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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2014 (18.09.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/144857 A3

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

(21) International Application Number:
PCT/US2014/029444

(22) International Filing Date:
14 March 2014 (14.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/792,313 15 March 2013 (15.03.2013) US

(71) Applicant: **POWER FINGERPRINTING INC.** [US/US]; 2200 Kraft Drive, Suite 1200 R, Blacksburg, Virginia 24060 (US).

(72) Inventors: **AGUAYO GONZALEZ, Carlos R.**; 1228 Wild Hawthorn Way, Reston, Virginia 20194 (US). **REED, Jeffrey H.**; 1105 Eheart Street, Blacksburg, Virginia 24060 (US). **CHEN, Steven C.**; 9844 Avenel Farm Drive, Potomac, Maryland 20854 (US).

(74) Agents: **HUTTER, Christopher R.** et al.; Cooley LLP, 1299 Pennsylvania Avenue, NW Suite 700, Washington, District of Columbia 20004-2400 (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, 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))*

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))*

(88) Date of publication of the international search report:
18 December 2014

(54) Title: ENHANCED INTEGRITY ASSESSMENT FOR POWER FINGERPRINTING COMPUTER SYSTEMS

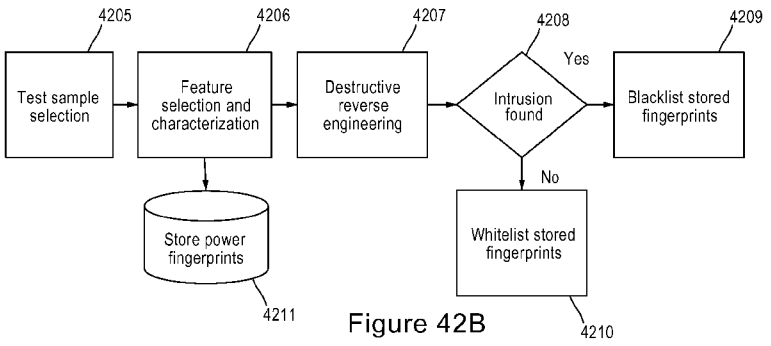

Figure 42B

(57) Abstract: A power fingerprinting system is adopted for assessing integrity of a target computer-based system. In one implementation, the power fingerprinting system may receive, at a first module, side-channel information of a first target component of a system, the first module being collocated with the first target component; obtain a power fingerprint for the first target component based on the side-channel information for the first target component, the power fingerprint for the first target component representing a plurality of execution statuses of the first target component; receive, at a second module, side-channel information of a second target component of the system, the second module being collocated with the second target component, the power fingerprint for the second target component representing a plurality of execution statuses of the second target component; and obtain a power fingerprint for the second target component based on the side-channel information for the second target component.

WO 2014/144857 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US14/29444

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/22 , 11/30 (2014.01)
USPC - 726/23; 714/25, 39; 713/340
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): G06F 11/22, 11/30, 21/50 (2014.01)
USPC Classification(s): 726/23; 714/25, 39; 713/340; CPC Classification(s): G06F 21/56, 21/52, 11/277; H04L 9/003

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C, B, DE-A, DE-T, DE-U, GB-A, FR-A); ProQuest; IEEE/IEEEXplore; Google/Google Scholar; KEYWORDS: power, fingerprint, analysis, status, execution, module

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/061663 A2 (REED, J et al.) 10 May 2012; Paragraphs [079], [0144], [0148], [0149], [0159], [0160], [0163]-[0167], [0182]; Figures 31, 34, 35	1-8
A	US 2013/0063179 A1 (MYERS, B et al.) 14 March 2013; entire document	1-8
A	US 2008/0091975 A1 (KLADKO, K et al.) 17 April 2008; entire document	1-8

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 2014 (09.09.2014)	17 OCT 2014

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US14/29444

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Group I: Claims 1-8; Group II: Claims 9-15; Group III: Claims 16-20

-***-Please see Supplemental Page-***-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-8

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US14/29444

-***-Continued from Box No. III - Observations where unity of invention is lacking-***-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-8 are directed toward a method representing authorized execution statuses of a first target component.
Group II: Claims 9-15 are directed toward a method comprising for an integrity of an untrusted electronic device.
Group III: Claims 16-20 are directed toward a method for preventing access to a device in response to an unauthorized access.

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include a first module being collocated with a first target component; a plurality of authorized execution statuses; a second module being collocated with a second target component; and sending a reporting signal, which are not present in Groups II-III.

The special technical features of Group II include sending a predefined input to an untrusted device, the predefined input being defined by the functionality of the untrusted electronic device; and assessing an integrity of the untrusted electronic device, which are not present in Groups I and III.

The special technical features of Group III include a power fingerprint monitor module configured to receive a signal representing an unauthorized access of a device; a response analysis module operatively coupled to the power fingerprint monitor module, the response analysis module configured to select a response module from a plurality of response modules in response to detection of the unauthorized access; a second response module from a plurality of response modules configured to prevent access to the device; and disabling at least a portion of the device subjected to the unauthorized access, which are not present in Groups I-II.

The common technical feature shared by Groups I-III is a method comprising: receiving side-channel information of an electronic device; and obtaining a power fingerprint for the device based on the side-channel information.

However, this common feature is previously disclosed by US 2007/0180285 A1 (DEMBO). Dembo discloses a method comprising: receiving side-channel information of an electronic device (receiving side-channel attack blocking routines; Abstract and paragraph [0047]); and obtaining a power fingerprint for the device based on the side-channel information (measure a change in power consumption of the IC Chip (device); Abstract and paragraph [0047]).

Since the common technical feature is previously disclosed by the Dembo reference, this common feature is not special and so Groups I-III lack unity.