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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2005 (06.05.2005)

PCT

(10) International Publication Number
WO 2005/041141 A2

(51) International Patent Classification[7]: G08B

(21) International Application Number:
PCT/US2004/032976

(22) International Filing Date: 6 October 2004 (06.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/685,726 15 October 2003 (15.10.2003) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ROWLAND, Craig, H.** [US/US]; 6908 Dogwood Hollow, Austin, TX 78750 (US).

(74) Agent: **SHOWALTER, Barton, E.**; Baker Botts LLP, 2001 Ross Ave, 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, 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.

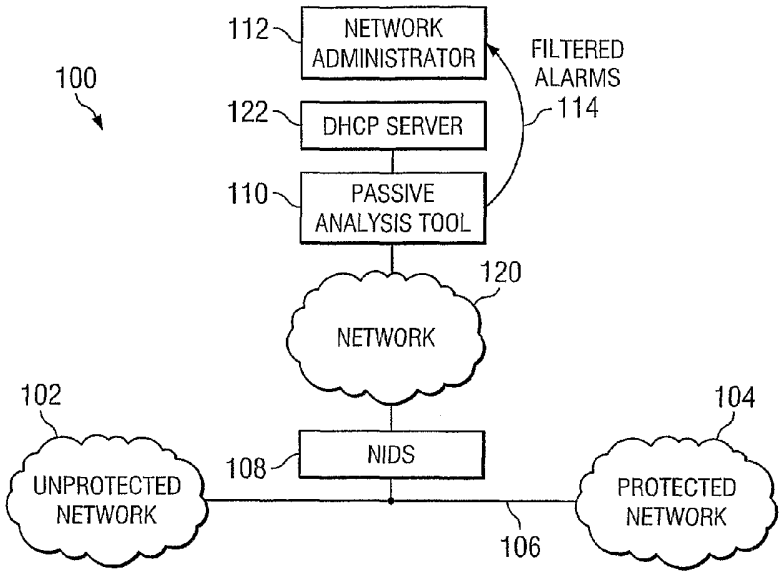
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU,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

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR REDUCING THE FALSE ALARM RATE OF NETWORK INTRUSION DETECTION SYSTEMS



(57) Abstract: According to one embodiment of the invention, a computerized method for reducing the false alarm rate of network intrusion detection systems includes receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host and identifying characteristics of the alarm from the data packets. The characteristics include at least an attack type and an operating system fingerprint of the target host. The method further includes identifying the operating system type from the operating system fingerprint, comparing the attack type to the operating system type, and indicating whether the target host is vulnerable to the attack based on the comparison.

WO 2005/041141 A2

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that report*

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 REDUCING THE FALSE ALARM RATE OF NETWORK INTRUSION DETECTION SYSTEMS

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to intrusion detection and, more particularly, to a method and system for reducing the false alarm rate of network intrusion detection systems using offline passive analysis.

BACKGROUND OF THE INVENTION

Network Intrusion Detection Systems ("NIDS") are typically designed to monitor network activity in real-time to spot suspicious or known malicious activity and to report these findings to the appropriate personnel. By keeping watch on all activity, NIDS have the potential to warn about computer intrusions relatively quickly and allow administrators time to protect or contain intrusions, or allow the NIDS to react and stop the attack automatically. In the security industry, a NIDS may either be a passive observer of the traffic or an active network component that reacts to block attacks in real-time.

False alarms in an NIDS may be reduced by using a technique called passive operating system (OS) analysis. The typical implementation watches network traffic in real-time to discern the operating system types of the hosts by looking at the raw network packets and matching them against a known list. This method requires that the NIDS have direct access to the network traffic to work and enough processing power to handle the additional workload.

SUMMARY OF THE INVENTION

According to one embodiment of the invention, a computerized method for reducing the false alarm rate of network intrusion detection systems includes receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host and identifying characteristics of the alarm from the data packets. The characteristics include at least an attack type and an operating system fingerprint of the target host. The method further includes identifying the operating system type from the operating system fingerprint, comparing the attack type to the operating system type, and indicating whether the target host is vulnerable to the attack based on the comparison.

Some embodiments of the invention provide numerous technical advantages. Other embodiments may realize some, none, or all of these advantages. For example, according to one embodiment, the false alarm rate of network intrusion detection systems ("NIDS") is substantially reduced or eliminated, which leads to a lower requirement of personnel monitoring of NIDS to respond to every alarm. This may be facilitated by a system in which there is no need to access the network stream to determine the operating system type of the target host. The system may reside anywhere in an enterprise and may be used with different types of NIDS, even legacy NIDS sensors that do not support passive OS fingerprinting. Such a system may free up the NIDS so that it runs more efficiently and at a faster speed. In addition, an offline passive analysis system according to one embodiment facilitates the analysis of target hosts that are behind strong or impenetrable firewalls.

Other advantages may be readily ascertainable by those skilled in the art from the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like reference numbers represent like parts, and which:

FIGURE 1 is a schematic diagram illustrating a system for reducing the false alarm rate of network intrusion detection systems by utilizing an offline passive analysis according to one embodiment of the invention;

FIGURE 2 is a block diagram illustrating various functional components a passive analysis tool according to the one embodiment of the invention;

FIGURE 3 is a flowchart illustrating a method for reducing the false alarm rate of network intrusion detection systems according to one embodiment of the invention; and

FIGURE 4 is a flowchart illustrating a method that may be used in conjunction with the method of FIGURE 3 according to one embodiment of the invention.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS OF THE INVENTION

Embodiments of the invention are best understood by referring to FIGURES 1 through 4 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

FIGURE 1 is a schematic diagram illustrating a system 100 for reducing the false alarm rate of a network intrusion detection system ("NIDS") 108 by utilizing an

offline passive analysis tool 110 in accordance with one embodiment of the present invention. In the illustrated embodiment, system 100 includes NIDS 108 coupled to a link 106 that communicatively couples an unprotected network 102 with a protected network 104, a network 120 that couples NIDS 108 with passive analysis tool 110, a dynamic host configuration protocol ("DHCP") server 122 coupled to passive analysis tool 110, and a network administrator 112 that utilizes passive analysis tool 110, as described in more detail below.

Unprotected network 102 may be any suitable network external to protected network 104. An example of unprotected network 102 is the Internet. Protected network 104 may be any suitable network, such as a local area network, wide area network, virtual private network, or any other suitable network desired to be secure from unprotected network 102. Link 106 couples unprotected network 102 to protected network 104 and may be any suitable communications link or channel. In one embodiment, communications link 106 is operable to transmit data in "packets" between unprotected network 102 and protected network 104; however, communications link 106 may be operable to transmit data in other suitable forms.

NIDS 108 may be any suitable network-based intrusion detection system operable to analyze data packets transmitted over communications link 106 in order to detect any potential attacks on protected network 104. NIDS 108 may be any suitable combination of hardware, firmware, and/or software. Generally, network intrusion detection systems include one or more sensors having the ability to monitor any suitable type of network having any suitable data link protocol. In addition, some network intrusion detection systems are passive observers

of network traffic and do not have their own network address.

In a particular embodiment of the invention, sensors associated with NIDS 108 are operable to examine data packets on an IP ("Internet Protocol") network using any suitable protocol, such as TCP ("Transmission Controlled Protocol"), UDP ("User Datagram Protocol"), and ICMP ("Internet Controlled Message Protocol"). Upon detection of a possible attack on protected network 104, NIDS 108 is operable to generate an alarm indicating that an attack on protected network 104 may have occurred. Alarm trigger packets are then transmitted to passive analysis tool 110 over network 120 along with one or more other data packets associated with the alarm for analysis, as described in more detail below.

According to the teachings of one embodiment of the present invention, passive analysis tool 110 is a backend application that receives, via network 120, one or more data packets from NIDS 108 and, using the information associated with the data packets, determines if an attack is real or merely a false alarm. These data packets, which may be any suitable portion of an information stream, include characteristics of the alarm, such as an attack type and an operating system ("OS") fingerprint for the target host so that passive analysis tool 110 may analyze the potential attack without having access to the network stream on link 106.

In this manner, passive analysis tool 110 significantly lowers the false alarm rate for network intrusion detection systems, such as NIDS 108, in the network environment and lowers the requirement of personnel, such as network administrator 112, monitoring these systems to respond to every alarm. In addition, passive analysis tool 110 may reside anywhere in an

enterprise and may be used with different types of NIDS, even legacy NIDS that do not support passive OS fingerprinting. Passive analysis tool 110 may also, in some embodiments, facilitate the analysis of target hosts that are behind strong or impenetrable firewalls.

Details of passive analysis tool 110 are described in greater detail below in conjunction with FIGURES 2 through 4. As illustrated in FIGURE 1, passive analysis tool is coupled to NIDS 108 via network 120, which may be any suitable network, or combination of networks, such as a local area network, wide area network, global network, virtual private network, or any other suitable network.

Network administrator 112 may be any suitable personnel that utilizes passive analysis tool 110 in order to monitor potential attacks on protected network 104 and respond thereto, if appropriate. Network administrator 112, in one embodiment, has passive analysis tool 110 residing on his or her computer in order to receive filtered alarms from passive analysis tool, as denoted by reference numeral 114.

FIGURE 2 is a block diagram illustrating various functional components of passive analysis tool 110 in accordance with one embodiment of the present invention. The present invention contemplates more, less, or different components than those shown in FIGURE 2. In the illustrated embodiment, passive analysis tool 110 includes an alarm input layer 202, an alarm interpretation layer 204, a target cache look-up 206, a passive offline fingerprinting mechanism 208, and an alarm output layer 210. The general functions of each of these components are now described before a more detailed description of the function of passive analysis tool 110 is undertaken in conjunction with FIGURES 3 and 4.

Alarm input layer 202 is generally responsible for receiving the data packets from NIDS 108 and determining if the alarm format is valid. If the alarm format is invalid, then the alarm is disregarded. If the alarm format is valid, then the alarm is sent to alarm interpretation layer 204. Alarm input layer 202 is preferably designed to be NIDS vendor independent so that it may accept alarms from multiple NIDS sources concurrently with no modification. Alarm input layer 202, in one embodiment, may also accept alarms from legacy NIDS that do not support passive OS fingerprinting.

Generally, alarm interpretation layer 204 receives the data packets from alarm input layer 202 and performs an analysis on the alarm. In one embodiment, alarm interpretation layer 204 determines whether the alarm is from a supported NIDS vendor. If the alarm is not from a supported NIDS vendor, an alert is generated and the alarm is disregarded. If the alarm is from a supported NIDS vendor, then alarm interpretation layer 204 is responsible for identifying the attack type, relevant operating system type being attacked (e.g., Microsoft Windows, Sun Solaris, Linux, UNIX, etc.), the source address, target network address, the alarm severity, the alarm description, and any other suitable parameters associated with the alarm. Some of this information is used by passive analysis 110 to test if the alarm is real or false, as described in more detail below in conjunction with FIGURES 3 and 4.

Target cache look-up 206 indicates that a look-up is performed by passive analysis tool 110 in order to determine if the target host has already been checked for the particular attack indicated by the alarm. The look-

up may be performed in any suitable storage location, such as a local state table or database.

Passive offline fingerprinting mechanism 208 performs a passive analysis of the target host by identifying, from the received data packets, the operating system fingerprint of the target host, which includes the operating system type, and comparing the operating system type to the attack type. An advantage of this type of OS fingerprinting is that it requires no access to the network stream. Passive offline fingerprinting mechanism 208 may store this information in a suitable storage location for later retrieval and use.

Alarm output layer 210 is responsible for taking the analyzed data from passive analysis tool 110 and either escalating or de-escalating the alarm. In other words, alarm output layer 210 functions to report a valid alarm; i.e., that a particular target host is vulnerable to an attack. A valid alarm may be reported in any suitable manner, such as a graphical user interface, a log file, storing in a database, or any other suitable output. In one embodiment, a valid alarm is automatically reported to network administrator 112 via any suitable method.

Additional description of the details of the functions of passive analysis tool 110, according to one embodiment of the invention, are described below in conjunction with FIGURES 3 and 4.

FIGURE 3 is a flow chart illustrating an example method for reducing the false alarm rate of network intrusion detection systems according to one embodiment of the present invention. The example method begins at step 300 where one or more data packets associated with an alarm is received from NIDS 108 by passive analysis tool 110. As discussed above, these data packets may be

any suitable portion of an information stream and may be communicated to passive analysis tool 110 via network 120 or other suitable communication means. From the data packets, passive analysis tool 110 identifies the attack type, as denoted by step 302, and an operating system fingerprint of the target host, as denoted by step 304. The operating system type of the target host may be identified by passive analysis tool 110 from the OS fingerprint, as denoted by step 306.

The attack type and the operating system type of the target host are compared at step 308 by passive analysis tool 110. At decisional step 310, it is determined whether the operating system type of the target host matches the attack type. If there is a match, then a confirmed alarm is reported by step 312. In one embodiment, the confirmed alarm is automatically reported to network administrator 112 in any suitable manner. If there is no match, then a false alarm is indicated, as denoted by step 314. For example, if the attack type is for a Windows system and the operating system fingerprint shows a Windows host, then the alarm is confirmed. However, if the attack type is for a Windows system and the operating system fingerprint shows a UNIX host, then this indicates a false alarm. This ends the example method outlined in FIGURE 3.

Although the method outlined in FIGURE 3 is described with reference to passive analysis tool 110 comparing an operating system type with an attack type, other suitable characteristics of the operating system may be compared to relevant characteristics of the attack type in order to determine if the alarm is real or false. This depends on the type of information passed from NIDS 108 via the data packets.

Thus, passive analysis tool 110 is intelligent filtering technology that screens out potential false alarms while not requiring access to protected network 104. Alarm inputs are received from a deployed NIDS, such as NIDS 108, and analyzed to determine if an attack is real or a false alarm.

FIGURE 4 is a flowchart illustrating an example method that may be used in conjunction with the example method outlined in FIGURE 3 in accordance with an embodiment of the present invention. The example method in FIGURE 4 begins at step 400 where DHCP server 122 (FIGURE 1) is monitored by passive analysis tool 110. The present invention contemplates any suitable dynamic configuration protocol server being monitored by passive analysis tool 110. At step 402, lease activity is detected by passive analysis tool 110. At decisional step 404 it is determined whether a lease issue is detected or a lease expire is detected.

If a lease expire is detected by passive analysis tool 110, then the system cache is accessed, as denoted by step 406. At decisional step 408, it is determined whether the target address associated with the lease expire is found in the system cache. If the target address is found in the system cache, then the entry is purged, at step 410, from the system cache. Passive analysis tool 110 then continues to monitor the DHCP server. If a target address is not found in the system cache, then the lease expire is disregarded, as denoted by step 412. Passive analysis tool 110 continues to monitor the DHCP server.

Referring back to decisional step 404, if a lease issue has been detected, then the system cache is accessed, as denoted by step 414. At decisional step 416, it is determined whether the target address

associated with the lease issue is found in the system cache. If the target address is found, then the entry is purged, at step 418. If the target address is not found in the system cache, then passive analysis tool 110 continues to monitor the DHCP server.

The method outlined in FIGURE 4 address the dynamic addition, subtraction, or modifying of hosts in protected network 104 in order that prior knowledge of protected network 104 is not required. This saves considerable time and money and is more accurate than prior systems in which prior knowledge of the network is required. Passive analysis tool 110 may more accurately keep track of changes regarding the target hosts of protected network 104.

Although the present invention is described with 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 they fall within the scope of the appended claims.

WHAT IS CLAIMED IS:

1. A computerized method for reducing the false alarm rate of network intrusion detection systems, comprising:

receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host;

identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

identifying the operating system type from the operating system fingerprint;

comparing the attack type to the operating system type; and

indicating whether the target host is vulnerable to the attack based on the comparison.

2. The computerized method of Claim 1, further comprising storing the operating system fingerprint of the target host in a storage location for a time period.

3. The computerized method of Claim 1, further comprising:

monitoring a dynamic configuration protocol server;

detecting that a lease issue has occurred for a new target host;

accessing a storage location;

determining whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then purging the existing operating system fingerprint for the new target host from the storage location.

4. The computerized method of Claim 1, further comprising:

monitoring a dynamic configuration protocol server;

detecting that a lease expire has occurred for an existing target host;

accessing a storage location;

determining whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then disregarding the lease expire; and

if the operating system fingerprint for the existing target host does exist, then purging the existing operating system fingerprint for the existing target host from the storage location.

5. The computerized method of Claim 1, further comprising:

after receiving the data packets, determining whether a format for the alarm is valid; and

if the format is not valid, then disregarding the alarm; otherwise

if the format is valid, then continuing the computerized method with the identifying characteristics step.

6. The computerized method of Claim 1, further comprising automatically alerting a network administrator if the target host is vulnerable to the attack.

7. A system for reducing the false alarm rate of network intrusion detection systems, comprising:

a network intrusion detection system operable to transmit one or more data packets associated with an alarm indicative of a potential attack on a target host;

a software program embodied in a computer readable medium, the software program, when executed by a processor, operable to:

receive the one or more data packets;

identify characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

identify the operating system type from the operating system fingerprint;

compare the attack type to the operating system type; and

indicate whether the target host is vulnerable to the attack based on the comparison.

8. The system of Claim 7, further comprising a storage location operable to store the operating system fingerprint of the target host for a time period.

9. The system of Claim 7, wherein the software program is further operable to:

monitor a dynamic configuration protocol server;

detect that a lease issue has occurred for a new target host;

access a storage location;

determine whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then the software program is

further operable to purge the existing operating system fingerprint for the new target host from the storage location.

10. The system of Claim 7, wherein the software program is further operable to:

monitor a dynamic configuration protocol server;

detect that a lease expire has occurred for an existing target host;

access a storage location;

determine whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then disregard the lease expire; and

if the operating system fingerprint for the existing target host does exist, then purge the existing operating system fingerprint for the existing target host from the storage location.

11. The system of Claim 7, wherein the software program is further operable to automatically alert a network administrator of the attack if the target host is vulnerable to the attack.

12. The system of Claim 7, wherein the software program has no knowledge of the protected network architecture.

13. The system of Claim 7, wherein the software program has no access to the protected network.

14. The system of Claim 7, wherein the NIDS is vendor independent.

15. The system of Claim 7, wherein the NIDS does not support passive operating system fingerprinting.

16. A system for reducing the false alarm rate of network intrusion detection systems, comprising:

means for receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host;

means for identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

means for identifying the operating system type from the operating system fingerprint;

means for comparing the attack type to the operating system type; and

means for indicating whether the target host is vulnerable to the attack based on the comparison.

17. The system of Claim 16, further comprising means for storing the operating system fingerprint of the target host for a time period.

18. The system of Claim 16, further comprising:

means for monitoring a dynamic configuration protocol server;

means for detecting that a lease issue has occurred for a new target host;

means for accessing a storage location;

means for determining whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then means for purging the existing operating system fingerprint for the new target host from the storage location.

19. The system of Claim 16, further comprising:

means for monitoring a dynamic configuration protocol server;

means for detecting that a lease expire has occurred for an existing target host;

means for accessing a storage location;

means for determining whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then means for disregarding the lease expire; and

if the operating system fingerprint for the existing target host does exist, then means for purging the existing operating system fingerprint for the existing target host from the storage location.

20. The system of Claim 16, further comprising:

after receiving the data packets, means for determining whether a format for the alarm is valid; and

if the format is not valid, then means for disregarding the alarm.

21. The system of Claim 16, further comprising means for automatically alerting a network administrator if the target host is vulnerable to the attack.

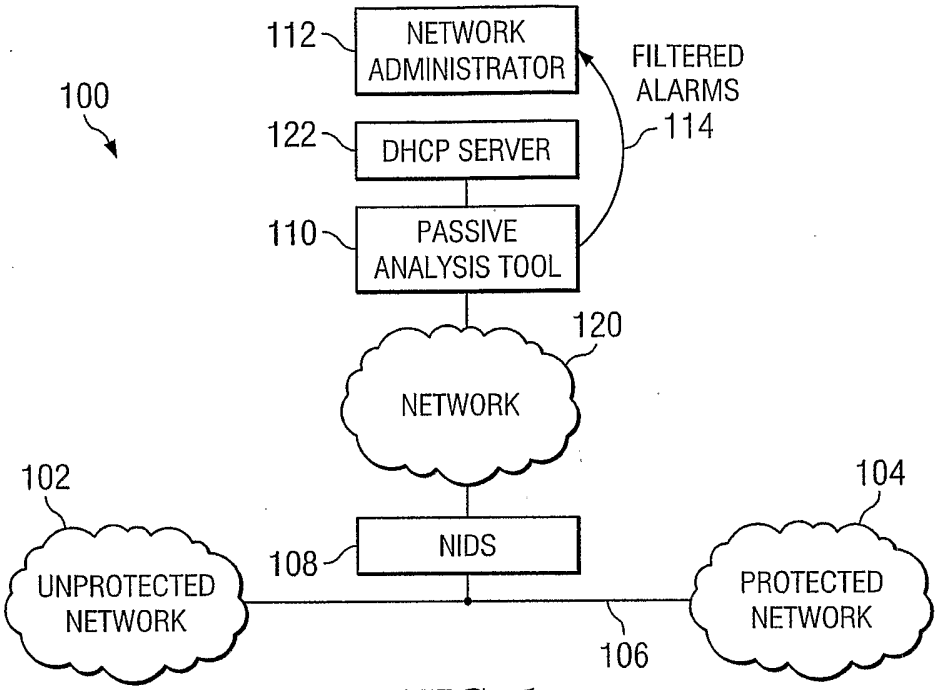

100
112
NETWORK ADMINISTRATOR
FILTERED ALARMS
114
122
DHCP SERVER
110
PASSIVE ANALYSIS TOOL
120
NETWORK
102
104
NIDS
108
UNPROTECTED NETWORK
PROTECTED NETWORK
106

FIG. 1

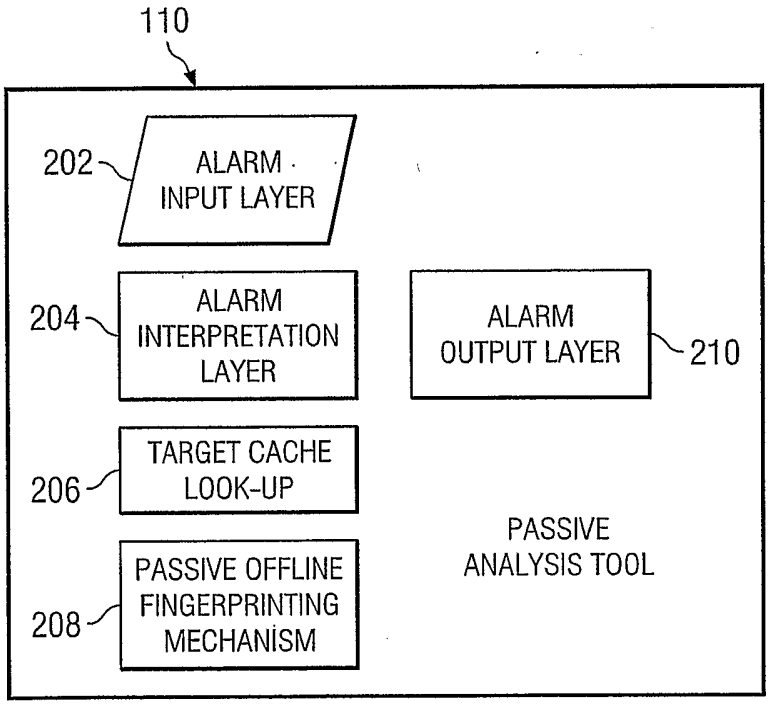

110
202
ALARM INPUT LAYER
204
ALARM INTERPRETATION LAYER
ALARM OUTPUT LAYER
210
206
TARGET CACHE LOOK-UP
PASSIVE ANALYSIS TOOL
208
PASSIVE OFFLINE FINGERPRINTING MECHANISM

FIG. 2

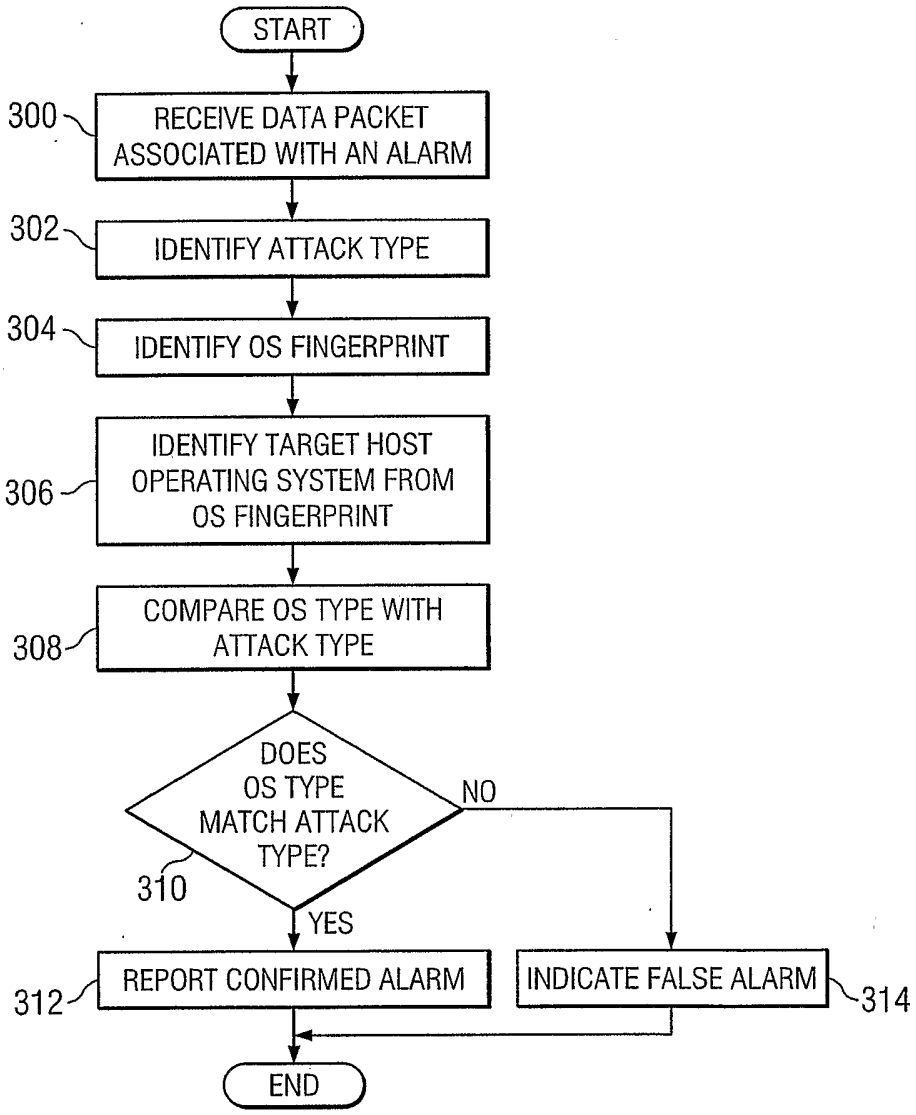

START
300
RECEIVE DATA PACKET ASSOCIATED WITH AN ALARM
302
IDENTIFY ATTACK TYPE
304
IDENTIFY OS FINGERPRINT
306
IDENTIFY TARGET HOST OPERATING SYSTEM FROM OS FINGERPRINT
308
COMPARE OS TYPE WITH ATTACK TYPE
DOES OS TYPE MATCH ATTACK TYPE?
310
NO
YES
312
REPORT CONFIRMED ALARM
INDICATE FALSE ALARM
314
END

FIG. 3

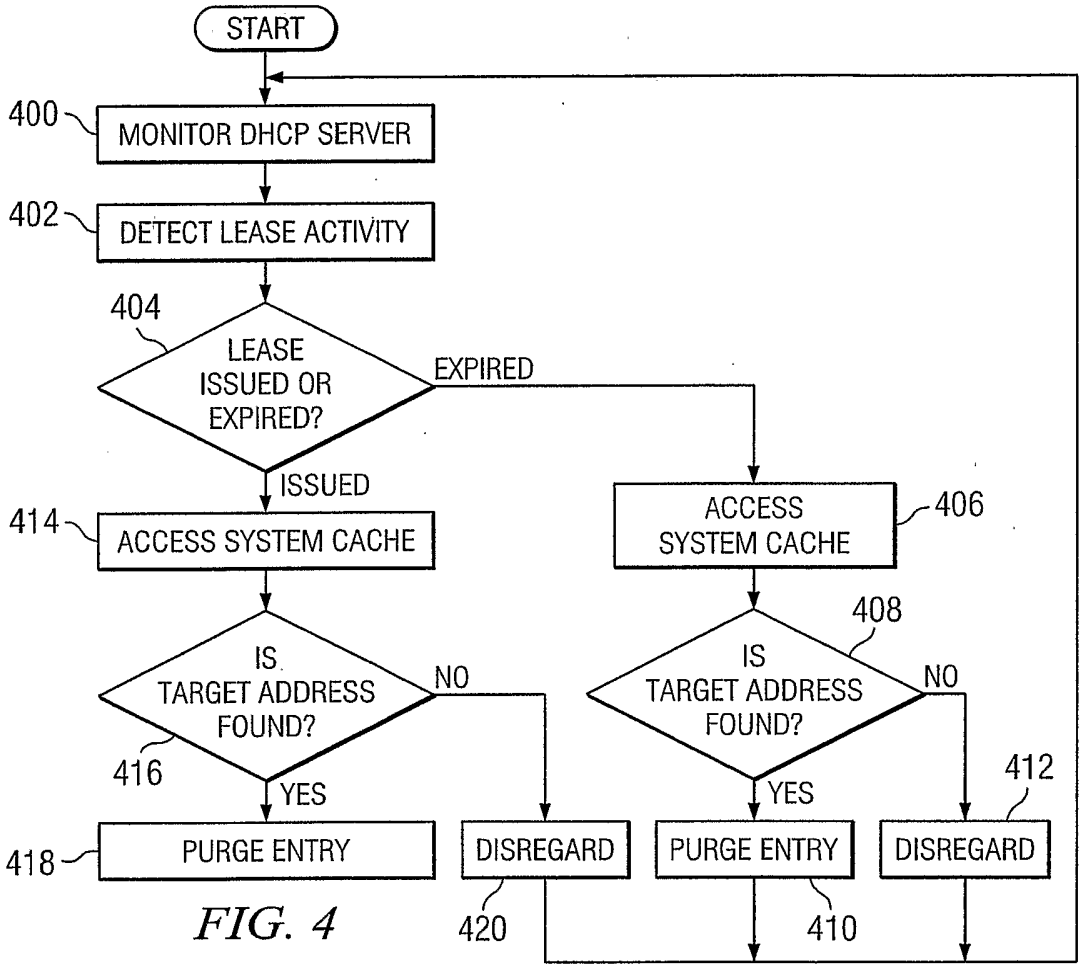

START
400
MONITOR DHCP SERVER
402
DETECT LEASE ACTIVITY
404
LEASE ISSUED OR EXPIRED?
EXPIRED
ISSUED
414
ACCESS SYSTEM CACHE
406
ACCESS SYSTEM CACHE
408
IS TARGET ADDRESS FOUND?
NO
YES
416
IS TARGET ADDRESS FOUND?
NO
YES
412
418
PURGE ENTRY
DISREGARD
PURGE ENTRY
DISREGARD
420
410

FIG. 4