

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
18 May 2007 (18.05.2007)

PCT

(10) International Publication Number
WO 2007/056391 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2006/043381

(22) International Filing Date:
7 November 2006 (07.11.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/735,690 11 November 2005 (11.11.2005) US
11/466,282 22 August 2006 (22.08.2006) US

(71) Applicant (for all designated States except US): **COM-
PUTER ASSOCIATES THINK, INC.** [US/US]; ONE
COMPUTER ASSOCIATES PLAZA, Islandia, NY 11749
(US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SHANKAR, Rohit**
[IN/IN]; 416, VARUNA BLOCK, MYHOME NAVAD-
WEEPA, Madhapur, Hyderabad, Andhra Pradesh 500081
XX (IN). **DESHPANDE, Sumit, B.** [IN/US]; 53 WAL-
NUT STREET, Central Islip, NY 11722 (US). **PORE,**
Ravi, R. [IN/IN]; 7-B, MAYANAGARI, DAPODI, Pune,

Manarashtra 411012 XX (IN). **GUDIPUDI, Srinivas**
[IN/IN]; 7-12/33, RAVINDRANAGAR, Nacharam,
Hyderabad 500076 XX (IN). **PURUSHOTHAMAN, Ab-
hilash, V.** [IN/IN]; D-39, SREEDEVI NAGAR, KARA-
MANA P O TRIVANDRUM, Kerala 695 002 XX (IN).
ZHU, Yidong [CN/US]; 307 RIVERSHIRE COURT, Lin-
colnshire, IL 60069 (US). **SHORT, Theodore** [US/US];
241 WATEREDGE DRIVE NORTH, Jacksonville, FL
32211 (US).

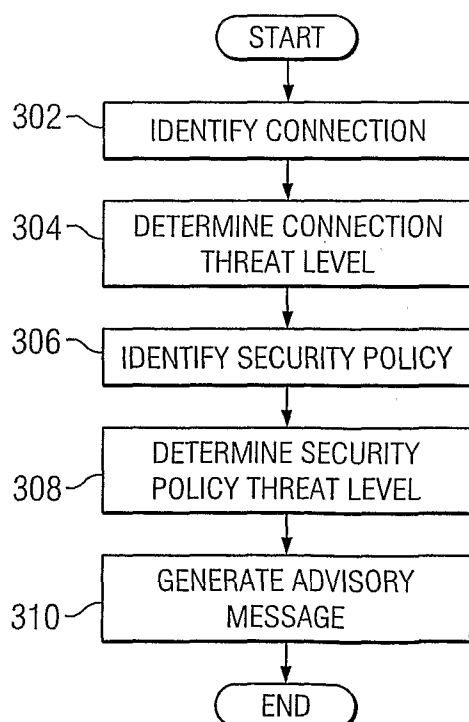
(74) Agent: **PEDERSEN, Luke, K.**; BAKER BOTTS L.L.P.,
2001 ROSS AVENUE, SUITE 600, Dallas, TX 75201
(US).

(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, GT, HN, HR, HU, ID, IL, IN, IS,
JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS,
LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY,
MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS,
RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR GENERATING AN ADVISORY MESSAGE FOR AN ENDPOINT DEVICE



(57) Abstract: According to one embodiment of the invention, a method for generating an advisory message for an endpoint device includes determining a threat level for the endpoint device by identifying a connection type between the endpoint device and the wireless network. The method also includes determining a second threat level for the endpoint device by identifying a security policy of the endpoint device. The method further includes generating an advisory message for the endpoint device based on the threat levels. The advisory message indicates vulnerability of the endpoint device.

WO 2007/056391 A1



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, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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*
- *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.

METHOD AND SYSTEM FOR GENERATING AN ADVISORY MESSAGE FOR
AN ENDPOINT DEVICE

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to wireless networks, and more particularly, to a method and system for generating an advisory message for an endpoint device.

BACKGROUND OF THE INVENTION

Recently, various wireless network technologies have emerged to enable portable endpoint devices (such as laptops, personal digital assistants, cellular telephones, etc.) to communicate both with each other and with wireless networking environments. However, wireless networks are inherently less secure than wired networks, because wired networks may be at least partially located inside a building that can be protected from unauthorized access. Wireless networks do not have the same physical protection and therefore are more vulnerable to attacks. An attacker may use a number of strategies to exploit this vulnerability to pierce network security, corrupt network communications, infiltrate network participants, or compromise routing of network traffic. Accordingly, it is generally desirable to provide an effective security mechanism in wireless networks.

OVERVIEW OF EXAMPLE EMBODIMENTS

According to one embodiment of the invention, a method for generating an advisory message for an endpoint device includes determining a threat level for the endpoint device by identifying a connection type between the endpoint device and a wireless network. The method

also includes determining another threat level for the endpoint device by identifying a security policy of the endpoint device. The method further includes generating an advisory message for the endpoint device based on the threat levels. The advisory message indicates vulnerability of the endpoint device.

Technical advantages of particular embodiments of the present invention include a method and system for generating an advisory message for an endpoint device that alerts a user of the vulnerability of the endpoint device. Thus, a user can take measures to prevent an unauthorized connection from being established.

Another technical advantage of particular embodiments of the present invention includes a method and system for generating an advisory message for an endpoint device that updates the advisory message using a security policy-driven mechanism. Accordingly, changes to the security policy may update the advisory message in approximately real-time, giving a user an updated vulnerability assessment.

Other technical advantages of the present invention will be readily apparent to one skilled in the art from the following figures, descriptions, and claims. Moreover, while specific advantages have been enumerated above, various embodiments may include all, some, or none of the enumerated advantages.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its features and advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates a system that incorporates aspects of the present invention;

FIGURE 2 is a simplified diagram of an example advisory message for an endpoint device; and

FIGURE 3 is a flow diagram for generating an advisory message for an endpoint device.

DESCRIPTION OF EXAMPLE EMBODIMENTS

Embodiments of the present invention and its advantages are best understood by referring to FIGURES 1 through 3 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

FIGURE 1 illustrates one embodiment of a system for generating an advisory message for an endpoint device according to the teachings of the present invention. As shown in FIGURE 1, system 10 generally includes a network 12, one or more wireless access points 14, and one or more endpoint devices 16. System 10 is particularly adapted for alerting a user of endpoint device 16 of the vulnerability of endpoint device 16.

Network 12 may refer to any interconnecting system capable of transmitting audio, video, signals, data, messages, or any combination of the preceding. Network 12 may comprise all or a portion of a public switched telephone network (PSTN), a public or private data network, a local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), a local, regional, or global communication or computer network such as the Internet, a wireline or wireless network, an enterprise intranet, other suitable communication link, or any combination of the preceding.

Network 12 may transmit information in packet flows, in one embodiment. A packet flow includes one or more

packets sent from a source to a destination. A packet may comprise a bundle of data organized in a specific way for transmission, and a frame may comprise the payload of one or more packets organized in a specific way for transmission. A packet-based communication protocol such as Internet Protocol (IP) may be used to communicate the packet flows.

A packet flow may be identified in any suitable manner. As an example, a packet flow may be identified by a packet identifier giving the source and destination of the packet flow. A source may be given by an address such as the IP address, port, or both. Similarly, a destination may be given by an address such as the IP address, port, or both.

Network 12 may utilize protocols and technologies to transmit information. Example protocols and technologies include those described by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.xx standards such as 802.11, 802.16, or WiMAX standards, the International Telecommunications Union (ITU-T) standards, the European Telecommunications Standards Institute (ETSI) standards, Internet Engineering Task Force (IETF) standards, the third generation partnerships project (3GPP) standards, or other standards.

Access point 14 may be any network point suitable to couple a wireless device, such as endpoint device 16, to a network, such as network 12. According to one embodiment of the invention, access point 14 may have a wired connection to network 12. According to another embodiment of the invention, access point 14 may have a wireless connection to network 12. According to another embodiment of the invention, access point 14 may include a receiver or transmitter or both a receiver and a

transmitter. As an example, access point 14 may include an omni-directional antenna operable to communicate with one or more endpoints.

In particular embodiments of the invention, communications between access point 14 and endpoint device 16 are communicated according to one or more secure wireless communication protocols or WLAN protocols, such as portions or all of the Wired Equivalent Privacy (WEP) protocol, the Robust Security Network (RSN) associated with the IEEE 802.11i protocol, the IEEE 802.1x protocol, the Advanced Encryption Standard (AES), the Temporal Key Integrity Protocol (TKIP), Extensible Authentication Protocol over LAN (EAPoL) algorithms or protocols (such as EAP-TTLS, PEAP, or CISCO's LEAP or EAP-FAST protocols, for example), WiFi Protected Access (WPA) protocol, WiFi Protected Access Pre-shared key (WPA-PSK) protocol, WiFi Protected Access Version 2 (WPA2) protocol, or WiFi Protected Access Version 2 Pre-shared key (WPA2-PSK) protocol, for example.

Endpoint device 16 may refer to any suitable device operable to communicate with network 12 through access point 14. In general, a device may include any suitable arrangement of components operable to perform the operations of the device, and may comprise logic. Logic may refer to hardware, software, other logic, or any suitable combination of the preceding. Endpoint device 16 may execute with any of the well-known MS-DOS, PC-DOS, OS-2, MAC-OS, WINDOWS™, UNIX, or other appropriate operating systems, including future operating systems. Endpoint device 16 may include, for example, a personal digital assistant, a computer such as a laptop, a cellular telephone, a mobile handset, or any other device

operable to communicate with network 12 through access point 14.

In various embodiments of the invention, an attacker 18 may attempt to gain access to system 10. Attacker 18 may attempt to gain unauthorized access to pierce network security, corrupt network communications, infiltrate network participants, or compromise routing of network traffic. For example, if access point 14 is not password protected, it may be relatively easy for attacker 18 to gain access to network 12 through access point 14. As another example, attacker 18 may attempt to detect, or "sniff," security information, such as password information, from wireless signals being communicated between endpoint device 16 and access point 14. Attacker 18 may use these, or other similar methods, in order to gain unauthorized connections to endpoint device 16.

According to one embodiment of the invention, a system and method are provided that alert a user of an endpoint device of the vulnerability of the endpoint device. Thus, a user can take measures to prevent an unauthorized connection from being established. This is effected by determining various threat levels at the endpoint device such as a security policy threat level and a connection type threat level and communicating that information to a user. Additional details of example embodiments of the invention are described in greater detail below in conjunction with portions of FIGURE 1, FIGURE 2, and FIGURE 3.

According to the illustrated embodiment of the invention, endpoint device 16 includes a processor 20, a storage device 22, an input device 24, a memory device 26, a communication interface 28, an output device 30, and an advisory manager 40.

Processor 20 may refer to any suitable device operable to execute instructions and manipulate data to perform operations for endpoint device 16. Processor 22 may include, for example, any type of central processing unit (CPU).

Storage device 22 may refer to any suitable device operable for storing data and instructions. Storage device 22 may include, for example, a magnetic disk, flash memory, or optical disk, or other suitable data storage device.

Input device 24 may refer to any suitable device operable to input, select, and/or manipulate various data and information. Input device 24 may include, for example, a keyboard, mouse, graphics tablet, joystick, light pen, microphone, scanner, or other suitable input device.

Memory device 26 may refer to any suitable device operable to store and facilitate retrieval of data, and may comprise Random Access Memory (RAM), Read Only Memory (ROM), a magnetic drive, a disk drive, a Compact Disk (CD) drive, a Digital Video Disk (DVD) drive, removable media storage, any other suitable data storage medium, or a combination of any of the preceding.

Communication interface 28 may refer to any suitable device operable to receive input for endpoint device 16, send output from endpoint device 16, perform suitable processing of the input or output or both, communicate to other devices, or any combination of the preceding. Communication interface 28 may include appropriate hardware (e.g. modem, network interface card, etc.) and software, including protocol conversion and data processing capabilities, to communicate through a LAN, WAN, or other communication system that allows endpoint

device 16 to communicate to other devices. Communication interface 28 may include one or more ports, conversion software, or both.

5 Output device 30 may refer to any suitable device operable for displaying information to a user. Output device 30 may include, for example, a video display, a printer, a plotter, or other suitable output device.

10 Advisory manager 40 may refer to any suitable logic embodied in computer-readable media, and when executed operable to generate an advisory message that indicates vulnerability of endpoint device 16. In the illustrated embodiment of the invention, advisory manager 40 resides in storage device 22. In other embodiments of the invention, advisory manager 40 may reside in memory
15 device 26, or any other suitable device operable to store and facilitate retrieval of data and instructions.

20 According to one embodiment of the invention, various criteria are considered by advisory manager 40 in generating an advisory message. The various criteria may include, but are not limited to, whether encryption is being used at endpoint device 16 and a connection type between endpoint device 16 and access point 14. For example, Table 1 describes such connection types between endpoint device 16 and access point 14, as well as a
25 corresponding threat level that indicates vulnerability of the connection type.

Table 1: Sample Connection Type Data

Connection Type	Connection Threat Level
Open/Share without 802.1x	High
Open/Share with 802.1x	Medium
WPA/WPA-PSK/WPA2/WPA2-PSK	Low

According to another embodiment of the invention, other criteria may also be used such as a security policy enforced at endpoint device 16. A security policy may include a variety of states at endpoint device 16. For example, one state may be whether internet sharing is allowed at endpoint device 16. Internet sharing may include any act of one endpoint device allowing others to connect to the endpoint device using an internet browser. Another state may be whether network file sharing is allowed at endpoint device 16. Network file sharing may include any act of making files on one endpoint device accessible to others on a network. Yet another state may be whether dual homing is allowed at endpoint device 16. Dual homing may include any act of connecting an endpoint device to a network in which there is a primary connection and a secondary connection. Still another state may be whether ad-hoc connections are allowed at endpoint device 16. Ad-hoc connections may include any connection where endpoint devices communicate directly with one another rather than through an access point. For example, Table 2 describes such states, as well as a corresponding security policy based on the variety of states.

Table 2: Sample State Data

State	Security Policy		
	High Security	Medium Security	Low Security
Network File Sharing	Disabled	Enabled	Enabled
Dual Homing	Disabled	Disabled	Enabled
Internet Sharing	Disabled	Disabled	Enabled
Ad-hoc Connectivity	Disabled	Disabled	Enabled

According to one embodiment of the invention, each security policy may have a corresponding threat level. Table 3 lists such security policies, as well as a corresponding threat level based on the security policy.

Table 3: Sample Security Policy Data

Security Policy	Security Policy Threat Level
High Security	Low
Medium Security	Medium
Low Security	High

According to another embodiment of the invention, the threat levels of various factors may be used in determining a an advisory message that indicates vulnerability of endpoint device 16. The various advisory messages for endpoint device 16 may include, but are not limited to, "Critical," "Warning," and "Low." For example, if advisory manager 40 determined a connection threat level of "Medium," and a security policy threat level of "Medium," advisory manager 40 may generate a "Warning" advisory message for endpoint device 16. As another example, if advisory manager 40 determined a connection threat level of "High," and a security policy threat level of "High," advisory manager

40 may generate a "Critical" advisory message for endpoint device 16. As another example, if advisory manager 40 determined a connection threat level of "Low," and a security policy threat level of "Low," advisory manager 40 may generate a "Normal" advisory message for endpoint device 16. For example, Table 4 describes such threat levels using the connection and security policy threat levels.

Table 4: Sample Threat Level Data

Connection Threat Level	Security Policy Threat Level		
	High	Medium	Low
High	Critical	Critical	Critical
Medium	Critical	Warning	Warning
Low	Critical	Warning	Normal

FIGURE 2 is a simplified diagram 200 of an example advisory message 202 for an endpoint device 16. Advisory message 202 reflects a "Critical" level of vulnerability for endpoint device 16. Advisory message 202 may be displayed using, for example, a window in a graphical application, a pop-up window, a dialog box, or any other suitable visual area operable to inform a user of vulnerability so that the user may take measures to secure endpoint device 16, and prevent an unauthorized connection from being established. Additionally, the present disclosure contemplates many types of levels to represent vulnerability of an endpoint device 16. Various embodiments may include some, all, or none of the enumerated levels.

FIGURE 3 is a flow diagram illustrating example acts associated with generating an advisory message for an endpoint device. At step 302, a connection type of an endpoint device is identified by the advisory message

system. In particular embodiments of the invention, the connection type may depend on whether encryption is being used, and the strength of the encryption used at the endpoint device. For example, if encryption is not used
5 at the endpoint device, the connection type may be Open without 802.1x. As another example, if encryption is used at the endpoint device, the connection type may be WPA.

At step 304, a connection threat level is determined
10 by the wireless network managing system. In particular embodiments of the invention, the connection threat level indicates vulnerability of the connection type identified in step 302. The connection threat level may range from "High," to "Medium," to "Low," or other similar
15 measurements. The connection threat level is determined by the security of the connection type. For example, if the connection type is Open without 802.1x, the connection threat level may be "High." As another example, if the connection type is WPA, the connection
20 threat level may be "Low."

At step 306, a security policy of the endpoint device is identified by the advisory message system. In particular embodiments of the invention, the security policy may include a variety of states at an endpoint
25 device. The settings of the various states may indicate a level of protection of the endpoint device. For example, one state may be whether ad-hoc connections are allowed at the endpoint device. If ad-hoc connections are allowed at the endpoint device, the security policy
30 may be a "Low Security" policy, indicating that the endpoint device is not well-protected. Alternatively, if ad-hoc connections are prevented at the endpoint device,

the security policy may be a "High Security" policy, indicating that the endpoint device is highly protected.

At step 308, a security policy threat level is determined by the wireless network managing system. In particular embodiments of the invention, the security policy threat level indicates vulnerability of the security policy identified in step 306. The security policy threat level may range from "High," to "Medium," to "Low," or other similar measurements. For example, if the security policy is a "Low Security" policy, the security policy threat level may be "High." As another example, if the security policy is a "High Security" policy, the security policy threat level may be "Low."

At step 310, an advisory message is generated by the advisory message system. In particular embodiments of the invention, the advisory message is generated based on the connection threat level and the security policy threat level. The advisory message indicates vulnerability of the endpoint device. For example, if the advisory message is "Critical," the endpoint device may be highly vulnerable to attacks. As another example, if the advisory message is "Normal," the endpoint device may be operating at a standard level of vulnerability.

In particular embodiments of the invention, the advisory message may be displayed to a user of the endpoint device so the user can take measures to prevent an unauthorized connection from being established. For example, an advisory message of "Critical" may alert a user that the endpoint device is highly vulnerable to attacks. Thus, the user may change the either the security policy or the connection type of the endpoint device to provide a higher level of protection and avoid attacks.

5

Although the present invention has been described in several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended that the present invention encompass such changes, variations, alterations, transformations, and modifications as falling within the spirit and scope of the appended claims.

WHAT IS CLAIMED IS:

1. A method for generating an advisory message for an endpoint device in a wireless network, comprising:

determining a first threat level for the endpoint device in the wireless network by identifying a connection type between the endpoint device and the wireless network, the connection type selected from the group consisting of:

open with IEEE 802.1x disabled;

open with IEEE 802.1x enabled;

Wi-Fi Protected Access (WPA);

Wi-Fi Protected Access Pre-shared key (WPA-PSK);

Wi-Fi Protected Access 2 (WPA2); and

Wi-Fi Protected Access 2 Pre-shared key (WPA2-PSK); and

determining a second threat level for the endpoint device by identifying a security policy of the endpoint device, the security policy comprising a plurality of states of the endpoint device, the plurality of states comprising a state indicative of whether the endpoint device allows internet sharing, a state indicative of whether the endpoint device allows dual homing, a state indicative of whether the endpoint device allows network file sharing, and a state indicative of whether the endpoint device allows ad-hoc connections; and

based on the first threat level and the second threat level, generating an advisory message for the endpoint device that indicates vulnerability of the endpoint device.

2. A method for generating an advisory message for an endpoint device in a wireless network, comprising:

determining a first threat level for the endpoint device in the wireless network by identifying a connection type between the endpoint device and the wireless network;

determining a second threat level for the endpoint device by identifying a security policy of the endpoint device; and

based on the first threat level and the second threat level, generating an advisory message for the endpoint device that indicates vulnerability of the endpoint device.

3. The method of Claim 2, wherein the connection type comprises a type selected from the group consisting of:

open with IEEE 802.1x disabled;

open with IEEE 802.1x enabled;

Wi-Fi Protected Access (WPA);

Wi-Fi Protected Access Pre-shared key (WPA-PSK);

Wi-Fi Protected Access 2 (WPA2); and

Wi-Fi Protected Access 2 Pre-shared key (WPA2-PSK).

4. The method of Claim 2, wherein the security policy comprises a plurality of states of the endpoint device.

5. The method of Claim 4, wherein the plurality of states comprises a state indicative of whether the endpoint device allows dual homing.

6. The method of Claim 4, wherein the plurality of states comprises a state indicative of whether the endpoint device allows internet sharing.

5 7. The method of Claim 4, wherein the plurality of states comprises a state indicative of whether the endpoint device allows network file sharing.

10 8. The method of Claim 4, wherein the plurality of states comprises a state indicative of whether the endpoint device allows ad-hoc connections.

9. A system for generating an advisory message, comprising:

15 a wireless network, the wireless network comprising one or more access points; and

an endpoint device operable to connect to the wireless network, the endpoint device comprising:

a processor; and

20 a storage device, readable by the endpoint device, embodying a program of instructions executable by the processor to perform steps for generating an advisory message, the steps comprising:

25 determining a first threat level for the endpoint device in the wireless network by identifying a connection type between the endpoint device and the wireless network;

30 determining a second threat level for the endpoint device by identifying a security policy of the endpoint device; and

based on the first threat level and the second threat level, generating an advisory message for the

endpoint device that indicates vulnerability of the endpoint device.

10. The system of Claim 9, wherein the connection
5 type comprises a type selected from the group consisting of:

open with IEEE 802.1x disabled;
open with IEEE 802.1x enabled;
Wi-Fi Protected Access (WPA);
10 Wi-Fi Protected Access Pre-shared key (WPA-PSK);
Wi-Fi Protected Access 2 (WPA2); and
Wi-Fi Protected Access 2 Pre-shared key (WPA2-PSK).

11. The system of Claim 9, wherein the security
15 policy comprises a plurality of states of the endpoint device.

12. The system of Claim 11, wherein the plurality
of states comprises a state indicative of whether the
20 endpoint device allows dual homing.

13. The system of Claim 11, wherein the plurality
of states comprises a state indicative of whether the
endpoint device allows internet sharing.

14. The system of Claim 11, wherein the plurality
of states comprises a state indicative of whether the
endpoint device allows network file sharing.

15. The system of Claim 11, wherein the plurality
of states comprises a state indicative of whether the
30 endpoint device allows ad-hoc connections.

16. Logic encoded in media, the logic being operable to:

determine a first threat level for an endpoint device in a wireless network by identifying a connection type between the endpoint device and the wireless network;

determine a second threat level for the endpoint device by identifying a security policy of the endpoint device; and

based on the first threat level and the second threat level, generate an advisory message for the endpoint device that indicates vulnerability of the endpoint device.

17. The logic of Claim 16, wherein the connection type comprises a type selected from the group consisting of:

open with IEEE 802.1x disabled;

open with IEEE 802.1x enabled;

Wi-Fi Protected Access (WPA);

Wi-Fi Protected Access Pre-shared key (WPA-PSK);

Wi-Fi Protected Access 2 (WPA2); and

Wi-Fi Protected Access 2 Pre-shared key (WPA2-PSK).

18. The logic of Claim 16, wherein the security policy comprises a plurality of states of the endpoint device.

19. The logic of Claim 18, wherein the plurality of states comprises a state indicative of whether the endpoint device allows dual homing.

20. The logic of Claim 18, wherein the plurality of states comprises a state indicative of whether the endpoint device allows internet sharing.

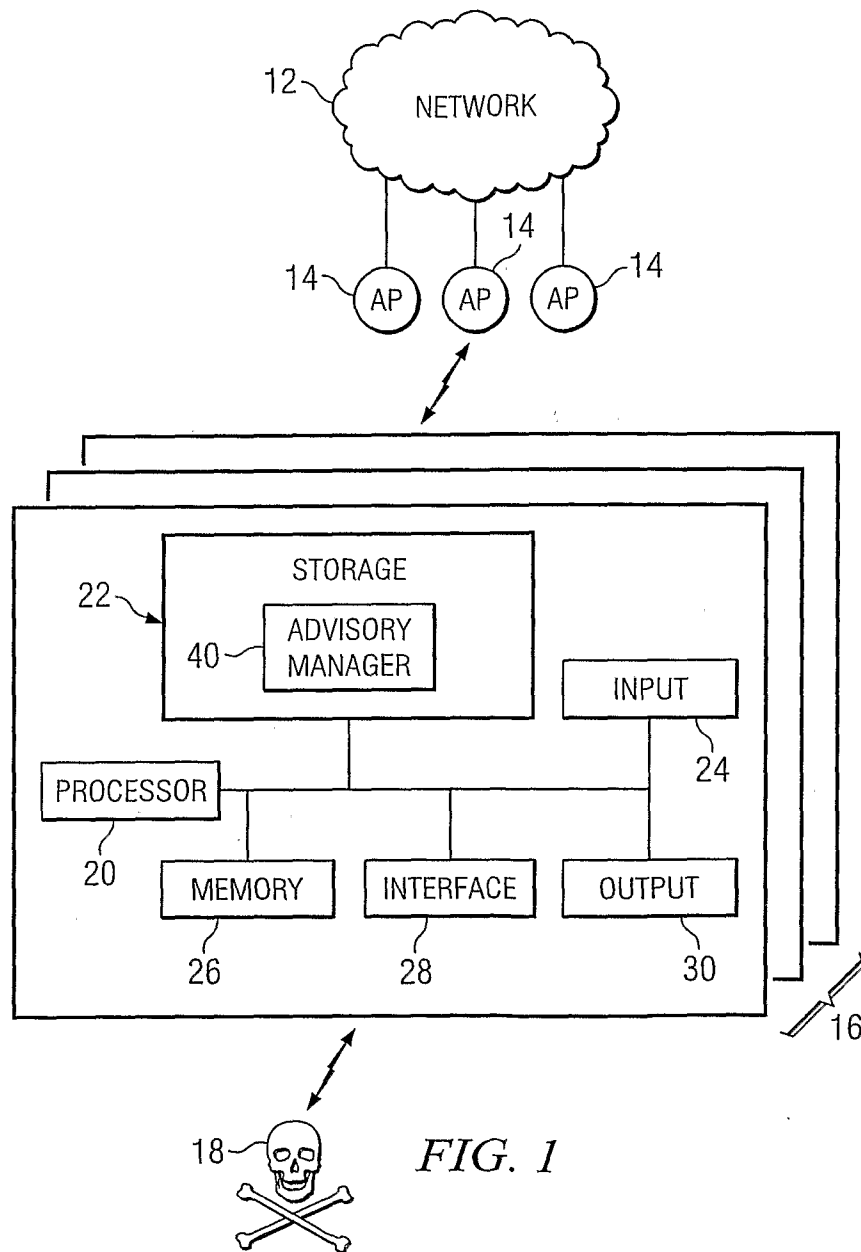
5

21. The logic of Claim 18, wherein the plurality of states comprises a state indicative of whether the endpoint device allows network file sharing.

10

22. The logic of Claim 18, wherein the plurality of states comprises a state indicative of whether the endpoint device allows ad-hoc connections.

1/2



2/2

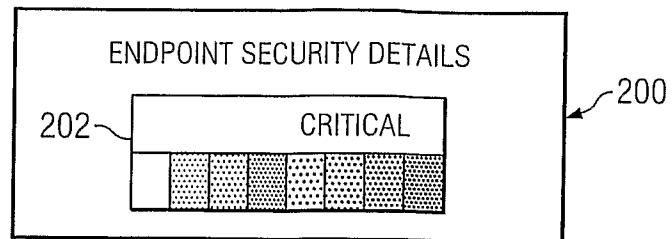


FIG. 2

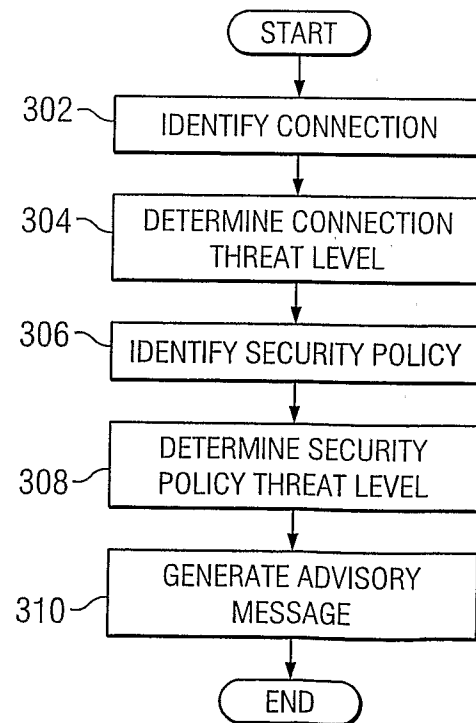


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/043381

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

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)

H04L

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 practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/008001 A1 (WILLIAMS JOHN LESLIE [US] ET AL) 13 January 2005 (2005-01-13) abstract paragraph [0005] - paragraph [0012] paragraph [0060] - paragraph [0063] paragraph [0067] - paragraph [0073] paragraph [0084] paragraph [0125] - paragraph [0135] paragraphs [0145], [0156] -----	1-22
X	US 2004/098610 A1 (HRASTAR SCOTT E [US]) 20 May 2004 (2004-05-20) paragraph [0162] - paragraph [0163] paragraph [0208] paragraph [0215] - paragraph [0216] ----- -/--	2, 9, 16

☒ 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 document but 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

6 March 2007

Date of mailing of the international search report

14/03/2007

Name and mailing address of the ISA/

European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Figiel, Barbara

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/043381

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/010821 A1 (COOPER GEOFFREY [US] ET AL) 13 January 2005 (2005-01-13) abstract paragraph [0035]; claim 1 -----	2,9,16
X	US 2003/056116 A1 (BUNKER NELSON WALDO [US] ET AL) 20 March 2003 (2003-03-20) paragraph [0019] - paragraph [0022] paragraphs [0362], [0367], [0382] -----	2,9,16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2006/043381

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2005008001	A1	13-01-2005	NONE		
US 2004098610	A1	20-05-2004	NONE		
US 2005010821	A1	13-01-2005	NONE		
US 2003056116	A1	20-03-2003	US 2003009696	A1	09-01-2003
			US 2003028803	A1	06-02-2003