CH 694 215 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 694 215 A5

(51) Int. Cl.[7]: H 04 L 012/56
G 06 F 015/163

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 01544/03

(22) Anmeldungsdatum: 10.09.2003

(24) Patent erteilt: 15.09.2004

(45) Patentschrift veröffentlicht: 15.09.2004

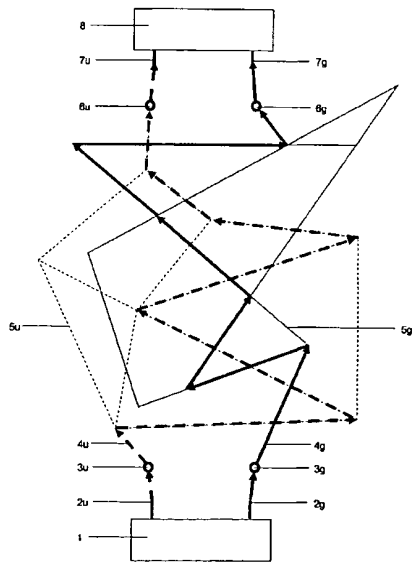
(73) Inhaber:
Csaba Bona, Säckingerstrasse 3
4310 Rheinfelden (CH)

(72) Erfinder:
Csaba Bona, Laufenburgerstrasse 5
4310 Rheinfelden (CH)

(54) Verfahren zum Übermitteln von elektronischen Daten über ein duales Netzwerk zur Erhhöhung der Internetsicherheit.

(57) Internet-Sicherheit durch Duales Netzwerk (zwei Netzwerke) und durch eine neue Methode der Paket-Aufbereitung, die jedes zweite Bit der Nutzinformation in zwei Arten von Paketen zusammenfasst. Eine der beiden Arten von Paketen nimmt die ungeraden Bits, die zweite die geraden Bits der ursprünglichen Information auf.

Die zwei Arten von implizit verschlüsselten Paketen (4u, 4g), werden in zwei getrennten Computer-Netzwerken (5u, 5g), mit einer Zeitverschiebung übermittelt, und nach der Übermittlung, beim Empfänger, entsprechend der ursprünglichen Information zusammengesetzt.



Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren, gemäss Patentanspruch 1, das die heute bekannten Raten von Hacker-Attacken auf Computer-Systeme drastisch reduziert. Für die Sicherheit von Computer-Systemen gibt es zahlreiche Einrichtungen, die ihren Zweck jedoch nicht erfüllen. Sie verbrauchen sehr viele Ressourcen, und trotzdem verursachen Computer-Hacker weltweit 600–800 Milliarden USD (Amerikanischer Dollar) Schaden jährlich.

Das zentrale Element in der Kommunikation unter Computer-Systemen ist das Paket. Die Daten werden seriell in Pakete aufgeteilt. Das heisst Folgendes: die ersten X-Bits werden als Paket 1, die zweiten X-Bits werden als Paket 2, usw. definiert. Diese Pakete werden dann in einem Netzwerk (z.B. im Internet) vom Absender zum Empfänger gesendet. Die Pakete enthalten – ausser Daten – Adressen und Regeln, wie sie beim Empfänger wieder zusammengesetzt werden müssen. Auch wenn zum Teil verschlüsselt, ist alles am selben Ort, zum selben Zeitpunkt (im selben Zeitfenster), in einem Paket und im selben Netzwerk zu finden. Gerade deshalb sind die Daten in solchen Paketen in einem Netzwerk für den unbefugten Zugriff so anfällig. Diese Tatsachen machen es für Hacker erst überhaupt möglich, Leitungen «anzuzapfen» und vertrauliche Daten zu lesen oder in fremde Computer-Systeme einzudringen. Unter «Leitungen» muss man auch die drahtlosen Kommunikationskanäle verstehen.

Alle Sicherheitseinrichtungen, die eingesetzt werden (Verschlüsselung, verschiedene Algorithmen, Signatur, Firewall, virtuelle Netzwerke, Secure Sockets Layer) ändern aber nichts an den oben aufgeführten Tatsachen, und damit sind sie auch nicht in der Lage, für die Sicherheit der beteiligten Computer-Systeme zufrieden stellend zu sorgen.

Die Aufgabe der Erfindung ist es, diese Nachteile zu eliminieren. Diese Aufgabe wird durch die Merkmale des Patentanspruchs 1 gelöst.

Die räumliche (geografische) und die spektrale Trennung der Daten während der zeitlich verschobenen Übermittlung in zwei Netzwerken geben dem unbefugten Zugriff auf die eigentlichen Daten so gut wie keine Chance.

Die Quintessenz des Verfahrens sind die räumliche (geografische) und die spektrale Trennung der Daten und eine geringe Zeitverschiebung der Übermittlung in zwei Netzwerken (Duales Netzwerk) Fig. 1, sodass die getrennten Daten – durch eine neue Methode der Paketaufbereitung Tabelle 1 – bereits implizit verschlüsselt sind.

Bit Nummer	0	1	2	3	4	5	6	7	8	9	10	N	Paket-Länge*
Paket heute	1	1	0	0	1	0	0	1	1	1	0	...	4096
U-Paket*		1		0		0		1		1		...	2048
G-Paket*	1		0		1		0		1		0	...	2048

*) U-Paket = ungerade Bits, G-Paket = gerade Bits, N = Nummer, Paket-Längen sind Beispiele

Tabelle 1

Diese neue Methode der Aufbereitung der Daten in U-Pakete und in G-Pakete erzeugt zwei, für sich nutzlose Hälften der Information, die durch Hacker nicht mehr ausgewertet werden können. Die implizite Verschlüsselung bewirkt auch ein Ersparnis an Bandbreite oder eine Erhöhung des Durchsatzes.

Im Beispiel sind es 2048 Bits/Paket/ Netzwerk (U-Netzwerk und G-Netzwerk), wie in der Tabelle 1 dargestellt. Weit über der kritischen Länge pro U-Paket und pro G-Paket. Die heutigen Computer können diese Länge der Pakete nicht – innerhalb nützlicher Frist – kombinatorisch errechnen. (Alle Möglichkeiten «ausprobieren», durch ein Computer-Programm.)

Adressen, Nachricht-Identifikation (Message-ID) und die Paketnummerierung, die ebenfalls zu einem Paket gehören, werden durch dieses Verfahren nicht geändert.

Anhand eines Ausführungsbeispiels wird die Erfindung mithilfe einer Figur (Fig. 1) erläutert. Fig. 1 zeigt eine Ausführungsform des erfindungsgemässen Dualen Netzwerkes, mit einem Absender und mit einem Empfänger, sowie mit dem zurückgelegten Weg im U-Netzwerk (gestrichelte Linien) eines U-Paketes (gestrichelte Pfeile) und mit dem zurückgelegten Weg im G-Netzwerk (durchgehende Linien) eines G-Paketes (durchgehende Pfeile).

Ein Absender 1, der eine Nachricht zu einem Empfänger 8 sendet. Die Nachricht besteht aus U-Paketen 4u und aus G-Paket 4g.

Ein U-Paket 4u im U-Netzwerk 5u legt folgenden Weg zurück:
U-Anschluss 2u des Absenders 1,
U-Provider 3u des Absenders 1,
U-Netzwerk 5u,
U-Provider 6u des Empfängers 8,
U-Anschluss 7u des Empfängers 8.

Ein G-Paket 4g im G-Netzwerk 5g legt folgenden Weg zurück:
G-Anschluss 2g des Absenders 1,
G-Provider 3g des Absenders 1,
G-Netzwerk 5g,
G-Provider 6g des Empfängers 8,
G-Anschluss 7g des Empfängers 8.

Nach der Aufbereitung der U-Pakete 4u und der G-Pakete 4g folgt die Übermittlung der Daten vom Absender zum Empfänger. Die U-Pakete über das U-Netzwerk 5u, die G-Pakete über das G-Netzwerk 5g. Hier handelt es sich um zwei, klar getrennte Netzwerke (Duales Netzwerk), ohne gemeinsamen Knoten. Die Netzwerke entstehen durch eine Quasi-Verdopplung der heutigen Netzwerke, die wir U-Netzwerk und G-Netzwerk nennen (U = ungerade, G = gerade). Unter Verdopplung, ist die Verdopplung der Anzahl der Knoten – im heutigen Netzwerk – zu verstehen. Nur Quasi-Verdopplung, weil die Anzahl der U-Knoten und die Anzahl der G-Knoten nicht identisch sein müssen. (Die Anzahl Routers oder Gateways im U-Netzwerk und im G-Netzwerk müssen nicht identisch sein.) Die Knoten der beiden Netzwerke sind an verschiedenen Orten.

Das zur Verfügung stehende Spektrum (Bandbreite) wird dynamisch genutzt. Diese dynamische Zuordnung der Kanäle, die Entfernung der Knoten der beiden Netzwerke und das dynamische Routing verschaffen die räumliche (geografische) und die spektrale Trennung der U-Pakete und der G-Pakete während der Übermittlung.

Jedes End-Gerät (PC, Server) verfügt über zwei Identitäten: U-Identität, G-Identität. Die eine verbindet es mit dem U-Netzwerk, die andere mit dem G-Netzwerk. Die U-Pakete suchen ihren Weg im U-Netzwerk, die G-Pakete im G-Netzwerk. Ohne Hinweis darauf, dass sie zusammengehören und dass sie dasselbe End-Gerät erreichen werden.

Geräte, die für das Weiterleiten der Pakete im jeweiligen Netzwerk zuständig sind (Router, Gateway), sind jeweils nur an ein Netzwerk angeschlossen (U-Netzwerk oder G-Netzwerk) und erfüllen ihre Aufgaben, als ob es nur ein Netzwerk gäbe. Wie es heute – vor der Einführung des Dualen Netzwerkes – üblich ist.

Beim Empfänger, nach der Übermittlung, werden die U-Pakete und die G-Pakete wieder zusammengesetzt.

Eine Sendung besteht meistens aus mehr als nur einem Paket. Ein Bestandteil der Pakete ist eine Identifikation der Sendung (Message-ID). Im Dualen Netzwerk, eine für das U-Netzwerk und eine für das G-Netzwerk. Am Ende der Übermittlung – als letztes U-Paket – sendet der Absender die G-Nachricht-Identifikation (G-Message-ID) der Sendung im G-Netzwerk (oder umgekehrt) an den Empfänger. So ist der (berechtigte) Empfänger in der Lage, die U-Pakete und G-Pakete wieder zusammenzusetzen.

Theoretisch kann das Duale Netzwerk als N-Netzwerk verallgemeinert werden (N = 1, 2, 3,...).

Das hier vorgeschlagene Duale Netzwerk ist für beliebiges Übermittlungsmedium geeignet. Zweifellos ist das Anschliessen der End-Geräte an die zwei Netzwerke im Falle der drahtlosen Kommunikation einfacher.

Herkömmliche Zertifizierung, Signatur, Kryptografie können in Kombination mit dem Dualen Netzwerk eingesetzt werden.

Patentansprüche

1. Verfahren zum Übermitteln von elektronischen Daten, dadurch gekennzeichnet, dass die Daten beim Absender in N Arten von Paketen aufbereitet werden, in dem die Paketaufbereitung jedes N-te Bit in eine Art der N Arten von Paketen zusammenfasst, und die N Arten von Paketen unabhängig von einander, über N Netzwerken, insbesondere N Computer-Netzwerken, mit einer Zeitverschiebung, zum Empfänger gesendet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Daten beim Absender in zwei Arten von Paketen (4u, 4g) aufbereitet werden, die unabhängig voneinander, über zwei Computer-Netzwerken (5u, 5g), mit einer Zeitverschiebung, zum Empfänger gesendet werden.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die zwei Arten von Paketen (4u, 4g) über zwei getrennten Computer-Netzwerken (5u, 5g), die keine gemeinsamen Knoten enthalten, gesendet werden.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die zwei Arten von Paketen als die geraden und die ungeraden Bits der ursprünglichen Bitabfolge der Nutzinformation definieren und eine implizite Verschlüsselung enthalten.

5. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass jedes der an die zwei Computer-Netzwerke angeschlossenen End-Geräte, Absender und Empfänger, über zwei Identitäten verfügt.

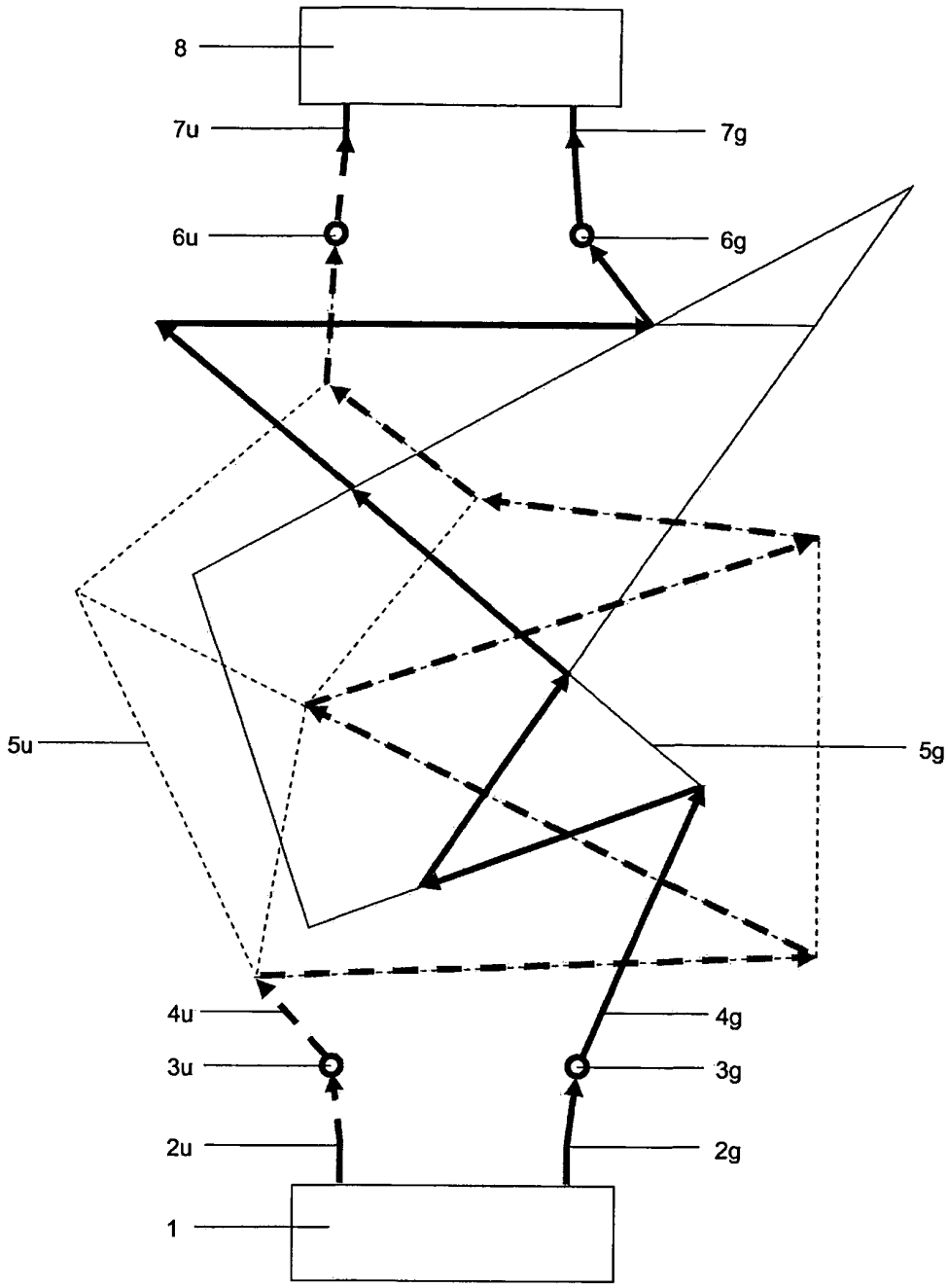
6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass je eine Identität des jeweiligen End-Gerätes, Absender und Empfänger, es mit je einem der beiden Computer-Netzwerke verbindet.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass Geräte, wie Router, Gateway, die für das Weiterleiten der Pakete im jeweiligen Computer-Netzwerk zuständig sind, jeweils nur an ein Computer-Netzwerk angeschlossen sind und ihre Aufgaben erfüllen, als ob es nur ein Computer-Netzwerk gäbe.

8. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die zwei Arten von Paketen durch die beiden, im letzten Paket gesendeten Nachricht-Identifikationen entsprechend der ursprünglichen Information sich zusammenfügen lassen.

9. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Zeitverschiebung zwischen den Übermittlungen in den zwei Computer-Netzwerken, durch die unterschiedlichen, zurückgelegten Wege, entsteht, die auch gesteuert werden kann.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Übermittlung in N Netzwerken, drahtgebunden und/oder drahtlos erfolgt.



Figur 1