



(51) International Patent Classification:

G06F 12/10 (2006.01) G06F 21/53 (2013.01)
G06F 9/455 (2006.01) G06F 21/62 (2013.01)
G06F 12/14 (2006.01)

(21) International Application Number:

PCT/RO2014/000006

(22) International Filing Date:

4 February 2014 (04.02.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/774,720 22 February 2013 (22.02.2013) US

(71) Applicant (for all designated States except US): **BITDEFENDER IPR MANAGEMENT LTD** [—/CY]; Kreontos 12, PC 1076, Nicosia (CY).

(72) Inventors; and

(71) Applicants (for US only): **LUȚAS, Andrei-Vlad** [RO/RO]; Bld. Cloșca nr.111, Satu Mare, județ Satu Mare (RO). **LUKACS, Sandor** [RO/RO]; Bld. Cetatea Fetei bl. 8, et. 3, Sat Florești, județ Cluj (RO). **LUȚAS, Dan-Horea** [RO/RO]; Str. Horea nr. 89-95, ap. 29, Cluj-Napoca, județ Cluj (RO).

(74) Agent: **TULUCA, Doina**; Bd. Lacul Tei nr. 56, bl. 19, sc. B, ap. 52, sector 2, RO-020392 Bucuresti (RO).

(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, 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, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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).

Declarations under Rule 4.17:

- 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))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: MEMORY INTROSPECTION ENGINE FOR INTEGRITY PROTECTION OF VIRTUAL MACHINES

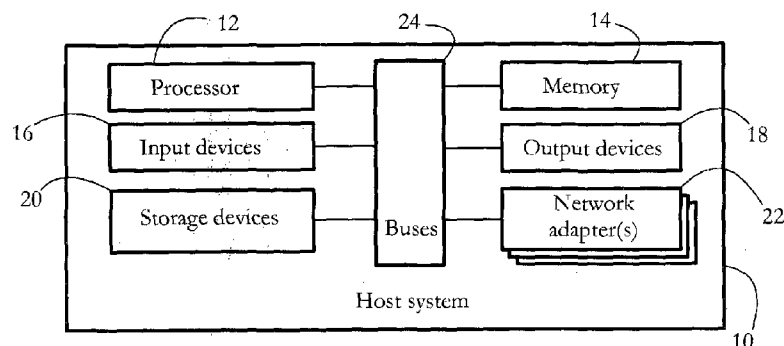


FIG. 1

(57) Abstract: Described systems and methods allow protecting a computer system from malware, such as viruses and rootkits. In some embodiments, a hypervisor configures a hardware virtualization platform hosting a set of operating systems (OS). A memory introspection engine executing at the processor privilege level of the hypervisor dynamically identifies each OS, and uses an protection priming module to change the way memory is allocated to a target software object by the memory allocation function native to the respective OS. In some embodiments, the change affects only target objects requiring malware protection, and comprises enforcing that memory pages containing data of the target object are reserved exclusively for the respective object. The memory introspection engine then write-protects the respective memory pages.