

of secure code blocks. This attack may be prevented by including the logical flash address in the HMAC-SHA1 digest. Fourth, an attacker may attempt to attack the flash keys by using the TPM as an oracle to encrypt arbitrary data. This attack may be prevented by restricting use of the TPM's keys.

[0215] In the event an attacker is able issue upgrade commands, the following techniques may be used to thwart potential attacks. First, the attacker may attempt to load arbitrary secure code descriptors or secure code blocks. This attack may be prevented by verifying the upgrade start and upgrade complete signatures. Second, the upgrade start command from one set of secure code information may be followed by upgrade updates from a second set of secure code information. Assuming the verification public key was not changed, this attack may be prevented by calculating a SHA1 digest across all upgrade commands.

[0216] The following techniques may be used to thwart attacks that could potentially result in a permanent loss of data. First, the attacker may attempt to remove power when the secure code descriptor is being updated. This attack may be prevented by double-buffering the secure code descriptor in flash. Second, the attacker may attempt to overwrite TPM flash data by issuing multiple upgrade update commands. This attack may be prevented by checking the maximum number of blocks (e.g., 256 byte blocks) that are written to flash. In addition, the TPM may only issue upgrade update or upgrade complete commands when the previous command was issued successfully.

[0217] Given the teachings herein, it will be apparent that a system constructed in accordance with the invention may be implemented in a variety of ways and may, therefore, incorporate a variety of components and operations. For example, the teachings of the invention may be implemented in a variety of processing systems other than those specifically mentioned. The teachings of the invention also may be applied to data memories or other components other than those specifically mentioned. Moreover, a variety of cryptographic techniques and algorithms other than those specifically mentioned may be used to support secure updates. In addition, the teachings of the invention may be used to update different types of information including, but not limited to, the forms of information specifically mentioned. Hence the teachings of the invention are not limited to the specific structure, components and operations disclosed herein.

[0218] It should be appreciated that the various components and features described herein may be incorporated in a system independently of the other components and features. For example, a system incorporating the teachings herein may include various combinations of these components and features. Thus, not all of the components and features described herein may be employed in every such system.

[0219] Different embodiments of the invention may include a variety of hardware and software processing components. In some embodiments of the invention, hardware components such as controllers, state machines and/or logic are used in a system constructed in accordance with the invention. In some embodiments code such as software or firmware executing on one or more processing devices may be used to implement one or more of the described operations.

[0220] Such components may be implemented on one or more integrated circuits. For example, in some embodiments several of these components may be combined within a single integrated circuit. In some embodiments some of the components may be implemented as a single integrated circuit. In some embodiments some components may be implemented as several integrated circuits.

[0221] The components and functions described herein may be connected/coupled in many different ways. The manner in which this is done may depend, in part, on whether the components are separated from the other components. In some embodiments some of the connections represented by the lead lines in the drawings may be in an integrated circuit, on a circuit board and/or over a backplane to other circuit boards. In some embodiments some of the connections represented by the lead lines in the drawings may comprise a data network, for example, a local network and/or a wide area network (e.g., the Internet).

[0222] The signals discussed herein may take several forms. For example, in some embodiments a signal may be an electrical signal transmitted over a wire while other signals may consist of light pulses transmitted over an optical fiber.

[0223] A signal may comprise more than one signal. For example, a signal may consist of a series of signals. Also, a differential signal comprises two complementary signals or some other combination of signals. In addition, a group of signals may be collectively referred to herein as a signal.

[0224] Signals as discussed herein also may take the form of data. For example, in some embodiments an application program may send a signal to another application program. Such a signal may be stored in a data memory.

[0225] The components and functions described herein may be connected/coupled directly or indirectly. Thus, in some embodiments there may or may not be intervening devices (e.g., buffers) between connected/coupled components.

[0226] A wide variety of devices may be used to implement the data memories discussed herein. For example, a data memory may comprise flash memory, one-time-programmable (OTP) memory or other types of data storage devices.

[0227] In summary, the disclosure herein generally relates to an improved secure code load mechanism. While certain exemplary embodiments have been described above in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive of the broad invention. In particular, it should be recognized that the teachings of the invention apply to a wide variety of systems and processes. It will thus be recognized that various modifications may be made to the illustrated and other embodiments of the invention described above, without departing from the broad inventive scope thereof. In view of the above it will be understood that the invention is not limited to the particular embodiments or arrangements disclosed, but is rather intended to cover any changes, adaptations or modifications which are within the scope and spirit of the invention as defined by the appended claims.