

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 100 22 014.2

Anmeldetag: 05. Mai 2000

Anmelder/Inhaber: Kryptografics GmbH,
Nürnberg/DE

Bezeichnung: Verfahren und Vorrichtung zur Sicherung der
Vertraulichkeit und Abhörsicherheit bei der
Kommunikation zwischen Rechnernetzen

IPC: H 04 L, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 31. Mai 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiebinger

Patentanmeldung

"Verfahren und Vorrichtung zur Sicherung der Vertraulichkeit
und Abhörsicherheit bei der
Kommunikation zwischen Rechnernetzen"

Beschreibung

Gegenstand der Erfindung ist ein Verfahren und eine damit zu verwendende Vorrichtung mit Hilfe deren bei der Kommunikation zwischen Rechnernetzen die übermittelten Daten vor Abhören und Manipulieren gesichert werden sollen. Dabei unterliegt die Kommunikation zwischen Rechnernetzen je nach Anwendung und Datenart verschiedenen Sicherheitsanforderungen. Dementsprechend müssen unterschiedlich intensive Abwehrmaßnahmen hinsichtlich von außerhalb der Rechnernetze zu befürchtenden Eingriffen geschaffen werden.

Ein zu verhindernder Eingriff kann im unberechtigten Aufbau von Kommunikationsverbindungen bestehen, wobei ein berechtigter Teilnehmer eine Kommunikationsverbindung mit einem unberechtigten Teilnehmer herstellt. Ursache hierfür kann ein fehlerhaftes Routing von Informationen aufgrund von Fehlern in Vermittlungsknoten sowie ein fehlerhaftes Routing von Informationen aufgrund einer fehlerhaften Zieladresse sein. Letzteres resultiert aus einer beabsichtigten oder unbeabsichtigten Fehlbedienung oder aus internen Softwarefehlern. Ebenso kann ein unberechtigter Teilnehmer eine Kommunikationsverbindung zu einem berechtigten Teilnehmer aufbauen, wobei die Ursachen in einem fehlerhaften Routing von Informationen aufgrund von Fehlern in Vermittlungsknoten sowie im Vortäuschen einer falschen Identität durch einen unberechtigten Teilnehmer liegen können.

Eine weitere Bedrohung der Sicherheit liegt in der Verletzung der Integrität von Nachrichten. Diese kann durch eine gezielte Manipulation von Nachrichten durch unberechtigte Teilnehmer oder Außenstehende erfolgen.

Ebenfalls zu vermeiden ist das Nichterkennen sicherheitskritischer Ereignisse. Gemeint ist damit der Umstand, daß der Systemverwalter keine Kenntnis über sicherheitskritische Ereignisse erlangt. Solche werden beispielsweise durch einen berechtigten Teilnehmer hervorgerufen, der entweder eine Kommunikation mit einem anderen berechtigten Teilnehmer oder Versuche zum Aufbau einer Kommunikationsverbindung mit einem unberechtigten Teilnehmer durchführt, oder durch einen unberechtigten Teilnehmer, der Versuche zum Aufbau einer Kommunikationsverbindung mit einem berechtigten Teilnehmer durchführt. Die stärkste Bedrohung rührt von der Kenntnisnahme von übertragenen Nachrichten. Dabei erhält ein Angreifer auf das System von den zwischen zwei berechtigten Teilnehmern übertragenen Nachrichten Kenntnis, was zumeist auch unbemerkt geschieht. Dabei werden die übertragenen Daten entweder abgehört oder aufgezeichnet, so daß die damit verbundenen Nachrichten bzw. Informationen von unberechtigter Seite zur Kenntnis genommen werden. Ebenso ist es möglich, daß derart abgehörte Daten unbemerkt manipuliert werden. Ziel der vorliegenden Erfindung ist es somit, ein derartiges Abhören geheimer Daten zu verhindern.

Bei den bisher bekannten Verfahren zur Sicherung der Kommunikation zwischen Rechnernetzen wird die Vertraulichkeit und die Authentifizierung mit kryptografischen Verfahren angestrebt. Die dabei verwendeten kryptografischen Verschlüsselungsverfahren beruhen allesamt auf symmetrischen Block-Chiffrieralgorithmen oder gleichwertigen asymmetrischen Verfahren. Dabei besteht immer der Nachteil, daß Dritte, die die Daten abhören, diese mit einem endlichen Zeitaufwand abhängig von der technischen Entwicklung entschlüsseln können und zwar unabhängig da-

von, ob dem Angreifer auf die abgehörten Daten der verwendete Chiffrierschlüssel absichtlich oder unabsichtlich bekannt gemacht wurde.

Häufig findet eine Verschlüsselung von Daten dergestalt statt, daß vor der eigentlichen Verbindungsaufnahme ein asymmetrischer und als relativ sicher geltender Algorithmus vereinbart wird, der die weitere Kommunikation durch Verwendung eines symmetrischen und damit schnelleren Verfahrens schützen soll. Andere Systeme werden derart verschlüsselt, daß jeweils ein Schlüssel für jedes einzelne Datenpaket neu festgelegt und übermittelt wird. Nachteil aller bisher verwendeten Verfahren ist die nachträgliche Korrumpierbarkeit durch das bloße Ausprobieren verschiedener Schlüssel.

Das vorliegende Verfahren ist in der Lage, die völlige Vertraulichkeit der zu übermittelnden Daten zu sichern, da der zur Verschlüsselung verwendete Schlüssel weder voreingestellt ist noch über eine Leitung gesendet wird. Ein wesentlicher Erfindungsgedanke ist dabei unter anderem, daß der verwendete Schlüssel als Bestandteil eines kompletten Schlüsselpakets an den Orten der Kommunikation jeweils physikalisch verifiziert vorliegt. Das Verschlüsselungsverfahren selbst besteht demgemäß aus zwei Komponenten, nämlich zum einen aus der Bereitstellung des eigentlichen Schlüssels und zum anderen aus der Operationsvorschrift, mit der dieser Schlüssel auf die zu sichernden Daten angewendet wird.

Als technische Voraussetzung ist eine Kombination aus Hardware und Software erforderlich, die sich durch folgende Eigenschaften auszeichnet: Die für die Realisierung der Erfindung wesentlichen Einheiten werden zwischen die zu schützenden Netzwerke und die entsprechenden Router fest installiert. Alle routingfähigen Netzwerkprotokolle können durch die Einheiten transparent geroutet und dabei verschlüsselt werden. Nicht routingfähige Protokolle können transparent übertragen werden. Alle Datenpakete müssen von der Software auf ihren Bestimmungsort hin

überprüft werden, wobei nach interner und externer Versendung unterschieden wird, und bei Bedarf verschlüsselt wird.

Die beiden Verschlüsselungsstationen werden durch zwei Computer repräsentiert, die mit mindestens zwei Netzwerkanschlüssen, einem geeigneten Betriebssystem und der vorteilhafterweise eigenerstellten Software ausgestattet sind. Das Betriebssystem ist so eingerichtet, daß Datenpakete, die auf einer Netzwerkschnittstelle empfangen werden, nicht ohne weiteres auf die andere Schnittstelle übertragen werden können. Bedingung für diese Verwendung ist die Bearbeitung durch die laufende Anwendungssoftware. Damit wird sichergestellt, daß die normalerweise vorhandenen Routingfunktionen des Betriebssystems umgangen werden und keine Datenpakete das System so durchdringen können. Angriffe durch sogenanntes "Hacken" mit Hilfe von Personen in den geschützten Netzen werden so nach Möglichkeit unterbunden.

Das installierte Betriebssystem ist von allen Hilfsmitteln und Unterprogrammen befreit, die nicht unbedingt für die Funktion benötigt werden. Die Stationen enthalten einen Massenspeicher, der idealisiert als unendlich groß angenommen wird. Dieser Massenspeicher ist als logische Festplatte ausgeformt, kann aber auch durch andere Hardware ersetzt werden. Der Massenspeicher dient lediglich der Aufnahme der zu erzeugenden Schlüsselbibliothek. Eine weitere Hardware-Komponente kann für das Kopieren neuer Schlüssel vorgesehen werden, die durch eine gleichartige Hardware-Komponente in der Schlüsselstation zur Verfügung gestellt wird.

Der sogenannte Schlüssel in seiner physikalischen Form ist Bestandteil einer Schlüsselbibliothek, die sich aus Zufallszahlen zusammensetzt. Diese Schlüsselbibliothek entsteht dadurch, daß ein Zufallszahlengenerator beliebige Werte erzeugt und diese als 8-Bit, 16-Bit oder 32-Bit-Zahlen mit Integer-Werten aufzeichnet. Als Zufallszahlengenerator kann dabei beispielsweise ein Rauschgenerator verwendet

werden, der durch einen elektrischen Kohleschichtwiderstand eine Rauschquelle enthält. Deren gegebenenfalls zu verstärkendes Signal in Form von sogenanntem Weißen Rauschen ist normalverteilt und rein statistisch, also nicht vorhersagbar. Jede andere Quelle von rein zufälligen Werten könnte gleichermaßen genutzt werden, wie beispielsweise der Zerfall von Uranatomen, Höhenstrahlung, Quantenvorgänge und dergleichen. Wichtig dabei ist nur, daß die genutzte Zufallsquelle quantendynamischen Prozessen unterliegt, die nach dem gegenwärtigen Erkenntnisstand der Physik als nicht vorhersagbar angenommen werden müssen. Das so erzeugte Rauschen wird aufgezeichnet und geeignet auf die Stationen übertragen. Dies kann durch jede Art von portablen Datenträgern geschehen, wie beispielsweise Disketten, Festplatten, Bänder, CD's oder DVD's. Entscheidend ist dabei nur, daß die erzeugten Zufallsdaten außer auf den verwendeten Schlüsseldatenträgern sonst nicht zugänglich sind.

Als Verschlüsselungsverfahren kann prinzipiell jedes bekannte Verfahren verwendet werden. Empfohlen wird jedoch ein Verfahren beruhend auf der bitweisen XOR-Operation und ihren mathematischen Eigenschaften. Jedes zu übermittelnde Datenpaket wird mit dem geheimen Schlüssel bitweise über die Rechenoperation XOR verknüpft. Der Schlüssel wird dabei nicht mitübertragen, sondern wie bereits dargelegt, an den Orten der Kommunikation - also beim Absender und beim Empfänger - als Teil einer Schlüsselbibliothek hinterlegt. Übermittelt wird somit nur noch die Position des Schlüssels innerhalb der Schlüsselbibliothek.

Eine erfindungsgemäße Datenübermittlung besteht demgemäß aus den folgenden grundlegenden Schritten:

- Erzeugen einer Schlüsselbibliothek
- Hinterlegen der Schlüsselbibliothek an den Kommunikationsstellen in identischer Form

- Auswählen eines Schlüssels aus der Schlüsselbibliothek
- Festlegen der zu übermittelnden unverschlüsselten Daten und Aufspalten in einzelne Datenpakete
- Verschlüsselung der Datenpakete mit dem ausgewählten Schlüssel
- Verknüpfung des ausgewählten Schlüssels mit dem Datenpaket
- Übermittlung der verschlüsselten Datenpakete und der Position des Schlüssels innerhalb der Schlüsselbibliothek vom Absender an den Empfänger
- Aufsuchen des Schlüssels innerhalb der Schlüsselbibliothek anhand der Positionsangabe beim Empfänger
- Anwendung des Schlüssels auf das verschlüsselte Datenpaket beim Empfänger.

Ein Errechnen oder Erraten des Schlüssels ist dabei nicht möglich, denn es entfällt die ansonsten üblicherweise verwendete Kontrollfunktion eines zweimaligen Anwendens desselben Schlüssels auf ein Datenpaket, um zu überprüfen, ob man den Originaltext erhält. Dies liegt an der mathematischen Natur der Rechenoperation XOR, da ein zweimaliges Anwenden von XOR mit demselben Schlüssel immer den Ursprungstext liefert, unabhängig davon, ob der Schlüssel richtig oder falsch war. Demgegenüber führt bei einem Block-Chiffrieralgorithmus lediglich der richtige Schlüssel bei zweimaliger Verwendung zum Ursprungstext. Die übliche Vorgehensweise, den entschlüsselten Text nochmals zu verschlüsseln, um so das Ergebnis zu kontrollieren, entfällt damit. Dementsprechend entfällt auch die Möglichkeit eines Angriffes basierend auf "Ausprobieren", da die Richtigkeit des geratenen Schlüssels nicht überprüft werden kann.

Aus diesem Grund ist eine korrekte und zufällige, also nicht nachvollziehbare Generierung der Schlüssel beziehungsweise der Schlüsselbibliothek Kernstück der

Erfindung und damit ein sauberes Management der Schlüsselbibliothek unabdingbar und als Verfahrensschritt ebenfalls Teil dieser Erfindung.

Da mit Entwendung des Schlüsseldatenträgers auch die Entschlüsselung möglich wird, besteht ferner die Notwendigkeit einer vollständigen Zerstörung des Schlüsseldatenträgers. Diese ist als Sicherungsmaßnahme damit ebenfalls Teil des erfindungsgemäßen Verfahrens.

Patentansprüche

1. Verfahren zur Sicherung der Vertraulichkeit und Abhörsicherheit bei der Kommunikation zwischen Rechnernetzen umfassend

das Erzeugen einer Schlüsselbibliothek,
das Hinterlegen der Schlüsselbibliothek an den Kommunikationsstellen in identischer Form,
das Auswählen eines Schlüssels aus einer Schlüsselbibliothek,
das Festlegen der zu übermittelnden unverschlüsselten Daten und deren Aufspalten in einzelne Datenpakete,
die Verschlüsselung der Datenpakete mit dem ausgewählten Schlüssel,
die Verknüpfung des ausgewählten Schlüssels mit dem Datenpaket,
Übermittlung der verschlüsselten Datenpakete und der Position des Schlüssels innerhalb der Schlüsselbibliothek vom Absender an den Empfänger,
das Aufsuchen des Schlüssels innerhalb der identisch beim Empfänger hinterlegten Schlüsselbibliothek anhand einer Positionsangabe,
die Anwendung des Schlüssels auf das verschlüsselte Datenpaket beim Empfänger.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß sich die Schlüsselbibliothek aus Zufallszahlen zusammensetzt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zufallszahlen durch eine Rauschquelle in Form eines elektrischen Kohleschichtwiderstandes erzeugt werden.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zufallszahlen durch den Zerfall von Uranatomen erzeugt werden.
5. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zufallszahlen durch Höhenstrahlung erzeugt werden.
6. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zufallszahlen durch Quantenvorgänge erzeugt werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Schlüsselbibliothek bei unbefugter Entwendung des Schlüsseldatenträgers vernichtet wird.
8. Vorrichtung zur Sicherung der Vertraulichkeit und Abhörsicherheit bei der Kommunikation zwischen Rechnernetzen umfassend

Zusammenfassung

Gegenstand der Erfindung ist ein Verfahren und eine damit zu verwendende Vorrichtung mit Hilfe deren bei der Kommunikation zwischen Rechnernetzen die übermittelten Daten vor Abhören und Manipulieren gesichert werden sollen.