

**PCT**  
**WELTORGANISATION FÜR GEISTIGES EIGENTUM**  
 Internationales Büro  
**INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE**  
**INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)**

<b>(51) Internationale Patentklassifikation 5 :</b>  G06F 11/00		<b>A1</b>	<b>(11) Internationale Veröffentlichungsnummer:</b> WO 92/13307  <b>(43) Internationales Veröffentlichungsdatum:</b> 6. August 1992 (06.08.92)
---	--	-----------	--

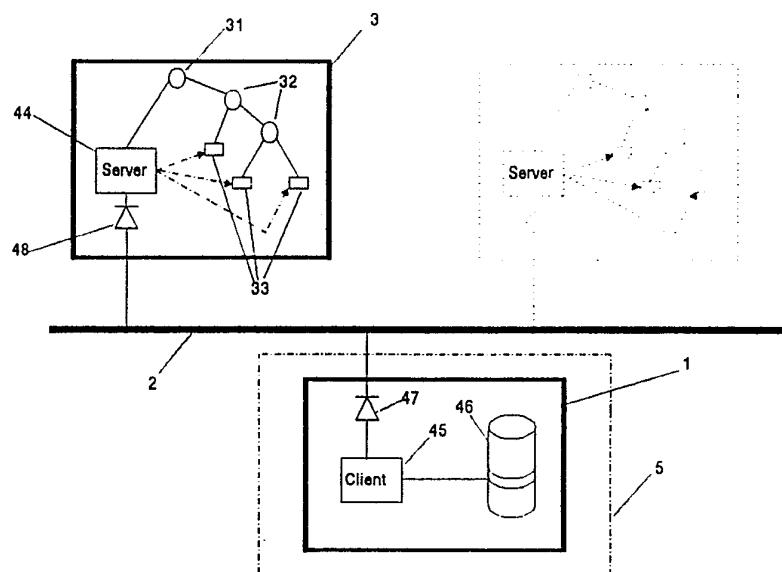
<b>(21) Internationales Aktenzeichen:</b> PCT/EP92/00061  <b>(22) Internationales Anmeldedatum:</b> 14. Januar 1992 (14.01.92)  <b>(30) Prioritätsdaten:</b> P 41 01 141.4 16. Januar 1991 (16.01.91) DE  <b>(71) Anmelder (für alle Bestimmungsstaaten ausser US):</b> SIE-MENS NIXDORF INFORMATIONSSYSTEME AG [DE/DE]; Fürstenallee 7, D-4790 Paderborn (DE).  <b>(72) Erfinder; und</b> <b>(75) Erfinder/Anmelder (nur für US):</b> GLASCHICK, Rainer [DE/DE]; Mentrupstr. 84, D-4790 Paderborn (DE).  <b>(74) Anwälte:</b> SCHAUMBURG, Karl-Heinz usw. ; Mauerkircherstr. 31, D-8000 München 80 (DE).	<b>(81) Bestimmungsstaaten:</b> AT (europäisches Patent), BE (europäisches Patent), CH (europäisches Patent), DE (europäisches Patent), DK (europäisches Patent), ES (europäisches Patent), FI, FR (europäisches Patent), GB (europäisches Patent), GR (europäisches Patent), IT (europäisches Patent), LU (europäisches Patent), MC (europäisches Patent), NL (europäisches Patent), NO, SE (europäisches Patent), US.  <b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht.</i>
---	---

**(54) Title:** METHOD AND DEVICE FOR MONITORING COMPUTER MANIPULATIONS

**(54) Bezeichnung:** VERFAHREN UND ANORDNUNG ZUR ÜBERWACHUNG VON RECHNERMANIPULATIONEN

**(57) Abstract**

Disclosed is a method and device for monitoring manipulations carried out on computers (3) connected into a net (2). The method calls for attributes of the data stored in the computers (3) to be automatically interrogated and compared with reference attributes stored under protection. In the event of non-correspondence, an alarm is triggered. Attribute interrogation, attribute comparison and triggering of the alarm are carried out by a monitoring device (1) which is connected to the computers (3) but physically inaccessible to intruders, and whose data storage containing the reference attributes cannot be interrogated.



**(57) Zusammenfassung**

Verfahren und Anordnung zur Überwachung von Manipulationen an Rechnern (3), die über ein Netzwerk (2) verbunden sind, wobei bei dem Verfahren automatisch Attribute von Datenbeständen der Rechner (3) abgefragt und mit geschützt gespeicherten Sollwerten der Attribute verglichen werden und bei einer Nicht-Übereinstimmung ein Alarm ausgelöst wird. Die Abfrage, der Vergleich und die Alarmauslösung werden von einer räumlich für Eindringlinge nicht zugänglichen, mit den Rechnern (3) verbundenen Überwachungseinrichtung (1) durchgeführt, deren die Sollwerte enthaltenden Datenbestände nicht abfragbar sind.

**LEDIGLICH ZUR INFORMATION**

Code, die zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AT	Österreich	FI	Finnland	MN	Mongolei
AU	Australien	FR	Frankreich	MR	Mauritanien
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgien	GB	Vereinigtes Königreich	NL	Niederlande
BF	Burkina Faso	GN	Guinea	NO	Norwegen
BG	Bulgarien	GR	Griechenland	PL	Polen
BJ	Benin	HU	Ungarn	RO	Rumänien
BR	Brasilien	IE	Irland	RU	Russische Föderation
CA	Kanada	IT	Italien	SD	Sudan
CF	Zentrale Afrikanische Republik	JP	Japan	SE	Schweden
CG	Kongo	KP	Demokratische Volksrepublik Korea	SN	Senegal
CH	Schweiz	KR	Republik Korea	SU	Soviet Union
CI	Côte d'Ivoire	LI	Liechtenstein	TD	Tschad
CM	Kamerun	LK	Sri Lanka	TG	Togo
CS	Tschechoslowakei	LU	Luxemburg	US	Vereinigte Staaten von Amerika
DE*	Deutschland	MC	Monaco		
DK	Dänemark	MG	Madagaskar		
ES	Spanien	ML	Mali		

Verfahren und Anordnung zur Überwachung von  
Rechnermanipulationen

Die vorliegende Erfindung betrifft ein Verfahren und eine Anordnung zur Überwachung von Manipulationen an Rechnern, die über ein Netzwerk verbunden sind, gemäß dem Oberbegriff der Ansprüche 1 bzw. 13.

Mit Manipulationen an Rechnern sind insbesondere Veränderungen an ausführbaren Programmen durch nicht-autorisierte Personen gemeint, also z.B. das "Infizieren" von Rechnern mit "Viren" oder "Trojanischen Pferden".

Zur Überprüfung, ob Manipulationen an einem Rechner stattgefunden haben, sind folgende Möglichkeiten bekannt:

- Regelmäßige manuelle Inspektion der Datenbestände. Dieser Aufwand ist nur für besonders gefährdete oder sicherheitsrelevante Fälle gerechtfertigt.
- Die Verwendung von klassifizierten Betriebssystemen. Klassifizierte Betriebssysteme sind solche, die nach Evaluationsrichtlinien wie den amerikanischen "Trusted Computer System Evaluation Criteria", den deutschen

"IT-Sicherheitskriterien" oder ähnlichen Regelsammlungen entsprechen. Klassifizierte Betriebssysteme haben ab bestimmten Klassen eingebaute Sicherheitsstufen, die Manipulationen erschweren. Beispielsweise sind ab der Klasse B2 der obengenannten "Trusted Computer System Evaluation Criteria" sogenannte "Access Control Lists" vorgeschrieben, die eine feinere Abstufung der Schreibprivilegien erlauben. Vorgeschriebene Protokolldateien erleichtern die Erkennung von Manipulationen, verhindern sie aber nicht. Gelingt es einem Eindringling jedoch, sich die entsprechenden Privilegien zu verschaffen, so kann er wie in herkömmlichen Systemen Dateien manipulieren.

- Versiegelung der Dateien und Dateiverzeichnisse durch Sig-naturen und Überprüfung bei Zugriff. Eine solche Versiegelung ist z.B. aus der DE-OS 37 36 760 oder der EP-0 137 075 bekannt. Um eine hinreichende Sicherheit zu erzielen, darf die Überprüfung der Versiegelung nicht auf der Anwenderebene erfolgen, sondern muß von einem speziell hierfür modifizierten Betriebssystem durchgeführt werden. Dabei wird vorausgesetzt, daß das Betriebssystem vom Eindringling nicht manipuliert wird. Dieses Verfahren bleibt problematisch, wenn die Versiegelung auf dem Rechner selbst erzeugt werden kann, weil dann ein Eindringling selbst neue Siegel für die manipulierten Dateien erzeugen kann. In dem IBM-Betriebssystem MVS ist z.B. ein Schutz gegen Manipulation möglich, indem gekennzeichnete Dateien nur nach Zustimmung durch den Systemverwalter geändert werden können. Diese Möglichkeit erfordert jedoch einen hohen systemadministrativen Aufwand, damit die Zustimmung des Systemverwalters auch immer zum geeigneten Zeitpunkt möglich ist.

- Automation der regelmäßigen Inspektion gemäß dem Oberbegriff des Anspruchs 1, wobei auf dem zu überwachenden Rechner in einer geschützten Datei Prüfsummen oder sonstige Attribute über die zu schützenden Dateien gespeichert werden und in regelmäßigen Abständen durch ein Programm verifiziert werden. Dieses Verfahren ist insofern wünschenswert, als es keinen Personalaufwand bedeutet und ohne Eingriff in das Betriebssystem auskommt. Es hat jedoch den Nachteil, daß es keinen geeigneten Schutz gegen Eindringlinge bietet. Hat sich ein Eindringling erst einmal Zugang zum Rechner verschafft, so wird er sich bevorzugt darüber informieren, welche Sicherheitsmechanismen vorhanden sind. Eine der ersten Manipulationen bestände dann darin, diese Schutzmechanismen auszuschalten, da die automatische Inspektion praktisch nicht zu verbergen ist. Dies ist für den Eindringling in der Regel praktikabel, weil das Programm, das die zu schützenden Dateien verifizieren soll, auf dem Rechner selbst vorhanden und somit Manipulationen ausgesetzt ist.

Es ist die Aufgabe der Erfindung, ein Verfahren und eine Anordnung zu schaffen, mit denen die Möglichkeit einer unbemerkten Manipulation an über ein Netzwerk verbundenen Rechnern verringert werden kann und die mit einem Standard-Betriebssystem betrieben werden.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den Merkmalen des Anspruchs 1 und eine Anordnung mit den Merkmalen des Anspruchs 13 gelöst. Vorteilhafte Weiterbildungen sind Gegenstand der Unteransprüche.

Die Erfindung geht davon aus, daß sich durch die Manipulation von Datenbeständen (z.B. Dateien und/oder Dateiverzeichnissen) auch deren Attribute ändern. Der besondere

Vorteil liegt in dem Prinzip, daß eine für Eindringlinge nicht zugängliche Überwachungseinrichtung (z.B. ein Rechner, der in einem abgeschlossenen Raum aufgestellt ist, zu dem nur eine sehr begrenzte Anzahl von Personen Zugang hat) mit den anderen Rechnern ventilartig verbunden ist. Ventilartig heißt in diesem Zusammenhang, daß die Überwachungseinrichtung zwar auf die an dem Netzwerk angeschlossenen Rechner zugreifen kann, ein Eindringling, der in einen dieser Rechner eingedrungen ist, jedoch nicht auf die Überwachungseinrichtung zugreifen kann. Somit liegt eine Art übergeordnete Überwachungsinstanz vor. Ein Programm zur Überprüfung von Dateibeständen liegt also nicht auf dem zu überprüfenden Rechner selbst vor, sondern in der geschützten Überwachungseinrichtung, die vorzugsweise ein Überwachungsrechner ist. Durch diese Aufteilung wird der für Eindringlinge notwendige Aufwand, den Schutz abzuschalten, ohne daß ein Alarm ausgelöst wird, erheblich erhöht.

Das erfindungsgemäße Verfahren wird vorzugsweise auf Dateien angewandt, die einer zentralen Administration, z.B. durch einen Systemverwalter, unterliegen. Insbesondere Teile des Betriebssystems und die das System steuernden Dateien fallen hierunter. Dieser Schutz ist besonders wichtig, da ihre Manipulation das gesamte System gefährden kann.

Das Abfragen der Datenbestandsattribute durch die Überwachungseinrichtung kann automatisch und in regelmäßigen Zeitabständen durchgeführt werden. Bei einer anderen bevorzugten Ausführungsform kann das Abfragen bewußt in unregelmäßigen Zeitabständen durchgeführt werden, so daß ein Eindringling die zwischen regelmäßigen Überprüfungen vorliegenden Zeiten nicht zur Manipulation ausnutzen kann.

Bevorzugt fragt die Überwachungseinrichtung die Datenbestandsattribute mehrerer Rechner zeitverschachtelt ab und

vergleicht sie mit Sollwerten. Dies ist insbesondere dann von Nutzen, wenn die Überwachung synchron abläuft, die Überwachungseinrichtung also nach der Abgabe einer Abfrage wartet, bis der Rechner das Dateiattribut zurückmeldet. Aus Gründen der Betriebssicherheit muß die Überwachungseinrichtung einen Zeitgeber enthalten, um ausbleibende Quittungen zu erkennen und als fehlgeschlagene Abfrage zu werten. Da das Zurückmelden von Abfragen durch die Rechner eine gewisse Zeit benötigt, ist es sinnvoll, die Abfragen durch die Überwachungseinrichtung zeitverschachtelt abzugeben.

Gemäß einem besonders bevorzugten Ausführungsbeispiel wird die Abfrage der Dateibestandsattribute durch eine sogenannte "Client-Server-Architektur" realisiert. Die Überwachungseinrichtung ist ein Überwachungsrechner, auf dem ein Prüferprogramm (client) und mindestens eine Datei vorhanden ist, in der die zu überprüfenden Dateibestände und die jeweiligen Sollwerte ihrer Attribute gespeichert sind. Auf den zu überprüfenden Rechnern ist jeweils mindestens ein Dienstprogramm (server) implementiert, das auf Auftrag die Attribute der Dateibestände auf diesem Rechner berechnen und über das Netzwerk zurückmelden kann.

Auf den Rechnern sind zur Kommunikation zwischen den Rechnern üblicherweise auch Dienstprogramme implementiert, die einen "Einstieg" in den Rechner über das Netzwerk ermöglichen. Zumindest ein solches Dienstprogramm darf auf dem Überwachungsrechner nicht implementiert sein, um den ventilartigen Anschluß des Überwachungsrechners an das Netzwerk zu gewährleisten.

Die bislang beschriebene Anordnung erhöht die Sicherheit erheblich, ohne daß das auf den zu überprüfenden Rechnern installierte Betriebssystem modifiziert werden müßte.

Ein Eindringling kann jedoch die Kommunikation zwischen Überwachungsrechner und zu überprüfenden Rechnern aufzeichnen und somit die Datei auf dem Überwachungsrechner rekonstruieren, die u.a. die Sollwerte der Attribute speichert. Es besteht also die Möglichkeit, daß ein Eindringling das Dienstprogramm auf dem zu überprüfenden Rechner durch ein Dienstprogramm ersetzt, welches die Attribute der Dateibestände auf dem Rechner gar nicht berechnet, sondern einfach der rekonstruierten Datei entnimmt. Dieses Ziel kann allerdings nicht einfach erreicht werden, da angenommen werden muß, daß ein Eindringling alle Dateien und Programme durch eigene ersetzen kann und ggfs. auch den Rechner auf dem Netzwerk nachbilden kann.

Um jedoch auch eine solche Manipulation zu verhindern, kann die Sicherheit des erfindungsgemäßen Verfahrens durch bevorzugte Ausführungsformen weiter erhöht werden.

Eine erste bevorzugte Möglichkeit der weiteren Absicherung besteht darin, die Kommunikation über das Netzwerk zu verschlüsseln. Da jedoch im Normalfall immer dieselben Meldungen übertragen werden (z.B. da sich die Dateiattribute von Betriebssystemdateien in der Regel nicht verändern), wird bevorzugt eine Verschlüsselung mit wechselnden Schlüsseln angewandt. Diese wechselnden Schlüssel könnten z.B. nach dem bekannten Verfahren von Diffie und Hellmann erzeugt werden (W. Diffie und M.E. Hellmann, New Directions in Cryptography, I.E.E. Trans. Inf. Series, Nr. 6, November 1976, S. 140). Dieses bekannte Verfahren ermöglicht die Erzeugung eines gemeinsamen Schlüssels zweier Teilnehmer durch einen öffentlichen Dialog, ohne daß ein Zuhörer den Schlüssel rekonstruieren kann.

Eine andere bevorzugte Möglichkeit zur weiteren Erhöhung der Sicherheit besteht darin, zur Eröffnung der Kommunikation

zwischen Prüferprogramm und Dienstprogramm ein sicheres Authentisierungsprotokoll ablaufen zu lassen. Ein solches Authentisierungsprotokoll ist z.B. aus der DE-OS 38 17 484 bekannt. Dabei ist im Dienstprogramm ein geheimer Schlüssel durch ein einfaches Verfahren, z.B. durch Verknüpfung mit XOR mit einem festen, gleichfalls gespeicherten Wert chiffriert.

Eine dritte Möglichkeit zur Erhöhung der Sicherheit besteht darin, das Dienstprogramm zur Berechnung und Abgabe der Dateiattribute in ein weiteres, bereits vorhandenes Dienstprogramm zu integrieren, wodurch der Aufwand eines Eindringlings erheblich steigt, da er nun ein Dienstprogramm durch eines ersetzen muß, das für die ursprünglich auszuführenden Dienste unverändert funktionieren muß. Falls dies nicht geschieht, würde das Fehlverhalten auffallen. Vorzugsweise kann der Programmtext dieses erweiterten Dienstprogramms vor einer Kommunikation mit dem Überwachungsrechner an diesen übermittelt werden, wo der tatsächliche Programmtext mit einem Sollwert verglichen wird.

Eine vierte Möglichkeit zur Erhöhung der Sicherheit besteht darin, daß man auf den Rechnern keine vollständigen Dienstprogramme zur Berechnung der Dateiattribute, sondern lediglich Ladeprogramme implementiert. Das eigentliche Dienstprogramm liegt lediglich auf dem Überwachungsrechner vor, der dieses vor Beginn einer Überprüfung eines Rechners an dessen Ladeprogramm sendet. Somit kann ein Eindringling das Dienstprogramm nicht modifizieren, da es auf dem Rechner gar nicht vorhanden ist. Um zu verhindern, daß ein Eindringling ein Täusch-Ladeprogramm implementiert, das das übermittelte Dienstprogramm einfach ignoriert, wird das Dienstprogramm im Überwachungsrechner vorzugsweise mit einer gewöhnlichen oder einer kryptographischen Prüfsumme versehen, die von dem Ladeprogramm zurückgegeben werden muß. Hierzu kann vor dem

Absenden des Dienstprogramms eine Zufallszahl in dieses eingetragen werden, so daß jedes Mal eine neue Prüfsumme übermittelt werden muß. Alternativ kann auf die Prüfsumme verzichtet und stattdessen im Dienstprogramm ein wechselnder Schlüssel für eine symmetrische Verschlüsselung der Dialoge versteckt gespeichert werden.

Wird bei einer Prüfung der Dateibestandattribute oder der Authentizität des zu überprüfenden Rechners eine Abweichung festgestellt, so sind verschiedene Möglichkeiten der Auswertung gegeben. Beispielsweise kann ein Eintrag in eine entsprechende Datei erfolgen. Es kann auch eine Nachricht an einen Systemverwalter geschickt werden. Alternativ kann eine Alarmglocke ausgelöst werden. Ein weiteres Dienstprogramm in dem zu überprüfenden Rechner kann angesprochen werden, das diesen Rechner deaktiviert. Wenn als Netzwerk ein Bus-Netzwerk wie Ethernet eingesetzt wird, kann der Rechner auch vom Überwachungsrechner aus vom Netzwerk isoliert werden. Hierzu kann eine Hardware-Einrichtung ständig die Datenpakete auf dem Netz überwachen. Sendet der Rechner ein Paket (oder soll er eines empfangen), so kann dieses durch die Hardware-Anordnung erkannt werden, da die Pakete die Adresse des Rechners in einer bestimmten Position tragen. Die Hardware-Einrichtung kann dann veranlassen, daß sich der Überwachungsrechner nicht protokollgemäß verhält, sondern den Rechner stört. Damit ist auf jeden Fall sichergestellt, daß der in Verdacht geratene Rechner vom Netzwerk isoliert ist.

Die Erfindung wird nachstehend anhand von bevorzugten Ausführungsbeispielen unter Bezugnahme auf die beigegebene Zeichnung beschrieben.

Fig. 1 ist eine schematische Darstellung einer Ausführungsform der Anordnung der Erfindung;

Fig. 2 ist eine detaillierte Darstellung der Anordnung gemäß Fig. 1;

Fig. 3 ist eine schematische Darstellung des Ablaufs der Kommunikation zwischen Prüferprogramm und Dienstprogramm;

Fig. 4 ist ein Beispiel der Datei auf dem Überprüfungsrechner, die zu überprüfende Dateien eines Rechners und Beispielen von diesen Dateien zugeordneten Attributen enthält;

Fig. 5 zeigt beispielhaft den Pseudo-Code für ein Dienstprogramm; und

Fig. 6 zeigt beispielhaft den Pseudo-Code für das Prüferprogramm.

Fig. 1 zeigt schematisch die erfindungsgemäße Anordnung mit einem Überwachungsrechner 1, der über ein (lokales) Netzwerk 2 mit einem oder mehreren zu überprüfenden Rechnern 3 verbunden ist. Als lokales Netzwerk wird im Beispiel das Bus-System 4 "Ethernet" mit dem Protokoll TCP/IP verwendet; es ist jedoch auch möglich, andere Arten von Netzwerken zu verwenden und das TCP/IP-Protokoll kann auch über serielle Leitungen und Vermittlungsrechner abgewickelt werden. Der Überwachungsrechner 1 ist durch eine Abschirmung 5 physisch gesichert, so daß zu ihm kein unbefugter Zugriff möglich ist. Hierzu kann beispielsweise ein besonderer, abschließbarer Raum dienen, zu dem nur eine bekannte kleine Anzahl von Mitarbeitern Zutritt hat.

Fig. 2 zeigt eine detailliertere Darstellung dieser Anordnung, auf der per Software eine Client-Server-Architektur implementiert ist. In dem zu überprüfenden Rechner 3 ist ein

Dateibaum mit einer Wurzel 31, Unterverzeichnissen 32 und Dateien 33 vorhanden. Auf diesem Rechner 3 ist auch ein Dienstprogramm (Server) 44 installiert.

In dem Überwachungsrechner 1 läuft das Prüferprogramm (Client) 45 ab, das aus einer Datei 46 die Namen und die Soll-Attribute der zu überprüfenden Dateien im Rechner erhält. Für jeden Eintrag in der Datei 46 wird ein Auftrag zur Berechnung der Attribute einer Datei an das Dienstprogramm 44 geschickt, das seinerseits die benannte Datei 33 ermittelt, deren Attribute bestimmt und als Antwort zurück zum Prüferprogramm 45 übermittelt. Diese Antwort wird von dem Prüferprogramm 45 mit den Sollwerten in der Datei 46 verglichen.

Die Diodensymbole 47 und 48 deuten die ventilartige Eigenschaft der verwendeten Client-Server-Architektur an. Dabei ist zumindest das Diodensymbol 48 redundant. Wesentlich ist, daß auf den Überwachungsrechner 1 nicht zugegriffen werden kann.

Der Überwachungsrechner 1 wird so konfiguriert, daß auf ihm keine Dienstprogramme aktiv sind oder aktiviert werden können. Der Überwachungsrechner ist insoweit vom Netzwerk isoliert.

Auf den Rechnern 3 können neben dem zur Überprüfung verwendeten Dienstprogramm 44 auch noch weitere Programme, also auch Prüferprogramme und Dienstprogramme aktiv sein. Auf dem Überwachungsrechner können noch weitere Prüferprogramme alternativ oder parallel aktiviert werden, um dem Bedienpersonal z.B. einen Dialogzugriff auf den zu testenden Rechner zu erlauben.

Fig. 3 zeigt schematisch den Ablauf der Kommunikation zw-

schen dem Prüferprogramm 45 und dem Dienstprogramm 44. Der Schritt "Auftrag erstellen" 23 findet im Prüferprogramm 45 statt. Der Schritt "Auftrag übermitteln" 24 erfolgt über das Netzwerk 2. Der Schritt "Auftrag bearbeiten" 25 findet im Dienstprogramm 44 statt, der Schritt "Auftrag rückmelden" 26 erfolgt wiederum über das Netzwerk 2 und der Schritt "Auftrag abschließend verarbeiten" 27 findet wiederum im Prüferprogramm 46 statt. Wie in Fig. 3 dargestellt, wird dieser Ablauf mehrfach wiederholt. Im vorliegenden Fall besteht ein Auftrag darin, die Attribute einer Datei auf dem zu überprüfenden Rechner 3 zu ermitteln.

Die Aufträge werden üblicherweise synchron durchgeführt, d.h. das Dienstprogramm 44 führt den Auftrag sofort aus und meldet das Resultat an das Prüferprogramm 45 zurück. Das Prüferprogramm 45 wiederum, nachdem es den Auftrag über das Netzwerk 2 geschickt hat, wartet auf das Eintreffen der Antwort vom Dienstprogramm 44. Um die Rechenkapazitätsauslastung insbesondere des Überwachungsrechners 1 zu erhöhen, können die Aufträge an die verschiedenen Rechner auch zeitverschachtelt abgegeben und empfangen werden.

Bei rechenzeit-kritischen Anwendungen kann das Dienstprogramm 44 für einen Auftrag auch eine Auftragsdatei zur späteren Ausführung bilden (Batch-Job); durch die erheblich größere Zeitschranke, die üblicherweise bis zu einer Stunde andauern kann, erhöht sich die Chance für einen Eindringling jedoch erheblich, die Auftragsdateien zu manipulieren. Dies ist in der Regel einfacher, als das Dienstprogramm zu manipulieren.

Die Client-Server-Architektur ist durch Software realisiert. Bei synchroner Ausführung wird jedoch in der Regel ein Netzwerk gefordert sein, das schnelle Transportfunktionen zur Verfügung stellt. Ethernet hat den Vorteil, daß mit dem

Zugang zum physikalischen Medium, dem Kabel, ein Zugang zu allen bislang angeschlossenen Rechnern möglich ist, ohne daß eine zentrale Konfigurationsverwaltung aktiviert werden muß. Für die vorgeschlagene Anordnung ist die Art des Netzwerks jedoch unerheblich. Es wird lediglich vorausgesetzt, daß das Prüferprogramm 45 auf dem Überwachungsrechner 1 das Dienstprogramm 44 auf dem zu überwachenden Rechner 3 initiieren kann und ein Resultat zurückhält. Die Ventilwirkung zwischen Netzwerk 2 und Überwachungsrechner 1 kann auch per Hardware erzeugt werden; diese Lösung ist jedoch nicht so elegant, da sie auf einer höheren Ebene erfolgen muß. Der Überwachungsrechner 1 muß ja Antworten vom zu überwachenden Rechner 3 erhalten, so daß eine bidirektionale Kommunikation notwendig ist. Eine Ventilwirkung der Hardware müßte daher auf die Inhalte der über das Netzwerk übertragenen Datenblöcke wirken. Es ist wesentlich einfacher, die Software auf dem Überwachungsrechner 1 so zu konfigurieren, daß sie die Inhalte der ankommenden Datenpakete nur im Rahmen des Überwachungsprotokolls interpretiert und keinen allgemeinen Zugriff zuläßt.

Die vorstehend beschriebene Anordnung und das Verfahren erhöhen die Sicherheit gegen unbemerkte Manipulationen von an dem Netzwerk angeschlossenen Rechnern beträchtlich. Eine noch weitergehende Sicherheit kann dadurch erreicht werden, daß - wie bereits beschrieben - die Kommunikation zwischen Prüferprogramm 45 und Dienstprogramm 44 verschlüsselt wird, vorzugsweise mit wechselnden Schlüsseln,

- daß vor der eigentlichen Abwicklung eines Auftrages ein sicheres Authentisierungs-Protokoll, z.B. nach Beth (DE 38 17 484) abläuft,
- daß das Dienstprogramm 44 in ein anderes auf dem Rechner 3 vorliegendes, möglichst komplexes Dienstprogramm

eingebunden wird oder

- daß auf dem Rechner 3 nicht das vollständige Dienstprogramm 44 vorliegt, sondern lediglich ein Ladeprogramm vorgesehen ist, welches das eigentliche Dienstprogramm 44 von dem Überwachungsrechner 1 erhält.

Diese Möglichkeiten der weiteren Erhöhung der Sicherheit gegen Rechnermanipulationen können ggfs. auch kombiniert werden.

Zu den einzelnen Möglichkeiten der Sicherheitserhöhung wird noch folgendes angemerkt.

Ein Authentisierungsverfahren ist keine Verschlüsselung eines Datenaustausches im herkömmlichen Sinne. Beim Authentisierungsverfahren ist nicht die Vertraulichkeit des Daten austausches zu sichern, sondern die Authentizität der Nachrichten. Es muß also sichergestellt sein, daß die erwartete Antwort auch unverfälscht vom angenommenen Dienstprogramm 44 kommt.

Das Verfahren des Ladeprogrammes erlaubt es, das Dienstprogramm 44 mit einer ständig wechselnden Kennung zu versehen. Damit ist für die oben angegebenen Authentisierungsprotokolle eine besser gesicherte Schlüsselspeicherung gegeben, weil die Zeitspanne zur Extraktion des Schlüssels und zum Einbau in ein Täuschungs-Dienstprogramm geringer ist, als wenn das Dienstprogramm permanent auf dem überwachenden Rechner vorhanden ist. Ein Täuscher-Ladeprogramm ist ohne Nutzen für einen Eindringling, da dieser das übermittelte Dienstprogramm 44 zur Ausführung bringen muß, um eine authentische Rückantwort zum Überwachungsrechner 1 zu erzeugen.

Als symmetrische Verschlüsselung wird üblicherweise ein

Verfahren bezeichnet, bei dem ein und derselbe Schlüssel zur Ver- und Entschlüsselung verwendet wird. Als Beispiel wird der umfassend bekannte amerikanische "Data Encryption Standard" (DES) genannt.

Eine Prüfsumme herkömmlicher Art, beispielsweise als Quer- summe oder cyclischer Code (cyclische Redundanzüberprüfung, CRC), erlaubt es mit einfachen Mitteln, zu einer Datei eine zweite Datei zu konstruieren, deren Prüfsumme gleich der ersten Datei ist. Als kryptographische Prüfsumme (genauer: kryptographisch sichere Prüfsumme) wird ein Verfahren bezeichnet, das zu einer Datei eine Prüfsumme berechnet, so daß diese Berechnung effizient erfolgen kann, es jedoch praktisch unmöglich ist, eine zweite Datei zu finden, die dieselbe Prüfsumme hat. Ein Beispiel hierfür ist das Verfahren von Juenemann, beschrieben im ISO-Standard X500, Teil III.

Es ist weiterhin anzumerken, daß zur Realisierung der oben angesprochenen Client-Server-Architektur in jüngster Zeit vermehrt eine spezielle Programmiertechnik zur Realisierung der Programm-zu-Programm-Kommunikation verwendet wird, die mit "Remote Procedure Call" bezeichnet wird.

Die Arten der zur Überprüfung verwendeten Attribute der Dateibestände haben keinen Einfluß auf die Erfindung; sie sind vielmehr eine der wesentlichen Eigenschaften des zu überwachenden Rechners. Allein die kontinuierliche Überprüfung der Attribute unter Verzicht auf Prüfsummen bietet einen signifikanten Schutz gegen Manipulationen, da viele Manipulationsverfahren bekannt sind, bei denen eine Änderung der Dateiattribute bewirkt wird.

Fig. 4 zeigt ein Beispiel der Inhalte einer Datei 46, die die zu überprüfenden Dateinamen (file name) und jeweils

dazugehörige Attribute wie eine Prüfsumme, Prioritätsattribute, die Zugehörigkeit, die Größe und das Datum der Datei enthält.

Fig. 5 zeigt ein Beispiel des Pseudocodes für ein Dienstprogramm 44, und Fig. 6 zeigt ein Beispiel für den Pseudocode eines Prüferprogramms 45.

Patentansprüche

1. Verfahren zur Überwachung von Manipulationen an Rechnern (3), die über ein Netzwerk (2) verbunden sind, bei dem automatisch Attribute von Datenbeständen der Rechner (3) abgefragt und mit geschützt gespeicherten Sollwerten der Attribute verglichen werden und bei dem bei einer Nicht-Übereinstimmung ein Alarm ausgelöst wird, dadurch gekennzeichnet, daß die Abfrage, der Vergleich und die Alarmauslösung von einer räumlich für Eindringlinge nicht zugänglichen, mit den Rechnern (3) verbundenen Überwachungseinrichtung (1) durchgeführt werden, deren die Sollwerte enthaltenden Datenbestände nicht abfragbar sind, wobei die Abfrage vorzugsweise über das Netzwerk (2) stattfindet.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Überwachungseinrichtung (1) die Datenbestandsattribute mehrerer Rechner (3) zeitverschachtelt abfragt und mit Sollwerten vergleicht.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Überwachungseinrichtung (1) das Abfragen der Datenbestandsattribute in regelmäßigen Zeitabständen durchführt.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Überwachungseinrichtung ein Überwachungsrechner (1) ist, der mindestens ein Prüfungsprogramm (45) und mindestens eine Datei (46) zur Speicherung von Namen der zu überprüfenden Datenbestände und von Sollwerten der Attribute der jeweiligen Datenbestände hat, daß die Rechner (3)

jeweils mindestens ein Dienstprogramm (44) haben, das Attribute von Datenbeständen des jeweiligen Rechners (3) berechnet und über das Netzwerk (2) abgibt, daß das Abfragen eines Attributs dadurch erfolgt, daß das Prüfungsprogramm (45) einen Auftrag an das entsprechende Dienstprogramm (44) abgibt und das über das Netzwerk (2) ankommende Attribut mit dem gespeicherten Sollwert des Attributs vergleicht, und daß die Datenbestände des Überwachungsrechners (1), der kein Dienstprogramm hat, nicht abfragbar sind.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Kommunikation zwischen Prüferprogramm (45) und Dienstprogramm (44), vorzugsweise mit wechselnden und gemäß dem Diffie-Hellmann-Verfahren erzeugten Schlüsseln verschlüsselt wird.
6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß vor der Abfrage der Datenbestandsattribute ein Authentisierungsverfahren abläuft, welches sicherstellt, daß die abgefragten Attribute von den Dienstprogrammen (44) stammen.
7. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß in den Rechnern jeweils anstelle eines Dienstprogrammes (44) nur ein Ladeprogramm gespeichert ist, das das Dienstprogramm (44) laden kann, und daß das Dienstprogramm (44) im Überwachungsrechner (1) gespeichert ist und vor der Abfrage der Dateibestandsattribute über das Netzwerk an das Ladeprogramm im jeweiligen Rechner (3) gesendet wird.
8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß das in dem Überwachungsrechner (1) vorliegende Dienstprogramm (44) vor dem Absenden an den Rechner

- (3) mit einer gewöhnlichen oder kryptographischen Prüfsumme beaufschlagt wird, und daß das Ladeprogramm diese Prüfsumme extrahiert und an den Überwachungsrechner (1) zur Überprüfung zurücksendet.
9. Verfahren nach einem Ansprüche 1 bis 8, dadurch gekennzeichnet, daß beim Auslösen eines Alarms eine Nachricht an den Systemverwalter abgegeben und/oder der betreffende Rechner (3) vom Netzwerk (2) getrennt wird.
10. Anordnung zur Überwachung von Manipulationen an Rechnern (3), die über ein Netzwerk (2) verbunden sind, dadurch gekennzeichnet, daß eine räumlich für Eindringlinge nicht zugängliche zentrale Überwachungseinrichtung (1) vorgesehen ist, die mit den Rechnern (3) verbunden und so eingerichtet ist, daß sie auf die Rechner (3) zugreifen kann, diese aber nicht auf sie zugreifen können, wobei die Überwachungseinrichtung vorzugsweise ein mit den Rechnern (3) über das Netzwerk (2) verbundener Überwachungsrechner (1) ist.

1 / 7

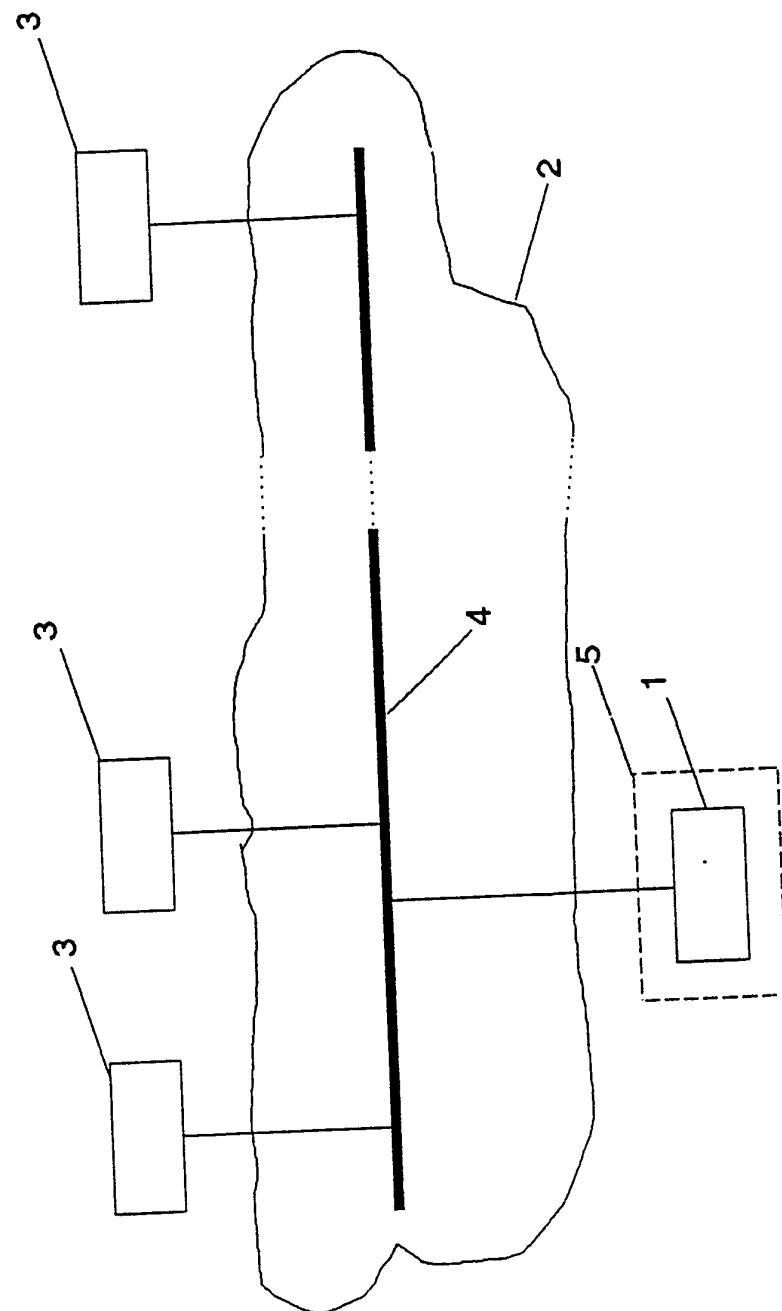


Fig. 1

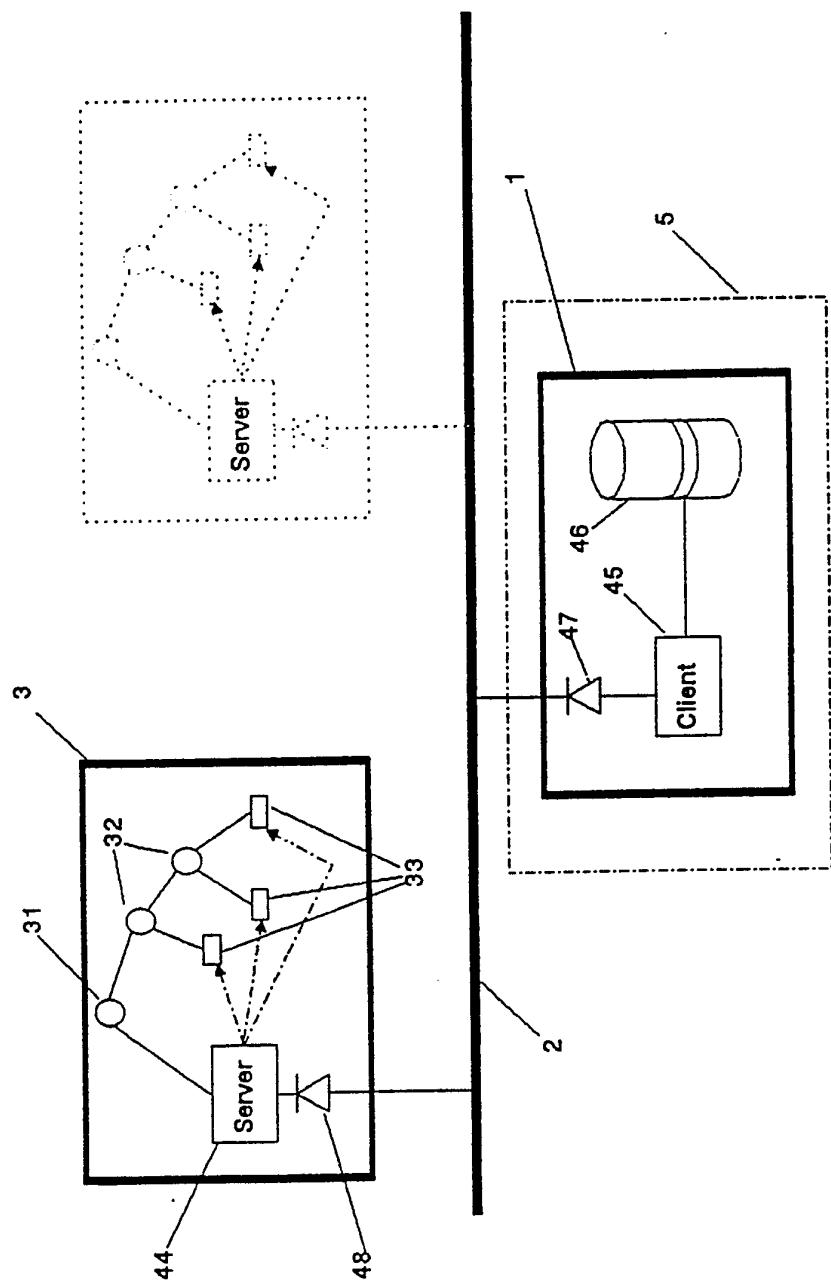


Fig. 2

3 / 7

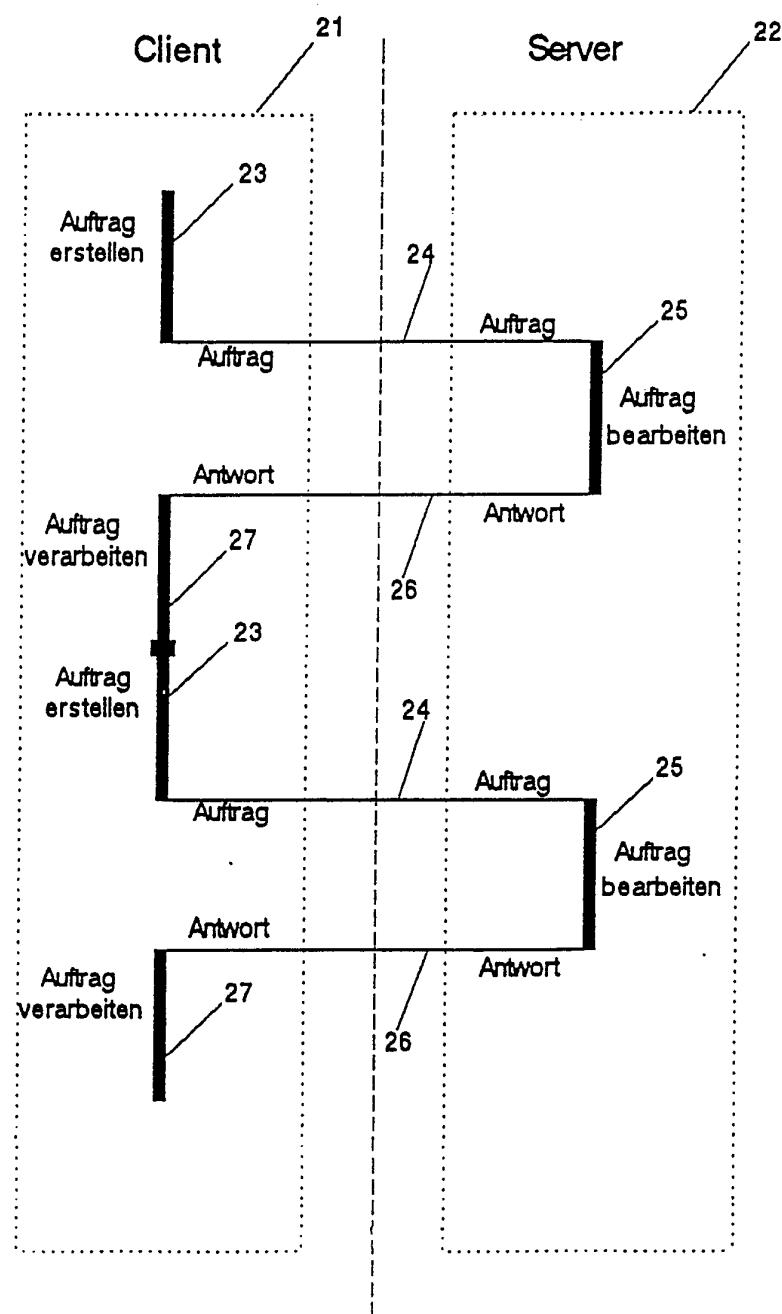


Fig. 3

4 / 7

Check Attributes		Owner	Size	Date	Filename
53262	-rwxr-xr-x	bin	1982	Jan 2 1987	/bin/cat
10001	-rwxr-xr-x	bin	2838	Jan 2 1987	/bin/cp
54895	-rwxr-xr-x	bin	738	Jan 2 1987	/bin/getlf
44447	-rwxr-xr-x	bin	7796	Jan 2 1987	/bin/ls
49875	-rwxr-xr-x	bin		25 Aug 26 1987	/bin/m
46614	-rwsr-xr-x	root	1862	Jan 2 1987	/bin/mkdir
53693	-rwxr-xr-x	bin	2792	Jan 2 1987	/bin/rm
22095	-rwxr-xr-x	bin	23252	Jan 2 1987	/bin/sh
49138	-rwxr-xr-x	bin	492	Jan 2 1987	/bin/sync
20799	-rwxr-xr-x	bin		23 Aug 26 1987	/bin/u
17310	-rw-r--r--	bin		20 Aug 26 1987	/etc/message
39939	-rwsr-xr-x	root	1720	Jan 2 1987	/etc/mount
32521	-rw-r--r--	bin	167	May 13 1989	/etc/passwd
29946	-rw-r--r--	bin	81	Jan 1 1970	/etc/rc
8244	-rw-r--r--	bin	4	Jan 2 1987	/etc/ttys
15331	-rwxr-xr-x	root	3443	Aug 30 1987	/etc/uhr
35933	-rwsr-xr-x	root	1588	Jan 2 1987	/etc/umount
57110	-rwxr-xr-x	bin	926	Jan 2 1987	/etc/update

Fig. 4

5 / 7

```
request_packet = record
    pathname: string;
end;

reply_packet = record
    checksum: integer;
    attributes: word;
    owner: integer;
    modification: date;
    pathname: string;
end;

procedure server;
in: request_packet;
out: reply_packet;

begin
    while get(in) do begin
        out.checksum = sum(in.pathname);
        out.attributes = get_from_dir(in.pathname, attr);
        out.owner = get_from_dir(in.pathname, ownr);
        out.modification = get_from_dir(in.pathname, mfd);
        put(out);
    end;
end;
```

Fig. 5

6 / 7

```
request_packet = record
    pathname: string;
end;

reply_packet = record
    checksum: integer;
    attributes: word;
    owner: integer;
    modification: date;
    pathname: string;
end;

line_in_file = record
    checksum: integer;
    attributes: word;
    owner: integer;
    modification: date;
    pathname: string;
end;

procedure check_one_system(sysname: string);
    in: request_packet;
    out: reply_packet;
    item: line_in_file;
    items: FILE;
    port: integer;
    ok: boolean;

begin
    port := open_server(sysname, "check_files");
    items := open(sysname);
```

Fig. 6-1

7 / 7

```
while readline(item) do begin
    in.pathname := item.pathname;
    send(port, in);
    out := receive(port);
    if (out.checksum = item.checksum)
    and (out.attributes = item.attributes)
    and (out.owner = item.owner)
    and (out.access = item.access)
    then continue;
    /* !!!! Difference found !!!! */
    Alarm(sysname, item.pathname);
end;

procedure main;
    sysname: string;
begin
    while read_next_sysname(sysname) do begin
        if EOF then exit;
        check_one_system(sysname);
    end;
end;
```

Fig. 6-2

# INTERNATIONAL SEARCH REPORT

PCT/EP 92/00061

International Application No

## I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) <sup>6</sup>

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl. <sup>5</sup> G06F11/00

## II. FIELDS SEARCHED

Minimum Documentation Searched <sup>7</sup>

Classification System	Classification Symbols
Int. Cl. <sup>5</sup>	G06F

Documentation Searched other than Minimum Documentation  
to the Extent that such Documents are Included in the Fields Searched <sup>8</sup>

## III. DOCUMENTS CONSIDERED TO BE RELEVANT<sup>9</sup>

Category *	Citation of Document, <sup>11</sup> with indication, where appropriate, of the relevant passages <sup>12</sup>	Relevant to Claim No. <sup>13</sup>
A	COMPUTERS & SECURITY. Volume 9, No. 2, April 1990, AMSTERDAM NL pages 131 - 137; GHANNAM M. AL-DOSSARY: 'Computer virus prevention and containment on mainframes' see page 136, middle column, line 23 - line 41 see page 134, right hand column, line 42 - page 135, left hand column, line 20  ----- A COMPUTERS & SECURITY. Volume 7, No. 2, April 1988, AMSTERDAM NL Pages 157 - 163; H.J. HIGHLAND: 'How to combat a computer virus' see page 162, left hand column, line 1 - line 10  -----  -----	1,4,5  1,4  -----
		-/-

\* Special categories of cited documents: <sup>10</sup>

- "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

"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

## IV. CERTIFICATION

Date of the Actual Completion of the International Search

15 April 1992 (15.04.92)

Date of Mailing of this International Search Report

16 April 1992 (16.04.92)

International Searching Authority

EUROPEAN PATENT OFFICE

Signature of Authorized Officer

**III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)**

Category *	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	EP,A,0 304 033 (SIEMENS AKTIENGESELLSCHAFT BERLIN UND MUNCHEN) 22 February 1989 see abstract; claim 2 -----	1-3
A	WO,A,9 005 418 (STEPHEN A. LENTZ) 17 May 1990 see abstract -----	7-9

ANNEX TO THE INTERNATIONAL SEARCH REPORT  
ON INTERNATIONAL PATENT APPLICATION NO. EP 9200061  
SA 55022

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.  
The members are as contained in the European Patent Office EDP file on  
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 15/04/92

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
EP-A-0304033	22-02-89	None			
WO-A-9005418	17-05-90	US-A-	4975950	04-12-90	
		AU-A-	4641989	28-05-90	
		CA-A-	2002240	03-05-90	
		EP-A-	0408689	23-01-91	
		JP-T-	3502263	23-05-91	

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 92/00061

## I. KLASSEKTIKATION DES ANMELDUNGSGEGENSTANDS (bei mehreren Klassifikationssymbolen sind alle anzugeben)<sup>6</sup>

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

Int.K1. 5 G06F11/00

## II. RECHERCHIERTE SACHGEBIETE

Recherchierter Mindestpräfistoff<sup>7</sup>

Klassifikationssystem	Klassifikationssymbole
Int.K1. 5	G06F

Recherchierte nicht zum Mindestpräfistoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Sachgebiete fallen<sup>8</sup>

## III. EINSCHLAGIGE VERÖFFENTLICHUNGEN<sup>9</sup>

Art. <sup>o</sup>	Kennzeichnung der Veröffentlichung <sup>11</sup> , soweit erforderlich unter Angabe der maßgeblichen Teile <sup>12</sup>	Betr. Anspruch Nr. <sup>13</sup>
A	COMPUTERS & SECURITY. Bd. 9, Nr. 2, April 1990, AMSTERDAM NL Seiten 131 - 137; GHANNAM M. AL-DOSSARY: 'Computer virus prevention and containment on mainframes' siehe Seite 136, mittlere Spalte, Zeile 23 - Zeile 41 siehe Seite 134, rechte Spalte, Zeile 42 - Seite 135, linke Spalte, Zeile 20 ----	1, 4, 5
A	COMPUTERS & SECURITY. Bd. 7, Nr. 2, April 1988, AMSTERDAM NL Seiten 157 - 163; H.J. HIGHLAND: 'How to combat a computer virus' siehe Seite 162, linke Spalte, Zeile 1 - Zeile 10 ---- ----	1, 4 ----

<sup>o</sup> Besondere Kategorien von angegebenen Veröffentlichungen<sup>10</sup>:

- "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 Anmelldatum 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 Anmelddatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

- "T" Spätere Veröffentlichung, die nach dem internationalen Anmelddatum 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 nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden
- "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erforderlicher 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

## IV. BESCHEINIGUNG

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
2 15. APRIL 1992	16. 04. 92
Internationale Recherchenbehörde  EUROPAISCHES PATENTAMT	Unterschrift des bevollmächtigten Beleihsteten  Alfredo Prein

III. EINSCHLAGIGE VEROFFENTLICHUNGEN (Fortsetzung von Blatt 2)		
Art o	Kennzeichnung der Veröffentlichung, soweit erforderlich unter Angabe der maßgeblichen Teile	Betr. Anspruch Nr.
A	EP,A,0 304 033 (SIEMENS AKTIENGESELLSCHAFT BERLIN UND MUNCHEN) 22. Februar 1989 siehe Zusammenfassung; Anspruch 2 ---	1-3
A	WO,A,9 005 418 (STEPHEN A. LENTZ) 17. Mai 1990 siehe Zusammenfassung ---	7-9

**ANHANG ZUM INTERNATIONALEN RECHERCHENBERICHT  
ÜBER DIE INTERNATIONALE PATENTANMELDUNG NR.**

EP 9200061  
SA 55022

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben.

Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am  
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

15/04/92

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie			Datum der Veröffentlichung
EP-A-0304033	22-02-89	Keine			
WO-A-9005418	17-05-90	US-A-	4975950	04-12-90	
		AU-A-	4641989	28-05-90	
		CA-A-	2002240	03-05-90	
		EP-A-	0408689	23-01-91	
		JP-T-	3502263	23-05-91	