

SYSTEM AND METHOD FOR PROTECTED MESSAGING

BACKGROUND

Field of the Invention

The invention relates to the field of computers and passing messages between a pre-operating system program and an operating system present program. More specifically, information may be passed among pre-operating system programs and operating system present programs on a computing device via a protected storage.

BACKGROUND OF THE INVENTION

As computers and computing devices are now ubiquitous in our society, computer security issues have become important. Ways of deterring theft of computers and computing devices are evolving to meet the challenges posed by the portable nature of laptop computers, cellular telephones, personal digital assistants, and other computing devices. Various methods of user authentication may be used to provide security and deter theft. These methods include passwords, retinal scan, fingerprint scan, and voice scan.

In some computers, upon powering up, the computer's basic input output system (BIOS) may require authentication such as a password before allowing an operating system to boot. In other computing devices, a password or other authentication must be provided to allow for completion of booting of an operating system, connecting to a network, accessing a database, or starting application programs such as, for example, an electronic mail program. Some programs provide for secure documents such that a document may not be viewed, or edited without entering a password or otherwise authenticating the user's right to access the document.

Although all these security measures exist in various forms, a user may become burdened by and annoyed at having to remember multiple passwords, at having to enter multiple password, and at having to regularly authenticate the user's rights to use the particular computing device, software program, etc.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an embodiment of a system architecture in which the system and method for protected messaging are practiced.

FIG. 2 illustrates an embodiment of a computing device in which the system and method for protected messaging are practiced.

FIG. 3 illustrates a flow of actions taken according to an embodiment of a system and method for protecting messaging.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an embodiment of a system architecture in which the system and method for protected messaging are practiced. This invention describes how a new platform primitive, protected storage **130**, may be used to send messages between the pre-operating system (Pre-OS) operating space **160** and the operating system present (OS-Present) operating space **170**. This protected message passing enables, among other things, the ability to have single, or at least simplified, log on capability. That is, information about the user who logs on to a computing device during

booting up and how they logged in may be placed in protected storage so that other Pre-OS programs and OS-Present user applications may access it. Similarly, OS-Present applications may send messages to other OS-Present applications and Pre-OS applications via the protected storage. One example of an OS-Present application leaving a message for a Pre-OS application via the protected storage may be to reconfigure hardware or software components. In this example, a high-level OS-Present application may be used to obtain configuration information that may be used by one or more Pre-OS applications to reconfigure the system. In a related embodiment, an OS Present application may store an executable routine in the protected storage which is run by a Pre-OS application upon rebooting/restarting. In addition, OS-Present applications may use the protected storage to transfer configuration data, security policies, authentication data and other information among themselves, and may also share this information with or receive this information from Pre-OS applications via the protected storage. Pre-OS applications **100** and OS-Present applications **140** use interfaces **125** and **155** to access protected storage medium **130** to accomplish this method and system. These interfaces are provided by Pre-OS driver **120** and OS-Present driver **150**. In this way, a general bi-directional messaging feature is provided.

As used herein, a Pre-OS application program may include a basic input output system (BIOS) program as well as other applications that may execute during boot up before the operating system is loaded and may include applications stored on optional read-only memory (ROM) devices associated with various peripherals attached to or part of the personal computing device. An OS-Present application program may be any application program that runs while the operating system is present.

In one embodiment, the protected storage medium may be the protected storage hardware or hardware layer of the Intel® Protected Access Architecture (EPAA) described in Application Interface Specification, Rev. 0.9.5 available from Intel Corporation of Santa Clara, California. (the "IPAA Specification"). In this embodiment, interface **125** may be the interface layer described in the IPAA Specification, and Pre-OS driver **120** may be the support layer or service provider described in the IPAA Specification.

FIG. 2 illustrates an embodiment of a computing device in which the system and method for protected messaging are practiced. Computing device **200** may be a personal computer, a portable computer, a server, a cellular telephone, a personal digital assistant, a computer tablet, or other computing device. The computing device **200** illustrated in FIG. 2 is of a personal computer embodiment in which processor **210** may execute instructions using main memory **212** which is accessed via memory controller **214**. Main memory may be any well known random access memory (RAM) or other volatile memory device. The instructions may be obtained from BIOS chip **216** and software stored on disk memory **224** such as operating system **226** and application programs **228**. In one embodiment, protected storage **220** may be exclusively coupled to processor **210**. In another embodiment, the protected storage may be coupled to the processor via bus **222**. In this embodiment, other components may be able to access the protected storage. Instructions may also be provided via drivers **218** which may be included on the BIOS chip **216**. Drivers **218** may, in another embodiment, be included as part of the protected storage medium. It is the drivers that provide the interfaces between the Pre-OS applications and the protected storage, and