

[0031] In some embodiments the secure code update scheme described herein is used in conjunction with a trusted platform module (“TPM”) in a computing system. In a typical application a TPM may generate and maintain keys for the computing system. For example, 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 associated with the TPM). To this end the TPM may include one or more cryptographic processors that perform cryptographic operations including, for example, one or more of encryption, decryption, authentication, verification, signing and key management. Specifications for a TPM are defined by the Trusted Computing Group organization.

[0032] FIG. 2 illustrates one embodiment of a computing system 200 that incorporates a TPM 202. In this embodiment, the TPM 202 is implemented in an integrated circuit 204. An external data memory such as a flash memory 206 may be associated with the integrated circuit 204. The computing system also includes a host processing component 208 (e.g., a processor) that performs the basic processing for the computing system. An external interface component 210 may enable the computing system to communicate with external systems via, for example, a wired or wireless network or a removable media via an external connection 212. Data busses 214, 216 and 218 may be used to enable communication between the various components of the computing system 200.

[0033] In some embodiments some or all of the components shown in FIG. 2 may be implemented on a motherboard (not shown). In this case the busses 214 and 216 may comprise, for example, a PCI bus (e.g., PCI, PCIX or PCI-Express), a low pin count (“LPC”) bus, etc.

[0034] In some embodiments the integrated circuit 204 may include other components to, for example, reduce the number of integrated circuits on the motherboard. For example, one or more cryptographic processor(s) 220 that may be used by the TPM 202 may be incorporated into the integrated circuit. In addition, the integrated circuit 204 may include one or more other processing component(s) 222 that may operate independently of the TPM 202. The integrated circuit also may include a flash controller 224 through which the TPM 202 and/or other processing component(s) 222 may access the flash memory 206.

[0035] Code routines for the TPM 202 may be stored in an internal memory 226. Several provisions may be made to ensure the security of these code routines. For example, the internal memory 226 may be a ROM that is not reprogrammable. In this case, the code routines may be incorporated into the integrated circuit when the integrated circuit is manufactured (e.g., taped out).

[0036] In one aspect of the invention the TPM 202 supports upgradeable code that may be securely stored in the flash memory 206. This allows field upgrades to be made even after the chip has taped out. In addition to fixing bugs or security holes, this flexibility may enable a manufacturer to tailor the code for each OEM that incorporates the integrated circuit 204 into its products. One advantage of using separate internal and external memories is that a relatively expensive fabrication process that may be required to generate a programmable non-volatile memory (e.g., flash memory) need not be used to fabricate the other components

of the system. For example, a relatively cost effective process (e.g., a standard CMOS process) may be used to manufacture the integrated circuit 204 while the other more expensive process is used to generate the flash memory 206. In this way, a lower total system cost may be realized.

[0037] In some embodiments the majority of the code will be stored on-chip in the ROM 226. In this way, the number of accesses to the flash memory 206 (which may have a relatively slow access time) may be kept to a minimum.

[0038] In the event code needs to be upgraded or new code added, the modified and/or new code is stored in the flash memory 206 on, for example, a function-by-function basis. Accordingly, provisions are made to enable the TPM 202 to execute code stored in the flash 206 and to determine whether routines are to be executed from the internal ROM 226 or the external flash memory 206.

[0039] In some embodiments a function table (not shown in FIG. 2) is used to determine whether a given function to be executed by the TPM 202 is stored in the internal memory 226 or the flash memory 206. In some embodiments the function table may be stored in the flash memory 206. For example, when a new and/or modified set of functions is loaded into the flash memory 206, a new function table that references the new and/or modified functions also may be loaded into the flash memory 206. The TPM may then access the new function table to determine whether it should retrieve code for a given function from ROM 226 or flash memory 206.

[0040] In some embodiments new code may be loaded into the computing system via the external interface 210. In this case the TPM 202 may receive code from the host processing component 208 via bus 312 (e.g., an LPC bus). The TPM 202 may then load the code into the flash memory 206 via the flash controller 224.

[0041] In some embodiments provisions may be made in an attempt to ensure that only authorized (e.g., secure) functions and function tables are loaded into the flash memory 206. For example, information that was received may be loaded into the flash memory only when the information was cryptographically signed (e.g., using a secure key) by a trusted source. A key that corresponds to the signing key also may be securely stored locally by the TPM 202. Thus, the TPM may verify any incoming information using its key. In this way, the TPM 202 may only load information into the flash memory 206 after that information is verified.

[0042] In some embodiments the trusted source uses a protected private key to sign any code that is to be downloaded into the flash. A public key that corresponds to the private key may be securely loaded in the computing system 200 when the system is manufactured or downloaded at a later time. The public key may then be securely stored in the computing system (e.g., in the TPM 202 or elsewhere in the integrated circuit 204 or stored in encrypted form in the flash memory 206).

[0043] In some embodiments the information received by the TPM 202 may be encrypted by the trusted source or the computing system 200. In this case, a key securely stored in the computing system (e.g., in the TPM 202, the integrated circuit 204 or encrypted in the flash memory 206) may be used to decrypt the received information.