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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2008 (04.09.2008)

PCT

(10) International Publication Number
WO 2008/106295 A1

(51) International Patent Classification:
H04L 12/28 (2006.01) *H04L 12/66* (2006.01)

(21) International Application Number:
PCT/US2008/053506

(22) International Filing Date: 8 February 2008 (08.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/680,518 28 February 2007 (28.02.2007) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **MALAKAPALLI, Heher P.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **GUO, Donghang**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **SWAMINATHAN, Gautam**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **BEN-SHACHAR, Ido**; One Microsoft Way, Redmond, Washington 98052-6399 (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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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))*

[Continued on next page]

(54) Title: STRATEGIES FOR SECURELY APPLYING CONNECTION POLICIES VIA A GATEWAY

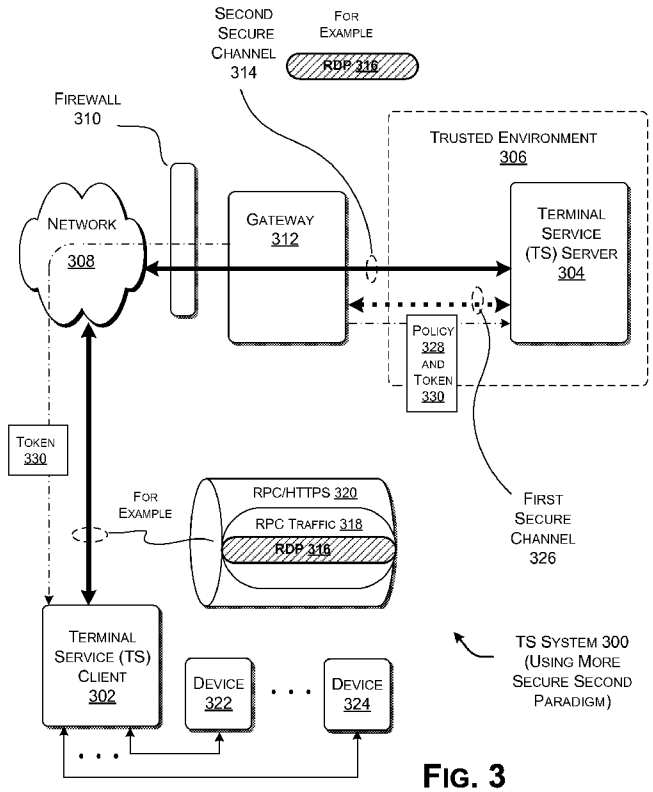

FIG. 3

(57) **Abstract:** A strategy is described for securely applying connection policies in a system that includes a first entity (e.g., a TS client) connected to a second entity (e.g., a TS server) via a gateway using a remote-operating protocol (e.g., RDP). The strategy involves establishing a first secure channel between the gateway and the TS server and transmitting policy information from the gateway to the TS server. The strategy then involves deactivating the first secure channel and setting up a second secure channel between the TS client and the TS server. The strategy uses the second secure channel to transmit RDP data from the TS client to the TS server. The TS server uses the previously-transmitted policy information to determine whether to enable or disable a feature that affects the TS client, such as device redirection.

WO 2008/106295 A1

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

STRATEGIES FOR SECURELY APPLYING CONNECTION POLICIES VIA A GATEWAY

BACKGROUND

[0001] A terminal service (TS) system allows a TS client to interact with an application being run on a remote TS server. A user who interacts with the application receives generally the same user experience that would be provided if the application were implemented locally by the TS client. Implementing the application on the TS server device affords a number of benefits. For instance, it may be easier to administer an application that is maintained at a central location.

[0002] In a first case, an organization (such as a corporation) may include a TS server that is accessible to a group of clients within the organization. In this scenario, the TS clients can access the TS server without special security provisions because the TS clients are presumed to be trusted entities. In a second case, the organization may wish to make its TS server available to another group of clients that are located outside the organization. For example, the organization may wish to allow employees to access its terminal server from their home via the Internet. In this scenario, the TS clients cannot access the TS server without special security provisions. According to one solution, the organization may use a gateway that sits behind a firewall to administer the interaction between external TS clients and the TS server.

[0003] However, there are potential vulnerabilities in above-described type of architecture. Consider the case of device redirection. In a TS system, device redirection allows a user who is interacting with a TS server to utilize devices that are associated with the TS server and devices that are associated with the TS client. For example, a user who is interacting with a word processing program that is being run on the TS server can specify that information is to be saved and retrieved from a storage device that is local with respect to the user's client device. This may allow a malicious user (or other entity) to potentially corrupt the data processing infrastructure of the organization by uploading viruses and the like to the TS server.

[0004] There is accordingly an exemplary need to improve the security of TS systems (and the like) that employ a gateway.

SUMMARY

[0005] A strategy is described for securely applying connection policies in a system that includes a first entity connected to a second entity via a gateway using a remote-operating protocol. The first entity can comprise a terminal service (TS) client, the second entity can comprise a TS server, and the remote-operating protocol can comprise Remote Desktop Protocol (RDP). The strategy involves establishing a first secure channel between the gateway and the TS server and transmitting policy information from the gateway to the TS server. The strategy then involves deactivating the first secure channel and setting up a second secure channel between the TS client and the TS server. The strategy uses the second secure channel to transmit RDP data from the TS client to the TS server. The TS server uses the previously-transmitted policy information to determine whether to enable or disable a feature that affects the TS client, such as device redirection.

[0006] The strategy confers a number of benefits. According to one exemplary benefit, the strategy allows a trusted TS server to enforce policy information that affects the TS client, rather than relying on the TS client (which may be malicious). According to another benefit, the strategy provides a centric management of policy; versus group policy, this facilitates each user policy management. According to another benefit, the additional secure channel is deployed between the gateway and the TS server; since these entities are "close," there is little extra delay for building up a connection.

[0007] Additional exemplary implementations and attendant benefits are described in the following.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Fig. 1 shows an exemplary terminal service (TS) system that uses a first paradigm to transmit data from a TS client to a TS server; the first paradigm may expose the TS system to malicious activity by the TS client.

[0009] Fig. 2 is a flowchart that illustrates an exemplary manner of operation of the TS system of Fig. 1.

[0010] Fig. 3 shows an exemplary TS system that uses a second paradigm to transmit data from a TS client to a TS server; the second paradigm provides safeguards against malicious activity by the TS client.

[0011] Fig. 4 is a flowchart that illustrates an exemplary manner of operation of the TS system of Fig. 3.

[0012] Figs. 5 and 6 show one exemplary implementation of the TS system of Fig. 3.

[0013] Fig. 7 shows exemplary processing functionality that can be used to implement any aspect of the systems of Figs. 3 and 5.

[0014] The same numbers are used throughout the disclosure and figures to reference like components and features. Series 100 numbers refer to features originally found in Fig. 1, series 200 numbers refer to features originally found in Fig. 2, series 300 numbers refer to features originally found in Fig. 3, and so on.

DETAILED DESCRIPTION

[0015] This disclosure sets forth a strategy for securely applying connection policies in a system that includes a first entity connected to a second entity via a gateway using a remote-operating protocol. The strategy can be manifested in various systems, apparatuses, modules, procedures, storage mediums, data structures, and other forms.

[0016] This disclosure includes the following sections. Section A describes an exemplary system for transmitting data using a first paradigm. The first paradigm may expose the system to certain security threats. Section B describes an exemplary system for transmitting data using a second paradigm. The second paradigm provides enhanced security compared to the first paradigm. Section C describes exemplary processing functionality that can be used to implement any aspect of the systems described in Sections A and B.

[0017] As a preliminary note, any of the functions described with reference to the figures can be implemented using software, firmware, hardware (e.g., fixed logic circuitry), manual processing, or a combination of these implementations. The term "logic, "module," "component," "system" or "functionality" as used herein generally represents software, firmware, hardware, or a combination of the

elements. For instance, in the case of a software implementation, the term "logic," "module," "component," "system," or "functionality" represents program code that performs specified tasks when executed on a processing device or devices (e.g., CPU or CPUs). The program code can be stored in one or more computer readable memory devices.

[0018] More generally, the illustrated separation of logic, modules, components, systems, and functionality into distinct units may reflect an actual physical grouping and allocation of software, firmware, and/or hardware, or can correspond to a conceptual allocation of different tasks performed by a single software program, firmware program, and/or hardware unit. The illustrated logic, modules, components, systems, and functionality can be located at a single site (e.g., as implemented by a processing device), or can be distributed over plural locations.

[0019] The terms "machine-readable media" or the like refers to any kind of medium for retaining information in any form, including various kinds of storage devices (magnetic, optical, static, etc.). The term machine-readable media also encompasses transitory forms for representing information, including various hardwired and/or wireless links for transmitting the information from one point to another.

[0020] Certain aspects of the technology set forth herein are explained in flow chart form. In these flow charts, certain operations are described as constituting distinct blocks performed in a certain order. Such implementations are exemplary and non-limiting. Certain blocks can be grouped together and performed in a single operation, and certain blocks can be performed in an order that differs from the illustrated order. The blocks shown in the flowcharts can be implemented by software, firmware, hardware, manual processing, any combination of these implementations.

[0021] Certain aspects of the technology set forth herein are explained in the context of a terminal service (TS) system that uses a remote operating protocol. For example, without limitation, the technology can be implemented using the Remote Desktop Protocol (RDP). A TS system using RDP allows a TS client to interact with one or more applications maintained on a remote TS server. The user

receives the same user experience that would be provided if the applications were being locally run on the TS client. While the following explanation uses the terms "TS client" (instead of "first entity"), "TS server" (instead of "second entity"), and "RDP" (instead of "remote operating protocol"), it should be noted that the principles described herein can be applied to other implementations.

A. System and Method Using First Paradigm

[0022] Fig. 1 shows a TS system 100 for transmitting RDP data between a TS client 102 and a TS server 104 using a first paradigm. As noted above, the first paradigm may expose the system 100 to certain malicious activity that the TS client 102 may perform. Thus, Section A mainly acts as a vehicle for more effectively communicating the solutions described in the next section.

[0023] The TS server 104 is provided within a trusted environment 106. The trusted environment 106 may correspond to a data processing infrastructure provided by any type of organization, such as a corporation, educational institution, governmental institution, and so on. Although not shown, the trusted environment 106 may generally include a collection of server computers, networks (such as intranets), "internal" clients, routers, data storage devices, and so on. The trusted environment 106 is trusted in the sense that there is an expectation that entities that interact with the TS server 104 from within the trusted environment 106 can be generally relied on to not deliberately cause damage to the trusted environment 106.

[0024] The TS client 102 is external to the trusted environment 106. For example, the TS client 102 may represent any type of client device that interacts with the TS server 104 via a network 108. For example, the client device 102 can comprise a personal computer, a laptop computer, a personal digital assistant (PDA), a stylus-type input device, a mobile telephone, a game console, a set-top box associated with a television set, and so on. The network 108 can comprise any type of communication mechanism that is not under the control of the trusted environment 106. For example, the network 108 can comprise the Internet.

[0025] The TS system 100 uses a firewall 110 and a gateway 112 to allow the external TS client 102 to access the TS server 104. The firewall 110 can comprise

a conventional mechanism for restricting the type of data being transmitted to the trusted environment 106 based on predefined rules. The gateway 112 acts as a proxy for forwarding RDP data between the TS client 102 and the TS server 104. The gateway 112 applies various policies which govern what actions are allowed and disallowed when interacting with external TS clients.

[0026] The system 102 can use a single secure channel 114 to transmit RDP data between the TS client 102 and the TS server 104. The RDP data that is sent over this channel 114 is encrypted, so it cannot be acted upon by any entity midstream between the TS client 102 and the TS server 104.

[0027] TS technology includes a feature referred to in the art as device redirection. First, consider the use of device redirection for clients within the trusted environment 106. When a user is interacting with an application being run on the TS server 104, device redirection allows the user to access devices associated with the TS server 104 as well as devices associated with the internal TS client. More specifically, the TS server 104 may have various devices associated therewith, such as various storage devices (associated with various drives), various printing devices, various scanning devices, various audio input and output devices, and so forth. Likewise, the internal TS client may have various devices associated therewith, including the same kinds of devices mentioned above. Device redirection allows a user to interact with any of these devices in the course of a TS session. For example, consider the case in which the user is using an internal TS client to interact with a word processing program being run on the TS server 104. The user can store and retrieve documents to/from storage locations that are considered local to the TS server 104. But the user can also store and retrieve documents to/from storage locations that are considered local to the internal client.

[0028] Device redirection that occurs within the confines of the trusted environment 106 may not pose a significant risk. This is because, as stated above, the users and components within the trusted environment 106 are trusted to not deliberately cause damage to the trusted environment 106. However, device redirection in the context of the external TS client 102 may pose a risk. This is

because the TS client 102 is situated outside the trusted environment 106, and therefore may be untrustworthy.

[0029] Consider the specific scenario in which the TS client 102 includes local devices (116, ... 118). A malicious user who is operating the TS client 102 can potentially introduce destructive code into the trusted environment 106 through the use of device redirection. For instance, consider the above example in which the user is interacting with a word processing program on the TS server 104 and wishes to retrieve a document from a drive that is local to a TS client. If this document contains destructive code or other harmful content, it can potentially cause damage to the TS server 104 or other parts of the trusted environment 106.

[0030] In certain circumstances, it may therefore be desirable to disable device redirection for the external TS client 102. Fig. 1 shows a first paradigm for accomplishing this result. However, the first paradigm has potential shortcomings. As will be explained below, there is a risk that a malicious external TS client can circumvent the provisions of the first paradigm and still cause damage to the trusted environment 106.

[0031] According to the first paradigm, the gateway 112 transmits policy information 120 to the TS client 102. The policy information 120 conveys the status of one or more features of a TS session between the TS client 102 and the TS server 104. For example, the policy information 120 can indicate whether these features are enabled or disabled. In the specific context of device redirection, the policy information 120 can be used to indicate that device redirection is disabled for external TS client 102. The policy information 120 can be expressed in various formats, such as a collection of one or more flags.

[0032] The first paradigm is based on the expectation that the TS client 102 will forward the policy information 120 (or information derived therefrom) to the TS server 104 at the start of sending RDP data to TS server 104. (The RDP data reflects the normal flow of data that enables the TS client 102 to interact with the TS server 104.) The first paradigm is based on the further expectation that the TS server 104, upon receiving the policy information 120, will take appropriate action based on the status information contained therein. For example, if the policy

information 120 informs the TS server 104 that it should disable device redirection, the TS server 104 will prevent the external TS client 102 from using device redirection.

[0033] Because the TS client 102 is external to the trusted environment 106, it cannot necessarily be trusted. As such, the TS client 102 may fail to carry out its proper role in forwarding the policy information 120 to the TS server 104. Alternatively, the TS client 102 can send tampered policy information 120 to the TS server 104. For example, the TS client 102 can change the policy information 102 to indicate that device redirection is enabled (when it should, in fact, be disabled). This will cause the TS server 104 to enable device redirection, which, in turn, provides an avenue through which the TS client 102 can upload destructive code to the TS server 104.

[0034] Fig. 2 is a procedure 200 which summarizes the above-described operation of the TS system 100.

[0035] In block 202, the gateway 112 sends the policy information 120 to the external TS client 102.

[0036] In block 204, the TS client 102 connects to the TS server 104 via the gateway 112 to conduct a TS session, e.g., involving the exchange of RDP data.

[0037] In block 206, the TS client 102 is expected to transmit the policy information to the TS server 104 when it starts sending RDP data. As described above, a malicious TS client 102 can subvert this operation in various ways.

[0038] In block 208, the TS server 104 receives the policy information 120 and the RDP data. The TS server 104 conducts a TS session based the policy information 120. As described above, the policy information 120 may have the effect of enabling or disabling one or more features of a TS session, such as such as device redirection.

[0039] Note that, while the gateway 112 performs a role in policing the interaction between external TS clients and the TS server 104, the gateway 112 cannot gain direct access to the RDP data. This is because the RDP data is encrypted en route between the TS client 102 and the TS server 104. This presents

various constraints on the use of the gateway 112 to directly disable device redirection.

B. System and Method Using Second Paradigm

[0040] A TS system 300 of Fig. 3 uses a second paradigm to transfer RDP data from a client 302 to a TS server 304. For frame of reference, the first TS system 100 of Fig. 1 was client-centric in the sense that it relied on the TS client 102 to disable device redirection. The solution provided in Fig. 3 is server-centric in the sense that it relies on the TS server 304 alone to disable device redirection. Since the TS server 304 is situated within a trusted environment 306, the second paradigm can more reliably disable device redirection compared to the first paradigm.

[0041] At the outset, it should be noted that the TS system 300 of Fig. 3 is described in the specific context of the disablement of device redirection. However, the TS paradigm can be applied to affect the status of any aspect of a TS session. In one general case, for instance, the second paradigm can allow the TS server 304 to disable any identified type of packet within the RDP data.

[0042] The TS system 300 of Fig. 3 includes a similar contextual setting to the TS system 100 of Fig. 100. Namely, the TS client 302 interacts with the TS server 304 in the trusted environment 306. The TS client 302 can access the TS server 304 via a network 308 (such as the Internet), firewall 310, and gateway 312. Without limitation, according to one exemplary implementation, certain aspects of the gateway 312 of Fig. 3 can be implemented using technology described in co-pending U.S. Applications: (1) U.S Serial No. 11/326,992, filed on January 5, 2006, entitled "Providing Consistent Application Aware Firewall Traversal"; and (2) U.S. Serial No. 11/067,125, filed on February 25, 2005, entitled "Enabling Terminal Services through a Firewall." Both of these applications are incorporated by reference herein in their respective entireties.

[0043] The TS client 302 can exchange RDP data with the TS server 304 via a second secure channel 314. (This channel is called a "second" channel to distinguish it from a first channel which is established temporally prior to the second channel 314, to be explained in greater detail below). According to one

exemplary implementation, to transmit RDP data 316 to the TS server 304, the TS system 300 can first wrap the RDP data 316 in an RPC-based protocol 318 (where RDC denotes Remote Procedure Call). This information, in turn, can then be layered over an HTTPS protocol 320 (where HTTPS denotes Hypertext Transfer Protocol Security). Prior to reaching the TS server 304, the TS system 300 can strip off the various layers to yield the RPC data 316 itself. Generally, the RDP data 316 transmitted via the second channel 314 is secure. For example, the RDP data can be protected using SSL (where SSL denotes Secure Socket Layers).

[0044] The TS client 302 can interact with one or more local devices, such as devices (322, ... 324). These devices (322, ... 324) can include local storage devices, printers, audio input and output devices, and so forth.

[0045] Now the features of the second paradigm will be set forth in greater detail. First note that the TS system 300 establishes a first secure channel 326 between the gateway 312 and the TS server 304. This channel 326 is used to transfer policy information 328 to the TS server 304 prior to the exchange of RDP data using the second channel 314. The policy information 328 conveys information regarding one or more features that affect the exchange of RDP data between the TS client 302 and the TS server 304. In one non-limiting case, the policy information 328 includes an instruction to disable device redirection for the TS client 302.

[0046] Like the second channel 314, the first channel 326 is secure. For instance, the TS system 300 can encrypt the information being transmitted via the first channel 326. In one implementation, the TS system 300 uses SSL for the first channel 326.

[0047] The TS system 300 deactivates the first channel 326 before sending the RDP data using the second channel 314. Upon receipt of the RDP data via the second channel 314, the TS server 304 enables or disables certain features in accordance with the instructions conveyed by the policy information 328. Note that the exchange of policy information 328 to the TS server 304 does not rely on the good-faith actions of the TS client 302. Thus, the second paradigm is potentially more secure than the first paradigm used by the first TS system 100.

[0048] Each TS session is governed by associated policy information. Thus, the TS system 300 may apply first policy information to a first TS client and second policy information to a second TS client, and so on. Further, the policy information may optionally be specific to each connection, such that the same TS client may receive first policy information when it connects to the TS server 304 at time X and receive second policy information when it connects to the TS server 304 at time Y.

[0049] To address the above issue, the gateway 312 can send a token 330 to the TS client 302 when the TS client 302 requests a connection with the TS server 304. The role of the token 330 is to identify the TS client 302. When the gateway 312 forwards the policy information 328 to the TS server 304, it can also forward the token 330 assigned to this particular TS client 302 (and this particular connection). The TS server 304 can subsequently use the token 330 to apply the correct policy information 328 to the TS client 302.

[0050] Fig. 4 shows a procedure 400 which summarizes the above-described operation of the TS system 300.

[0051] In block 402, the TS client 302 requests a connection to the TS server 304 to conduct an RDP session with the TS server 304.

[0052] In block 404, the gateway 312 passes the token 330 to the TS client 302. The token 330 is used to identify the TS client 302.

[0053] In block 406, the gateway 312 and the TS server 304 establish the first secure channel 326. Through this channel 326, the gateway 312 sends the policy information 328 and token information 330 to the TS server 304. The policy information 328 identifies features of an RDP session which are enabled or disabled with respect to the particular TS client 302 and the particular connection, as identified by the token 330.

[0054] In block 408, the TS system 300 closes the first channel 326 and establishes the second channel 314.

[0055] In block 410, the TS client 302 sends RDP data with the token 330 to the TS server 304 via the second channel 314. The TS server 304 can apply the correct policy information 328 to the TS client 302 according to the token 330.

[0056] In block 412, the TS server 304 can govern the ensuing exchange of RDP data based on the instructions contained in the policy information 328. In one particular case, this may involve disabling device redirection. This reduces the possibility that the TS client 302 can corrupt the trusted environment 306 through its local devices (322, … 324).

[0057] Figs. 5 and 6 shows one exemplary implementation of the principles set forth in Figs. 3 and 4.

[0058] Fig. 5 indicates that the gateway 312 can include a protocol module 502 and a gateway security filter module 504. These components are relevant to the secure transfer of RDP data described herein. The policy module 502 generates the policy information 328 and the token 330. The gateway security filter module 504 establishes secure exchange of information from the perspective of the gateway 312. That is, the gateway security filter module 504 generates a security context and performs encryption and decryption.

[0059] The TS server 306 can include a negotiation module 506 and a server security filter module 508. These components are relevant to the secure transfer of RDP data described herein. The negotiation module 506 acts on information sent to the TS server 306 in a manner set forth more fully below in the context of Fig. 6 below. The server security filter module 508 establishes secure exchange of information in the TS system 300 from the perspective of the TS server 304. (Although not shown, the TS client 302 includes a client security filter module for establishing the secure exchange of information from the perspective of the TS client 302.)

[0060] Fig. 6 shows how the components set forth in Fig. 5 interact with each other, according to one exemplary implementation. The operations in Fig. 6 are numbered based on an exemplary order in which these operations can be performed. The ordering of these operations can be modified in various ways.

[0061] In operation (1), the TS client 302 issues a channel creation request to the gateway 312.

[0062] In operation (2), the gateway 312 generates the token 330 and sends the token 330 to the TS client 302. The token 330 can be expressed as a unique GUID.

[0063] In operation (3), the gateway 312 activates the gateway security filter module 504.

[0064] In operation (4), the gateway security filter module 504 sends a SSL hello to the TS server 304.

[0065] In operation (5), the server negotiation module 506 recognizes the SSL hello message and activates the server security filter module 508.

[0066] In operation (6), an SSL handshake occurs between the gateway 312 and the TS server 306 to establish the first secure channel 326. Schannel can be used for this security channel 326.

[0067] In operation (7), the gateway 312 generates policy information 328. In this example, the policy information 328 takes the form a device redirection data unit. The gateway 312 sends the device redirection data unit to the TS server 304 along with the token 330.

[0068] In operation (8), the gateway 312 sends a reset command to the TS server 304.

[0069] In operation (9), the TS server 304 instructs the server security filter module 508 to be ready for restarting.

[0070] In operation (10), the TS client 302 sends messages to the TS server 304 via the gateway 312. More specifically, a first message sent by the TS client 302 is a protocol negotiation message or a SSL hello. This message will pass through the gateway security filter module 504 and the server security filter module 508. This message can possibly reach the gateway 312 before the gateway/server authentication. If so, the message remains waiting to be handled.

[0071] In operation (11), the gateway 312 deactivates the gateway security filter module 504 after sending out the above-described message (in operation 10).

[0072] In operation (12), the TS client 302 and the TS server 204 perform authorization to establish the second channel 314.

[0073] In operation (13), the TS client 302 sends a first RDP packet along with the stored token 330 to the TS server 304.

[0074] In operation (14), the TS server 304 enables or disables device redirection based on the policy information 328 and the token 330.

C. Exemplary Processing Functionality

[0075] Fig. 7 sets forth exemplary processing functionality 702 that can be used to implement any aspect of systems shown in Figs. 3 and 5. In one non-limiting case, for instance, the processing functionality 702 may represent any TS client, any TS server, any computer used by the gateway, and so on.

[0076] The processing functionality 702 can include various volatile and non-volatile memory, such as RAM 704 and ROM 706, as well as one or more central processing units (CPUs) 708. The processing functionality 702 can perform various operations identified above when the CPU 708 executes instructions that are maintained by memory (e.g., 704, 706, or elsewhere). The processing functionality 702 also optionally includes various media devices 710, such as a hard disk module, an optical disk module, and so forth.

[0077] The processing functionality 702 also includes an input/output module 712 for receiving various inputs from the user (via input devices 714), and for providing various outputs to the user (via output devices 716). One particular output device may include a display apparatus and an associated graphical user interface (GUI) 718. The processing functionality 702 can also include one or more network interfaces 720 for exchanging data with other devices via one or more communication conduits 722. One or more communication buses 724 communicatively couple the above-described components together.

[0078] The communication conduits 722 can be implemented in different ways to suit different technical and commercial environments. For instance, the communication conduits 722 can include any kind of network (or combination of networks), such as a wide area network (e.g., the Internet), an intranet, Digital Subscriber Line (DSL) network infrastructure, point-to-point coupling infrastructure, and so on. In the case where one or more digital networks are used to exchange information, the communication conduits 722 can include various hardwired and/or wireless links, routers, gateways, name servers, and so on. The communication conduits 722 can be governed by any protocol or combination of protocols.

[0079] In closing, a number of features were described herein by first identifying exemplary problems that these features can address. This manner of explication does not constitute an admission that others have appreciated and/or articulated the problems in the manner specified herein. Appreciation and articulation of the problems present in the relevant art(s) is to be understood as part of the present invention.

[0080] More generally, although the invention has been described in language specific to structural features and/or methodological acts, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claimed invention.

CLAIMS

What is claimed is:

1. A method for securely transmitting data from a first entity to a second entity via a gateway using a remote-operating protocol, comprising:

establishing a first secure channel between the gateway and the second entity (406);

receiving policy information from the gateway at the second entity via the first secure channel, the policy information identifying a manner in which the second entity is to interact with first entity (406);

establishing a second secure channel between the first entity and the second entity (408);

receiving data at the second entity from the first entity via the second secure channel (412); and

taking action on the data at the second entity based on the policy information which was previously transmitted from the gateway to the second entity (412).

2. The method of claim 1, wherein the remote-operating protocol is Remote Desktop Protocol (RDP).

3. The method of claim 1, wherein the first entity is a terminal service (TS) client and the second entity is a TS server.

4. The method of claim 1, wherein the first secure channel is formed as a Secure Sockets Layer (SSL) channel.

5. The method of claim 1, wherein the second secure channel is formed as a Secure Sockets Layer (SSL) channel.

6. The method of claim 1, further comprising deactivating the first secure channel prior to transmitting the data to the second entity using the second secure channel.

7. The method of claim 1, where the policy information indicates whether a feature that affects the first entity should be enabled or disabled.

8. The method of claim 7, wherein the feature is device redirection.

9. The method of claim 7, wherein the feature is associated with at least one packet of the remote-operating protocol.

10. The method of claim 1, wherein the data received via the second secure channel includes a token that has been previously sent from the gateway to the first entity, wherein the second entity uses the token to identify the first entity.

11. One or more machine-readable media containing machine-readable instruction ns for implementing the method of claim 1.

12. One or more computing devices, comprising:

one or more processors; and

memory to store computer-executable instructions that, when executed by the one or more processors, perform the method of claim 1.

13. A method for securely transmitting data from a terminal service (TS) client to a TS server via a gateway using a remote-operating protocol, comprising:

establishing a first secure channel between the gateway and the TS server (406);

sending policy information from the gateway to the TS server via the first secure channel, the policy information identifying a manner in which the TS server is to interact with the TS client (406);

deactivating the first secure channel (408); and

sending data to the TS server via a second secure channel (410).

14. The method of claim 13, further comprising sending a token from the gateway to the TS client.

15. The method of claim 14, wherein the data sent to the TS server includes the token previously sent to the TS client, wherein the token is used by the TS server to associate the policy information with the TS client.

16. One or more machine-readable media containing machine-readable instructions for implementing the method of claim 13.

17. One or more computing devices, comprising:

one or more processors; and

memory to store computer-executable instructions that, when executed by the one or more processors, perform the method of claim 13.

18. A system (300) for securely transmitting data using a remote-operating protocol, comprising:

a terminal service (TS) server (304); and

a gateway (312) for proxying the data between at least one TS client (302) and the TS server (304),

wherein the system (300) is configured to establish a first secure channel (326) between the gateway (312) and the TS server (304) to transmit policy information (328) from the gateway (312) to the TS server (304),

wherein the system (300) is configured to establish a second secure channel (314) between said at least one TS client (302) and the TS server (304) to receive data from said at least one client (302),

wherein the TS server (304) is configured to take action on the received data based on the policy information (328) which was previously transmitted from the gateway (312).

19. The system of claim 18, wherein the remote-operating protocol is Remote Desktop Protocol (RDP).

20. The system of claim 18, wherein the TS server is configured to receive a token from said at least one TS client along with the data, wherein the TS server is configured to use the token to associate the policy information with the TS client.

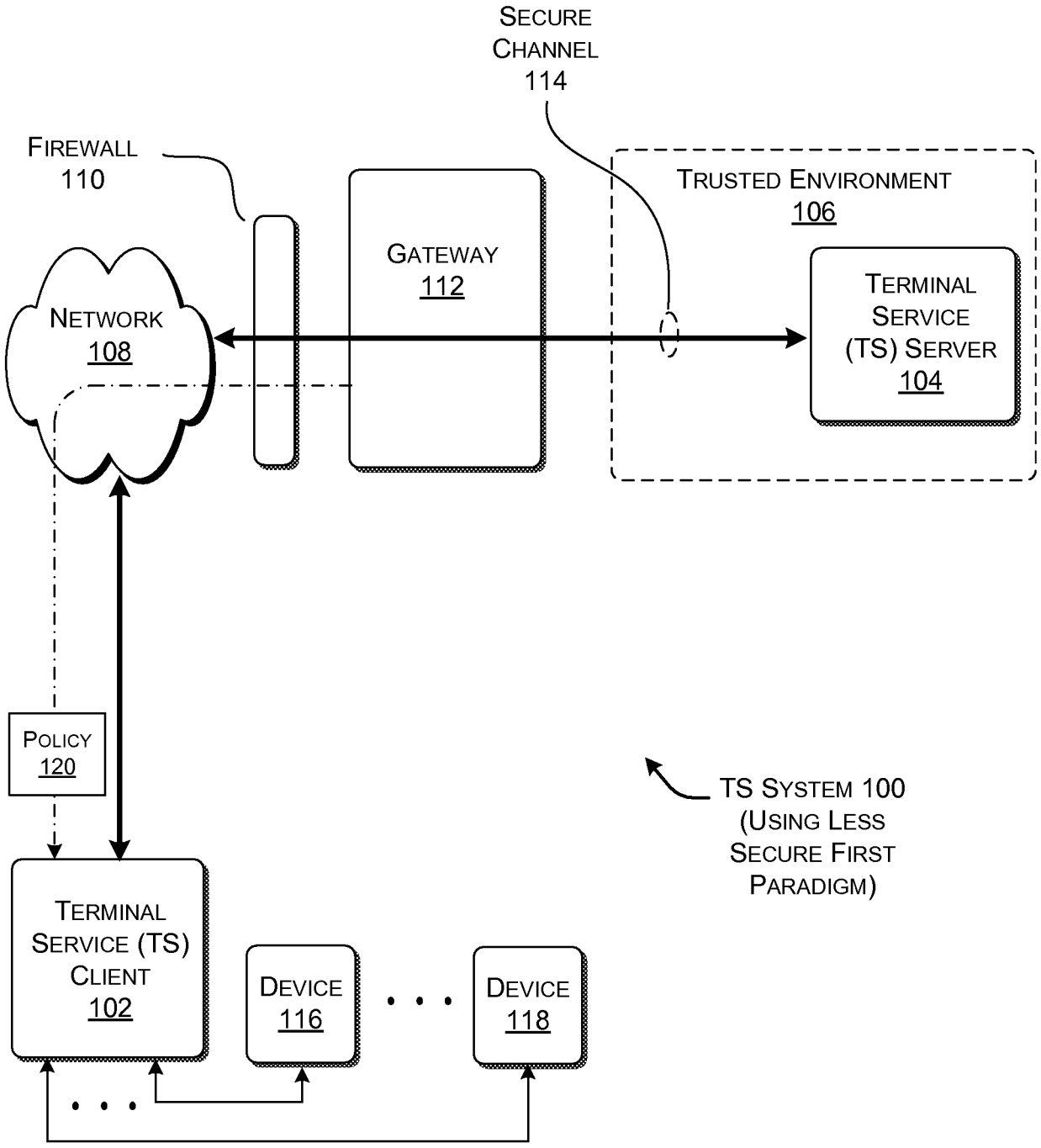
SECURE CHANNEL 114
FIREWALL 110
TRUSTED ENVIRONMENT 106
GATEWAY 112
NETWORK 108
TERMINAL SERVICE (TS) SERVER 104
POLICY 120
TS SYSTEM 100 (USING LESS SECURE FIRST PARADIGM)
TERMINAL SERVICE (TS) CLIENT 102
DEVICE 116
DEVICE 118

FIG. 1

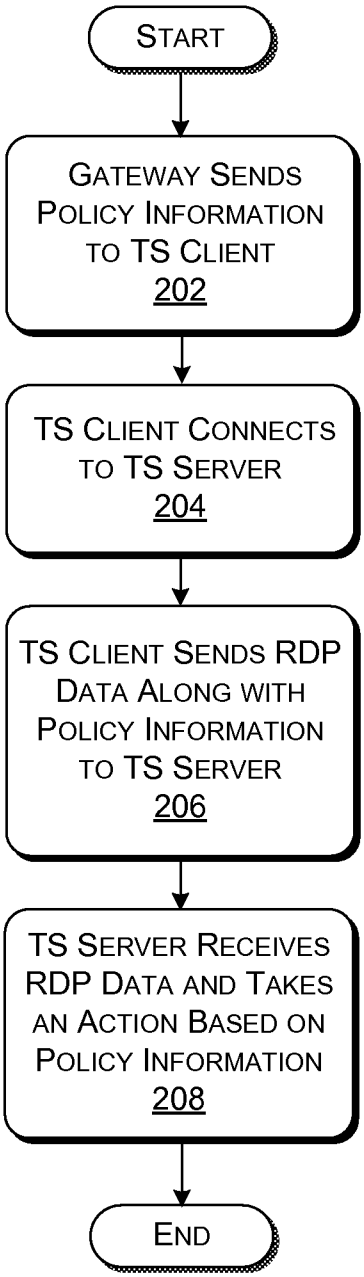
START
GATEWAY SENDS POLICY INFORMATION TO TS CLIENT
202
TS CLIENT CONNECTS TO TS SERVER
204
TS CLIENT SENDS RDP DATA ALONG WITH POLICY INFORMATION TO TS SERVER
206
TS SERVER RECEIVES RDP DATA AND TAKES AN ACTION BASED ON POLICY INFORMATION
208
END
POTENTIALLY INSECURE OPERATION
200

FIG. 2

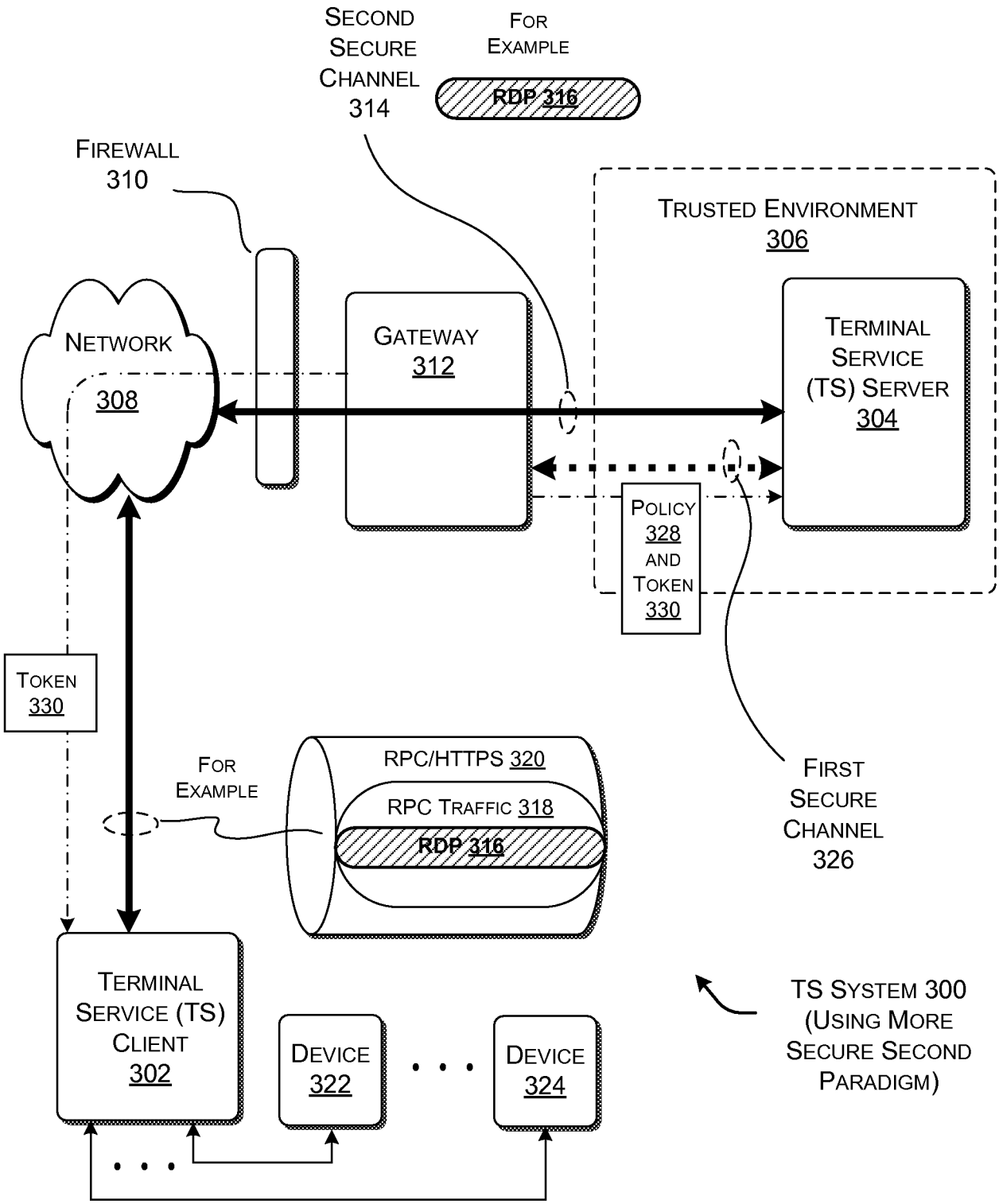
SECOND SECURE CHANNEL 314
FOR EXAMPLE
RDP 316
FIREWALL 310
TRUSTED ENVIRONMENT 306
NETWORK 308
GATEWAY 312
TERMINAL SERVICE (TS) SERVER 304
POLICY 328 AND TOKEN 330
TOKEN 330
FOR EXAMPLE
RPC/HTTPS 320
RPC TRAFFIC 318
RDP 316
FIRST SECURE CHANNEL 326
TERMINAL SERVICE (TS) CLIENT 302
DEVICE 322
DEVICE 324
TS SYSTEM 300 (USING MORE SECURE SECOND PARADIGM)

FIG. 3

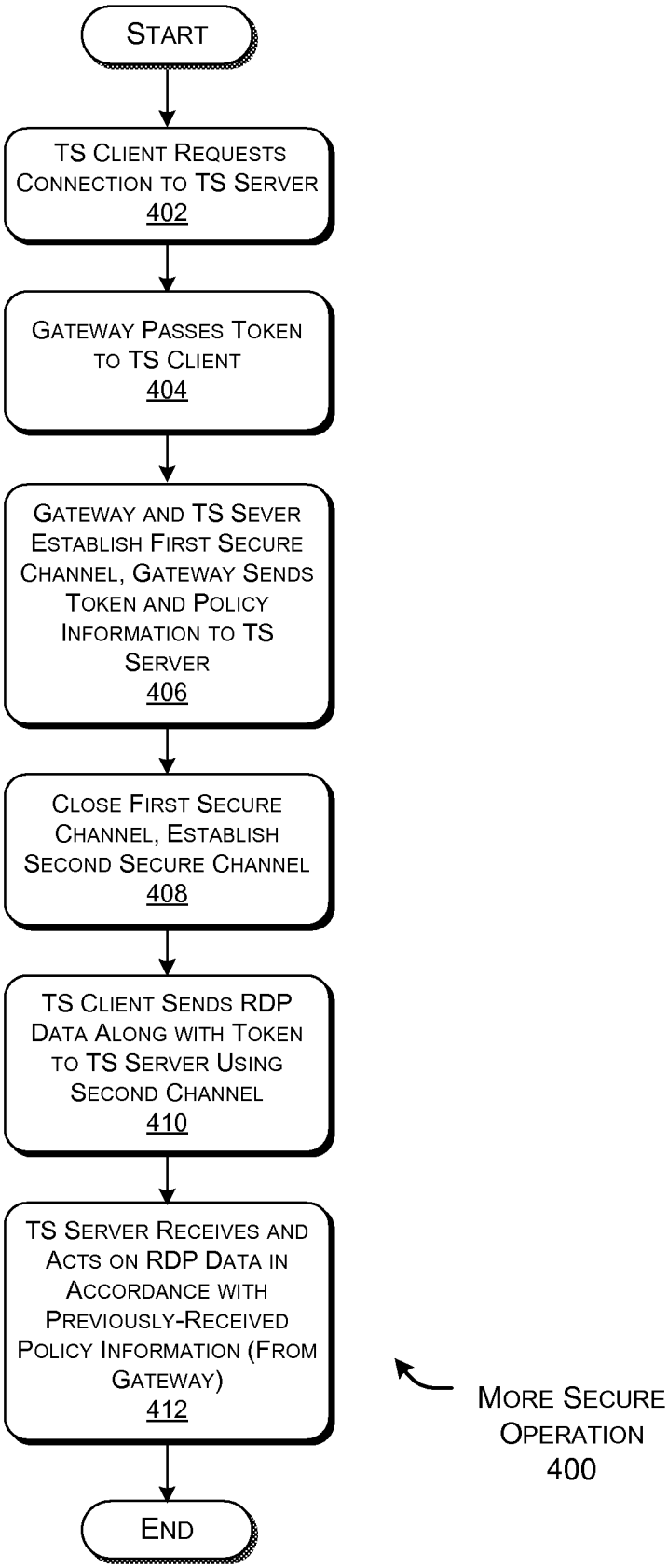
START
TS CLIENT REQUESTS CONNECTION TO TS SERVER
402
GATEWAY PASSES TOKEN TO TS CLIENT
404
GATEWAY AND TS SEVER ESTABLISH FIRST SECURE CHANNEL, GATEWAY SENDS TOKEN AND POLICY INFORMATION TO TS SERVER
406
CLOSE FIRST SECURE CHANNEL, ESTABLISH SECOND SECURE CHANNEL
408
TS CLIENT SENDS RDP DATA ALONG WITH TOKEN TO TS SERVER USING SECOND CHANNEL
410
TS SERVER RECEIVES AND ACTS ON RDP DATA IN ACCORDANCE WITH PREVIOUSLY-RECEIVED POLICY INFORMATION (FROM GATEWAY)
412
MORE SECURE OPERATION
400
END

FIG. 4

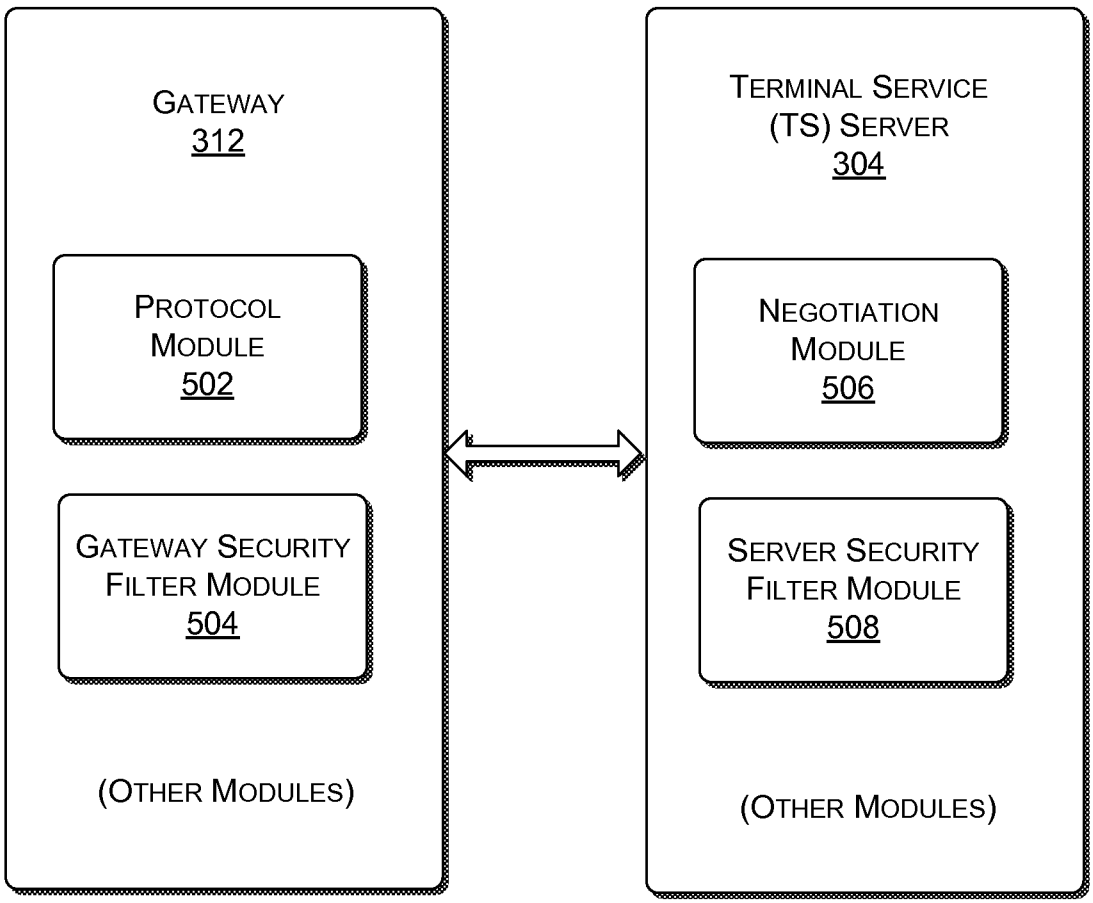
GATEWAY
312
PROTOCOL MODULE
502
GATEWAY SECURITY FILTER MODULE
504
(OTHER MODULES)
TERMINAL SERVICE (TS) SERVER
304
NEGOTIATION MODULE
506
SERVER SECURITY FILTER MODULE
508
(OTHER MODULES)

FIG. 5

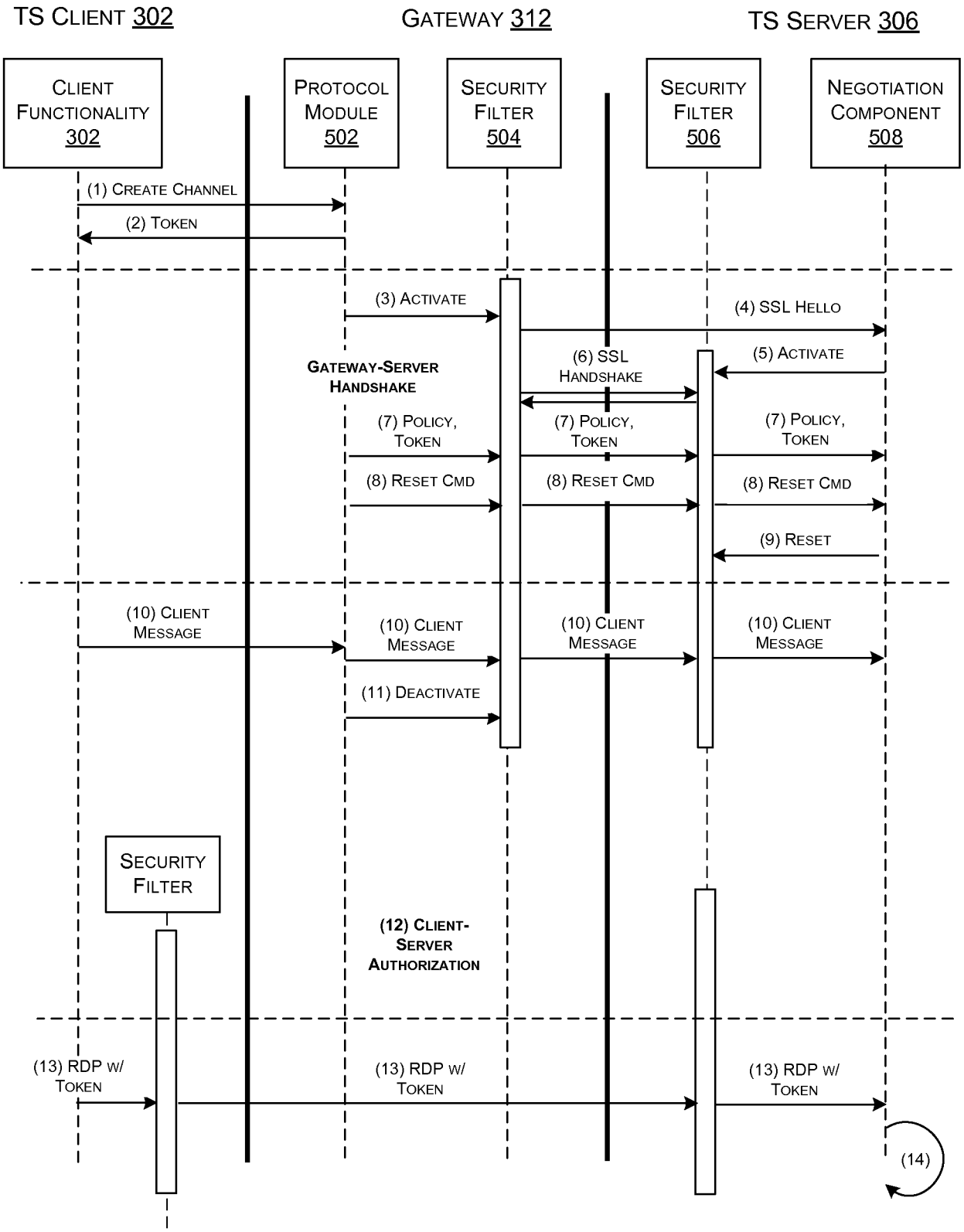
TS CLIENT 302
GATEWAY 312
TS SERVER 306
CLIENT FUNCTIONALITY 302
PROTOCOL MODULE 502
SECURITY FILTER 504
SECURITY FILTER 506
NEGOTIATION COMPONENT 508
(1) CREATE CHANNEL
(2) TOKEN
(3) ACTIVATE
(4) SSL HELLO
(5) ACTIVATE
(6) SSL HANDSHAKE
GATEWAY-SERVER HANDSHAKE
(7) POLICY, TOKEN
(7) POLICY, TOKEN
(7) POLICY, TOKEN
(8) RESET CMD
(8) RESET CMD
(8) RESET CMD
(9) RESET
(10) CLIENT MESSAGE
(10) CLIENT MESSAGE
(10) CLIENT MESSAGE
(10) CLIENT MESSAGE
(11) DEACTIVATE
SECURITY FILTER
(12) CLIENT-SERVER AUTHORIZATION
(13) RDP W/ TOKEN
(13) RDP W/ TOKEN
(13) RDP W/ TOKEN
(14)

FIG. 6

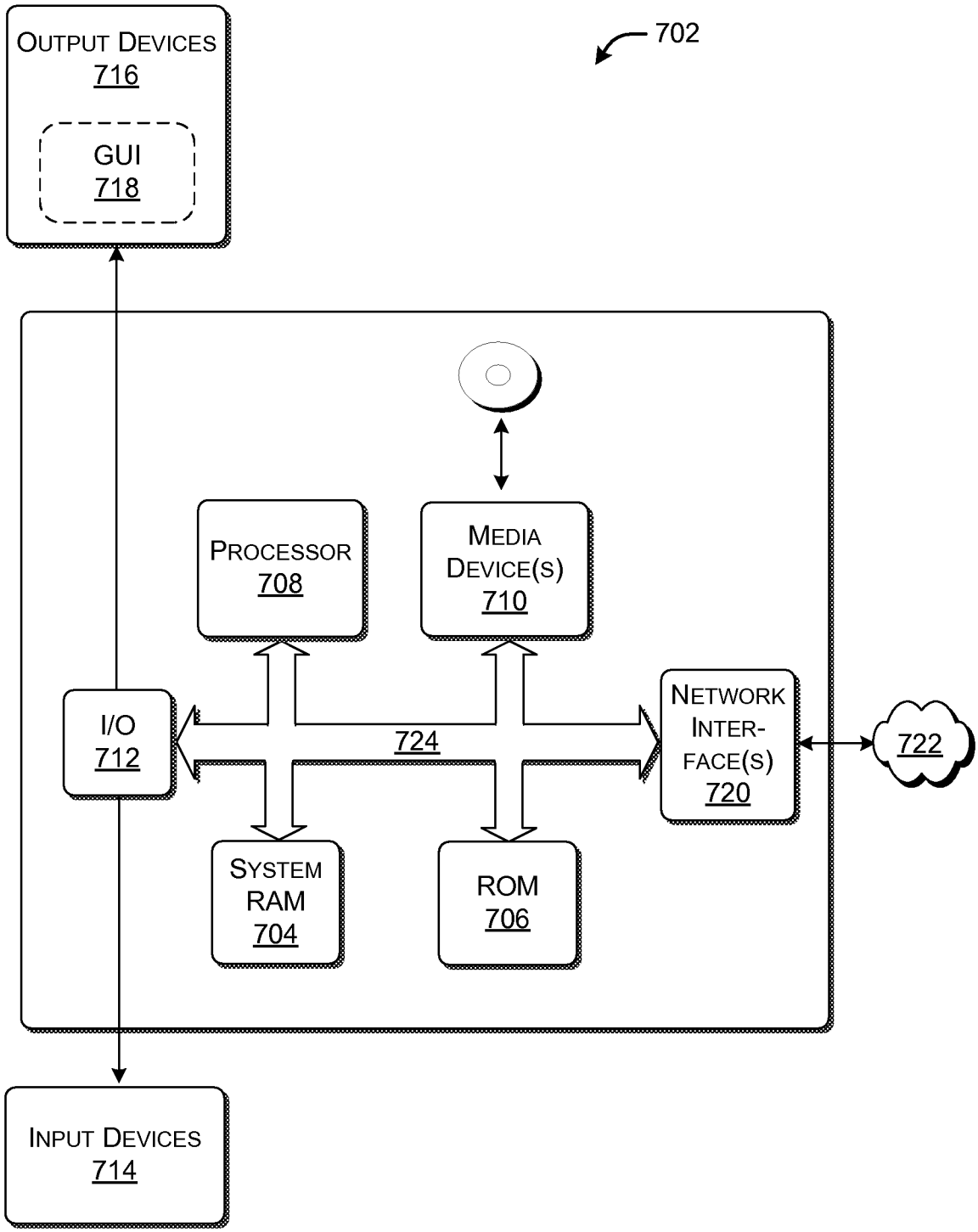
OUTPUT DEVICES
716
GUI
718
702
PROCESSOR
708
MEDIA
DEVICE(S)
710
I/O
712
724
NETWORK
INTER-
FACE(S)
720
722
SYSTEM
RAM
704
ROM
706
INPUT DEVICES
714

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/053506

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28(2006.01)i, H04L 12/66(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and application for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS (KIPO internal), IEEE xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/0080909 A1 (ANATOLIY PANASYUK, et al.) 14 Apr. 2005 See page 3 paragraph[0028] - page 4 paragraph[0043]	1-20
A	US 6,675,198 B1 (HIDEKAZU HAGIWARA, et al.) 6 Jan. 2004 See column 1 line 55 - column 2 line 45; Figure 1	1, 13
A	KR 10-2003-0003314 A (METAGENSOFT, INC.) 10 Jan. 2003 See page 3 lines. 1-25; Figure 1	1, 13

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 JUNE 2008 (24.06.2008)	**24 JUNE 2008 (24.06.2008)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

JANG, Dae Geun

Telephone No. 82-42-481-5645

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/053506

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005/0080909 A1	14.04.2005	AU 2004-284747 A1	06.05.2005
		CA 2541916 A1	06.05.2005
		EP 1671204 A1	21.06.2006
		JP 2007-509389 T2	12.04.2007
		KR 2006134925 A	28.12.2006
		WO 2005-041004 A1	06.05.2005
US 6,675,198 B1	06.01.2004	CN 1260662 C	21.06.2006
		CN 1275741 A	06.12.2000
		JP 2000-339064 A2	08.12.2000
		JP 3220862 B2	22.10.2001
KR 10-2003-0003314 A	10.01.2003	NONE	