

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
4 December 2003 (04.12.2003)

PCT

(10) International Publication Number  
WO 2003/100559 A3

(51) International Patent Classification<sup>7</sup>: G06F 11/30,  
12/14, H04L 9/00, 9/32

(21) International Application Number:  
PCT/US2003/015844

(22) International Filing Date: 20 May 2003 (20.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/381,829 20 May 2002 (20.05.2002) US  
10/161,137 3 June 2002 (03.06.2002) US  
10/161,142 3 June 2002 (03.06.2002) US  
10/161,440 3 June 2002 (03.06.2002) US  
10/161,443 3 June 2002 (03.06.2002) US  
10/160,904 3 June 2002 (03.06.2002) US  
10/360,587 6 February 2003 (06.02.2003) US  
60/464,464 21 April 2003 (21.04.2003) US

(71) Applicant: AIRDEFENSE, INC. [US/US]; 11475 Great Oak Way, Suie 200, Alpharetta, GA 30022 (US).

(72) Inventors: HRASTAR, Scott, E.; 2125 Noblin Ridge Trail, Duluth, GA 30097 (US). TANZELLA, Fred C.; 3235 Roswell Road, NE, #818, Atlanta, GA 30305

(US). LYNN, Micheal Thomas; 2425 Hemingway Lane, Roswell, GA 30075 (US). SALE, Edwin L.; 290 Galesburg Drive, Lawrenceville, GA 30044 (US). HOLLINGSWORTH, Dawn M.; 1466 Monroe Drive, Atlanta, GA 30324 (US).

(74) Agents: KERVEN, David S. et al.; Jones Day, 3500 Sun Trust Plaza, 303 Peachtree Street, Atlanta, GA 30308-3242 (US).

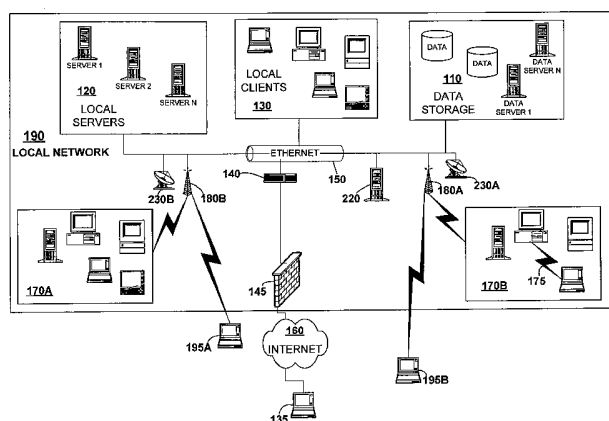
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, 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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:  
— with international search report

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MAKING MANAGING WIRELESS NETWORK ACTIVITY



(57) Abstract: A network security system includes a system data store (110) capable of storing a variety of data associated with a wireless computer network (180A, 180B) and communication transmitted thereon, a communication interface supporting communication over a communication channel and a system processor. Data corresponding communications transmitted over the wireless communication network (180A, 180B) are received. One or more tests are applied to the received data to determine whether a particular communication represents a potential security violation. An alarm may be generated based upon the results of the applied test or tests. In some systems, configuration data associated with an access point on a wireless computer network potentially compromised by an intruder is received. Information contained within and/or derived from the received configuration data is stored. Communication with the intruder is continued by emulating the identification characteristics of the potentially compromised access point. A channel change request is transmitted to the potentially compromised access point and reroute communication between the potentially compromised access point and authorized stations such that communications may continue on a different channel.

WO 2003/100559 A3



---

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

13 May 2004

*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/US03/15844

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(7) : G06F 11/30, 12/14; H04L 9/00, 9/32 US CL : 713/201 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/201, 200; 380/270 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) IEEE, ACM		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,T	US 2003/0135762 A1 (Macaulay) 17 July 2003 (17.07.2003) Figure 2; page 2, paragraphs 19-26; page 3, paragraphs 44, 49-50, 52; Page 5, paragraphs 92-105; page 7, paragraphs 141-149; page 8, paragraphs 161-165.	1-15, 17-26, 58-102, 104-112
A,P	US 2002/0087882 A1 (Schneier et al.) 4 July 2002 (04.07.2002), Page 1, paragraphs 5, 7, 17; page 2, paragraphs 17, 35-37.	1-29, 88-140
A	US 6,188,681 B1 (Vesuna) 13 February 2001 (13.02.2001), column 2, lines 20-45, column 2, line 63 through column 4, line 52	30-44
A,P	US 6,484,029 B2 (Hughes et al.) 19 November 2002 (19.11.2002), column 2, line 28 through column 4, line 35	30-44, 68-87
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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	"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 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		
Date of the actual completion of the international search	Date of mailing of the international search report	
11 February 2004 (11.02.2004)	<b>26 FEB 2004</b>	
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 Gilberto Barrón Telephone No. (703) 305-3900	

## INTERNATIONAL SEARCH REPORT

## C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 2002/0090952 A1 (Cantwell) 11 July 2002 (11.07.2002), figure 2; figure 3; page 1, paragraphs 17-33	68-87
A,T	US 2003/0196115 A1 (Karp) 16 October 2003 (16.10.2003), page 2 paragraphs 25-28; page 3, paragraphs 38-39.	30-44
A,P	US 2002/0178383 A1 (Hrabik et al.) 28 November 2002 (28.11.2002), Page 2, paragraphs 16-24.	1-29, 45-67, 88-115
A,P	US 2003/0084323 A1 (Gales) 1 May 2003 (01.05.2003), Figure 2; page 1, paragraph 5; page 2, paragraphs 14-16; page 3, paragraphs 18, 20-23.	1-29, 88-115
A,P	US 2002/0094777 A1 (Cannon et al.) 18 July 2002 (18.07.2002), all	68-87
A,P	US 2002/0090089 A1 (Branigan et al.) 11 July 2002 (11.07.2002), page 1, paragraph 8; page 3, paragraph 21; page 4, paragraphs 22-24.	1-29, 88-115
A,P	US 2003/0070084 A1 (Satomaa et al.) 10 April 2003 (10.04.2003), page 3, paragraphs 29, 31-35; page 4, paragraphs 40-41.	1-29, 88-115
A,T	US 2003/0123420 A1 (Sherlock) 3 July 2003 (.03.07.2003), page 1, paragraphs 8-9	1-29, 88-115
A,T	US 2003/0105976 A1 (Copeland, III) 5 June 2003 (05.06.2003), all	1-29, 87-115
A,T	US 2003/0217289 A1 (Ammon et al.) 20 November 2003 (20.11.2003)	1-29, 57-115

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/15844

## Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international 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 II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:  
Please See Continuation Sheet

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.

**BOX II. 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 fees must be paid

Group I, claim(s) 1-29, 88-115, drawn to a network security system utilizing testing means to detect violations

Group II, claim(s) 30-44, drawn to a network security system capable of determining access points potentially compromised by an intruder

Group III, claim(s) 45-67, drawn to a network security system capable of applying defensive actions

Group IV, claim(s) 68-87, drawn to a node location system

Group V, claim(s) 116-134, 138-140, drawn to a wireless network sensor

Group VI, claim(s) 135-137, drawn to a wireless network sensor for deriving relevant security information

The special technical feature of the group I invention is the particular claimed detection of violations by performing comparison tests. The special technical feature of the group II invention is determining access points potentially compromised by an intruder. The special technical feature of the group III invention is the application of defensive actions. The special technical feature of the group IV invention is the node location system. The special technical feature of the group V invention is the wireless network sensor used to extract, inspect, and store information. The special technical feature of group VI is the wireless network sensor used for deriving relevant security information. Each of the groups having a particular special technical feature which is not required by any of the other groups