Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2977500 A1 2016/09/01

(21) 2 977 500

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2016/02/05
(87) Date publication PCT/PCT Publication Date: 2016/09/01
(85) Entrée phase nationale/National Entry: 2017/08/22
(86) N° demande PCT/PCT Application No.: US 2016/016752
(87) N° publication PCT/PCT Publication No.: 2016/137721
(30) Priorité/Priority: 2015/02/26 (US14/632,812)

(51) Cl.Int./Int.Cl. *G06F 17/00* (2006.01), *G06F 21/00* (2013.01), *G06F 21/55* (2013.01)

(71) Demandeur/Applicant:
SYMANTEC CORPORATION, US

(72) Inventeur/Inventor:
EFSTATHOPOULOS, PETROS, US

(74) Agent: PARLEE MCLAWS LLP

(54) Titre : COURTIER TIERS DE CONFIANCE DE COLLECTE ET DE PARTAGE PRIVE DE PRATIQUES DE SECURITE INFORMATIQUE REUSSIES

(54) Title: TRUSTED THIRD PARTY BROKER FOR COLLECTION AND PRIVATE SHARING OF SUCCESSFUL COMPUTER SECURITY PRACTICES

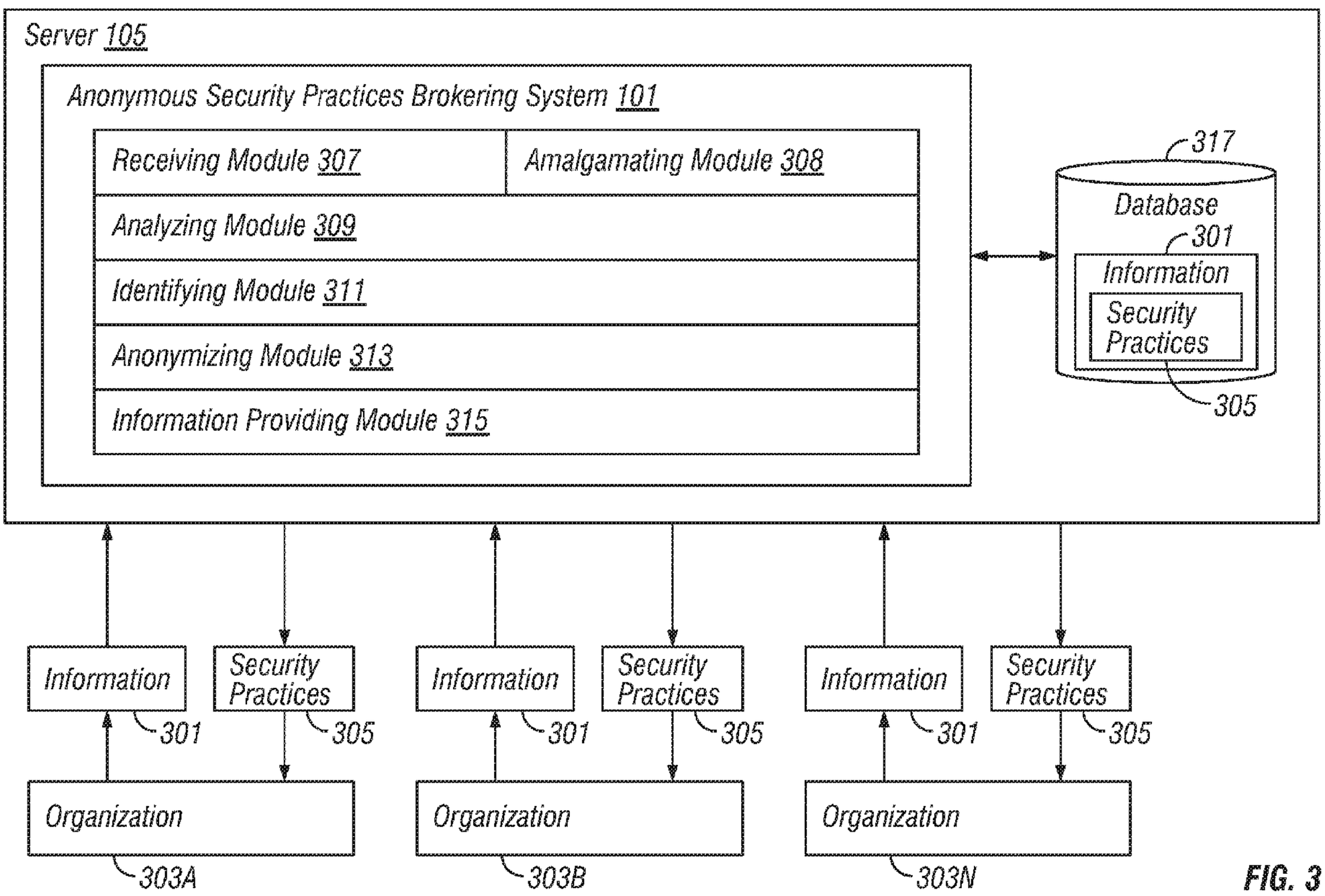

FIG. 3

(57) Abrégé/Abstract:
A trusted third party broker collects information concerning successful computer security practices from multiple organizations, and privately shares collected information at an inter-organizational level. Information concerning empirically successful computer

(21) 2 977 500

(13) A1

(57) Abrégé(suite)/Abstract(continued):
security practices is received from multiple source organizations. The information concerning empirically successful computer security practices received from the multiple source organizations is amalgamated and analyzed. Based on the analysis, specific information conceming empirically successful computer security practices is identified to share with specific target organizations. Once information to share with a target organization has been identified, any explicit and/or implicit source information that could identify the organization(s) from which the information originated is removed. The identified specific information concerning empirically successful computer security practices is then provided to the specific target organizations, with the source identifying information removed.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 September 2016 (01.09.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/137721 A1

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/US2016/016752

(22) International Filing Date:
5 February 2016 (05.02.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/632,812 26 February 2015 (26.02.2015) US

(71) Applicant: **SYMANTEC CORPORATION** [US/US]; 350 Ellis Street, Mountain View, CA 94043 (US).

(72) Inventor: **EFSTATHOPOULOS, Petros**; C/o Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 (US).

(74) Agents: **BRILL, Jeffrey** et al.; Patent Law Works LLP, 201 S. Main Street, Suite 250, Salt Lake City, UT 84111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: TRUSTED THIRD PARTY BROKER FOR COLLECTION AND PRIVATE SHARING OF SUCCESSFUL COMPUTER SECURITY PRACTICES

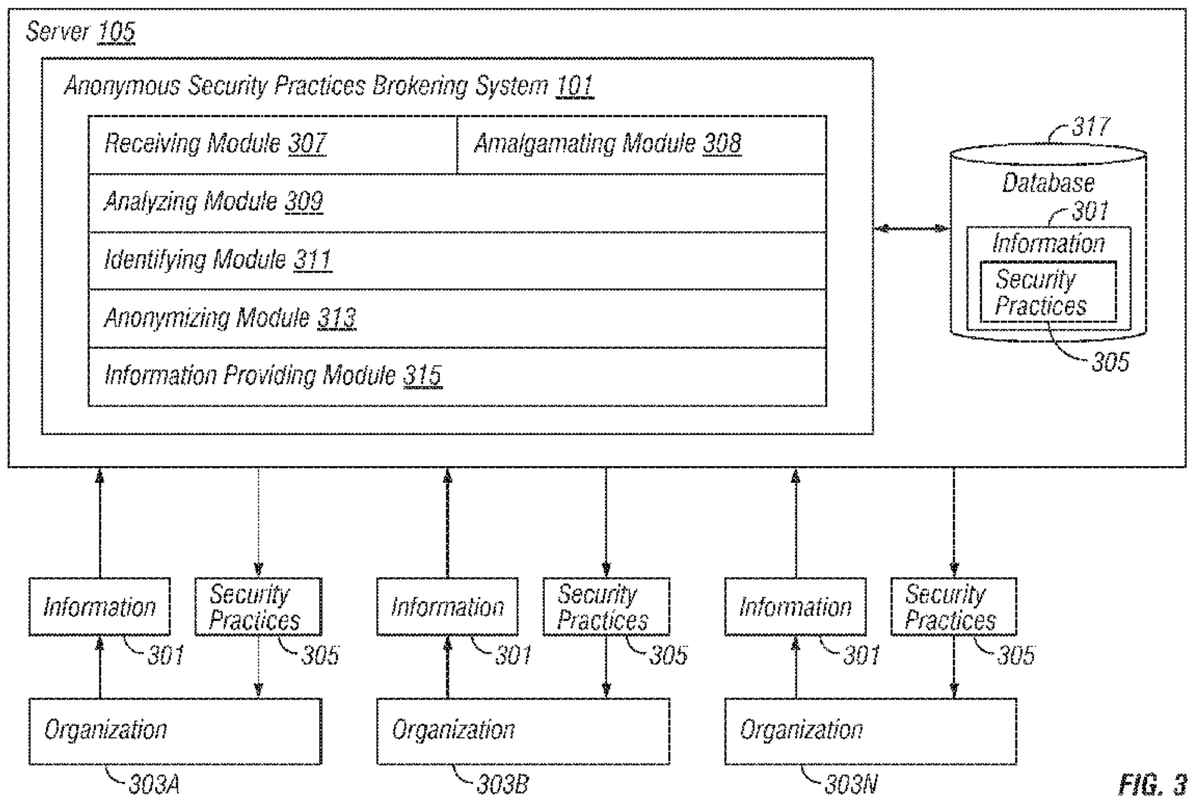

FIG. 3

(57) Abstract: A trusted third party broker collects information concerning successful computer security practices from multiple organizations, and privately shares collected information at an inter-organizational level. Information concerning empirically successful computer security practices is received from multiple source organizations. The information concerning empirically successful computer security practices received from the multiple source organizations is amalgamated and analyzed. Based on the analysis, specific information conceming empirically successful computer security practices is identified to share with specific target organizations. Once information to share with a target organization has been identified, any explicit and/or implicit source information that could identify the organization(s) from which the information originated is removed. The identified specific information concerning empirically successful computer security practices is then provided to the specific target organizations, with the source identifying information removed.

WO 2016/137721 A1

Trusted Third Party Broker for Collection and Private Sharing of Successful Computer Security Practices

Technical Field

[001] This disclosure pertains generally to information technology administration, and more specifically to a trusted third party broker for the collection and private sharing of successful computer security practices.

Background

[002] In order to defend against threats to networks and other information technology (IT) infrastructure in the field, telemetry and other indicators of potentially malicious behavior can be collected from various sources and analyzed. By gleaning information concerning events that signify anomalous behavior from a wide range of sites, ongoing attacks can be detected and future attacks can be blocked proactively.

[003] IT administrators of large enterprises could also benefit greatly from sharing intelligence regarding security best practices. For example, many intrusion detection systems (IDS) are constantly updated by experienced IT administrators with new rules capable of catching or defending against new types of threats. Collecting information concerning effective security best practices (so-called "positive telemetry") could provide a valuable resource for IT administrators, especially when shared among organizations in the same industry. However, organizations are reluctant to openly share/expose information regarding specific attacks directed against their infrastructure. Where organizations do not share such information concerning their own successful practices, IT administrators at other organizations have to "re-invent the wheel."

[004] It would be desirable to address these issues.

Summary

[005] A trusted third party broker (e.g., on a central cloud based computer) collects information concerning successful computer security practices from multiple organizations, and privately shares collected information at an inter-organizational level. Information concerning empirically successful computer security practices is received from multiple remote computers associated with multiple source organizations. Different ones of the empirically successful computer security practices have been and/or are being used to prevent attacks and other vulnerabilities at different ones of the source organizations.

[006] The received information can comprise rules used in an intrusion detection system or firewall to prevent attacks, rules used in a data loss prevention system to prevent the loss of data, anti-malware settings used to prevent infection, etc. Information concerning empirically successful computer security practices can be explicitly transmitted to the central computer by different specific source organizations. In addition or instead, information concerning empirically successful computer security practices on remote computers associated with specific source organizations can be read by the central computer. Computer security practices utilized by various ones of the source organizations can be monitored, and successful security practices can be inferred based on the results of utilizing the monitored computer security practices on the source organizations over time. Updated computer security practices can be periodically received (passively and/or actively) from the source organizations.

[007] The information concerning empirically successful computer security practices received from the multiple source organizations is amalgamated and analyzed.

Analyzing the amalgamated information can involve, for example, categorization based on the industry, type or size of the source organization. Based on the analysis, specific information concerning empirically successful computer security practices is identified to share with specific target organizations. This can involve identifying specific information concerning specific empirically successful computer security practices to be shared with specific target organizations based on industry, type and/or size of the organization, as well as specific computer security vulnerabilities to which the target organization is subject. Once information to share with a target organization has been identified, the information is anonymized, by removing any information that could explicitly or implicitly identify the originating source organization(s).

[008] The identified specific information concerning empirically successful computer security practices is then provided to the specific target organizations, with the source identifying information removed. Thus, the target organizations do not receive information identifying the source organization(s) of the successful computer security practices. The information can be provided to the target organizations in a number of ways. For example, recommendations concerning computer security practices can be transmitted to target organizations, or target organization level security settings can be automatically updated.

[009] The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the relevant art in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the

inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

Brief Description of the Drawings

[010] Figure 1 is a block diagram of an exemplary network architecture in which an anonymous security practices brokering system can be implemented, according to some embodiments.

[011] Figure 2 is a block diagram of a computer system suitable for implementing an anonymous security practices brokering system, according to some embodiments.

[012] Figure 3 is a high level block diagram of the operation of an anonymous security practices brokering system, according to some embodiments.

[013] Figure 4 is a flow chart of the steps an exemplary method of the operation of an anonymous security practices brokering system, according to some embodiments.

[014] The Figures depict various embodiments for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles described herein.

Detailed Description

[015] Figure 1 is a block diagram illustrating an exemplary network architecture 100 in which an anonymous security practices brokering system 101 can be implemented. The illustrated network architecture 100 comprises multiple clients 103A, 103B and 103N, as well as multiple servers 105A and 105N. In Figure 1, the anonymous security practices brokering system 101 is illustrated as residing on server 105A. It is to be understood that this is an example only, and in various embodiments various

functionalities of this system 101 can be instantiated on a client 103, a server 105, or can be distributed between multiple clients 103 and/or servers 105.

[016] Clients 103 and servers 105 can be implemented using computer systems 210 such as the one illustrated in Figure 2 and described below. The clients 103 and servers 105 are communicatively coupled to a network 107, for example via a network interface 248 or modem 247 as described below in conjunction with Figure 2. Clients 103 are able to access applications and/or data on servers 105 using, for example, a web browser or other client software (not shown). Clients 103 can but need not be in the form of mobile computing devices, comprising portable computer systems 210 capable of connecting to a network 107 and running applications. Such mobile computing devices are sometimes referred to as smartphones, although many mobile phones not so designated also have these capabilities. Tablet computers and laptop computers are other examples of mobile computing devices.

[017] Although Figure 1 illustrates three clients 103 and three servers 105 as an example, in practice many more (or fewer) clients 103 and/or servers 105 can be deployed. In one embodiment, the network 107 is in the form of the Internet. Other networks 107 or network-based environments can be used in other embodiments.

[018] Figure 2 is a block diagram of a computer system 210 suitable for implementing an anonymous security practices brokering system 101. Clients 103 and servers 105 can all be implemented in the form of such computer systems 210. As illustrated, one component of the computer system 210 is a bus 212. The bus 212 communicatively couples other components of the computer system 210, such as at least one processor 214, system memory 217 (e.g., random access memory (RAM), read-only memory (ROM), flash memory, an input/output (I/O) controller 218, an audio output interface 222 communicatively coupled to an audio output device such as a speaker 220, a display

adapter 226 communicatively coupled to a video output device such as a display screen 224, one or more interfaces such as Universal Serial Bus (USB) ports 228, serial ports 230, parallel ports (not illustrated), etc., a keyboard controller 233 communicatively coupled to a keyboard 232, a storage interface 234 communicatively coupled to one or more hard disk(s) 244 (or other form(s) of storage media), a host bus adapter (HBA) interface card 235A configured to connect with a Fibre Channel (FC) network 290, an HBA interface card 235B configured to connect to a SCSI bus 239, an optical disk drive 240 configured to receive an optical disk 242, a mouse 246 (or other pointing device) coupled to the bus 212, e.g., via a USB port 228, a modem 247 coupled to bus 212, e.g., via a serial port 230, and one or more wired and/or wireless network interface(s) 248 coupled, e.g., directly to bus 212.

[019] Other components (not illustrated) may be connected in a similar manner (e.g., document scanners, digital cameras, printers, etc.). Conversely, all of the components illustrated in Figure 2 need not be present (e.g., smartphones and tablets typically do not have optical disk drives 240, external keyboards 242 or external pointing devices 246, although various external components can be coupled to mobile computing devices via, e.g., USB ports 228). In different embodiments the various components can be interconnected in different ways from that shown in Figure 2.

[020] The bus 212 allows data communication between the processor 214 and system memory 217, which, as noted above may include ROM and/or flash memory as well as RAM. The RAM is typically the main memory into which the operating system and application programs are loaded. The ROM and/or flash memory can contain, among other code, the Basic Input-Output system (BIOS) which controls certain basic hardware operations. Application programs can be stored on a local computer readable medium (e.g., hard disk 244, optical disk 242, flash memory) and loaded into system

memory 217 and executed by the processor 214. Application programs can also be loaded into system memory 217 from a remote location (i.e., a remotely located computer system 210), for example via the network interface 248. In Figure 2, the anonymous security practices brokering system 101 is illustrated as residing in system memory 217. The workings of the anonymous security practices brokering system 101 are explained in greater detail below in conjunction with Figure 3.

[021] The storage interface 234 is coupled to one or more hard disks 244 (and/or other standard storage media). The hard disk(s) 244 may be a part of computer system 210, or may be physically separate and accessed through other interface systems.

[022] The network interface 248 and/or modem 247 can be directly or indirectly communicatively coupled to a network 107 such as the internet. Such coupling can be wired or wireless.

[023] Figure 3 illustrates an anonymous security practices brokering system 101 running on a server 105 in the cloud, and being accessed through a network 107 (e.g., the Internet) by computers 210 in multiple organizations. As described above, the functionalities of the anonymous security practices brokering system 101 can reside on specific computers 210 or be otherwise distributed between multiple computer systems 210, including within a fabric/cloud-based computing environment in which the functionality of the anonymous security practices brokering system 101 is provided as a service over a network 107. It is to be understood that although the anonymous security practices brokering system 101 is illustrated in Figures 3 as a single entity, the illustrated anonymous security practices brokering system 101 represents a collection of functionalities, which can be instantiated as a single or multiple modules as desired (instantiation of a specific, multiple module anonymous security practices brokering system 101 is illustrated in Figure 3). It is to be understood that the modules of the

anonymous security practices brokering system 101 can be instantiated (for example as object code or executable images) within the system memory 217 (e.g., RAM, ROM, flash memory) of any computer system 210, such that when the processor 214 of the computer system 210 processes a module, the computer system 210 executes the associated functionality. As used herein, the terms "computer system," "computer," "client computer," "server computer" and "computing device" mean one or more computers configured and/or programmed to execute the described functionality. Additionally, program code to implement the functionalities of the anonymous security practices brokering system 101 can be stored on computer-readable storage media. Any form of tangible computer readable storage medium can be used in this context, such as magnetic, optical or solid state storage media. As used herein, the term "computer readable storage medium" does not mean an electrical signal separate from an underlying physical medium.

[024] Figure 3 illustrates an anonymous security practices brokering system 101 running on a server 105, and functioning as a trusted third party broker for information 301 concerning successful computer security practices 305 from multiple organizations 303. In Figure 3, three organizations 303A, 303B and 303N are illustrated exchanging computer security practice information 301 through the anonymous security practices brokering system 101. It is to be understood that when deployed in the field, the anonymous security practices brokering system 101 can interact with orders of magnitude more organizations 303 (e.g., hundreds, thousands, hundreds of thousands, etc.). As the term is used herein, an organization 303 can be any entity which maintains at least one networked computer 210 with administrated computer security infrastructure. One example of an organization 303 is a corporation or other commercial enterprise that maintains a professionally administrated and secured computer network

107. Universities, government departments and other educational and/or not-for-profit institutions are other examples of organizations 303. An organization 303 can also be in the form of a small business, a private home network 107 or even an individual computer 210 connected to the Internet on which computer security infrastructure is installed (e.g., anti-malware software, a firewall, etc.).

[025] As described in detail below, the anonymous security practices brokering system 101 enables secure sharing/crowdsourcing of computer security information 301. To achieve this, the anonymous security practices brokering system 101 amalgamates the information 301 received from the various organizations 303, analyzes the amalgamated information 301, identifies empirically successful practices 305 to share with specific target organizations 303_{TARGET}, anonymizes the information 301 to protect the privacy and identity of the source organization(s) 303_{SOURCE}, and provides identified successful computer security practices 305 to the target organizations 303_{TARGET}. This results in the crowdsourcing of security practice information 301, and enables the sharing of best practices 305 in a secure and reliable fashion. The use of the anonymous security practices brokering system 101 enables IT professionals and other parties responsible for securing computer systems 210 to privately share their successful security practices 305 through a trusted third-party, and benefit from learning what practices 305 are working for other organizations 303. The anonymous security practices brokering system 101 itself becomes a security crowdsourcing broker platform, thereby adding value to the collected information 301, both by analyzing it and by identifying and anonymously sharing relevant successful security practices 305 with specific target organizations 303_{TARGET}.

[026] An information receiving module 307 of the anonymous security practices brokering system 101 receives information 301 concerning empirically successful

computer security practices 305 from multiple source organizations 303_{SOURCE}. IT administrators and other responsible parties at the level of the source organizations 303_{SOURCE} elect to provide or otherwise make available information 301 concerning computer security practices 305 that have been empirically successful for them. One example of such information 301 is specific rules that a given organization 303 has used in an intrusion detection system to successfully prevent one or more given attacks. Specific firewall rules used successfully to prevent attempted breaches are another example. Other examples include rules successfully used in a data loss prevention system by a source organization 303_{SOURCE} to prevent loss of data, and anti-malware system settings successfully used to prevent infection. It is to be understood that these are non-exhaustive examples, and in different embodiments different ones of the multiple source organizations 303_{SOURCE} can provide different types of information 301 relating to various security practices 305 that have been empirically successful for them in different contexts. In this manner, the anonymous security practices brokering system 101 is capable of collecting information 301 related to successful security best practices 305 from the various participating organizations 303.

[027] In some instances, a given source organization 303_{SOURCE} explicitly transmits information 301 concerning empirically successful computer security practices 305 to the information receiving module 307 of the anonymous security practices brokering system 101. In other instances, the information receiving module 307 remotely reads or otherwise gleans this information 301, for example by reading settings within the computer security infrastructure (e.g., instruction detection system settings, anti-malware system settings, etc.) of the given source organization 303_{SOURCE}. In these cases, an IT administrator or the like of the given source organization 303_{SOURCE} sets

the relevant access permissions such that the information receiving module 307 can read the appropriate settings.

[028] In one embodiment, the receiving module 307 monitors the use of various security practices 305 by one or more specific source organizations 303_{SOURCE} over time, and infers which security practices 305 are successful. In other words, the anonymous security practices brokering system 101 observes which computer security practices 305 work over time to achieve desired results on given organizations 303_{SOURCE} (e.g., an organization 303_{SOURCE} did X, Y and Z, and was never successfully attacked). Based on the results in practice of monitored source organizations 303_{SOURCE} utilizing various security practices 305, the anonymous security practices brokering system 101 infers which security practices 305 are successful, and receives information 301 from those source organizations 303_{SOURCE} in this way.

[029] Despite the specific route by which information 301 arrives, the information receiving module 307 can receive (actively or passively) updated information 301 periodically, thereby maintaining current information from the various source organizations 303_{SOURCE}. The frequency at which source organizations 303_{SOURCE} transmit (or at which the receiving module 307 actively gleans) updated information 301 is a variable design parameter, which can be set as desired according to different scenarios.

[030] As part of or in addition to the information 301 concerning empirically successful computer security practices 305, the source organizations 303_{SOURCE} can provide, and the receiving module 307 can receive, various metadata comprising information such as the identity, size, industry, type or other factors describing the source organization 303_{SOURCE}, which specific attacks/breaches/compromises different specific computer security practices 305 have been successful against, times of

deployment of given computer security practices 305, information concerning the hardware/software configurations of the source organizations 303_{SOURCE}, etc. The specific format and/or content of the information 301 concerning empirically successful computer security practices 305 originating from different source organizations 303_{SOURCE} is a variable design parameter.

[031] An amalgamating module 308 of the anonymous security practices brokering system 101 amalgamates the information 301 received from the multiple source organizations 303_{SOURCE}. This has the effect of maintaining a collection of information 301 concerning empirically successful computer security practices 305 received from each one of the multiple source organizations 303_{SOURCE}. A database 317 or other suitable information storage mechanism can be used to store and maintain the amalgamated information 301.

[032] An analyzing module 309 of the anonymous security practices brokering system 101 analyzes the amalgamated information 301 concerning empirically successful computer security practices 305 received from the multiple source organizations 303_{SOURCE}. In one embodiment, this analysis can take the form of categorizing amalgamated information 301 based on the industry of the source organization 303_{SOURCE} that provided it (e.g., software, electronics, financial services, retailing, automotive, etc.). The industry of the source organization 303_{SOURCE} can be gleaned from the received information 301, in which it can be embedded explicitly, or from which it can be implicitly determined (e.g., from the name of organization 303, from the IP address from which the transmission originates, etc.). In other embodiments, information can be categorized based on the organization type from which it originated (e.g., publically traded corporation, privately held start-up, educational institution, government, home network, etc.) or the size thereof (e.g., more than 5000 computers,

fewer than 100, individual user). Furthermore, the amalgamated information 301 can be minded according to various techniques, in order to extract additional usage and success patterns and other intelligence as desired.

[033] An identifying module 311 of the anonymous security practices brokering system 101 identifies specific information 301 concerning empirically successful computer security practices 305 to share with specific target organizations 303_{TARGET}, based on the analysis of the amalgamated information 301. The matching of computer security practices 305 that were empirically successful for one or more source organizations 303_{SOURCE} to specific target organizations 303_{TARGET} can be performed at any level of granularity. For example, in one embodiment computer security practices 305 that have been empirically successful for source organizations 303_{SOURCE} in a given industry (e.g., banking, military contracting, etc.) are identified as being desirable to share with target organizations 303_{TARGET} that operate in the same industry (e.g., other banks, other military contractors, etc.). In another embodiment, computer security practices 305 that have worked well for specific types or sizes of source organizations 303_{SOURCE} are identified for sharing with target organizations 303_{TARGET} of the same type and/or size. Computer security practices 305 that have been empirically successful for specific types or sizes of source organizations 303_{SOURCE} can also be identified for sharing with target organizations 303_{TARGET} that are of a different type and/or size. For example, security practices 305 that have prevented attacks at large industrial organizations can be identified for sharing with small home networks and individuals. In other embodiments, computer security practices that have been empirically successful at protecting against specific computer security vulnerabilities (e.g., preventing specific attacks, types of attacks or other specific breaches or compromises of computer systems 210) can be identified for sharing with target organizations

303_{TARGET} that are considered subject (e.g., vulnerable) to the given attack/breach/etc., based on, for example, geolocation, type of hardware or operating system, prevalence of the attack, etc.

[034] Prior to sharing identified information 301 with target organizations 303_{TARGET}, an anonymizing module 313 of the anonymous security practices brokering system 101 anonymizes the shared information, by removing any information that explicitly and/or implicitly identifies any source organization 303_{SOURCE}. This information can include source organization 303_{SOURCE} names, as well as any other information that could be used to identify any specific source organization 303_{SOURCE} from which the computer security practices 305 being shared originated, such as physical or network address, etc. This enables source organizations 303_{SOURCE} to be confident that their identities, as well what threats they have been subject to and other such information, including even the fact that they are participating in the program at all, will be kept confidential.

[035] An information providing module 315 of the anonymous security practices brokering system 101 provides identified information 301 concerning empirically successful computer security practices 305 to specific target organizations 303_{TARGET}, with all information identifying the originating source organization(s) 303_{SOURCE} removed. Thus, participating target organizations 303_{TARGET} are able to benefit from receiving and utilizing information about best practices 305 for computer security as crowdsourced from the multiple participating organizations 303, thereby leveraging the experience and knowhow of a large group of IT administrators and other computer security professionals for protecting against threats. Because the organizations 303_{TARGET} do not receive information identifying the source(s) of the provided information 301, the privacy and anonymity of the participants is maintained.

[036] In one embodiment, providing information 301 concerning successful security practices 305 can take the form of transmitting recommendations to target organizations 303_{TARGET}. For example, the information providing module 315 can transmit alerts recommending to implement specific security practices 305, along with information describing how to do so. Such recommendations can be transmitted to, for example, an IT administrator or the like, or to a software system installed on the target 303_{TARGET} which can in turn alert the responsible party.

[037] In another embodiment, providing information 301 concerning successful security practices 305 can involve automatically updating or otherwise configuring settings on the target 303_{TARGET}. For example, the information providing module 315 can automatically modify or update settings, rulesets or the like on an intrusion detection system, firewall, anti-malware system, data loss prevention system or other tool present at the target organization 303_{TAGRET}, in order to apply the empirically successful computer security practices there.

[038] In some embodiments the same set of organizations 303 both provides and receives information 301 concerning successful computer security practices 305. In other embodiments, some organizations 303 receive information 301 concerning successful computer security practices 305 without themselves providing any (for example, for a fee). It is also possible for some organizations 303 to provide information 301 without receiving any themselves.

[039] The anonymous security practices brokering system 101 enables anonymous sharing of computer security best practices 305. Organizations 303 tend to be very secretive about their IT operations, and are otherwise hesitant to share their successful security practices 305, even in return for receiving those of other organizations 303. By serving as a trusted third party, the anonymous security practices brokering system 101

provides this functionality as a cloud service in a secure fashion. Crowdsourcing security best practices 305 adds value for all receiving organizations 303, especially so for parties in the same or adjacent industries. The anonymous security practices brokering system 101 enables such organizations 303 to benefit from the knowledge obtained by their competitors from having successfully responded to computer security incidents that they experienced, without revealing the identity of the specific sources 303_{SOURCE} of any shared information 301.

[040] Figure 4 illustrates steps performed during the operation of an anonymous security practices brokering system 101, according to some embodiments. The information receiving module 307 receives 401 information 301 concerning empirically successful computer security practices 305 from multiple remote computers 210 associated with multiple source organizations 303_{SOURCE}. The amalgamating module 308 amalgamates 403 the information 301 concerning empirically successful computer security practices 305 received from the multiple remote computers 210 associated with the multiple source organizations 303_{SOURCE}. The analyzing module 309 analyzes 405 the amalgamated information 301 concerning empirically successful computer security practices 305. The identifying module 311 identifies 407 specific information 301 concerning empirically successful computer security practices 305 to share with specific target organizations 303_{TARGET}, based on the analysis of the amalgamated information 301. The anonymizing module 313 removes 409 explicit and/or implicit source information from the identified information 301 concerning empirically successful computer security practices 305 to be shared with the specific target organizations 303_{TARGET}. The information providing module 315 provides 411 the identified specific information 301 concerning empirically successful computer

security practices 305 to the specific target organizations 303_{TARGET}, with the explicit and/or implicit source information removed.

[041] As will be understood by those familiar with the art, the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Likewise, the particular naming and division of the portions, modules, agents, managers, components, functions, procedures, actions, layers, features, attributes, methodologies, data structures and other aspects are not mandatory or significant, and the mechanisms that implement the invention or its features may have different names, divisions and/or formats. The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or limiting to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain relevant principles and their practical applications, to thereby enable others skilled in the art to best utilize various embodiments with or without various modifications as may be suited to the particular use contemplated.

What is claimed is:

1. A computer implemented method for a trusted third party broker to collect information concerning successful computer security practices from a plurality of source organizations, and to share collected information at an inter-organizational level privately, the method comprising the steps of:

receiving, by a central computer, information concerning empirically successful computer security practices, from a plurality of remote computers associated with a plurality of source organizations, wherein different ones of the empirically successful computer security practices are being used at different ones of the plurality of source organizations;

amalgamating the information concerning empirically successful computer security practices received from the plurality of remote computers associated with the plurality of source organizations;

analyzing the amalgamated information concerning empirically successful computer security practices received from the plurality of remote computers associated with the plurality of source organizations;

identifying specific information concerning empirically successful computer security practices to share with at least one specific target organization, based on analyzing the amalgamated information;

removing source information from the identified specific information concerning empirically successful computer security practices to share with the at least one specific target organization; and

providing the identified specific information concerning empirically successful computer security practices to share with the at least one specific target organization, with the source information removed, wherein the at least one target organization does not receive information identifying the source of the

provided information concerning empirically successful computer security practices.

2. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, rules used in an intrusion detection system by at least one specific source organization to prevent at least one attack, from at least one remote computer.

3. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, rules used in a firewall by at least one specific source organization to prevent at least one attack, from at least one remote computer.

4. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, rules used in a data loss prevention system by at least one specific source organization to prevent loss of data, from at least one remote computer.

5. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, settings used in an anti-malware system by at least one specific source organization to prevent infection, from at least one remote computer.

6. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, information concerning empirically successful computer security practices explicitly transmitted to the central computer by at least one specific source organization.

7. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

reading, by the central computer, information concerning empirically successful computer security practices on at least one remote computer associated with at least one specific source organization.

8. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

monitoring, by the central computer, computer security practices utilized by the plurality of source organizations; and

inferring successful security practices based on results of utilizing the monitored computer security practices by the plurality of source organizations over time.

9. The method of claim 1 wherein receiving information concerning empirically successful computer security practices further comprises:

receiving, by the central computer, updated computer security practices utilized by the plurality of remote computers associated with the plurality of source organizations over time.

10. The method of claim 1 further comprising:

identifying specific information concerning empirically successful computer security practices to share with at least one specific target organization based on type of organization.

11. The method of claim 1 further comprising:

identifying specific information concerning empirically successful computer security practices to share with at least one specific target organization based on size of organization.

12. The method of claim 1 further comprising:

identifying specific information concerning empirically successful computer security practices to share with at least one specific target organization based on at least one specific computer security vulnerability which the identified security practices have been empirically successful protecting against for at least one source organization.

13. The method of claim 1 further comprising:

identifying specific information concerning empirically successful computer security practices to share with at least one specific target organization based on at least one specific computer security vulnerability to which the at least one specific target organization is subject.

14 The method of claim 1 wherein providing the identified specific information concerning empirically successful computer security practices to the at least one specific target organization further comprises:

transmitting, by the central computer, at least one recommendation concerning computer security practices to the at least one specific target organization.

15. The method of claim 1 wherein providing the identified specific information concerning empirically successful computer security practices to the at least one specific target organization further comprises:

automatically updating, by the central computer, security settings of at least one remote computer associated with the at least one specific organization.

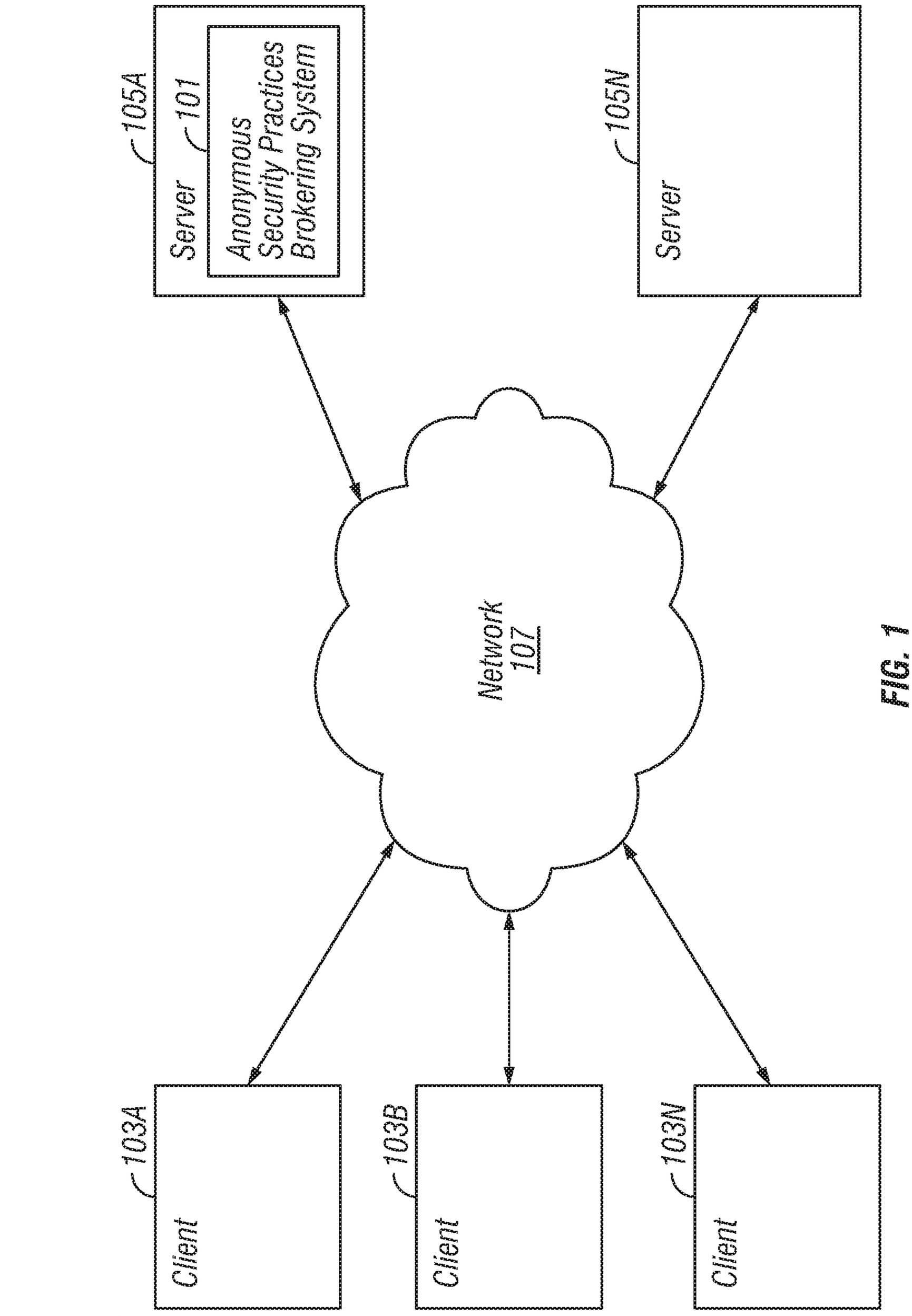
Network Architecture 100
Client 103A
Client 103B
Client 103N
Network 107
Server 105A
Anonymous Security Practices Brokering System 101
Server 105N

FIG. 1

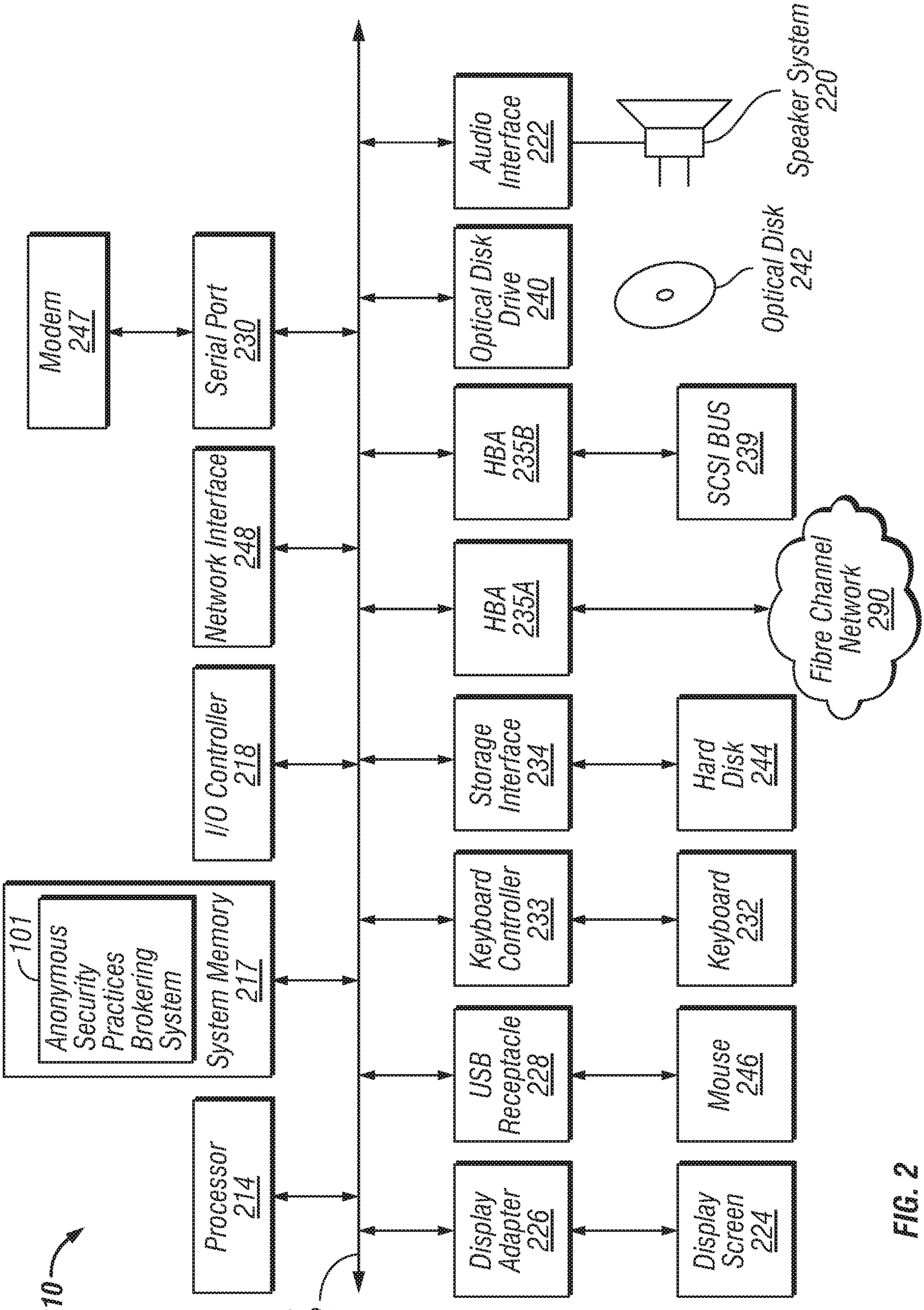
210
Processor 214
Bus 212
System Memory 217
101
Anonymous Security Practices Brokering System
I/O Controller 218
Network Interface 248
Serial Port 230
Modem 247
Display Adapter 226
Display Screen 224
USB Receptacle 228
Mouse 246
Keyboard Controller 233
Keyboard 232
Storage Interface 234
Hard Disk 244
HBA 235A
HBA 235B
SCSI BUS 239
Fibre Channel Network 290
Optical Disk Drive 240
Optical Disk 242
Audio Interface 222
Speaker System 220

FIG. 2

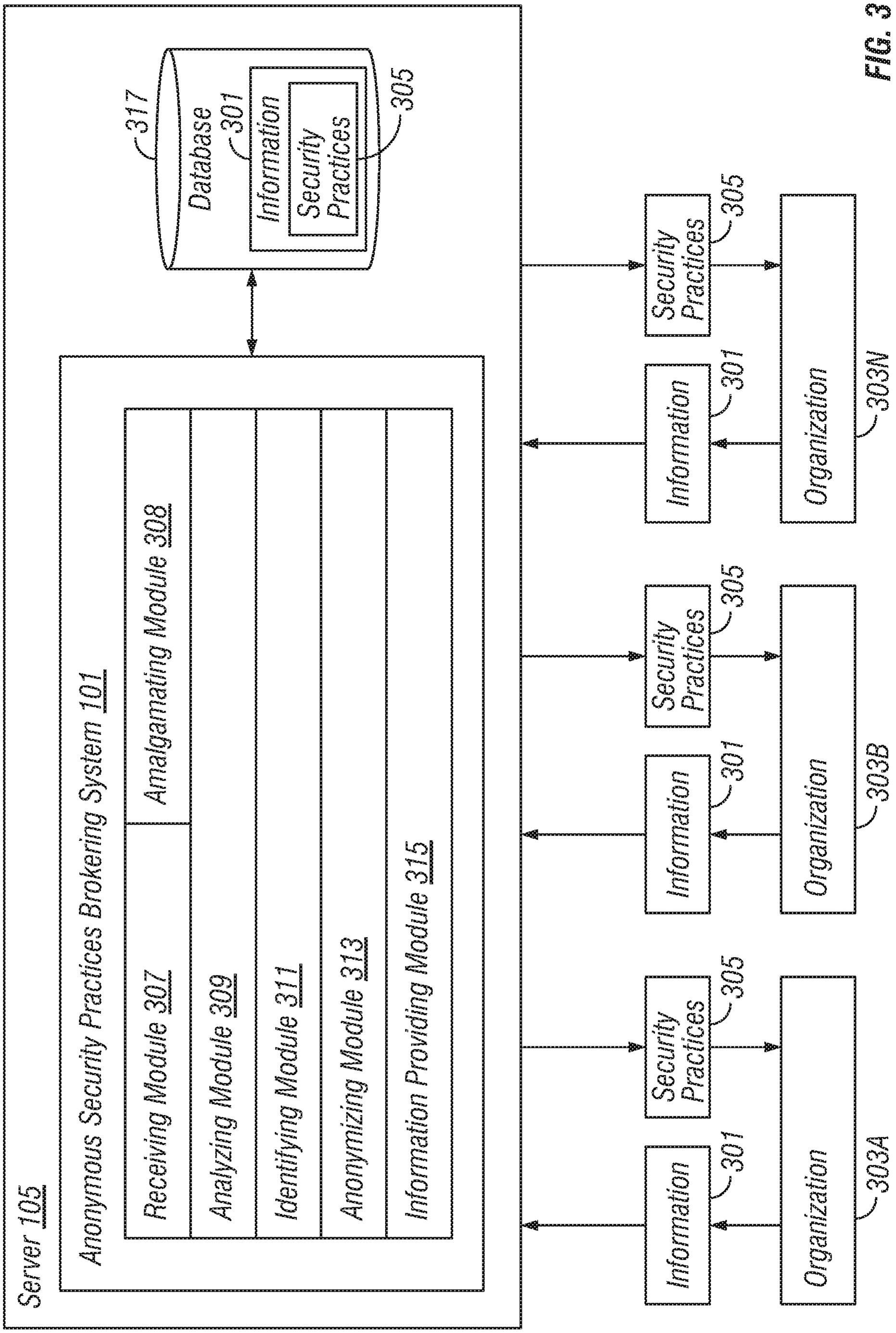
Server 105
Anonymous Security Practices Brokering System 101
Anonymous Security Practices Brokering Module 307
Amalgamating Module 308
Receiving Module 309
Analyzing Module 311
Identifying Module 313
Anonymizing Module 315
Information Providing Module 315
Database 317
Information 301
Security Practices 305
Organization 303N
303B
303A

FIG. 3

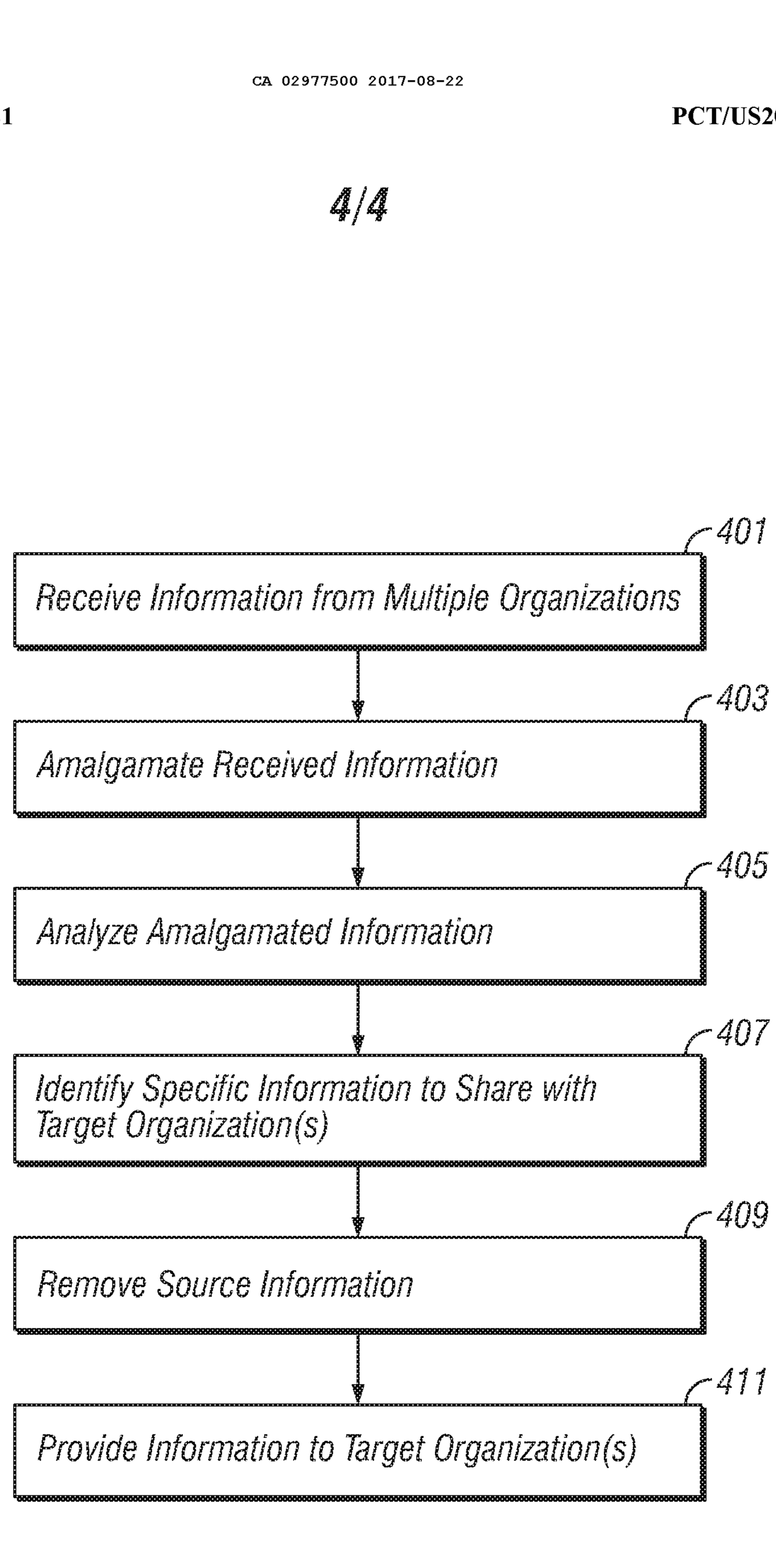
401
Receive Information from Multiple Organizations
403
Amalgamate Received Information
405
Analyze Amalgamated Information
407
Identify Specific Information to Share with Target Organization(s)
409
Remove Source Information
411
Provide Information to Target Organization(s)

FIG. 4

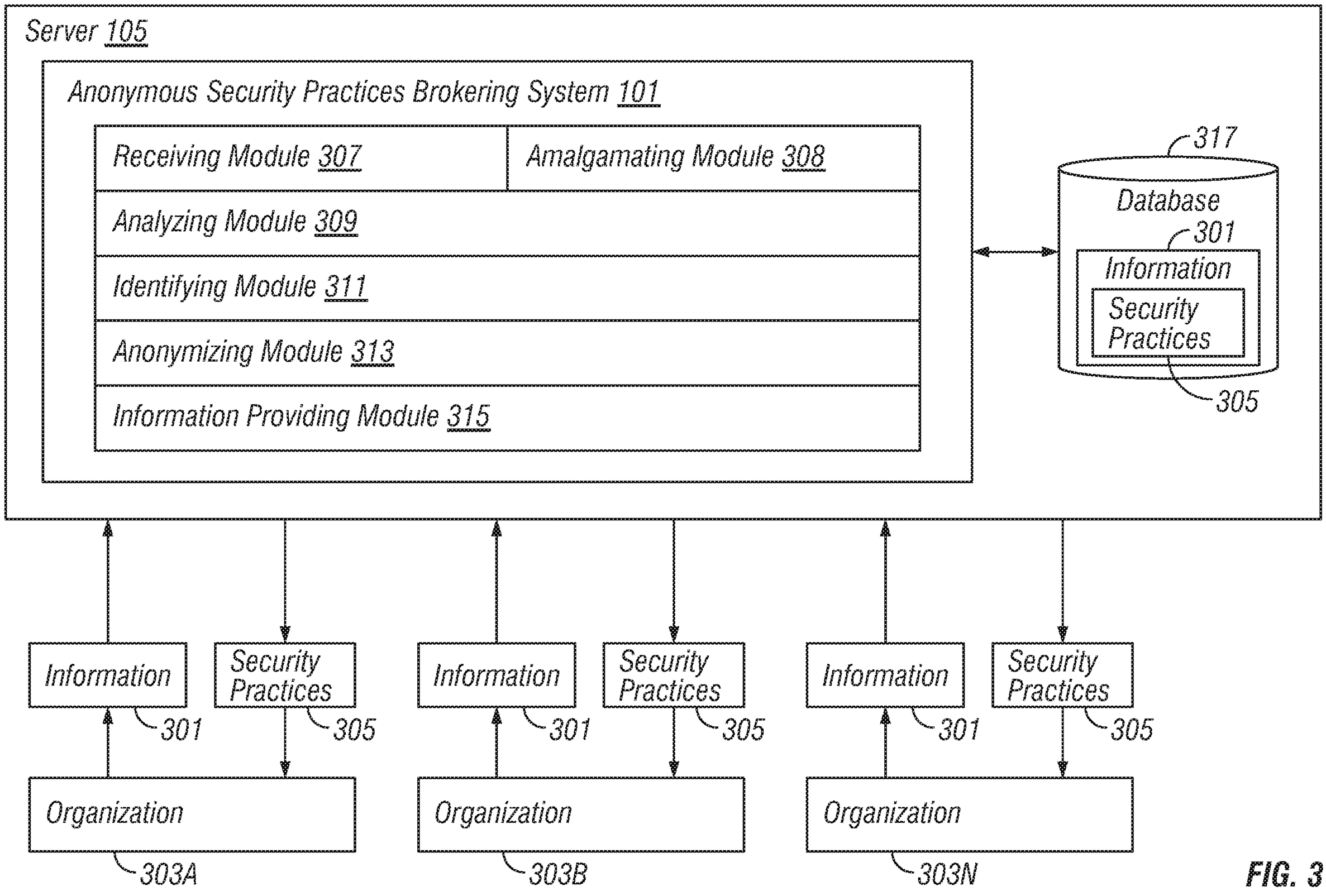
Server 105
Anonymous Security Practices Brokering System 101
Receiving Module 307
Amalgamating Module 308
Analyzing Module 309
Identifying Module 311
Anonymizing Module 313
Information Providing Module 315
317
Database
301
Information
Security Practices
305
Information
301
Security Practices
305
Organization
303A
Information
301
Security Practices
305
Organization
303B
Information
301
Security Practices
305
Organization
303N

FIG. 3