktor. Daar moet egter ook bepaal word of al die data geënkripteer moet word. Daar mag dalk groot hoeveelhede data wees wat glad nie geënkripteer behoort te word nie. In so 'n geval mag dit goedkoper wees om stadiger en goedkoper apparatuur en programmatuur aan te skaf, in plaas van duur toerusting wat baie vinnig is.

- Watter individue indien enige, sal verantwoordelik wees vir die kriptografie?
  Daar moet bepaal word wie verantwoordelik sal wees vir die kriptografieseproses. As die apparatuur so geïnstaleer is dat die hele proses outomaties en deursigtig geskied, is daar geen opleiding van personeel ter sprake nie. Indien die toerusting fisies geaktiveer moet word as dit gebruik moet word, sal personeel die nodige opleiding moet ondergaan. Die personeel mag bestaan uit rekenaarkundiges of selfs persone met die minimum rekenaarkennis. In so 'n geval sal die toerusting so eenvoudig en maklik bruikbaar as moontlik wees. Wat veral belangrik is, is dat daar genoegsame en duidelik verstaanbare handleidings moet wees.

- Wat is die beperkings op die fondse beskikbaar?
  Hier moet bepaal word watter hoeveelheid fondse is beskikbaar vir die aankoop van die toerusting. Indien 'n beperkte bedrag beskikbaar is, kan sekere produkte wat die bedrag oorskry reeds vroeg in die evaluasie proses buite rekening gelaat word.

7.7.2. Fase 2 - Evaluasie omgewing.

Om te verseker dat alle produkte 'n gelyke beoordeling ontvang, behoort die produkte in 'n gekontroleerde omgewing, waar omstandighede en toestande so identies as moontlik is, getoets te word. Die toets omgewing moet ook so na as moontlik ooreenkom met die werklike omgewing waar die gekose produk aangewend sal word.

In die eerste plek moet die toerusting gekies word waarop die produkte getoets gaan word. Daar moet duidelik gelet word op die verskillende moontlike konfigurasies waarin die produkte aangewend sal word. 'n Bepaalde produk kan goed presteer vir een konfigurasie, maak nie vir 'n ander nie. In die netwerkomgewing is veral die verskillende netwerkbestuursstelsels en bedryfsstelsels van belang.

- Produk evaluasie oorsiglys.
  Hier word slegs 'n kort oorsig van die belangrikste kenmerke en fasiliteite van die bepaalde produk opgestel. Die inligting behoort gewoonlik sommer vanaf produk inligtingstukke opgestel te word.
  - Watter bedryfsstelsels word deur die produk ondersteun.
  - Wat is die prys van die produk en wat is die moontlikheid dat 'n demonstrasie weergawe van die produk kostevry verkry kan word vir die evaluasieproses.
  - Bestaan die produk uit apparatuur, programmatuur of albei.

- Produk oorsig.
  Hier word aandag geskenk aan kenmerke soos handleidings, installasie, opleiding. Die volgende punte is hier van belang:

  - Bestaan daar handleidings vir die produk?
  - Hoe volledig en duidelik is die handleidings?
  - Wat is die installasieproses?
  - Is gespesialiseerde persone nodig vir die installering?
  - Beskik die onderneming oor die personeel of voorsien verkoper die diens?
  - Sal die verkoper personeel oplei vir installasie, werking en onderhoud?

7.7.3. Fase 3 - Evaluasie van enkripsie kenmerke.

In hierdie fase word die verskillende kriptografiese fasiliteite van die produk bestudeer. Die meeste van die inligting wat hier benodig word, kan gevind word in die handleidings en die produk se reklame materiaal. Die belangrikste punt wat hier bestudeer moet word is die algoritme of algoritmes wat beskikbaar is.

Sekere programmatuur beskik oor verskillende algoritmes vir data-enkripsie en dan weer ander vir kommunikasie of uitvoerbare programme. Die volgende is 'n paar punte wat in aanmerking geneem kan word by die evaluasie :

- Kan meervoudige enkripsie toegepas word met dieselfde algoritme met verskillende sleutels?
- Kan meervoudige enkripsie toegapas word met verskillende algoritmes met dieselfde sleutel?
- Word lêers gepak ("compressed") voor enkripsieproses?

7.7.4. Fase 4 - Enkripsie tyd en lêer grote.

Vanuit 'n netwerksekerheidsoogpunt is die spoed van die enkripsie en dekripsieprosesse en die grote van die uitvoer van groot belang. As 'n produk te lank neem om die twee prosesse uit te voer, mag die afname in reaksietyd in die netwerk dit noodsaak dat enkripsie nie meer gebruik sal wil word nie.

7.7.5. Fase 5 - Sleutel en herwinningskenmerke.

In fase 5 word die produk se sleutelkenmerke en herwinningsfasiliteite bestudeer.

- Sleutelkenmerke.
  Die programmatuur se sleutelvereistes en kenmerke moet deeglik bestudeer word en die volgende is punte wat hier in aanmerking geneem behoort te word. :
  - Is die sleutellengte 'n veilige lengte, byvoorbeeld meer as 6 karakters?
  - Wat is die maksimum en minimum lengte van die sleutels?
  - Kan slegs vertoonbare karakters in sleutels gebruik word?
  - Kan karakters en syfers gemeng word in die sleutel?
  - Kan die gebruiker die sleutel kies, of word die sleutel deur die programmatuur gegenereer?

- Herwinning.
  Dit is belangrik om te bepaal wat gaan gebeur in die geval van verlore sleutels. Sal daar in manier wees om die lêer of boodskap te herwin as die sleutel verlore geraak het?

7.7.6. Fase 6 - Addisionele kenmerke.

In fase 6 word die addisionele fasiliteite van die produk bestudeer. Hier word veral aandag gegee aan fasiliteite wat nie vir die onderneming 'n prioriteit by die keuse van die produk is nie. Voorbeelde hiervan is duidelike help-fasiliteite en ouditspoor.

7.8. SAMEVATTING.

Kriptografie is 'n baie wye veld en om die hele veld te dek sal onmoontlik wees. Slegs 'n oorsig van 'n paar van die belangrikste aspekte van kriptografie is in hierdie hoofstuk gedek. Vir lesers wat meer inligting benodig word daar verskeie verwysings aangedui in die hoofstuk.

Kriptografie kan 'n baie belangrike bydrae lewer tot netwerksekerheidsmaatreëls in 'n netwerk. Dit is egter belangrik om die hele omvang en probleme verbonde aan kriptografie deeglik te verstaan. Dit is belangrik dat die gebruikers en implimenteerders veral die eise van sleutelbestuur deeglik verstaan en bestudeer.

In paragraaf 7.7. is gepoog om die leser 'n idee te gee oor die ingewikkeldheid van die evaluasieproses van verskillende kriptografiese toerusting en programmatuur.

Twee verdere belangrike velde in kriptografie wat nie hier aandag gekry het nie is waarmerking en die gebruik van elektroniese handtekeninge. Die twee velde is baie belangrik maar het elk sy eie bespeking nodig.

- Watter individue indien enige, sal verantwoordelik wees vir die kriptografie?
  Daar moet bepaal word wie verantwoordelik sal wees vir die kriptografieseproses. As die apparatuur so geïnstaleer is dat die hele proses outomaties en deursigtig geskied, is daar geen opleiding van personeel ter sprake nie. In dien die toerusting fisies geaktiveer moet word as dit gebruik moet word, sal personeel die nodige opleiding moet ondergaan. Die personeel mag bestaan uit rekenaarkundiges of selfs persone met die minimum rekenaarkennis. In so 'n geval sal die toerusting so eenvoudig en maklik bruikbaar as moontlik wees. Wat veral belangrik is, is dat daar genoegsame en duidelik verstaanbare handleidings moet wees.

- Wat is die beperkings op die fondse beskikbaar?
  Hier moet bepaal word watter hoeveelheid fondse is beskikbaar vir die aankoop van die toerusting. Indien 'n beperkte bedrag beskikbaar is, kan sekere produkte wat die bedrag oorskry reeds vroeg in die evaluasie proses buite rekening gelaat word.

7.7.2. Fase 2 - Evaluasie omgewing.

Om te verseker dat alle produkte 'n gelyke beoordeling ontvang, behoort die produkte in 'n gekontroleerde omgewing, waar omstandighede en toestande so identies as moontlik is, getoets te word. Die toets omgewing moet ook so na as moontlik ooreenkom met die werklike omgewing waar die gekose produk aangewend sal word.

In die eerste plek moet die toerusting gekies word waarop die produkte getoets gaan word. Daar moet duidelik gelet word op die verskillene moontlike konfigurasies waarin die produkte aangewend sal word. 'n Bepaalde produk kan goed presteer vir een konfigurasie, maak nie vir 'n ander nie. In die netwerkomgewing is veral die verskillende netwerkbestuursstelsels en bedryfsstelsels van belang.

- Produk evaluasie oorsiglys.
  Hier word slegs 'n kort oorsig van die belangrikste kenmerke en fasiliteite van die bepaalde produk opgestel. Die inligting behoort gewoonlik sommer vanaf produk inligtingstukke opgestel te word.
  - Watter bedryfsstelsels word deur die produk ondersteun.
  - Wat is die prys van die produk en wat is die moontlikheid dat 'n demonstrasie weergawe van die produk kostevry verkry kan word vir die evaluasieproses.
  - Bestaan die produk uit apparatuur, programmatuur of albei.

- Produk oorsig.
  Hier word aandag geskenk aan kenmerke soos handleidings, installasie, opleiding. Die volgende punte is hier van belang:

  - Bestaan daar handleidings vir die produk?
  - Hoe volledig en duidelik is die handleidings?
  - Wat is die installasieproses?
  - Is gespesialiseerde persone nodig vir die instalering?
  - Beskik die onderneming oor die personeel of voorsien verkoper die diens?
  - Sal die verkoper personeel oplei vir installasie, weking en onderhoud?

7.7.3. Fase 3 - Evaluasie van enkripsie kenmerke.

In hierdie fase word die verskillende kriptografiese fasiliteite van die produk bestudeer. Die meeste van die inligting wat hier benodig word, kan gevind word in die handleidings en die produk se reklame materiaal. Die belangrikste punt wat hier bestudeer moet word is die algoritme of algoritmes wat beskikbaar is.

Sekere programmatuur beskik oor verskillende algoritmes vir data-enkripsie en dan weer ander vir kommunikasie of uitvoerbare programme. Die volgende is 'n paar punte wat in aanmerking geneem kan word by die evaluasie :

- Kan meervoudige enkripsie toegapas word met dieselfde algoritme met verskillende sleutels?
- Kan meervoudige enkripsie toegapas word met verskillende algoritmes met dieselfde sleutel?
- Word lêers gepak ("compressed") voor enkripsieproses?

7.7.4. Fase 4 - Enkripsie tyd en lêer grote.

Vanuit 'n netwerksekerheidsoogpunt is die spoed van die enkripsie en dekripsieprosesse en die grote van die uitvoer van groot belang. As 'n produk te lank neem om die twee prosesse uit te voer, mag die afname in reaksietyd in die netwerk dit noodsaak dat enkripsie nie meer gebruik sal wil word nie.

7.7.5. Fase 5 - Sleutel en herwinningskenmerke.

In fase 5 word die produk se sleutelkenmerke en herwinningsfasiliteite bestudeer.

- Sleutelkenmerke.
  Die programmatuur se sleutelvereistes en kenmerke moet deeglik bestudeer word en die volgende is punte wat hier in aanmerking geneem behoort te word. :
  - Is die sleutellengte 'n veilige lengte, byvoorbeeld meer as 6 karakters?
  - Wat is die maksimum en minimum lengte van die sleutels?
  - Kan slegs vertoonbare karakters in sleutels gebruik word?
  - Kan karakters en syfers gemeng word in die sleutel?
  - Kan die gebruiker die sleutel kies, of word die sleutel deur die programmatuur gegenereer?

- Herwinning.
  Dit is belangrik om te bapaal wag gaan gebeur in die geval van verlore sleutels. Sal daar in manier wees om die lêer of boodskap te herwin as die sleutel verlore geraak het?

7.7.6. Fase 6 - Addisionele kenmerke.

In fase 6 word die addisionele fasiliteite van die produk bestudeer. Hier word veral aandag gegee aan fasiliteite wat nie vir die onderneming 'n prioriteit by die keuse van die produk is nie. Voorbeelde hiervan is duidelike help-fasiliteite en ouditspoor.

7.8. SAMEVATTING.

Kriptografie is 'n baie wye veld en om die hele veld te dek sal onmoontlik wees. Sleeg 'n oorsig van 'n paar van die belangrikste aspekte van kriptografie is in hierdie hoofstuk gedek. Vir lesers wat meer inligting benodig word daar verskeie verwysings aangedui in die hoofstuk.

Kriptografie kan 'n baie belangrike bydrae lewer tot netwerksekerheidsmaatreëls in 'n netwerk. Dit is egter belangrik om die hele omvang en probleme verbonde aan kriptografie deeglik te veerstaan. Dit is belangrik dat die gebruikers en implimenteerders veral die eise van sleutelbestuur deeglik verstaan en bestudeer.

In paragraaf 7.7. is gepoog om die leser 'n idee te gee oor die ingewikkeldheid van die evaluasieproses van verskillende kriptografiese toerusting en programmatuur.

Twee verdere belangrike velde in kriptografie wat nie hier aandag gekry het nie is waarmerking en die gebruik van elektroniese handtekeninge. Die twee velde is baie belangrik maar het elk sy eie bespeking nodig.

HOOFSTUK 8.

'n METODOLOGIESE BENADERING TOT DIE IMPLIMENTERING VAN NETWERKSEKERHEID.

8.1. INLEIDING.

Die doel van hierdie hoofstuk is om die moontlikheid van die ontwikkeling van 'n metodologiese benadering tot netwerksekerheid te ondersoek. Vir doeleindes van hierdie bespreking is 'n metodologie 'n stel riglyne wat gevolg kan word om netwerksekerheid te implimenteer. Heelwat probleme word deur ondernemings ondervind in die ontwikkeling en implimentasie van rekenaar- en netwerksekerheid binne die ondernemings. Verskeie redes kan gevind word vir die probleme, maar die belangrikste is die volgende :

- Gebrek aan betrokkenheid van personeel, bestuur en veral topbestuur van die onderneming. Selfs die beste sekerheidsmaatreëls sal faal as die personeel van die onderneming nie die redes vir die maatreëls verstaan nie. Ondersteuning van die topbestuur van die onderneming is nodig om die maatreëls genoeg gewig te gee en selfs af te dwing indien nodig.
- Onvoldoende probleemstelling en ontwikkeling van rekenaar- en netwerksekerheids maatreëls. Baie ondernemings word sklelik bewus van sekerheid en wil dit dan onmiddelik implimenteer sonder om eers regtig te bepaal wat die probleem is en dan genoeg tyd aan die ontwikkeling van behoorlike maatreëls te bestee.
- Poging om rekenaar- en netwerksekerheid te implimenteer sonder die teenwoordigheid van 'n sekerheidsbeleid.
- Afwesigheid van 'n goed gestruktureerde metodologie tydens die ontwikkeling en implimentasie.
- Afwesigheid van die gebruik van 'n bekende kommunikasie- of sekerheidsstandaard soos byvoorbeeld die ISO-standaard.

Die gebruik van 'n metodologiese benadering tot netwerksekerheid kan verseker dat bogenoemde probleme uitgeskakel kan word. Die probleem is dat daar in die literatuur uiters min aandag aan die ontwikkeling van netwerksekerheidsmetodologiê gegee is. Slegs twee artikels is opgespoor wat aandag aan 'n metodologiese benadering tot netwerksekerheid gee.[129][130]

In die res van die hoofstuk sal daar aandag geskenk word aan twee metodologiese benaderings naamlik :

- Metodologie vir netwerksekerheid ontwerp soos bespreek in [129].
- Die RS-metodologie.

Beide benaderings beskik oor voordele en nadele. Die Rekenaarsekerheidsmetodologie (RS-Metodologie) is ontwikkel aan die Randse Afrikaanse Universiteit deur Prof J.H.P. Eloff en K.P. Badenhorst.

Die doel van die RS-Metodologie is om 'n gestruktureerde benadering vir die spesifikasie van rekenaarsekerheid en die toepassing van 'n rekenaarsekerheidsbeleid binne 'n onderneming daar te stel. Daar sal dan sekere uitbreidings gemaak word aan die RS-metodologie om sodoende op 'n meer effektiewe wyse voorsiening te maak vir netwerksekerheid.

8.2 METODOLOGIE VIR NETWERKSEKERHEID ONTWERP.

In hierdie afdeling sal die Metodologie vir netwerksekerheidontwikkeling wat ontwikkel is deur Graft en Pabrai, [129], bespreek word. Die metodologie is gebasseer op die ISO se OSI-Verwysingsmodel en Sekerheidsargitektuur. Die metodologie is ontwikkel deur ingenieurs en dus is daar vanuit 'n ingenieursoogpunt na die probleem gekyk. Die benadering het egter'n paar probleme wat later in die hoofstuk bespreek word.

'n Oorsigtelike opsomming van die metodologie word gegee in FIG 8.1. :

1] Spesifikasiefase.
- Bepaal stelselvereistes.
  - Uiteensetting van toepassing.
  - Definieer sekerheidsbuitelyne.
  - Definieer nodige sekerheidsdienste.
  - Definieer nodige sekerheidsbestuurskenmerke.
- Identifiseer beperkings op ontwerp.
  - Hersien toepaslike standaarde.
  - Bepaal netwerktipe en topologie.
  - Oorweeg organisatoriese faktore.

2] Ontwerpfase.
- Definieer sekerheidsargitektuur.
- Plasing van funksionaliteit binne argitektuur.
- Definieer sekerheidsprimitiewe.
- Kies onderliggende sekerheidsmeganismes.
- Definieer diensprotokolle.

3] Implimentasiefase.
- Ontwikkel benodigde apparatuur en programmatuur.
- Toetsing en verifikasie.
- Prestasieontleding.
- Akkreditasie en Sertifikasie.
- Herhaal Ontwerpfase indien nodig.
-

FIG 8.1. Oorsig van metodologie vir Netwerksekerheid.

Die metodologie word in die volgende drie hooffases opgedeel :

- Spesifikasiefase.
- Ontwerpfase.
- Implimentasiefase.

8.2.1. SPESIFIKASIEFASE.

'n Belangrike kenmerk van die metodologie is die duidelike onderskeid tussen wat die doel van die stelsel naamlik die spesifikasie- en ontwerpfases, en die implimentasie van die stelsel naamlik die implimentasiefase. Die benadering dui duidelik op die ingenieursbenadering tot programmatuurontwikkelingsmetodologië. Die metode veroorsaak dat 'n probleemgeoriënteerde benadering gevolg word en dat die probleem deeglik bestudeer word, voordat aandag aan enige implementasie aspekte gegee word.

Die spesifikasiefase word verder ook opgedeel in die bepaling van stelselvereistes en identifisering van beperkings. Die vereistes word bepaal deur die probleem self, terwyl die beperkings meer afhang van die omgewing van die probleem as die probleem self.

Bepaal stelsel vereistes.

Hier word die probleem wat opgelos moet word beskryf. Dit is belangrik dat hier nie aandag aan enige implimentasie aspekte gegee moet word nie.

'n Belangrike benadering is om te kyk na die werkslas van die stuurder en die indringer. Die stuurder se werkslas is die aktiwiteite nodig om die inligting by die ontvanger te kry. Die indringer se werkslas is weer die aktiwiteite nodig om die inligting te onderskep en dit te interpreteer. In 'n onveilige stelsel is die stuurder se werkslas laag terwyl die indringer se werkslas ook laag is. In 'n meer veilige stelsel is die stuurder se werkslas hoër maar die indringer se werkslas is ook hoër. Die doelwit is om die indringer se werkslas vinniger te laat toeneem as die stuurder se werkslas. In die ideale stelsel behoort die stuurder se werkslas laag te wees terwyl die indringer se werkslas baie hoog is.

- Uiteensetting van toepassing.
  Hierdie stap is slegs 'n stelling van die beplande toepassing. Die probleemstelling behoort die ontwerpers se aandag op die probleem te vestig sonder om inligting in volgende stappe te dupliseer.

Byvoorbeeld : Onderneming XYZ ontwikkel groot programmatuurstelsels. Dienste word gelewer aan verskillende kliënte wie se besigheid van sensitiewe aard is. Ontwerps en ander data moet geheim gehou word, maar as gevolg van hoë frekwensie van kontak tussen XYZ en kliënte, is kommunikasie met behulp van netwerke noodsaaklik.

Kommunikasie bestaan uit kontrakte, ontwerpspesifikasies, voltooide ontwerpe en rekeninge. Beide partye moet ontvangs van boodskappe en transaksies erken. XYZ werknemers werk soms met terminale wat aan die onderneming se hoofrekenaar gekoppel is deur middel van modems en publieke telefoonnetwerke.

- Definieer sekerheidsbuitelyne.
  'n Belangrike beginpunt is om die domein of omvang van die sekerheidsdienste te identifiseer.

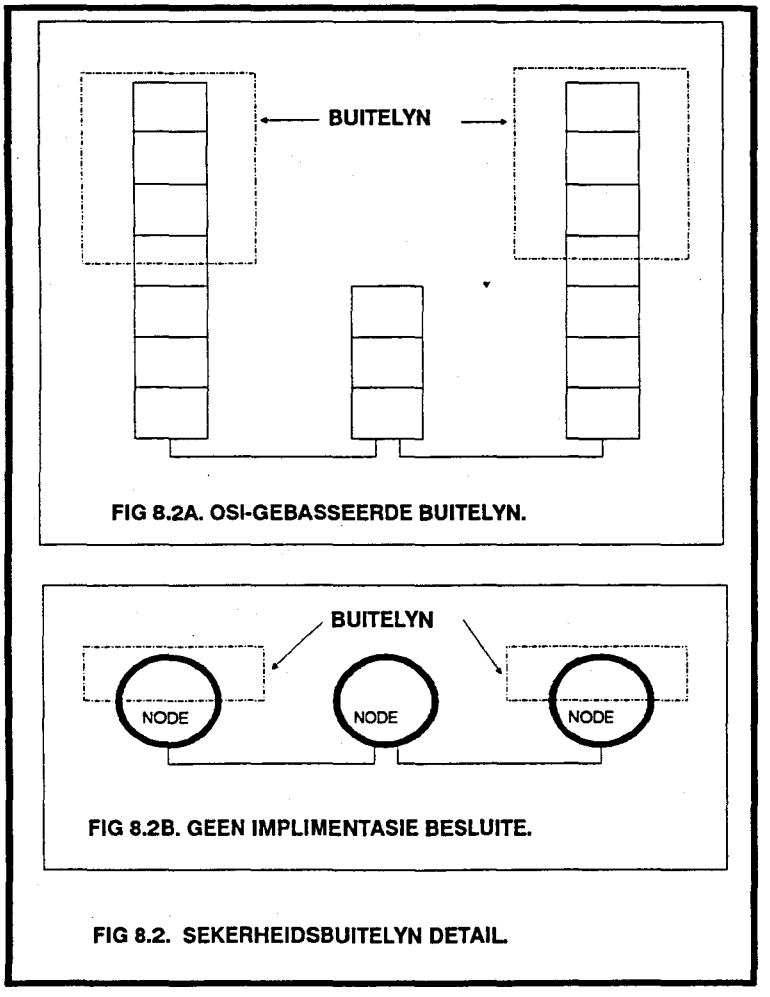


FIG 8.2A. OSI-GEBASSEERDE BUITELYN.

FIG 8.2B. GEEN IMPLIMENTASIE BESLUITE.

FIG 8.2. SEKERHEIDSBUITELYN DETAIL.

'n Sekerheidsbuitelyn is 'n logiesegrens wat om 'n gebied getrek word wat betroubaar moet wees. Dit is areas waarin sekerheidsdienste nie voorkom nie, en sekerheid word verskaf met behulp van betroubare personeel en stelsels. Die dele van die netwerk buite die sekerheidsbuitelyne moet beskerm word deur sekerheidsdienste. Die grense stem ooreen met die sekerheidsbuitelyne wat in hoofstuk 2 bespreek is.[8]

Aandag moet gegee word aan die detail waarmee die buitelyne bespreek word. Te veel detail veroorsaak 'n implimentasiegeoriënteerde benadering. Byvoorbeeld in fig 8.2a, word aangedui dat die sekerheidsbuitelyn een van die OSI-vlakke sny. Daar word reeds implimentasie besluite aangedui naamlik dat die OSI-argitektuur gebruik word, en dat die buitelyn deur vlak 4 loop. Figuur 8.2b dui geen implimentasie detail aan nie en is dus die gewenste vlak van detail.

- Definieer nodige sekerheidsdienste.
  Hier word aandag geskenk aan die uiteensetting van die nodige sekerheidsdienste. Die inligting behoort in terme van die toepassingsvereistes gestel te word en nie in terme van enige sekerheidsmeganismes of protokolle nie.

  Die sekerheidsdienste wat hier van toepassing is, is dieselfde wat reeds in hoofstuk 2 gelys en bespreek is.Vir verdere doeleindes word verwys TABEL 2.1 in hoofstuk 2.

- Definieer nodige sekerheidsbestuurskenmerke.
  Die stap bestaan uit die beskrywing van die vereistes vir die bestuur van netwerk sekerheid. Voorbeelde is, of sekere dienste onderhandelbaar is of nie en watter kombinasies van dienste is moontlik. So kan daar beide DES- en RSA-enkripsie algoritmes vir enkripsie beskikbaar wees. Daar moet besluit word of dit wel moontlik sal wees om te kies watter een van die twee metodes gebruik sal word en of die metode vasgestel sal wees.

Identifiseer beperkings op ontwerp.

Beperkings is faktore wat die ontwerpers se opsies beperk, maar nie deur die probleem self veroorsaak word nie.

- Hersien toepaslike standaarde.
  Hier moet bepaal word of daar enige standaarde bestaan waaraan voldoen behoort te word. Indien wel, moet die standaarde bestudeer word en indien meer as een bestaan, moet daar 'n keuse gemaak word.

Dit mag soms nodig wees om standaarde aan te pas vir die spesifieke toepassing. Belangrike standaarde wat in aanmerking geneem kan word is onder andere die volgende :

- INTERNATIONAL STANDARDS ORGANISATION(ISO),[9][34][61][Hoofstuk 2]
- INTERNATIONAL CONSULTATIVE COMMITTEE FOR TELEPHONE AND TELEGRAPH(CCITT), Die CCITT is 'n lid van die Internasionale Telekommunikasie Unie (ITU). CCITT doen aanbevelings vir telekommunikasie- en datakommunikasienetwerke.[34]
- NATIONAL BUREAU OF STANDARDS(NBS), Die NBS behoort aan verskillende internasionale organisasies en spesialiseer veral in die implimentasie van die boonste vlakke van die OSI-standaarde.[34]
- DATA ENCRYPTION STANDARD(DES),[Hst 5]
- AMERICAN NATIONAL STANDARDS INSTITUTE(ANSI). Dit is 'n koördinerings agentskap vir standaarde wat vrywillig in die V.S.A. gebruik word. ANSI is lid van die ISO maar pas ISO-standaarde aan om by Noord-Amerikaanse omstandighede aan te pas.[34]

- Bepaal netwerktipe en topologie.
  Spesifieke tipes nètwerke en netwerktopologië kan die implimentasie keuse beperk. Dit is byvoorbeeld onmoontlik om die identiteit van die ontvanger te waarmerk voor kommunikasie begin, as van 'n skakellose netwerk gebuik gemaak word.

- Oorweeg organisatoriese faktore.
  Die faktore wat hier van belang is, is die beperkings wat deur die bepaalde organisasie opgestel word. Voorbeelde hier is beperkings in fondse en vasgestelde implimentasie datums.

8.2.2. ONTWERPFASE.

Tydens die ontwerpfase word 'n oplossing ontwikkel wat die spesifikasies van die spesifikasiefase bevredig.

- Definieer sekerheidsargitektuur.
  In die fase word die oorhoofse sekerheidsargitektuur gedefinieer. Baie bestaande implimentasies is gebaseer op die OSI-Verwysingsmodel, maar daar bestaan ook ander opsies onder andere :
  - "National Computer Security Center" of NCSEC.[129]
  - "Trusted Network Security Evaluation Criteria" of TNSEC.[129]

Die benadering wat vir die metodologie gevolg is, is die OSI-benadering.

- Plasing van funksionaliteit binne argitektuur.
  Hier word aandag gegee aan die plasing van die funksies in die gekose argitektuur. In die geval van die OSI-Argitektuur is die plasing van die sekerheidsfunksies in spesifieke vlakke 'n kontroversiële aspek soos reeds in hoofstuk 2 bespreek. Hier moet deeglik aandag gegee word aan tegniese sowel as funksionele en praktiese aspekte.

- Definieer sekerheidsprimitiewe.
  Die definisie van die sekerheidsprimitiewe is van uiters groot belang aangesien die primitiewes die koppelvlakke tussen die gebruiker en die toepassing sowel as die parameters tussen die vlakke beskryf.

- Kies onderliggende sekerheidsmeganismes.
  Hier moet die onderliggende meganismes gekies word waarmee die sekerheidsdienste geïmplimenteer gaan word. Hier moet duidelik onderskei word tussen onderliggende meganismes en protokolle. 'n Meganisme is 'n basiese tegnologie of algoritme, terwyl 'n protokol 'n end-tot-end operasie is wat een of meer meganisme gebruik om 'n diens mee te implimenteer.

  Die meganismes behoort gekies te word na aanleiding van die dienste benodig sowel as die beperkings en prestasie faktore.

- Definieer diensprotokolle.
  In die volgende stap word die diensprotokolle wat die verskillende diensmeganismes saamvoeg om 'n bepaalde diens te lewer ontwikkel. Net soos met die diensmeganismes, word protokolle gekies op grond van die dienste benodig sowel as die beperkings en prestasiefaktore. 'n Belangrike aspek wat hier aandag moet geniet is dat 'n bepaalde protokol nie die sekerheid van die onderliggende meganismes moet ondermyn nie.

  'n Diensprotokol word hier beskou as enige end-tot-end aksie wat help om 'n sekerheidsdiens te implimenteer. So kan sleutelverspreiding byvoorbeeld deur drie verskillende protokolle verrig word. Naamlik:
  - Sleuteluitruilingsprotokol deur netwerk self.
  - Sleutels word versprei deur gebruik te maak van geregistreerde pos.
  - Sleutels word versprei deur 'n koerier wat die sleutels per hand aflewer.

Al drie die metodes kan gesamentlik gebruik word om sleuteverspreiding te beskerm. Daar kan tussen die verskillende metodes gerotteer word om die sleutels te versprei. Die oortolligheid verbeter die beskerming van die sleutels aangesien die indringer nie sal weet watter protokol op 'n bepaalde tydstip in gebruik is nie. Dus sal hy al die protokolle moet monitor om te verseker dat hy die sleutels kan onderskep.[129]

8.2.3. IMPLIMENTASIEFASE.

Die implimentasiefase se doel is om die ontwerp in die vorige fase om te skakel na 'n praktiese toepassing. Die artikel wat bestudeer is skenk slegs aandag aan die spesifikasie- en ontwerpfases. In die implimentasiefase word slegs die hoofpunte sonder 'n verdere beskrywing gegee. Die skrywer sal wel sy siening oor die punte gee.

- Ontwikkel benodigde apparatuur en programmatuur.
  In hierdie stap sal aandag gegee word aan die fisiese ontwikkeling en implimentasie van die stelsel of toepassing. Die ontwikkeling kan bestaan uit beide apparatuur en programmatuur.

- Toetsing en verifikasie.
  Die toetsing en verifikasie van die netwerkgebasseerdetoepassing is een van die belangrikste stappe van die hele metodologie. Geen stelsel kan met die eerste probeerslag suksesvol wees nie. Dit is dus noodsaaklik dat 'n deeglike toetsing en verifikasieprosedure as deel van die metodologie ontwikkel moet word.

- Herhaal Ontwerpfase indien nodig.
  Indien die toepassing nie volgens plan presteer nie, kan die hele proses vanaf die ontwerpfase herhaal word.

8.3. KRITIEK OP DIE VOORAFGAANDE METODOLOGIE.

Die belangrikste kritiek wat teen die metodologie gelewer kan word, ontstaan uit die feit dat die metodologie vanuit 'n ingenieurs- en sagtewareontwikkelingsoogpunt ontwikkel is. Die metodologie behoort uitstekend te wees vir ontwikkeling van programmatuur en klein tot gemiddeldegrote stelsels. Na bestudering van die metodologie raak dit egter duidelik dat daar verskeie belangrike aspekte is wat glad nie in aanmerking geneem is nie.

Netwerksekerheid op sy eie is reeds 'n uiters komplekse probleem en bestaan ook nie geïsoleerd binne 'n bepaalde onderneming of binne 'n bepaalde toepassing nie. Netwerksekerheid word sterk beïnvloed deur algemene rekenaarsekerheid en word soms as 'n onderafdeling van rekenaarsekerheid gesien. Die belangrike punt hier is nie watter van die twee velde die ander insluit nie, maar wel die feit dat die een die ander uiters sterk beïnvloed. Die voorafgaande metodologie neem glad nie algemene rekenaarsekerheid in ag nie.

'n Verdere probleem met die metodologie is die feit dat dit nie voorsiening maak vir die ontwikkeling van 'n sekerheidsstrategie of sekerheidsbeleid nie. Soos reeds in afdeling 8.1. genoem is dit uiters belangrik dat 'n metodologie 'n sekerheidsbeleid of strategie insluit.

'n Probleem wat aansluit by die vorige punt is die betrokkenheid van die bestuur en veral die senior- of topbestuur van die onderneming. Die metodologie maak geen melding van waar die bestuur by die hele metodologie inpas nie.

Die metodologie het egter nie net swakpunte nie. Daar is verskeie punte in die metodologie wat baie belangrik is en in baie gevalle nie genoeg aandag kry nie. So is die gebruik van sekerheidsbuitelyne, netwerktipe en netwerktopologië belangrike punte wat wel in die metodologie voorkom.

8.4. RS-METODOLOGIE.

Die Rekenaarsekerheidsmetodologie (RS-Metodologie) is ontwikkel aan die Randse Afrikaanse Universiteit deur Prof J.H.P. Eloff en K.P. Badenhorst. Die doel van die RS-Metodologie is om 'n gestruktureerde benadering vir die spesifikasie van rekenaarsekerheid en die toepassing van 'n rekenaarsekerheidsbeleid binne 'n onderneming daar te stel.

Vir volledige besprekings van die RS-metodologie kan die volgende bronne geraadpleeg word.[121][125][128]

Volgens Badenhorst [121], word die RS-Metodologie gedefinieer as 'n gestruktureerde benadering met die doel om eerstens die oorhoofste, totale implimentering van rekenaarsekerheid in die algemeen te handteer, verwys na as **tegnologieserekenaarsekerheid**; en tweedens om rekenaarsekerheid in toepassingsgeoriënteerde programmatuursteisels te bespreek, i.e. **toepassingsrekenaarsekerheid**.

Die metodologie bestaan uit duidelik identifiseerbare fases, take en stappe wat in 'n voorafbepaalde volgorde gerangskik is. Verder kom die lewenssiklus van rekenaarsekerheid binne 'n onderneming se fases ooreen met die fases van die gewone programmatuurontwikkelingslewenssiklus. Die hoof fases van die RS-Metodologie word voorgestel in Fig 8.3.

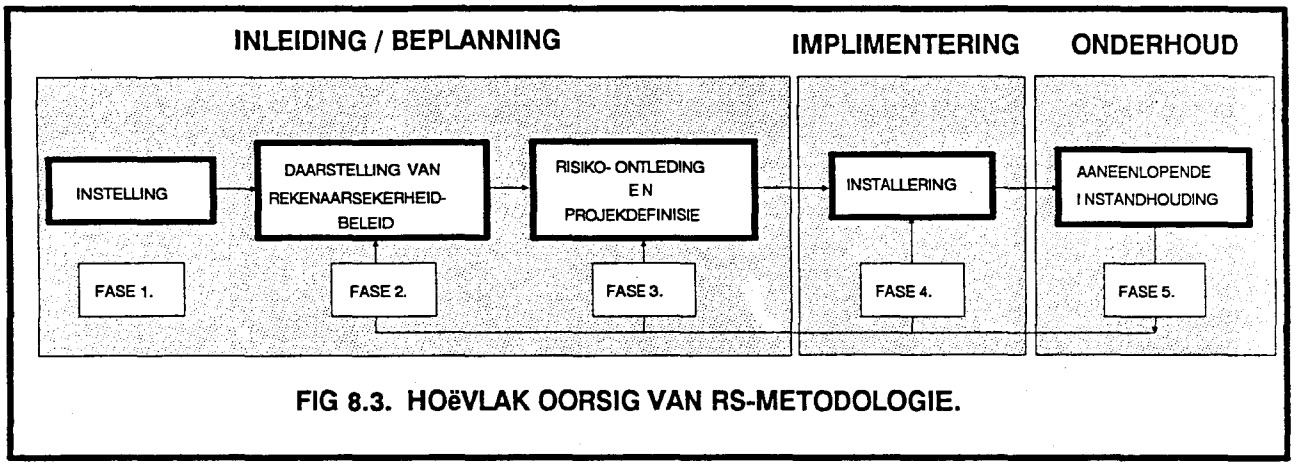


FIG 8.3. HOëVLAK OORSIG VAN RS-METODOLOGIE.

Die drie hooffases, naamlik : Inleiding/Beplanning, Implimentering en Onderhoud, stem ooreen met die meeste programmatuur- en stelselontwikkelingsmetodologië

8.4.1. INLEIDING / BEPLANNING.

8.4.1.1. Fase 1 : Instelling.

In hierdie fase moet aandag gegee word aan die top- of seniorbestuur van die onderneming se sekerheidsbewustheid. Die belangrikste doel van die fase is die skep van 'n oorhoofse klimaat vir rekanaarsekerheid binne die onderneming deur middel van sekerheidsbewustheidssessies.

Verder moet daar 'n mandaat vir die ontwikkeling van 'n sekerheidsstrategie opgestel word. Verder is dit nodig om 'n rekenaarsekerheidsloodskomitee te skep om die strategie te ontwikkel. Die strategie moet dan deur die topbestuur van die onderneming goedgekeur word. FIG 8.4. dui die verskillende take wat in fase 1 voorkom aan.

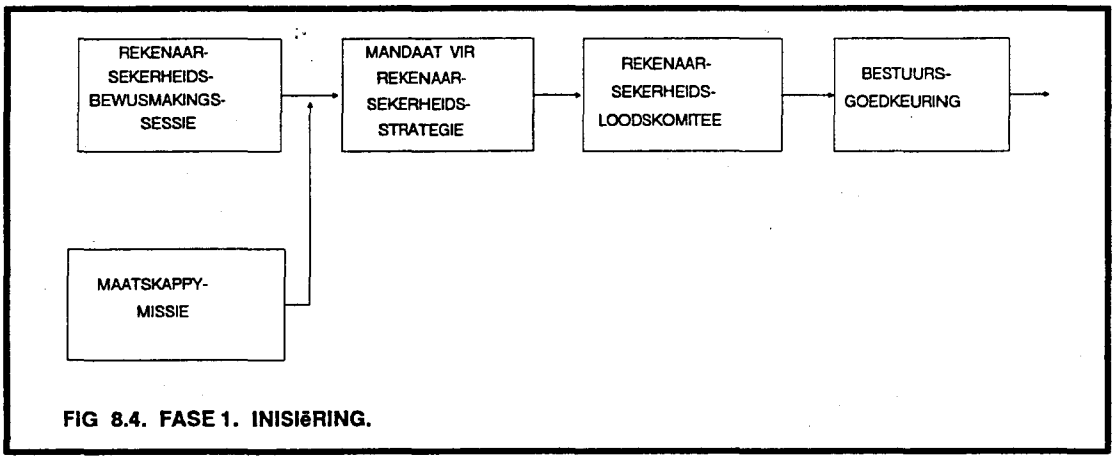


FIG 8.4. FASE 1. INISIëRING.

8.4.1.2. Fase 2 : Rekenaarsekerheidsbeleid.

Dit is 'n belangrike saak vir enige onderneming om 'n rekenaarsekerheidsbeleid op te stel wat die topbestuur van die onderneming betrek en beide tegnologiese- en toepassingsrekenaarsekerheid insluit. Verantwoordelikhede moet so duidelik as moontlik uiteengesit word sodat alle werknemers presies weet wat die maatreëls is. Figuur 8.5. dui die verskillende take in fase 2 aan.

Die volgende aktiwiteite behoort uitgevoer te word tydens die opstelling van die rekenaarsekerheidsbeleid :

- Samestelling van 'n stel gemeenskaplike rekenaarsekerheidsterme vir gebruik deur onderneming.
- Beskryf kortliks die doel van rekenaarsekerheid.
- Definieer die omvang van rekenaarsekerheid.
- Definieer verantwoordelikhede van alle betrokke partye.

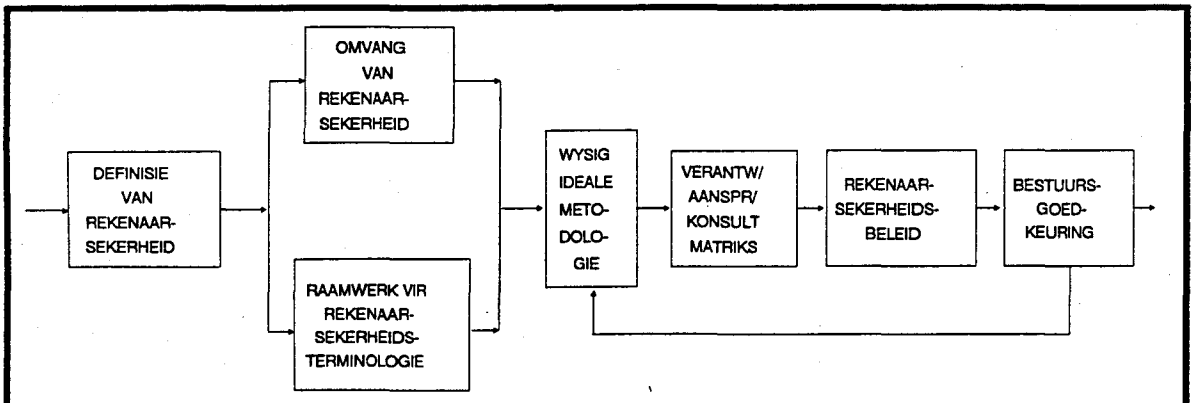


FIG 8.5. DAARSTELLING VAN REKENAARSEKERHEIDSBELEID.

Areas wat van belang is tydens die installeringsfase is die volgende.

- Fisiese toegangsbeheer.
- Gebeurlikheidsbeplanning.
- Rekenaarpersoneel.
- Logiesetoegangsbeheer.
- Kommunikasienetwerke en kriptografie. Die afdeling sal dus ook Netwerksekerheid insluit wat veral by die uitbreiding van die metodologie aandag sal geniet.
- Aantekeningsfasiliteite.

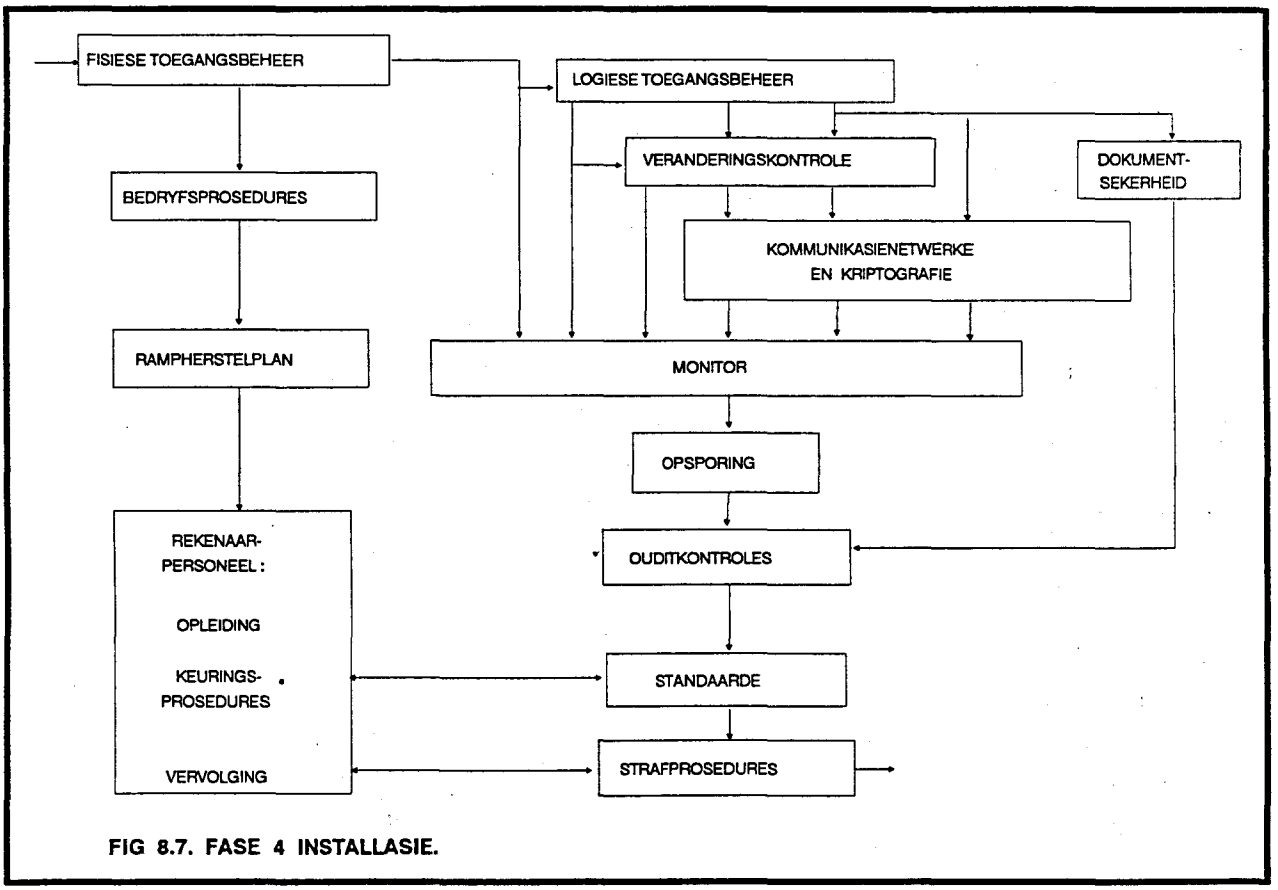


FIG 8.7. FASE 4 INSTALLASIE.

8.4.3. FASE 5. : ONDERHOUD.

Figuur 8.8. dui die belangrikste take van fase 5 aan.

Fase 5 maak voorsiening vir aaneenlopende onderhoud en die verskillende take kan in drie hoof doelwitte verdeel word. Eerstens alle maatreëls ten opsigte van toepassingsrekenaarsekerheid. Tweedens word hier aandag gegee aan voortgaande aktiwiteite soos onderhoudprosedures, ouditfunksies ensovoorts. Laastens die hersiening van die projekplan en gereelde statusverslae aan die top- of seniorbestuur.

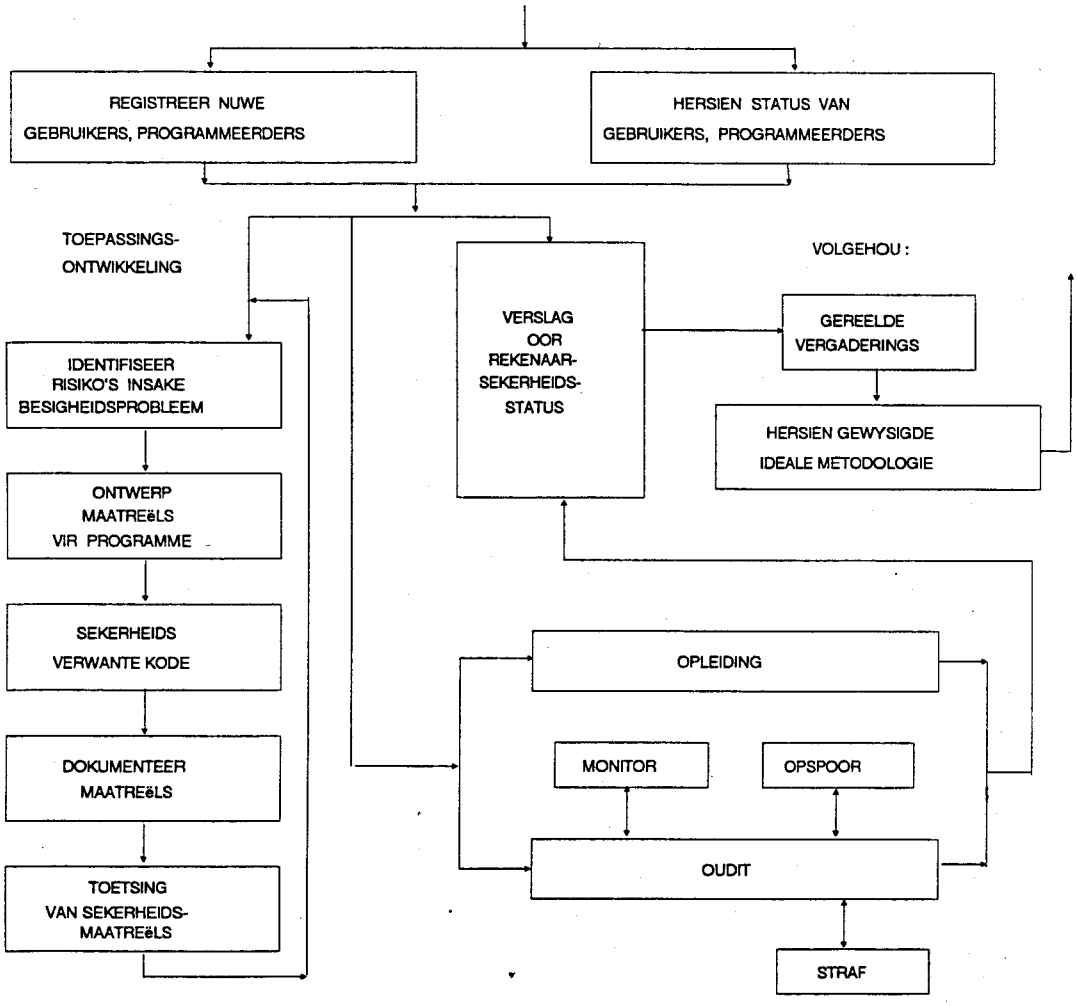


FIG 8.8. ONDERHOUD.

8.5. UITBREIDING VAN RS-METODOLOGIE.

Die RS-Metodologie is 'n baie meer omvangryke metodologie as die metodologie bespreek in afdeling 8.3. Die meeste van die nadele van die metodologie word wel in die RS-Metodologie aangespreek. Daar is wel ook tekortkominge aan die metodologie. Die belangrikste is die gebrek aan aandag aan netwerk- en kommunikasiesekerheid.

Die res van die afdeling sal poog om die RS-metodologie verder uit te brei om wel netwerk- en kommunikasiesekerheid in aanmerking te neem. Die doel is nie hier om die hele RS-Metodologie weer oor te bespreek nie. Daar sal slegs aandag gegee word aan die dele van die metodologie wat verander of uitgebrei sal word. In figure 8.9. tot 8.13. word die punte wat uitgebrei word aangedui deur die donker geskakeerde blokke.

8.5.1. INLEIDING/BEPLANNING.

8.5.1.1. FASE 1. : INSTELLING.

FIG 8.9. is 'n herhaling van FIG 8.4. Take wat uitgebrei word, word met donker blokke aangedui.

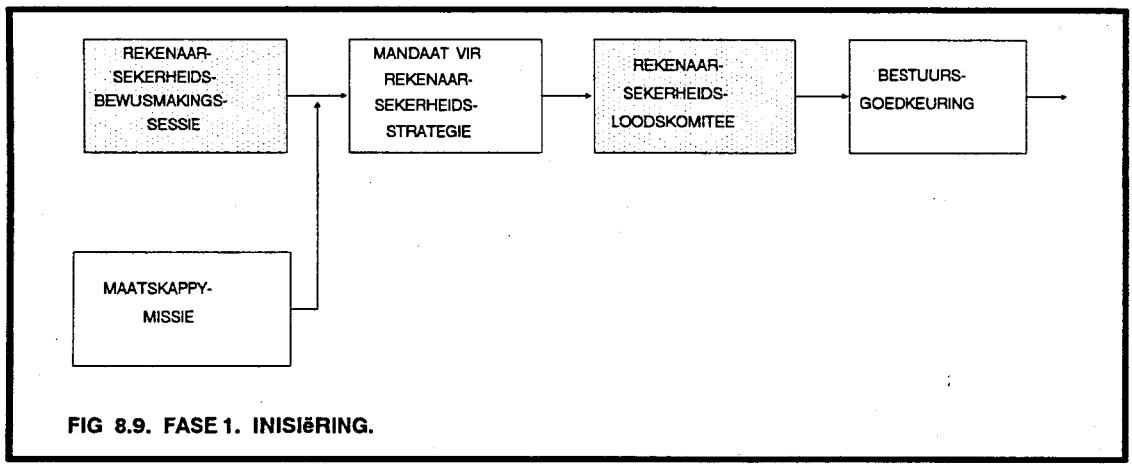


FIG 8.9. FASE 1. INISIëRING.

Die belangrikste uitbreidings wat hier gemaak sal word is om personeel en kliënte te betrek by die beplanning van die sekerheidsmetodologie.

In die eerste plek is dit belangrik dat die bestuur van die onderneming besef dat die die netwerk- en kommunikasiesekerheidsmaatreëls ook 'n groot invloed buite die onderneming sal hê. Afhangende van die aard van die onderneming, sal persone en ondernemings buite die onderneming self ook in 'n mate hier betrek moet word. 'n Bankinstelling sal byvoorbeeld deeglik moet bepaal watter maatreëls vir die publiek aanvaarbaar sal wees. In hoofstuk 5 waar identifikasiemetodes bespreek is, is reeds aangedui hoe belangrik gebruikeraanvaarding is. Verder sal bewus-makingsprogramme ook buite die onderneming aangepak moet word om die publiek die nodige inligting in verband met die maatreëls te gee.

Gebruikersvriendelikheid by intydse stelsels, byvoorbeeld ATMs, is krities belangrik en is omgekeerd eweredig aan netwerksekerheid. Dit kan gebeur dat 'n onderneming, byvoorbeeld 'n bankinstelling, 'n baie hoë graad van netwerksekerheid implimenteer. Die gebruik van die dienste vanuit 'n gebruikersoogpunt kan egter te moeilik wees.

Dit sal uiters moeilik wees om te bepaal wat genoeg en wat te min inligting is, veral as inligting aan die publiek verskaf moet word. Dit is belangrik dat die Sekerheidsloodskomitee ook personeel van die netwerk- en kommunikasieafdelings insluit.

Vir personeel buite die afdelings sal dit soms moeilik wees om te verstaan waarom sekere maatreëls nodig is. Selfs die bestuur, wat die loodskommitee se aanbevelings moet goedkeur, sal goed ingelig moet van veral die netwerk- en kommunikasiesekerheidsaspekte.

In hierdie fase moet aandag gegee word aan die top- of seniorbestuur van die onderneming se sekerheidsbewustheid. Die belangrikste doel van die fase is die skep van 'n oorhoofse klimaat vir rekenaarsekerheid binne die onderneming deur middel van sekerheidsbewustheidssessies.

8.5.1.2. FASE 2. : REKENAARSEKERHEIDSBELEID.

In figuur 8.10 dui die donker blokke die uitbreidings aan wat aan figuur 8.5. aangebring is.

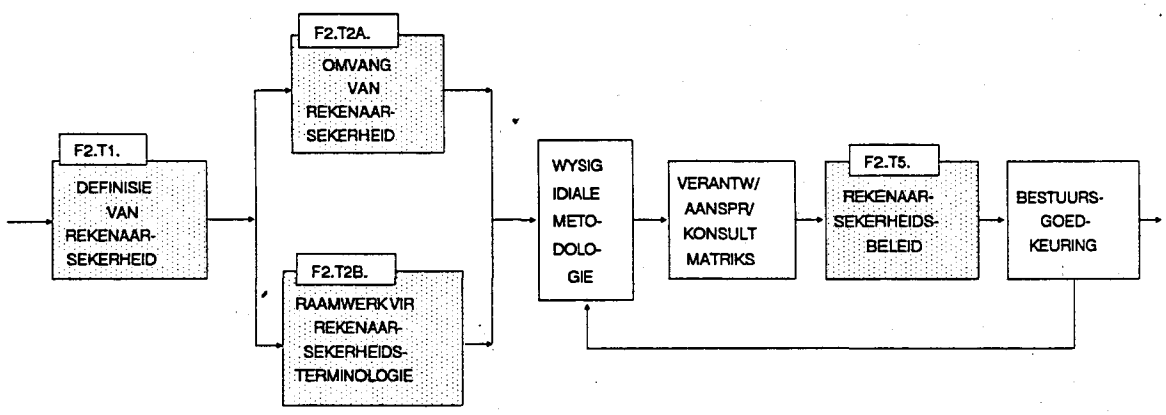


FIG 8.10. FASE 2. DAARSTELLING VAN REKENAARSEKERHEIDSBELEID.

Die uitbreidings wat aan hierdie fase gedoen moet word is om netwerksekerheid by die verskillende take in die fase by te werk.

Die volgende take behoort spesiale aandag te geniet :

DEFINISIE VAN REKENAARSEKERHEID (F2.T1):

Die definisie van rekenaarsekerheid sal uitgebrei moet word sodat dit ook netwerksekerheid sal insluit . Die definisie sal dan as volg daar uitsien :

REKENAARSEKERHEID kan opgedeel word in twee duidelike dele naamlik tegnologieserekenaarsekerheid en toepassingsrekenaarsekerheid.

- **TEGNOLOGIESEREKENAARSEKERHEID** bestaan weer uit logiese- en fisiesesekerheid.
  - **LOGIESESEKERHEID** beskerm die data ,inligting en programmatuur wat in enige deel van die netwerk of losstaande rekenaars voorkom. Dit sluit aksies in soos die voorkoming van weerhouding van toegang tot 'n program deur 'n ongemagtigde gebruiker en ongemagtigde vrystelling van inligting of data. Verder sluit logiese aspekte ook in datakommunikasieaspekte, soos beskerming van die integriteit, weerhouding en ongemagtigde verandering van die inligting tydens transmissie.

    Logiese sekerheid beheer ook die toegang tot en tussen verskillende programme. Dit sluit in programme wat in geheel op een enkele terminaal of rekenaar uitgevoer word sowel as verspreide programme waar dele van 'n program tussen verskillende rekenaars of terminale versprei is.

  - **FISIESESEKERHEID** is die aksies wat fisiese beskadiging of binnedringing van die apparatuur hulpbronne van 'n rekenaar of die netwerk verhoed. Die apparatuur hulpbronne kan byvoorbeeld losstaande rekenaars, kabels, terminale en drukkers wees.

- **TOEPASSINGSREKENAARSEKERHEID** hanteer die ontwerp, implimentasie en onderhoud van sekerheid binne 'n bepaalde toepassing. Hier word aandag gegee aan sekerheidsmaatreëls wat nie deur die netwerk of res van die onderneming se sekerheidsmaatreëls voorsien word nie. Die maatreëls word dan direk in die bepaalde toepassing geïmplimenteer.

OMVANG VAN REKENAARSEKERHEID (F2.T2A).

Die beskrywing van die omvang van rekenaarsekerheid sal uitgebrei moet word om ook netwerksekerheid in te sluit. Hier kan byvoorbeeld 'n lys opgestel word van al die toerusting, programmatuur, data en inligting wat beskerm moet word. Die lys moet dan spesifiek verwys na netwerkapparatuur en programmatuur soos byvoorbeeld modems en kommunikasieverbindings.

RAAMWERK VIR REKENAARSEKERHEIDSTERMINOLOGIE (F2.T2B):

Die Raamwerk van rekenaarsekerheidsterminologie is nodig om te verseker dat personeel van die onderneming eenvormige terminologie gebruik. Die raamwerk sal uitgebrei moet word om ook die terminologie van netwerke en netweksekerheid in te sluit.

Die volgende is netwerksekerheidsspesifieke terme wat in die raamwerk opgeneem behoort te word:

- Wat is 'n netwerk?
- Integriteit.
- Toegangsbeheer.
- Enkripsie.
- Sleutelbestuur.
- Protokol.

Sommige van die terme sal nie spesifiek sekerheidsterme wees nie, maar ook algemene rekenaarterme wat nodig sal wees om sekerheidsterme meer duidelik te maak. So byvoorbeeld sal die definisies van modems, bruê, en roeteerders ook in die raamwerk opgeneem moet word.

REKENAARSEKERHEIDSBELEID (F2.T5):

Netwerksekerheid maak nou 'n baie groot en belangrike deel van die onderneming se algemene rekenaarsekerheidsomgewing uit. By die opstelling van die rekenaarsekerheidsbeleid sal die opstellers moet verseker dat daar by die beleidstelling genoeg aandag gegee word aan veral netwerke en netwerksekerheid.

'n Ideale rekenaarsekerheidsbeleid volgens die RS-Metodologie behoort die volgende in te sluit.

- Beskrywing van die doel van rekenaarsekerheid binne die onderneming.
  Dit is belangrik dat daar in baie duidelike terme bepaal word wat die onderneming se doel is met rekenaarsekerheid. Dit sal help verseker dat die werknemers van die onderneming ook deeglik sal verstaan en begryp waarom die beplande maatreëls nodig is.

Daar moet ook verseker word dat netwerksekerheid genoeg aandag in die beskrywing ontvang.

- Verantwoordelikheid van verskillende betrokke partye.
  Al die partye wat betrokke is by rekenaarsekerheid binne die onderneming moet duidelik geïdentifiseer word, en elk se verantwoordelikheid moet duidelik gespesifiseer word. Dit sal verseker dat elk van die partye presies sal weet waar hy in die sekerheidsmaatreëls inpas.

8.5.1.3. FASE 3.: RISIKO-ONTLEDING EN PROJEKDEFINISIE.

Die gebruik van netwerke en datakommunikasie binne en buite die onderneming sal 'n groot invloed hê op die risiko-ontleding van die onderneming. Risiko-ontleding val buite die studieveld wat in die verhandeling gedek word. Daar sal egter 'n kort bespreking gegee word van die bydrae wat die gebruik van netwerke in die onderneming het op die risiko in die onderneming. Taak F3.T7. handel oor die implimentasiekosteontleding en sal ook hier kortliks bespreek word.

Netwerke beskik oor spesiale kenmerke wat veroorsaak dat sekerheid op spesiale maniere beïnvloed en wat dus die risiko in die onderneming verhoog.'n Beknopte opsomming volg.[7][10][11]

- Deling van hulpbronne veroorsaak dat baie gebruikers potensieel toegang kan verkry op plekke waar toegang nie wenslik is nie. Dus is spesiale maatreëls nodig.
- Stelsel is baie kompleks en sekerheidsmaatreëls moet dus ook kompleks wees.
- Netwerke kan ook aan mekaar gekoppel word en dit is moelik om te bepaal wat die invloed van sekerheid van een netwerk op ander sal hê.
- Op 'n netwerk is daar baie punte wat aangeval kan word, byvoorbeeld nodes en skakels.
- Daar kan baie roetes van een gasheer na 'n ander wees en elke roete lewer addisionele probleme op.
- As gevolg van die toenemende gebruik van netwerke om afstandstoegang tot rekenaarfasiliteite te gebruik, is dit vir indringers 'n makliker en aantrekliker teiken.
- Die hoeveelheid en waarde van die inligting wat verkry kan word as 'n netwerk binnegedring kan word, neem ook toe.
- Ontwikkeling van netwerktegnologie maak sekere aanvalle moontlik, bv monitor van radio- en satelietverbindings.

IMPLIMENTASIEKOSTEANALISE.(F3.T7.)

In figuur 8.11. word die taak F3.T7. deur die donker blok aangedui.

Rekenaarsekerheidsmaatreëls kan geklassifiseer word as 'n bokoste van die normale rekenaarstelsel aangesien dit gewoonlik die reaksietyd en prestasie van die stelsel nadelig beïnvloed.[131] Die koste verbonde aan die implimentasie van sekerheidsmaatreëls sluit nie slegs direkte koste soos ontwikkeling, implimentasie en onderhoud in nie, maar ook indirekte kostes soos rekenaarhulpbronne en rekenaartyd.

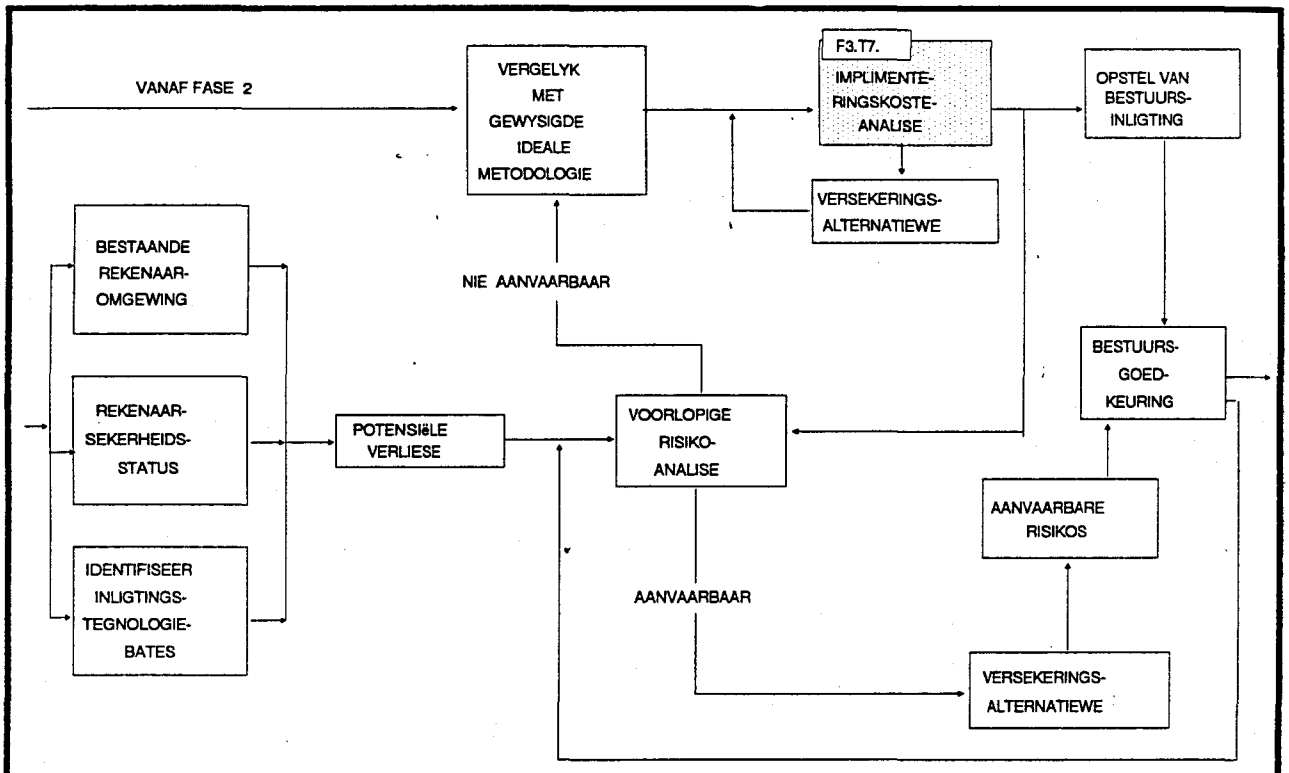


FIG 8.11. FASE 3 . RISIKOANALISE EN PROJEKDEFINISIE.

Netwerksekerheidsmaatreëls sal 'n baie groot deel van die totale implimentasiekoste van enige sekerheidsmaatreëls in 'n onderneming uitmaak. Om dus 'n deeglike kosteanalise te maak, sal hier reeds aandag geskenk moet word aan besluite wat in F4.T4. geneem sal word met betrekking tot die beplanning van netwerksekerheid. Die keuse van 'n bepaalde sekerheidsstandaard en ook die keuse van sekerheidsdienste sal 'n baie groot invloed op die implimentasiekoste uitoefen.

8.5.2. FASE 4. : INSTALLASIE.

Figuur 8.12. dui die take in die donker blokke wat verder uitgebrei. Fase 4 is die fase wat die meeste beïnvloed word deur die uitbreiding van die metodologie. Die volgende areas word geraak by die uitbreiding :

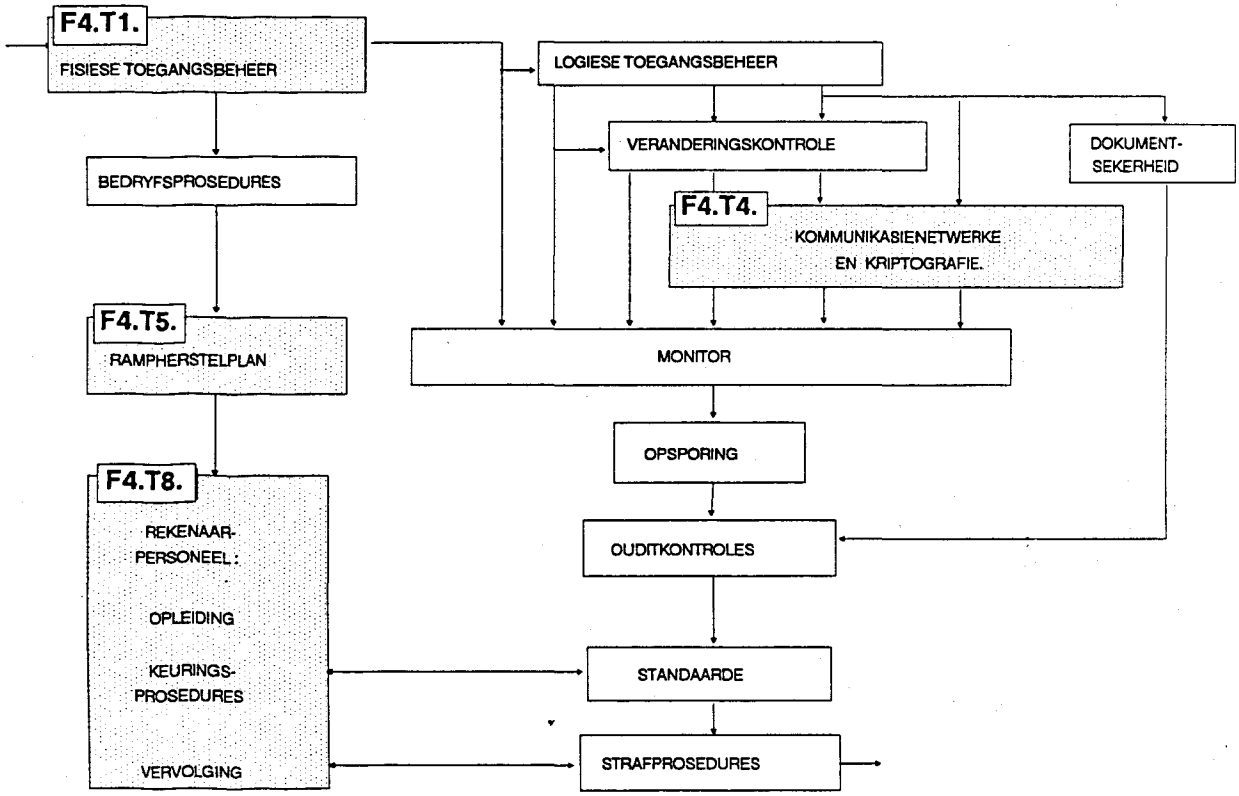


FIG 8.12. FASE 4 INSTALLASIE.

8.5.2.1. FISIESE TOEGANGSBEHEER. (F4.T1.)

Fisiese toegangsbeheer tot terminale en kommunikasietoerusting word nou baie belangrik. Die toerusting kom in baie gevalle op onbeskermde plekke buite die onderneming voor. 'n Voorbeeld hier is die ATMs van bankinstellings wat in publieke areas geïnstalleer word. Meer aandag sal gegee moet word aan die beskerming van die toerusting. Dit is feitlik onmoontlik om die toerusting fisies te beskerm deur dit toe te sluit, of om 24 uur per dag sekuriteitswagte by die toerusting te plaas.

8.5.2.2. RAMPHERSTEL (F4.T5)

RAMPHERSTEL moet voorsiening maak vir addisionele aspekte rakende rekenaarkommunikasie. As gevolg van die hoë vlak van hulpbrondeling, wat een van die hoof kenmerke van die gebruik van netwerke is, verhoog die moontlikheid van vernieteging of beskadiging van hierdie hulpbronne. Dit veroorsaak 'n behoefte en die toenemende belangrikheid van goed ontwikkelde rampherstelprosedures, veral by intergeskakelde netwerke.

Van die belangrikste probleme wat hier kan opduik is die verbreking van kommunikasie tussen twee punte. Voorbeeld van so 'n onderbreking is die fisiese beskadiging van die telefoonlyn tussen twee terminale. Daar moet dus reëlings getref word vir alternatiewe kommunikasieverbindings. Die potensiële skade wat aangerig kan word aan die data binne 'n onderneming is nou baie groter.

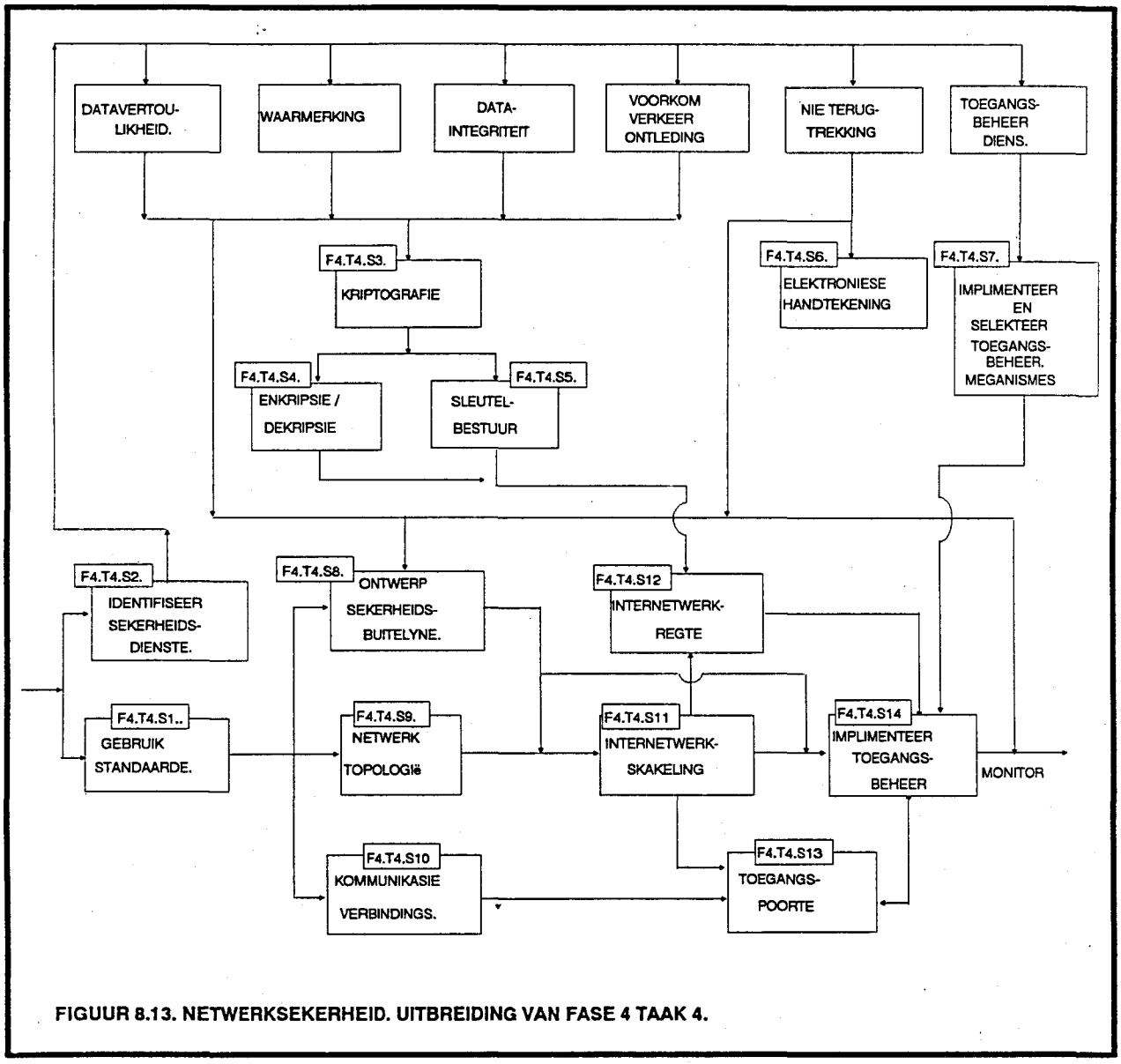
8.5.2.3. PERSONEEL. (F4.T8)

'n Baie belangrike aspek van netwerksekerheid wat in baie gevalle geïgnoreer word is die behoorlike opleiding van rekenaar- en ander personeel binne die onderneming Personeel sal nou ook verdere opleiding moet ontvang, nie net in sekerheidsaspekte nie, maar ook in algemene netwerk en kommunikasie aspekte. So sal selfs sekretaresses en tiksters deeglik bewus moet wees van netwerksekerheidsmaatreëls, soos die gebruik van modems en beskerming van wagwoorde en sleutelbestuursprosedures aangesien die rekenaars waarop hulle werk ook aan die netwerk gekoppel kan wees.

8.5.2.4. KOMMUNIKASIENETWERKE EN KRIPTOGRAFIE.

Daar bestaan verskeie sekerheidsmaatreëls wat net op kommunikasienetwerke van toepassing is. Die maatreëls verg spesiale beplanning en implimentasie en word aangedui in figuur 8.13. Die meeste van die maatreëls is reeds in vorige hoofstukke van hierdie verhandeling bespreek. Daar sal dus hier net 'n oorsigtelike bepreking wees, en dan terugverwys word na die relevante hoofstukke.

Slegs die stappe in figuur 8.13. wat genommer is sal bespreek word. Ongenommerde stappe word as deel van die voorafgaande genommerde stap bespreek.



FIGUUR 8.13. NETWERKSEKERHEID. UITBREIDING VAN FASE 4 TAAK 4.

Identifisering en gebruik van standaarde. F4.T4.S1.

In stap een moet daar besluit word watter standaarde gevolg gaan word vir die implimentering van netwerksekerheid in die onderneming. Daar bestaan verskeie organisasies wat standaarde opstel vir kommunikasienetwerke en ook vir sekerheid. Voorbeelde van sulke organisasies is.

- INTERNATIONAL STANDARDS ORGANISATION(ISO),[9][34][61][Hoofstuk 2] Wat die OSI-model en sekerheidsbylaag opgestel het.
- INTERNATIONAL CONSULTATIVE COMMITTEE FOR TELEPHONE AND TELEGRAPH(CCITT), Die CCITT is 'n lid van die Internasionale

- Telekommunikasie Unie (ITU). CCITT doen aanbevelings vir telekommunikasie- en datakommunikasienetwerke.[34]
- NATIONAL BUREAU OF STANDARDS(NBS), Die NBS behoort aan verskillende internasionale organisasies en spesialiseer veral in die implimentasie van die boonste vlakke van die OSI-standaarde.[34]
- DATA ENCRYPTION STANDARD(DES),[Hst 5]
- AMERICAN NATIONAL STANDARDS INSTITUTE(ANSI). Dit is 'n koördinerings agentskap vir standaarde wat vrywillig in die V.S.A. gebbruik word.

Dit mag soms nodig wees om standaarde aan te pas vir die spesifieke toepassing. Dit was byvoorbeeld voor die publikasie van die OSI-Sekerheydsbylaag nodig om self sekerheidsmaatreëls te ontwikkel as die OSI-standaarde gebruik is. Die belangrikste faktor wat in aanmerking geneem moet word by die keuse van so 'n standaard is of dit voorsiening maak vir sekerheid. Vir verdere doeleindes word aanvaar dat die ISO se OSI-standaard en sekerheidsbylaag gekies is.

Identifiseer sekerheidsdienste. F4.T4.S2.

In die tweede stap moet daar besluit word watter sekerheidsdienste nodig sal wees. In die OSI-sekerheidsbylaag word verskillende dienste aanbeveel. 'n Sekerheidsdiens is 'n prosedure wat sekere sekerheidsfunksies verrig binne die netwerk.

Tabel 8.1. dui die volledige lys van dienste aan wat deur die ISO-sekerheidsbylaag aanbeveel word. Dit sal in baie gevalle nie nodig wees om al die moontlike dienste te implimenteer nie. Sekerheidsdienste word in meer detail bespreek in hoofstuk 2 en sal nie verder in hierdie hoofstuk bespreek word nie.

Keuse van sekerheidsmeganismes.

Volgende stap moet besluit word watter meganismes gebruik gaan word om die dienste, wat in stap 2 gekies is, mee te implimenteer. Daar bestaan weereens verskillende meganismes om die dienste mee te implienteer. Vir 'n volledige lys sien tabel 8.1. In die tabel 8.1. kan duidelik gesien word dat al die dienste geïmplimenteer kan word deur die gebruik van drie meganismes naamlik kriptografie, elektroniese handtekeninge en toegangsbeheer meganismes.

SEKERHEIDSDIENSTE.	SEKERHEIDSMEGANISMES.							
	ENKRIPSIE	SYFERHANDTEKENINGE	TOEGANGSBEHEER	DATAINTEGRITEIT	WAARMERKING	VERKEEROPVULLING	ROETEBEHEER	NOTARISASIE
GELYKE ENTITEITWAARMERKING.	*	*			*			
TOEGANGSBEHEER.			*					
SKAKEL VERTROULIKHEID.	*							
ONGESKAKELDE VERTROULIKHEID.	*							
SELEKTIEWE VELDVERTROULIKHEID.	*							
VERKEERSVLOEI SEKERHEID.	*							
SKAKEL INTEGRITEIT MET HERSTEL.	*			*				
SKAKEL INTEGRITEIT SONDER HERSTEL	*			*				
SELEKTIEWE VELD ONGESKAKELDE INTEGRITEIT.	*	*		*				
DATAOORSPRONG WAARMERKING.	*	*						
NIE-TERUGTREKKING DEUR OORSPRONG		*		*				*
NIE-TERUGTREKKING DEUR ONTVANGER		*		*				*

TABEL 8.1. MEGANISMES WAT ALLEEN OF IN KOMBINASIE GEBRUIK KAN WORD OM SEKERHEIDSDIENSTE MEE TE IMPLIMENTEER.

Kriptografie. F4.T4.S3. en Enkripsie\Dekripsie. F4.T4.S4.

Enkripsie kan beskou word as verreweg die belangrikste hulpmiddel of meganisme wat in netwerk- en kommunikasiesekerheid aangewend kan word vir die beskerming van data en ander inligting. Die literatuur maak in die meeste gevalle van die term enkripsie gebruik om enkripsie, dekripsie en sleutelbestuur in te sluit.[7][10][25] Die korrekte term hier is egter **Kriptografie**, wat beide enkripsie, dekripsie en ook sleutelbestuur insluit.[16][61]

In TABEL 8.1 word aangedui dat enkripsie die sekerheidsmeganisme is wat gebruik kan word om feitlik enige sekerheidsdiens mee te implimenteer. Enkripsie word gebruik om die inhoud van 'n boodskap onverstaanbaar te maak vir enige iemand wat nie oor die fasiliteite en regte beskik om die boodskap weer te dekripteer nie. Dekripsie is weer die teenoorgestelde proses wat gebruik kan word om die geënkripteerde boodskap of data weer terug te verander, of te dekripteer, na die oorspronklike, verstaanbare vorm.

Daar bestaan drie basiese enkripsiemetodes naamlik Skakelenkripsie, Node-vir-Node enkripsie en End-tot-End enkripsie. Die verskillende metodes word in meer detail in hoofstuk 7 bepreek. Tabel 8.2. en Tabel 8.3. dui die belangrikste kenmerke van die drie metodes aan.

TABEL 8.2. BELANGRIKSTE SEKERHEIDSKENMERKE.

	VERKEERONTLEDING	BOODSKAP BESKERMING
SKAKELENKRIPSIE	ONMOONTLIK	SLEGS OP SKAKELS
END-TOT-END ENKRIPSIE	GEEN BESKERMING	HELE NETWERK
NODE-VIR-NODE ENKRIPSIE	GEEN BESKERMING	TUSSEN NODES

TABEL 8.3. KENMERKE VAN VERSKILLENDE ENKRIPSIEMETODES.

SKAKELENKRIPSIE	NODE-VIR-NODE ENKRIPSIE	END-TOT-END ENKRIPSIE
BOODSKAP SLEGS OP SKAKEL GEëNKRIPTEER.	BOODSKAP TUSSEN NODES GEëNKRIPTEER	BOODSKAP VANAF STUURDER TOT ONTVANGER GEëNKRIPTEER
BOODSKAP ONBESKERM TUSSEN ENKRIPSIETOESTEL EN NODE	BOODSKAP ONBESKERM IN NODE.	BOODSKAP BESKERM DEUR HELE NETWERK
ELKE SKAKEL MOET OOR TWEE KRIPTOGRAFIESE-TOESTELLE BESKIK.	ELKE NODE MOET OOR 'N KRIPTOGRAFIESE TOESTEL BESKIK.	KRIPTOGRAFIESE TOESTELLE SLEGS IN EINDPUNTE NODIG.
VERSPREIDING VAN SLEUTELS SLEGS NODIG TUSSEN TWEE TOESTELLE OP ELKE SKAKEL	VERSPREIDING VAN SLEUTELS NODIG TUSSEN TWEE AANGRENSENDE NODES	VERSPREIDING VAN SLEUTELS NODIG TUSSEN TWEE EINDPUNTE.

Sleutelbestuur. F4.T4.S5.

'n Baie belangrike aspek in kriptografie is die bestuur en beheer van die sleutels wat in die kriptografiese proses gebruik word. Die sukses van enige kriptografieseproses berus op die geheimhouding en beskerming van die enkripsie- en dekripsiesleutels. In die netwerksekerheidsomgewing word die probleem van beskerming van die sleutels baie meer gekompliseer, aangesien die stuurder en die ontvanger vêr uitmekaar kan wees. Die probleem wat op netwerke bestaan dat data ongemagtig onderskep kan word deur indringers, geld ook vir die verspreiding van sleutels. Daar moet dus metodes bestaan wat die veilige vervoer van sleutels deur die netwerk verseker.

Die probleem eindig egter nie met die vervoer van die sleutels nie. Die generering en berging van die sleutels is ook 'n prosesse wat beskerm moet word, terwyl die vernietiging van sleutels, wat nie meer gebruik word nie, 'n aspek is wat in baie gevalle in die literatuur oor die hoof gesien word.

Sleutelbestuur sluit alle aspekte ten opsigte van die hantering van sleutels in die netwerk in, vanaf die generering van die sleutels, tot die uiteindelike vernieteging van die sleutels. Die meeste probleme word ondervind met die verspreiding van die sleutels en die berging daarvan.[15][16][61]

Sleutelbestuur word in meer detail bespreek in hoofstuk 7 onder die volgende punte:

- Tipiese lewenssiklus van 'n sleutel.
- Generering en toetsing van sleutels vir gebruik in netwerksekerheid.
- Verspreiding, laai en berging van sleutels deur die netwerk.
- Vernieteging van sleutels na gebruik.
- Tipes sleutels en hulle karakteristieke.

Elektroniese handtekeninge. F4.T4.S6.

'n Elektroniese handtekening is 'n protokol wat dieselfde effek het as die gebruik van 'n gewone handtekening. Dit is 'n merk of teken wat net die stuurder maak maar wat maklik deur die ontvanger en ander gebruikers herken kan word as die stuurder se elektroniese handtekening. Die handtekening word net soos 'n gewone handtekening gebruik om 'n ooreenkoms of bevestiging van 'n boodskap te erken.

Die belangrikste vereistes van 'n elektroniese handtekening is dat dit :

- Onvervalsbaar moet wees.
- Waarmerkbaar moet wees. Dit beteken daar moet bewys kan word wie se handtekening dit is en dat hy dit gemaak het.

Elektroniese handtekeninge kan verkry word as daar van Publieke sleutelenkripsie gebruik gemaak word. Die proses is as volg :

- Stuuder S1 wil 'n getekende boodskap stuur aan Ontvanger O1. S1 enkripteer die boodskap met sy geheime sleutel en stuur dit aan die O1. O1 dekripteer die boodskap met S1 se publieke sleutel wat algemeen bekend is. Aangesien slegs S1 weet wat sy geheime sleutel is, kan dit net hy wees wat die boodskap aanvanklik geënkripteer het. Die proses berus egter totaal en al op die geheimhouding van die geheimesleutels van gebruikers. Dit is belangrik dat onthou word dat elektroniese handtekening nie die geheimhouding van die boodskap verseker nie aangesien die dekripsiesleutel openbare kennis is.

Elektroniese handtekeninge is 'n baie interessante veld maar daar is nog baie navorsing nodig voor dit algemeen aanvaar sal word. Die voorafgaande bespreking was net bedoel om die leser 'n idee te gee waaroor elektroniese handtekeninge gaan. Vir verdere doeleindes kan die volgende bronne geraadpleeg word [10][15][16][124]

Toegangsbeheermeganismes. F4.T4.S7.

Hierdie stap word saam met stap F4.T4.S14. bespeek.

Ontwerp sekerheidsbuitelyne. F4.T4.S8.

n Sekerheidsbuitelyn is 'n logiesegrens wat om 'n gebied getrek word wat betroubaar moet wees. Dit is areas waarin sekerheidsdienste nie voorkom nie, en sekerheid word verskaf met behulp van betroubare personeel en stelsels. Die dele van die netwerk buite die sekerheidsbuitelyne moet beskerm word deur sekerheidsdienste. Die grense stem ooreen met die sekerheidsbuitelyne wat in hoofstuk 2 bespreek is.[8][129]

Sekerheidsbuitelyne kan op drie maniere gebruik word, naamlik :

- Buitelyn om hele netwerk.
- Buitelyn om elke toepassing.
- Buitelyn om boonste vlakke van argitektuur.

Vir verdere bespreking van sekerheidsbuitelyne raadpleeg hoofstuk 2.

Netwerktopologieë. F4.T4.S9.

Netwerktopologië kan 'n groot uitwerking hê op die sekerheidsmaatreëls wat in 'n netwerk geïmplimenteer word. Die verskil tussen lokaleareanetwerke en ander tipes rekenaarnetwerke begin al hoe kleiner word. Die belangrikste verskil is dat lokaleareanetwerke(LAN) en mediumareanetwerke(MAN) in 'n beperkte gebied voorkom soos byvoorbeeld 'n gebou of beperkte geografiese area. Met die interskakeling van netwerke, begin wyeareanetwerke(WAN) en groter netwerke opgebou word. Die verskillende tipes netwerke bestaan ook uit dieselfde basiese toerusting soos byvoorbeeld lêerbedienners, kommunikasieverbindings, modems, drukkers en terminale. Diè basiese toerusting sal vir die res van die beskrywing slegs as 'n nodus bekend staan. Die volgende bronne kan geraadpleeg word vir 'n algemene beskrywing van netwerk topologië [10][9][17][22][25][34][35][68][74][104].

So beskik die verskillende tipes netwerke ook oor dieselfde basiese topologië. Die doel van hierdie taak is nie om 'n volledige bespreking van netwerktopologië te gee nie. Slegs die belangrikste kenmerke van die belangrikste topologië sal gegee word, sowel as die sekerheidskenmerke van die topologië.

Die mees algemene topologië is die volgende :

- Gemeenskaplike bus.("Common Bus") Soos die naam aandui bestaan daar 'n gemeenskaplike bus waaraan al diê terminale en ander rekenaartoerusting gekoppel is. Die bus is in eenvoudige gevalle slegs 'n kabel wat die verskillende nodi aanmekaar koppel. Fig 8.15A is 'n voorstelling van 'n Bustopologie.

  Elke nodus is verantwoordelik vir die stuur en ontvang van al sy kommunikasie. Die nodus moet gedurig die bus monitor om boodskappe te ontvang. Sodra 'n nodus 'n boodskap ontvang kontoleer hy die adres en aanvaar die boodskappe wat vir hom bedoel is en ignoreer boodskappe wat vir ander nodi bedoel is. Die belangrikste sekerheidsnadeel van die bus is die feit dat enige nodi wat aan die bus gekoppel is enige boodskap op die netwerk kan onderskep. Daar bestaan geen sentrale beheernodus wat die netwerk beheer en sekerheid kan afdwing nie.

- Ster.("Star") In 'n ster is elke nodus aan 'n sentrale beheernodus gekoppel. Die beheernodus ontvang alle kommunikasie vanaf stuurders en stuur dit dan aan die ontvangers. Daar bestaan net een pad tussen 'n stuurder en 'n ontvanger en dit is deur die beheernodus. Die belangrike voordeel vir sekerheid is dat die beheernodus moet verseker dat die boodskap by die regte ontvanger uitkom. Fig 8.15B is 'n voorstelling van 'n Stertopologie.

- Ring.("Ring") In 'n Ring beweeg al die boodskappe in een rigting van een nodus na 'n ander. Elke nodus ontvang al die boodskappe op die netwerk, selekteer sy eie boodskappe en stuur die res aan na die volgende nodus in die ry. Vanuit 'n netwerksekerheidsoogpunt is die probleem dat al die nodi elke boodskap op die netwerk ontvang en dus ook ander nodi se boodskappe kan lees. 'n Verdere nadeel is dat 'n nodus 'n boodskap van 'n ander nodus ongemagtig kan terughou. Hier is net soos by die bus geen sentrale beheernodus wat kan verseker dan boodskappe by die regte ontvangers uitkom nie. Fig 8.15C is 'n voorstelling van 'n Ringtopologie.

Uit die kort bespreking is dit duidelik dat daar ook aandag gegee behoort te word aan die topologie wat gebruik word as sekerheidsmaatreëls beplan en geïmplimenteer word.

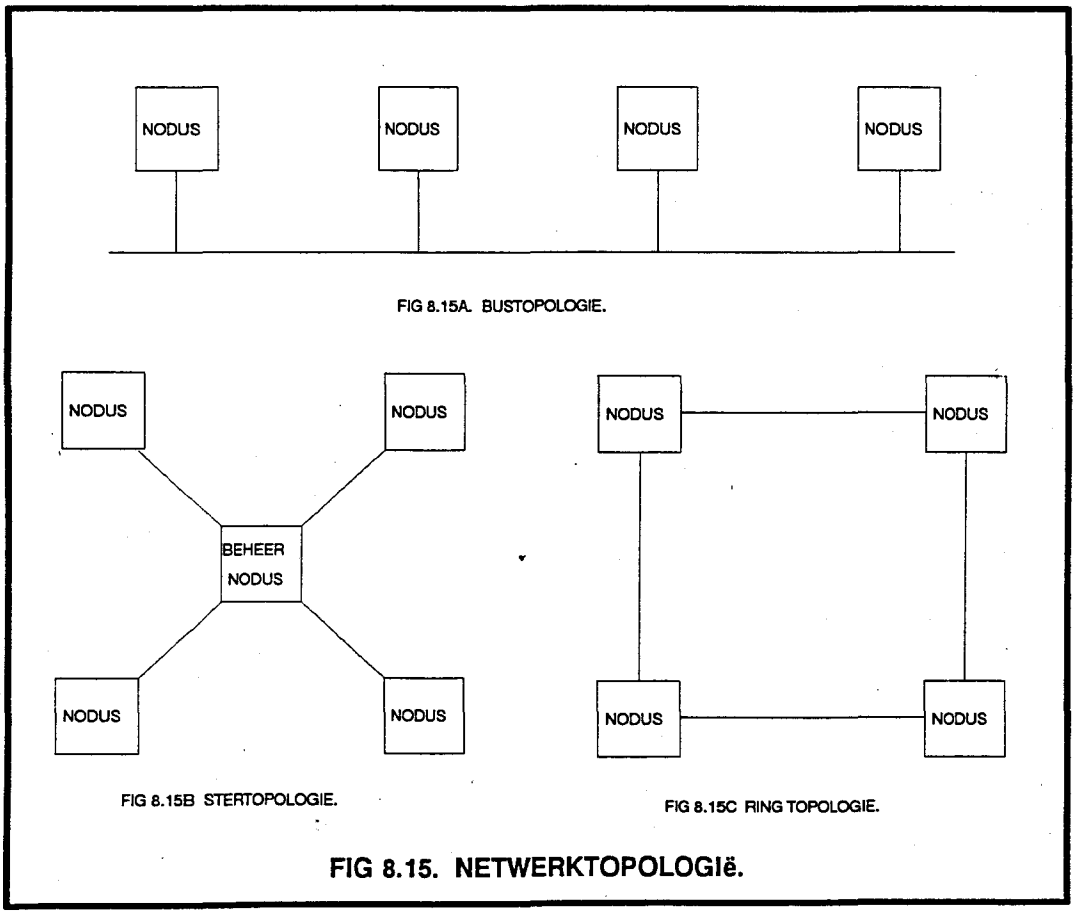


FIG 8.15. NETWERKTOPOLOGIë.

Kommunikasieverbindings. F4.T4.S10.

In stap 4 word daar besluit oor die soort kommunikasieverbinding wat in die netwerk gebruik sal word. Dit is belangrik dat die keuse hier nie slegs op 'n kosteoogpunt moet berus nie, maar dat sekerheidsaspekte hier voorkeur moet geniet. Tabel 8.4. dui die kenmerke van die belangrikste geleidingsverbindings aan en tabel 8.5. dui die kenmerke van die belangrikste uitstralingsverbindings aan.

TABEL 8.4. GELEIDINGSVERBINDINGS.

	GEDRAAIDE-PAAR. (ONBESKERM)	GEDRAAIDE-PAAR. (BESKERM)	KOAKSIALE KABEL	OPTIESEVESEL-KABEL
KOSTE	GOEDKOOP	GOEDKOOP	DUUR	BAIE DUUR
BANDWYDTE	LAAG	LAAG	HOOG	BAIE HOOG
ISOLERING	GEEN	SWAK - GOED	GOED	GOED
UITSTRALING	BAIE HOOG	GEMIDDELD	LAAG	GEEN
INVLOED VANBUITE	BAIE HOOG	HOOG (WISSEL)	LAAG	GEEN
INTEGRITEIT	SWAK	SWAK - REDELIK	GOED	BAIE GOED
KABELGEWIG	SWAAR	HOOG	HOOG	LAAG
GEVAAR VAN AFTAPPING	BAIE HOOG	BAIE HOOG	HOOG	BAIE HOOG
GEMAK VAN AFTAPPING	BAIE MAKLIK	MAKLIK	MOEILIK	BAIE MOEILIK
INSTANDHOUD-ING. (PERIODE)	GEREELD	GEREELD	MINDER GEREELD	BAIE MIN

TABEL 8.5. UITSTRALINGSVERBINDINGS.

	RADIO	MIKROGOLF	SATELLIET	SELLULRE TELEFOON
KOSTE	GOEDKOOP	GEMIDDELD	DUUR	GEMIDDELD
BANDWYDTE	LAAG	GEMIDDELD	BAIE HOOG	GEMIDDELD
UITSTRALING	BAIE HOOG	BAIE HOOG	BAIE HOOG	BAIE HOOG
INVLOED VAN BUITE	BAIE HOOG	HOOG	LAAG	HOOG
INTEGRITEIT	SWAK	GOED	GOED	REDELIK
GEVAAR VAN MEELUISTER	BAIE HOOG	HOOG	HOOG	BAIE HOOG
GEMAK VAN MEELUISTER	BAIE MAKLIG	MOEILIK	MOEILIK	BAIE MAKLIK
UITBREIBAAR-HEID	HOOG	HOOG	HOOG (DUUR)	LAAG (MIN FREKWENSIES)

Internetwerkskakeling. F4.T4.S11.

Toenemende gebruik van netwerke bring mee dat netwerke aanmekaar gekoppel moet word om gebruikers toe te laat om hulpbronne en inligting op verskillende netwerke te bekom. Die interskakeling van netwerke kan 'n groot invloed op bestaande en ook beplande netwerksekerheidsmaatreëls uitoefen. Veral die punt waar die netwerke aanmekaar gekoppel word moet deeglik beplan en bestudeer word.

Daar bestaan drie tipes netwerkskakelingsmetodes naamlik:

- Brug: 'n Brug word gebruik om netwerke wat van identiese protokolle gebruik maak te skakel.
- Deurgang: 'n Deurgang word gebruik om netwerke te skakel wat van totaal verskillende protokolle en argitekture gebruik maak.
- Roetteerder: 'n Roetteerder word gebruik om netwerke te skakel wat van verskillende protokolle gebruik maak, maar wel van dieselfde internetprotokol gebruik maak.

Al drie die metodes word in hoofstuk 3 bespreek.

Internetwerkregte. F4.T4.S12.

Die beheer en bestuur van Internetwerkregte hou verband met die probleem van internetwerkskakeling. Dit is belangrik dat daar 'n metode moet bestaan om regte tussen verskillende netwerke te kan beheer aangesien die probleem kan ontstaan dat ongemagtigde regte op indirekte wyse op netwerke bekom kan word.

In hoofstuk 4 word twee toegangsbeheerlyste en toegangsbeheermatrikse bespreek as twee van die algemeenste benaderings vir die bestuur en beheer van netwerkregte. Die twee metodes word meestal ook gebruik om vir internetwerkregte. Die Pad-Konteksmodel wat ontwikkel is by die Randse Afrikaanse Universiteit word ook bespreek as 'n moontlike moderne benadering tot die bestuur en beheer van internetwerkregte.

Vir meer inligting kan hoofstuk 4 geraadpleeg word..

Toegangspoorte. F4.T4.S13.

'n Baie kwesbare punt in enige netwerk is die toegangspoorte waarmee 'n gebruiker van buite die netwerk toegang tot die netwerk kan verkry. Die toegangspoorte is in die meerderheid gevalle aan modems en telefoonlyne gekoppel.

Daar bestaan verskillende soorte modems en toepassings wat aangewend kan word om die toegangspoorte te beskerm en word in hoofstuk 6 bespreek.

Toegangsbeheer. F4.T4.S14 en F4.T4.S7.

Toegangsbeheer in 'n netwerk is een van die belangrikste aspekte van netwerksekerheid wat aangespreek moet word. Geen toegangsbeheermaatreël sal iets werd wees as 'n wettige gebruiker nie op 'n effektiewe manier geïdentifiseer kan word nie. Daar bestaan verskillende metodes wat gebruik kan word om die identiteit van 'n gebruiker te bapaal. Die metodes kan in twee groeppe opgedeel word naamlik Biometriese en Nie-Biometriese metodes.

In Tabel 8.6. word die kenmerke van die belangrikste biometriese metodes aangedui, terwyl Tabel 8.7. die belangrikste nie-biometriese metodes se kenmerke aandui. 'n Meer volledige beskrywing kan gevind word in hoofstuk 6.

TABEL 8.5. KENMERKE VAN BIOMETRIESE METODES.

	VINGER-MERK	PALM-AFDRUK	RETINA-PATROON	POLSAAR-PATROON	DINAMIESE HANDTEKE-NING	STEM-HERKENN ING
EENHEDE VERKOOP 1987	260	60	125		125	600
EENHEDE VERKOOP 1988	475	130	175		195	625
KOSTE per EENHEID 1989	1800	3000	5000		640	1200
EFFEKTIWI-TEIT	REDELIK	REDELIK	BAIE HOOG	REDELIK	REDELIK TOT HOOG	HOOG
PRAKTIES TOEPAS-BAAR	REDELIK.	REDELIK	HOOG	LAAG	REDELIK	HOOG
GEBRUIKER AANVAAR-BAARHEID	LAAG	LAAG	LAAG - REDELIK	ONBEKEND	HOOG	HOOG
REAKSIE-TYD	VINNIG	STADIG	VINNIG	ONBEKEND	VINNIG	STADIG

TABEL 8.6. KENMERKE VAN NIE-BIOMETRIESE METODES.

	WAGWOORDE	MAGNEETKAART	SLIMKAART
EFFEKTIWITEIT	HOOG	REDELIK	HOOG
PRAKTIESE TOEPAS-BAARHEID	HOOG	HOOG	HOOG
GEBRUIKERAAN-VAARBAARHEID	HOOG	HOOG	HOOG
REAKSIETYD	VINNIG	VINNIG	VINNIG
PRYS	GOEDKOOP	GEMIDDELD	DUUR

8.6. SAMEVATTING.

Die ontwikkeling en implimentasie van netwerksekerheids behoeftes het in organisasies reg oor die wêreld belangrike aspekte geword waaraan aandag gegee moet word. Van die belangrikste probleme is dat tegnologie en die vermoëns van rekenaar misdadigers verstommend vinnig toeneem. Dus sal feitlik geen sekerheidsmaatreëls wat ontwikkel word permanent suksesvol wees nie. Dit is veral van toepassing by netwerksekerheid. Die enigste oplossing is die aaneenlopende ontwikkeling, implimentasie en instandhouding van sekerheidsmaatreëls.

Vir die doel is dit nodig om van 'n Rekenaarsekerheidsmetodologie gebruik te maak. Twee sulke metodologië is in hoofstuk 8 bespreek. Die RS-Metodologie is die mees omvangrykste van die twee metodologië en daar is ook gepoog om die bestaande RS-Metodologie uit te brei om netwerksekerheid deeglik in aanmerking te neem.

HOOFSTUK 9.

TOEKOMSBLIK.

9.1. INLEIDING.

As gevolg van die toenemende belangrikheid van rekenaars en rekenaarnetwerke word die ontwikkeling en implimentasie van sekerheid op die netwerke 'n uiters belangrike saak. Rekenaarnetwerke word ook al hoe meer die teiken van misdadigers wat al hoe meer gesofistikeerd word. Die behoefte van gebruikers om ten alle tye en op alle plekke rekenaars en netwerke tot hulle beskikking te hê het gelei tot die interskakeling tussen netwerke. Die interskakeling lei verder tot probleme wat betref netwerksekerheid wat al hoe meer ingewikkeld raak. Aanhangsel 1 bevat 'n artikel wat voogelê is aan die internasionale tydskrif "Computers & Security". Die artikel is ook as referaat voorgelê aan twee internasionale konferensies naamlik COMPSEC 91 in die Verenigde Koninkryk en NIST 91 in die Verenigde State van Amerika..

9.2. TOEKOMSBLIK.

In die raamwerk wat opgestel is in hoofstuk 1 is daar sekere aspekte wat nie aandag gekry het nie en wat in die toekoms in verdere studie aandag sal geniet. Verder is daar ook van die onderwerpe wat in hierdie verhandeling bestudeer is wat meer aandag nodig het.

Onderwerpe wat in verdere studie gedek kan word is die volgende :

- Die rol wat fisiese sekerheid speel in netwerksekerheid.
- Bestudering en ontwikkeling van Aktiwiteitboekhoudingsfasiliteite.
- Elektroniese handtekeninge is net kortliks bespreek en meer aandag is hier nodig.
- Netwerkrisikobestuur en rampherstel word reeds gedek in navorsing wat gedoen word by R.A.U.
- Die gebruik van die Pad-Konteksmodel in netwerke en internetwerke.
- Die rol van kennisgebasseerde tegnieke in netwerksekerheid. Hierdie punt kan saam met die volgende punt bestudeer word.
- Die rol van netwerkbestuur by netwerksekerheid is 'n veld wat nog baie aandag nodig het.

Die skrywer is van plan om self die laaste twee punte te dek in 'n Ph.D studie. Die doelwit van die studie sal wees om die ontwikkeling en ontwerp van 'n intelligente netwerksekerheidsdatabasis en kennisgebaseerde toepassing vir 'n netwerkomgewing te ondersoek. Die databasis en ekspertstelsel sal die insameling en ontleding van sekerheidsverwante inligting uit ander netwerkbestuurs- en sekerheidstoepassings op netwerke en internetwerke waarneem.

Die wye verskeidenheid netwerkbestuurs- en sekerheidstoepassings wat op netwerke gevind word maak dit nodig om inligting te versamel uit die verskillende toepassings en 'n standaard voorstellingsformaat vir die inligting daar te stel.

AANHANGSEL 1.

ARTIKEL.

COMPUTER SECURITY MANAGEMENT : METHODOLOGY

AND

NETWORK SECURITY.

Prof. Jan H P Eloff
Mr. A.J. Nel.

Department Computer Science
Rand Afrikaans University
P.O. Box 524
Johannesburg South Africa.

ABSTRACT

This paper aims to address the complicated issue of network security. Network security is approached from a management and more specifically from a methodical point of view as opposed to the usual technical descriptions. Network security needs to be addressed from a technical as well as from an application systems perspective. The technological issues on network security addresses the broader concepts such as the provision of a variety of network security services and mechanisms for example authentication and traffic analyses. Applications network security assures that a network oriented application system be designed to adhere to the computer security policy of the organization in general. Both these network security issues will be addressed within the framework of a methodical view on information security in general.

Keywords : computer security, network security, methodology, computer security management.

BIOGRAPHY.

Jan H.P. Eloff received a BSc (Computer Science) degree at the Rand Afrikaans University, Johannesburg, South Africa in 1978. In 1980 he received an MSc in Computer Science at the same university. His dissertation involved an in-depth study of all the logical aspects of computer security. Part of this research was published in "Computers & Security" (Nov. 1983) under the title "Selection Process for Security Packages". In 1985 he received a PhD (Computer Science) with a thesis titled "The Development of a Specification Language for a computer security system". Part of the research done for his PhD was published in "Computers & Security" under the same title. He also delivered papers at the IFIP/SEC'84 and IFIP/SEC'85 conferences. He gained practical experience by working as a computer consultant as well as a manager of a large information centre. He is currently a professor in Computer Science at the Rand Afrikaans University, South Africa.

Awie J. Nel received a B.Com (Information Systems) degree at the Rand Afrikaans University in Johannesburg, South Africa in 1988. In 1989 he received a B.Com.Hons (Informations Systems) degree at the same university. He is currently working towards a M.COM(Information Systems) degree under the guidance of Prof Eloff.

0. INTRODUCTION.

Network security should be included in the scope of the information security policy of an organization. Interconnectivity is one of the most widely used computer buzzwords today, however very few organizations attempt to take a reliable and security consistent approach in implementing interconnectivity. Practical experience from the authors manifested the following problems :

- In cases where network security has been addressed it is the authors experience that it happened on a too low or heavy technical oriented level.
- A number of organizations are not sure what is really meant with the term "Network", furthermore they had problems in addressing the complete scope of network security [6].
- Senior managements comprehension of network security at the majority of organizations lacks an understanding of the technical details thereof. They also have difficulty in understanding the concept of addressing network security specifically in the information security policy for the organization.
- Organizations experience difficulty in addressing the implementation of counter measures for network security as part and furthermore in synchronization with the counter measures implemented for information security. This approach is costing organizations large sums of money due to the fact that synchronized and combined counter measures has a much more powerful effect on the displacement of risks as opposed to the implementation of individual counter measures.
- Very few organizations takes a methodical approach towards the implementation of information security (including network security) counter measures.

The authors very strongly believe that a methodical approach towards the implementation of information and network security will address the above mentioned problems. However, following a literature study undertaken by the project team it became evident that very little attention has been paid to this subject. Current literature regarding such an approach could be briefly summarized as follows [2],[3],[4],[6]:

- methodology for the design for a secure network oriented application system
- methodology for the implementation of information security.

The objectives of this paper is to address both the above mentioned issues within the framework of a methodology, the so-called IS-Methodology.

1. INFORMATION SECURITY METHODOLOGY : IS-METHODOLOGY.

The basis of the IS-Methodology was developed at the Rand Afrikaans University by Prof. J.H.P. Eloff and K.P. Badenhorst. The reason for the development are to design a structured approached for the specification and implementation of information security in an organization.

Fig 1. gives a short overview of the 5 main phases of the methodology and Fig 2. show a high-level view of the IS-Methodology.

(1) PHASE 1 - INITIATION : Senior management need to be made aware of the risks involved when too little or no information security exists in their company. A specially selected steering committee needs to be established to guide the information security plan through its phases. The manager responsible for data communications and networks need to be represented on this committee.

(2) PHASE 2 - INFORMATION SECURITY POLICY: The establishment of a formal information security policy, which is in line with organizational strategies and company mission, forms an essential basis from which to launch a risk analysis study. It contains the definition, framework of terminology, with special reference to network terminology, as well as a matrix depicting responsibility and accountability functions within such a framework. These will also include responsibilities for network security. The information security policy should address the very important issue of network security perimeters, this concept will be discussed in paragraph 4.

(3) PHASE 3. RISK ANALYSIS AND PROJECT DEFINITION: Information security risks and associated potential losses need to be quantified and weighed against factors such as productivity, users satisfaction, network response times, cost of controls, and the like. This action will result in cost effective countermeasures and the compilation of a well-defined project plan for the installation of those measures. The compilation of a project plan at this stage of the process will force integration between countermeasures planned for network security and other information security related projects such as procedures for access control on mainframes.

(4) PHASE 4- INSTALLATION: The timely installation of information security countermeasures as depicted in the project plan. It is during this phase that an organization has to implement security services and mechanisms. Last mentioned is especially true in the network environment where implementation of technologies such as gateways, inter-network protocols and communication links will take place.

(5) PHASE 5 - MAINTENANCE: The on-going maintenance includes a regular review of the information security status and requirements as well as the on-going implementation of controls within the development of application systems. This phase also provides for design procedures to implement application systems running in a network environment. This concepts will not be discussed in the context of this paper, the reader is referred to [2] for further reading material.

FIG 1. OVERVIEW OF THE IS-METHODOLOGY.

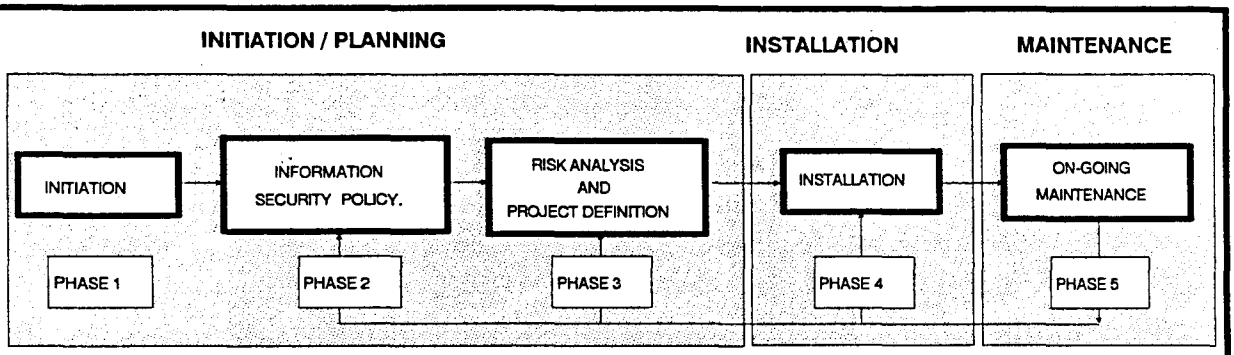


FIG 2. IS-METHODOLOGY: A HIGH-LEVEL VIEW.

The remainder of this paper will discuss the concepts on technological network security as described in the installation phase (phase 4) of the IS-Methodology.

2. IS-METHODOLOGY PHASE 4 : INSTALLATION.

Fig 3. shows the main tasks in phase 4 of the IS-Methodology.

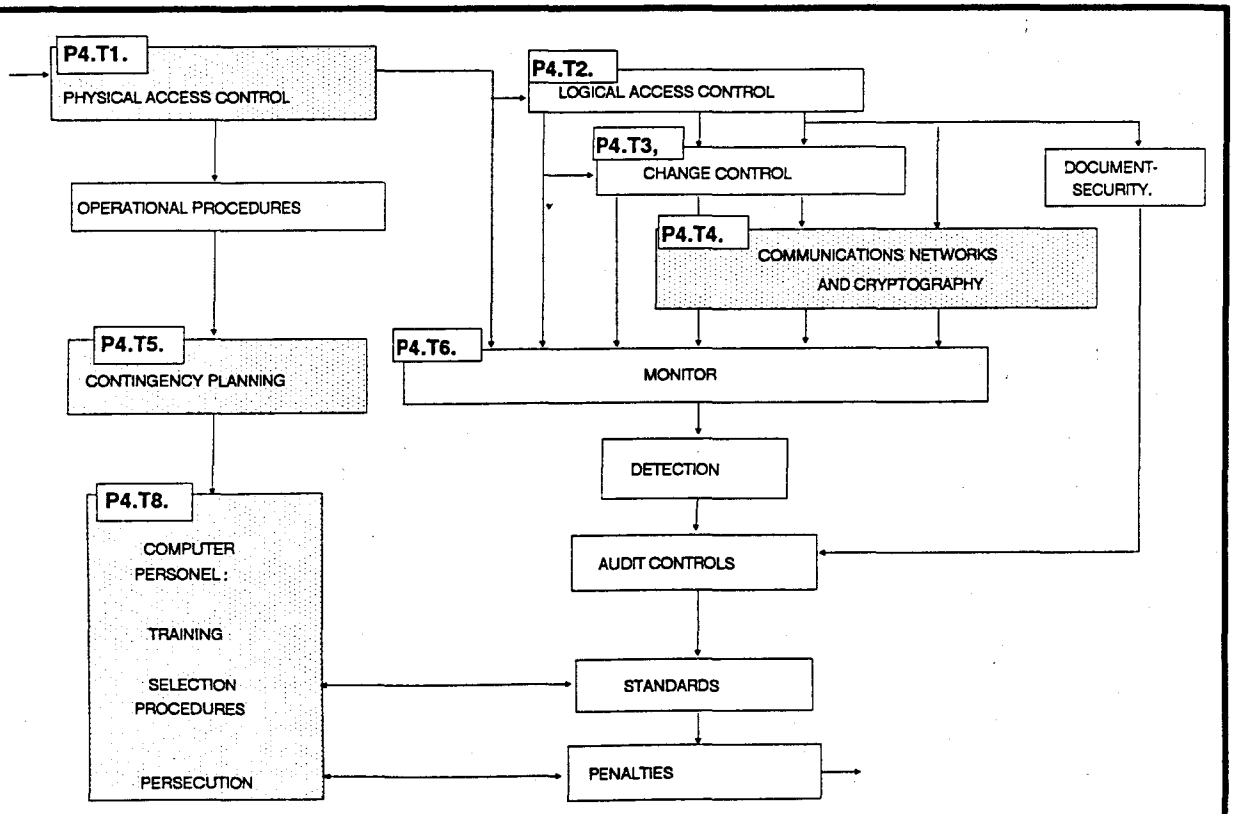


FIG 3. PHASE 4. INSTALLATION.

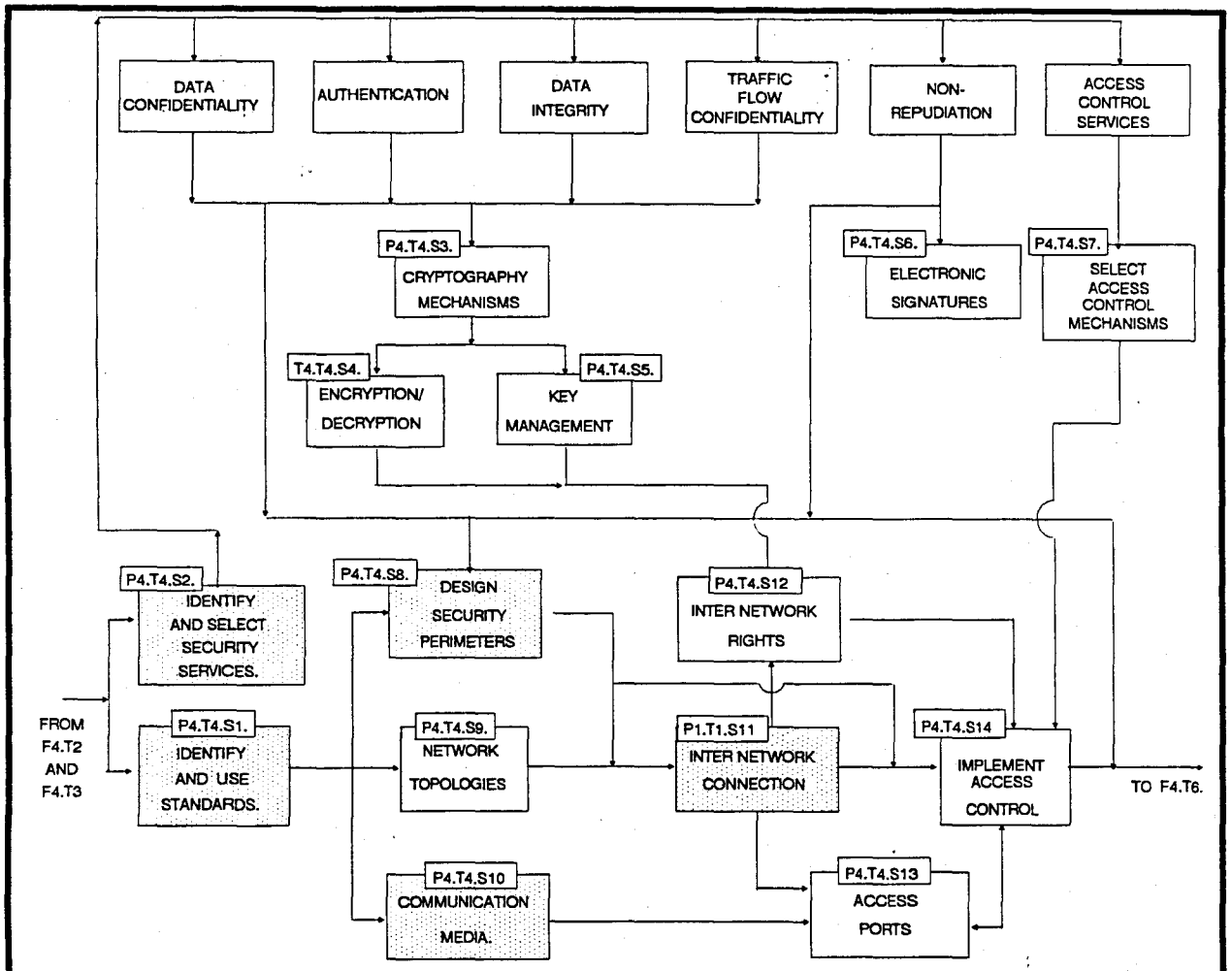


FIG 4. PHASE 4. TASK 4. NETWORK SECURITY.

This phase of the IS-Methodology addresses all the aspects of technological information security such as physical and logical access, cryptography, disaster recovery, planning, and the like. The installation phase of the IS-Methodology turned out to be one of the most critical due to the variety of specialized skills and line personnel involved. Some of the more important tasks in phase 3 are the following:

PHYSICAL ACCESS (P4.T1): Physical Access to computer terminals and communications equipment are a very important aspect of network security. These terminals and equipment are mostly situated outside the organization itself where strict physical security are difficult. An example are the use of Automatic Teller Machines (ATMs), of banking organizations which are installed in public areas where the equipment can't be protected by measures like security guards and strong rooms.

- **COMMUNICATION NETWORKS AND CRYPTOGRAPHY. (P4.T4)**: This is the part of the IS-Methodology that includes technological network security and that will receive more attention in the rest of this paper.

- **CONTINGENCY PLANNING (P4.T5)**: Because of the high level of resource sharing, that is one of the main features in the use of computer and communications networks, the possibility of destruction or corruption of these resources is very high. This leads to the need and increased importance of well developed contingency planning especially for interconnected networks.

- **COMPUTER PERSONNEL (P4.T8)**: A important aspect of network security that are often overlooked, are the proper training of personnel in the organization. When security includes network security, it will be important that the personnel are also trained in aspects of network communications, as well as the special aspects of network security. Examples here are the use of modems and the need for safe password and key management procedures.

3. ACHIEVING NETWORK SECURITY - IS-METHODOLOGY : PHASE 4, TASK 4.

Fig 4. shows the main steps in Phase 4, Task 4, of the IS-Methodology regarding technological network security. We will not discuss all of the steps mentioned, but only the most important. There are a variety of security measures that are only applicable to computer and communications networks. These measures need special attention when they are planned and implemented.

A few steps, (those shaded in the above diagram) out of P4.T4. will now be discussed.

P4.T4.S1. Identify and select standards.

The first step will be to identify applicable standards for the implementation of network security in the organization, and to select the standards that will be used. There are quite a few international organizations that develop standards for communications networks, as well as security. To name only a few of them :

- **INTERNATIONAL STANDARDS ORGANIZATION(ISO)**. The ISO developed the Open Systems Interconnecting model (OSI- model) as well as a security addendum for the model.[1][[9][10]
- **INTERNATIONAL CONSULTATIVE COMMITTEE FOR TELEPHONE AND TELEGRAPH (CCITT)**. The CCITT are a member of the International Telecommunications Union, and make recommendations on telecommunications and data networks.[9]
- **AMERICAN NATIONAL STANDARDS INSTITUTE(ANSI)**. ANSI is a coordinating agency for standards implemented in the U.S.A. on a voluntary basis.[9]

It may at times be necessary to customize standards for a specific application. The most important factor to consider in the selection process for standards, are the attention given to security in the standard. If the ISO standards are selected, security are already included in the security addendum to the OSI model [10]. For the rest of this paper it is assumed that the OSI-model and security addendum was selected as standards.

P4.T4.S2. Identify and select security services.

The next step will be to decide what security services will be needed. The OSI security addendum[10] recommend a number of services but not all of them may be necessary. For the rest of the discussion only the following services are selected :

- **DATA CONFIDENTIALITY**, to protect against unauthorized disclosure of data. The data can be any information or messages that are transmitted over the network.
- **AUTHENTICATION**, used for authenticating the identity of a communicating peer entity and the source of received information. This service will be used to make sure that the two entities that are communicating with each other are who they claim they are.
- **DATA INTEGRITY**. These services counter the threat of accidental or intentional corruption of data. Accidental corruption may be the loss of a message or part thereof due to a break in the transmission media or faulty equipment. Intentional corruption may be the intentional duplication or deletion of whole or part of messages by unauthorised intruders.
- **NON-REPUDIATION**. Uses to protect against denial of receipt or origin of data and messages. This service ensures that a sender of a message cannot deny sending the message or deny the contents of the message. It also ensures that the receiver cannot deny receiving the message or the contents of the message.

- **ACCESS CONTROL.** Used for the protection against unauthorized use of resources accessible through a network.

In this step a desision must also be taken on which security mechanisms will be used to implement the selected security services. There are again a range of mechanisms available. Not all of these mechanisms needs to be selected.[10] Only three are needed to implement the majority of the services, these mechanisms are cryptography, electronic signatures and access control mechanisms.

P4.T4.S8. Design of security perimeters.

A Security perimeter are a logical boundary around a area in a network that can be trusted. It is not necessary to implement security services in these areas since security are assured by trusted personnel and equipment.[2] Those parts of the network outside the perimeters must be protected by security services as discussed under P4.T4.S2.

Security perimeters can be used in three ways:

- Perimeter around the whole network as seen in fig 5.1. Here the whole network are trusted and no special services need to be implemented.
- Perimeter around each application. In this case the whole network can't be trusted. Each application must therefore implement its own security services.
- Perimeter around top layers of architecture as seen in fig 5.B. In this case only parts of the network are untrusted. The perimeters are drawn around the trusted layers of the network architecture.

P4.T4.S10. Communications media.

In this step a decision must be made about the type of transmission media that will be used, or are used already in the network. The most used criteria for selecting transmission media has always been the cost of the media. This approach can lead to a number of problems when trying to implement security measures. Table 1 and table 2 gives an overview of the most important characteristics of some of the most used transmission media. Both these tables attempt to show the importance of security related characteristics.

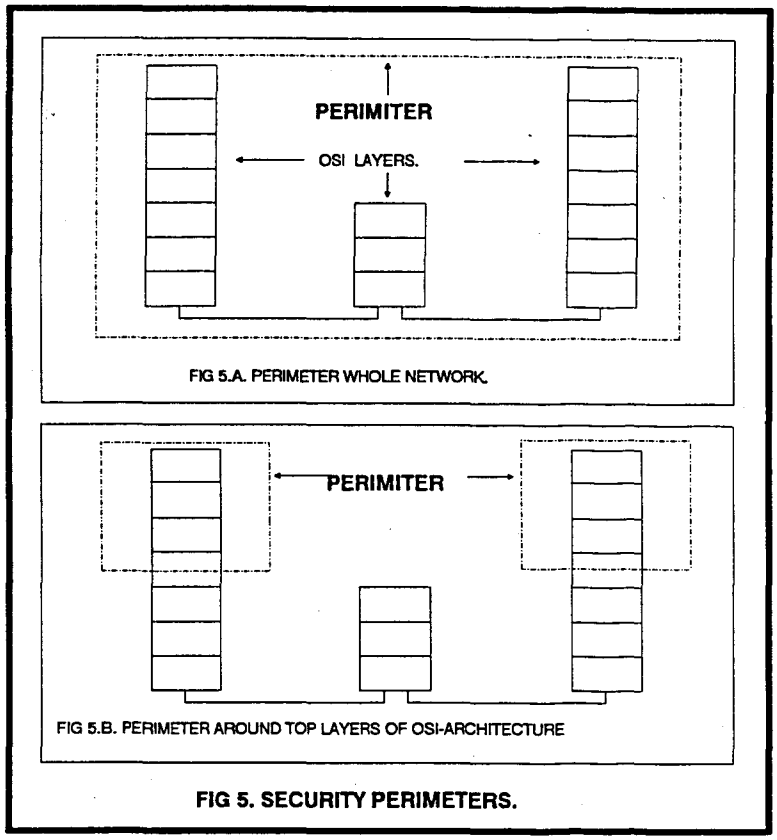


FIG 5.A. PERIMETER WHOLE NETWORK.

FIG 5.B. PERIMETER AROUND TOP LAYERS OF OSI-ARCHITECTURE

FIG 5. SECURITY PERIMETERS.

TABLE 1. CONDUCTED MEDIA.

	TWISTED PAIR (UNPROTECTED)	TWISTED PAIR (PROTECTED)	COAXIAL CABLE	OPTICAL CABLE
COST	VERY LOW	LOW	EXPENSIVE	VERY EXPENSIVE
BANDWIDTH	LOW	LOW	HIGH	VERY HIGH
INSOLATION	NONE	NONE - GOOD	GOOD	GOOD
RADIATION	VERY HIGH	AVERAGE	LOW	NONE
INFLUENCE ON SURROUNDINGS	VERY HIGH	HIGH (VARYING DEGREES)	LOW	NONE
INTEGRITY	BAD	BAD - AVERAGE	GOOD	VERY GOOD
CABLE WEIGHT	VERY HIGH	HIGH	HIGH	LOW
DANGER OF TAPPING	VERY HIGH	VERY HIGH	HIGH	VERY HIGH
EASE OF TAPPING	VERY EASY	EASY	DIFFICULT	VERY DIFFICULT
MAINTENANCE (FREQUENCY)	FREQUENTLY	FREQUENTLY	LESS FREQUENTLY	LOW

TABLE 2. RADIATED MEDIA.

	RADIO	MICROWAVE	SATELLITE	CELLULAR TELEPHONE
COST	LOW	HIGH	VERY HIGH	HIGH
BANDWIDTH	LOW	AVERAGE	HIGH	AVERAGE
RADIATION	VERY HIGH	LOW	HIGH	LOW
INFLUENCE ON SURROUNDINGS	VERY HIGH	LOW	LOW	HIGH
INTEGRITY	LOW	AVERAGE	GOOD	AVERAGE
THREAT OF TAPPING	VERY HIGH	HIGH	HIGH	VERY HIGH
EASE OF TAPPING	VERY EASY	DIFFICULT	DIFFICULT	VERY EASY
EXTENDABILITY	HIGH	HIGH	HIGH (EXPENSIVE)	LOW (FEW FREQUENCIES)

P4.T4.S11. Inter-network connection .

Because of the increase in network usage, the need for sharing resources on different networks also rises. This leads to the need for connecting different networks to each other.

This interconnection between planned and existing networks can lead to unexpected effects on network security. Special attention should be given in the planning and design of the connection point between the networks. Especially regarding the use of inter-network access rights, also discussed in the complete methodology under F4.T4.S11. Very important work in this area was done on "baggage collection".[11]

The idea of "baggage collection" works as follows. Any object that wants to get access to an object needs certain software and hardware components to satisfy the request. These components that are needed may for example be operating system software, networking software, cryptographic software, storage media of communications links. This means that there are a certain "access path" between the object and the subject.

In terms of the discussion in this paper, the object is the user that wants to send a message to a receiver, the object, by using the network. The route that the message must follow through the network is the access path. There may be a number of different access paths the object can use.

If the object's accesses to any of the components in the access path can be controlled, he can be forced to use a specific path or even be denied access to the subject. By associating with each object one or more selected paths, access to the object can be controlled by allowing only access to the object if the right access path are used.

The access paths associated with each object can be called the objects "Security profile". The software and hardware components making up the access path is called the "Baggage". If a subject tries to access a object, baggage is collected all along the access path. If the request reaches the object, the baggage is validated with the object's security profile, and access can be granted or refused.

This system is based on the "Path Context Model"(PCM) developed by Von Solms and Boshoff [11]. The system are so far only implemented for a microcomputer environment under the MS-DOS operating system. The next phase on development will be for using the PCM in networks. The authors are of opinion that the PCM system can be of great use in the field of inter-network rights.

There are three type of network interconnection methods:

- Bridge: Bridges are used to connect two networks using identical protocols.
- Router: Routers are used to connect networks that use different protocols, but where the same internet protocol are found in both the networks.
- Gateways: Gateways connect networks that use totally different protocols and architectures. The gateway application must translate each protocol package from the one protocol to the other.

Each of these methods have their own characteristics and must be studied for its effects on the planned network security measures.

4. CONCLUSION

The development and implementation of security requirements in organizations around the world have became major issues to be addressed. One of the main problems is that technology as well as the abilities of intruders are developing at an alarming rate. This means that security measures that are developed will not give protection for an indefinite time. For this reason, development and implementation of security countermeasures are an on-going proses as is shown in the high-level view of the IS-Methodology.

The aim of this paper was to show that communications and network security need additional attention if security measures are planned and implemented. For this purpose this paper gives special attention to the place of network security in the IS-Methodology.

BIBLIOGRAPHY.

[1] Barnstad D.K.
Considerations for security in the OSI architecture.
IEEE Network Magazine, April 1987. Vol. 2. No 1.

[2] Graft D, Pabrai M.
Methodology for Network Security Design.
IEEE Communications Magazine. NOV. 1990. Vol. 28. No 11.

[3] Badenhorst K.P, Eloff J.H.P.
Framework of a Methodology for the Life Cycle of Computer Security in an Organisation.
Computers & Security. 8(1989).
Elsivier Publishers LTD , England.

[4] Badenhorst K.P, Eloff J.H.P.
Managing Computer Security: Methodology and Policy.
Information Age. Vol. 12 No 4. OCT 1990.
Butterworth-Heinemann Ltd.

[5] Badenhorst K.P, Eloff J.H.P.
Computer Security Methodology.: Risk Analysis and Project Definition.
Computers & Security. 9(1990).

[6] Lobel J.
Proactive Network Risk Management.
IFIP/SEC'90 Proceedings.
Elsivier Publishers LTD , (North Holland) 1990.

[7] Pfleeger C.P.
Security in Computing.
Prentice-Hall Int Editions 1989.

[8] Davies D.W. Price W.L.
Security for Computer Networks: An Introduction to Data Security In Teleprocessing and EFT.
John Wiley & Sons. 2987.

[9] Black U.
Data Networks : Concepts, Theory and Practice.
Prentice-Hall. 1989.

[10] International Standard ISO 7498-2.
First Edition 1989-02-15.
Information Processing Systems- Open Systems Interconnection-Basic Reference Model.
Part 2. Security Architecture.

[11] Boshoff W.H, Von Solms S.H.
A Path Context Model for Addressing Security in Potentially Non-secure Environments.
Computers & Security. 8(1989).
Elsivier Publishers LTD , England.

AANHANGSEL 2.

LYS MET TERME : AFRIKAANS - ENGELS.

AFRIKAANS	ENGELS.
Aftap	Tap.
Aktiwiteitboekhouding	Activity log.
Bedryfstelsel	Operating system.
Betroubaa	Trusted.
Brug	Bridge.
Deurgang	Gateway.
Draersein	Carrier signal.
Elektroniese Data Oordrag	Electronic Data Interchange (EDI).
Gebruiker	User.
Gedifferensieerde toegangsregte	Differensiated access rights.
Herhalers	Repeaters.
Identiteitverifikasie	Identity verification
Internetwerkskakeling	Inter-network connection.
Kommunikasieverbindings	Communications media.
Koaksialekabel	Coaxial cable.
Kriptografie	Cryptography.
Metodologie	Methodology.
Netwerksekerheid	Network security.
Nodus	Node.
Nodi	Nodes.
Objek	Object.
Onderhandelde sekerheid	Negotiated security.
Ontvange	Receiver.
Optiesevesel	Optical fiber.
OSI-Sekreheidsbuitelyn	OSI Security perimeter.
OSI-Verwysingsmodel	OSI Referance model.
Pad-Konteksmodel	Path Context Model.
Poortbeskerming	Port protection.
Publieke sleutel	Public key.
Roeteerder	Router.
Sekerheid	Security.
Sekerheidsbuitelyn	Security perimeter.
Sekerheidsdiens	Security service.
Skakelenkripsie	Link encryption.
Sleutelbestuur	Key management.

AFRIKAANS	ENGELS.
Slimkaart	Smartcard.
Stuurder	Sender.
Subjek	Subject.
Toegang	Access.
Toegangspoort	Gateway.
Uitstralingsverbinding	Radiated media.
Waarmerking	Authentication.
Wagwoord	Password.
Wyeareanetwerk	Wide Area Network.

BIBLIOGRAFIE.

[1] AMSEL E.
"NETWORK SECURITY AND ACCESS CONTROLS."
COMPUTERS & SECURITY, 7(1988).

[2] LOOMIS M.E.S.
"DATA COMMUNICATIONS."
PRENTICE-HALL INC, 1983.

[3] LONG L.
"INTRODUCTION TO COMPUTERS AND INFORMATION PROCESSING."
PRENTICE-HALL INC, 1984.

[4] HIGHLAND H.J.
"NETWORK COMMUNICATION MANAGEMENT."
"RANDOM BITS & BYTES"
COMPUTERS & SECURITY, 8 (1989).

[4] BRUSIL P.J. ,STOKESBERRY D.P.
"TOWARD A UNIFIED THEORY OF MANAGING LARGE NETWORKS."
IEEE SPECTRUM, APRIL 1989.

[5] KLERER S.M.
"THE OSI MANAGEMENT ARCHITECTURE: AN OVERVIEW."
IEEE NETWORK, MAART 1988, VOL 2 NO 2.

[6] FERIDUN M. ,LIEB M. ,NODINE M. en ONG J.
"ANM : AUTOMATED NETWORK MANAGEMENT SYSTEM."
IEEE NETWORK, MAART 1988, VOL 2 NO 2.

[7] ABRAMS M.D. en JENG A.B.
"NETWORK SECURITY : PROTOCOL REFERENCE MODEL AND TRUSTED
COMPUTER SYSTEM EVALUATION CRITERIA."
IEEE NETWORK, APRIL 1987. VOL 1 NO2.

[8] BARNSTAD D.K.
"CONSIDERATIONS FOR SECURITY IN THE OSI ARCHITECTURE."
IEEE NETWORK. APRIL 1987. VOL 2, NO 1.

[9] BLACK U.D.
"DATA COMMUNICATIONS AND DISTRIBUTED NETWORKS."
PRENTICE-HALL INC. 1987.

[10] PFLEEGER.
"SECURITY IN COMPUTING."
PRENTICE-HALL INTERNATIONAL EDITIONS. 1989.

[11] CLAASEN G.J.
"IMPLEMENTATION OF SECURITY MEASURES IN HIGHER LAYER PROTOCOLS."
VERRIGTINGE, INFOSEK KONFERENSIE WNNR. 1990.

[12] Onderhoude met personeel verbonde aan SASOL GID :
Struwig D.
Zylstra C.
Roodt J.

[13] Onderhoud met Mnr G. Cardon van GENCOR GIS.

[14] TERPLAN C.
"COMMUNICATIONS NETWORK MANAGEMENT.".
PRENTICE-HALL INTERNATIONAL. 1987.

[15] FULLARD R.
"CRYPTOGRAPHIC KEY MANAGEMENT."
VERRIGTINGE, INFOSEK KONFERENSIE WNNR 1990.

[16] DAVIES D.W., PRICE W.L.
"SECURITY FOR COMPUTER NETWORKS : AN INTRODUCTION TO
DATA SECURITY IN TELEPROCESSING AN EFT".
JOHN WILEY & SONS. 1987.

[17] GEE K.C.E.
"INTRODUCTION TO LOCAL AREA NETWORKS."
MACMILLAN PUBLISHERS. LONDON. 1983.

[18] STALLINGS W.
"WHEN ONE LAN IS NOT ENOUGH."
BYTE. JAN 1989. PRENTICE-HALL.

[19] NANCE B.
"EVERYONE INTO THE POOL."
BYTE. NOV 1989. PRENTICE-HALL.

[20] APIKI S., DIEHL S., GREHAN R.
"BATTLE OF THE NETWORK STARS."
BYTE. JULY 1989. PRENTICE-HALL.

[21] VAN NAME M.L., CATCHINGS B.
"THE LAN ROAD TO OSI."
BYTE. 1989. PRENTICE-HALL.

[22] KEISER G.E.
"LOCAL AREA NETWORKS."
Mc GRAW-HILL BOOK COMPANY. 1989.

[23] FOLTS H.
"OPEN SYSTEMS STANDARDS."
IEEE NETWORK MAGAZINE.
JAN 1987. VOL1 NO1.

[24] BURROWS B.C. ,MAYNE A.J.
"OPEN SYSTEMS INTERCONNECTION."
"STATE OF THE ART REPORT."
PERGAMON INFOTECH LTD. 1987.

[25] STALLINGS W.
"BUISINESS GUIDE TO LOCAL AREA NETWORKS."
HOWARD W. SAMS AND COMPANY. 1990.

[26] STAMPER W.
"BUISINESS DATA COMMUNICATIONS." 2ND ED.
ADDISON WESLEY. 1989.

[27] ELLIOTT L.
"HUNT FOR THE HACKER SPY."
READERS DIGEST. MAY 1990.
READERS DIGEST ASSOCIATION SOUTH AFRICA(PTY)LTD.

[28] MURRAY G. (ED)
"SECURITY."
DATA COMMUNICATIONS : ANALYSIS.
"STATE OF THE ART REPORT."
PERGAMON INFOTECH LTD. 1980.

[29] PRICE W.L.
"DATA SECURITY IN COMMUNICATIONS NETWORKS."
DATA COMMUNICATIONS : INVITED PAPERS.
"STATE OF THE ART REPORT."
PERGAMON INFOTECH LTD. 1980.

[30] ETTINGER J.E.
"TRANSMISSION MEDIA OF THE FUTURE."
"STATE OF TE ART REPORT."
PERGAMON INFOTECH LTD. 1984.

[31] KEENAN T.
"EMERGING VULNERABILITIES IN OFFICE AUTOMATION ECURITY."
COMPUTERS & SECURITY, 8 (1989).

[32] HELD G.
"UNDERSTANDING DATA COMMUNICATIONS." 2nd ED
HOWARD W.SAMS & CO. 1988.

[33] CURTIS C. , MAJHOR D.L.
"MODEM CONNECTIONS BIBLE."
THE WAITE GROUPE, INC. 1985.

[34] BLACK U.
"DATA NETWORKS. CONCEPTS, THEORY AND PRACTICE."
PRENTICE-HALL, INC. 1989.

[35] KUMMERLE K, LIMB J.O., TOBAGI F.A.
"ADVANCES IN LOCAL AREA NETWORKS"
IEEE PRESS, 1978.

[36] GREEN P.E.
"NETWORK INTERCONNECTION AND PROTOCOL CONVERSION."
IEEE PRESS, 1988.

[37] MASARANI R., KEENAN T.P.
"SECURITY AND PRIVACY IN CELLULAR TELEPHONE SYSTEMS."
IFIP 1984 PROCEEDINGS.
ELSEVIER SCIENCE PUBLISHERS B.V. (NORTH-HOLLAND) 1984.

[38] COX D.C.
"PORTABLE DIGITAL RADIO COMMUNICATIONS- A APPROACH TO TETHERLESSACCESS."
IEEE COMMUNICATIONS MAGAZINE. JULY 1989.

[39] SMULDERS P.
"THE THREAT OF INFORMATION THEFT BY RECEPTION OF ELECTROMAGNETIC RADIATION FROM RS-323 CABLES."
COMPUTERS & SECURITY, 9 (1990).

[40] DREXHAGE M.G., MOYNIHAN C.T.
"INFRARED OPTICAL FIBERS."
SCIENTIFIC AMERICAN, NOV 1988.

[41] BRYCE Y.B.
"FIBER VS. METAL."
BYTE. JAN 1989. PRENTICE-HALL.

[42] TRISCHITTA P.R., CHEN D.T.S.
"REPEATERLESS UNDERSEA LIGHTWAVE SYSTEMS."
IEEE COMMUNICATIONS MAGAZINE. MARCH 1989.

[43] GOLDING L.G., VITERBI A.J.
"VSATs: EXPERT VIEWS ON FUTURE TRENDS."
IEEE COMMUNICATIONS MAGAZINE. MAY 1989.

[44] GLASS L.B.
"THE LIGHT AT THE END OF THE LAN."
JULY 1989. BYTE, PRENTICE-HALL.

[45] HUTCHINSON G., DESMOND C.L.
"ELECTRONIC DATA INTERCHANGE."
IEEE NETWORK.
OCTOBER 1987. VOL 1. NO4.

[45] HSIE W., GITMAN I.
"ROUTING STRATEGIES IN COMPUTER NETWORKS."
COMPUTER. JUN 1984.

[46] CASE J.D., DAVIN J.
"INTRODUCTION TO THE SIMPLE GATEWAY MONITORING PROTOCOL."
IEEE NETWORK.
MARCH 1988. VOL 2 NO2.

[47] RAPPAPORT T.S.
"INDOOR RADIO COMMUNICATIONS FOR FACTORYS OF THE FUTURE."
IEEE COMMUNICATIONS MAGAZINE.
MAY 1989.

[48] STREMLER F.G.
"INTRODUCTION TO COMMUNICATION SYSTEMS."
ADDISON-WESLEY PUBLISHING COMPANY.
1982.

[49] SHANMUGAM K.S.
"DIGITAL AND ANALOG COMMUNICATION SYSTEMS."
JOHN WILEY & SONS, INC.
1985.

[50] CANNON D.L., LUECKE G.
"UNDERSTANDING COMMUNICATIONS SYSTEMS."
HOWARD W. SAMS & CO.
1989.

[51] GRILLO D.
"FUTURE PAN-EUROPEAN LAND MOBILE RADIO SYSTEM -
ARCHITECTURE AND PERFORMANCE ISSUES."
NIE GEPUBLISEER.

[52] MNR DIPPENAAR
SAPT. PRETORIA.
ONDERHOUD.

[53] HIGHLAND J.H.
"HOW SECURE ARE FIBER OPTIC COMMUNICATIONS?"
COMPUTERS & SECURITY, 7(1988).

[54] HIGHLAND J.H.
"TAPPING FIBER-OPTIC CABLES.
COMPUTERS & SECURITY, (1989).

[55] SCHNEIDEWIND N.F.
"INTERCONNECTING LOCAL NETWORKS TO LONG-DISTANCE NETWORKS."
IEEE COMPUTER.
SEPT 1983. VOL 16 NO 9.

[56] BENHAMOU E. ,ESTRIN J.
"MULTILEVEL INERNETWORKING GATEWAYS : ARCHITECTURE AND APPLICATIONS."
IEEE COMPUTER.
SEPT 1983. VOL 16 NO 9.

[57] HINDEN R., HAVERTY J., SHELTZER A.
"THE DARPA INTERNET : INTERCONNECTING HETEROGENEOUS COMPUTER NETWORKS WITH GATEWAYS."
IEEE COMPUTER.
SEPT 1983. VOL 16 NO 9.

[58] SEIFERT W.
"BRIDGES AND ROUTERS."
IEEE NETWORK MAGAZINE.
JAN 1988. VOL 2. NO1.

[59] BEHAMOU E.
"INTEGRATING BRIDGES AND ROUTERS AN A LARGE INTERNETWORK."
IEEE NETWORK MAGAZINE.
JAN 1988. VOL 2. NO1.

[60] GERLA M., KLEINROCK L.
"CONGESTION CONTROL IN INTERCONNECTED LANs."
IEEE NETWORK MAGAZINE.
JAN 1988. VOL 2. NO1.

[61] INTERNATIONAL STANDERD ISO 7498-2.
FIRST EDITION 1989-02-15.
INFORMATION PROCESSING SYSTEMS - OPEN SYSTEMS
INTERCONNECTION - BASIC REFERENCE MODEL.
PART 2. SECURITY ARCHITECTURE.

[62] STRAUSS K.S.G.
ELEKTRONIESE SEKERHEIDSASPEKTE VAN ELEKTROMAGNETIESE UITSTRALING.
PROCEEDINGS INFOSEK KONFERENSIE WNNR. 1990.

[63] WRIGHT P.
"TO CATCH A SPY."
WILLIAM HEINEMAN AUSTRALIA. 1988.

[64] W.H. BOSHOFF, DR S.H. VON SOLMS.
"A PATH CONTEXT MODEL FOR ADDRESSING SECURITY IN
POTENTIALY NON SECURE ENVIRONMENTS."
PROCEEDINGS INFOSEK KONFERENSIE WNNR. 1990.

[65] G.A. CASSIDY, G.W. ROLFE.
"BIOMETRIC VERIFICATION FOR ACCESS CONTROL."
PROCEEDINGS INFOSEK KONFERENSIE WNNR. 1990.

[66] JOBUSCH D.L., OLDEHOEFT A.E.
"A SURVEY OF PASSWORD MECHANISMS : WEAKNESSES AND
POTENTIAL IMPROVEMENTS. PART 1."
COMPUTERS & SECURITY, 8(1989)

[67] JOBUSCH D.L., OLDEHOEFT A.E.
"A SURVEY OF PASSWORD MECHANISMS : WEAKNESSES AND
POTENTIAL IMPROVEMENTS. PART 2."
COMPUTERS & SECURITY, 8(1989)

[68] WEISS J.
"FIVE WAYS TO SECURE YOUR NETWORK."
TELECOMMUNICATIONS PRODUCTS AND TECHNOLOGY. SEPT 1990.

[69] BROWN L.R.
"COMPUTER SYSTEM ACCESS CONTROL USING PASSWORDS."
IFIP 1984 PROCEEDINGS.
ELSEVIER SCIENCE PUBLISHERS B.V. (NORTH-HOLLAND) 1984.

[70] STEINAUER D.D.
"SECURITY GUIDLINES FOR THE MANAGEMENT OF PERSONAL
COMPUTING SYSTEMS."
IFIP 1984 PROCEEDINGS.
ELSEVIER SCIENCE PUBLISHERS B.V. (NORTH-HOLLAND) 1984.

[71] LOBEL J.
"PROACTIVE NETWORK RISK MANAGEMENT."
IFIP 1990 PROCEEDINGS.
ELSEVIER SCIENCE PUBLISHERS B.V. (NORTH-HOLLAND) 1990.

[72] PARKER D.B.
"SEVENTEEN INFORMATION SECURITY MYTHS DEBUNKED."
IFIP 1990 PROCEEDINGS.
ELSEVIER SCIENCE PUBLISHERS B.V. (NORTH-HOLLAND) 1990.

[73] SOBOL M.I.
"SECURITY CONSERNS IN IN A LOCAL AREA NETWORK
ENVIRONMENT."
TELECOMMUNICATIONS. MAART 1988.

[74] WOOD C.C..
"PLANNING: A NEW MEANS TO ACHIEVE DATA COMMUNICATIONS SECURITY."
COMPUTERS & SECURITY, 8(1989)

[75] JAMIESON R., LOW G.
"SECURITY AND CONTROL ISSUES IN LOCAL AREA NETWORK DESIGN."
COMPUTERS & SECURITY, 8(1989)

[76] MENKUS B.
"UNDERSTANDING DATA COMMUNICATIONS SECURITY VULNERABILITIES."
COMPUTERS & SECURITY, 9(1990)

[77] HIGHLAND H.J.
"NETWORK COMMUNICATIONS SECURITY."
"RANDOM BITS AND BYTES."
COMPUTERS & SECURITY, 8(1989)

[78] OLSEN F.
"SECURITY BREACHES UP DRAMATICALLY ON MILNET."
GOVERNMENT COMPUTER NEWS. 11 DEC 1989.

[79] LUNT T.F.
"ACCESS CONTROL POLICIES: SOME UNANSWERED QUESTIONS."
COMPUTERS & SECURITY, 8(1989)

[80] SPECIAL REPORT.
"NEW LOCKS AND KEYS FOR ELECTRONIC INFORMATION."
COMPUTERS & SECURITY, 7(1988)

[81] MENKUS B.
"PHYSICAL SECURITY: SELECTING AN ACCESS CONTROL SYSTEM."
COMPUTERS & SECURITY, 8(1989)

[82] ZAJAC B.P.
"DIAL-UP COMMUNICATION LINES: CAN THEY BE SECURED?"
COMPUTERS & SECURITY, 7(1988)

[83] MADSEN C.W.
"THE WORLD MMEGANETWORK AND TERRORISM."
COMPUTERS & SECURITY, 7(1988)

[84] ABRAMS M.D.
"OBSERVATIONS ON LOCAL AREA NETWORK SECURITY."
"TUTORIAL COMPUTER AND NETWORK SECURITY."
IEEE COMPUTER SOCIETY PRESS. 1986.

[85] WOOD C.C.
"PLANNING AS A MEANS TO ACHIEVE APPROPRIATE DATA COMMUNICATIONS SECURITY."
PROCEEDINGS IFIP SEC 1990.

[86] HABER L.
"BALANCING NETWORK OPTIONS."
DATAMATION. AUG 1, 1989.

[87] FITZGERALD K.
"THE QUEST FOR INTRUDER-PROOF COMPUTER SYSTEMS."
IEEE SPECTRUM. AUGUST 1989.

[88] BAIRD L.L.
"SENSIBLE NETWORK SECURITY."
DATAMATION, 31 (3) (1985).

[89] HIGHLAND J.H.
"HOW TO EVALUATE MICROCOMPUTER ENCRYPTION SOFTWARE AND HARDWARE."
COMPUTERS & SECURITY 6(1987).

[90] CHRISTOFFERSON P., ET AL.
"CRYPTO USERS' HANDBOOK."
NORTH-HOLLAND. 1988.

[91] SEBERRY J., PIEPRZYK.
"CRYPTOGRAPHY. AN INTRODUCTION TO COMPUTER SECURITY."
PRENTICE-HALL OF AUSTRALIA PTY LTD. 1989.

[92] HELLMANN M.E.
"COMMERCIAL ENCRYPTION."
IEEE NETWORK MAGAZINE. APRIL 1987.

[93] KENT S.
"COMMENTS ON SECURITY PROBLEMS IN THE TCP/IP PROTOCOL SUITE."
COMPUTER COMMUNICATIONS REVIEW 19 (2), MARCH 1989.

[94] NOVELL NetWare HANDLEIDINGS.
NOVELL INC.
PROVO UTAH V.S.A. 1988.

[95] HIGHLAND H.J.
"US ENCRYPTION UNDER FIRE."
COMPUTER FRAUD & SECURITY. NOV 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[96] MENKUS B.
"US GOVERNMENT ISSUES PUBLIC KEY ENCRYPTION STANDARD."
COMPUTER FRAUD & SECURITY. NOV 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[97] WONG K.
"COMPUTER RELATED FRAUD."
"A SURVAY OF THE BIS CASEBOOK."
COMPUTER FRAUD & SECURITY. NOV 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[98] HIGHLAND J.H.
"HOW SECURE IS YOUR NETWORK?."
COMPUTERS & SECURITY 9(1990).

[99] HIGHLAND J.H.
"NOTES ABOUT RSA."
COMPUTERS & SECURITY 9(1990).

[100] MADSEN W.
"COMPUTER SECURITY : PERISTROIKA STYLE."
"AN OVERVIEW OF PROBLEMS IN THE EASTERN BLOCK."
COMPUTER FRAUD & SECURITY. OCT 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[101] MENKUS B.
"WHY DATA COMMUNICATIONS ARE INSECURE.."
COMPUTERS & SECURITY 9(1990).

[102] HUGHES T.
"SECURING NETWORKS."
"SUPPLIERS VIEW."
COMPUTER FRAUD & SECURITY. APRIL 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[103] ZAJAC B.P.
"THE 1990s - WHAT WILL THEY HOLD."
COMPUTERS & SECURITY 9(1990).

[104] "AN INTRODUCTION TO LOCAL AREA NETWORKS."
ISM INFORM.
PUBLICATION OF PUBLIC AFFAIRS AND COMMUNICATIONS DEPARTMENT OF ISM.
AUGUST 1990.

[105] WAINAPEL A.
"FDDI : APPLICATIONS."
COMPUTER WEEK.
VOL 13 NO 34. 27 AUGUST 1990.
SYSTEMS PUBLISHERS (PTY) LTD.

[106] VAN GRAAN S.
"GATEWAY FLEXIBILITY."
ISM INFORM.
AUGUST 1990.

[107] CHRISTOFFERSON P.
"MESSAGE AUTHENTICATION AND ENCRYPTION COMBINED."
COMPUTERS & SECURITY, 7(1988)
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[108] HELLMAN M.E.
"THE MATHEMATICS OF PUBLIC-KEY CRYPTOGRAPHY."
SCIENTIFIC AMERICAN.
AUGUST 1979.

[109] WALKER S.T.
"NETWORK SECURITY OVERVIEW."
"TUTORIAL COMPUTER AND NETWORK SECURITY."
IEEE COMPUTER SOCIETY PRESS. 1986.

[110] NEL G.
"BRIDGES AND ROUTERS."
ISM INFORM.
AUGUST 1990.

[111] "ANNOUNCING IBM S/390: FOR THE 90s AND BEYOND."
ISM INFORM.
SEPTEMBER 1990.

[112] "CRYPTOGRAPHY : ENCRYPTION AND AUTHENTICATION."
"TUTORIAL COMPUTER AND NETWORK SECURITY."
IEEE COMPUTER SOCIETY PRESS. 1986.

[113] HUGHES T.
"SECURING NETWORKS."
"SUPPLIERS VIEW."
COMPUTER FRAUD & SECURITY. APRIL 1990.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[114] VAN HEURCK P.
"TRASEC : BELGIAN SECURITY SYSTEM FOR ELECTRONIC FUNDS TRANSFER."
COMPUTERS & SECURITY. 6(1987).

[115] JOHNSTONE R.J.
"KEY UPDATING FLAGS IN EFT-POS SECURITY SYSTEMS."
COMPUTERS & SECURITY. 6(1987).

[116] RUSHBY J..
"NETWORKS ARE SYSTEMS : A DISCUSSION PAPER."
"TUTORIAL COMPUTER AND NETWORK SECURITY."
IEEE COMPUTER SOCIETY PRESS. 1986.

[117] KAK S.C.
"DATA SECURITY IN COMPUTER NETWORKS."
IEEE COMPUTER. FEBRUARY 1983.

[118] GREENLEE M.B.
"REQUIREMENTS FOR KEY MANAGEMENT PROTOCOLS IN THE
WHOLESALE FINANCIAL SERVICES."
IEEE COMMUNICATIONS MAGAZINE. SEPT 1985.

[119] SHAIN M.
"SECURITY IN ELECTRONIC FUNDS TRANSFER : MESSAGE INTEGRITY IN MONEY TRANSFER AND BOND SETTLEMENTS THROUGH GE INFORMATION SERVICES GLOBAL NETWORK."
COMPUTERS & SECURITY. 8(1989)..
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[120] JUENEMAN R.R.
"ELECTRONIC DOCUMENT AUTHENTICATION."
"TUTORIAL COMPUTER AND NETWORK SECURITY."
IEEE COMPUTER SOCIETY PRESS. 1986.

[121] BADENHORST K.P.
'n METODOLOGIE VIR IMPLIMENTERING VAN REKENAARSEKERHEID IN 'n GROOT ONDERNEMING.
PROEFSKRIF, RANDSE AFRIKAANSE UNIVERSITEIT. MEI 1990.

[122] RASMUSSEN O.S.
"COMMUNICATIONS AND NETWORK PROTECTION : PRACTICAL EXPERIENCES."
PROCEEDINGS COMPUTER SECURITY CONFERENCE.
IFIP 1985.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[123] WEBER R.
"CONTROLS IN ELECTRONIC FUNDS TRANSFER SYSTEMS : A SURVEY AND SYNTHESES."
COMPUTERS & SECURITY. 8(1989)..
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[124] VON SOLMS S.H.
"DIGITAL SIGNATURES FOR SECURE DATA."
SOUTH AFRICAN JOURNAL OF SCIENCE. VOL 85.
JANUARY 1989.

[125] BADENHORST K.P. ELOFF J.H.P..
"FRAMEWORK OF A METHODOLOGY FOR THE LIFE CYCLE OF COMPUTER SECURITY IN AN ORGANIZATION."
COMPUTERS & SECURITY. 8(1989)..
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[126] VAN ZYL P.W.J, VON SOLMS A.H.
" A MICROCOMPUTER IMPLEMENTATION OF THE PATH CONTEXT MODEL."
VERRIGTINGE VAN DIE VYFDE NASIONALE KONFERENSIE VIR MEESTERS EN PhD REKENAARWETENSKAPSTUDENTE.
30 AUGUSTUS 1990.
PUBLIKASIEREEKS UNIVERSITEIT PORT ELIZABETH.

[127] WORTHINGTON T.K, CHAINER T.J, WILINFORD J.D.
"IBM DINAMIC SIGNATURE VERIFICATION."
PROCEEDINGS COMPUTER SECURITY CONFERENCE.
IFIP 1985.
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[128] BADENHORST K.P. ELOFF J.H.P..
"MANAGING COMPUTER SECURITY : METHODOLOGY AND POLICY."
INFORMATION AGE. VOL 12 NO 4. OCT 1990.
BUTTERWORTH-HEINEMANN LTD.

[129] GRAFT D, PABRAI M.
"METHODOLOGY FOR NETWORK SECURITY DESIGN."
IEEE COMMUNICATIONS MAGAZINE.
VOL 28 NO 11. NOV 1990.

[130] PIERSON L.G., WITZKE E.L.
"A SECURITY METHODOLOGY FOR COMPUTER NETWORKS."
AT&T TECHNICAL JOURNAL.
MAY/JUN 1988.

[131] BADENHORST K.P. ELOFF J.H.P..
"COMPUTER SECURITY METHODOLOGY : RISK ANALYSES AND PROJECT DEFINITION."
COMPUTERS & SECURITY. 9(1990)..
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.

[132] BOSHOFF W.H, VON SOLMS S.H.
"A PATH CONTEXT MODEL FOR ADDRESSING SECURITY IN POTENTIALLYNON-SECURE ENVIRONMENTS."
COMPUTERS & SECURITY. 8(1989)..
ELSEVIER SCIENCE PUBLISHERS LTD, ENGLAND.