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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 April 2005 (07.04.2005)

PCT

(10) International Publication Number
WO 2005/031499 A3

(51) International Patent Classification[7]: H04L 9/00, 9/32, G06F 11/30

(21) International Application Number: PCT/US2004/022743

(22) International Filing Date: 16 July 2004 (16.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/634,117 4 August 2003 (04.08.2003) US
10/605,689 17 October 2003 (17.10.2003) US

(71) Applicant *(for all designated States except US)*: **SBC KNOWLEDGE VENTURES, L.P.** [US/US]; 645 E. Plumb Lane, Reno, Nevada 98502 (US).

(72) Inventors: **DOHERTY, James, M.**; 411 Thunderbay Drive, Georgetown, Texas 78626 (US). **ADAMS, Thomas, Lee**; 13313 Ivywood Cove, Austin, Texas 78729 (US). **MUELLER, Stephen, Mark**; 14912 Thatcher Drive, Austin, Texas 78717 (US).

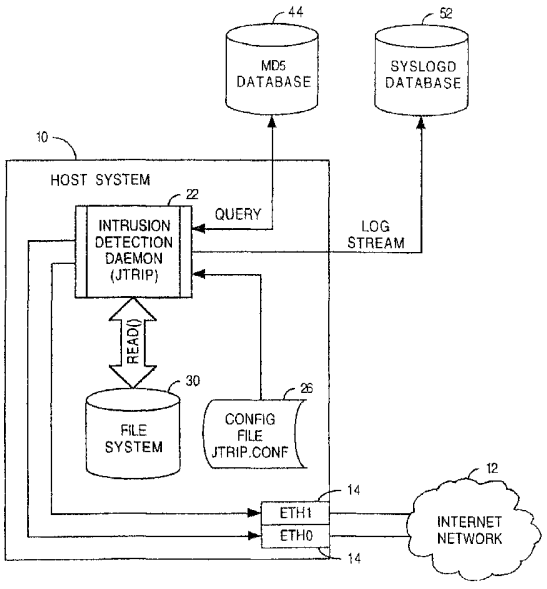
(74) Agent: **TOLER, Jeffrey, G.**; TOLER, LARSON & ABEL, LLP, Suite 265, 5000 Plaza on the Lake, Austin, TX 78746 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: HOST INTRUSION DETECTION AND ISOLATION



(57) Abstract: A system daemon starts through normal system startup procedures and reads its configuration file to determine which data entities (e.g., directories and files) are to be monitored. The monitoring includes a valid MD5 signature, correct permissions, ownership of the file, and an existence of the file. If any modification are made to the data entities, then the system daemon generates an alarm (intended for the administrator of the host) that an intrusion has taken place. Once an intrusion is detected, then the isolating steps or commands are issued in a real-time continuous manner to protect the host system from attack or intrusion.

WO 2005/031499 A3

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
2 June 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/22743

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00, 9/32; G06F 11/30
US CL : 713/176, 187
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)
U.S. : 713/176, 187, 168, 165, 189, 193, 201; 707/1, 9, 10

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,321,338 B1 (PORRAS et al) 20 November 2001 (20.11.2001), entire document.	1, 3-7, 9-15, 17-21, 23-33, 35-40, 42-48, 50, 51 --- 8, 22, 34, 41, 49
Y	SCHNEIER, B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C, 1996. pages 38-39, 429-431, 435-441.	8, 22, 34, 41, 49
A	US 2002/0129264 A1 (ROWLAND et al) 12 September 2002 (12.09.2002), entire document.	1, 3-15, 17-51
A	WO 99/29066 A1 (RVT TECHNOLOGIES, INC.) 10 June 1999 (10.06.1999), entire document.	1, 3-15, 17-51
A	US 2002/0144140 A1 (ELLISON et al) 3 October 2002 (03.10.2002), entire document.	1, 3-15, 17-51
A	US 5,923,884 A (PEYRET et al) 13 July 1999 (13.07.1999), entire document, especially column 9, lines 50-57.	7-10, 14, 21-24, 28-51

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

* 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 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
03 March 2005 (03.03.2005)	01 APR 2005
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. (703) 305-3230	Authorized officer Andrew Caldwell Telephone No. (571) 272-2100

Form PCT/ISA/210 (second sheet) (January 2004)

Continuation of B. FIELDS SEARCHED Item 3:
EAST (USPAT, US-PGPUB, EPO, JPO, DERWENT, IBM_TDB)
search terms: intrusion detection, signature, verification, virus, worm, malware, disable, disconnect, isolate, network, interface

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/22743

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.: 2 and 16
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:
Claims 2 and 16 each recite the limitation "a JTRIP system daemon". However, the acronym JTRIP is not defined in the specification.

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:

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 an additional fee, this Authority did not invite payment of any additional fee.
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.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.