(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
1. Dezember 2016 (01.12.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/189048 A1

(51) Internationale Patentklassifikation:
G06F 21/64 (2013.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2016/061830

(22) Internationales Anmeldedatum:
25. Mai 2016 (25.05.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2015 108 336.1 27. Mai 2015 (27.05.2015) DE

(71) Anmelder: **FUJITSU TECHNOLOGY SOLUTIONS INTELLECTUAL PROPERTY GMBH** [DE/DE]; Mies-van-der-Rohe-Str. 8, 80807 München (DE).

(72) Erfinder: **FILIMON, Diana**; Kaltererstr. 9, 86368 Gersthofen (DE). **ATZKERN, Jürgen**; Rosenbergstr. 11, 86505 Münsterhausen (DE). **CESTONARO, Thilo**; Bobinger Str. 93, 86199 Augsburg (DE).

(74) Anwalt: **EPPING HERMANN FISCHER PATENTANWALTSGESELLSCHAFT MBH**; Schloßschmidstr. 5, 80639 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

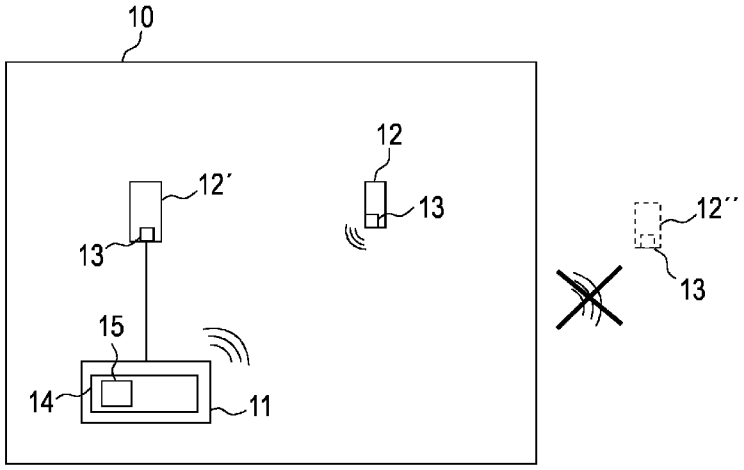
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) Title: METHOD FOR EXECUTING A SECURITY-RELEVANT APPLICATION, COMPUTER SYSTEM AND ARRANGEMENT

(54) Bezeichnung : VERFAHREN ZUM AUSFÜHREN EINER SICHERHEITSRELEVANTEN ANWENDUNG, COMPUTERSYSTEM UND ANORDNUNG

Fig. 1



(57) Abstract: The invention relates to a method for executing a security-relevant application on a computer system (12, 12'). In this case, a data network connection is established between the computer system (12, 12') and a server (11). After the data network connection has been established, the computer system (12, 12') searches for at least one predetermined file (14) on the server (11). If the at least one predetermined file (14) has been found, a signature (15) of the at least one predetermined file (14) is checked. The at least one predetermined file (14) is downloaded if the checking of the signature (15) was successful. The at least one predetermined file (14) which has been downloaded is executed. A system file is changed in this case. If the at least one predetermined file (14) has been executed, the security-relevant application is then started. The invention also relates to a computer system (12, 12', 12") having a data network interface (13) and to an arrangement comprising a computer system (12, 12') and a server (11).

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2016/189048 A1

Die Erfindung betrifft ein Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung auf einem Computersystem (12, 2'). Hierbei wirdeine Datennetzwerkverbindung zwischen dem Computersystem (12, 12') und einem Server (11) hergestellt. Nachdem die Datennetzwerkverbindung hergestellt wurde, wird auf dem Server (11) durch das Computersystem (12, 12') nach wenigstens einer vorbestimmten Datei (14) auf dem Server (11) gesucht. Wurde die wenigstens eine vorbestimmte Datei (14) gefunden, so wird eine Signatur (15) der wenigstens einen vorbestimmten Datei (14) überprüft. Die wenigstenseine vorbestimmte Datei (14) wird heruntergeladen, wenn die Überprüfung der Signatur (15) erfolgreich war. Die heruntergeladene wenigstens eine vorbestimmte Datei (14) wird ausgeführt. Hierbei wird eine Systemdatei geändert. Wurde die wenigstens eine vorbestimmte Datei (14) ausgeführt, so wird im Anschluss die sicherheitsrelevante Anwendunggestartet. Die Erfindung betrifft des Weiteren ein Computersystem (12, 2', 12") mit einer Datennetzwerkschnittstelle (13) und eine Anordnung umfassend ein Computersystem (12, 12') und einen Server (11).

Beschreibung

Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung, Computersystem und Anordnung

Die Erfindung betrifft ein Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung auf einem Computersystem, ein Computersystem mit einer Datennetzwerkschnittstelle sowie eine Anordnung umfassend ein Computersystem und einen Server.

Computersysteme, wie beispielsweise Bezahlterminals zum Ausführen von finanziellen Transaktionen, bei denen sich ein Benutzer authentifizieren muss, schränken in der Regel einen Zugriff auf Systemdateien stark ein.

Aufgabe der Erfindung ist es, ein Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung auf einem Computersystem aufzuzeigen. Auch ist es Aufgabe der Erfindung, Vorrichtungen zum Durchführen des Verfahrens zu beschreiben.

Gemäß einem ersten Aspekt der Erfindung wird die Aufgabe durch ein Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung auf einem Computersystem in einer gesicherten Umgebung gelöst. Hierbei wird eine Datennetzwerkverbindung über ein internes Netzwerk der gesicherten Umgebung zwischen dem Computersystem und einem Server hergestellt, der in der gesicherten Umgebung angeordnet ist. Im Anschluss hieran wird nach wenigstens einer vorbestimmten Datei auf dem Server durch das Computersystem gesucht. Wurde die wenigstens eine vorbestimmte Datei gefunden, so wird eine Signatur der wenigstens einer vorbestimmten Datei überprüft. War die Überprüfung der Signatur erfolgreich, so wird die wenigstens

eine vorbestimmte Datei heruntergeladen und ausgeführt, wobei durch das Ausführen der wenigstens einen vorbestimmten Datei eine Systemdatei geändert wird. Im Anschluss hieran wird die sicherheitsrelevante Anwendung gestartet.

Solche Geräte müssen bei Auftreten von Defekten gewartet werden können. Ein Wartungsdienst oder Servicedienst muss sich somit auch Zugang zu sicherheitsrelevanten Bereichen des geschützten Peripheriegeräts verschaffen können. Dies muss in einem sicheren Umfeld, nicht unerlaubt oder aus Versehen erfolgen. Auf den Server ist durch eine Überprüfung eines Nutzerzertifikats kein unautorisierter Zugriff möglich. Das Computersystem stellt eine Datennetzwerkverbindung mit einem Server her. Beispielsweise stellt das Computersystem die Datennetzwerkverbindung mit einem Updateserver her, um nach automatischen Updates zu suchen. Hierbei wird nach wenigstens einer vorbestimmten Datei gesucht. Die Überprüfung der Signatur der vorbestimmten Datei dient der Verifikation der Sicherheit der Datei. Ist die Datei authentifiziert, so wird sie heruntergeladen und ausgeführt. Hierbei wird eine Systemdatei des Computersystems verändert. Durch die Veränderung kann eine sicherheitsrelevante Anwendung, insbesondere ein Flashen des Speichers, bzw. ein vollständiges Flashen des Computersystems (englisch: complete system reflash) ausgeführt werden. Das Ausführen umfasst hierbei ein Installieren der wenigstens einen vorbestimmten Datei und ein hierauf folgendes Aufrufen der installierten Datei durch die Datei selber oder ein Programm.

In einer vorteilhaften Ausgestaltung umfasst das Ausführen der wenigstens einen vorbestimmten Datei ein Umbenennen der Systemdatei.

Eine bestimmte Systemdatei kann umbenannt oder verändert werden, um die Wartung an dem Computersystem durchzuführen. Beispielsweise wird eine Bootdatei, insbesondere ein sogenanntes bootup-file, neu benannt, sodass ein Systemflashen möglich wird.

Gemäß einer weiteren vorteilhaften Ausgestaltung ist die wenigstens eine vorbestimmte Datei Teil eines Dateipakets und das Dateipaket wird gesucht, überprüft, heruntergeladen und ausgeführt.

Das Dateipaket kann verschiedene vorbestimmte Dateien umfassen, durch die verschiedene Funktionen und Wartungsalgorithmen auf dem Computersystem durchgeführt werden können.

Gemäß einer weiteren vorteilhaften Ausgestaltung wird beim Ausführen der sicherheitsrelevanten Anwendung ein Flashspeicher des Computersystems programmiert.

Durch das Programmieren beziehungsweise Umprogrammieren des Flashspeichers können Systemeinstellungen des Computersystems verändert werden.

Gemäß einer weiteren vorteilhaften Ausgestaltung wird beim Ausführen der sicherheitsrelevanten Anwendung ein Wiederherstellungsmodus aufgerufen.

Durch das Aufrufen des Wiederherstellungsmodus kann das Computersystem beispielsweise in einen ursprünglichen Werkszustand zurückversetzt werden.

Gemäß einem zweiten Aspekt der Erfindung wird die Aufgabe durch ein Computersystem mit einer Datennetzwerkschnittstelle gelöst. Das Computersystem ist hierbei dazu eingerichtet, in einer gesicherten Umgebung eine Datennetzwerkverbindung über ein internes Netzwerk zu einem Server aufzubauen, der in der gesicherten Umgebung angeordnet ist, und nach wenigstens einer vorbestimmten Datei auf dem Server zu suchen, nachdem die Datennetzwerkverbindung aufgebaut wurde. Das Computersystem ist weiter dazu eingerichtet, eine Signatur der wenigstens einen vorbestimmten Datei zu überprüfen, wenn die wenigstens eine vorbestimmte Datei auf dem Server gefunden wurde. Des Weiteren ist das Computersystem dazu eingerichtet, die wenigstens eine vorbestimmte Datei herunterzuladen, auszuführen und hierauf folgend eine sicherheitsrelevante Anwendung zu starten. Beim Ausführen der wenigstens einen vorbestimmten Datei wird eine Systemdatei geändert.

Der Server kann hierbei ein Updateserver sein. Ein derartiges Computersystem kann während einer Suche nach Updates automatisch nach Konfigurationsdateien suchen und diese ausführen. Wird der vorbestimmten Datei hierbei vertraut, so können sicherheitsrelevante Eingriffe in das Computersystem durchgeführt werden. Eine Sicherheit des Servers kann durch eine Überprüfung einer Signatur des Servers und über eine Https-Verbindung mit einem Nutzerzertifikat, das von dem gleichen Aussteller stammt, wie die Signatur des Servers. Ein physikalischer Zugriff auf den Server kann auch durch eine Beschränkung eines Zutritts zu dem Server, beispielsweise einem Sicherheitsbereich, und durch ein vier-Augen-Prinzip abgesichert sein, so dass keine Person alleine physikalisch an dem Server arbeiten kann.

Gemäß einem dritten Aspekt der Erfindung wird die Aufgabe durch eine Anordnung umfassend ein Computersystem und einen Server gelöst. Der Server ist hierbei in einer gesicherten Umgebung mit einem internen Netzwerk angeordnet. Der Server bietet wenigstens eine vorbestimmte Datei für das Computersystem an. Hierbei ist das Computersystem dazu eingerichtet, nach wenigstens einer vorbestimmten Datei auf dem Server zu suchen und nach Finden der wenigstens einen vorbestimmten Datei, eine Signatur der wenigstens einen vorbestimmten Datei zu überprüfen. Des Weiteren ist das Computersystem dazu eingerichtet, nach erfolgreicher Überprüfung der Signatur die wenigstens eine vorbestimmte Datei herunterzuladen, auszuführen und hierauf folgend eine sicherheitsrelevante Anwendung zu starten.

Der Server stellt die vorbestimmte Datei beispielsweise als Updatedatei zur Verfügung. Dadurch, dass sich der Server in einer gesicherten Umgebung befindet, ist davon auszugehen, dass ausschließlich vertrauenswürdige Personen Zugriff zu dem Server haben. Somit ist eine Überprüfung der Signatur der vorbestimmten Datei ausreichend, um eine Sicherheit für das Computersystem weiter zu gewährleisten. Beispielsweise ist die sichere Umgebung ein Sicherheitsbereich in einer Firma. Ein Zutritt zu dem Sicherheitsbereich kann durch ein vier-Augen-Prinzip abgesichert sein.

Gemäß einer vorteilhaften Ausgestaltung sind der Server und das Computersystem mit einem internen Netzwerk eines Wartungszentrums oder Servicezentrums verbunden.

Ist die gesicherte Umgebung ein Wartungszentrum oder ein Servicezentrum, so können sich das Computersystem und der Server mit dem internen Netzwerk des Wartungszentrums oder

Servicezentrums verbinden. Der Server ist hierbei nicht von außerhalb des Wartungszentrums oder Servicezentrums zugängig. Somit ist eine hohe Sicherheit der Anordnung gewährleistet.

Gemäß einer vorteilhaften Ausgestaltung ist die sicherheitsrelevante Anwendung dazu eingerichtet einen Flashspeicher des Computersystems zu programmieren.

Gemäß einer weiteren vorteilhaften Ausgestaltung ist die sicherheitsrelevante Anwendung zum Aufrufen eines Wiederherstellungsmodus eingerichtet.

Ein Wiederherstellungsmodus eignet sich bevorzugt zur Wartung eines Computersystems. Hierbei können Defekte, insbesondere fehlerhafte Software, repariert werden.

Die Erfindung wird im Folgenden anhand von Ausführungsbeispielen und Figuren näher erläutert. In den Figuren zeigen:

Figur 1 eine schematische Darstellung einer Anordnung gemäß einer Ausgestaltung der Erfindung; und

Figur 2 ein Ablaufdiagramm eines Verfahrens gemäß einer Ausgestaltung der Erfindung.

Figur 1 zeigt eine gesicherte Umgebung 10. Bei der gesicherten Umgebung 10 handelt es sich um ein Wartungszentrum zum Warten von Computersystemen 12, 12'. In anderen Ausgestaltungen kann es sich bei der gesicherten Umgebung 10 ebenso um andere gesicherte Umgebungen, wie beispielsweise räumlich begrenzte Gelände handeln, beispielsweise um eine Fertigungsanlage oder Servicezentrum.

Beispielsweise ist die sichere Umgebung 10 ein Sicherheitsbereich in einer Firma. Ein Zutritt zu dem Sicherheitsbereich ist durch ein vier-Augen-Prinzip abgesichert, so dass keine Person alleine physikalisch an dem Server arbeiten kann.

In der gesicherten Umgebung 10 ist ein Server 11 angeordnet. Der Server 11 steht beispielsweise in einem besonders gesicherten Serverraum in dem Wartungszentrum, zu dem lediglich ein ausgewählter Personenkreis Zutritt hat. Der Zugriff auf den Server 11 ist beschränkt, beispielsweise durch eine Zugriffsfreigabe für lediglich den ausgewählten Personenkreis. Der Server 11 dient dazu, Servicepakete und Wartungssoftware für eine Wartung der Computersysteme 12, 12' bereitzustellen. Im Ausführungsbeispiel ist ein Computersystem 12'' von der gesicherten Umgebung ausgeschlossen. Mitarbeiter des Wartungszentrums oder der gesicherten Umgebung können so indirekt in Computersysteme 12, 12' eingreifen. Der Standort des Servers 11 ist durch die gesicherte Umgebung 10 gesichert. Zusätzlich ist für einen Zugriff auf den Server 11 eine kryptografische Sicherung vorgesehen. Beispielsweise muss ein Mitarbeiter ein Passwort eingeben, um einen Serverschrank zu öffnen und an dem Server 11 arbeiten zu können.

Die Computersysteme 12, 12', 12'' sind im Ausführungsbeispiel eingebettete Computersysteme in Form von Bezahlterminals zum Durchführen finanzieller Transaktionen eines Benutzers, beispielsweise an Supermarktkassen oder in Kaufhäusern. Ein Benutzer benutzt das Computersystem 12, 12', 12'' hierbei beispielsweise zum Authentifizieren personenbezogener Daten. In anderen Ausgestaltungen handelt es sich bei den Computersystemen 12, 12', 12'' um Computersysteme zur

Überprüfung von Zutrittskontrollen, um Bankautomaten, Bordcomputer von Fahrzeugen oder im Allgemeinen um Computersysteme, die sicherheitsrelevante Daten speichern und/oder verarbeiten.

Die Computersysteme 12, 12', 12'' können eine Datennetzwerkverbindung aufbauen. Hierzu verfügten sie über eine Datennetzwerkschnittstelle 13. Das Computersystem 12 weist als Datennetzwerkschnittstelle 13 ein WLAN-Modul auf. Das Computersystem 12' weist als Datennetzwerkschnittstelle 13 einen LAN-Anschluss auf. In der schematischen Darstellung gemäß Figur 1 sind die Computersysteme 12 und 12' in die gesicherte Umgebung 10 eingebracht und haben Zugriff auf ein internes Netzwerk der gescherten Umgebung 10. Das Computersystem 12'' ist nicht in die gesicherte Umgebung 10 eingebracht (gestrichelte Darstellung). Das Computersystem 12'' hat keinen Zugriff auf das interne Netzwerk und den Server 11.

Die Computersysteme 12 und 12' sind mit dem Server 11 über das interne Netzwerk der gesicherten Umgebung 10 verbunden. Das Computersystem 12 ist drahtlos über ein WLAN mit dem Server 11 verbunden, das Computersystem 12' ist über eine Kabelverbindung, insbesondere eine LAN-Verbindung, mit dem Server 11 direkt verbunden. In nicht dargestellten Ausführungen sind die Computersysteme 12 und 12' indirekt, beispielsweise über einen Router mit dem Server 11 verbunden.

Das interne Netzwerk der gesicherten Umgebung 10 ist räumlich auf die gesicherte Umgebung 10 begrenzt. Im Falle einer WLAN-Verbindung ist die WLAN-Intensität so gewählt, dass auf das WLAN außerhalb der gesicherten Umgebung 10 nicht zugegriffen werden kann.

Figur 2 zeigt ein Ablaufdiagramm 20. In Schritt 21 wird eine Datennetzwerkverbindung hergestellt. Die Computersysteme 12 und 12' melden sich jeweils in dem internen Netzwerk der gesicherten Umgebung 10 an und bauen so die Datennetzwerkverbindung über die Datennetzwerkschnittstelle 13 auf. In einem alternativen Ausführungsbeispiel bauen die Computersysteme 12 und/oder 12' ein Datennetzwerk auf, in dem sich andere Computersysteme, wie der Server 11 anmelden können, um die Datennetzwerkverbindung herzustellen.

Wurde die Datennetzwerkverbindung hergestellt, so sucht das Computersystem 12, bzw. 12' in Schritt 22 nach durch den Server 11 bereitgestellten Dateien. Im Ausführungsbeispiel sucht das Computersystem 12, bzw. 12' nach Updatedateien, um das Computersystem 12, bzw. 12' auf einem aktuellen Stand zu halten. Insbesondere sucht das Computersystem 12, bzw. 12' nach einer Datei oder einem Dateipaket mit einem vorbestimmten Namen der wenigstens einen vorbestimmten Datei 14 auf allen Servern, die mit dem Computersystem 12, bzw. 12' verbunden sind. Wird eine Datei oder ein Dateipaket mit dem vorbestimmten Namen gefunden, beispielsweise ein "set_to_manufacturing_mode"-Paket, so wird in Schritt 23 eine Signatur 15 der gefundenen wenigstens einen vorbestimmten Datei 14 überprüft.

In Schritt 23 wird die Signatur 15 der wenigstens einen vorbestimmten Datei 14 überprüft. Im Ausführungsbeispiel wird eine Prüfsumme (Hash-Wert) der Signatur 15 von dem Computersystem 12, bzw. 12' überprüft. Somit wird sichergestellt, dass die wenigstens eine vorbestimmte Datei 14 aus einer legitimierten Quelle stammt. Ist die Überprüfung

der Signatur 15 erfolgreich, so wird die wenigstens eine vorbestimmte Datei 14 in Schritt 24 heruntergeladen.

In Schritt 25 wird die heruntergeladene wenigstens eine vorbestimmte Datei 14 ausgeführt. Beispielsweise wird beim Ausführen der wenigstens einen vorbestimmten Datei 14 ein Programm gestartet, das auf eine Systemdatei des Computersystems 12, bzw. 12' eingreifen kann. Die Systemdatei wird hierbei umbenannt. Im Ausführungsbeispiel wird eine Bootdatei, die zum Starten des Computersystems notwendig ist, verändert. Dies stellt einen sicherheitskritischen Eingriff dar. Durch die vorherige Authentifizierung der wenigstens einen vorbestimmten Datei 14 in dem Netzwerk in der gesicherten Umgebung 10 ist sichergestellt, dass es sich nicht um Schadsoftware handelt.

In Schritt 26 wird nun eine sicherheitsrelevante Anwendung auf dem Computersystem 12, 12' ausgeführt. Im Ausführungsbeispiel handelt es sich bei der sicherheitsrelevanten Anwendung um einen kompletten Systemflash. In einer alternativen Ausgestaltung können auf weitere, einzelne Firmware- oder Softwaredateien des Computersystems 12 bzw. 12' zugegriffen und diese verändert werden. Somit kann eine Wartung des Computersystems 12, bzw. 12' sicher und schnell durchgeführt werden. Das Computersystem 12 bzw. 12' kann beispielsweise auf Werkseinstellungen zurückgesetzt werden.

Ergab die Überprüfung der Signatur 15 in Schritt 23, dass die Signatur 15 nicht vertrauenswürdig ist, so wird die vorbestimmte Datei 14 nicht heruntergeladen. In einer weiteren Ausgestaltung kann zusätzlich die Datennetzwerkverbindung zu dem Datennetzwerk getrennt werden.

In einem weiteren Ausführungsbeispiel wird bei der Herstellung der Datennetzwerkverbindung in Schritt 21 zusätzlich eine Überprüfung des Datennetzwerks und/oder des Servers 11 in dem Datennetzwerk durchgeführt. Hierbei wird eine MAC-Adresse des Servers 11 überprüft. In weiteren Ausführungsbeispielen werden weitere oder alternative Überprüfungen durchgeführt, wie beispielsweise die Überprüfung eines Serverzertifikats oder eines Netzwerknamens.

Tritt bei dieser Überprüfung eine Unregelmäßigkeit oder ein Hinweis auf eine Manipulation auf, so wird die Datennetzwerkverbindung nicht aufgebaut bzw. unterbrochen. Das Computersystem 12 bzw. 12' ist somit vor Zugriffen geschützt.

In einem weiteren Ausführungsbeispiel wird in Schritt 25 die wenigstens eine vorbestimmte Datei 14 auf dem Computersystem 12 bzw. 12' installiert. Während des Installierens wird die wenigstens eine vorbestimmte Datei 14 verändert, insbesondere umbenannt.

In einem weiteren Ausführungsbeispiel sind die Computersysteme 12, 12', 12'' zusätzlich wartungsfreie Computersysteme. In solchen Computersystemen sind Defekte üblicherweise nicht reparierbar. Durch das oben beschriebene Verfahren, können derartige Computersysteme 12, 12', 12'' wiederhergestellt werden. Sind die Computersysteme gemäß dem in Figur 1 gezeigten Ausführungsbeispiel wartungsfrei, so können die Computersysteme 12 und 12' in der gesicherten Umgebung 10 wiederhergestellt werden.

Bezugszeichenliste

10	gesicherte Umgebung
11	Server
12, 12', 12''	Computersystem
13	Datennetzwerkschnittstelle
14	vorbestimmte Datei
15	Signatur
20	Flussdiagramm
21-27	Verfahrensschritte

Patentansprüche

1. Verfahren zum Ausführen einer sicherheitsrelevanten Anwendung auf einem Computersystem (12, 12') in einer gesicherten Umgebung (10), umfassend die Schritte:
   - Herstellen einer Datennetzwerkverbindung über ein internes Netzwerk der gesicherten Umgebung (10) zwischen dem Computersystems (12, 12') und einem Server (11), der in der gesicherten Umgebung (10) angeordnet ist;
   - Suchen nach wenigstens einer vorbestimmten Datei (14) auf dem Server (11) durch das Computersystem (12, 12'), nachdem die Datennetzwerkverbindung hergestellt wurde;
   - Überprüfen einer Signatur (15) der wenigstens einen vorbestimmten Datei (14), wenn die wenigstens eine vorbestimmte Datei (14) gefunden wurde;
   - Herunterladen der wenigstens einen vorbestimmten Datei (14), wenn die Überprüfung der Signatur (15) erfolgreich war;
   - Ausführen der wenigstens einen vorbestimmte Datei (14) nach dem Herunterladen, wobei durch das Ausführen der wenigstens einen vorbestimmten Datei (14) eine Systemdatei geändert wird; und
   - Starten der sicherheitsrelevanten Anwendung, nachdem die wenigstens eine vorbestimmte Datei (14) erfolgreich ausgeführt wurde.

2. Verfahren nach Anspruch 1, wobei das Ausführen der wenigstens einen vorbestimmten Datei (14) ein Umbenennen der Systemdatei umfasst.

3. Verfahren nach einem der Ansprüche 1 oder 2, wobei die wenigstens eine vorbestimmte Datei (14) Teil eines Dateipakets ist und das Dateipaket gesucht, überprüft, heruntergeladen und ausgeführt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei beim Ausführen der sicherheitsrelevanten Anwendung ein Flashspeicher des Computersystems (12, 12') programmiert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei beim Ausführen der sicherheitsrelevanten Anwendung ein Wiederherstellungsmodus aufgerufen wird.

6. Computersystem (12, 12', 12'') mit einer Datennetzwerkschnittstelle (13), wobei das Computersystem (12, 12', 12'') dazu eingerichtet ist, in einer gesicherten Umgebung (10) eine Datennetzwerkverbindung über ein internes Netzwerk über die Datennetzwerkschnittstelle (13) zu einem Server (11) aufzubauen, der in der gesicherten Umgebung (10) angeordnet ist und nach wenigstens einer vorbestimmten Datei (14) auf dem Server (11) zu suchen, nachdem die Datennetzwerkverbindung aufgebaut wurde, und eine Signatur (15) der wenigstens einen vorbestimmten Datei (14) zu überprüfen, wenn die wenigstens eine vorbestimmte Datei (14) auf dem Server (11) gefunden wurde, und die wenigstens eine vorbestimmte Datei (14) herunterzuladen, auszuführen und hierauf folgend eine sicherheitsrelevante Anwendung zu starten, wobei beim Ausführen der wenigstens einen vorbestimmten Datei (14) eine Systemdatei geändert wird.

7. Anordnung umfassend ein Computersystem (12, 12') und einen Server (11), wobei der Server (11) in einer gesicherten Umgebung (10) mit einem internen Netzwerk angeordnet ist und wenigstens eine vorbestimmte Datei (14) für das Computersystem (12, 12') anbietet, wobei das Computersystem (12, 12') dazu eingerichtet ist, nach der wenigstens einen vorbestimmten Datei (14) auf dem Server (11) zu suchen und nach Finden der wenigstens einen vorbestimmten Datei(14), eine Signatur (15) der wenigstens einen vorbestimmten Datei (14) zu überprüfen und nach erfolgreicher Überprüfung der Signatur (15) die wenigstens eine vorbestimmte Datei (14) herunterzuladen, auszuführen und hierauf folgend eine sicherheitsrelevante Anwendung zu starten.

8. Anordnung nach Anspruch 7, wobei der Server (11) und das Computersystem (12, 12') mit einem internen Netzwerk eines Wartungszentrums oder Servicezentrums verbunden sind.

9. Anordnung nach einem der Ansprüche 7 oder 8, wobei die sicherheitsrelevante Anwendung dazu eingerichtet ist, einen Flashspeicher des Computersystems (12, 12') zu programmieren.

10. Anordnung nach einem der Ansprüche 7 bis 9, wobei die sicherheitsrelevante Anwendung zum Aufrufen eines Wiederherstellungsmodus eingerichtet ist.

Fig. 1

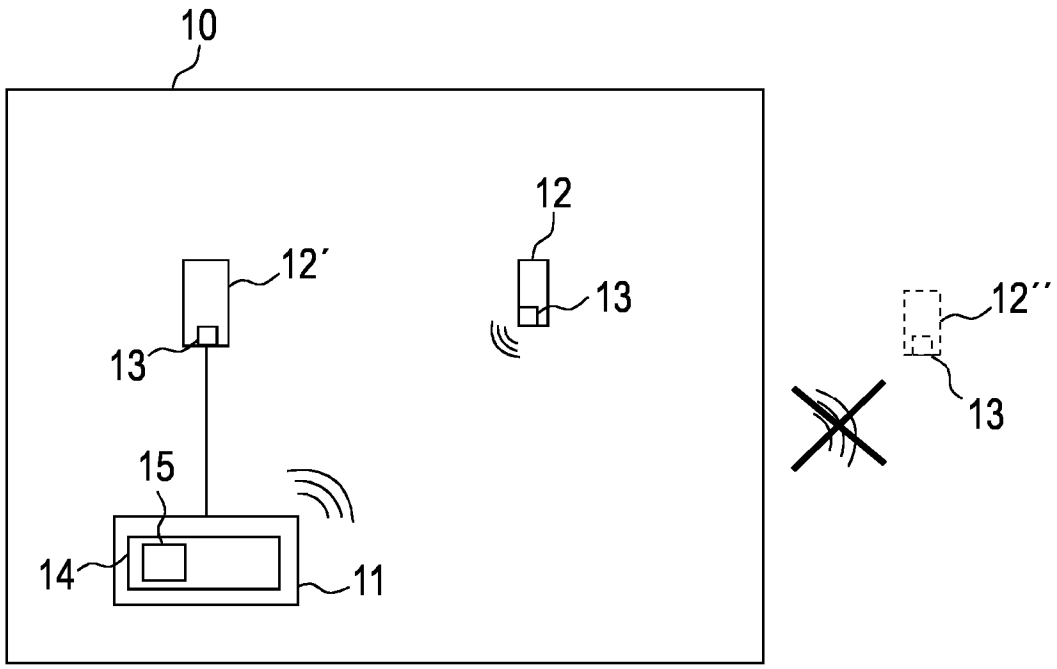
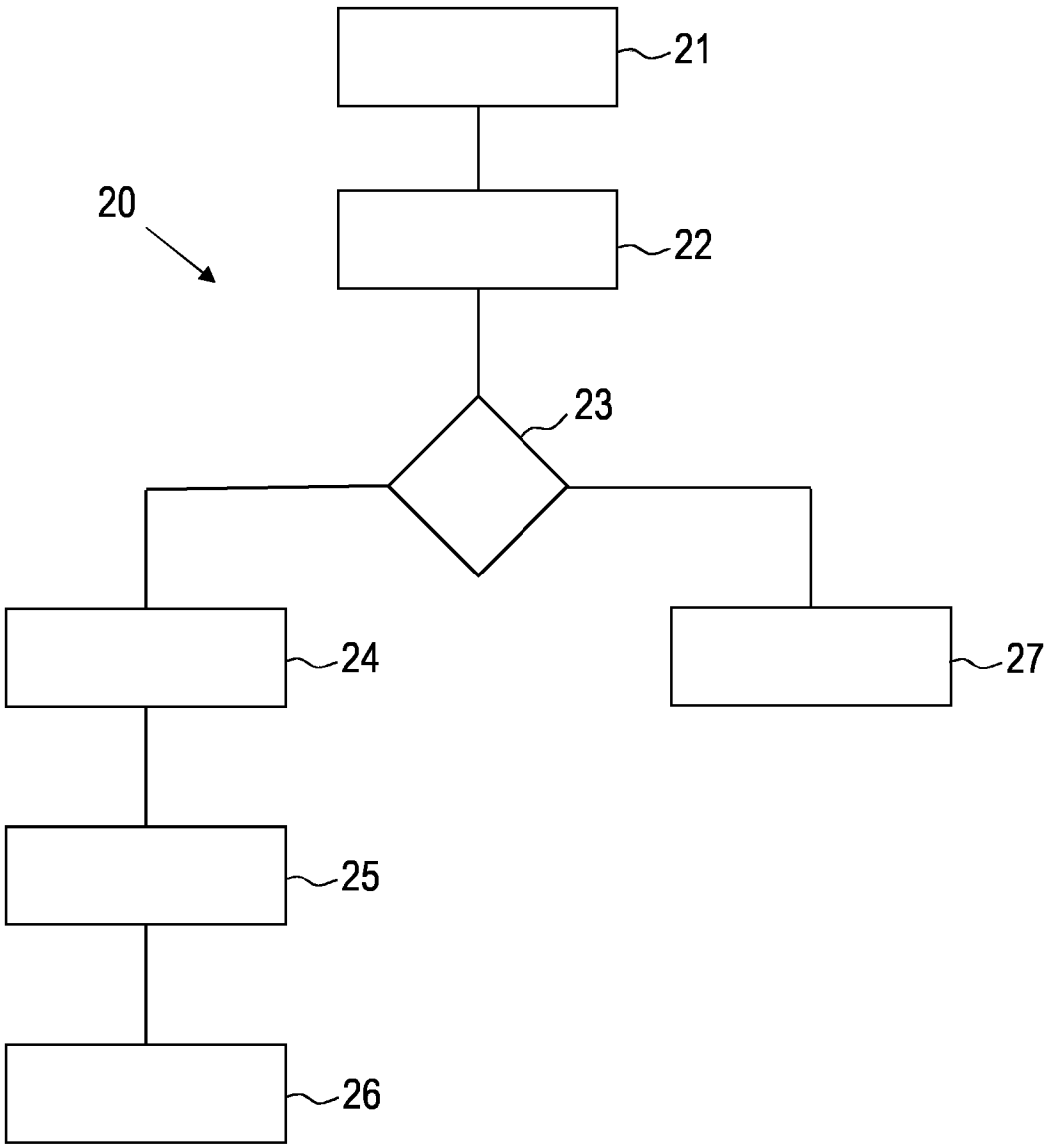


Fig. 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/061830

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/64 H04L29/08 H04L29/06
ADD.

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)
G06F 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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/326494 A1 (NUNEZ YONESY F [US]) 5 December 2013 (2013-12-05) paragraph [0016] paragraph [0026] - paragraph [0027] paragraph [0033] paragraph [0036] paragraph [0038] paragraph [0049] - paragraph [0050] ----- -/--	1-10

[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 application or patent 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
18 July 2016	25/07/2016

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, Fax: (+31-70) 340-3016	Tenbieg, Christoph

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/185548 A1 (DJABAROV GUEORGUI [US] ET AL) 18 July 2013 (2013-07-18) paragraph [0015] - paragraph [0017] paragraph [0026] paragraph [0035] paragraph [0038] paragraph [0040] - paragraph [0042] paragraph [0044] paragraph [0046] - paragraph [0049] paragraph [0051] - paragraph [0055] paragraph [0057] - paragraph [0060] paragraph [0064] paragraph [0072] -----	1-10
A	MENEZES A ET AL: "Handbook of applied cryptography, chapter 9, HASH FUNCTIONS AND DATA INTEGRITY", 1 January 1997 (1997-01-01), HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 321 - 383, XP002414177, ISBN: 978-0-8493-8523-0 the whole document -----	1-10
A	MENEZES A ET AL: "Handbook of Applied Cryptography, Chapter 11: Digital Signatures; Signatures with additional functionality ED - Menezes A J; Van Oorschot P C; Vanstone S A", 1 January 1997 (1997-01-01), HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 476 - 488, XP001091097, ISBN: 978-0-8493-8523-0 the whole document -----	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/061830

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013326494 A1	05-12-2013	NONE	
US 2013185548 A1	18-07-2013	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2016/061830

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/64 H04L29/08 H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F 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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2013/326494 A1 (NUNEZ YONESY F [US]) 5. Dezember 2013 (2013-12-05) Absatz [0016] Absatz [0026] - Absatz [0027] Absatz [0033] Absatz [0036] Absatz [0038] Absatz [0049] - Absatz [0050] ----- -/--	1-10

[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" frühere Anmeldung oder Patent, die bzw. 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 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
18. Juli 2016	25/07/2016

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tenbieg, Christoph

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2013/185548 A1 (DJABAROV GUEORGUI [US] ET AL) 18. Juli 2013 (2013-07-18) Absatz [0015] - Absatz [0017] Absatz [0026] Absatz [0035] Absatz [0038] Absatz [0040] - Absatz [0042] Absatz [0044] Absatz [0046] - Absatz [0049] Absatz [0051] - Absatz [0055] Absatz [0057] - Absatz [0060] Absatz [0064] Absatz [0072] -----	1-10
A	MENEZES A ET AL: "Handbook of applied cryptography, chapter 9, HASH FUNCTIONS AND DATA INTEGRITY", 1. Januar 1997 (1997-01-01), HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 321 - 383, XP002414177, ISBN: 978-0-8493-8523-0 das ganze Dokument -----	1-10
A	MENEZES A ET AL: "Handbook of Applied Cryptography, Chapter 11: Digital Signatures; Signatures with additional functionality ED - Menezes A J; Van Oorschot P C; Vanstone S A", 1. Januar 1997 (1997-01-01), HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 476 - 488, XP001091097, ISBN: 978-0-8493-8523-0 das ganze Dokument -----	1-10

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2016/061830

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2013326494 A1	05-12-2013	KEINE	
US 2013185548 A1	18-07-2013	KEINE	