

SECURE CODE EXECUTION USING EXTERNAL MEMORY

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 60/628,795, filed Nov. 17, 2004, and U.S. Provisional Patent Application No. 60/667,350, filed Mar. 31, 2005, the disclosure of each of which is hereby incorporated by reference herein.

TECHNICAL FIELD

[0002] This application relates to processing systems and, more specifically, to an upgradeable and secure computing 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 to a PC may be stored on the PC in an encrypted form. The operating system may then decrypt the 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 be 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] Various standards have been developed to enhance the level of trust for users of computing systems. For example, the Trusted Computing Group organization has developed standards for a platform known as a trusted platform module ("TPM"). A TPM may provide a set of cryptographic capabilities that enable certain computer functions to be securely executed within the TPM environment (e.g., hardware). In a typical embodiment, a TPM (e.g., an integrated circuit incorporating TPM hardware and code) may be incorporated into a computer. Also, requirements such as FIPS 140-2 have been developed that relate to methods of upgrading firmware using approved authentication techniques.

[0008] The secure protection provided by systems such as TPMs may make it more difficult to upgrade the systems in the field. For example, in some applications the upgrade process must satisfy the system's security requirements or the upgrade may need to be performed by actually replacing one or more components in the system. These factors may adversely affect the cost of the system. Accordingly, a need exists for improved techniques for upgrading secure systems.

SUMMARY

[0009] A system and/or method of providing code for a system, substantially as shown in and/or described in connection with at least one of the figures, as set forth more completely in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] 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 drawings, wherein:

[0011] **FIG. 1** is a simplified block diagram of one embodiment of a system constructed in accordance with the invention;

[0012] **FIG. 2** is a simplified block diagram of one embodiment of a computing system constructed in accordance with the invention;

[0013] **FIG. 3** is a simplified block diagram of one embodiment of a TPM system constructed in accordance with the invention;

[0014] **FIG. 4** is a flow chart of one embodiment of manufacturing-related operations that may be performed in accordance with the invention;

[0015] **FIG. 5** is a flow chart of one embodiment of boot-related operations that may be performed in accordance with the invention;

[0016] **FIG. 6** is a flow chart of one embodiment of instruction-related operations that may be performed in accordance with the invention;

[0017] **FIG. 7** is a flow chart of one embodiment of update operations that may be performed in accordance with the invention;

[0018] **FIG. 8** is a flow chart of one embodiment of update operations that may be performed in accordance with the invention;

[0019] **FIG. 9** is a simplified diagram relating to one embodiment of secure code operations in accordance with the invention; and

[0020] **FIG. 10** is a flow chart of one embodiment of key upgrade operations that may be performed in accordance with the invention.

[0021] In accordance with common practice the various features illustrated in the drawings may not be drawn to scale. Accordingly, the dimensions of the various features may be arbitrarily expanded or reduced for clarity. In addition, some of the drawings may be simplified for clarity. Thus, the drawings may not depict all of the components of