



- (51) International Patent Classification:
H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/US2014/047762
- (22) International Filing Date:
23 July 2014 (23.07.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/857,377 23 July 2013 (23.07.2013) US
- (71) Applicant: **CRYPTEIA NETWORKS S.A.** [GR/GR]; 1 Irakleous Str., 12133 Athens (GR).
- (72) Inventor; and
(71) Applicant (for US only): **GIOKAS, Ioannis** [GR/US]; 10 Jamaicaaway, Boston, Massachusetts 02130 (US).
- (74) Agents: **MCKENNA, Christopher J.** et al.; Foley & Lardner LLP, 3000 K Street N.W., Suite 600, Washington, District of Columbia 20007-5109 (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))
- 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))

(88) Date of publication of the international search report:
26 November 2015

(54) Title: SYSTEMS AND METHODS FOR SELF-TUNING NETWORK INTRUSION DETECTION AND PREVENTION

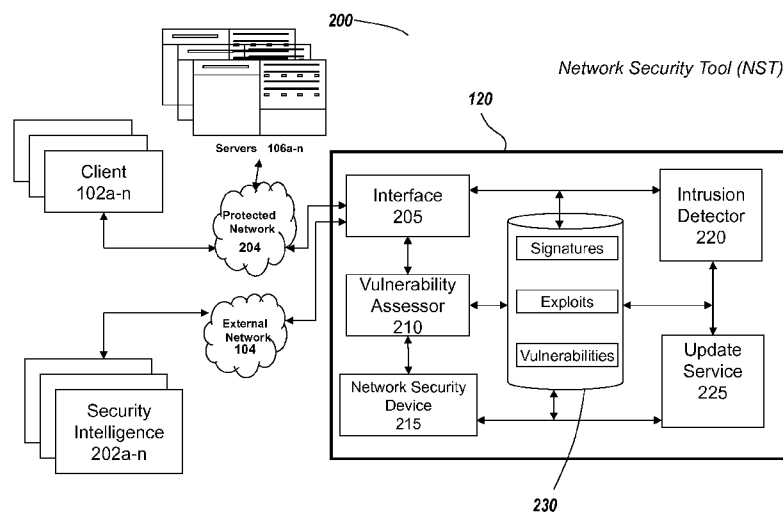


Fig. 2

(57) Abstract: Systems and method of the present disclosure are directed to a network security tool. In some embodiments, the tool identifies a current vulnerability of a private network. The tool can determine a signature of an attack configured to exploit the current vulnerability. The tool can comparing the signature with active and inactive signatures stored in a signature repository. The tool can compare the signatures to identify an inactive signature corresponding to the signature of the attack configured to exploit the current vulnerability. The tool can automatically activate, responsive to the comparison, the identified inactive signature. The tool can use the activated signature to identify an exploit based on data packets received via the private network.

WO 2015/013376 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/047762

<p>A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - H04L 29/06 (2014.01) CPC - H04L 63/20 (2014.09) According to International Patent Classification (IPC) or to both national classification and IPC</p>																										
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols) IPC(8) - H04L 29/06, G06F 21/00, H04L 12/24, G06F 12/14, G06F 1/00, G06F 21/06, G06F 11/30, G06F 15/16, H04L 12/26 (2014.01) USPC - 726/22, 726/23, 726/24</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched CPC - H04L 63/20, G06F 2221/2101, G06F 21/552, H04L 63/1416, G06F 21/55, G06F 21/554, H04L 63/1408, H04L 43/06, H04L 63/1425, H04L 12/2602, H04L 43/00, H04L 63/1433, H04L 43/16 (2014.09)</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Orbit, Google Patents, Google Scholar, Google.</p>																										
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>US 2005/0235360 A1 (PEARSON) 20 October 2005 (20.10.2005), entire document</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>US 2010/0242114 A1 (BUNKER et al) 23 September 2010 (23.09.2010), entire document</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>US 2008/0052774 A1 (CHESLA et al) 28 February 2008 (28.02.2008), entire document</td> <td>6, 16</td> </tr> <tr> <td>A</td> <td>US 2007/0162973 A1 (SCHNEIER et al) 12 July 2007 (12.07.2007), entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2008/0196102 A1 (ROESCH) 14 August 2008 (14.08.2008), entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2006/0156404 A1 (DAY) 13 July 2006 (13.07.2006), entire document</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2010/0100961 A1 (SCHEIDELL) 22 April 2010 (22.04.2010), entire document</td> <td>1-20</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	Y	US 2005/0235360 A1 (PEARSON) 20 October 2005 (20.10.2005), entire document	1-20	Y	US 2010/0242114 A1 (BUNKER et al) 23 September 2010 (23.09.2010), entire document	1-20	Y	US 2008/0052774 A1 (CHESLA et al) 28 February 2008 (28.02.2008), entire document	6, 16	A	US 2007/0162973 A1 (SCHNEIER et al) 12 July 2007 (12.07.2007), entire document	1-20	A	US 2008/0196102 A1 (ROESCH) 14 August 2008 (14.08.2008), entire document	1-20	A	US 2006/0156404 A1 (DAY) 13 July 2006 (13.07.2006), entire document	1-20	A	US 2010/0100961 A1 (SCHEIDELL) 22 April 2010 (22.04.2010), entire document	1-20
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																								
Y	US 2005/0235360 A1 (PEARSON) 20 October 2005 (20.10.2005), entire document	1-20																								
Y	US 2010/0242114 A1 (BUNKER et al) 23 September 2010 (23.09.2010), entire document	1-20																								
Y	US 2008/0052774 A1 (CHESLA et al) 28 February 2008 (28.02.2008), entire document	6, 16																								
A	US 2007/0162973 A1 (SCHNEIER et al) 12 July 2007 (12.07.2007), entire document	1-20																								
A	US 2008/0196102 A1 (ROESCH) 14 August 2008 (14.08.2008), entire document	1-20																								
A	US 2006/0156404 A1 (DAY) 13 July 2006 (13.07.2006), entire document	1-20																								
A	US 2010/0100961 A1 (SCHEIDELL) 22 April 2010 (22.04.2010), entire document	1-20																								
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/></p>																										
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td>“A” document defining the general state of the art which is not considered to be of particular relevance</td> <td>“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</td> </tr> <tr> <td>“E” earlier application or patent but published on or after the international filing date</td> <td>“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</td> </tr> <tr> <td>“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)</td> <td>“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</td> </tr> <tr> <td>“O” document referring to an oral disclosure, use, exhibition or other means</td> <td>“&” document member of the same patent family</td> </tr> <tr> <td>“P” document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table>			“A” document defining the general state of the art which is not considered to be of particular relevance	“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	“E” earlier application or patent but published on or after the international filing date	“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	“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)	“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	“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family	“P” document published prior to the international filing date but later than the priority date claimed															
“A” document defining the general state of the art which is not considered to be of particular relevance	“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																									
“E” earlier application or patent but published on or after the international filing date	“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																									
“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)	“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																									
“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family																									
“P” document published prior to the international filing date but later than the priority date claimed																										
<p>Date of the actual completion of the international search 12 October 2014</p>		<p>Date of mailing of the international search report 14 NOV 2014</p>																								
<p>Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201</p>		<p>Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774</p>																								