

[0044] In some embodiments provisions may be made in an attempt to ensure that only secured functions and function tables are retrieved from the flash memory 206. For example, the TPM 202 may encrypt and/or authenticate information using a secure key before storing the information in the flash memory 206. In this way the TPM 202 may be configured to only execute code from flash memory 206 in the event the code was successfully decrypted and/or authenticated after it was retrieved from the flash memory 206. Again, the key(s) used for the encryption, decryption and authentication operations may be securely stored in the computing system (e.g., in the TPM 202, the integrated circuit 204 or encrypted in the flash memory 206).

[0045] Referring now to FIGS. 3-10, exemplary components and operations of a TPM-based secure system will now be discussed in more detail. FIG. 3 is a simplified block diagram of one embodiment of a TPM and associated flash memory components. FIGS. 4-8 and 10 are simplified flowcharts illustrating various embodiments of operations that may be performed in conjunction with and/or by the secure system. FIG. 9 is a simplified diagram illustrating one embodiment of how information stored in the flash memory may be authenticated.

[0046] In FIG. 3 a secure data processing system 300 includes a TPM 302, a flash controller 304 and an external data memory 306 such as a flash memory. In some embodiments the TPM 302 (and optionally the flash controller 304) may be implemented within a single integrated circuit (i.e., chip) and the flash memory 306 may be implemented within another chip (i.e., on a different die).

[0047] Several of the TPM components communicate via one or more data busses (hereafter "data bus 316"). For example, in the embodiment of FIG. 3 a processor 308, one or more data buffers (hereafter data buffer 318), an LPC bus interface 320 and an external interface module 322 are connected to the data bus 316.

[0048] The data buffer 318 provides storage for the processor 308 and other system components. In particular, the data buffer 318 may provide persistent memory, volatile memory, stack/heap space and I/O space for the processor 308. In some embodiments the persistent memory may be used to store data (e.g., data 356 and 358 discussed below) that is loaded in from the flash memory 306.

[0049] The external interface module 322 provides a mechanism for the processor 308 or other components to access the flash memory 306. To this end the external interface module 322 communicates with the flash controller 304 to send data to and receive data from the flash memory 306.

[0050] The LPC bus interface 320 provides an interface to an LPC bus 324. As discussed in conjunction with FIG. 2, the TPM 302 may communicate with other processing components in the system (e.g., a host processor 208) via the LPC bus 324.

[0051] The processor 308 controls the main operations of the TPM 302. To this end, the processor 308 executes code that is stored in either an instruction ROM 310 or the external flash 306. In an attempt to ensure the integrity of the code executed by the TPM 302, the TPM 302 may include several secure code components. The secure code components shown in FIG. 3 include an instruction multiplexer

312, an instruction cache controller 326 and associated instruction cache 328, one or more cryptographic processor(s) 330 and a one-time programmable memory 332.

[0052] In some embodiments the instruction multiplexer 312 is used to facilitate retrieving code from the instruction ROM 310 or the external flash 306. For example, the processor 308 may request code via an instruction bus 314. Based on the particular function call associated with the code, the instruction multiplexer 312 may retrieve code from the appropriate data memory.

[0053] In some embodiments the instruction cache 328 may be used to cache code, a function table and other information that is stored in the flash 306. In some embodiments the cache comprises a fully-associative 32 kbyte instruction cache that contains 128 cache lines of 256 bytes each. It should be understood, however, that this is but one example and that an instruction cache may be implemented in various ways and store various data grouped in various ways.

[0054] The instruction cache controller 326 provides any required interfaces and processing for retrieving information from the flash memory 306, storing the information in the cache 328 and providing the information to the instruction multiplexer 312. On a cache miss, the instruction cache controller 326 may fetch, for example, a block (e.g., 256 bytes, 512 bytes, etc.) of secure code and an HMAC (e.g., 16 bytes, 20 bytes, etc.) from the external flash memory. The block of secure code may be decrypted (e.g., 3DES) and authenticated (e.g., HMAC-SHA1) against the HMAC. To this end, the instruction cache controller 326 may include one or more cryptographic processor(s) 334 for performing the decryption and authentication operations.

[0055] The cryptographic processor(s) 330 may be used to provide cryptographic processing for the TPM 302. For example, the cryptographic processor(s) 330 may include a public key core 350 for performing asymmetric cryptographic operations such as DSA, RSA and Diffie-Hellman. In addition, the cryptographic processor(s) 330 may include an authentication core 352 for performing algorithms such as HMAC-SHA1. Also, the cryptographic processor(s) 330 may include a symmetric cryptographic core 354 for performing algorithms such as DES, 3DES and AES. It should be understood that the above algorithms are examples only and that the cryptographic processor(s) 330 may implement one or more of a variety of cryptographic algorithms and perform one or more of a variety of operations.

[0056] The one-time programmable ("OTP") memory 332 may be used to store security information such as key material for security routines. For example, when the TPM 302 is manufactured security routines may be used to generate secret keys that are unique to each TPM. These keys may then be stored in the OTP memory 332. Moreover, provisions may be made to ensure that these secret keys are not allowed to be read out of the TPM (or the integrated circuit within which the TPM resides) in the clear (e.g., in unencrypted form). Through the use of these keys and/or keys derived from these keys, the TPM may securely store information outside of the TPM (or the integrated circuit within which the TPM resides). For example, the cryptographic processor(s) 330 may use these keys to encrypt and/or authenticate any data that is stored in an external memory such as the flash memory 306.