

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
26 November 2020 (26.11.2020)



(10) International Publication Number
WO 2020/234155 A1

(51) International Patent Classification:

G06F 9/46 (2006.01) G06F 12/14 (2006.01)
G06F 9/54 (2006.01) G06F 21/62 (2013.01)

(21) International Application Number:

PCT/EP2020/063618

(22) International Filing Date:

15 May 2020 (15.05.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/416,229 19 May 2019 (19.05.2019) US

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

(71) Applicant (for MG only): **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).

(72) Inventors: **RAPOPORT, Michael**; IBM ISRAEL, HAI-FA UNIVERSITY CAMPUS, MOUNT CARMEL, 31905 HAIFA (IL). **NIDER, Joel, Kelly**; IBM ISRAEL, IN-TELLECTUAL PROPERTY LAW, HAIFA UNIVERSI-TY, MOUNT CARMEL, 31905 HAIFA (IL). **BOTTOM-**

LEY, James; IBM CORPORATION, 1100 OLIVE WAY, SUITE 1700, SEATTLE, Washington 98101 (US).

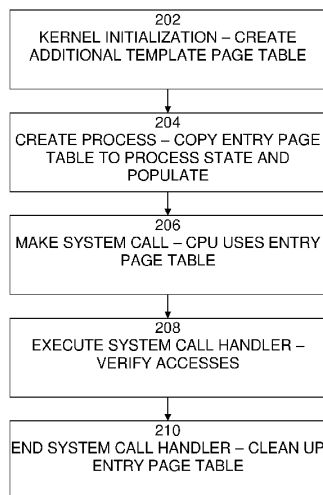
(74) Agent: **SHAW, Anita**; IBM UNITED KINGDOM LIMIT-ED, INTELLECTUAL PROPERTY LAW, HURSLEY PARK, HURSLEY, WINCHESTER Hampshire SO21 2JN (GB).

(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, 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: EXECUTING SYSTEM CALLS IN ISOLATED ADDRESS SPACE IN OPERATING SYSTEM KERNEL

Fig. 2



(57) Abstract: Embodiments of the present systems and methods may provide additional security mechanisms inside an operating system kernel itself by executing system calls in a dedicated address space to reduce the amount of shared resources that are visible to and thus exploitable by a malicious application. For example, in an embodiment, a method implemented in a computer may comprise a processor, memory accessible by the processor, and computer program instructions stored in the memory and executable by the processor, the method may comprise: when a user process makes a system call, switching to kernel mode and using a system call page table for the user process to execute a system call handler, when the system call handler attempts to access unmapped kernel space memory, generating a page fault, and handling the page fault by determining whether the attempted access to unmapped kernel space memory is allowed.

WO 2020/234155 A1

[Continued on next page]

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))*