

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 May 2012 (10.05.2012)

PCT

(10) International Publication Number
WO 2012/061663 A2

(51) International Patent Classification:
G06F 21/00 (2006.01) **G06F 11/22** (2006.01)
G06F 11/30 (2006.01)

(21) International Application Number:
PCT/US2011/059244

(22) International Filing Date:
3 November 2011 (03.11.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/409,670 3 November 2010 (03.11.2010) US
61/475,713 15 April 2011 (15.04.2011) US

(71) Applicant (for all designated States except US): **VIRGINIA TECH INTELLECTUAL PROPERTIES, INC.** [US/US]; 2200 Kraft Drive, Suite 1050, Blacksburg, VA 24060 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **REED, Jeffrey, H.** [US/US]; 1105 Eheart St., Blacksburg, VA 24060 (US). **AGUAYO GONZALEZ, Carlos, R.** [MX/US]; 308 Apartment Heights Dr. K-4, Blacksburg, VA 24060 (US).

(74) Agents: **WHITHAM, Michael, E.** et al.; Whitham, Curtis, Christofferson & Cook, P.C., 11491 Sunset Hills Road, Suite 340, Reston, VA 20190 (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, 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, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: USING POWER FINGERPRINTING (PFP) TO MONITOR THE INTEGRITY AND ENHANCE SECURITY OF COMPUTER BASED SYSTEMS

(57) Abstract: Procedures are described for enhancing target system execution integrity determined by power fingerprinting (PFP): by integrating PFP into the detection phase of comprehensive defense-in-depth security; by deploying a network of PFP enabled nodes executing untrusted devices with predefined inputs forcing a specific state sequence and specific software execution; by embedding module identification information into synchronization signaling; by combining signals from different board elements; by using malware signatures to enhance PFP performance; by automatic characterization and signature extraction; by providing secure signature updates; by protecting against side-channel attacks; performing real-time integrity assessment in embedded platform by monitoring their dynamic power consumption and comparing it against signatures from trusted code, including pre-characterizing power consumption of the platform by concentrating on trace sections carrying the most information about the internal execution status; by using PFP from sequence of bit transitions to detect deviations from authorized execution of software in a digital processor.



WO 2012/061663 A2