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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 March 2006 (30.03.2006)

PCT

(10) International Publication Number
WO 2006/034201 A2

(51) International Patent Classification: Not classified

(21) International Application Number: PCT/US2005/033495

(22) International Filing Date: 19 September 2005 (19.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/610,764 17 September 2004 (17.09.2004) US

(71) Applicant *(for all designated States except US)*: **HOB-NOB, INC.** [US/US]; 5850 Ellsworth Avenue, Suite 300, Pittsburgh, PA 15232 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HALL, Aron** [US/US]; 710 Ivy Street, Pittsburgh, PA 15232 (US). **BERNARD, Andrew, B.** [US/US]; 830 Savannah Avenue, Pittsburgh, PA 15221 (US).

(74) Agents: **LAZZARA, Michael, D.** et al.; Kirkpatrick & Lockhart Nicholson Graham LLP, Henry W. Oliver Building, 535 Smithfield Street, Pittsburgh, PA 15222-2312 (US).

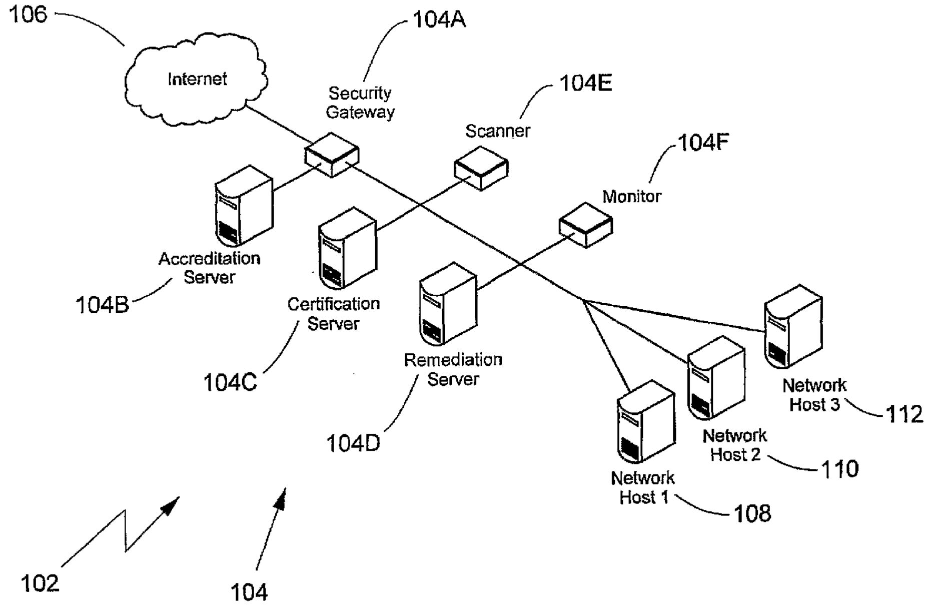
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, 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)) for the following designations 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,*

[Continued on next page]

(54) **Title:** QUARANTINE NETWORK



(57) **Abstract:** Various network security systems and methods are provided. The system can apply security policies based on user and/or system responses to security probes generated by the system. The system can automatically apply prophylactic protection to an end user network host to prevent the host from being exploited by various types of attacks or malicious network traffic. The system may also be configured to attempt to exploit unpatched security vulnerabilities on a target system or network. If the exploitation attempt is successful, network access to the vulnerable system can be restricted until the vulnerabilities are corrected.

IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *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.

QUARANTINE NETWORK

INVENTORS

Aron B. Hall

Andrew B. Bernard

CROSS-REFERENCE TO RELATED APPLICATION / PRIORITY CLAIM

The present application claims the priority of United States Provisional Patent Application Serial No. 60/610,764, which was filed on September 17, 2004, and which is hereby incorporated by reference in its entirety into the present application.

FIELD OF THE INVENTION

The present invention generally relates to providing security for computer networks and computer systems.

BRIEF DESCRIPTION OF THE FIGURES

The utility of the embodiments of the present invention will be readily appreciated and understood from consideration of the following description of the embodiments of the invention when viewed in connection with the accompanying drawings.

Figure 1 schematically depicts various aspects of system and method embodiments of the present invention;

Figure 2 schematically illustrates various aspects of system and method embodiments of the present invention;

Figure 3 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention;

Figure 4 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention;

Figure 5 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention;

Figure 6 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention;

Figure 7 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention; and,

Figure 8 schematically illustrates an example of a network security system provided in accordance with various embodiments of the present invention.

DESCRIPTION

As applied herein, a computer network (or "network") is a means by which a computer can communicate with another computer or some other electronic device.

A network host is a device that is capable of communicating on a computer network.

A security vulnerability is a flaw in the hardware or the software of a computer that can be exploited by an individual or program to cause the computer to malfunction or otherwise behave contrary to the intentions of its owner or operator.

A network security vulnerability is a security vulnerability that can be exploited by communicating with the host over a network.

A security breach is a security vulnerability that has been exploited.

An inline security gateway is a network router, switch, or hub in which communication between two or more network hosts is restricted based on a security policy set by an operator or another network security device. The security gateway might control communications between two or more networks, or it might control communications between individual hosts on one or more networks.

Prohibited communication is any attempt by two or more hosts to communicate, when that attempt is prevented by an inline security gateway based on its security policy.

A security vulnerability scanner is a network host that actively communicates with one or more target network hosts with the purpose of detecting one or more network security vulnerabilities on the target host(s).

A security breach scanner is a network host that actively communicates with one or more target network hosts with the purpose of detecting one or more security breaches on the target host(s).

A security vulnerability monitor is a network host that passively monitors the network communication of one or more network hosts with the purpose of detecting one or more security vulnerabilities on the target host(s).

A security breach monitor is a network host that passively monitors the network communication of one or more network hosts with the purpose of detecting one or more security breaches on the target host(s).

An indirect security vulnerability scanner is a security vulnerability scanner in which some communication with the target host takes place indirectly through one or more additional hosts. For example, an indirect security vulnerability scanner might transmit electronic mail through a relay host that is ultimately delivered to the target host.

An indirect security breach scanner is a security breach scanner in which some communication with the target host takes place indirectly through one or more additional hosts.

A server-based security vulnerability scanner is a security vulnerability scanner in which some communication with the target host is initiated by the target host. For example, a server-based security vulnerability scanner might transmit an HTML document that exploits a security vulnerability to a target host after receiving a request for the document from the target host.

A server-based security breach scanner is a security breach scanner in which some communication with the target host is initiated by the target host.

A remediation server is a network host that provides software to other hosts for the purpose of correcting security vulnerabilities and repairing security breaches. The remediation server might store software locally, or it might automatically manage communication with another such server (perhaps provided by a software vendor), or it might redirect a host to such a server.

A certification server is a network host that provides other hosts with information about current restrictions on their communications, as enforced by the security gateway.

An accreditation server is a network host with an arbitrarily large database that records vulnerability and security breach information and provides this data to other hosts for the purpose of satisfying security accreditation authorities.

A quarantine network is a computer network in which communication with any given host is restricted based on the policy of a security gateway.

A mobile program is an executable program that is transmitted from one network host to another network host.

A threat/response scanner is a network host that actively communicates with one or more target network hosts with the purpose of determining how the operators of the target network hosts will respond to typical security threats.

An indirect threat/response scanner is a threat/response scanner in which some communication with the target host takes place indirectly through one or more additional hosts.

A server-based threat/response scanner is a threat/response scanner in which some communication with the target host is initiated by the target host.

In various embodiments, the present invention relates generally to a network security architecture and methodology that applies a security policy based on user and/or system responses to security probes, for example. With reference to Figure 1, a network security system 102 may include a quarantine network 104 configured for communication with one or more external networks 106 (e.g., Internet) and/or one or more network hosts 108, 110, 112. As described hereinafter in more detail, the quarantine network 104 may include one or more of the following components: a security gateway 104A; an accreditation server 104B; a certification server 104C; a remediation server 104D; one or more scanners 104E; and/or one or more monitors 104F. The network security system 102 may be operatively associated with, or may be incorporated as a part of, one or more networks of commercial or non-commercial enterprises such as, for example and without limitation, companies, firms, institutions, governmental agencies, and/or other entities capable of employing computer networks in their operations.

In operation, in certain embodiments, the system may send a user a security probe attached to an email disguised as a known virus. If the user opens the attachment, as may be prohibited under the network security policy, the probe can send a message alerting the security system of the potential security breach that allows the system to restrict the user's network access. In another variation, the security probe may automatically apply prophylactic protection to the end user's host to prevent the host from being exploited by that type of email attack. As shown in Figure 2, for example, a vulnerability scanner 152 may send an e-mail message 154 through an e-mail relay 156 to a target host 158. The e-mail message 154, which includes a "safe" e-mail exploit as a security probe attachment 160, is designed to appear to contain a real virus or other exploit (e.g., the "MyDoom" virus). If the operator at the host 158 opens or executes the exploit or virus associated with the security probe attachment 160, an alert 162 may be transmitted from the security probe 160 back to the vulnerability scanner 152. This alert 162 notifies the vulnerability scanner 152 that the host 158 can be considered vulnerable to the type of security breach risk represented by the exploit or virus contained in the security probe attachment 160. The vulnerability scanner 152, in accordance with a network security policy, may then restrict the host's 158 network access. For example, executable attachments may be stripped from e-mail messages sent to the host 158, or e-mail access to the host 158 may be blocked entirely.

As another example, the system may attempt to exploit unpatched security vulnerabilities on a target system. If the exploitation attempt is successful, network access to the vulnerable system can be restricted until the vulnerabilities are corrected. Attempts to connect to the network can be redirected to the remediation server. In various embodiments, the remediation server can provide the user with detailed instructions on how to regain full network access.

The system may also apply prophylactic protection at the network level based on the user's response to an acceptable use policy test given to the user prior to providing network access. For example, after a user's host is scanned and found to have no security breaches, a quiz server may test the user about a network acceptable use policy by posing one or more hypothetical questions to the user. The quiz server may then restrict the security policy for that user based on the extent of correct answers supplied by the user with regard to the acceptable use policy.

When a new host connects to the network, its access privileges may be restricted until it has demonstrated that it does not pose a security risk (either due to unpatched vulnerabilities, or because the system has been compromised). The host may be permitted to connect to only a limited set of servers that have been specifically "hardened" to resist malicious or exploitative network traffic. All or any portion of network traffic to and from the host can be actively monitored while it is in the restricted state. Once such monitoring shows that the host is not a source of malicious traffic and/or that the host is not vulnerable to malicious traffic, restrictions on network access by the host can be lifted in whole or part. Access to additional network services may be granted automatically as the host establishes a record of responsible activity (as may be determined by the monitoring gateway, for example).

In various embodiments of the invention, with reference to Figure 3, a network security system 201 can be provided with a quarantine network 202 including a security vulnerability scanner 202A, and a security gateway 202B for which a security policy can be determined at least in part based on data produced by the security vulnerability scanner 202A. The quarantine network 202 may also include a remediation server 202C. The quarantine network may also include a certification server 202D, which can be configured to receive at least some or all prohibited communications that may be automatically redirected to the certification server 202D in association with detection of the prohibited communications by the network security system 201. In addition, at least some or all of the prohibited communications may be automatically redirected to another network host 204 in association with detection of the prohibited communications by the network security system 201.

In various embodiments, the security vulnerability scanner 202A of the quarantine network may include an indirect security vulnerability scanner. For example, the indirect security vulnerability scanner may be configured to transmit one or more electronic mail messages or mobile programs that may exploit or attempt to exploit one or more security vulnerabilities and/or breaches of a target host 206. The security vulnerability scanner 202A may also be a server-based security vulnerability scanner.

For example, the server-based security vulnerability scanner may transmit HTML documents or mobile programs that exploit or attempt to exploit one or more security vulnerabilities and/or breaches of the target host 206.

In various embodiments of the invention, with reference to Figure 4, a network security system 301 can be provided with a quarantine network 302 including a security breach scanner 302A, and a security gateway 302B for which a security policy of the network security system 301 can be determined at least in part based on data produced by the security breach scanner 302A. The quarantine network 301 may also include a remediation server 302C. The quarantine network 301 may also include a certification server 302D, which can be configured to receive at least some or all prohibited communications that may be automatically redirected to the certification server 302D in association with detection of the prohibited communications by the network security system 301. In addition, at least some or all of the prohibited communications may be automatically redirected to another network host 304 in association with detection of the prohibited communications by the network security system 301.

In various embodiments, the security breach scanner 302A of the quarantine network 302 may include an indirect security breach scanner. For example, the indirect security breach scanner may be configured to transmit one or more electronic mail messages or mobile programs that may exploit or attempt to exploit one or more security vulnerabilities and/or breaches of a target host 306. The security breach scanner may also be a server-based security breach scanner. For example, the server-based security breach scanner may transmit HTML documents or mobile programs that exploit or attempt to exploit one or more security vulnerabilities and/or breaches of the target host 306.

In various embodiments of the invention, with reference to Figure 5, a network security system 401 can be provided with a quarantine network 402 including a security vulnerability monitor 402A, and a security gateway 402B for which a security policy of the network security system 401 can be determined at least in part based on data produced by the security vulnerability monitor 402A. The quarantine network 402 may also include a remediation server 402C. The quarantine network 402 may also include a certification server 402D, which can be configured to receive at least some or all prohibited communications that may be automatically redirected to the certification server 402D in association with detection of the prohibited communications by the network security system 401. In addition, at least some or all of the prohibited communications may be automatically redirected to another network host 404 in association with detection of the prohibited communications by the network security system 401. In certain embodiments of the quarantine network 402, communications restrictions placed on a target network host 406 may be removed entirely or gradually lifted based on subsequent detection of no or substantially no security vulnerabilities.

In various embodiments of the invention, with reference to Figure 6, a network security system 501 can be provided with a quarantine network 502 including a security breach monitor 502A, and a security gateway 502B for which a security policy of the network security system 501 can be determined at least in part based on data produced by the security breach monitor 502A. The quarantine network 501 may also include a remediation server 502C. The quarantine network 502 may also include a certification server 502D, which can be configured to receive at least some or all prohibited communications that may be automatically redirected to the certification server 502D in association with detection of the prohibited communications by the network security system 501. In addition, at least some or all of the prohibited communications may be automatically redirected to another network host 504 in association with detection of the prohibited communications by the network security system 501. In certain embodiments of the quarantine network 502, communications restrictions placed on a target network host 506 may be removed entirely or gradually lifted based on subsequent detection of no or substantially no security vulnerabilities.

In various embodiments of the invention, with reference to Figure 7, a network security system 601 can be provided with a quarantine network 602 including an accreditation server 602A, and a security gateway 602B for which a security policy of the network security system 601 can be determined at least in part based on data stored in the accreditation server 602A. The quarantine network 602 may additionally include a security vulnerability scanner 602C which may be in communication with the accreditation server 602A. The quarantine network 602 may also include a security breach scanner 602D which may communicate with the accreditation server 602A. The quarantine network 602 may also include a security vulnerability monitor 602E which may communicate with the accreditation server 602A. The quarantine network 602 may also include a security breach monitor 602F which may communicate with the accreditation server 602A. The quarantine network 602 may also be configured to redirect at least some or all prohibited communications to the accreditation server 602A and/or to another network host 604 in association with detection of the prohibited communications by the network security system 601.

In various embodiments of the invention, with reference to Figure 8, a network security system 701 can be provided with a quarantine network 702 including a threat/response scanner 702A, and a security gateway 702B for which a security policy of the network security system 701 can be determined at least in part based on data produced by the threat/response scanner 702A. The quarantine network 702 may also include a remediation server 702C and/or a certification server 702D. The certification server 702D can be configured to receive at least some or all prohibited communications that may be automatically redirected to the certification server 702D in association with detection of the prohibited communications by the network security system 701. In addition, at least some or all of the prohibited communications may be automatically redirected to another network host 704 in association with detection of the prohibited communications by the network security system 701.

The threat/response scanner 702A may be configured as an indirect threat/response scanner. For example, the indirect threat/response scanner can be configured to transmit one or more electronic mail messages and/or mobile programs that are intended to appear to be of a dubious nature to an operator or a target network host 706. In certain embodiments, the threat/response scanner 702A may be provided as a server-based threat/response scanner. For example, the server-based threat/response scanner can be configured to transmit one or more HTML documents or mobile programs intended to appear to be of a dubious nature to the operator or the target network host 706. The server-based threat/response scanner may also be configured to transmit hypothetical questions or a security policy quiz, for example, to the operator or the target network host 706.

In various embodiments of network security systems and quarantine networks described herein, security vulnerability data and security breach data may be used to provide documentation or reports as required by accreditation authorities, for example.

The examples presented herein are intended to illustrate potential and specific implementations of the present invention. It can be appreciated that the examples are intended primarily for purposes of illustration of the invention for those skilled in the art. No particular aspect or aspects of the examples is/are intended to limit the scope of the present invention.

It is to be understood that the figures and descriptions of the present invention have been simplified to illustrate elements that are relevant for a clear understanding of the present invention, while eliminating, for purposes of clarity, other elements. For example, certain operating system details and modules of network platforms are not described herein. Those of ordinary skill in the art will recognize, however, that these and other elements may be desirable in a typical computer system or database system. However, because such elements are well known in the art and because they do not facilitate a better understanding of the present invention, a discussion of such elements is not provided herein.

Any element expressed herein as a means for performing a specified function is to encompass any way of performing that function including, for example, a combination of elements that perform that function. Furthermore the invention, as defined by such means-plus-function claims, resides in the fact that the functionalities provided by the various recited means are combined and brought together in a manner as defined by the appended claims. Therefore, any means that can provide such functionalities may be considered equivalents to the means shown herein.

In general, it will be apparent to one of ordinary skill in the art that some of the embodiments as described hereinabove may be implemented in many different embodiments of software, firmware, and/or hardware. The software code or specialized control hardware used to implement some of the present embodiments is not limiting of the present invention. For example, the embodiments described hereinabove may be implemented in computer software using any suitable computer software language type such as, for example, C or C++ using, for example, conventional or object-oriented techniques. Such software may be stored on any type of suitable computer-readable medium or media such as, for example, a magnetic or optical storage medium. Thus, the operation and behavior of the embodiments are described without specific reference to the actual software code or specialized hardware components. The absence of such specific references is feasible because it is clearly understood that artisans of ordinary skill would be able to design software and control hardware to implement the embodiments of the present invention based on the description herein with only a reasonable effort and without undue experimentation.

Moreover, the processes associated with the present embodiments may be executed by programmable equipment, such as computers. Software that may cause programmable equipment to execute the processes may be stored in any storage device, such as, for example, a computer system (non-volatile) memory, an optical disk, magnetic tape, or magnetic disk. Furthermore, some of the processes may be programmed when the computer system is manufactured or via a computer-readable medium. Such a medium may include any of the forms listed above with respect to storage devices and may further include, for example, a carrier wave modulated, or otherwise manipulated, to convey instructions that may be read, demodulated/decoded and executed by a computer.

It can also be appreciated that certain process aspects described herein may be performed using instructions stored on a computer-readable medium or media that direct a computer system to perform process steps. A computer-readable medium may include, for example, memory devices such as diskettes, compact discs of both read-only and read/write varieties, optical disk drives, and hard disk drives. A computer-readable medium may also include memory storage that may be physical, virtual, permanent, temporary, semi-permanent and/or semi-temporary. A computer-readable medium may further include one or more data signals transmitted on one or more carrier waves.

In various embodiments of the present invention disclosed herein, a single component may be replaced by multiple components, and multiple components may be replaced by a single component, to perform a given function or functions. Except where such substitution would not be operative to practice embodiments of the present invention, such substitution is within the scope of the present invention. Any of the servers described herein, for example, may be replaced by a "server farm" or other grouping of networked servers that are located and configured for cooperative functions. It can be appreciated that a server farm may serve to distribute workload between/among individual components of the farm and may expedite computing processes by harnessing the collective and cooperative power of multiple servers. Such server farms may employ load-balancing software that accomplishes tasks such as, for example, tracking demand for processing power from different machines, prioritizing and scheduling tasks based on network demand, and/or providing backup contingency in the event of component failure or reduction in operability.

While various embodiments of the invention have been described herein, it should be apparent, however, that various modifications, alterations and adaptations to those embodiments may occur to persons skilled in the art with the attainment of some or all of the advantages of the present invention. The disclosed embodiments are therefore intended to include all such modifications, alterations and adaptations without departing from the scope and spirit of the present invention as set forth in the appended claims.

CLAIMS

WHAT IS CLAIMED IS:

1. A quarantine network comprising:

a security vulnerability scanner; and,

a security gateway for which a security policy is determined at least in part based on data produced by the security vulnerability scanner.

2. The network of Claim 1, further comprising a remediation server.

3. The network of Claim 1, further comprising a certification server.

4. The network of Claim 3, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the certification server.

5. The network of Claim 1, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

6. The network of Claim 1, wherein the security vulnerability scanner includes an indirect security vulnerability scanner.

7. The network of Claim 6, further comprising the indirect security vulnerability scanner being configured to transmit at least one electronic mail or mobile

program that exploits at least one security vulnerability or security breach of a target host.

8. The network of Claim 1, wherein the security vulnerability scanner includes a server-based security vulnerability scanner.

9. The network of Claim 8, further comprising the server-based security vulnerability scanner being configured to transmit at least one HTML document or mobile program that exploits at least one security vulnerability or security breach of a target host.

10. A quarantine network comprising:

a security breach scanner; and,

a security gateway for which a security policy is determined at least in part based on data produced by the security breach scanner.

11. The network of Claim 10, further comprising a remediation server.

12. The network of Claim 10, further comprising a certification server

13. The network of Claim 12, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the certification server.

14. The network of Claim 10, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

15. The network of Claim 10, wherein the security breach scanner includes an indirect security breach scanner.

16. The network of Claim 15, further comprising the indirect security breach scanner being configured to transmit at least electronic mail message or mobile program that exploits at least one security vulnerability or security breach of a target host.

17. The network of Claim 10, wherein the security breach scanner includes a server-based security breach scanner.

18. The network of Claim 17, further comprising the server-based security breach scanner being configured to transmit at least one HTML document or mobile program that exploits at least one security vulnerability or security breach of a target host.

19. A quarantine network comprising:

a security vulnerability monitor; and,

a security gateway for which a security policy is determined at least in part based on data produced by the security vulnerability monitor.

20. The network of Claim 19, further comprising a remediation server.

21. The network of Claim 19, further comprising a certification server.

22. The network of Claim 21, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the certification server.

23. The network of Claim 19, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

24. The network of Claim 19, further comprising the quarantine network being configured to at least gradually lift communication restrictions on a network host.

25. A quarantine network comprising:

a security breach monitor; and,

a security gateway for which a security policy is determined at least in part based on data produced by the security breach monitor.

26. The network of Claim 25, further comprising a remediation server.

27. The network of Claim 25, further comprising a certification server.

28. The network of Claim 27, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the certification server.

29. The network of Claim 25, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

30. The network of Claim 25, further comprising the quarantine network being configured to at least gradually lift communication restrictions on a network host.

31. A quarantine network comprising:

an accreditation server; and,

a security gateway for which a security policy is determined at least in part based on data stored in the accreditation server.

32. The network of Claim 31, further comprising a security vulnerability scanner.

33. The network of Claim 32, wherein the security vulnerability scanner is in communication with the accreditation server.

34. The network of Claim 31, further comprising a security breach scanner.

35. The network of Claim 34, wherein the security breach scanner is in communication with the accreditation server.

36. The network of Claim 31, further comprising a security vulnerability monitor.

37. The network of Claim 36, wherein the security vulnerability monitor is in communication with the accreditation server.

38. The network of Claim 31, further comprising a security breach monitor.

39. The network of Claim 38, wherein the security breach monitor is in communication with the accreditation server.

40. The network of Claim 31, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the accreditation server.

41. The network of Claim 31, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

42. A quarantine network comprising:

a threat/response scanner; and,

a security gateway for which a security policy is determined at least in part based on data produced by the threat/response scanner.

43. The network of Claim 42, further comprising a remediation server.

44. The network of Claim 42, further comprising a certification server.

45. The network of Claim 44, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to the certification server.

46. The network of Claim 42, further comprising the quarantine network being configured to automatically redirect at least some prohibited communications to a network host.

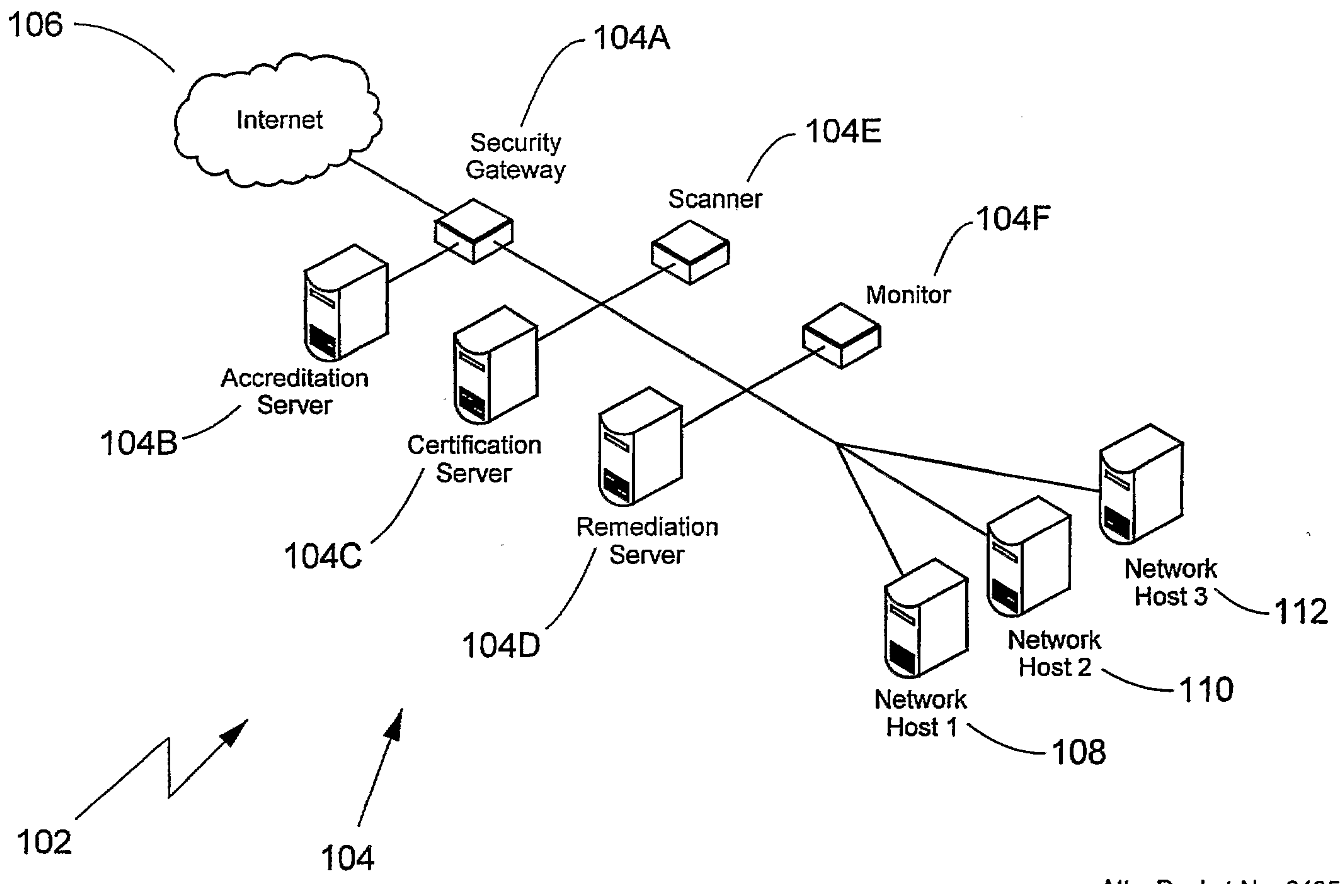
47. The network of Claim 42, wherein the threat/response scanner includes an indirect threat/response scanner.

48. The network of Claim 47, further comprising the indirect threat/response scanner being configured to transmit at least one electronic mail message or mobile program intended to appear to be of a dubious nature to an operator.

49. The network of Claim 42, wherein the threat/response scanner includes a server-based threat/response scanner.

50. The network of Claim 49, further comprising the server-based threat/response scanner being configured to transmit at least one electronic mail message or mobile program intended to appear to be of a dubious nature to an operator.

51. The network of Claim 49, further comprising the server-based threat/response scanner being configured to transmit at least one hypothetical question to an operator.



Atty. Docket No. 040589PCT

FIGURE 1

Atty. Docket No. 040589PCT

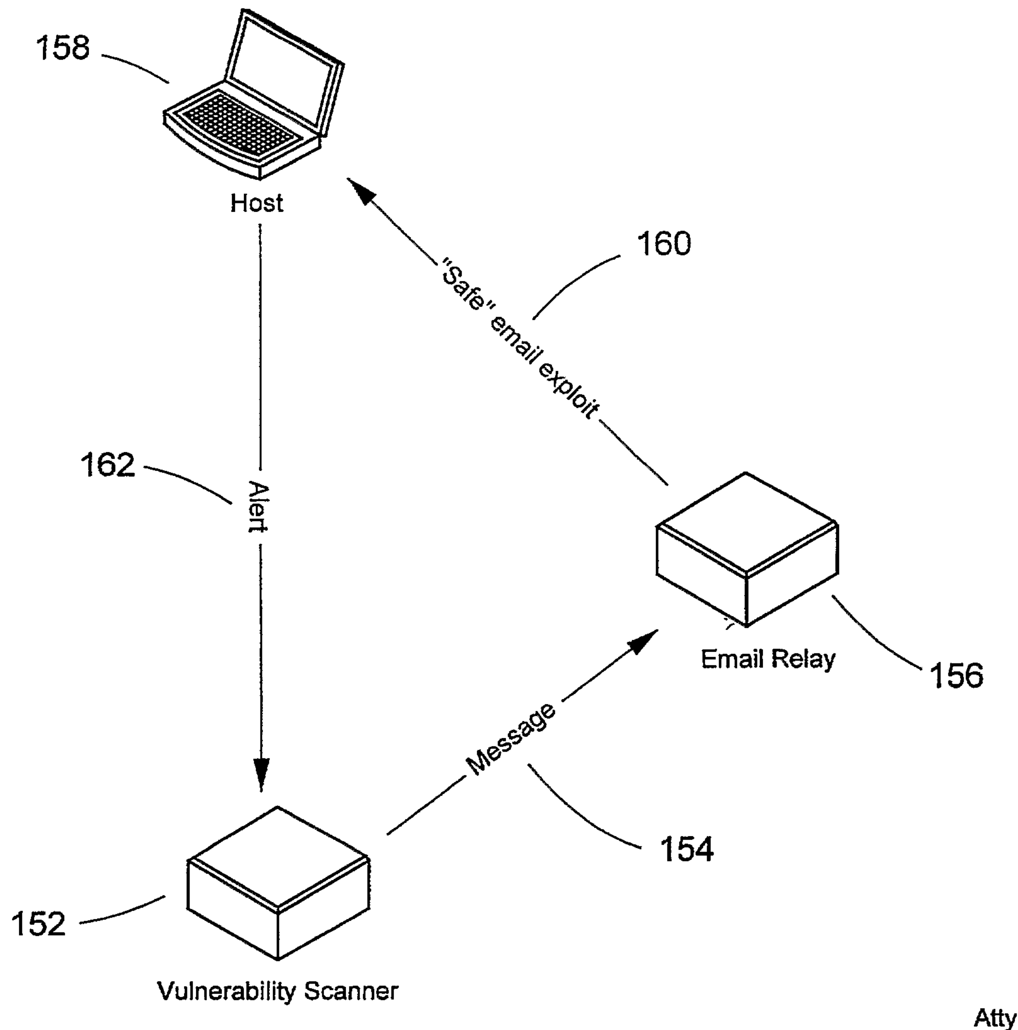


FIGURE 2

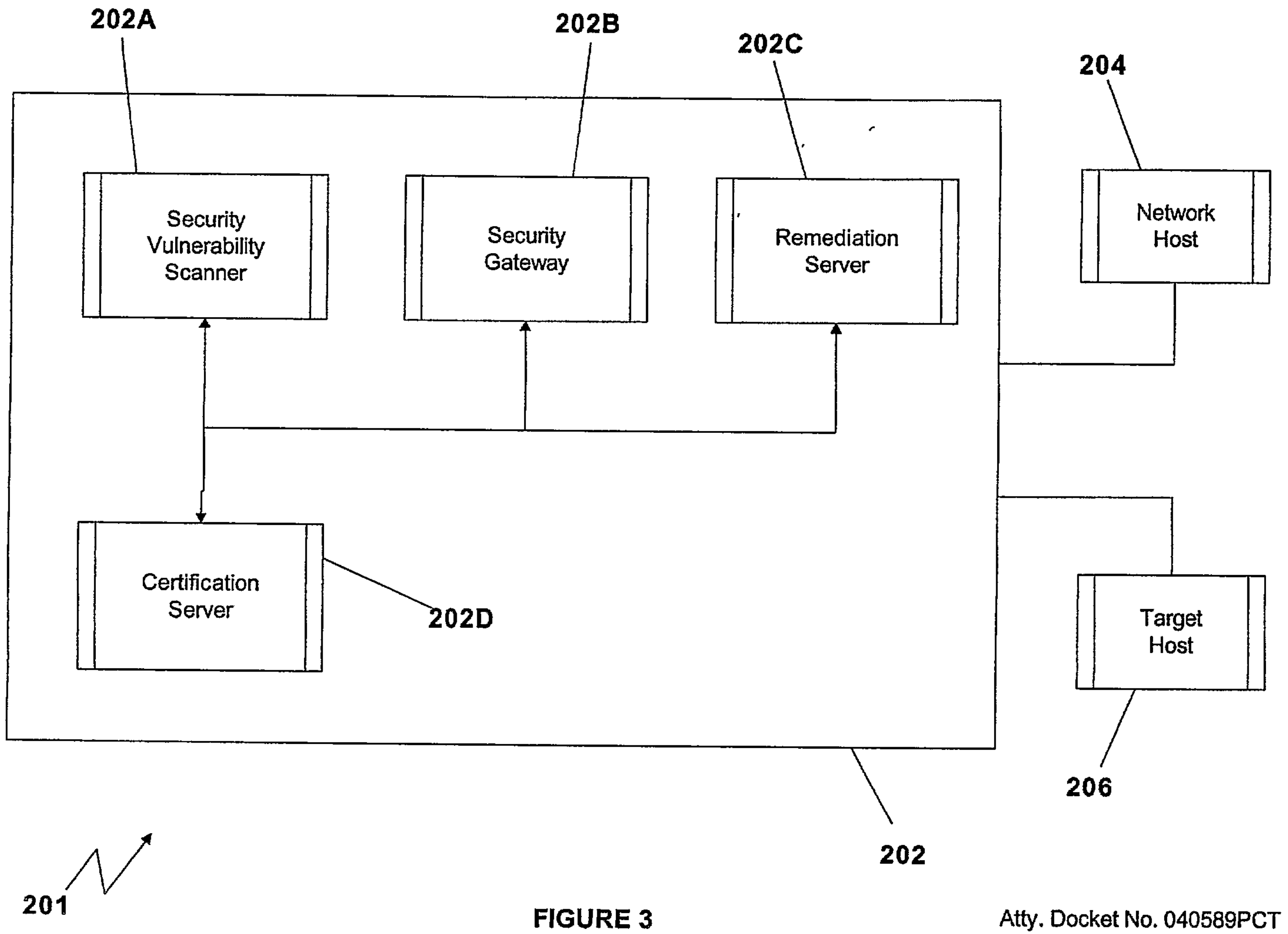


FIGURE 3

Atty. Docket No. 040589PCT

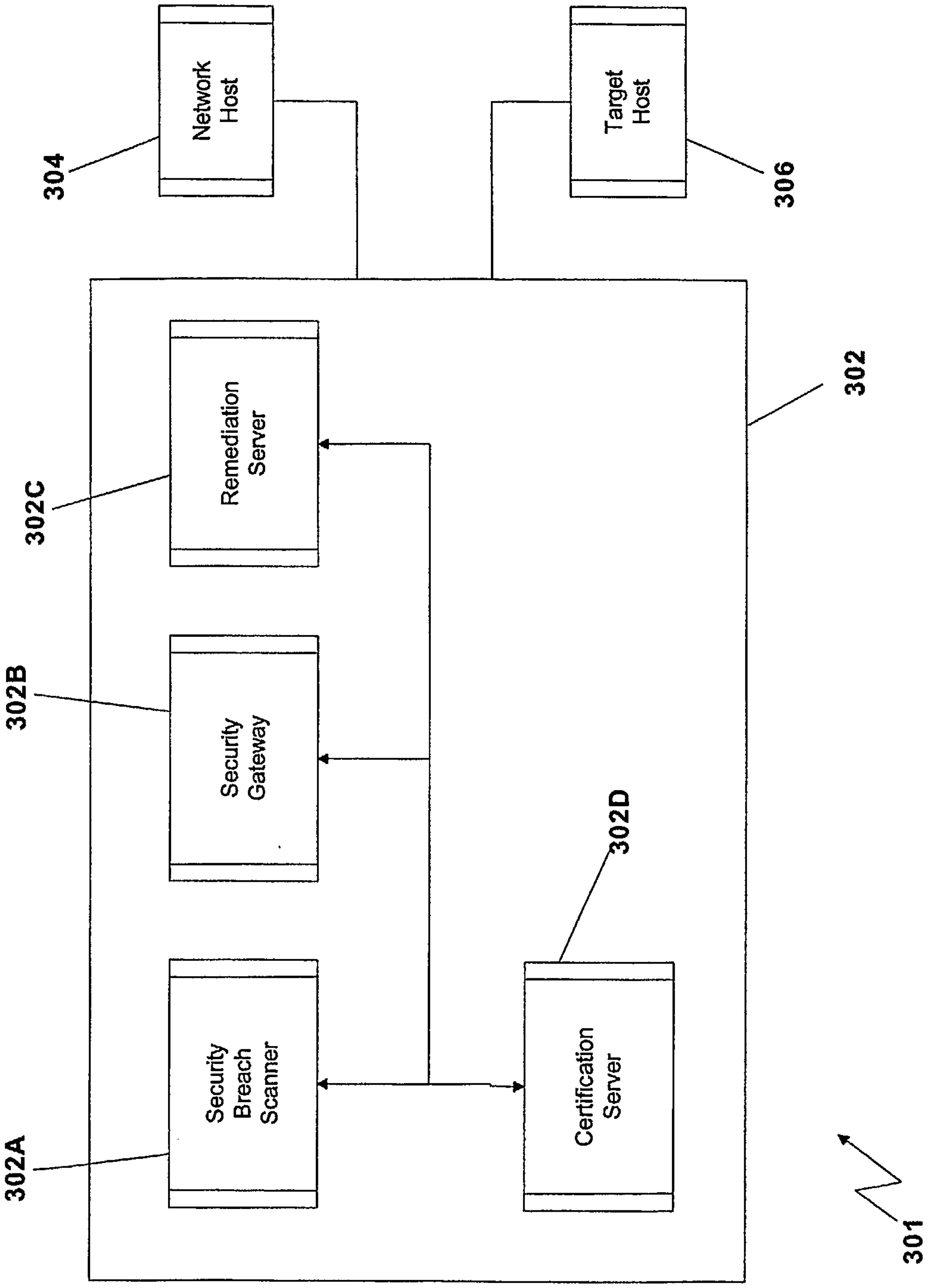


FIGURE 4

Atty. Docket No. 040589PCT

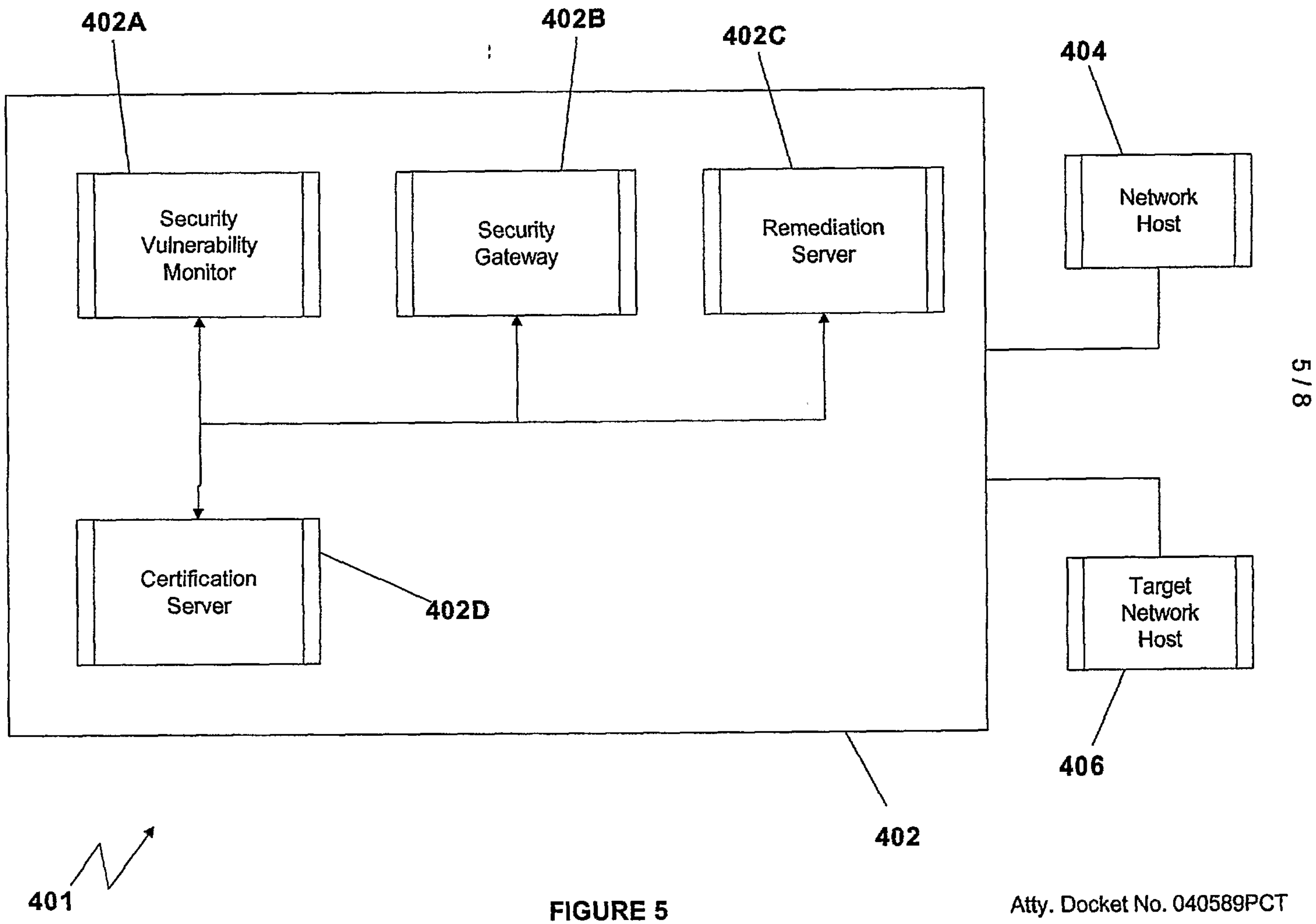


FIGURE 5

Atty. Docket No. 040589PCT

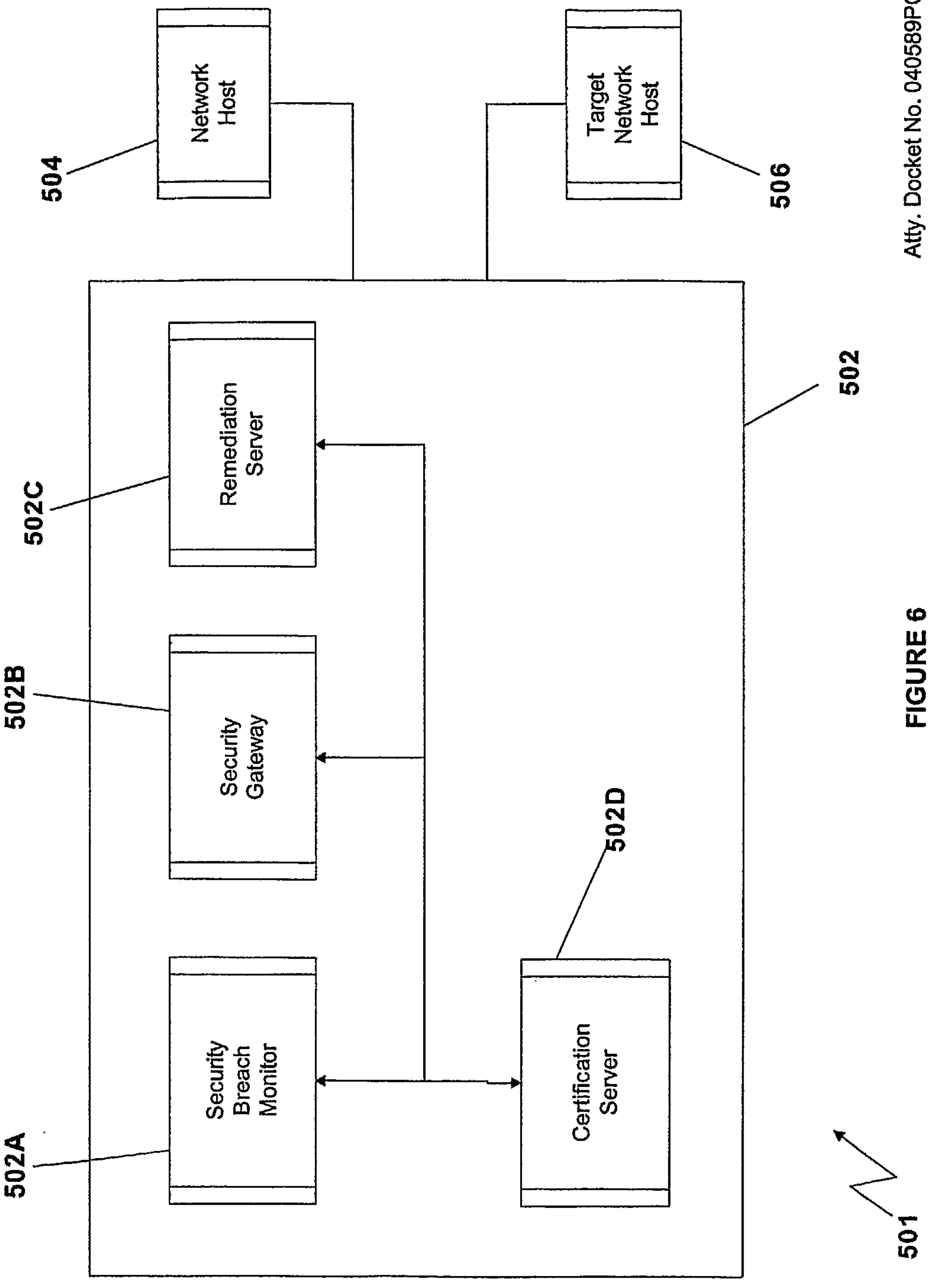


FIGURE 6

Atty. Docket No. 040589PCT

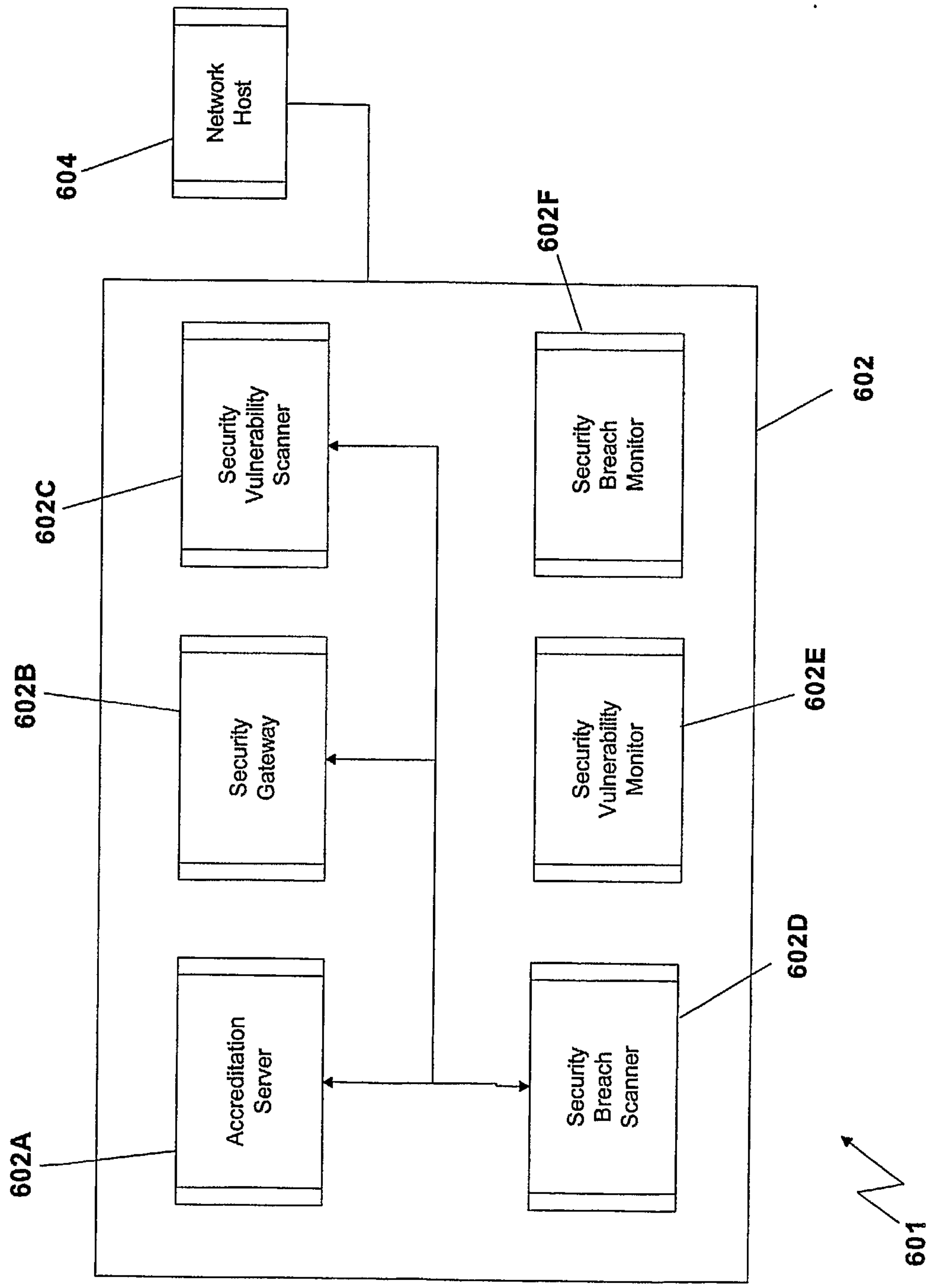


FIGURE 7

Atty. Docket No. 040589PCT

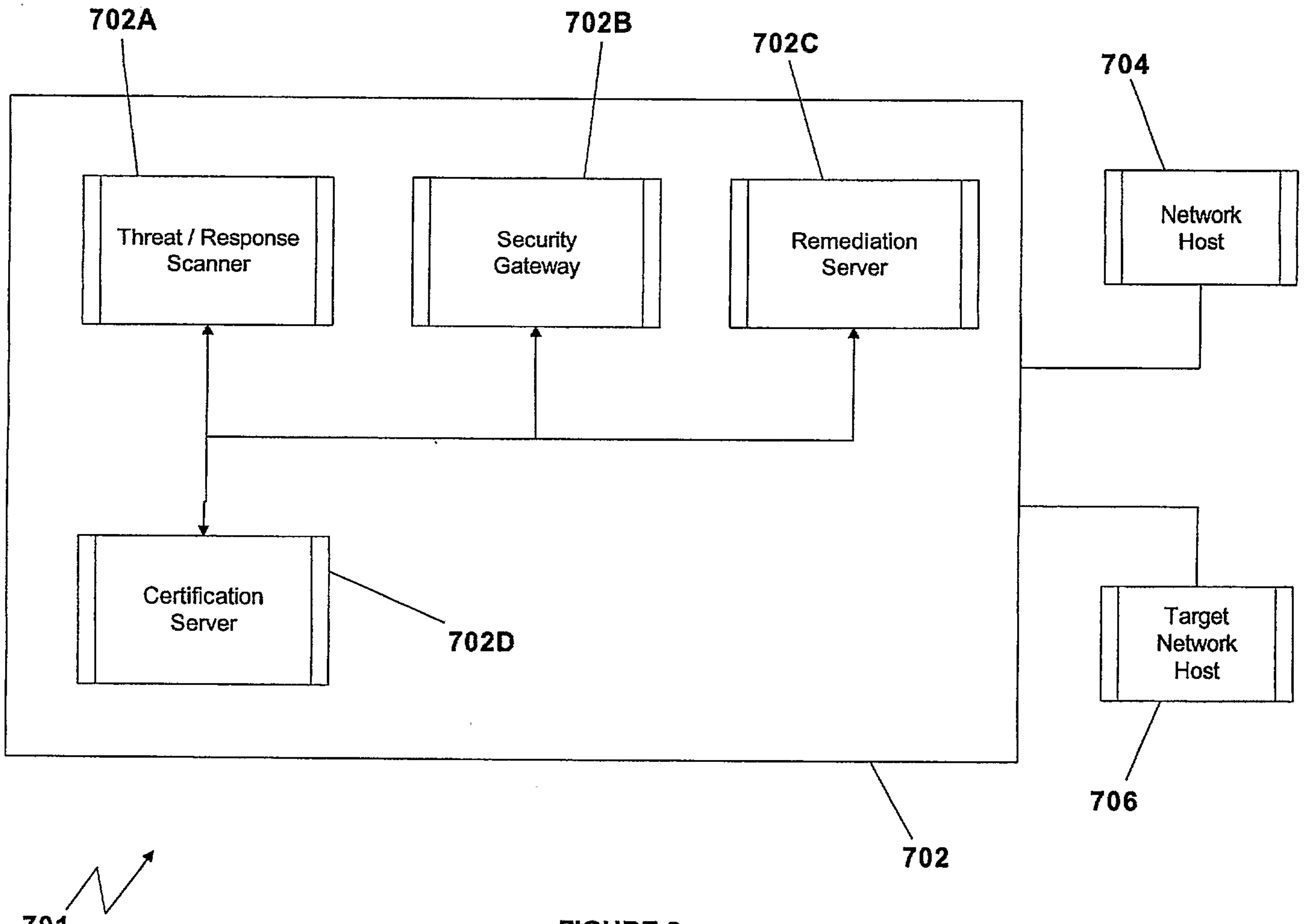


FIGURE 8

Atty. Docket No. 040589PCT