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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2017 (13.04.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/060778 A3

(51) International Patent Classification:
H04L 12/26 (2006.01) *G06F 21/00* (2013.01)

(21) International Application Number:
PCT/IB2016/001957

(22) International Filing Date:
4 September 2016 (04.09.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/214,969 5 September 2015 (05.09.2015) US

(71) Applicant: **NUDATA SECURITY INC.** [CA/CA]; 999 Canada Place, #550, Vancouver, British Columbia, V6C 3T4 (CA).

(72) Inventors: **BAILEY, Christopher, Everett**; 9393 Waska Street, Langley, British Columbia, V1M 4G3 (CA). **LUKASHUK, Randy**; 875 Englishman River Road, Errington, British Bolumbia, V0R1V0 (CA). **RICHARDSON, Gary, Wayne**; 106-300 Panorama Place, Port Moody, British Columbia, V3H 5H5 (CA).

(74) Agent: **SMART & BIGGAR**; 900-55 Metcalfe Street, Ottawa, Ontario K1P 6L5 (CA).

(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, 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, 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))*

— *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:
20 July 2017

(54) Title: SYSTEMS AND METHODS FOR DETECTING AND SCORING ANOMALIES

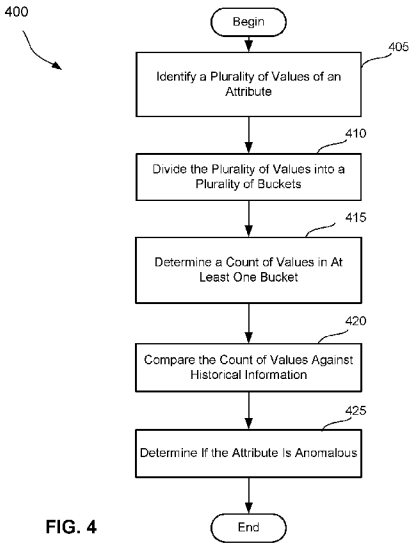

FIG. 4

(57) Abstract: Systems and methods for detecting and scoring anomalies. In some embodiments, a method is provided, comprising acts of: (A) identifying a plurality of values of an attribute, each value of the plurality of values corresponding respectively to a digital interaction of the plurality of digital interactions; (B) dividing the plurality of values into a plurality of buckets; (C) for at least one bucket of the plurality of buckets, determining a count of values from the plurality of values that fall within the at least one bucket; (D) comparing the count of values from the plurality of values that fall within the at least one bucket against historical information regarding the attribute; and (E) determining whether the attribute is anomalous based at least in part on a result of the act (D).

WO 2017/060778 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2016/001957

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 12/26*** (2006.01) , ***G06F 21/00*** (2013.01)

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: H04L 12/26, G06F 21/00

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)

Databases: Questel-Orbit (Fampat), Canadian Patents Database, CIPO Library Discovery Tool, IEEEXplore, Google
Keywords: bucket/category/cluster, divide/split, detect/score anomalies/anomalous, compare historical/past info/data/values, time range, hash, analyze interactions/data, count, record, security, detect web attack, distributed, real-time, compare current values/statistics, threshold, profile, high volume, aggregate, penalty score

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7 523 016 B1 (SURDULESCU et al.) 21 April 2009 (21-04-2009) *abstract; col. 1, line 25 - col. 2, line 22; col. 2, line 55 - col. 12, line 47; col. 14, line 37 - col. 15, line 23; claims 1-20; figs. 1-8*	1-10, 28 and 29
Y	US 2004/0054924 A1 (CHUAH et al.) 18 March 2004 (18-03-2004) *abstract; paragraphs [0002]-[0005], [0019]-[0046], [0056]-[0062]*	1-17, 28 and 29
Y	US 2007/0140131 A1 (MALLOY et al.) 21 June 2007 (21-06-2007) *paragraphs [0043]-[0047]; fig. 5B*	1-17, 28 and 29
Y	KOMPELLA, R.R. et al., "On Scalable Attack Detection in the Network", IEEE/ACM Transactions on Networking, vol. 15, no. 1, pages 14-25, February 2007 (01-02-2007) *abstract; section III. "Detection of TCP Scans and Partial Completion Attacks"; fig. 1*	1-17, 28 and 29

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 31 May 2017 (31-05-2017)	Date of mailing of the international search report 13 June 2017 (13-06-2017)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Daniela Savin (819) 635-6286

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015/0033086 A1 (SASTURKAR et al.) 29 January 2015 (29-01-2015) *abstract; paragraphs [0174]-[0182]; figs. 8, 9A*	11-17
Y	US 2012/0210429 A1 (STUTE) 16 August 2012 (16-08-2012) *paragraphs [0009]-[0011]; claims 1-11*	11-17
A	US 2012/0207046 A1 (DI PIETRO et al.) 16 August 2012 (16-08-2012) *whole document*	
A	US 2014/0229414 A1 (GOLDBERG et al.) 14 August 2014 (14-08-2014) *whole document*	
A	US 8 887 286 B2 (DUPONT et al.) 11 November 2014 (11-11-2014) *whole document*	
A	US 2008/0250497 A1 (MULLARKEY et al.) 9 October 2008 (09-10-2008) *whole document*	
A	YEN T.F. et al., "Traffic Aggregation for Malware Detection", Proceedings of the 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2008, Paris, France, pages 207-227, 10-11 July 2008 (10-07-2008) *whole document*	
A	FUSCO, F. et al., "NET-FLi: On-the-fly Compression, Archiving and Indexing of Streaming Network Traffic", Proceedings of the Proceedings of the Very Large Database (VLDB) Endowment, vol. 3, no. 1-2, pages 1382-1393, 1 September 2010 (01-09-2010) *whole document*	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2016/001957

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the 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. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim 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. ☐ Claim 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:

Claims 1-29 are directed to a plurality of alleged inventions as follows:

Group A: Claims 1-10, 28 and 29;

Group B: Claims 11-17; and

Group C: Claims 18-27.

See the extra sheet for a detailed description of the groups.

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 claim 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 claim Nos.:

Group A: Claims 1-10, 28 and 29; and

Group B: Claims 11-17.

Note: This Authority did not invite payment of additional fees for Group B as claims 11-17 of this group could be searched without effort justifying additional fees.

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.

Continuation of Box III

Claims 1-29 are directed to a plurality of alleged inventions as follows:

Group A: Claims 1-10, 28 and 29 are directed to a method for analyzing a plurality of digital interactions, the method comprising identifying a plurality of values of an attribute, each value corresponding respectively to a digital interaction; dividing the plurality of values into a plurality of buckets; determining a count of values that fall within at least one bucket and comparing the count of values against historical information regarding the attribute; and determining whether the attribute is anomalous based at least in part on a result of the comparison;

Group B: Claims 11-17 are directed to a method for analyzing a digital interaction, the method comprising identifying a plurality of attributes from a profile, for each attribute determining whether the digital interaction matches the profile with respect to the attribute, and determining a penalty score based at least in part on a count of attributes with respect to which the digital interaction matches the profile; and

Group C: Claims 18-27 are directed to a method for analyzing first data collected from a suspicious digital interaction by a security probe of a first type and deploying a security probe of a second type to collect second data from the digital interaction if the digital interaction continues to appear suspicious; or deploying a security probe of a third type to collect third data from the digital interaction if the first data collected from the digital interaction indicates that the digital interaction no longer appears suspicious.

The claims must be limited to one inventive concept as set out in Rule 13 of the PCT.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2016/001957

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US7523016B1	21 April 2009 (21-04-2009)	None	
US2004054924A1	18 March 2004 (18-03-2004)	US8201252B2	12 June 2012 (12-06-2012)
US2007140131A1	21 June 2007 (21-06-2007)	WO2007070711A2	21 June 2007 (21-06-2007)
US2015033086A1	29 January 2015 (29-01-2015)	US9632858B2	25 April 2017 (25-04-2017)
		US2015033084A1	29 January 2015 (29-01-2015)
		US9558056B2	31 January 2017 (31-01-2017)
US2012210429A1	16 August 2012 (16-08-2012)	US8448247B2	21 May 2013 (21-05-2013)
		AT374493T	15 October 2007 (15-10-2007)
		AU2003223379A1	13 October 2003 (13-10-2003)
		DE60316543D1	08 November 2007 (08-11-2007)
		EP1490768A1	29 December 2004 (29-12-2004)
		US2005044406A1	24 February 2005 (24-02-2005)
		US8205259B2	19 June 2012 (19-06-2012)
		WO03083660A1	09 October 2003 (09-10-2003)
US2012207046A1	16 August 2012 (16-08-2012)	US8953472B2	10 February 2015 (10-02-2015)
		EP2474130A1	11 July 2012 (11-07-2012)
		JP2013503584A	31 January 2013 (31-01-2013)
		JP5536891B2	02 July 2014 (02-07-2014)
		WO2011026604A1	10 March 2011 (10-03-2011)
US2014229414A1	14 August 2014 (14-08-2014)	US2014224714A1	14 August 2014 (14-08-2014)
		US2016239368A1	18 August 2016 (18-08-2016)
		WO2014124357A1	14 August 2014 (14-08-2014)
US8887286B2	11 November 2014 (11-11-2014)	US2014096249A1	03 April 2014 (03-04-2014)
		US2012137367A1	31 May 2012 (31-05-2012)
US2008250497A1	09 October 2008 (09-10-2008)	US8601575B2	03 December 2013 (03-12-2013)
		EP2142994A2	13 January 2010 (13-01-2010)
		JP2010531553A	24 September 2010 (24-09-2010)
		WO2008121945A2	09 October 2008 (09-10-2008)