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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2019 (21.03.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/051935 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/CN2017/107490

(22) International Filing Date:
24 October 2017 (24.10.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/707,528 18 September 2017 (18.09.2017) US

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors: **GIGOV, Nikolay**; 45 Caroline Street N, Unit 301, Waterloo, Ontario N2L 2Y6 (CA). **TAN, Yin**; 403-White Birch Ave, Waterloo, Ontario N2V 2T3 (CA). **LAMBERT, Robert**; 300 Hagey Blvd., Suite 302, Waterloo, Ontario N2L 0A4 (CA).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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: SECURING DELEGATED CREDENTIALS IN THIRD-PARTY NETWORKS

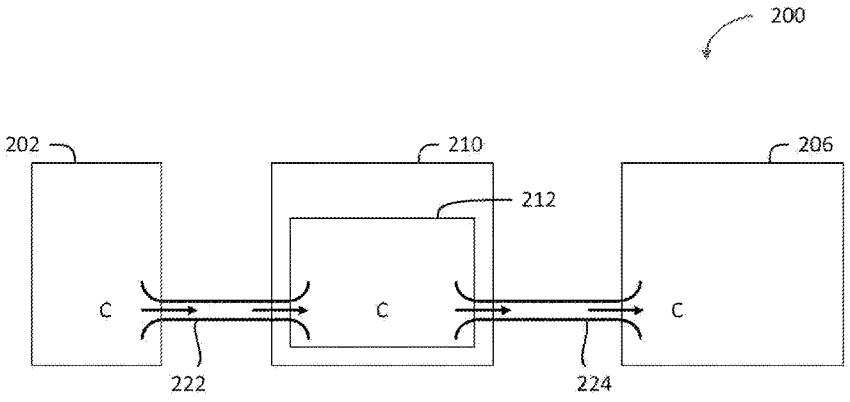


FIGURE 2

(57) Abstract: Methods and systems for providing an endpoint device with access to a remote resource are disclosed. A first secure tunnel with the endpoint device is established from an intermediate device, the first tunnel terminating within a trusted execution environment (TEE) in the intermediate device. At least one credential is received within the TEE and via the first secure tunnel from the endpoint device. The at least one credential is transmitted from the intermediate device to the remote resource via a second secure tunnel, the second tunnel located between the remote resource and the intermediate device and originating within the TEE. In response to the at least one credential being accepted by the remote resource, communications between the endpoint device and the remote resource via the TEE in the intermediate device through the first and second secure tunnels are enabled.

WO 2019/051935 A1

SECURING DELEGATED CREDENTIALS IN THIRD-PARTY NETWORKS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims priority to U.S. Patent Application No. 15/707,528, filed on September 18, 2017 and entitled "SECURING DELEGATED CREDENTIALS IN THIRD-PARTY NETWORKS", which is hereby incorporated by reference herein as if reproduced in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates generally to secured access to networks and information technology services, and more specifically to cloud-based secured access of networks and information technology services using credentials.

[0003]

BACKGROUND OF THE ART

[0004] Credential-based access, typically using a combination of a username and a password, has a long history of use in secure access protocols. A user of an endpoint device seeking to access some remote resource provides credentials to an authentication server of the remote resource and, if accepted, is granted access to the remote resource. Increasingly, users are accessing remote resources through a third-party, and having the third-party make use of the remote resource on their behalf. For example, a user or an endpoint device may request that a third-party access an email server, and to do so the user device provides the third-party with the user's credentials.

[0005] However, in providing the third-party with their credentials via their endpoint device, the user now risks theft or exposure of their credentials. It is impossible for the user to know whether the third-party has deleted their credentials after using them to access the remote resource. If the third-party does not delete the user's credentials, then the third-party is a node at which the user's credentials may be acquired by a malicious actor, or may be exposed following a breach.

[0006] Therefore, there is room for improved techniques for delegating credentials to third-parties.

SUMMARY

[0007] In accordance with a broad aspect, there is provided a method for providing an endpoint device with access to a remote resource, comprising: establishing, from an intermediate device, a first secure tunnel with the endpoint device, the first tunnel terminating within a trusted execution environment (TEE) in the intermediate device; receiving, within the

TEE and via the first secure tunnel, at least one credential from the endpoint device; transmitting the at least one credential from the intermediate device to the remote resource via a second secure tunnel, the second secure tunnel located between the remote resource and the intermediate device and originating within the TEE; and in response to the at least one credential being accepted by the remote resource, enabling communications between the endpoint device and the remote resource via the TEE in the intermediate device through the first and second secure tunnels.

[0008] In some embodiments, the method further comprises receiving, at the intermediate device, a request to access the remote resource from the endpoint device prior to establishing the first secure tunnel, and establishing the first secure tunnel in response to the request.

[0009] In some embodiments, the method further comprises constructing the TEE within the intermediate device in response to receiving the request.

[0010] In some embodiments, the method further comprises establishing the second secure tunnel in response to the request to access the remote resource.

[0011] In some embodiments, the method further comprises storing the at least one credential within the TEE.

[0012] In some embodiments, the method further comprises: receiving, at the intermediate device, a request from the endpoint device to terminate access to the remote resource; deleting the at least one credential from the TEE; and terminating at least one of the first secure tunnel and the second secure tunnel.

[0013] In some embodiments, enabling communication between the endpoint device and the remote resource comprises: receiving, at the intermediate device, plaintext data from the endpoint device within the TEE; encrypting the plaintext data with a data encryption key within the TEE to produce encrypted data; and transmitting the encrypted data to the remote resource via the second secure tunnel.

[0014] In some embodiments, the method further comprises deleting the plaintext data from the TEE after encrypting the plaintext data.

[0015] In some embodiments, the method further comprises instructing the endpoint device to delete the plaintext data from the endpoint device after transmitting the encrypted data to the remote resource.

[0016] In some embodiments, establishing the first secure tunnel with the endpoint device comprises establishing a transport-layer security connection between the endpoint device and the TEE.

[0017] In accordance with another broad aspect, there is provided a system for providing an endpoint device with access to a remote resource, comprising a processing unit; and a non-transitory computer-readable memory communicatively coupled to the processing unit. The computer-readable memory comprises computer-readable program instructions executable by the processing unit for: establishing, from an intermediate device, a first secure tunnel with the endpoint device, the first tunnel terminating within a trusted execution environment in the intermediate device; receiving, within the TEE and via the first secure tunnel, at least one credential from the endpoint device; transmitting the at least one credential from the intermediate device to the remote resource via a second secure tunnel, the second secure tunnel located between the remote resource and the intermediate device and originating within the TEE; and in response to the at least one credential being accepted by the remote resource, enabling communications between the endpoint device and the remote resource via the TEE in the intermediate device through the first and second secure tunnels.

[0018] In some embodiments, the program instructions are further executable by the processing unit for receiving, at the intermediate device, a request to access the remote resource from the endpoint device prior to establishing the first secure tunnel, and establishing the first secure tunnel in response to the request.

[0019] In some embodiments, the program instructions are further executable by the processing unit for constructing the TEE within the intermediate device in response to receiving the request.

[0020] In some embodiments, the program instructions are further executable by the processing unit for establishing the second secure tunnel in response to the request to access the remote resource.

[0021] In some embodiments, the program instructions are further executable by the processing unit for storing the at least one credential within the TEE.

[0022] In some embodiments, the program instructions are further executable by the processing unit for: receiving, at the intermediate device, a request from the endpoint device to terminate access to the remote resource; deleting the at least one credential from the TEE; and terminating at least one of the first secure tunnel and the second secure tunnel.

[0023] In some embodiments, enabling communication between the endpoint device and the remote resource comprises: receiving, at the intermediate device, plaintext data from the endpoint device within the TEE; encrypting the plaintext data with a data encryption key within the TEE to produce encrypted data; and transmitting the encrypted data to the remote resource via the second secure tunnel.

[0024] In some embodiments, the program instructions are further executable by the processing unit for deleting the plaintext data from the TEE after encrypting the plaintext data.

[0025] In some embodiments, the program instructions are further executable by the processing unit for instructing the endpoint device to delete the plaintext data from the endpoint device after transmitting the encrypted data to the remote resource.

[0026] In some embodiments, establishing the first secure tunnel with the endpoint device comprises establishing a transport-layer security connection between the endpoint device and the TEE.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] Reference is now made to the accompanying figures in which:

[0028] Figure 1 is a diagram of an example prior art credential delegation system;

[0029] Figure 2 is a block diagram of an example credential delegation system;

[0030] Figures 3A-B are a flowchart illustrating an example method for providing an endpoint device with access to a remote resource;

[0031] Figure 4 is a flowchart illustrating an example method for performing third-party encryption;

[0032] Figure 5 is a block diagram of an example third-party encryption system; and

[0033] Figure 6 is a block diagram of an example computer system for implementing the methods of Figure 3A-B and 4.

[0034] It will be noted that throughout the appended drawings, like features are identified by like reference numerals.

DETAILED DESCRIPTION

[0035] With reference to Figure 1, in prior art systems, an endpoint device 102 requests a third-party device 104 to access a remote resource 106 and to perform one or more actions at the remote resource 106 on behalf of the endpoint device 102. For example, the third-party device 104 is an identity access manager, which implements a single sign-on service. The endpoint device 102 is a laptop or desktop computer, a smartphone or other mobile device, or any other suitable communication device. The third-party device 104 is a cloud-based server or any other suitable type of server, and the remote resource 106 is an email server, a media repository, a social-media site, or any other suitable resource. The endpoint device 102 sends the third-party server 104 a credential C via a communication path 112, and the third-party server 104 uses the credential C to access the remote resource 106. This

approach, however, means that the credential C resides at the third-party device 104 and is at risk of being exposed or stolen by a malicious actor.

[0036] With reference to Figure 2, a network 200 is illustrated, including an endpoint device 202, a remote resource 206, and an intermediate device 210. The intermediate device 210 serves as an intermediary and provides the endpoint device 202 with access to the remote resource 206. The endpoint device 202 is substantially similar to the endpoint device 102, and the remote resource is substantially similar to the remote resource 106.

[0037] The intermediate device 210, which can be a cloud server or any other suitable server, is configured for implementing a trusted execution environment (TEE) 212. The TEE 212 is any suitable kind of trusted execution environment, for example as provided by Intel™ SGX™ technology. In other embodiments, other types of trusted execution environments, for example Trusted Platform Module™ or TrustZone™, are used. The TEE 212 operates by performing processor-based encryption on all computer-readable instructions and data used by the execution of the instructions. In this fashion, the instructions and data used within the TEE 212 are encrypted and inscrutable to the intermediate device 210 itself, and to any person having access to the intermediate device 210.

[0038] Communications between the endpoint device 202 and the intermediate device 210 are exchanged over a secure tunnel 222, and communications between the intermediate device 210 and the remote resource 206 are exchanged over a secure tunnel 224. Both secure tunnels 222 and 224 are established with an end-point within the TEE 212 at the intermediate device 210. For example, the secure tunnel 222 originates at the endpoint device 202 and terminates within the TEE 212, and the secure tunnel 224 originates within the TEE 212 and terminates at the remote resource 206. It should be noted that in some embodiments, the directionality of the secure tunnels 222 and 224 is reversed. In other embodiments, the secure tunnels 222 and 224 are direction-agnostic.

[0039] In some embodiments, the first and second secure tunnels 222 and 224 are transport layer security (TLS) connections which are terminated within the TEE 212. TLS certificates, including private keys associated with the secure tunnels 222 and 224, and session keys are kept within the TEE 212. In some embodiments, the TEE 212 also stores a tunnel key associated with the secure tunnel 222 and/or the secure tunnel 224. In some embodiments, the endpoint device 202, remote resource 206, and/or the intermediate device 210 perform one or more additional security verifications, for example to ensure that the secure tunnels 222 and 224 are terminated within the TEE 212. For example, the endpoint device 202 and/or the remote resource 206 can use one or more remote attestation techniques to verify the authenticity of the TEE 212 at the intermediary node 210. For instance, the remote

attestation techniques are used to verify an identity or other identification information associated with the TEE 212, to confirm that the TEE 212 is trustworthy for the purposes of the endpoint device 202 and/or the remote resource 206.

[0040] With reference to Figures 3A-B, a method 300 for providing the endpoint device 202 with access to the remote resource 206 is illustrated. At step 302, optionally the intermediate device 210 receives a request to access the remote resource 206 from the endpoint device 202. In some embodiments, the request is sent over a secured communication path. In other embodiments, the request is sent over an unsecured communication path. The request is sent using any suitable communications protocol. In some embodiments, the request specifies the remote resource 206 which the endpoint device 202 wishes to access. In other embodiments, the request indicates that the endpoint device 202 wishes to access one of a plurality of remote resources, including the remote resource 206, and a later request is received at the intermediate device to specify the remote resource 206. In still further embodiments, the intermediate device 210 is configured for periodically performing one or more actions on behalf of the endpoint device 202 according to a predetermined schedule. In embodiments in which the method 300 is performed according to the predetermined schedule, step 302 is omitted.

[0041] At step 304, optionally the TEE 212 is constructed within the intermediate device 210 in response to receiving the request. The TEE 212 is constructed by way of one or more API calls or other suitable instructions performed by the intermediate device 210. In some embodiments, the TEE 212 is a trusted execution environment constructed using Intel™ SGX™ technology. In other embodiments, the TEE 212 has been previously constructed, and step 304 is omitted.

[0042] At step 306, the first secure tunnel 222 is established with the endpoint device 202. The first secure tunnel 222 is established from the intermediate device 210 and terminates within the TEE 212. In some embodiments, the first secure tunnel 222 is a transport layer security (TLS) connection which is terminated within the TEE 212. TLS certificates, including private keys associated with the first secure tunnel 222, and session keys are kept within the TEE 212. In some embodiments, the TEE 212 also stores a tunnel key associated with the secure tunnel 222, and additional tunnel keys for any subsequent tunnels. In some embodiments, the endpoint device 202 and/or the intermediate device 210 perform one or more additional security verifications, for example to ensure that the first secure tunnel 222 is terminated within the TEE 212. For instance, one or more remote attestation techniques are used. In other embodiments, other network protocols are used to establish the first secure tunnel 222.

[0043] At step 308, optionally the second secure tunnel 224 is established with the remote resource 206. The second secure tunnel 224 is established from the intermediate device 210 and terminates within the TEE 212. In some embodiments, the second secure tunnel 224 is established in similar fashion as the first secure tunnel 222; alternatively, the second secure tunnel is established using other techniques. In other embodiments, the second secure tunnel 224 has been previously established, and step 308 is omitted.

[0044] At step 310, at least one credential C is received from the endpoint device 202 within the TEE 212 and via the first secure tunnel 222. The credential C is received in any suitable way, using any suitable communications protocols. The credential C may include one or more usernames, one or more passwords, any suitable combination thereof, including hashes, authentication tokens, and convolutions, and any other suitable information. Because the credential C is received within the TEE 212, it remains inscrutable to the intermediate device 210 and cannot be obtained therefrom other than within the TEE 212.

[0045] At step 312, the credential C is transmitted from the intermediate device to the remote resource 206 via the second secure tunnel 224. The credential C is transmitted in any suitable way, using any suitable communications protocols. It should be noted that the credential C is located within the TEE 212, and is transmitted from the TEE 212 to the remote resource 206.

[0046] At decision step 314, a determination is made regarding whether the credential C is accepted by the remote resource 206. In some embodiments, the remote resource 206 communicates to the intermediate device 210 and/or the TEE 212 an indication of whether the credential C is accepted by the remote resource 206. In other embodiments, the remote resource 206 communicates to the intermediate device 210 and/or the TEE 212 an acknowledgement when the credential C is accepted by the remote resource 206, and does not communicate when the credential C is not accepted. When the credential C is accepted, the method 300 proceeds to step 316. When the credential C is not accepted, the method 300 returns to some previous step, for example to step 310. In some embodiments, when the credential C is not accepted, the intermediate device 210 and/or the TEE 212 sends to the endpoint device 202 an indication that the credential C was not accepted by the remote resource 206.

[0047] At step 316, in response to the at least one credential being accepted by the remote resource, communications between the endpoint device 202 and the remote resource 206 are enabled via the TEE 212 through the first and second secure tunnels 222 and 224. In some embodiments, the TEE 212 acts as a conduit for communications between the

endpoint device 202 and the remote resource 206. In other embodiments, the request received at step 302 includes one or more actions which were requested to be performed by the intermediate device 210 on behalf of the endpoint device 202. The intermediate device 210, by way of the TEE 212, communicates with the remote resource 206 to cause the actions to be performed at the remote resource 206. In some embodiments, the list of possible actions to be performed by the intermediate device 210 is limited by the TEE 212. For example, the automatic integrity checking performed by the TEE 212 limits the list of possible actions to be performed by the intermediate device 210. This prevents a malicious device or client from injecting bad requests and/or a malicious administrator of the intermediate device 210 from modifying requests sent to the intermediate device 210.

[0048] Optionally, at step 318, the credential C is stored within the TEE 212. In some embodiments, the TEE 212 is substantially permanent within the intermediate device 210. Once the endpoint device 202 provides the TEE 212 with the credential C, the credential C is stored therein to avoid having to provide the credential C again. The credential C is stored in any suitable fashion, for instance in any suitably encrypted form, and in some embodiments is encoded using any suitable techniques.

[0049] Optionally, at step 320, a request is received at the intermediate device 210 from the endpoint device 202 to terminate access to the remote resource 206. In some embodiments, the request is received at the TEE 212 of the intermediate device 210. In some embodiments, the request is received over the secure tunnel 222; alternatively the request is received over another encrypted or otherwise secure communication path, as appropriate. The request is received in any suitable way, using any suitable communications protocols. In some embodiments, the request includes additional information, for example instructions to delete one or more credentials, for instance the credential C, instructions to terminate the TEE 212, and the like. Depending on the nature of the request received at step 320, any one or more of steps 322, 324, and 326 is performed.

[0050] In some embodiments, at step 322, the credential C is deleted from the TEE 212. In some other embodiments, at step 324, at least one of the first secure tunnel 222 and the second secure tunnel 224 is terminated. In still further embodiments, at step 326, the TEE is destroyed. In some embodiments, one or more of steps 322, 324, and 326 are performed substantially simultaneously by the intermediate device 210.

[0051] In some embodiments, any one or more of steps 322, 324, and 326 is performed following a timeout period during which no communications are exchanged between the endpoint device 202 and the remote resource 206. For example, after a timeout period step

324 is performed and the second secure tunnel is terminated. In the event that a communication from the endpoint device 202 destined for the remote resource is received after the timeout period, step 308 is performed to re-establish the second secure tunnel.

[0052] It should be noted that in some embodiments, various steps of the method 300 are performed substantially concurrently. For example, steps 306 and 308 are performed concurrently after receiving the request to access the remote resource 206. In another example, steps 322, 324, and 326 are performed concurrently after receiving the request to terminate access to the remote resource 206. In addition, in some embodiments the order in which steps are illustrated in Figures 3A and 3B is varied. For instance, step 308 is performed before step 306, and the order of steps 322, 324, and 326 is altered.

[0053] By ensuring that access to remote resource 206 for the endpoint device 202 is brokered through the TEE 212, exposure of credentials, including the credential C, can be limited or prevented, thereby improving the security of accessing the remote resource 206.

[0054] With reference to Figure 4, the TEE 212 is used to enable communications between the endpoint device 202 and the remote resource 206 through the first and second secure tunnels 222 and 224. In some embodiments, this includes performing the method 400. At step 402, plaintext data is received from the endpoint device 202 at the intermediate device 210, within the TEE. The plaintext data is received over the first secure tunnel 222. The plaintext data is text, photos, video, other media, or any other suitable type of data that is considered to be unencrypted. In some cases, the plaintext data also includes previously-encrypted data that a user of the endpoint device 202 wishes to further encrypt.

[0055] At step 404, the plaintext data is encrypted with a data encryption key within the TEE 212 to produce encrypted data. The encryption process performed by the intermediate device 210 within the TEE 212 uses any suitable ciphering techniques, and any suitable level of encryption. Because the plaintext data is only ever received within the TEE 212, and because the encryption process takes place within the TEE 212, the plaintext data and the encryption steps are inscrutable to intermediate device 210, or to any malicious actor having access to the intermediate device 210.

[0056] At step 406, the encrypted data is transmitted to the remote resource 206 via the second secure tunnel 224. In some embodiments, the encrypted data is transmitted to the remote resource 206 for storage. The encrypted data is transmitted in any suitable way, using any suitable communications protocols. In some embodiments, the data encryption key is transmitted alongside the encrypted data. For example, the data encryption key is wrapped with, or alongside, the encrypted data.

[0057] Optionally, at step 408, the plaintext data is deleted from the TEE 212. Deleting the plaintext data from the TEE 212 ensures that even in the unlikely event that the processor-based encryption of the TEE 212 is breached, a malicious actor will not have access to the plaintext data. In some embodiments, step 408 also includes deleting the encrypted data from the TEE 212.

[0058] Optionally, at step 410, the endpoint device 202 is instructed to delete the plaintext data from the endpoint device 202. In some embodiments, the intermediate device 210, for example via the TEE 212, sends instructions to the endpoint device 202 to cause the endpoint device 202 to delete the plaintext data. Because the plaintext data is retrievable from the encrypted data stored on the remote resource 206, the user of the endpoint device 202 is able to retrieve the plaintext data even after the plaintext data is deleted from the endpoint device 202. In addition, deleting the plaintext data from the endpoint device 202 ensures that if the endpoint device 202 becomes compromised, for example is stolen by a malicious actor, the malicious actor cannot acquire the plaintext data.

[0059] With reference to Figure 5, a graphical representation of the method 400 is illustrated. Plaintext data P is received at the intermediate device 210 via the first secure tunnel 222 and within the TEE 212, as per step 402. The data encryption key K is used to encrypt the plaintext data P to produce encrypted data E, as per step 404. The encrypted data E is transmitted to the remote resource 206 via the second secure tunnel 224, as per step 406. Thereafter, in some embodiments the plaintext data P and/or the encrypted data E is deleted from the endpoint device 202 and/or from the intermediate device 210, as appropriate, as per steps 408 and 410.

[0060] In some embodiments, the intermediate device 210 and the TEE 212 are used to perform remote encryption of data, thereby offloading computationally-intensive calculations from the endpoint device 202. This helps reduce energy requirements for the endpoint device 202, which may be particularly helpful if the endpoint device 202 is a smartphone or other battery-powered device. In addition, the use of the TEE 212 ensures that malicious actors having access to the intermediate device 210 cannot acquire the plaintext data P, the encrypted data E, or the data encryption key K.

[0061] In some embodiments, the TEE 212 is configured for logging usage of the TEE 212, including one or more of access timestamps, access locations and/or IP addresses, and types of actions performed via the TEE 212. For example, the TEE 212 flags suspicious use of particular credentials, or too-frequent access of the TEE 212 from a particular location. In some embodiments, the TEE 212 and/or the intermediate device 210 are configured for

providing the endpoint device 202 and/or a network administrator or other responsible entity with an indication that suspicious activity has been flagged.

[0062] With reference to Figure 6, the methods 200 and 400 may be implemented by a computing device 610, comprising a processing unit 612 and a memory 614 which has stored therein computer-executable instructions 616. The processing unit 612 may be any suitable device configured to implement the methods 200 and 400 such that instructions 616, when executed by the computing device 610 or other programmable apparatus, causes the functions/acts/steps performed as part of the methods 200 and 400 as described herein to be executed. The processing unit 612 may be, for example, any type of general-purpose microprocessor or microcontroller, a digital signal processing (DSP) processor, a central processing unit (CPU), an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, other suitably programmed or programmable logic circuits, or any combination thereof. The processing unit 612 is configured to encrypt any suitable regions of the memory 614, including those portions of the memory used to implement the TEE 212. The processing unit 612 is also configured for providing measurements and/or guarantees relating to the validity, authenticity, and integrity of computer-executable instructions 616 being executed in the TEE 212.

[0063] The memory 614 may be any suitable known or other machine-readable storage medium. The memory 614 may be non-transitory computer readable storage medium, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. The memory 614 includes a suitable combination of any type of computer memory that is located either internally or externally to device, for example random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, erasable programmable read-only memory (EPROM), and electrically-erasable programmable read-only memory (EEPROM), Ferroelectric RAM (FRAM) or the like. Memory 614 may be any storage means (e.g., devices) suitable for retrievably storing machine-readable instructions 616 executable by processing unit 612.

[0064] The methods and systems for providing an endpoint device with access to a remote resource described herein may be implemented in a high level procedural or object oriented programming or scripting language, or a combination thereof, to communicate with or assist in the operation of a computer system, for example the computing device 610. Alternatively, the methods and systems for providing an endpoint device with access to a remote resource may be implemented in assembly or machine language. The language may be a compiled or interpreted language. Program code for implementing the methods and systems for

providing an endpoint device with access to a remote resource may be stored on a storage media or a device, for example a ROM, a magnetic disk, an optical disc, a flash drive, or any other suitable storage media or device. The program code may be readable by a general or special-purpose programmable computer for configuring and operating the computer when the storage media or device is read by the computer to perform the procedures described herein. Embodiments of the methods and systems for providing an endpoint device with access to a remote resource may also be considered to be implemented by way of a non-transitory computer-readable storage medium having a computer program stored thereon. The computer program may comprise computer-readable instructions which cause a computer, or more specifically the processing unit 612 of the computing device 310, to operate in a specific and predefined manner to perform the functions described herein, for example those described in the methods 200 and 400.

[0065] Computer-executable instructions may be in many forms, including program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0066] The above description is meant to be exemplary only, and one skilled in the art will recognize that changes may be made to the embodiments described without departing from the scope of the invention disclosed. Still other modifications which fall within the scope of the present invention will be apparent to those skilled in the art, in light of a review of this disclosure.

[0067] Various aspects of the methods and systems for providing an endpoint device with access to a remote resource may be used alone, in combination, or in a variety of arrangements not specifically discussed in the embodiments described in the foregoing and is therefore not limited in its application to the details and arrangement of components set forth in the foregoing description or illustrated in the drawings. For example, aspects described in one embodiment may be combined in any manner with aspects described in other embodiments. Although particular embodiments have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspects. The scope of the following claims should not be limited by the embodiments set forth in the examples, but should be given the broadest reasonable interpretation consistent with the description as a whole.

CLAIMS

1. A method for providing an endpoint device with access to a remote resource, comprising:

establishing, from an intermediate device, a first secure tunnel with the endpoint device, the first tunnel terminating within a trusted execution environment (TEE) in the intermediate device;

receiving, within the TEE and via the first secure tunnel, at least one credential from the endpoint device;

transmitting the at least one credential from the intermediate device to the remote resource via a second secure tunnel, the second secure tunnel located between the remote resource and the intermediate device and originating within the TEE; and

in response to the at least one credential being accepted by the remote resource, enabling communications between the endpoint device and the remote resource via the TEE in the intermediate device through the first and second secure tunnels.

2. The method of claim 1, further comprising receiving, at the intermediate device, a request to access the remote resource from the endpoint device prior to establishing the first secure tunnel, and establishing the first secure tunnel in response to the request.

3. The method of claim 2, further comprising constructing the TEE within the intermediate device in response to receiving the request.

4. The method of claim 2, further comprising establishing the second secure tunnel in response to the request to access the remote resource.

5. The method of any one of claims 1 to 4, further comprising storing the at least one credential within the TEE.

6. The method of any one of claims 1 to 5, further comprising:

receiving, at the intermediate device, a request from the endpoint device to terminate access to the remote resource;

deleting the at least one credential from the TEE; and

terminating at least one of the first secure tunnel and the second secure tunnel.

7. The method of any one of claims 1 to 6, wherein enabling communication between the endpoint device and the remote resource comprises:

receiving, at the intermediate device, plaintext data from the endpoint device within the TEE;

encrypting the plaintext data with a data encryption key within the TEE to produce encrypted data; and

transmitting the encrypted data to the remote resource via the second secure tunnel.

8. The method of claim 7, further comprising deleting the plaintext data from the TEE after encrypting the plaintext data.

9. The method of claim 7, further comprising instructing the endpoint device to delete the plaintext data from the endpoint device after transmitting the encrypted data to the remote resource.

10. The method of any one of claims 1 to 9, wherein establishing the first secure tunnel with the endpoint device comprises establishing a transport-layer security connection between the endpoint device and the TEE.

11. A system for providing an endpoint device with access to a remote resource, comprising:

a processing unit; and

a non-transitory computer-readable memory communicatively coupled to the processing unit and comprising computer-readable program instructions executable by the processing unit for:

establishing, from an intermediate device, a first secure tunnel with the endpoint device, the first tunnel terminating within a trusted execution environment in the intermediate device;

receiving, within the TEE and via the first secure tunnel, at least one credential from the endpoint device;

transmitting the at least one credential from the intermediate device to the remote resource via a second secure tunnel, the second secure tunnel located between the remote resource and the intermediate device and originating within the TEE; and

in response to the at least one credential being accepted by the remote resource, enabling communications between the endpoint device and the remote resource via the TEE in the intermediate device through the first and second secure tunnels.

12. The system of claim 11, wherein the program instructions are further executable by the processing unit for receiving, at the intermediate device, a request to access the remote

resource from the endpoint device prior to establishing the first secure tunnel, and establishing the first secure tunnel in response to the request.

13. The system of claim 12, wherein the program instructions are further executable by the processing unit for constructing the TEE within the intermediate device in response to receiving the request.

14. The system of claim 12, wherein the program instructions are further executable by the processing unit for establishing the second secure tunnel in response to the request to access the remote resource.

15. The system of any one of claims 11 to 14, wherein the program instructions are further executable by the processing unit for storing the at least one credential within the TEE.

16. The system of any one of claims 11 to 15, wherein the program instructions are further executable by the processing unit for:

receiving, at the intermediate device, a request from the endpoint device to terminate access to the remote resource;

deleting the at least one credential from the TEE; and

terminating at least one of the first secure tunnel and the second secure tunnel.

17. The system of any one of claims 11 to 16, wherein enabling communication between the endpoint device and the remote resource comprises:

receiving, at the intermediate device, plaintext data from the endpoint device within the TEE;

encrypting the plaintext data with a data encryption key within the TEE to produce encrypted data; and

transmitting the encrypted data to the remote resource via the second secure tunnel.

18. The system of claim 17, wherein the program instructions are further executable by the processing unit for deleting the plaintext data from the TEE after encrypting the plaintext data.

19. The system of claim 17, wherein the program instructions are further executable by the processing unit for instructing the endpoint device to delete the plaintext data from the endpoint device after transmitting the encrypted data to the remote resource.

20. The system of any one of claims 11 to 19, wherein establishing the first secure tunnel with the endpoint device comprises establishing a transport-layer security connection between the endpoint device and the TEE.

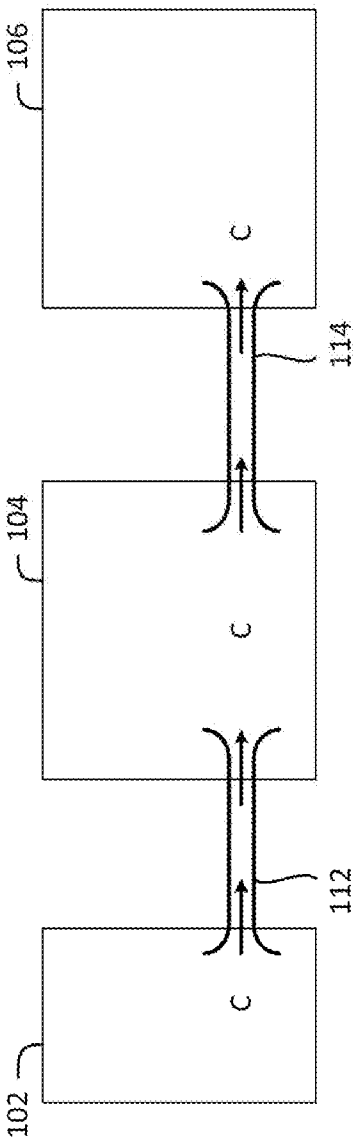


FIGURE 1
(PRIOR ART)

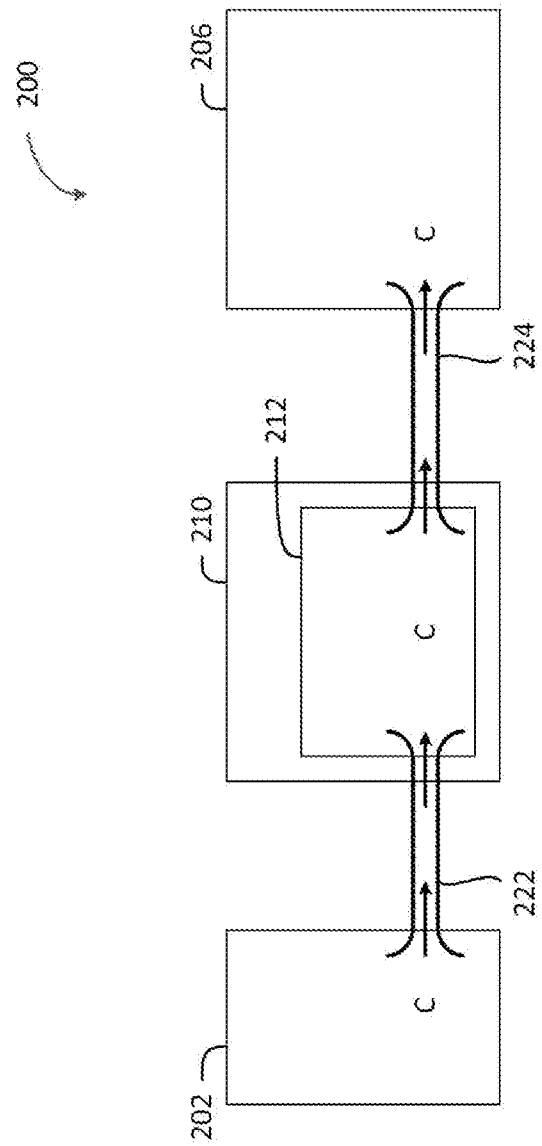


FIGURE 2

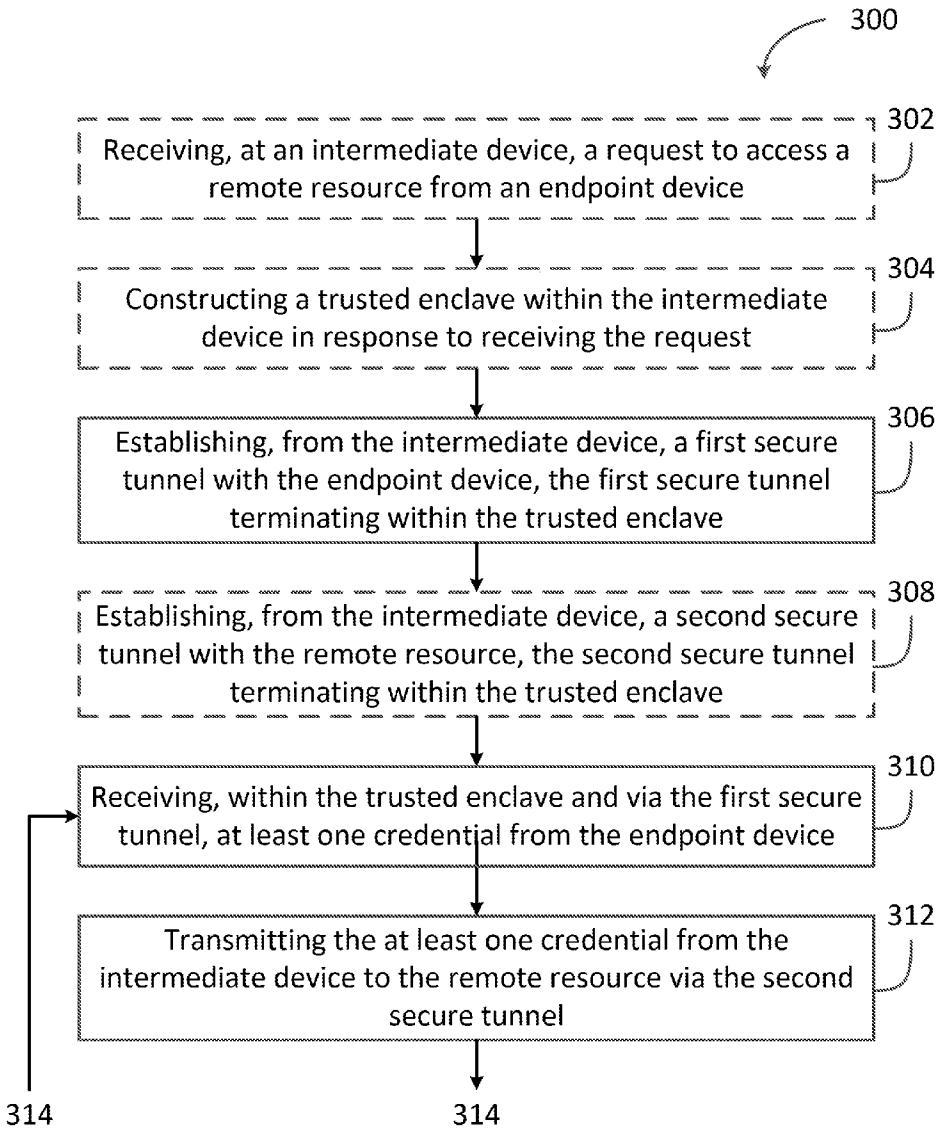

300
302
Receiving, at an intermediate device, a request to access a remote resource from an endpoint device
304
Constructing a trusted enclave within the intermediate device in response to receiving the request
306
Establishing, from the intermediate device, a first secure tunnel with the endpoint device, the first secure tunnel terminating within the trusted enclave
308
Establishing, from the intermediate device, a second secure tunnel with the remote resource, the second secure tunnel terminating within the trusted enclave
310
Receiving, within the trusted enclave and via the first secure tunnel, at least one credential from the endpoint device
312
Transmitting the at least one credential from the intermediate device to the remote resource via the second secure tunnel
314
314

FIGURE 3A

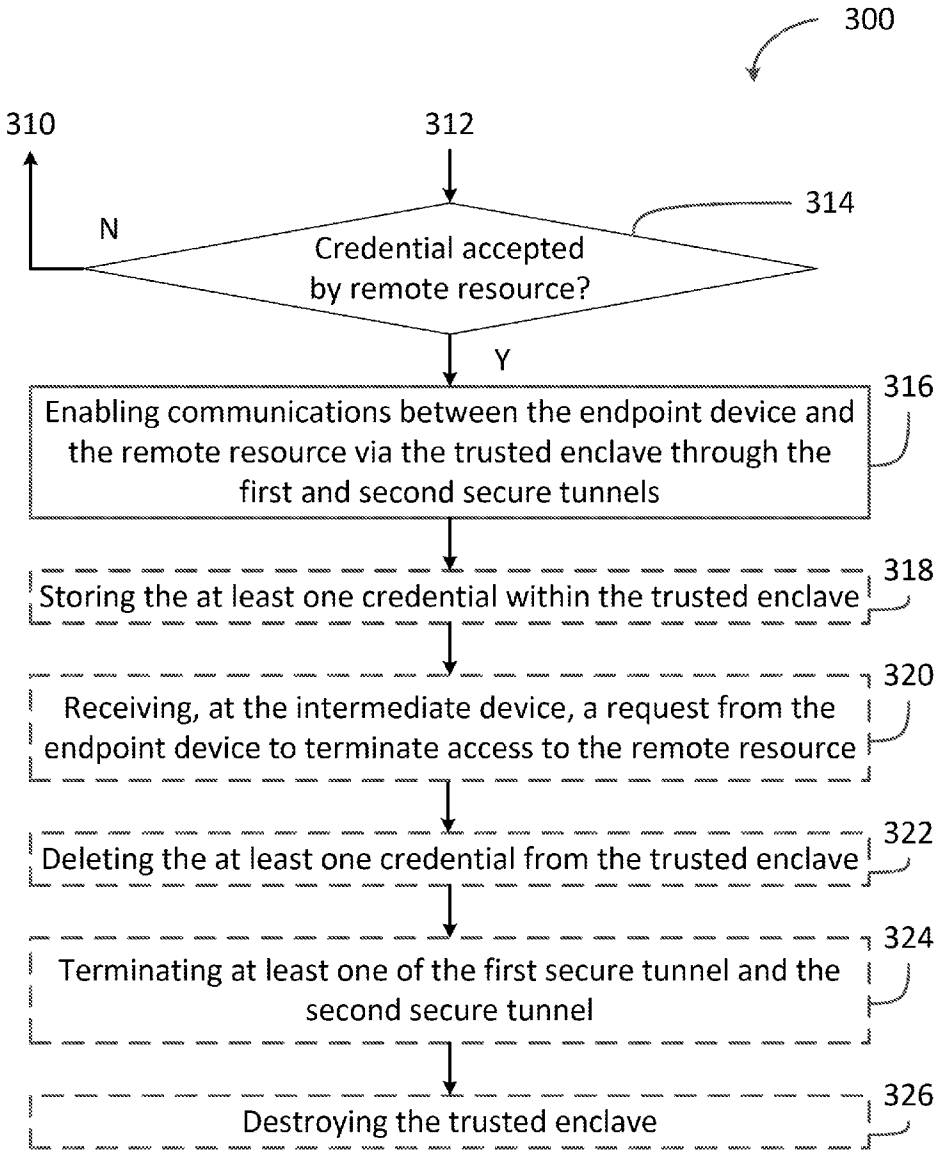

300
310
312
314
N
Credential accepted by remote resource?
Y
316
Enabling communications between the endpoint device and the remote resource via the trusted enclave through the first and second secure tunnels
318
Storing the at least one credential within the trusted enclave
320
Receiving, at the intermediate device, a request from the endpoint device to terminate access to the remote resource
322
Deleting the at least one credential from the trusted enclave
324
Terminating at least one of the first secure tunnel and the second secure tunnel
326
Destroying the trusted enclave

FIGURE 3B

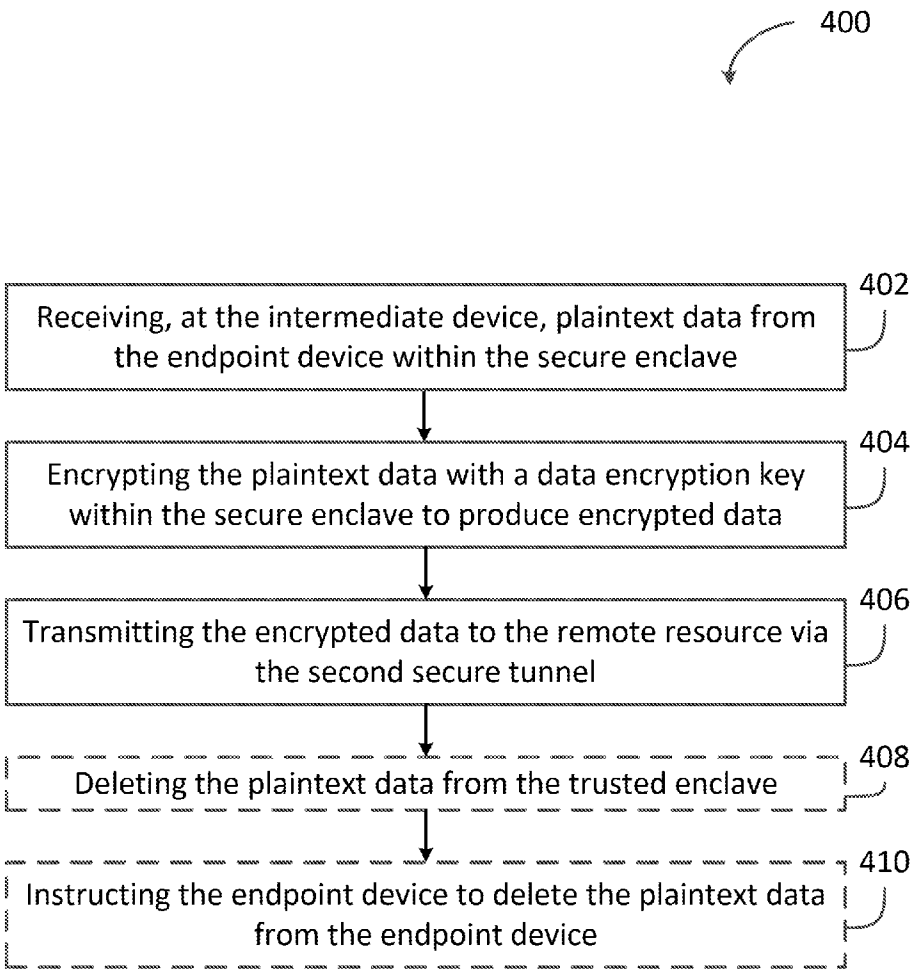

400
Receiving, at the intermediate device, plaintext data from the endpoint device within the secure enclave
402
Encrypting the plaintext data with a data encryption key within the secure enclave to produce encrypted data
404
Transmitting the encrypted data to the remote resource via the second secure tunnel
406
Deleting the plaintext data from the trusted enclave
408
Instructing the endpoint device to delete the plaintext data from the endpoint device
410

FIGURE 4

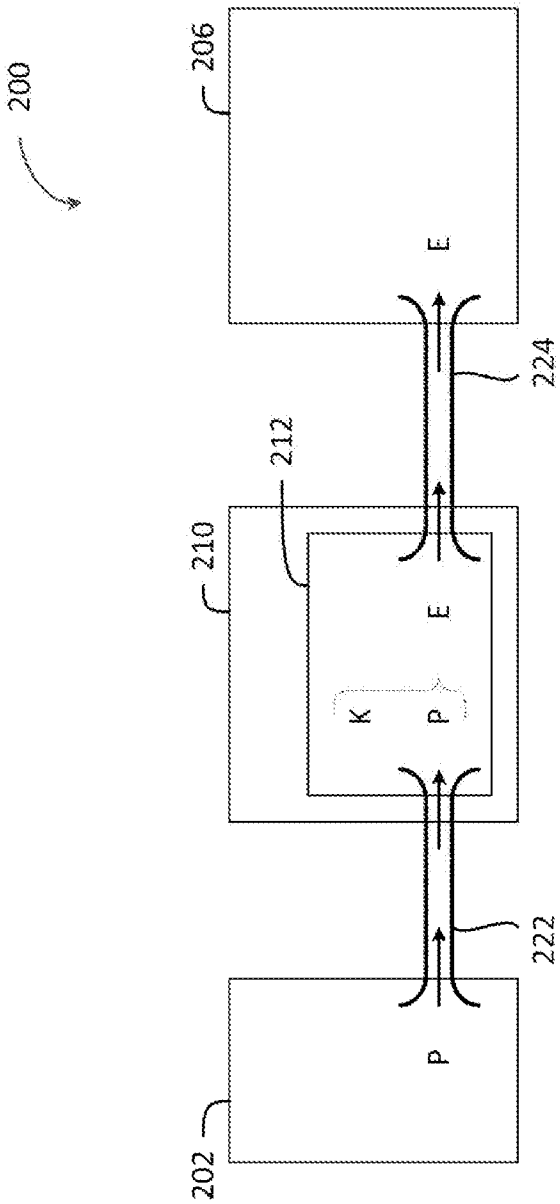


FIGURE 5

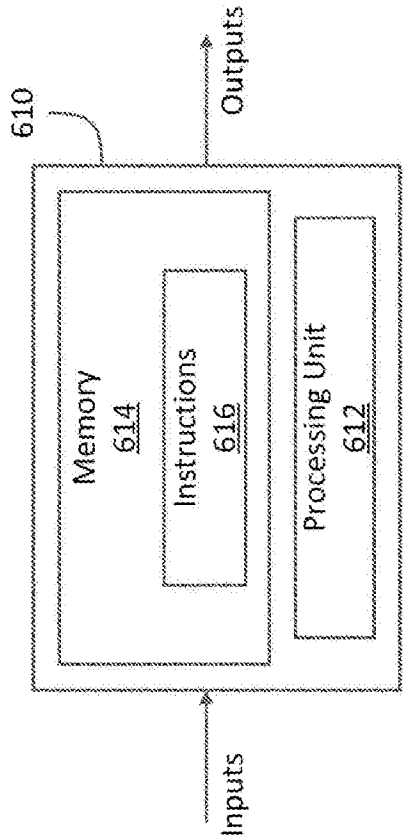

610
Outputs
Memory
614
Instructions
616
Processing Unit
612
Inputs

FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/107490

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

H04L 9/-, H04L 29/-

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

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

CNABS, DWPI, CNKI, SIPOABS: third w party, remote, TEE, trusted, authentication, encrypt, request, intermediate, secure, tunnel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104125216 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 October 2014 (2014-10-29) the whole document	1-20
A	CN 105429760 A (SHENZHOU RONGAN TECHNOLOGY BEIJING CO., LTD.) 23 March 2016 (2016-03-23) the whole document	1-20
A	CN 105101169 A (CHINA MOBILE COMMUNICATION CORPORATION) 25 November 2015 (2015-11-25) the whole document	1-20
A	CN 101202760 A (MICROSOFT CORPORATION) 18 June 2008 (2008-06-18) the whole document	1-20
A	CN 104158791 A (BEIJING FOUNDER ELECTRONICS CO., LTD. ET AL) 19 November 2014 (2014-11-19) the whole document	1-20
A	CN 101039186 A (CHINESE ACAD SCI SOFTWARE INST.) 19 September 2007 (2007-09-19) the whole document	1-20

☑ 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 another citation or other special reason (as specified)

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 April 2018	**11 May 2018**
Name and mailing address of the ISA/CN **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **LIU,Jia** Telephone No. **62089528**

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102571359 A (SHANGHAI KAIZHUO INFORMATION TECHNOLOGY CO., LTD.) 11 July 2012 (2012-07-11) the whole document	1-20
A	CN 101447007 A (DONGGUAN ZHIDUN ELECTRONIC TECHNOLOGY CO., LTD. ET AL) 03 June 2009 (2009-06-03) the whole document	1-20
A	CN 101848207 A (WUXI CINSEC INFORMATION TECHNOLOGY CO., LTD.) 29 September 2010 (2010-09-29) the whole document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/107490

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104125216	A	29 October 2014	CN	104125216	B	15 December 2017
CN	105429760	A	23 March 2016		None		
CN	105101169	A	25 November 2015		None		
CN	101202760	A	18 June 2008	CN	101202760	B	04 July 2012
				WO	2008071124	A1	19 June 2008
CN	104158791	A	19 November 2014	EP	2999158	A1	23 March 2016
				JP	2016519540	A	30 June 2016
				WO	2014183392	A1	20 November 2014
				US	2016119141	A1	28 April 2016
				EP	2999158	A4	11 January 2017
CN	101039186	A	19 September 2007	CN	101039186	B	04 August 2010
CN	102571359	A	11 July 2012		None		
CN	101447007	A	03 June 2009	CN	101447007	B	22 June 2011
CN	101848207	A	29 September 2010		None		