

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
8 August 2002 (08.08.2002)

PCT

(10) International Publication Number
WO 02/062049 A3

(51) International Patent Classification⁷: **H04L 9/00**

(21) International Application Number: PCT/US02/04989

(22) International Filing Date: 31 January 2002 (31.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/265,519 31 January 2001 (31.01.2001) US

(71) Applicants and

(72) Inventors: **DODD, Timothy David** [US/US]; 2126 Brownings Trace, Tucker, GA 30084-4628 (US). **HEINRICH, Nicolas**, [FR/FR]; 23 Avenue Ste. Marguerite, F-05200 Nice (FR).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

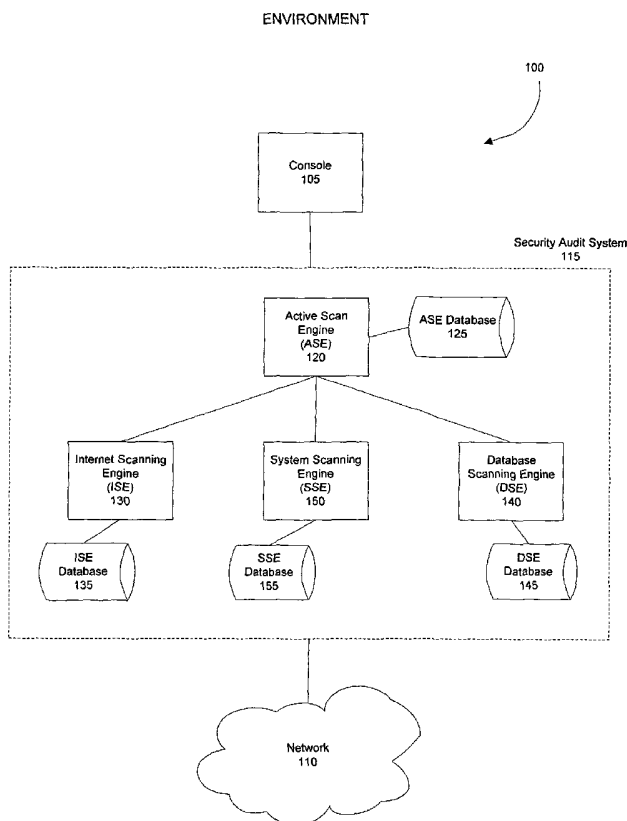
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(74) Agent: **NEUFELD, Robert T.**; King & Spalding, 191 Peachtree Street, Atlanta, GA 30303-1763 (US).

Published:
— with international search report

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR CALCULATING RISK IN ASSOCIATION WITH A SECURITY AUDIT OF A COMPUTER NETWORK



(57) Abstract: Calculating risk based on information collected during a security audit of a computing network (110). The computer network (110) is surveyed to determine the significance of elements in the network (110) and to identify vulnerabilities associated with the elements. Using this information, the security audit system (115) calculates a risk value for each vulnerability. The risk value is a function of the asset value, the probability that the vulnerability will be exploited, and the potential severity of damage to the network (110) if the vulnerability is exploited. The risk value can be adjusted based on the ease with which the vulnerability can be fixed. A network element may have one or more risk values associated with it based on one or more vulnerabilities. The security audit system (115) employs a band calculation method for summing risk values and computing a single security score for the element. The band calculation method can also be used to produce a security score for a group of elements. The band calculation method produces a more accurate score for comparing elements and groups of elements throughout a network (110).



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

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.

(88) Date of publication of the international search report:

21 November 2002

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/04989

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L; 9/00

US CL : 713/200

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. : 713/200-202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
EAST: (network security vulnerability) with (audit\$ scan\$ monitor\$), 11 and (compute\$ calculate\$), 12 and (value\$ score\$)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,006,016 A (FAIGON, ET AL.) 21 December 1999, see column 6, lines 30-65; column 7, line 42 thru column 8, line 65; column 10, lines 14-34; column 12, lines 4-55; column 13 thru column 14; column 16, lines 22-60; column 18, lines 12-65	1-49
X, P	US 6,301,668 B1 (GLEICHAUF, ET AL.) 09 October 2001, see column 4, lines 25-67; column 5, line 52 thru column 6, line 65; column 7, lines 26-59.	1,11,18,29,38,43
A	US 5,734,697 A (JABBARNEZHAD) 31 March 1998, see column 6 thru column 9.	1-49
A	US 5,311,593 A (CARMI) 10 May 1994, see column 4, line 51 thru column 5, line 63; column 7, lines 10-64; column 8, line 48 thru column 9, line 14.	1-49
A	US 6,298,445 B1 (SHOSTACK, ET AL.) 02 October 2001, see column 4, line 33 thru column 5, line 51; column 7, line 11 thru column 8; column 9, line 55 thru column 10, line 40; column 12.	1-49



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

26 July 2002 (26.07.2002)

Date of mailing of the international search report

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)746-7239

Authorized officer

Hayes Gail

Telephone No. (703) 305-3853

19 SEP 2002
Peggy Harrod