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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
05 October 2017 (05.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/171987 A8

(51) International Patent Classification:
G06F 21/53 (2013.01) *G06F 21/70* (2013.01)
G06F 21/57 (2013.01)

(21) International Application Number:
PCT/US2017/014494

(22) International Filing Date:
23 January 2017 (23.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/084,564 30 March 2016 (30.03.2016) US

(71) Applicant: **MCAFEE, LLC** [US/US]; 2821 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventors: **KHARE, Atul A.**; 5308 NW 126th Terrace, Portland, Oregon 97229 (US). **KOTARY, Karunakara**; 14682 NW Delia Street, Portland, Oregon 97229 (US). **POORNACHANDRAN, Rajesh**; 15317 NW Twoponds Drive, Portland, Oregon 97229 (US). **ZIMMER, Vincent J.**; 1937 S. 369th Street, Federal Way, Washington 98003 (US). **DAS, Sudeep**; 19400 Sorenson Avenue #138, Cupertino, California 95014 (US).

(74) Agent: **SCHAFER, Richard A.** et al.; Blank Rome LLP, 717 Texas Avenue, Suite 1400, Houston, TX 77002 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: SYSTEM, APPARATUS AND METHOD FOR PERFORMING SECURE MEMORY TRAINING AND MANAGEMENT IN A TRUSTED ENVIRONMENT

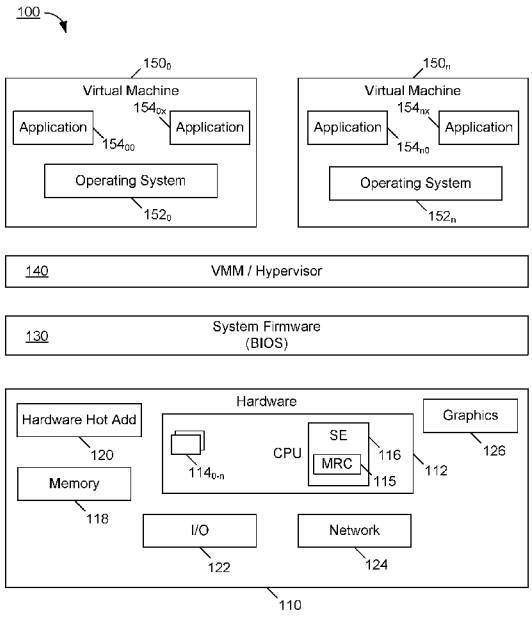

FIG. 1

(57) Abstract: In one embodiment, a system includes: a processor; a security processor to execute in a trusted executed environment (TEE), the security processor to execute memory reference code (MRC) stored in a secure storage of the TEE to train a memory coupled to the processor; and the memory coupled to the processor. Other embodiments are described and claimed.

[Continued on next page]

WO 2017/171987 A8

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

(48) Date of publication of this corrected version:
20 June 2019 (20.06.2019)

(15) Information about Correction:
see Notice of 20 June 2019 (20.06.2019)