(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
7. Februar 2008 (07.02.2008)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2008/015191 A1

(51) Internationale Patentklassifikation:
H04L 12/26 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2007/057841

(22) Internationales Anmeldedatum:
30. Juli 2007 (30.07.2007)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2006 035 834.1 1. August 2006 (01.08.2006) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **NOKIA SIEMENS NETWORKS GMBH & CO. KG** [DE/DE]; St. Martin Str. 76, 81541 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **CHARZINSKI, Joachim** [DE/DE]; Groschenweg 49, 81825 München (DE).

(74) Gemeinsamer Vertreter: **NOKIA SIEMENS NETWORKS GMBH & CO. KG**; Postfach 80 17 60, 81617 München (DE).

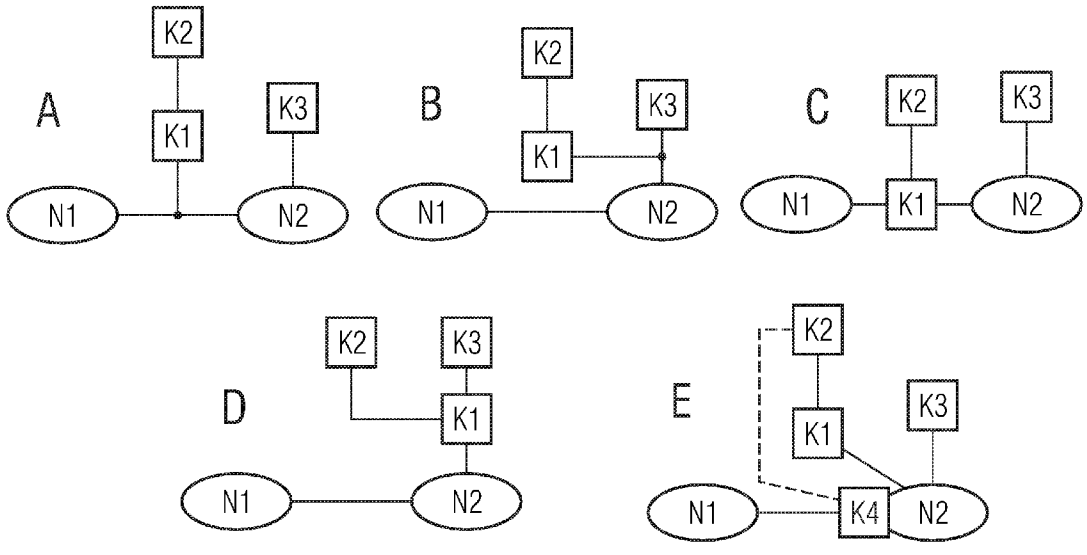
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** ANALYSIS UNIT FOR A PACKET-SWITCHED COMMUNICATION NETWORK

(54) **Bezeichnung:** ANALYSEEINHEIT FÜR EIN PAKETVERMITTELNDES KOMMUNIKATIONSNETZ



(57) **Abstract:** Analysis unit for a packet-switched communication network. The invention relates to a packet-switched communication network having a plurality of network nodes which are at least to some extent connected to one another. An analysis unit is arranged and designed such that it attendantly reads the packets transmitted between two network nodes and ascertains statistics about the transmitted packets.

(57) **Zusammenfassung:** Die Erfindung betrifft ein paketvermittelndes Kommunikationsnetz mit mehreren zumindest teilweise miteinander verbundenen Netzknoten. Eine Analyseeinheit ist derart angeordnet und ausgestaltet, dass sie die zwischen zwei Netzknoten übertragenen Pakete mitliest und Statistiken über die übertragenen Pakete ermittelt.

WO 2008/015191 A1

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Beschreibung

Analyseeinheit für ein paketvermittelndes Kommunikationsnetz

Die Erfindung betrifft eine Analyseeinheit für ein paketvermittelndes Kommunikationsnetz nach dem Oberbegriff von Patentanspruch 1.

Bei allen Diensten, die auf paketvermittelnden Kommunikationsnetzen, wie Internet-Protokoll-Netzen, basieren, werden heute Angriffe gegen diese Dienste oder gegen die entsprechenden Endgeräte beobachtet. Dies können so genannte Denial of Service, kurz DoS-Angriffe sein, mit dem Ziel, die Nutzbarkeit eines Dienstes einzuschränken. Ferner Theft of Service, kurz ToS-Angriffe, mit dem Ziel auf Kosten eines anderen Nutzers einen Dienst zu nutzen. Weiterhin Angriffe gegen Netzknoten bzw. Netzkomponenten oder Netzelementen mit dem Ziel, Filtereinrichtungen oder andere Einschränkungen und Abwehrmaßnahmen zu deaktivieren oder Angriffe zur Vorbereitung weiterer Angriffe durchzuführen. Falls ein Kommunikationsnetz oder Dienst aus dem öffentlichen Internet erreichbar ist, werden die Angriffe häufig über das Internet ausgeführt. Aber auch vom Internet abgeschirmte Netze und Dienste sind nicht sicher. Einerseits gibt es gelegentlich Fehlkonfigurationen, die zu einer versehentlichen Erreichbarkeit über das Internet führen, andererseits reicht es für viele Angriffe schon aus, wenn ein Endgerät, das normalerweise Bestandteil eines abgeschotteten Netzes ist, wie ein Voice over IP Netz, kurz VoIP-Netz, Managementnetz, Intranet einer Firma, gelegentlich an das Internet angeschlossen wird oder auch nur in Berührung mit Daten aus dem Internet kommt. Dies kann beispielsweise über portable Datenspeicher, wie Disketten, USB-Sticks oder CD's erfolgen. Wenn über einen solchen Datenaustausch ein System mit beispielsweise einem Wurmprogramm infiziert wird, kann sich dieses anschließend auch in einem Netz ausbreiten, welches ansonsten vom Internet abgeschottet ist.

Insbesondere bei der Sprachübertragung über das Internet / Voice-Over-IP, kurz VoIP, sind folgende Störungen des Netzbetriebes bzw. eines Dienstes zu erwarten:
- Störung von Teilnehmern durch Anrufe,
- Absturz von Endgeräten durch fehlerhafte Pakete oder falsches Protokollverhalten,
- Absturz von Servern durch fehlerhafte Pakete oder falsches Protokollverhalten,
- Beenden von Verbindungen durch „gespoofte" Pakete,
- DoS-Attacken gegen Teilnehmer durch gefälschte Deregistrierung,
- Umleitungen von Anrufen durch gefälschte Registrierung,
- Störung von Teilnehmern durch Initiierung von Klingeln, dazu reicht bereits ein einziges Datenpaket,
- Umgehen von Zugangsbeschränkungen durch „gespoofte" Pakete,
- Veränderung des Routings.

Für Internetprotokollnetze gibt es bereits so genannte Intrusion Detection Systeme, kurz IDS, und Intrusion Prevention Systeme, kurz IPS. Diese können in der Regel Angriffe auf der Basis von Verkehrsmustern erkennen. Gegen andere Angriffe gibt es noch keine Abwehrsysteme.

Die meisten Systeme zur Erkennung von dienste-spezifischen Angriffen werten Signaturen aus, d. h. sie suchen nach Bitmustern in Paketen. Hierzu wird zum einen ein hoher Aufwand bei der Suche der Muster in Echtzeit benötigt, was zu Performance Problemen führen kann, und zum anderen ein hoher Aufwand zur Erkennung neuer Muster und der Pflege der Musterkonfigurationen in den Filtersystemen benötigt. Ein typisches Beispiel für diese Pattern basierte IDS sind die heute auf vielen Computern verwendeten Virenscanner.

Aufgabe der vorliegenden Erfindung ist es, ein Kommunikationsnetz zu verbessern.

Diese Aufgabe wird durch eine Analyseeinheit mit den Merkmalen des Patentanspruchs 1 gelöst.

Erfindungsgemäß wird vorgeschlagen, eine Analyseeinheit in einem paketvermittelnden Kommunikationsnetz vorzusehen, die die zwischen zwei Netzknoten übertragenen Pakete mitliest und statistisch auswertet. Dies hat den Vorteil, dass Angriffe auf Kommunikationsnetze erkannt werden können.

In einer vorteilhaften Ausgestaltung der Erfindung sind die Netzknoten unterschiedlichen (Kommunikations-)Netzen zugeordnet, mit dem Vorteil, dass Angriffe auf ein Netz erkennbar sind.

In einer vorteilhaften Ausgestaltung der Erfindung ist die Analyseeinheit zwischen zwei Netzknoten angeordnet bzw. zwischengeschaltet, so dass übertragene Pakete verworfen bzw. gesperrt oder verändert werden können. Dies hat den besonderen Vorteil, dass bei Angriffen in den Paketverkehr eingegriffen werden kann.

In einer weiteren vorteilhaften Ausgestaltung ist die Analyseeinheit einem Netzknoten zugeordnet. Dies hat den Vorteil, dass eine integrierte Lösung gegeben ist.

In einer weiteren vorteilhaften Ausgestaltung ist die Analyseeinheit für die Auswertung von Paketen des Session Initiation Protokoll, kurz SIP, ausgestaltet. Dies hat den Vorteil, dass Voice-over-IP Verkehr überwacht und gegebenenfalls geschützt werden kann.

In einer weiteren vorteilhaften Ausgestaltung ist die Analyseeinheit einem Proxy oder Server für SIP Pakete vorgeschaltet, d. h. einer der beiden Netzknoten ist ein SIP-Server oder SIP-Proxy. Dies hat den Vorteil, dass Angriffe durch SIP Pakete vor dem Server verhindert werden.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung ist die Analyseeinheit mit einem Netzknoten gekoppelt, so dass dieser bestimmte Pakete verwerfen kann oder seine Konfi-

guration ändern kann, um das Netz, Netzkomponenten oder sich selbst vor Angriffen zu schützen. Dies hat den Vorteil, dass eine individuelle Gefahrenabwehr erzielt wird, auch wenn die Analyseeinheit nicht im Netzknoten integriert ist.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen und dem Ausführungsbeispiel angegeben.

Ein Ausführungsbeispiel der Erfindung wird im Folgenden anhand der Zeichnung näher erläutert. Dabei zeigt:

Figur 1 Kommunikationsnetze mit einer erfindungsgemäßen Analyseeinheit,
Figur 2 ein Ablaufdiagramm zur Auswertung von Daten,
Figur 3 ein zweites Ablaufdiagramm für die Klassifikation von SIP-Signalisierungsnachrichten.

In den Figuren 1a bis 1e sind mehrere Netzkonfigurationen dargestellt, aufweisend Netzknoten N1 und N2, wobei Netzknoten N1 zu einem ersten Netz und Netzknoten N2 zu einem zweiten Netz gehört. Ferner sind Netzknoten K1 zur Erfassung von Datenpaketen und K2 zur Auswertung der Datenpakete eingezeichnet, sowie ein SIP-Server oder SIP-Proxy K3, sowie ein weiterer Netzknoten K4. Die Netzknoten können Router, Switches, HUBs, Gateways, Bridges oder beliebige andere Netzelemente sein. Die erfindungsgemäße Analyseeinheit ist in Figur 1 durch eine Serienschaltung zweier Netzknoten K1 und K2 realisiert. Die Funktionalität der Analyseeinheit ist hierbei auf diese beiden Netzknoten verteilt.
In Figur 1a ist die Serienschaltung der beiden Netzknoten K1 und K2 an die Verbindung zwischen den Netzknoten N1 und N2 angeschaltet, so dass Netzknoten K1 die Datenpakete zwischen Netzknoten N1 und N2 mitlesen kann. An Netzknoten N2 bzw. dessen Netz ist der SIP-Server oder SIP-Proxy K3 angeschlossen.
In Figur 1b befindet sich die Serienschaltung der Netzknoten K1 und K2 an der Verbindung zwischen Netzknoten N2 bzw. des-

sen Netz und Netzknoten K3, der ein SIP-Server oder SIP-Proxy ist.
In Figur 1c geht die Verbindung zwischen Netzknoten N1 und N2 über den Netzknoten K1, so dass dieser aktiv in die Paketübertragung eingreifen kann.
In Figur 1d ist analog zu Figur 1c der Netzknoten K1 in der Verbindung zwischen Netzknoten N2 bzw. dessen Netz und Netzknoten K3 integriert.
In Figur 1e ist die Serienschaltung der Netzknoten K1 und K2 an das zweite Netz des Netzknotens N2 angeschlossen. Das zweite Netz umfasst einen weiteren Netzknoten K4, der mit dem Netzknoten K2 in Verbindung steht.

In Figur 1 umfasst die erfindungsgemäße Analyseeinheit jeweils zwei Netzknoten K1 und K2. Der Netzknoten K1 liest die übertragenen Pakete zwischen zwei Netzknoten bzw. zwischen zwei Netzen mit, wie in Figur 1a und 1b gezeigt, und kann, falls er sich in der Verbindung zwischen zwei Netzknoten befindet, wie in Figur 1c und 1d gezeigt, in die übertragenen Pakete eingreifen. Netzknoten K2 analysiert die mitgelesen Pakete, wertet diese aus und gibt gegebenenfalls entsprechende Kommandos an Netzknoten K1, falls bestimmte Pakete gesperrt, blockiert oder verändert werden sollen. Die Serienschaltung der Netzknoten K1 und K2 kann sich auch an einer beliebigen Stelle in einem Netz befinden, wie in Figur 1e gezeigt, um den Datenpaketverkehr mitzulesen und gegebenenfalls die Konfiguration von Netzknoten wie Routern oder Firewalls oder andere Komponenten über eine Verbindung zur diesen Netzknoten oder einer Netzkomponente, wie Netzknoten K4, ändern.

Der Funktionsumfang der Analyseeinheit kann fest oder konfigurierbar eine der folgenden Funktionen umfassen:
- Beobachtung, Auswertung, Logging von Anomalien oder Bedrohungen
- Visualisierung von Anomalien oder Bedrohungen
- Analyse momentaner Bedrohungen
- Generierung von Alarmen

- Ausgabe von Empfehlungen zur Konfigurationsänderung , z. B. einen Teilnehmer vom Netz nehmen, keine Pakete mehr von einer IP-Adresse oder einem bestimmten Nachbarn oder Netzknoten empfangen
- Veranlassung von Blockierung von Rufen in/aus anderen Netzen oder Systemen,
- direkte Blockierung von Signalisierungsnachrichten (falls die Analyseeinrichtung in der Verbindung liegt, gemäß Figur 1c oder 1d).

Durch die Analyseeinheit werden Datenpakete analysiert und gegebenenfalls Statistiken erstellt. Dies ist besonders vorteilhaft für SIP-Pakete wie sie für das Telefonieren über Internet verwendet werden. Beispielsweise kann die Größenverteilung der Pakete bzw. SIP-Pakete ermittelt werden. Eine Aufteilung der UDP- und TCP-Pakete für die SIP-Pakete ermittelt werden. Die Häufigkeiten verschiedener SIP-Kommandos wie INVITE, ACK, PRACK, BYE, CANCEL, OPTIONS, REGISTER ermittelt werden.
Wenn für einen Absender, gekennzeichnet z. B. durch eine User-ID, IP-Adresse (von der das Paket kommt) oder andere Header-Einträge eine Häufung von Anomalien, d. h. Abweichungen von de üblichen Paketübertragung festgestellt werden, kann automatisch eine vollständige Aufzeichnung der Datenpakete für diesen Nutzer oder Absender veranlasst werden.
Ebenso kann für einen Absender für eine gewisse Zeit der Paket- bzw. Signalisierungsverkehr vollständig aufgezeichnet werden, nachdem von diesem Absender ein nicht definiertes Kommando oder eine nicht definierte Antwort in einem übertragenen Paket beobachtet wurde.

Zur Analyse der mitgelesenen Pakete werden die ausgewerteten Parameter mit Erfahrungswerten bzw. Standard- oder Defaultwerten, die durch einen Standard oder ein Experimente ermittelt oder im Grundzustand des Netzes bei störungsfreiem Betrieb für normales Protokollverhalten gemessen wurden, verglichen.

Beispielsweise gehört zu einem normalen Anruf bzw. Basic-Call mit dem SIP-Protokoll die Abfolge:
INVITE - 100 Trying - 180 ringing - 200 OK - ACK - BYE - 200 OK
Entsprechend sind die Zahlen pro beobachteten INVITE:
1x 100 Trying,
1x 180 ringing,
2x 200 OK,
1x ACK,
1x BYE

Im Fall der Beendigung eines Anrufes vor dem Abheben des gerufenen Teilnehmers:
INVITE - 100 Trying - 180 ringing - CANCEL - 200 OK
Pro INVITE also:
1x 100 Trying,
1x 180 ringing,
1x 200 OK,
0x ACK,
0x BYE,
1x CANCEL

Für verschiedene Arten von Anrufen bzw. Call-Typen werden so die typischen Anzahlen von Nachrichten der zu beobachtenden Pakete bzw. wie im vorliegenden Fall des entsprechenden SIP-Protokolls ermittelt und in einer oder mehreren Referenzlisten abgelegt. Ebenso sind verschiedene Fehlerfälle wie temporäre Überlast, Paketverluste usw. zu analysieren und mit erwarteten Häufigkeiten zu bewerten.

Zu einem Angriffsmuster auf einem SIP-Server, insbesondere bei Angriffen die verschiedene Möglichkeiten bzw. Variablen durchprobieren, wird eine Erhöhung der Anzahl von Fehlermeldungen festzustellen sein. Beispielsweise werden bei einem Angriff mit gefälschten INVITE-Paketen, mit dem Ziel Telefone zum Klingeln zu bringen ohne eine Verbindung aufzubauen, die Endgeräte mit „100“ und „180“ Antworten und daraufhin vom

SIP-Server aber eine Antwort vom Typ „481" „Call/Transaction does not exist" bekommen.

So werden für bekannte/erwartete Angriffsmuster die entsprechenden Anzahlen von Kommandos und Antworten für die entsprechenden Protokolle analysiert und in den Referenzlisten abgelegt.

Bei der statistischen Analyse in der Analyseeinrichtung werden nun die beobachteten Anzahlen von Kommandos mit den in den Referenzlisten abgelegten Anzahlen verglichen und signifikante Abweichungen ermittelt, wobei bei bereits bekannten Referenzen für Angriffszenarien dem Netzbetreiber ein Hinweis auf die vermuteten Angriffe gegeben wird. Gleichzeitig wird für jeden Kommando- und Antworttyp, der in einem übertragenen Paket enthalten ist, geprüft, ob seine Häufigkeit momentan auffällig ist. Bei der Online-Bewertung von SIP-Nachrichten kann ein Überschreiten von Grenzwerten für diese Häufigkeiten für manche Nachrichten als Kriterium für die sofortige Blockierung einer neuen Nachricht desselben Typs verwendet werden.

Ferner können:
- Die Häufigkeiten nicht definierter (SIP-)Kommandos und (SIP-)Antworten summarisch erfasst oder für jedes neu erkannte Kommando und jede neu erkannte Antwort zusätzlich ein neuer Statistikzähler angelegt werden.
- Die Auswertung kann schritthaltend oder nachträglich, z. B. durch Auswerten einer Trace-Datei, in der die mitgelesen Pakete gespeichert sind, geschehen.
- Im Falle der schritthaltenden Auswertung können verdächtige Pakete sofort blockiert werden.
- Die vollständige Aufzeichnung verdächtigen Paketverkehrs kann an Schwellwerte gekoppelt sein, die fest vorgegeben, an einer Auswertung relativ zu einem definierten Normalverhalten oder zum beobachteten mittleren Verhalten basieren.
- Wenn ein Absender gehäuft auffällig wird, kann ein Alarm generiert werden.

- Eine transaktionsverfolgende Variante der Erfindung kann zusätzlich abnormales Verhalten innerhalb einer Transaktion erkennen, z. B. 180 ringing als Antwort auf ein BYE-Kommando oder 481 Call/Transaction does not exist als Antwort auf ein INVITE-Kommando.
- Eine rufverfolgende Variante der Analyseeinrichtung kann zusätzlich abnormales Verhalten innerhalb eines Rufes erkennen, z. B. „BYE" oder „CANCEL" ohne vorheriges „INVITE".
- Die gesammelten Statistiken können Mittelwerte, Verteilungen und/oder Quantile registrieren.
- Die durch die Analyseeinrichtung ermittelten Statistiken können beispielsweise pro SIP-Teilnehmer, pro Absender-IP-Adresse, pro Ziel-IP-Adresse, pro SIP-Ursprungsdomäne oder per E.164-Präfix, wie z. B. Länderkennung, ermittelt werden.

Tabelle 1 zeigt den Zustand eines Teils eines Erfassungszählers in einer Analyseeinheit für zwei verschiedene Fälle A und B.

Kommando/Antwort	Anzahl A	Anzahl B
INVITE	1000	1211
ACK	923	923
PRACK	300	300
REGISTER	80	163
BYE	923	923
CANCEL	75	75
OPTIONS	3	3
100 trying	1000	1211
180 ringing	1000	1187
200 OK	2040	2040
401 unauthorized	40	123
403 forbidden	2	2
481 call does not exist	0	211
Undefinierte SIP-Nachrichten	0	329

Im Fall A wurden 1000 Calls, 40 Registrierungen und 75 Call-Abbrüche beobachtet. Zwei der Anrufer waren durch eine Blacklist gesperrt. Dreimal wurde das ‚OPTIONS' Kommando verwendet.

Im Fall B wurden zusätzlich zu Fall A 211 INVITE-Angriffe mit IP-Spoofing und 83 erfolglose Registrierungsversuche getätigt. Die IP-Spoofing-Angriffe haben Reaktionen mit den Antwort-Typen 100, 180 und 481 hervorgerufen. Die erfolglosen Registrierversuche haben zu einer erhöhten Anzahl von Antworten des Typs 401 geführt. Zusätzlich sind viele undefinierte Nachrichten beobachtet worden, die ein Anzeichen für einen Angriff gegen einen SIP-Server, SIP-Proxy bzw. SIP-Stack sein können.

In Figur 2 sind Analysebestandteile und Analyseoptionen für eine Analyseeinrichtung an Hand eines Ablaufdiagramms dargestellt. Dabei bedeutet:

P1: statistische Analyse
P2: Anzeige auf einem Operator Interface (visuelle Anzeige)
P3: Analyse möglicher Hintergründe
P4: Anzeige der Analyseergebnisse (visuelle Anzeige)
P5: Ableitung von Sperr-Mechanismen
P6: Vorschlag von Sperr-Mechanismen auf einem Operator Interface (visuelle Anzeige)
P7: Aktivierung von ausgewählten Sperr-Mechanismen

Die erfindungsgemäße Analyseeinrichtung kann jeweils umfassen:

- ein System oder Gruppe von Systemen zur Beobachtung von Paketen, beispielsweise mit SIP-Signalisierverkehr, und Erfassung von Statistiken.
- eine Auswertung der Pakete nach bekannten und unbekannten Kommando- und Antworttypen.
- ein automatisches Anstoßen des Tracing (mitschreiben von Paketen bzw. dessen relevanten Inhalts) für auffällige Pakete bzw. User und/oder auffällige Kommandos/Antworten.
- eine Hinterlegung von Normalfällen und bekannten Angriffen / Angriffsmustern in der Analyseeinrichtung.

- eine Auswertung in der Analyseeinrichtung bezogen auf zulässige bzw. mögliche Antworten für Transaktionen.
- eine Auswertung hinsichtlich sinnvoller oder zulässiger Abfolgen von Befehlen / Nachrichten / Kommandos in Paketen, beispielsweise für Transaktionen in Anrufen / Calls.
- eine Auswertung bezogen auf einen Absender (User, Ursprungs-IP, Nummernbereich, Ursprungsbetreiber).
- eine Auswertung der Statistiken und Ableitung von Hinweisen auf Angriffszenarien für einen Operator / Netzbetreiber.
- eine Ableitung von Blockierungsaktionen aus Angriffs-Hinweisen.
- eine Auswertung von Trace-Dateien.
- eine automatische Konfiguration von Blockierungsaktionen oder ein Vorschlag und dessen Bestätigung.
- eine Analyseeinrichtung spezifisch für IDS/IPS bei VoIP, d.h. optimal abgestimmt auf Angriffe gegen VoIP.
- eine Auswertung von Antworten in den Paketen lässt bereits während eines Normalbetriebs schnell eine Häufung von Fehlerfällen erkennen. Die Fehlerfälle können durch Untersuchung der im adaptiven Tracing aufgezeichneten Pakete analysiert werden.
- bei einer Analyseeinrichtung ausschließlich für VoIP kann eine kostengünstige Realisierung erreicht werden, da die VoIP Signalisierungsströme relativ geringe Datenraten haben.

Die Analyseeinheit kann beispielsweise in einem IDS oder IPS System für das SIP-Protokoll, in einem SPIT-Erkennungs- oder Vermeidungssystem, in einem Session Border Controller (SBC), in einem SIP Server, SIP Proxy, SIP Application Server oder in einer Firewall verwendet werden.

Figur 3 zeigt einen Ablaufplan für die Klassifikation einer SIP-Signalisierungsnachricht und den Umgang mit unbekannten Nachrichten.
Dabei bedeuten:

Aktionen:
A1: Größenverteilung Paket
A2: Längenverteilung erste Zeile
A3: Extraktion erste 8 Zeichen
A4: Verteilung Kommando-Typen
A5: Paket zählen (unbekanntes Kommando)
A6: Paket komplett speichern
A7: Verteilung Antwort-Typen (100…999)
A8: Paket zählen (unbekannter Antwort-Typ)
A9: Paket zählen (unbekannter Typ)

Entscheidungen:
D1: erste Bytes: Kommando / 3 Ziffern / sonstige
D2: bekanntes Kommando?
D3: Anzahl der Kommandos unbekannten Typs bereits > T_UC?
D4: Antwort zwischen 100 und 999?
D5: Anzahl der Antworten unbekannten Typs bereits > T_UR?
D6: Anzahl „sonstige" > T_UT?
D7: bekannter Antwort-Typ?

Resultate:
R11: Kommando
R12: Antwort
R13: sonstige

Die Entscheidung D1 wird anhand der ersten Zeichen der SIP-Nachricht gefällt: Falls es sich um ASCII-Buchstaben (A-Z, a-z) handelt, wird R11 zurückgegeben. Falls es sich um Ziffern handelt, wird R12 zurückgegeben. Andernfalls wird R13 zurückgegeben.
Die Entscheidung D2 prüft, ob die Buchstabenfolge einem der bekannten Kommandos (INVITE, ACK, PRACK, BYE, CANCEL, OPTIONS, REGISTER) entspricht.
Die Entscheidung D7 prüft, ob die Ziffern einen in den einschlägigen RFC's definierten Antwort-Typ anzeigen.

Analyse gehäuft auftretender SIP-Antworten:

- Typ 481 "Call/Transaction does not exist", deutet auf fehlerhafte SIP-Implementierungen, IP-Spoofing-Angriffe oder auf call-termination-Angriffe.
- Typ 401 „Unauthorized", Typ 407 „Proxy Authentication Required" deuten auf Versuche, Passwörter durchzuprobieren oder nach offenen Servern zu suchen.
- Typ 400 „Bad Request", 405 „Method not allowed" oder 500 „internal server error", 501 „not implemented" deuten auf fehlerhafte SIP-Implementierungen oder Angriffe mit nicht standardkonformen Paketen.
- Typ 403 „forbidden", Typ 603 „decline": Hinweise auf wiederholte Anrufe bei blacklisting (auch lokal).
- Typ 406 „not acceptable", Typ 413 „Request entity too large", 414 "request-URI too long", 415 "Unsupported media type", 416 "Unsupported URI scheme", 420 "bad extension", 606 "not acceptable" deuten auf Versuche hin, Schwachstellen in SIP-Stacks auszunutzen.
- Typ 408 "request timeout" kann ein indirekter Hinweis auf Überlast (und damit auf DoS-Angriffe) sein.
- Typ 423 „Interval Too Brief" kann ein Hinweis auf einen versuchten DoS-Angriff sein.
- Typ 482 „loop detected" kann ein Hinweis auf eine Fehlkonfiguration oder einen Angriff sein.
- Typ 483 ist ein Hinweis auf einen Konfigurationsfehler.
- Typ 484 ist unproblematisch, kann aber auch ein Hinweis auf einen DoS-Angriff sein.
- Typ 404 oder Typ 485 oder Typ 604 kann ein Hinweis auf Adress-Harvesting sein.
- Typ 486 kann ein Hinweis auf einen DoS-Angriff sein.
- Typ 503 „service unavailable" Hinweis auf DoS (Überlast).
- Typ 504 „server time-out" Hinweis auf DoS durch Nachbarserver, eventuell tar pit.
- Typ 505 „version not supported" Hinweis auf DoS-Angriff durch Durchprobieren von Parametern.
- Typ 513 „message too large" Hinweis auf Angriff mit zu langen Nachrichten.

Patentansprüche

1. Analyseeinheit für ein paketvermittelndes Kommunikationsnetz mit mehreren zumindest teilweise miteinander verbundenen Netzknoten,
dadurch gekennzeichnet,
dass die Analyseeinheit derart angeordnet und ausgestaltet ist, dass sie die zwischen zwei Netzknoten übertragenen Pakete mitliest und Statistiken über die übertragenen Pakete ermittelt.

2. Analyseeinheit nach Anspruch 1,
dadurch gekennzeichnet,
dass einer der beiden Netzknoten zu einem ersten Netz und der andere der beiden Netzknoten zu einem zweiten Netz gehört.

3. Analyseeinheit nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die Analyseeinheit den beiden Netzknoten zwischengeschaltet ist und die übertragenen Pakete verändern oder verwerfen kann.

4. Analyseeinheit nach Anspruch 1, 2 oder 3,
dadurch gekennzeichnet,
dass die Analyseeinheit einem der beiden Netzknoten zugeordnet ist.

5. Analyseeinheit nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Analyseeinheit Statistiken über die Größenverteilung der übertragenen Pakete und/oder Häufigkeiten der Pakettypen und/oder Häufigkeiten der in den Paketen enthaltenen Befehle und/oder Abfolgen der in den Paketen enthaltenen Befehle erstellt.

6. Analyseeinheit nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass erstellte Statistiken mit abgespeicherten Norm-Statistiken verglichen werden.

7. Analyseeinheit nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
dass einer der beiden Netzknoten ein SIP-Server oder SIP-Proxy ist und/oder die Analyseeinheit SIP-Pakete auswertet.

8. Analyseeinheit nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
dass SIP-Pakete ausgewertet werden und Statistiken über die Größenverteilung der SIP-Pakete und/oder Aufteilungen nach UDP/TCP-Paketen für die SIP-Pakete und/oder Häufigkeiten der übertragenen SIP-Kommandos und/oder Häufigkeiten der übertragenen SIP-Antworten erstellt werden.

9. Analyseeinheit nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
dass die Analyseeinheit mit einem Netzknoten verbunden ist und diesen dahingehend steuert, dass bestimmte Pakete verworfen werden.

10. Analyseeinheit nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
dass ermittelte Statistiken mit abgespeicherten Norm-Statistiken verglichen werden und bei Überschreitung eines ersten Schwellwertes die übertragenen Pakete aufgezeichnet werden und/oder ein Alarm generiert wird.

11. Analyseeinheit nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
dass ein übertragenes Paket hinsichtlich einer Norm-Konformität überprüft wird und ein nicht norm-konformes Paket aufgezeichnet wird.

FIG 1A

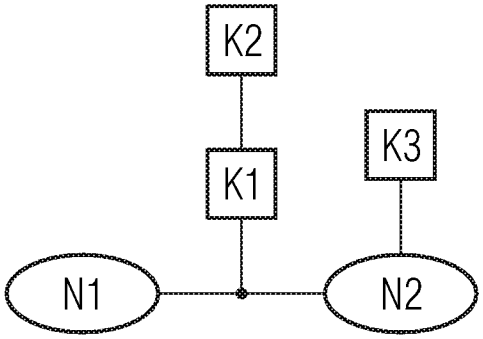


FIG 1B

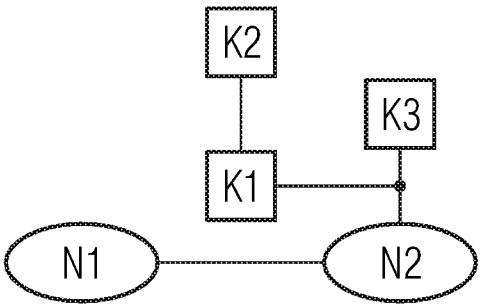


FIG 1C

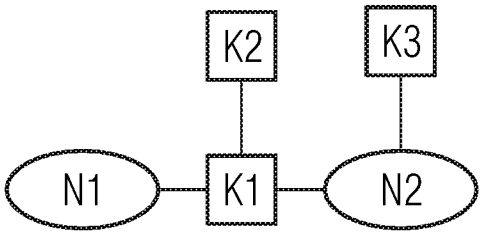


FIG 1D

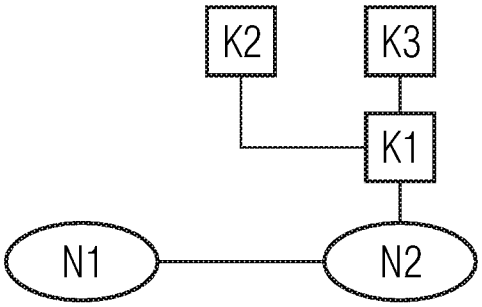


FIG 1E

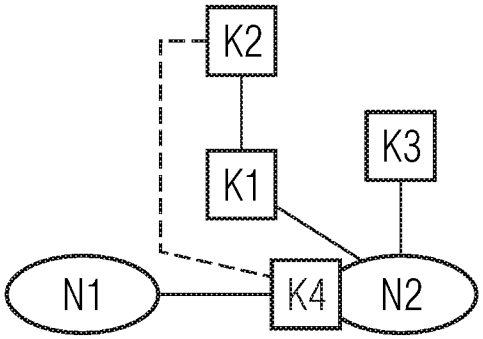


FIG 2

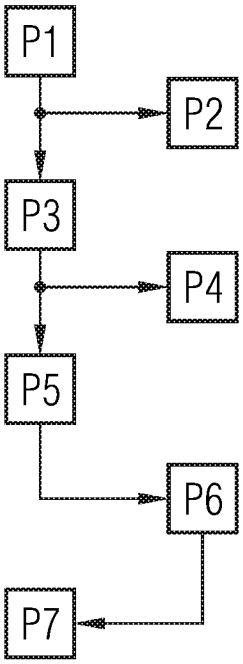
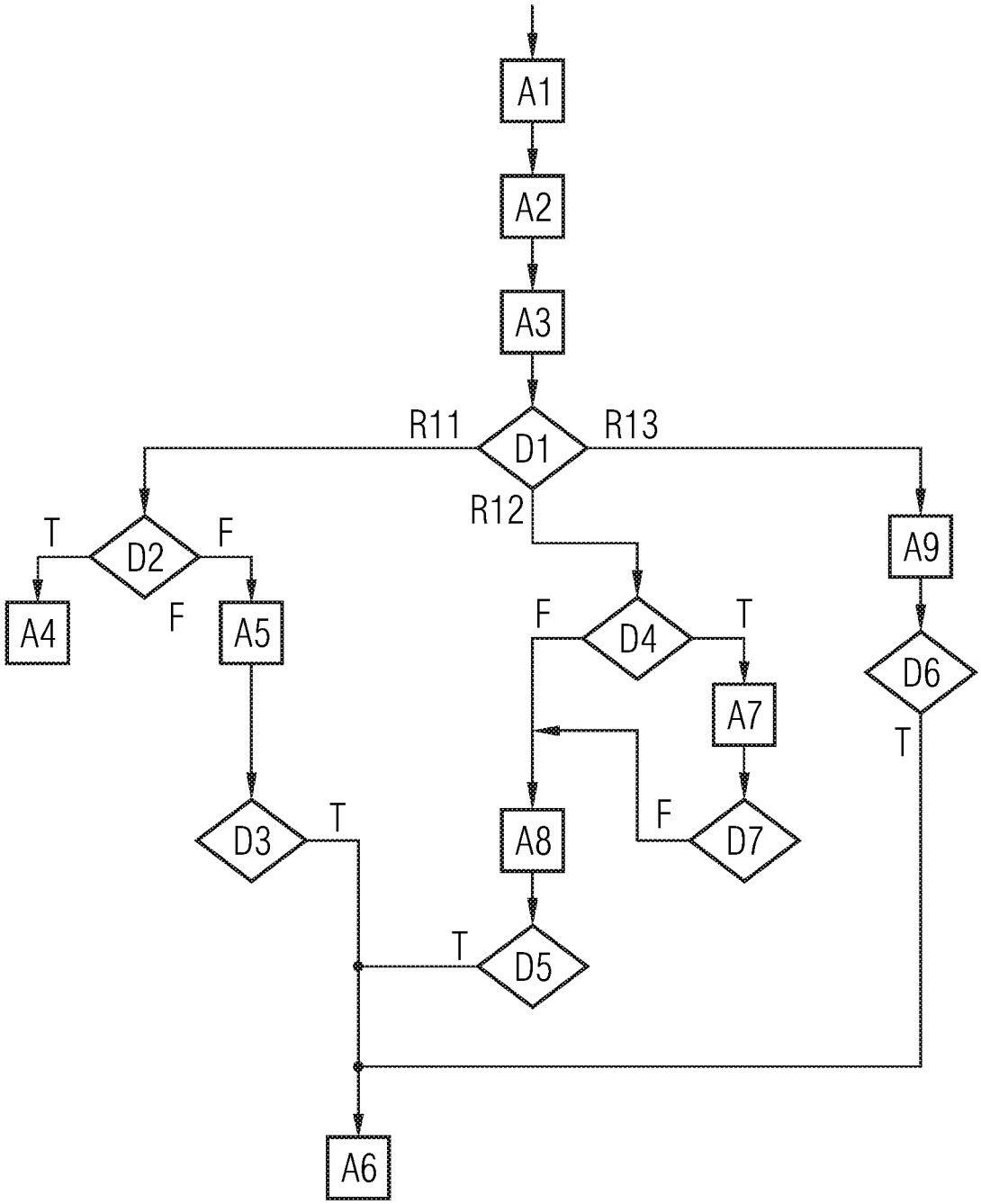


FIG 3


A1
A2
A3
R11
D1
R13
R12
T
D2
F
A9
A4
F
A5
F
D4
T
D6
A7
T
T
D3
A8
F
D7
T
D5
A6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/057841

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, IBM-TDB, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 2003/212903 A1 (PORRAS PHILLIP ANDREW [US] ET AL) 13 November 2003 (2003-11-13) abstract figure 1 paragraph [0035] paragraph [0038] paragraphs [0040], [0041] paragraph [0045] paragraph [0071] -----	1,2,4-6, 10 3,7-9 11
Y	P.A. PORRAS: "Live Traffic Analysis of TCP/IP Gateways"[Online] 1 March 1988 (1988-03-01), XP002460519 Retrieved from the Internet: URL:http://www.csl.sri.com/papers/live-traffic/live-traffic.html> [retrieved on 2007-11-28] paragraph [0007] -----	3,9
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2007	19/12/2007

Name and mailing address of the ISA/	Authorized officer
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	Cichra, Michael

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/057841

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/286430 A1 (KOGA YOSHIHIKO [JP] ET AL) 29 December 2005 (2005-12-29)	1-5,8,11
A	abstract figures 1,5 paragraphs [0050] - [0062] paragraph [0076] paragraphs [0080], [0081] paragraph [0106] paragraph [0354]	6,7,9,10
X	WO 01/88731 A (NIKSUN INC [US]; PRUTHI PARAG [US]) 22 November 2001 (2001-11-22)	1,2,4,10
A	abstract page 7, lines 1-12 page 7, line 25 - page 8, line 4 page 38, lines 22,23 page 39, lines 24-27 figure 1 figures 10-20	3,5-9,11
Y	CHEN E Y: "Detecting DoS attacks on SIP systems" VOIP MANAGEMENT AND SECURITY, 2006. 1ST IEEE WORKSHOP ON APRIL 3, 2006, PISCATAWAY, NJ, USA,IEEE, 3 April 2006 (2006-04-03), pages 51-56, XP010919088 ISBN: 1-4244-0144-5 page 55, right-hand column, line 4 - page 56, left-hand column, line 5	7,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/057841

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003212903 A1	13-11-2003	US 2004010718 A1	15-01-2004
		US 2004221191 A1	04-11-2004
US 2005286430 A1	29-12-2005	JP 2006013737 A	12-01-2006
WO 0188731 A	22-11-2001	AU 6312701 A	26-11-2001
		EP 1297440 A1	02-04-2003
		JP 2003533925 T	11-11-2003

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/057841

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L12/26

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, IBM-TDB, INSPEC, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y A	US 2003/212903 A1 (PORRAS PHILLIP ANDREW [US] ET AL) 13. November 2003 (2003-11-13) Zusammenfassung Abbildung 1 Absatz [0035] Absatz [0038] Absätze [0040], [0041] Absatz [0045] Absatz [0071] --- P.A. PORRAS: "Live Traffic Analysis of TCP/IP Gateways"[Online] 1. März 1988 (1988-03-01), XP002460519 Gefunden im Internet: URL:http://www.csl.sri.com/papers/live-traffic/live-traffic.html> [gefunden am 2007-11-28] Absatz [0007] --- -/--	1,2,4-6, 10 3,7-9 11 3,9

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
29. November 2007	19/12/2007

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Cichra, Michael

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/057841

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2005/286430 A1 (KOGA YOSHIHIKO [JP] ET AL) 29. Dezember 2005 (2005-12-29)	1-5,8,11
A	Zusammenfassung Abbildungen 1,5 Absätze [0050] - [0062] Absatz [0076] Absätze [0080], [0081] Absatz [0106] Absatz [0354]	6,7,9,10
X	WO 01/88731 A (NIKSUN INC [US]; PRUTHI PARAG [US]) 22. November 2001 (2001-11-22)	1,2,4,10
A	Zusammenfassung Seite 7, Zeilen 1-12 Seite 7, Zeile 25 - Seite 8, Zeile 4 Seite 38, Zeilen 22,23 Seite 39, Zeilen 24-27 Abbildung 1 Abbildungen 10-20	3,5-9,11
Y	CHEN E Y: "Detecting DoS attacks on SIP systems" VOIP MANAGEMENT AND SECURITY, 2006. 1ST IEEE WORKSHOP ON APRIL 3, 2006, PISCATAWAY, NJ, USA,IEEE, 3. April 2006 (2006-04-03), Seiten 51-56, XP010919088 ISBN: 1-4244-0144-5 Seite 55, rechte Spalte, Zeile 4 - Seite 56, linke Spalte, Zeile 5	7,8

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2007/057841

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003212903 A1	13-11-2003	US 2004010718 A1	15-01-2004
		US 2004221191 A1	04-11-2004
US 2005286430 A1	29-12-2005	JP 2006013737 A	12-01-2006
WO 0188731 A	22-11-2001	AU 6312701 A	26-11-2001
		EP 1297440 A1	02-04-2003
		JP 2003533925 T	11-11-2003