(19) Bureau voor de Industriële Eigendom Nederland

(11) 1015389

(12) C OCTROOI[20]

(21) Aanvrage om octrooi: 1015389

(22) Ingediend: 07.06.2000

(51) Int.Cl.[7] H04L29/14, H04L29/06, H04L12/26

(41) Ingeschreven: 10.12.2001

(47) Dagtekening: 10.12.2001

(45) Uitgegeven: 01.02.2002 I.E. 2002/02

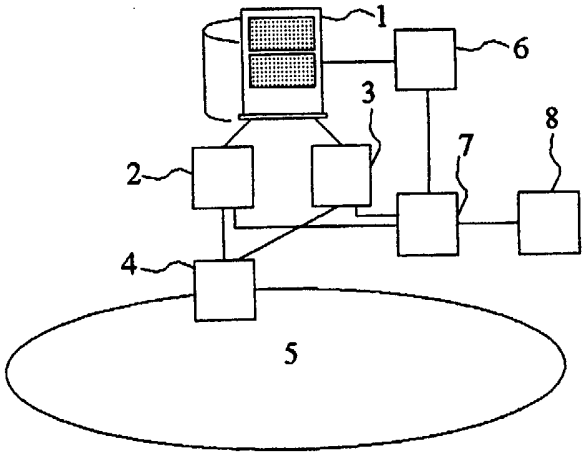
(73) Octrooihouder(s): Koninklijke KPN N.V. te Groningen.

(72) Uitvinder(s): Willem Pieter Dijkstra te Groningen
Ate Sander van Steenbergen te Groningen

(74) Gemachtigde: Drs. B. Klein te 2509 CH Den Haag.

(54) Methode en systeem voor het beveiligen van een datasysteem.

(57) Methode en systeem voor het beveiligen van een datasysteem (1) dat door verbindingsmiddelen (5) in verbinding staat met andere systemen en via die verbindingsmiddelen data uitwisselt met die andere systemen. In bufferorganen (2,3) wordt doorlopend de meest recente uitgewisselde data gebufferd. De normale werking van het datasysteem wordt bewaakt door een bewakingsorgaan (6), dat bij abnormaliteit in de werking van het datasysteem een uitvoerorgaan (7) activeert om de gebufferde data uit de bufferorganen uit te lezen en voor analyse ter beschikking te stellen.



NL C 1015389

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

Methode en systeem voor het beveiligen van een datasysteem

ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een methode voor het beveiligen van een datasysteem dat door verbindingsmiddelen in verbinding staat met andere systemen en via die verbindingsmiddelen data uitwisselt met die andere systemen. De uitvinding betreft tevens een beveiligingssysteem voor het bewaken van een datasysteem dat via verbindingsmiddelen data met andere systemen uitwisselt.

Huidige (internet) security tools kunnen alleen bekende aanvallen tegen een datasysteem identificeren. Onbekende aanvallen worden niet geïdentificeerd en kunnen diensten onklaar maken. Zogeheten "network sniffers" kunnen al het verkeer op een netwerk loggen. Door toename van de bandbreedtes in de netwerken leveren sniffers echter een enorme hoeveelheid informatie en het onderzoeken van al het gesnifte verkeer bij aankomst wordt hierdoor onmogelijk.

"Intrusion Detection Systems" zijn tools die boven op een sniffer in real-time netwerk stromen proberen te correleren op zoek naar aanvallen. Nadelen: door de toenamen van de snelheden en bandbreedtes op netwerken worden deze tools steeds moeilijker inzetbaar. Met gigabit netwerk snelheiden zijn er geen systemen meer die dit aankunnen.

SAMENVATTING VAN DE UITVINDING

De onderhavige uitvinding berust op het inzicht dat pas op het moment dat een datasysteem disfunctioneert, bijvoorbeeld als gevolg van een "data-attack" het van belang is dat de laatste communicatie met de server bewaard wordt (vergelijk een "black box" in vliegtuigen). Deze bewaarde communicatie kan dan worden gebruikt om de oorzaak van het disfunctioneren te analyseren en vast te stellen en een eventuele nieuwe attack te identificeren en het datasysteem er tegen te beveiligen.

De methode volgens de uitvinding wordt erdoor gekenmerkt dat voortdurend (alleen) de meest recente uitgewisselde data gebufferd wordt, dat de normale werking van het datasysteem bewaakt wordt en dat (alleen) bij een abnormaliteit in de werking van het datasysteem de gebufferde data voor analyse ter beschikking wordt gesteld. Over de uitgewisselde (binnenkomende en/of uitgaande) datastroom wordt als het ware een "moving window" gezet, waarvan de inhoud normaliter niet wordt bewerkt (geanalyseerd). Pas na het constateren van een abnormaliteit in de werking van het te beveiligen datasysteem wordt de inhoud van de moving window bewaard en kan die geanalyseerd worden. De uitvinding lost dus het probleem van de grote hoeveelheid informatie en de beperkte analysetijd op door niet continue te

analyseren maar dat alleen te doen als het nodig is.

UITVOERINGSVOORBEELDEN

De methode volgens de uitvinding wordt geïllustreerd met behulp van figuur 1. Figuur 1 toont een datasysteem 1, voorzien van een invoerbufferorgaan 2 en een uitvoerbufferorgaan 3, door middel waarvan het datasysteem 1 verbinding maakt met de node 4 van een netwerk 5 waarop andere (data)systemen kunnen zijn aangesloten, waarmee het datasysteem 1 data uitwisselt. Het datasysteem wordt beveiligd doordat de meest recente uitgewisselde data gebufferd wordt in de bufferorganen 2 en 3. De normale werking van het datasysteem 1 wordt bewaakt in een bewakingsorgaan 6. Het bewakingsorgaan 6 bestuurt een uitvoerorgaan 7 zodanig dat alleen bij een abnormaliteit in de werking van het datasysteem de in de bufferorganen 2 en 3 gebufferde, meest recente data door het uitvoerorgaan 7 worden opgevraagd. Het uitvoerorgaan 7 kan een beeldscherm omvatten waarop, nadat een storing in het datasysteem is opgetreden, de uit de buffers 2 en 3 opgevraagde data kunnen worden bekeken. Ook kan het uitvoerorgaan 7 een printer omvatten. Over de uitgewisselde (binnenkomende en/of uitgaande) datastroom wordt als het ware een "moving window" gezet, waarvan de inhoud normaliter niet wordt bewerkt. Pas na het constateren van een abnormaliteit in de werking van het te beveiligen datasysteem wordt de inhoud van de moving window (in de bufferorganen 2 resp. 3) bewaard en kan die geanalyseerd worden. Analyse van de in de laatste ogenblikken voor de storing uitgewisselde data kan "op het oog" geschieden, door gekwalificeerd personeel. Ook kan -evnetueel aanvullend- gebruik worden gemaakt van een analysesysteem 8.

Opgemerkt wordt dat het beveiligen van het datasysteem 1 ook -bijvoorbeeld via het netwerk 5- op afstand kan worden gerealiseerd, zoals figuur 2 toont. In figuur 2 zijn de nodige connecties tussen de enerzijds de organen 1, 2 en 3 en anderzijds de organen 6 en 7 via de netwerknode 4 en een netwerknode 9 gerealiseerd. Uiteraard worden die connecties, afhankelijk van het netwerk, bij voorkeur gerealiseerd door virtuele kanalen. De organen 6, 7 en 8 kunnen deel uitmaken van een beveiligingsserver 10, zoals figuur 3 toont, die een groot aantal datasystemen 1 kan monitoren. Het gedrag van de te beveiligen datasystemen 1 wordt real time gemonitored vanaf beveiligingsserver 10, die informatie ontvangt van de te beschermen datasystemen 1. Indien een datasysteem 1 afwijkend gedrag vertoont, wordt de inhoud van de bufferorganen 2 en 3 door de beveiligingsserver "afgetapt" en onderzocht, al dan niet met behulp van geautomatiseerde analysemiddelen zoals orgaan 8 in figuur 2.

Opgemerkt wordt dat, waar in het bovenstaande twee bufferorganen, 2 en 3, worden voorgesteld, één voor inkomende data en één voor uitgaande data, deze functies in de praktijk ook kunnen worden uitgevoerd door één invoer/uitvoer-buffer. Bij het optreden van een calamiteit in de werking van het datasysteem 1 wordt die I/O-buffer dan uitgelezen en de daarin op dat moment aanwezige communicatiedata aan het orgaan 7 ter beschikking gesteld.

Afwijkend gedrag van een datasysteem 1 kan bijvoorbeeld zijn: een karakteristieke grootheid wijkt van zijn statistische waarde, een piekbelasting, een continue zeer hoge belasting, het vollopen van een harddisk, het onderuitgaan van lopende processen, etc.

De analyse zou gebruikt kunnen worden voor:

* Forensische onderzoek en het oplossen van schuldvragen etc.
* Identificeren van (onbekende) "netwerkaanvallen"; de verkregen informatie kan daarna gebruikt worden om de datasystemen nog beter te beschermen.

CONCLUSIES

1. Methode voor het beveiligen van een datasysteem dat door verbindingsmiddelen in verbinding staat met andere systemen en via die verbindingsmiddelen data uitwisselt met die andere systemen, MET HET KENMERK DAT doorlopend de meest recente uitgewisselde data gebufferd wordt, dat de normale werking van het datasysteem bewaakt wordt en dat bij een abnormaliteit in de werking van het datasysteem de gebufferde data voor analyse ter beschikking wordt gesteld.

2. Beveiligingssysteem voor het bewaken van een datasysteem (1) dat via verbindingsmiddelen (5) data met andere systemen uitwisselt, GEKENMERKT DOOR buffermiddelen (2,3) voor het doorlopend bufferen van de door het datasysteem meest recentelijk uitgewisselde data en door uitvoermiddelen (7) voor het ter beschikking stellen van die gebufferde data.

3. Beveiligingssysteem volgens conclusie 2, GEKENMERKT DOOR bewakingsmiddelen (6) voor het bewaken van het datasysteem op normale werking en voor het activeren van de uitvoermiddelen (7) bij abnormaliteit in de werking van het datasysteem.

4. Beveiligingssysteem volgens conclusie 3, GEKENMERKT DOOR analysemiddelen (8) voor het analyseren van de door de geactiveerde uitvoermiddelen (7) ter beschikking gestelde data.

1015389

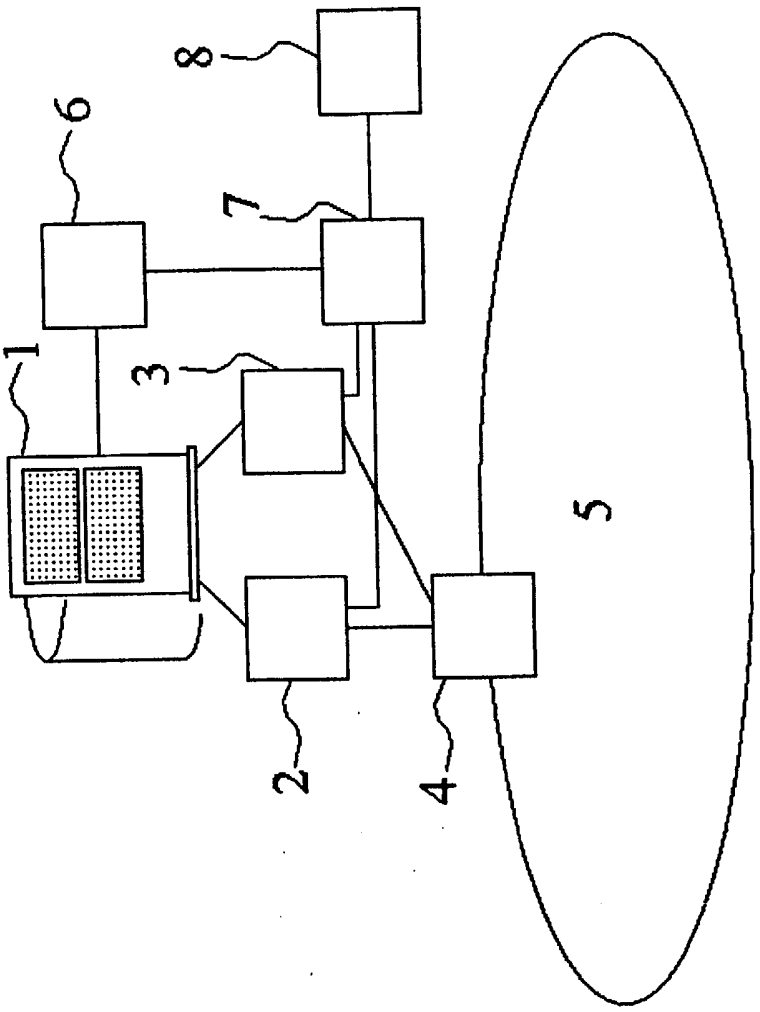


FIG. 1

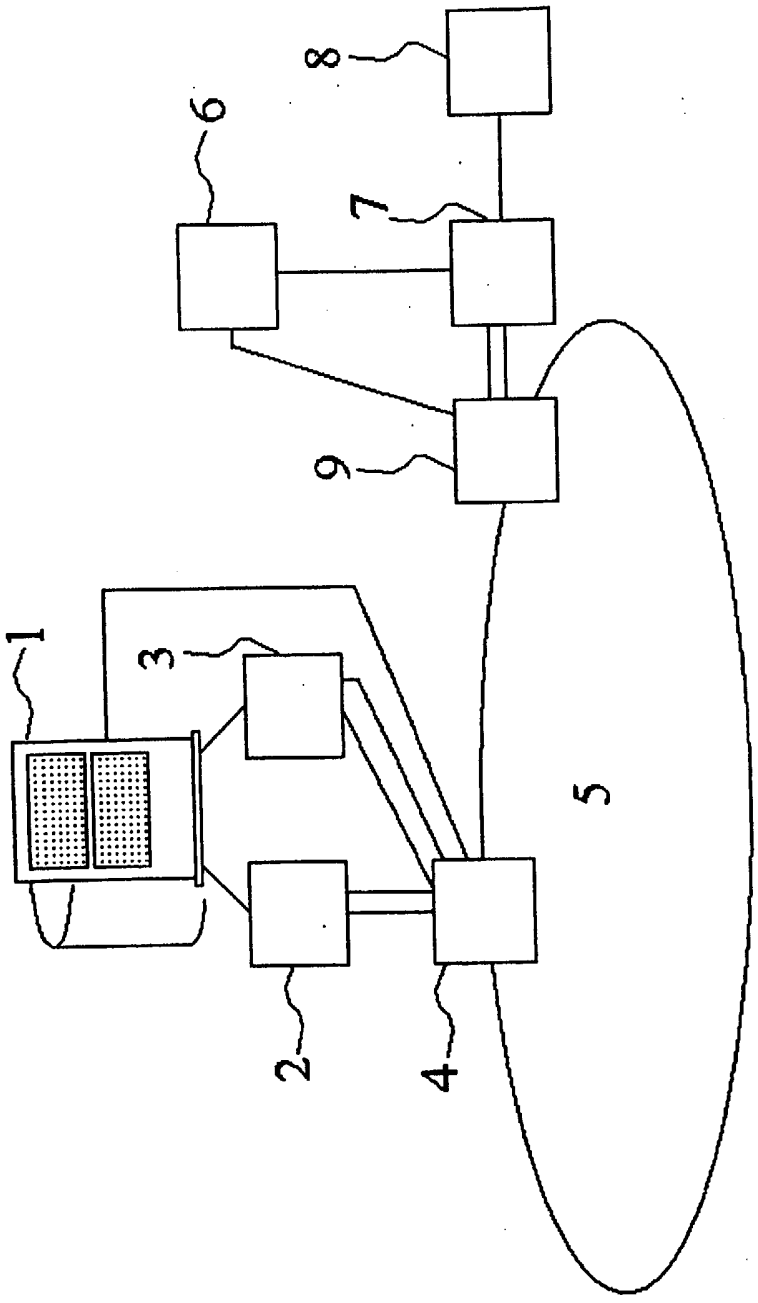
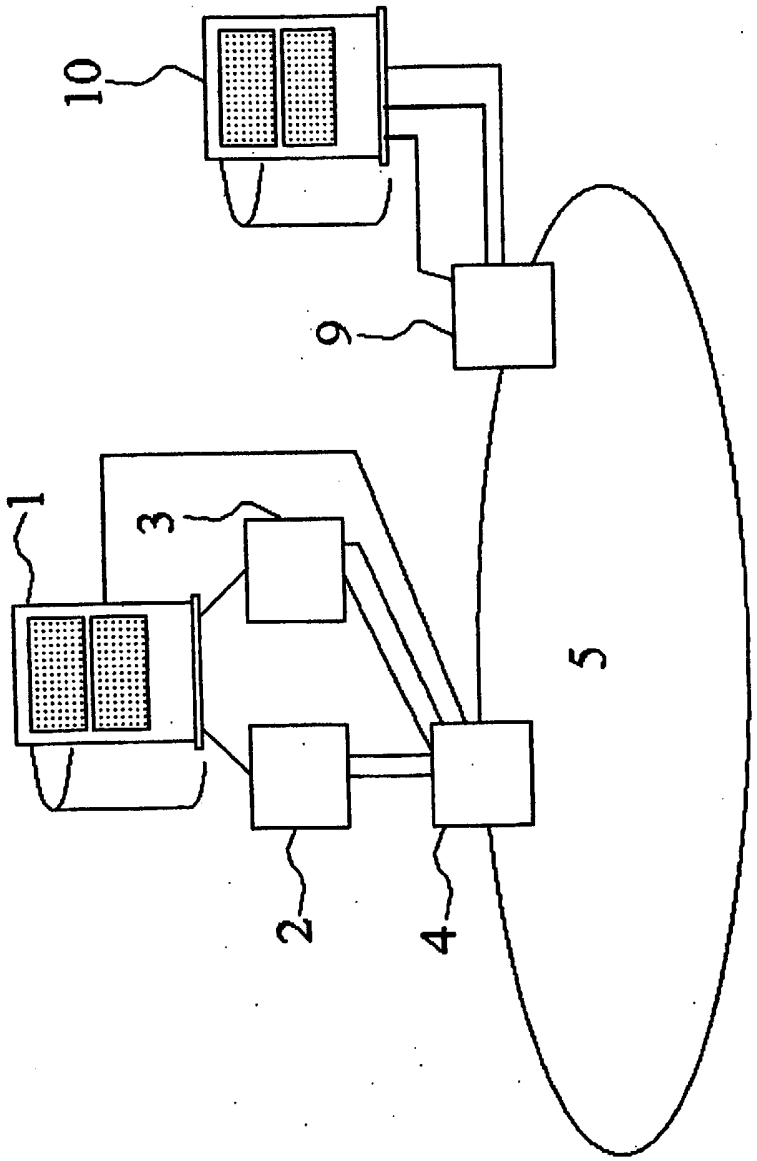


FIG. 2

FIG. 3



SAMENWERKINGSVERDRAG (PCT)

RAPPORT BETREFFENDE NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFICATIE VAN DE NATIONALE AANVRAGE	KENMERK VAN DE AANVRAGER OF VAN DE GEMACHTIGDE 402659NE
Nederlands aanvraag nr. 1015389	Indieningsdatum 07 juni 2000
	Ingeroepen voorrangsdatum
Aanvrager (Naam) KONINKLIJKE KPN N.V.	
Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr. SN 35243 NL

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de internationale classificatie (IPC)

Int.Cl.7: H04L29/06 H04L12/26

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie

Classificatiesysteem	Classificatiesymbolen
Int.Cl.7:	H04L G06F

Onderzochte andere documentatie dan de minimum documentatie, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ **GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES** (opmerkingen op aanvullingsblad)

IV. ☐ **GEBREK AAN EENHEID VAN UITVINDING** (opmerkingen op aanvullingsblad)

16

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1015389

A. CLASSIFICATIE VAN HET ONDERWERP
IPC 7 H04L29/06 H04L12/26

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte miminum documentatie (classificatie gevolgd door classificatiesymbolen)
IPC 7 H04L G06F

Onderzochte andere documentatie dan de mimimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie °	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	US 5 557 742 A (SMAHA STEPHEN E ET AL) 17 September 1996 (1996-09-17) kolom 5, regel 36 -kolom 6, regel 5; figuur 1 kolom 6, regel 61 -kolom 7, regel 3; figuur 2B kolom 11, regel 8 - regel 23; figuur 6B ---	1-4
A	US 5 796 942 A (ESBENSEN DANIEL) 18 Augustus 1998 (1998-08-18) samenvatting; figuren 1,3 kolom 3, regel 49 -kolom 4, regel 5 kolom 4, regel 60 - regel 67 kolom 5, regel 22 - regel 34 --- -/--	1-4

[X] Verdere documenten worden vermeld in het vervolg van vak C.

[X] Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

° Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang

"E" eerder document, maar gepubliceerd op de datum van indiening of daarna

"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven

"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel

"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvrage, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octrooifamilie

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid	Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type
17 Mei 2001	

Naam en adres van de instantie	De bevoegde ambtenaar
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Peeters, D

1

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1015389

C.(Vervolg). VAN BELANG GEACHTE DOCUMENTEN

Categorie °	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	WO 00 05842 A (RAYTHEON CO) 3 Februari 2000 (2000-02-03) bladzijde 2, regel 27 - regel 30 bladzijde 3, regel 7 - regel 15 bladzijde 7; figuur 1 bladzijde 9, regel 17 - regel 21 bladzijde 6, regel 26 - regel 28 bladzijde 21, regel 6 - regel 36; figuur 6 ---	1-4
A	LUNT T F: "A SURVEY OF INTRUSION DETECTION TECHNIQUES" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, deel 12, nr. 4, 1 Juni 1993 (1993-06-01), bladzijden 405-418, XP000382979 ISSN: 0167-4048 alinea '0002! -----	1-4

1

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1015389

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)		Datum van publicatie
US 5557742 A	17-09-1996	CA	2144105 A	08-09-1995
US 5796942 A	18-08-1998	AU	7303198 A	10-06-1998
		CN	1269030 A	04-10-2000
		EP	1008046 A	14-06-2000
		WO	9822875 A	28-05-1998
WO 0005842 A	03-02-2000	AU	4953999 A	14-02-2000