

SYSTEM AND METHOD FOR AUTHENTICATION VIA A PROXIMATE DEVICE

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 60/637,668, filed Dec. 20, 2004, the disclosure of which is hereby incorporated by reference herein.

TECHNICAL FIELD

[0002] This application relates to data processing and, more specifically, to a system and method of authenticating devices via at least one proximate device.

BACKGROUND

[0003] A variety of services may be accessed using computing devices such as personal computers and wireless handsets. For example, a user may access data stored on or applications running on the computing device. In addition, a user may connect to a data network to gain access to data and applications on remote servers.

[0004] In some cases, access to a service may be limited to authorized users. For example, a service may provide access to sensitive data such as financial information or personal information. In addition, access to a service may require payment of a fee.

[0005] A variety of techniques are known for securing access to services via a computing device. For example, a user may be required to present some form of credential to a computing device that provides the service (the "service provider"). Here, the credential may indicate that a particular user (or anyone who knows the credential) may access a given service. In some applications a credential may take the form of a user name and password that was provided to the user and the service provider by a system administrator. When the user accesses a service, the user may present the user name and password to the service provider. The service provider then verifies that this credential is assigned to an authorized user of the requested service.

[0006] In a typical data network, access to the data network is limited to devices that have been properly installed on the network. As part of this installation, cryptographic techniques may be employed to ensure that only authorized devices are connected to the network. In general, cryptographic techniques may include one or more of encryption, decryption, authentication, signing and verification.

[0007] For example, a network administrator may load one or more cryptographic keys (hereafter "key(s)") into each device that is authorized to connect to the network. The network administrator also loads corresponding keys into a network access device (e.g., a router) that is connected to, for example, a wide area network ("WAN"). When the device attempts to access the network, the network access device verifies that a proper key has been loaded into that device. Once verified, the network access device enables the requesting device access to the network.

[0008] In practice, the process of authorizing a user to use a service and installing devices on a network may be relatively cumbersome and time consuming. As described

above, these operations tend to be relatively manual in nature. However, distributed computing services are becoming increasingly prevalent and affordable to access. For example, the proliferation of wireless computing networks and handheld devices enables a user to use a variety of devices to access a variety of different networks that may exist throughout a city, etc. Accordingly, a need exists for more efficient techniques for enabling a user to access secured services.

[0009] Moreover, conventional methods of entering or loading a credential or a cryptographic key into a device may be compromised in some circumstances. For example, when a user uses a computing device to access a secured service, the user may first need to enter the credential into the computing device. Typically, this is accomplished using an input device such as a keyboard. The computing device may then forward these credentials to a service provider that determines whether the user is authorized to use the requested service.

[0010] 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. For example, a personal computer may incorporate a trusted computing module ("TPM") to control access to certain secured services (e.g., access to an encrypted data file or a secured network). Here, the TPM may require a user to enter a password or other credential before the TPM allows the user to access these services. If the user uses a keyboard to enter this information, the password may be routed through the personal computer from the keyboard to the TPM via an insecure path. For example, the keyboard may connect to a USB port and a software driver may be used to transfer the data from the USB bus to a TPM that, for example, is connected to a South Bridge of the personal computer. However, the hacker or virus may be able to access data that is forwarded and/or stored by the software driver. As a result, an unauthorized person may acquire the password and gain access to the secured service.

[0011] Similarly, secret key information used in wireless devices may be compromised. For example, to enable secure communication between two Bluetooth devices, complementary keys may need to be loaded into each device. In some applications, a key is transferred from one Bluetooth device to the other Bluetooth device via the Bluetooth network. However, an unauthorized person may be able to intercept the broadcast Bluetooth signal containing the key. As a result an unauthorized person may acquire the key and gain access to secured services.

[0012] Serious consequences may result when the secured services control and provide access to sensitive information such as financial data or personal information. Accordingly, a need exists for more secure techniques for providing access to secured services.

SUMMARY

[0013] The invention relates to a system and method for authenticating a user or users to use one or more devices in a communication system. For convenience, an embodiment of a system constructed or a method practiced according to the invention may be referred to herein simply as an "embodiment."