

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
17 September 2020 (17.09.2020)



(10) International Publication Number
WO 2020/182420 A1

- (51) **International Patent Classification:**
G06F 21/57 (2013.01) *G06F 9/455* (2018.01)
- (21) **International Application Number:**
PCT/EP2020/054101
- (22) **International Filing Date:**
17 February 2020 (17.02.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
16/296,334 08 March 2019 (08.03.2019) US
- (71) **Applicant:** **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).
- (71) **Applicant (for MG only):** **IBM DEUTSCHLAND GMBH** [DE/DE]; c/o IBM Deutschland Management & Business Support GmbH, Patentwesen und Urheberrecht, IBM Allee 1, 71139 Ehningen (DE).
- (72) **Inventors:** **BUENDGEN, Reinhard**; c/o IBM Deutschland Research & Development GmbH, Schoenaicher Strasse 220, 71032 Boeblingen (DE). **BORNTAEGER, Christian**; c/o IBM Deutschland Research & Development GmbH, Schoenaicher Strasse 220, 71032 Boeblingen (DE).

BRADBURY, Jonathan; c/o IBM Corp., 2455 South Road, Poughkeepsie, New York 12601 (US). **BUSABA, Fadi**; c/o IBM Corp., 2455 South Road, Poughkeepsie, New York 12601 (US). **HELLER, Lisa**; c/o IBM Corp., 2455 South Road, Poughkeepsie, New York 12601 (US). **MIHA-JLOVSKI, Viktor**; c/o IBM Deutschland Research & Development GmbH, Schoenaicher Strasse 220, 71032 Boeblingen (DE).

(74) **Agent:** **LAUX, Felix**; c/o IBM Deutschland Management & Business Support GmbH, Patentwesen und Urheberrecht, IBM Allee 1, 71139 Ehningen (DE).

(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, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

(54) **Title:** INCREMENTAL DECRYPTION AND INTEGRITY VERIFICATION OF A SECURE OPERATING SYSTEM IMAGE

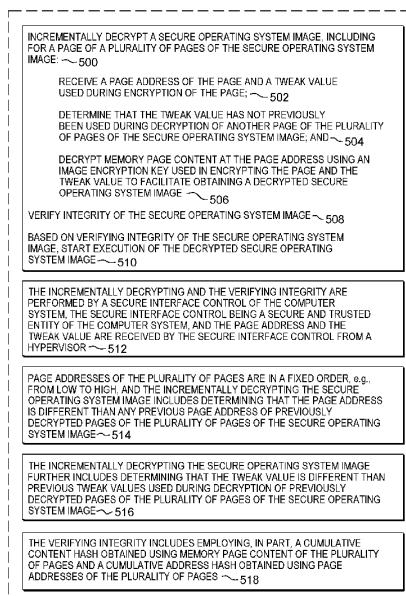


FIG. 5A

(57) **Abstract:** Secure processing within a computing environment is provided by incrementally decrypting a secure operating system image, including receiving, for a page of the secure operating system image, a page address and a tweak value used during encryption of the page. Processing determines that the tweak value has not previously been used during decryption of another page of the secure operating system image, and decrypts memory page content at the page address using an image encryption key and the tweak value to facilitate obtaining a decrypted secure operating system image. Further, integrity of the secure operating system image is verified, and based on verifying integrity of the secure operating system image, execution of the decrypted secure operating system image is started.

WO 2020/182420 A1

[Continued on next page]

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

Published:

- with international search report (Art. 21(3))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE