(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 39 332 T2** 2009.07.16

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 899 647 B1**
(21) Deutsches Aktenzeichen: **698 39 332.5**
(96) Europäisches Aktenzeichen: **98 306 651.5**
(96) Europäischer Anmeldetag: **19.08.1998**
(97) Erstveröffentlichung durch das EPA: **03.03.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.04.2008**
(47) Veröffentlichungstag im Patentblatt: **16.07.2009**

(51) Int Cl.[8]: ***G06F 21/00*** (2006.01)

(30) Unionspriorität:
927096 **29.08.1997** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Compaq Computer Corp., Houston, Tex., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Angelo, Michael F., Houston, Texas 77068, US;
Olarig, Sompong P., Cypress, Texas 77429, US

(54) Bezeichnung: **Ferngesteuerte Sicherheitstechnologie**

Beschreibung

[0001] Diese Erfindung betrifft ein Verfahren zur Computersicherheit, wobei Befehle aus der Ferne (remotely) an den Computer gesendet werden können, so dass ein Betrieb freigegeben oder gesperrt wird.

[0002] Physikalische Computerausrüstung und auf Festplatten in tragbaren Computern gespeichertes geistiges Eigentum kann für die Eigentümer-Unternehmen einen Wert von Millionen Dollar besitzen. Insbesondere dann, wenn kleine, kostspielige und tragbare Computer involviert sind, wird die Vermögensverwaltung sehr schwierig.

[0003] Mit der Einführung des Internets und der Verbreitung von Computern im Geschäfts- und Privatleben ist es nur natürlich, dass sich der Diebstahl derartiger Geräte, Komponenten und auf diesen Systemen gespeicherter Informationen immer weiter verbreitet. Betriebsangehörige sind auch weiterhin die hauptsächliche Quelle für Verluste auf Grund von Diebstahl. Beispielsweise können Betriebsangehörige, die kompatible Systeme zu Hause besitzen, versucht sein, Platinen (boards) und Eingabegeräte an ihrem Arbeitsplatz auszutauschen, um ihre Systeme zu Hause zu reparieren. Betriebsangehörige sind jedoch nicht die einzige Bedrohung. Techniker, Hausmeister, Lieferpersonal, andere Lieferanten, Kunden, geladene Gäste und selbst Sicherheitsangestellte haben Gelegenheit, Computereigentum zu entwenden.

[0004] Auch die Größe und die Tragbarkeit sind weitere Faktoren. In dem Maß, wie Hersteller von integrierten Schaltungen die Größe von Computerchips verringern und sich darüber hinaus deren Leistungsfähigkeit und Güte stark verbessern, werden die Gehäuse, in die die Computerchips eingebaut werden, immer kleiner. Es ist wahrscheinlich, dass sich Diebstähle „im Vorbeigehen" auf die kleinsten Geräte konzentrieren. In dem Maß, wie Computergeräte immer kleiner werden (beispielsweise Subnotebooks und kleinere Computer), steigt die Möglichkeit, dass diese durch Diebstahl abhanden kommen. Die Verringerung der Größe ist mit Sicherheit die Richtung der Zukunft.

[0005] Das geistige Eigentum stellt einen signifikanten Teil des Anlagenbestandes eines Unternehmens dar. In vielen Fällen übersteigt der Wert eines Elementes geistigen Eigentums bei Weitem den Wert der Hardware, auf der es gespeichert ist. Wenn folglich die Hardware gestohlen wird, ist es von höchster Wichtigkeit, den Zugriff auf diese Informationen zu verhindern; die Wiederbeschaffung der Hardware ist dabei nur ein sekundäres Ziel. Eine Umfrage unter 325 Unternehmen in den USA durch die amerikanische Gesellschaft für Industriesicherheit (American Society for Industrial Security) ergab, dass potenzielle Verluste für US-amerikanische Unternehmen bis zu 24 Milliarden US-Dollar pro Jahr erreichen können.

[0006] Computer und verwandte Peripheriegeräte sowie geistiges Eigentum sind jedoch nicht das einzige Ziel für High-rech-Diebstahl. Modernste Instrumente und Prüfgeräte sind ebenfalls gefährdete Ziele, darüber hinaus sind diese üblicherweise pro Einheit wesentlich kostspieliger als ein typischer Heimcomputer. Diese Geräte lassen sich zwar weniger leicht zu Geld machen als Computergeräte, sie können jedoch für Unternehmen, die derartige Geräte verwenden, einen beträchtlichen Verlust darstellen.

[0007] Unternehmen sorgen sich zunehmend über den Verlust oder die rechtswidrige Offenbarung unternehmenseigener Informationen. Der Schutz gespeicherter Informationen wird hauptsächlich über Festplatten-Softwaresicherheitsschlösser und Datenverschlüsselung erzielt. Diese Maßnahmen sind jedoch nicht absolut diebstahlsicher und können in vielen Fällen relativ leicht umgangen werden. Darüber hinaus ist das System verwendbar, sobald die Sperre umgangen wurde. Beispielsweise lässt sich der Diebstahl eines Laptops durch eine durch Software geschützte Festplatte nicht vereiteln, in diesem Fall wird das geschützte Laufwerk einfach durch ein neues oder anderes, systemkompatibles Laufwerk ohne den Softwareschutz ausgetauscht: dies ist im Vergleich zu dem Wert des Gesamtsystems ein relativ geringer zu zahlender Preis. Darüber hinaus stellt das Entfernen des Laptop-Computers an einen anderen Standort in vielen Fällen ausreichend Zeit bereit, um die Softwaresicherungen und Verschlüsselungen zu umgehen, die zum Schutz der Informationen verwendet wurden.

[0008] In einigen Fällen erfolgt der Diebstahl jedoch wegen des Wertes der Hardware und nicht wegen der auf den Systemspeichervorrichtungen enthaltenen Informationen. Somit versuchen die meisten Hardware-Sicherheitssysteme, das Computersystem zu schützen, indem es an einem anderen, weniger mobilen Objekt befestigt wird. Sobald jedoch ein Sicherheitskabel entfernt wurde, ist der Computer nach wie vor voll betriebsbereit und leicht zu verkaufen.

[0009] Diese Maßnahmen nach dem Stand der Technik sind wirkungslos, wenn die Computergeräte erst noch zu sichern sind, beispielsweise während des Versandes zu dem Verbraucher oder während des Zusammenbaus bei dem Hersteller. Darüber hinaus sind die herkömmlichen Verfahren wirkungslos gegen Diebstahl aus einem Kraftfahrzeug oder von der Person. Da, wie vorstehend bereits erwähnt, integrierte Schaltungen immer kleiner werden, können auch immer mehr Funktionen in einen Computerchip integriert und Platinen immer dichter bestückt wer-

den. Schlussendlich können alle elektronischen Funktionen des Computers in eine Platine integriert werden. Herkömmliche Diebstahlschutzverfahren stellen in diesen Situationen nicht den Grad von Schutz bereit, um wirkungsvoll von dem Diebstahl einer Platine oder eines Systems abzuschrecken.

[0010] Eine Schwierigkeit beim Verhindern dieses Problems besteht darin, dass die meisten Benutzer nicht willens sind, die Unbequemlichkeit auf sich zu nehmen, Passwörter oder andere Sicherheitsmaßnahmen zu nutzen. Obwohl in einige der modernen Systeme Passwörter für eine POST-Prozedur oder Verschlüsselungsvorrichtungen eingebaut sind, sind nur sehr wenige dieser Funktionen tatsächlich aktiviert, und daher ist es schwierig für Unternehmen sicherzustellen, dass die Systeme sicher sind. Wenn zurzeit ein solches System verloren geht oder gestohlen wird, während seine Sicherheitsfunktionen gesperrt sind, hat der Eigentümer keine Möglichkeit, die unberechtigte Verwendung des Systems zu verhindern.

[0011] Die Kraftfahrzeugindustrie hat einigen Gebrauch von aus der Ferne aktivierbaren Diebstahlschutzvorrichtungen gemacht. Ein gängiges System wird LoJack genannt und zum Verfolgen gestohlener Fahrzeuge verwendet. Zum Schutz eines Fahrzeugs wird an unauffälliger Stelle eine Sende-/Empfangseinheit befestigt. Wenn das Fahrzeug gestohlen wird, benachrichtigt der Eigentümer die Polizei. Anschließend aktiviert die Polizei den Sender aus der Ferne, dieser sendet ein Dauersignal, mit dem die Polizei das Fahrzeug lokalisieren und sicherstellen kann. Der Nachteil dieses Systems besteht darin, dass der Eigentümer zunächst feststellen und die Behörden darüber in Kenntnis setzen muss, dass sein Eigentum gestohlen wurde. Somit ist es möglich, dass die Diebe das Fahrzeug entwenden, wobei der Eigentümer den Diebstahl nicht gleich bemerkt, und mehrere Stunden daran arbeiten können, den Diebstahlschutz zu umgehen oder das Fahrzeug auseinanderzubauen. Darüber hinaus kann ein erfahrener Dieb die Sende-/Empfangsvorrichtung leicht deaktivieren oder sogar entfernen, wodurch die Effizienz dieses Diebstahlschutzsystems umgangen wird.

[0012] Andere Produkte verwenden GPS-Satelliten (Global Positioning System), mit denen Fahrzeugführer in einer Notlage Hilfe rufen oder Behörden gestohlene Fahrzeuge verfolgen können. Der Fahrzeugführer muss ein in das Fahrzeug eingebautes Mobiltelefon verbinden und beim Starten des Fahrzeugs einen Pass-Code eingeben.

[0013] Weitere Nachteile dieser und verwandter Systeme bestehen darin, dass der Eigentümer monatliche Servicegebühren für die Nutzung des Systems zahlt. Bei einer anderen Konstruktion muss das System aktiv und in ein Telefonsystem eingesteckt sein. Die im Voraus entstehenden Kosten für Teile und Einbau sind hoch. Darüber hinaus verringern viele Lösungen die Fähigkeit zu arbeiten und werden daher nicht verwendet.

[0014] Im Allgemeinen besitzt jedes aus der Ferne aktivierte Diebstahlschutz-Zusatzsystem, das nicht betriebsbereit ist, wenn das System nicht betriebsbereit ist, eine gravierende Schwäche: wenn das System physikalisch entfernt werden kann, während es nicht betriebsbereit ist, kann ein Dieb es zu einem abgeschirmten Standort bringen und ausführlich daran arbeiten, das System auseinanderzubauen oder den Schutz zu entfernen.

[0015] Das Dokument US-A-5046082 beschreibt ein aus der Ferne zugängliches Mobiltelefon und ein Host-System. Es wird ein Sicherheitsschlüssel bereitgestellt, der unberechtigten Zugriff auf das aus der Ferne zugängliche Mobiltelefon verhindert. Dieses Dokument stellt jedoch keine Maßnahmen bereit, um das Mobiltelefon funktionsunfähig zu machen.

[0016] Gemäß der vorliegenden Erfindung werden ein tragbares Computersystem gemäß Anspruch 1 und ein Systemsicherheitsverfahren gemäß Anspruch 11 bereitgestellt.

[0017] Der Computer enthält eine RF-Empfängereinheit, die immer aktiv ist, selbst dann, wenn der Computer dies nicht ist. Wenn der Computer als gestohlen gemeldet wird, wird ein Signal an den Empfänger gesendet, um eine Sicherheitsfunktion zu aktivieren, selbst wenn der Benutzer diese Sicherheitsfunktion vorher deaktiviert hat. Wenn der Computer das nächste Mal eingeschaltet wird, hindert diese Sicherheitsfunktion den Dieb daran, den Computer zu verwenden.

[0018] Diese Sicherheitsarchitektur in der derzeit bevorzugten Ausführungsform zerstört den Betrieb des Systems nicht dauerhaft, sondern stellt einfach die in das System eingebauten Sicherheits-Schutzoptionen wieder her. Dies erfolgt durch das Setzen eines Bits in einem nichtflüchtigen Speicher, wonach das System anschließend ein Passwort benötigt, um einen Zugang für den Betrieb des Systems bereitzustellen. (Wenn der Benutzer den Passwortschutz nicht aktiviert hat, muss er sich ein Not-Passwort von seinem Systemadministrator oder von der technischen Unterstützung (technical support) holen.) Es ist ein wichtiges Merkmal dieser Ausführungsform, dass dies während der Selbsttest-Prozedur des Systems beim Hochfahren (Power-On Self-Test-Prozedur – "POST-Prozedur") des Systems durchgeführt wird und somit nicht umgangen werden kann.

[0019] Ein Vorteil besteht darin, dass diese Funktion an bestehende Kommunikationssysteme von Drittanbietern gekoppelt werden kann, um es zu ermögli-

chen, dass der Computer einen Befehl empfangen kann, um den Betrieb für unberechtigte Eigentümer zu unterbinden. Beispielsweise stellt das Unternehmen Eagle Eye Technologies, Inc., ein Verfolgungssystem her, das in der Lage ist, einen Wiedergabesender (transponder) mit einer Genauigkeit von 3 Metern um den tatsächlichen Standort zu orten. Die vorliegende Anmeldung verwendet ein etwas unterschiedliches Verfahren, das auf derselben Funkfrequenz(RF)-Schnittstellen-Hardware basiert, um ein elektronisches Schlüsselbit in dem nichtflüchtigen RAM eines Computers (oder einer mobilen oder tragbaren Einheit vergleichbarer Komplexität) zu setzen, was den Betrieb der Einheit verhindert, wenn ein Sicherheitsbefehl gesendet wird. Diebe werden zögern, eine Vorrichtung mit dieser Funktion zu stehlen.

[0020] Ein anderer Vorteil wird auf einer niedrigeren Ebene erhalten. Wenn die Funktion auf der Systemplatine integriert ist, kann der Betrieb der Platine selbst gesperrt werden. Dies verhindert einen Austausch der Platinen mit Heimcomputern durch Betriebsangehörige.

[0021] Ein weiterer Vorteil ist der Schutz von Benutzerdaten auf einer höheren Ebene. Der Diebstahl geschützter Informationen wird schwieriger, da dem Prozess ein weiteres Hemmnis hinzugefügt wird. Wenn das System gesperrt ist, muss der Dieb die Speichereinheit entfernen und sie in ein kompatibles System einbauen, um die Informationen zu stehlen.

[0022] Ein weiterer Vorteil gegenüber Sicherheitssystemen nach dem Stand der Technik besteht darin, dass Systeme auch während des Versands und der Lagerung in einem Lager geschützt sind. Wenn eine Warenladung verschwindet, kann ihr unrechtmäßiger Betrieb von jedem Punkt im Land oder möglicherweise sogar der Welt aus gesperrt werden.

[0023] Vorzugsweise ist der Satellitenempfänger immer eingeschaltet und kann somit Befehle empfangen, um die Sicherheitsfunktion selbst dann zu aktivieren, wenn das System stromlos geschaltet ist. Dies verhindert, dass Diebe einen gestohlenen Computer an einen abgeschirmten Ort bringen können, um dessen Schutz zu umgehen.

[0024] Ein weiterer Vorteil besteht darin, dass das System, nachdem es verloren gegangen oder gestohlen wurde, selbst dann gesichert werden kann, wenn der ursprüngliche Benutzer herkömmliche Sicherheitsfunktionen nicht genutzt hat.

[0025] Während die Aktivierung einer Startpasswort-Anforderung die bevorzugte Sicherheitsfunktion ist, können stattdessen bei alternativen Ausführungsformen andere Sicherheitsfunktionen aktiviert werden. Beispielsweise besteht eine einfache (jedoch weniger bevorzugte) Wahl darin, das System bedingungslos zu sperren. Dies wird weniger bevorzugt, da es wahrscheinlicher ist, dass dies einem rechtmäßigen Benutzer erhebliche Unbequemlichkeiten bereiten kann, wenn es versehentlich aktiviert wurde.

[0026] In einer anderen Ausführungsform kann das System die Sicherheitsfunktion dauerhaft aktivieren, indem eine Sicherung in einer Schlüsselschaltung durchbrennt, statt ein Bit in dem nichtflüchtigen Speicher zu markieren.

[0027] In einer anderen Ausführungsform kann das System die Hardware deaktivieren, indem eine Sicherung in einer Schlüsselschaltung durchbrennt, statt ein Bit in dem nichtflüchtigen Speicher zu markieren.

[0028] In einer anderen Ausführungsform kann das System alternativ ein Bit in dem CMOS setzen, statt ein Bit in dem nichtflüchtigen Speicher zu markieren. Diese Alternative wird jedoch weniger bevorzugt, da die CMOS-Einstellungen gelöscht werden können, indem die CMOS-Sicherungsbatterie physikalisch entfernt wird.

[0029] In noch einer anderen Ausführungsform kann die Sicherheitsfunktion auch zu anderen Zeiten geprüft werden, beispielsweise dann, wenn eine Plug-and-Plag-Aktualisierung erfolgt oder immer dann, wenn das System aus einem Ruhemodus (sleep mode) wieder hochfährt (wakeup).

[0030] In anderen Ausführungsformen können anstelle des Verwendens eines Boot-Passwortes (boot passwording) und/oder der oben genannten Sperrfunktionen oder zusätzlich dazu auch andere Sicherheitsfunktionen verwendet werden.

[0031] Anstelle des Aufzeichnens des Zeitpunktes, zu dem ein Signal empfangen wurde, kann das System einen Zeitgeber verwenden, um zu bestimmen, ob innerhalb der zugewiesenen Zeitdauer ein gültiges Signal empfangen wurde.

[0032] Die bevorzugte Ausführungsform verwendet ein System, bei dem ein periodisches Signal an die Einheit gesendet wird, um sicherzustellen, dass eine Kommunikation nach wie vor möglich ist. Alternativ kann das Programm für die POST-Prozedur eine Anforderung für eine Zustandsprüfung initiieren und anschließend auf eine Antwort warten.

[0033] Das offenbarte Sicherheitssystem kann zusammen mit anderen Kommunikationsprodukten von Drittanbietern verwendet werden, wie beispielsweise globale Nachverfolgungssysteme (global tracking systems) zum Lokalisieren des Systems nach einem Diebstahl.

[0034] Beispielhafte Ausführungsformen der Erfin-

dung werden nun in Bezug auf die beigefügten Zeichnungen beschrieben, in denen:

[0035] Fig. 1A ein Ablaufdiagramm des Sicherheitssteuerungsprozesses darstellt.

[0036] Fig. 1B stellt ein Ablaufdiagramm des Sicherheitssteuerungsprozesses des Empfängersystems dar.

[0037] Fig. 1C stellt ein Ablaufdiagramm des gesamten Sicherheitssteuerungsprozesses dar, sobald bestimmt wird, dass eine Vorrichtung ihrem Eigentümer gestohlen wurde.

[0038] Fig. 2 stellt ein Blockdiagramm eines tragbaren Computers dar, der die innovative, entfernte Sicherheitsarchitektur verwenden kann.

[0039] In Bezug auf das Ablaufdiagramm aus Fig. 1C empfängt die Einheit, die für das Aktivieren des Sicherheitsmechanismus verantwortlich ist, nach einer ersten Benachrichtigung von dem Eigentümer, dass eine Vorrichtung mit der innovativen Ausführungsform gestohlen wurde, den Bericht über gestohlenes Eigentum und initiiert den Sicherheitsprozess (Schritt **180**). Anschließend wird ein Überprüfungsprozess ausgeführt, um sicherzustellen, dass der Eigentümer mit dem geeigneten Gerät korrekt identifiziert wurde (Schritt **182**). Wenn der Überprüfungsprozess abgeschlossen ist, werden die notwendigen Befehle zu einem weltweiten Positionierungssystem (worldwide positioning system) hochgeladen (Schritt **184**), um per Satellitenfunk an die Vorrichtung gesendet zu werden (Schritt **186**). Danach wird eine „Lokalisieren und Sperren"-Sequenz ausgeführt (Schritt **188**), die dazu führt, dass die Vorrichtung durch die jeweiligen Verriegelungsschaltungen gesperrt wird. In diesem Fall stellt ein Computerchip, der von M2M hergestellt wurde, ein Bit in dem NVRAM ein (Schritt **190**), wodurch der im Folgenden dargelegte Sicherheitsabfrageprozess ausgelöst wird.

[0040] Fig. 1B stellt ein Ablaufdiagramm der Aktionen des Empfängerteils des Sicherheitssteuerungsprozesses dar. Dieser Teil des Prozesses wird durch den Empfang eines Signals initiiert (Schritt **150**). Immer dann, wenn ein Signal von dem Sicherheitssystem empfangen wird, wird das Signal bewertet (Schritt **160**), um zu bestimmen, ob diese spezielle Einheit als gestohlen gemeldet wurde und somit gesperrt werden muss. Solange das Signal anzeigt, dass die Einheit nicht als gestohlen gemeldet wurde, protokolliert das Sicherheitssystem einen Zeitpunkt, zu dem das letzte Signal empfangen wurde (Schritt **155**), kehrt dann zurück und wartet auf das nächste Signal. Wenn jedoch das Signal anzeigt, dass die Einheit als gestohlen gemeldet wurde, setzt das System ein Bit in dem nichtflüchtigen Speicher, um anzuzeigen, dass die Einheit gesperrt werden muss (Schritt **170**).

[0041] Es ist darauf hinzuweisen, dass die Empfängerschaltung immer aktiv ist, selbst dann, wenn das System selbst ausgeschaltet ist. Da dies der Fall ist, kann das Sperrsignal zu jeder Zeit gesendet werden, und das System wird gesichert. Wie nachstehend beschrieben, ist es dem Benutzer möglicherweise bis zu der nächsten Nutzung nicht bewusst, dass das System gesperrt ist.

[0042] Fig. 1A stellt ein Ablaufdiagramm des Sicherheitssteuerungsprozesses dar, wenn der Computer aktiviert ist. Zuerst schaltet der Benutzer den Strom für das System ein (Schritt **100**). Kurz danach wird die Ausführung der POST-Prozedur (Schritt **101**) des Computers gestartet. Das System führt eine Speicherprüfung (Schritt **103**) und eine NVRAM-Prüfung durch (Schritt **106**). Wenn irgendeine der Speicherprüfungen fehlschlägt, wird das System gesperrt (Schritt **115**). Wenn die Speicherprüfungen korrekt durchlaufen, setzt der Prozess mit Hardwareprüfungen der Empfängerschaltungen fort (Schritt **109**). Wenn das Fehlerbit in dem NVRAM entweder durch einen vorherigen Sperrbefehl oder durch Versuche, die Schaltungen zu deaktivieren, gesetzt wurde (Schritt **112**), bleibt der Systembetrieb gesperrt (Schritt **115**). Wenn die Prüfung des Empfängers korrekt durchläuft (Schritt **109**), wird im nächsten Schritt bestimmt, ob ein Befehl empfangen wurde, der das Fehlerbit in dem NVRAM einstellt (Schritt **112**), wodurch das System gesperrt wird (Schritt **115**). Ist dies der Fall, wird das System gesperrt (Schritt **115**). Ist dies nicht der Fall, überprüft das System, dass innerhalb der vorgeschriebenen Zeitverzögerungsbegrenzung ein periodisches Freigabesignal empfangen wurde (Schritt **118**), indem der Zeitpunkt, zu dem das letzte Signal empfangen wurde, mit der inneren Uhr verglichen wird. Ist dies der Fall, setzt die POST-Prozedur (Schritt **124**) fort und ermöglicht bei einem erfolgreichen Abschluss den vollständigen Systembetrieb (Schritt **130**). Wenn die Verzögerungsspanne abgelaufen ist (Schritt **118**), unternimmt das System einen weiteren Versuch, das erforderliche Passwort zu erhalten (Schritt **121**) und das System betriebsbereit zu halten. Wenn das Passwort ungültig ist (Schritt **127**), wird das System gesperrt (Schritt **115**). Wenn das Passwort gültig ist (Schritt **127**), bleibt das System vollständig betriebsbereit (Schritt **130**). Das Autorisierungsschema ist so angelegt, dass eine Dienstverweigerungssituation (denial-of-service) nur bei extremen Fällen verwendet wird.

[0043] Fig. 2 stellt einen tragbaren Computer dar, der die innovative, entfernte Sicherheitsarchitektur verwenden kann. Das System umfasst einen Stromumrichter **205**, der zum Aufladen einer Batterie **215** verwendet wird. Optional ist eine Batterie-Schnittstelle **210** zwischen die Batterie und den Rest der Schaltungen zwischengeschaltet. Der

Stromumrichter **205** ist über einen Zweiweg-Brückengleichrichter **200** verbunden, um Strom aus einer Netzspannungsquelle zu erhalten, und er ist verbunden, um der Batterie **215** eine Gleichspannung bereitzustellen. Die Batterie **215** (oder der Wandler **205**), die über einen Spannungsregler **220** verbunden ist, kann das gesamte, tragbare Computersystem mit Strom versorgen, dies umfasst in diesem Beispiel:
Benutzereingabegeräte (beispielsweise eine Tastatur **235** und eine Maus **240**);
wenigstens einen Mikroprozessor **225**, der in Wirkbeziehung verbunden ist, um Eingaben von dem genannten Eingabegerät über einen Schnittstellenverwaltungschip **230** (der darüber hinaus den verschiedenen Anschlüssen eine Schnittstelle bereitstellt) zu empfangen;
einen Speicher (beispielsweise einen Flash-Speicher **255** und einen RAM **260**), auf den der Mikroprozessor zugreifen kann;
eine Datenausgabevorrichtung (beispielsweise eine Anzeige **250** und eine Videoanzeige-Adapterkarte **245**), die verbunden ist, um Daten auszugeben, die durch den Mikroprozessor erzeugt wurden;
ein Magnetscheiben-Laufwerk **270**, auf das der Mikroprozessor über eine Schnittstellen-Einheit **265** Lese-Schreib-Zugriff hat; sowie
eine elektronische Optionsschaltung **295** zum Empfangen aktueller Standortinformationen von einem weltweiten Positionierungssystem und zum selektiven Entsperren oder Sperren des Betriebs des Computersystems.

[0044] Optional können selbstverständlich viele andere Komponenten enthalten sein, und diese Konfiguration ist auf keine Weise bestimmend. Beispielsweise kann der tragbare Computer darüber hinaus ein CD-ROM-Laufwerk **280** und ein Diskettenlaufwerk (floppy disk drive – FDD) **270** enthalten, die eine Schnittstelle zu der Scheiben-Schnittstellensteuereinheit **265** (disk interface controller) besitzen können. Des Weiteren kann ein L2-Zwischenspeicher **285** hinzugefügt werden, um den Datenzugriff von den Scheibenlaufwerken zu dem Mikroprozessor zu beschleunigen, und in einem PCMCIA-**290**-Schlitz können Peripherieerweiterungen untergebracht werden.

[0045] In einem weiteren Beispiel ermöglicht es der Einsatz der Erfindung Behörden, bei Motorfahrzeugen einen Betrieb des Fahrzeuges zu sperren, wenn der Diebstahl desselben gemeldet wurde oder wenn dies aus anderen Gründen für notwendig gehalten wird.

[0046] Ein weiterer Einsatz der Erfindung bei kostspieligen Mobiltelefonen stellt ein Abschreckungsmittel gegen Diebstahl bereit. Die Möglichkeit, den Betrieb einer Vorrichtung zu sperren, wenn die Vorrichtung ihrem rechtmäßigen Eigentümer gestohlen wurde, hat einen erheblichen Einfluss auf ihren Wert für einen Dieb.

[0047] Vermögensverwaltung ist in großen Unternehmen häufig ein Problem. Wenn ein bestimmtes Gerät (beispielsweise ein tragbarer Computer) bei der Bestandsaufnahme nicht auffindbar ist, kann bei einer weiteren Klasse von Ausführungsformen das offenbarte Sicherheitssystem dazu verwendet werden, das Gerät einfach zu sperren. Wenn das Gerät rechtmäßig übertragen wurde, ist der rechtmäßige Benutzer gezwungen, sich wegen der Sperrung an den Service zu wenden, und das Gerät kann dann reaktiviert werden. (Selbstverständlich sind geeignete Vorsichtsmaßnahmen nötig, bevor eine solche Prozedur auf Geräte angewendet werden kann, die durch eine plötzliche Außerbetriebsetzung Schäden hervorrufen können.)

[0048] Implementierungen der Funktion der Erfindung in Instrumente der Hochtechnologie verhindern einen Diebstahl dieser sehr kostspieligen Art von Geräten. Derartige Komponenten können einen oder mehrere programmierbare Prozessoren enthalten und eine System-Reset-Prozedur besitzen, in die die beschriebenen Sicherheitsbeziehungen eingefügt werden können.

[0049] Eine Person mit gewöhnlicher Erfahrung auf dem Gebiet der Technik kann erkennen, dass das in der vorliegenden Anmeldung beschriebene, innovative Konzept über einen gewaltigen Bereich von Anwendungen modifiziert und variiert werden kann, und demgemäß ist der Umfang des patentierten Gegenstandes nicht durch irgendeine der angegebenen, spezifizierten, beispielhaften Lehren begrenzt.

Patentansprüche

1. Tragbares Computersystem, das optional die Eingabe eines Startpasswortes während der Systeminitialisierung erfordert, wobei das tragbare Computersystem umfasst:
wenigstens einen Mikroprozessor (**225**),
einen nichtflüchtigen Speicher (**255**), der Einstellungen für administrative Konfigurationen enthält,
einen Speicher, der so verbunden ist, dass durch den Mikroprozessor Schreib/Lesezugriff darauf erfolgen kann,
eine Power-On Self-Test-Prozedur (S101) (POST-Prozedur), ausgeführt während der Initialisierung des tragbaren Computersystems, wobei die POST-Prozedur erfordern kann, dass ein Benutzer ein Startpasswort eingibt, um den Systembetrieb freizugeben, und wenn ein Startpasswort erforderlich ist und kein gültiges Startpasswort eingegeben wird, die Initialisierung nicht abgeschlossen wird und das System nicht betriebsfähig sein wird (S115),
Eingabe-/Ausgabeschaltungen, die in Wirkbeziehung mit dem Mikroprozessor verbunden sind, und

einen RF-Empfänger (**295**), selbst dann aktiv, wenn das System ausgeschaltet ist, wirkend verbunden, um in den nichtflüchtigen Speicher zu schreiben, wobei der Empfänger, unabhängig davon, ob der tragbare Computer ein- oder ausgeschaltet ist, sowohl für einen Sicherheitsaktivierungsbefehl als auch ein periodisches Freigabesignal, empfangen aus einer RF-Sendequelle über ein Kommunikationssystem, empfänglich ist,
wobei das tragbare Computersystem wenigstens eine Sicherheitsfunktion enthält, die durch Befehlsgebung an den Empfänger, wenigstens eine der Einstellungen in dem nichtflüchtigen Speicher zu modifizieren, oder entweder durch Empfangen eines Sicherheitsaktivierungsbefehls durch das Kommunikationssystem oder, falls der Empfänger verfehlt, das periodische Freigabesignal innerhalb einer vorgeschriebenen Zeitverzögerungsbegrenzung zu empfangen, aktiviert werden kann, wobei die Sicherheitsfunktion umfasst:
(i) wenn der tragbare Computer ausgeschaltet ist, Anfordern der Eingabe eines gültigen Startpasswortes während sich anschließender Systeminitialisierung, oder
(ii) wenn der tragbare Computer eingeschaltet ist, Erzwingen eines Resets des Computers und Anfordern der Eingabe eines gültigen Startpasswortes, um den Systembetrieb bei der sich anschließenden Systeminitialisierung freizugeben.

2. System nach Anspruch 1, wobei der Empfänger (**295**) mit dem System integral ist.

3. System nach einem der vorhergehenden Ansprüche, wobei das System ohne den Empfänger (**295**) nicht funktioniert.

4. System nach einem der vorhergehenden Ansprüche, wobei der Empfänger (**295**) eine drahtlose Vorrichtung ist.

5. System nach einem der vorhergehenden Ansprüche, wobei das Kommunikationssystem Funkfrequenz nutzt.

6. System nach einem der vorhergehenden Ansprüche, wobei der Empfänger in eine Systemplatine integriert ist, die ebenso den Mikroprozessor (**225**) trägt.

7. System nach einem der vorhergehenden Ansprüche, wobei der Empfänger selbst dann aktiv ist, wenn der Mikroprozessor (**225**) im Schlafmodus ist.

8. System nach einem der vorhergehenden Ansprüche, wobei der Empfänger ebenso wirkend verbunden ist, um den Mikroprozessor (**225**) in eine Reset-Prozedur zu zwingen.

9. System nach einem der vorhergehenden Ansprüche, wobei der Betrieb des Systems automatisch gesperrt wird, wenn ein elektronisches Schlüsselbit in den Speicher (**255**) gesetzt wird.

10. System nach einem der vorhergehenden Ansprüche, wobei der Betrieb des Systems automatisch gesperrt wird, wenn der Empfänger nicht betriebsfähig ist.

11. Verfahren zum Sichern eines tragbaren Computersystems, das optional die Eingabe eines Startpasswortes während der Systeminitialisierung erfordert, wobei das Verfahren die folgenden Schritte umfasst:
Empfangen, unabhängig davon, ob der Computer ein- oder ausgeschaltet ist, eines periodischen Freigabesignals von einer RF-Sendequelle und
Aktivieren wenigstens einer Sicherheitsfunktion entweder, wenn das nächste der periodischen Freigabesignale nicht empfangen wird oder wenn ein Sicherheitsaktivierungsbefehl empfangen wird, und
Aktivieren der Sicherheitsfunktion durch das Setzen eines Bits in den nichtflüchtigen Speicher (**255**),
Reagieren auf das Setzen des Bits, durch:
(i) wenn der tragbare Computer ausgeschaltet ist, Anfordern der Eingabe eines gültigen Startpasswortes während der sich anschließenden Systeminitialisierung, oder
(ii) wenn der tragbare Computer eingeschaltet ist, Erzwingen eines Resets des Computers und Anfordern der Eingabe eines gültigen Startpasswortes, um den Systembetrieb bei der sich anschließenden Systeminitialisierung freizugeben.

12. Verfahren nach Anspruch 11, wobei der Empfangsschritt einen Empfänger nutzt, der konstant aktiv ist, selbst wenn andere Teile des Systems inaktiv sind.

13. Verfahren nach Anspruch 11 oder 12, wobei die Sicherheitsfunktion während einer automatischen Power-On Self-Test-Prozedur des Computers bedingt aktiviert ist.

14. Verfahren nach einem der Ansprüche 11 bis 13, wobei die Sicherheitsfunktion den Betrieb des Systems sperrt.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1A

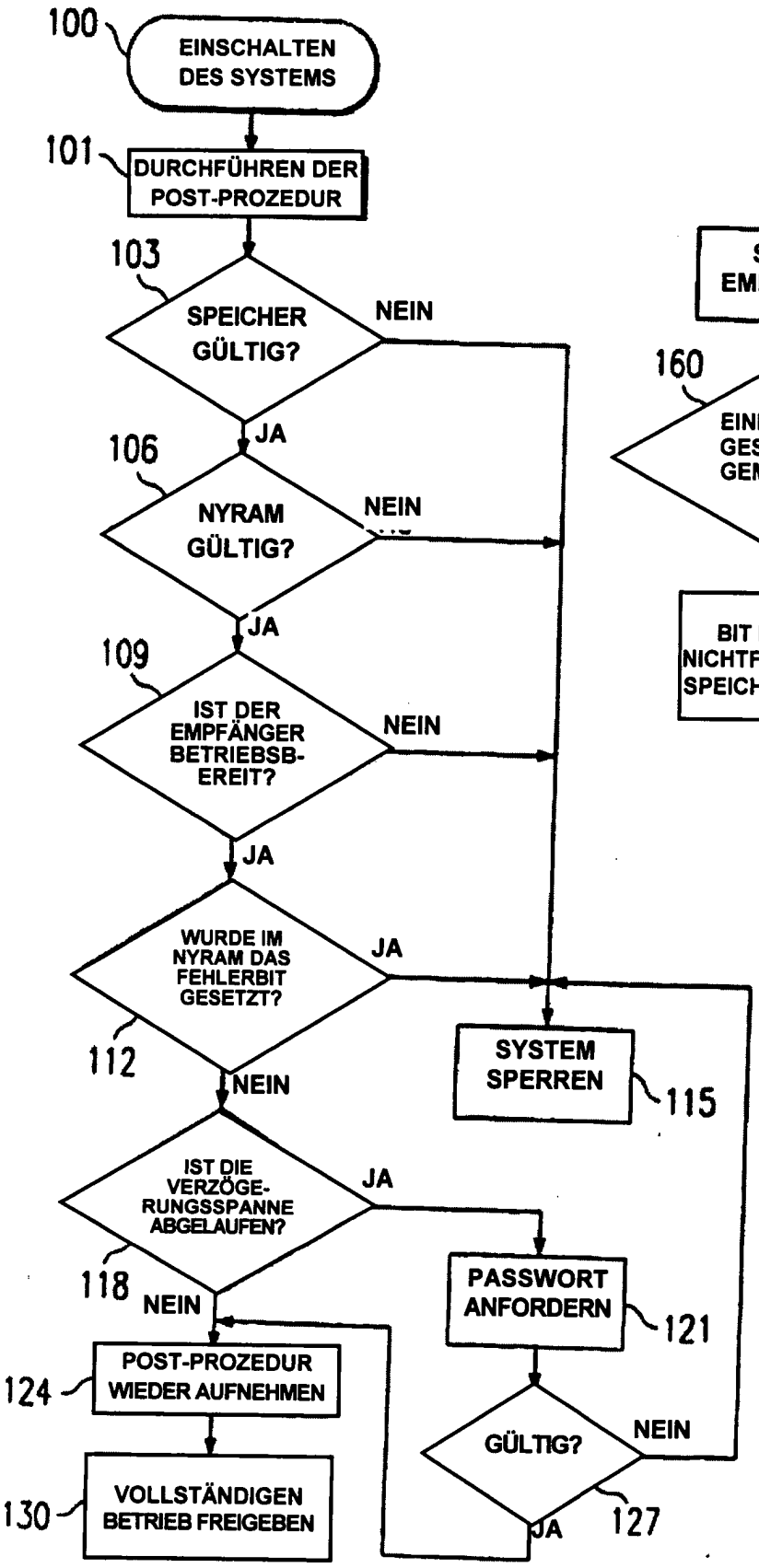
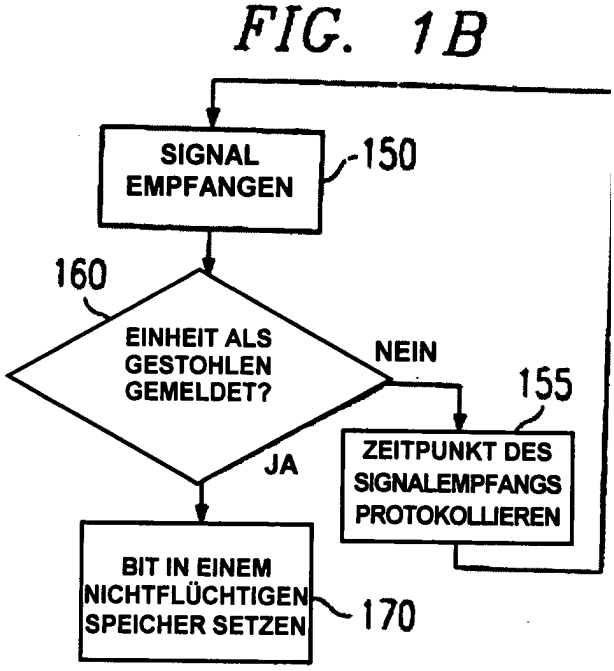


FIG. 1B



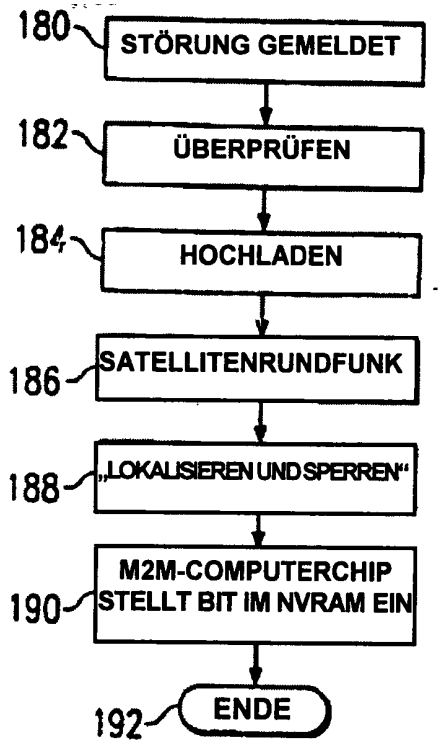

180
STÖRUNG GEMELDET
182
ÜBERPRÜFEN
184
HOCHLADEN
186
SATELLITENRUNDFUNK
188
„LOKALISIEREN UND SPERREN"
190
M2M-COMPUTERCHIP STELLT BIT IM NVRAM EIN
192
ENDE

FIG. 1C

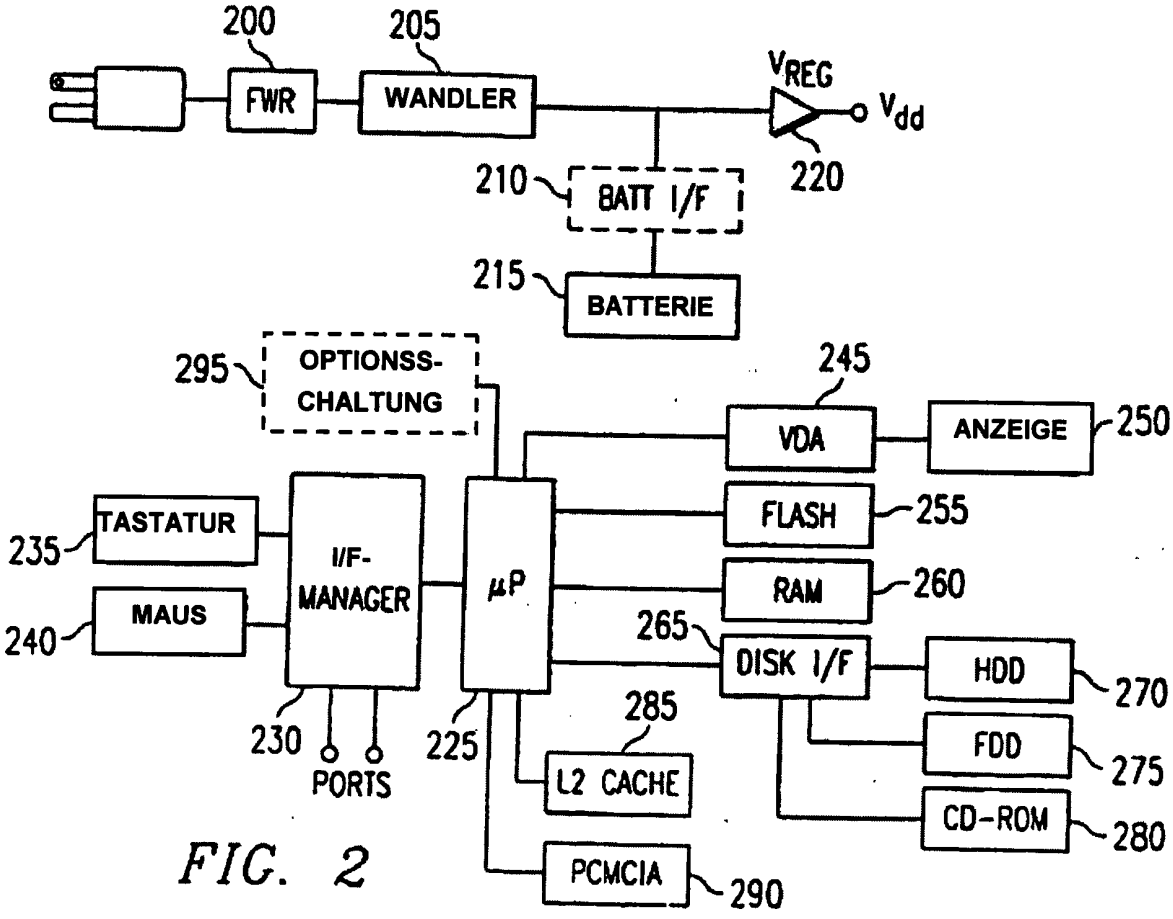

200
205
FWR
WANDLER
V_{REG}
V_{dd}
220
210
BATT I/F
215
BATTERIE
295
OPTIONSS-CHALTUNG
245
VDA
ANZEIGE
250
TASTATUR
235
MAUS
240
I/F-MANAGER
µP
FLASH
255
RAM
260
265
DISK I/F
HDD
270
FDD
275
CD-ROM
280
230
PORTS
225
285
L2 CACHE
PCMCIA
290

FIG. 2