(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 January 2005 (20.01.2005)

PCT

(10) International Publication Number
WO 2005/006109 A3

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number:
PCT/US2003/039809

(22) International Filing Date:
15 December 2003 (15.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/464,884 19 June 2003 (19.06.2003) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NJ 10504 (US).

(72) Inventor: CRAFT, David, J.; 114 Bluff Park Circle, Austin, TX 78746-4300 (US).

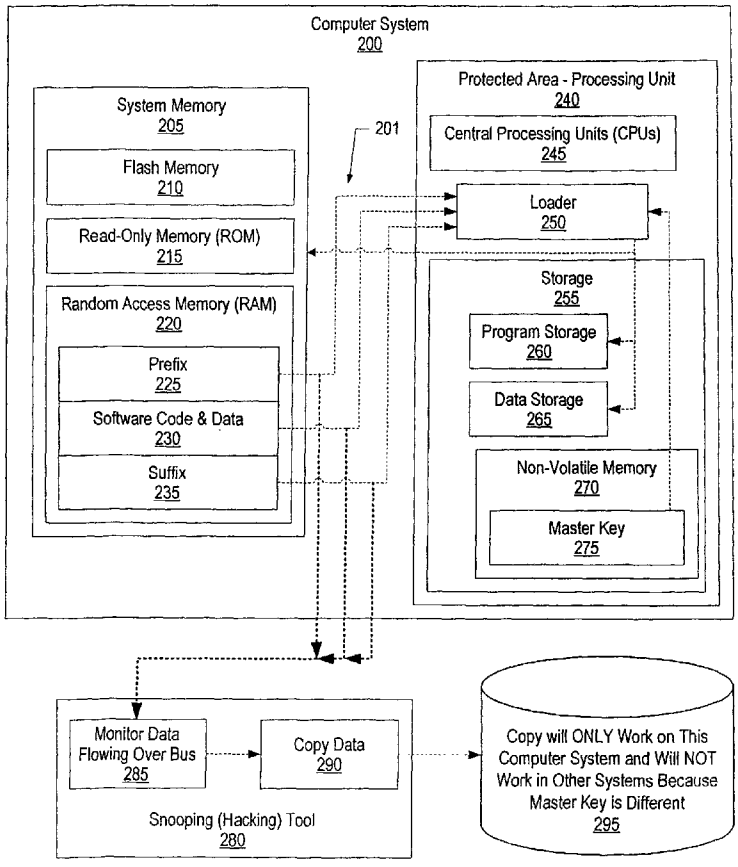
(74) Agent: BLECKER, Ira, D.; International Business Machines Corporation, Dept. 18G, Bldg. 300/482, 2070 Route 52, Hopewell Junction, NY 12533 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING SOFTWARE USING HIDDEN INTERMEDIATE KEYS



(57) Abstract: A processing unit (300) includes a read-only encryption key (394). Loader code image (250) is loaded into system memory (205) from non-volatile storage (270). Loader code image (250) includes a prefix value (225) and a suffix value (235). The prefix value (225) is combined with the master key (394) from the processing unit (300) to create a random value that is the seed for a hashing algorithm. The hashing algorithm uses the seed value with a signature formed from the blocks of code to form a result. During the hashing algorithm, intermediate key values are generated and stored in a memory area inaccessible by the user. The intermediate key values are used by the loader code after the loader has been authenticated and loaded. The loader combines one or more of the intermediate key values with prefix and suffix values that correspond to other software modules to authenticate the software, using a hashing algorithm, and load the software upon authentication.

WO 2005/006109 A3

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
3 March 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.