



US 20060107032A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2006/0107032 A1**

Paaske et al.

(43) **Pub. Date: May 18, 2006**

(54) **SECURE CODE EXECUTION USING EXTERNAL MEMORY**

Publication Classification

(76) Inventors: **Timothy R. Paaske**, San Jose, CA (US); **Jeffrey C. Glover**, Longmont, CO (US)

(51) **Int. Cl.**
G06F 9/24 (2006.01)
(52) **U.S. Cl.** 713/2

Correspondence Address:
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068 (US)

(57) **ABSTRACT**

New code routines for a secure system (e.g., a TPM) are stored in a memory (e.g., a flash memory) that is located external to the secure system. For example, a chip may include a TPM and an external flash memory may be connected to the chip. New routines for the TPM may then be stored in the flash. A function table may be used to determine whether a given function to be executed by the TPM is stored in on-chip memory (e.g., ROM) or in the flash. New function tables may be stored in the flash. For example, when a new set of functions is loaded into the flash, a new function table that references the new functions also may be loaded into the flash.

(21) Appl. No.: **11/250,265**

(22) Filed: **Oct. 13, 2005**

Related U.S. Application Data

(60) Provisional application No. 60/628,795, filed on Nov. 17, 2004. Provisional application No. 60/667,350, filed on Mar. 31, 2005.

