(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 536 306 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
01.06.2005 Bulletin 2005/22

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **04023384.3**

(22) Date of filing: **30.09.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **30.09.2003 US 507586 P**
13.09.2004 US 609537 P

(71) Applicant: **Broadcom Corporation**
Irvine, California 92618-7013 (US)

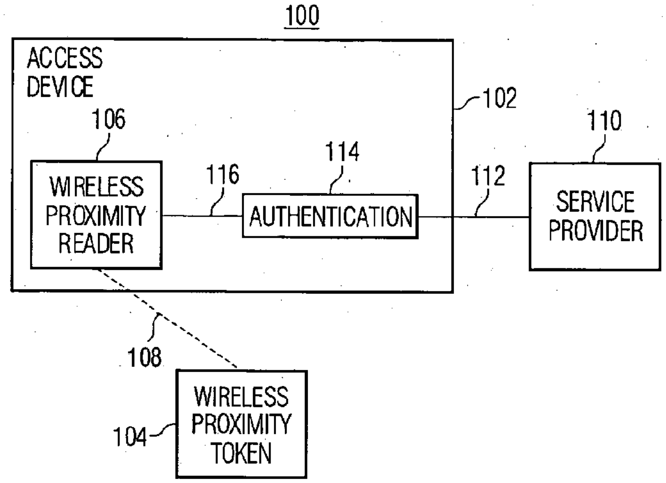
(72) Inventors:
- **Buer, Mark**
Gilbert, AZ 85296 (US)
- **Frank, Edward H.**
Atherton, CA 94027 (US)
- **Seshadri, Nambirajan**
Irvine, CA 92612 (US)

(74) Representative: **Jehle, Volker Armin, Dipl.-Ing.**
Patentanwälte
Bosch, Graf von Stosch, Jehle,
Flüggenstrasse 13
80639 München (DE)

(54) Proximity authentication system

(57) Access to secured services may be controlled based on the proximity of a wireless token to a computing device through which access to the secured services is obtained. An authorized user may be provided access to a service only when a wireless token assigned to the user is in the proximity of the computing device. A user's credential may be stored on an RFID token and an RFID reader may be implemented within a security boundary on the computing device. Thus, the credential may be passed to the security boundary without passing through the computing device via software messages or applications. The security boundary may be provided, in part, by incorporating the RFID reader onto the same chip as a cryptographic processing component. Once the information is received by the RFID reader it may be encrypted within the chip. As a result, the information may never be presented in the clear outside of the chip. The cryptographic processing component may cryptographically encrypt/sign the credential received from the token so that assurance may be provided to a service provider that the credentials came from a token that was proximate to the computing device. An RFID reader, cryptographic processing components and a wireless network controller may be implemented on a single chip in a mobile device.

FIG 1



Description

CROSS-REFERENCE TO RELATED APPLICATION (S)

[0001] This application claims the benefit of U.S. Provisional Patent Application No. _______________, filed September 13, 2004, entitled PROXIMITY AUTHENTICATION SYSTEM, Attorney Docket No. 53492/SDB/B600, and U.S. Provisional Patent Application No. 60/507,586, filed September 30, 2003, the disclosures of which are hereby incorporated by reference herein.

TECHNICAL FIELD

[0002] This application relates to data communication systems and, more specifically, to techniques for authenticating proximity of a wireless token in a communication system.

BACKGROUND

[0003] A variety of security techniques are known for protecting information in and controlling the operation of a computing device such as a personal computer ("PC"), a server or a mobile device. For example, physical and/or cryptographic techniques may be employed to control access to the computing device and to data stored in the computing device.

[0004] Physical security techniques may include locating the computing device in a secure location, locking the computing device in an enclosure, protecting integrated circuits (i.e., chips) from invasive monitoring by encapsulating the chips in, for example, an epoxy.

[0005] Cryptographic techniques may include one or more of encryption, decryption, authentication, signing and verification. In some applications data encryption and decryption techniques may be used to prevent unauthorized applications or persons from accessing data stored in the computing device. For example, security passwords that are used to restrict access a PC may be stored on the PC in an encrypted form. The operating system may then decrypt password when it needs to compare it with a password typed in by a user.

[0006] In some applications authentication techniques may be used to verify that a given set of data is authentic. For example, when a server receives a message from a remote client, authentication information associated with the message may used to verify that the message is from a specific source. In this way, the server may ensure that only authorized clients access the applications and data provided by the server.

[0007] In practice, there may be circumstances under which the process of sending secret credentials such as a password or cryptographic key may be compromised. For example, when a user uses a computing device to access a secured service, the user may first need to enter the secret credentials into the computing device. The computing device may then forward these credentials to a service provider that then determines whether the user is authorized to use the requested service.

[0008] In the event the computing device has been comprised by a hacker or a computer virus, an unauthorized person may gain access to these credentials. As a result, an unauthorized person may be able to access the secured service. Serious consequences may result when the secured service includes sensitive information such as financial data or personal information. Accordingly, a need exists for improved techniques for providing access to secured services.

SUMMARY

[0009] The invention relates to a system and method for authenticating the proximity of a wireless token to a computing device. For convenience, an embodiment of a system constructed or a method practiced according to the invention will be referred to herein simply as an "embodiment."

[0010] In one aspect, the invention relates to a system and method for providing access to a secured service based on a user's proximity to a proximity reader. Once the proximity is authenticated the user may then be allowed to access the secured service.

[0011] In some embodiments an authorized user is provided access to a service only when a wireless token assigned to the user is in the proximity of a computing device through which access to the secured services is obtained. In this way, a reasonable assumption may be made that the authorized user is in fact using the computing device to request the service. In contrast, if the request was being made by a hacker or a computer virus, access may be denied since the token may not be in the proximity of the computing device.

[0012] In some embodiments a user's credential are stored on an RFID token and an RFID reader is implemented within a security boundary on the computing device. In this way, the credential may be passed to the security boundary without passing through the computing device via software messages or applications. As a result, the credentials may not be intercepted by a hacker or computer virus that may have compromised the software executing on the computing system.

[0013] In some embodiments the security boundary may be provided, in part, using tamper resistant and/or tamper evident hardware. Thus, in the event the computer was physically tampered with in an attempt to compromise the security of the security boundary, such tampering may be ineffective or it may be evident to the user. In the latter case, the user may then take appropriate steps to re-secure the system.

[0014] In some embodiments, the RFID reader is incorporated onto the same chip as a cryptographic processing component. In this way, once the information from the RFID token is received by the RFID reader it may be encrypted within the chip. As a result, the information may never be presented in the clear (e.g., unencrypted) outside of the chip. Accordingly, the information may only be compromised by a clandestine RFID reader or by inspecting the internal contents of the chip. In conventional commercial settings, these scenarios may be unlikely. Accordingly, a system constructed according to the invention may provide improved access control for secured services.

[0015] In some embodiments, a cryptographic processing component may cryptographically encrypt and/or sign credentials received from a token. Thus, when a service provider receives the credentials, a high level of assurance may be provided to the effect that the credentials came from a token that was proximate to the particular computing device.

[0016] In some embodiments an RFID reader, a cryptographic processing component and one or more wireless network controller(s) may be implemented on a single chip in a mobile device. This may provide a cost effective and secure mechanism to limit access to the wireless network(s). In this case, network access may only be provided to the mobile device when a token is proximate to the mobile device and when that token has been assigned to an authorized user of that mobile device and the network(s).

[0017] According to an aspect of the invention, a communication system comprises:

> an wireless proximity reader configured to receive an RF signal from a wireless token located within a defined proximity to the proximity reader and configured to extract information from the received RF signal; and
>
> a wireless network interface coupled to receive the information from the proximity reader and send the information over a wireless network.

[0018] Advantageously, the system comprises a security boundary within which the information is extracted and received.

[0019] Advantageously, the wireless proximity reader is an RFID reader.

[0020] Advantageously, the system comprises an authentication processor configured to authenticate the information sent over the wireless network.

[0021] Advantageously, the system comprises a cryptographic processor configured to encrypt or authenticate the information sent over the wireless network.

[0022] Advantageously, the cryptographic processor uses a key to cryptographically sign the information that is sent over the wireless network.

[0023] Advantageously, the wireless network interface supports at least one of 802.11 and Bluetooth.

[0024] Advantageously, the wireless network interface comprises at least one of an 802.11 media access controller and a Bluetooth media access controller.

[0025] Advantageously, the wireless network interface comprises an 802.11 media access controller and a Bluetooth media access controller.

[0026] Advantageously, the wireless network interface uses the information to provide authentication to the wireless network.

[0027] Advantageously, the system comprises a service processor coupled to receive the information sent over the wireless network and configured to provide access to a service in response to the information.

[0028] Advantageously, the system comprises a wireless access point adapted to receive the information sent over the wireless network and provide the information to a service provider.

[0029] Advantageously, the system comprises a wireless access point adapted to receive the information sent over the wireless network and provide access to the wireless network in response to the information.

[0030] Advantageously, the information comprises a password or key.

[0031] Advantageously, the system comprises an RFID token comprising:

> a data memory for storing the information;
>
> an RF circuit coupled to the data memory for generating a signal according to the information; and
>
> an antenna coupled to receive the signal from the RF circuit and adapted to transmit the signal to the wireless proximity reader.

[0032] According to an aspect of the invention, a method of controlling access to a service comprises:

> verifying whether a wireless token is within a defined proximity to a processing device;
>
> authenticating information associated with the wireless token; and
>
> providing the authenticated information to a service provider.

[0033] Advantageously, the method comprises establishing a security boundary for the verifying, authenticating and providing.

[0034] Advantageously, at least a portion of the security boundary comprises a cryptographic boundary.

[0035] Advantageously, at least a portion of the security boundary comprises an integrated circuit.

[0036] Advantageously, authenticating comprises cryptographically signing the information with a key.

[0037] Advantageously, the authenticated information comprises a response to a challenge from the service provider.

[0038] Advantageously, providing comprises encrypting data sent to the service provider.

[0039] Advantageously, the method comprises requesting access to a service from a service provider.

[0040] Advantageously, the method comprises receiving a challenge from the service provider.

[0041] Advantageously, the service provider provides access to a service in response to the authenticated information.

[0042] Advantageously, the service provider provides access to a data network in response to the authenticated information.

[0043] Advantageously, the service provider provides access to at least one of an 802.11 network and a Bluetooth network.

[0044] Advantageously, the service provider provides access to an 802.11 network and a Bluetooth network.

[0045] Advantageously, the service provider provides access to encrypted data in response to the authenticated information.

[0046] Advantageously, the service provider provides a key in response to the authenticated information.

[0047] Advantageously, the information comprises credentials associated with a user of the token.

[0048] Advantageously, an RFID proximity reader verifies whether the wireless token is within the defined proximity to the wireless proximity reader.

[0049] According to an aspect of the invention, a method of controlling access to a service comprises:

> receiving an RF signal from a proximate wireless token;
> obtaining information from the RF signal;
> authenticating the information from the RF signal; and
> providing the authenticated information to a service provider.

[0050] Advantageously, the method comprises establishing a security boundary for the obtaining, authenticating and providing.

[0051] Advantageously, authenticating comprises cryptographically signing the information with a key.

[0052] Advantageously, providing comprises encrypting the signed information.

[0053] Advantageously, the method comprises requesting access to a service from a service provider.

[0054] Advantageously, the method comprises receiving a challenge from the service provider in response to the request.

[0055] Advantageously, the authenticated information comprises a response to the challenge.

[0056] Advantageously, the service provider provides access to a service in response to the authenticated information.

[0057] Advantageously, the RF signal is an RFID signal.

[0058] Advantageously, the information comprises credentials associated with a user of the token.

[0059] According to an aspect of the invention, an integrated circuit comprises:

> a wireless proximity reader configured to receive an RF signal from a wireless token located within a defined proximity to the integrated circuit;
> at least one lead that is only routed within the integrated circuit for coupling the wireless proximity reader to a wireless network interface; and
> a wireless network interface coupled to receive the information from the wireless proximity reader and provide the information to a port on the integrated circuit to send the information over a wireless network.

[0060] Advantageously, the integrated circuit comprises a security boundary.

[0061] Advantageously, the wireless proximity reader is an RFID reader.

[0062] Advantageously, the integrated circuit comprises a cryptographic processor configured to encrypt or authenticate the information sent over the wireless network.

[0063] Advantageously, the cryptographic processor uses a key to cryptographically sign the information that is sent over the wireless network.

[0064] Advantageously, the wireless network interface comprises at least one of an 802.11 media access controller and a Bluetooth media access controller.

[0065] Advantageously, the wireless network interface comprises an 802.11 media access controller and a Bluetooth media access controller.

[0066] Advantageously, the wireless network interface uses the information to provide authentication to the wireless network.

[0067] Advantageously, the information comprises a password or key.

[0068] According to an aspect of the invention, a communication system comprises:

> a wireless proximity reader configured to receive an RF signal from a wireless token located within a defined proximity to the wireless proximity reader and configured to extract information from the received RF signal; and
> a key management component coupled to receive the information from the wireless proximity reader and send the information to a service provider.

[0069] Advantageously, the system comprises a security boundary within which the information is extracted and received.

[0070] Advantageously, the key management component comprises a trusted platform module.

[0071] Advantageously, a user is authenticated to the trusted platform module by moving the wireless token within the defined proximity to the wireless proximity reader.

[0072] Advantageously, the trusted platform module provides access to a protected service after the user is authenticated.

[0073] Advantageously, the trusted platform module provides access to encrypted data after the user is authenticated.

[0074] Advantageously, the trusted platform module enables use of protected keys after the user is authenticated.

[0075] Advantageously, the system comprises a network interface wherein the trusted platform module provides access to a network via the network interface after the user is authenticated.

[0076] Advantageously, the network interface comprises a wireless interface.

[0077] Advantageously, the network interface comprises at least one of an 802.11 network interface and a Bluetooth network interface.

[0078] Advantageously, the network interface comprises an 802.11 network interface and a Bluetooth network interface.

[0079] Advantageously, the system comprises a service provider configured to provide access to data and a service.

[0080] Advantageously, the system comprises a service provider configured to supply cryptographic keys.

[0081] Advantageously, the wireless proximity reader is included within a boundary of the key management component.

[0082] Advantageously, the wireless proximity reader is an RFID reader.

[0083] According to an aspect of the invention, a method of providing access to a service comprises:

> receiving an RF signal from a proximate wireless token;
> obtaining information from the RF signal;
> authenticating the information to a key management component; and
> providing, by the key management component, access to a service.

[0084] Advantageously, the method comprises establishing a security boundary for the receiving, obtaining, authenticating and providing.

[0085] Advantageously, at least a portion of the security boundary comprises a cryptographic boundary.

[0086] Advantageously, at least a portion of the security boundary comprises an integrated circuit.

[0087] Advantageously, the method comprises authenticating the information and providing the authenticated information to a service provider.

[0088] Advantageously, authenticating the information comprises cryptographically signing the information with a key.

[0089] Advantageously, the key management component comprises a trusted platform module.

[0090] Advantageously, the trusted platform module enables key usage after the user is authenticated.

[0091] Advantageously, the trusted platform module enables access to processing resources after the user is authenticated.

[0092] Advantageously, the trusted platform module enables access to data network services after the user is authenticated.

[0093] Advantageously, the RF signal is an RFID signal.

[0094] Advantageously, the information comprises credentials associated with a user of the token.

[0095] Advantageously, the service comprises at least one of 802.11 network access and Bluetooth network access.

[0096] Advantageously, the service comprises 802.11 network access and Bluetooth network access.

[0097] According to an aspect of the invention, an integrated circuit comprises:

> a wireless proximity reader configured to receive an RF signal from a wireless token located within a defined proximity to the wireless proximity reader and configured to extract information from the received RF signal; and
> at least one connection within the integrated circuit for coupling the wireless proximity reader to a wireless network interface; and
> a key management component coupled to receive the information from the wireless proximity reader and provide the information to a port on the integrated circuit to send the information to a service provider.

[0098] Advantageously, the integrated circuit comprises a security boundary within which the information is extracted and received.

[0099] Advantageously, the wireless proximity reader is an RFID reader.

[0100] Advantageously, the wireless proximity reader is included within a boundary of the key management component.

[0101] Advantageously, the key management component comprises a trusted platform module.

[0102] Advantageously, the wireless proximity reader is included within a boundary of the trusted platform module.

[0103] Advantageously, the integrated circuit comprises a network interface wherein the trusted platform module provides access to a network via the network interface after the user is authenticated.

[0104] Advantageously, the network interface comprises a wireless interface.

[0105] Advantageously, the wireless network interface comprises at least one of an 802.11 network interface and a Bluetooth network interface.

[0106] Advantageously, the wireless network interface comprises an 802.11 network interface and a Bluetooth network interface.

BRIEF DESCRIPTION OF THE DRAWINGS

[0107] These and other features, aspects and advantages of the present invention will be more fully understood when considered with respect to the following detailed description, appended claims and accompanying

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**