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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2017 (05.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/003584 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2016/033863

(22) International Filing Date:
24 May 2016 (24.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/752,888 27 June 2015 (27.06.2015) US

(71) Applicant: **MCAFEE, INC.** [US/US]; 2821 Mission College Boulevard, Santa Clara, California 95054-1838 (US).

(72) Inventors: **KAPOOR, Aditya**; 13686 NW Henninger Lane, Portland, Oregon 97229 (US). **EDWARDS, Jonathan L.**; 2535 NE 46th Avenue, Portland, Oregon 97213 (US).

(74) Agent: **PEMBERTON, John D.**; Patent Capital Group, c/o CPA Global, 900 Second Avenue South, Suite 600, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PROTECTION OF SENSITIVE DATA

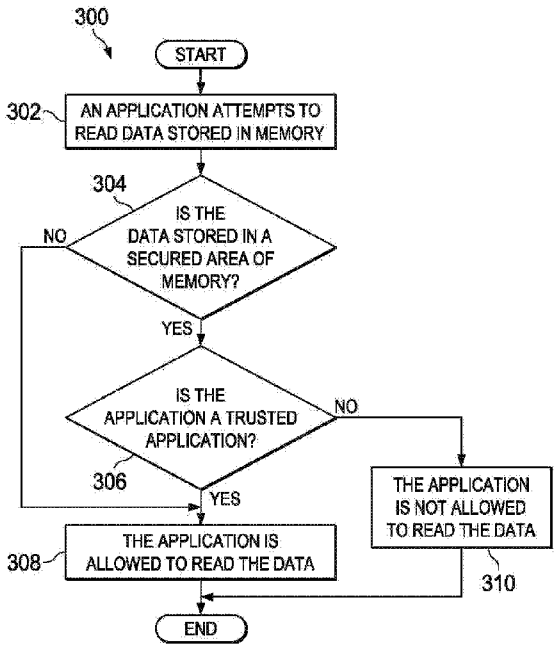


FIG. 3

(57) Abstract: Particular embodiments described herein provide for an electronic device that can be configured to monitor access to data in a secured area of memory at a hypervisor level, receive a request from a process to the data in the secured area, and deny the request if the process is not a trusted process. In an example, the electronic device is a point of sale device.

WO 2017/003584 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

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

Published:

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

PROTECTION OF SENSITIVE DATA

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of and priority to U.S. Nonprovisional (Utility) Patent Application No. 14/752,888 filed 27 June 2015 entitled "PROTECTION OF SENSITIVE DATA", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This disclosure relates in general to the field of information security, and more particularly, to the protection of sensitive data.

BACKGROUND

[0003] The field of network security has become increasingly important in today's society. The Internet has enabled interconnection of different computer networks all over the world. In particular, the Internet provides a medium for exchanging data between different users connected to different computer networks via various types of client devices. While the use of the Internet has transformed business and personal communications, it has also been used as a vehicle for malicious operators to gain unauthorized access to computers and computer networks and for intentional or inadvertent disclosure of sensitive information.

[0004] Malicious software ("malware") that infects a host computer may be able to perform any number of malicious actions, such as stealing sensitive information from a business or individual associated with the host computer, propagating to other host computers, and/or assisting with distributed denial of service attacks, sending out spam or malicious emails from the host computer, etc. Hence, significant administrative challenges remain for protecting computers and computer networks from malicious and inadvertent exploitation by malicious software and devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] To provide a more complete understanding of the present disclosure and features and advantages thereof, reference is made to the following description, taken in

conjunction with the accompanying figures, wherein like reference numerals represent like parts, in which:

[0006] FIGURE 1A is a simplified block diagram of a communication system for the protection of sensitive data, in accordance with an embodiment of the present disclosure;

[0007] FIGURE 1B is a simplified block diagram of a communication system for the protection of sensitive data, in accordance with an embodiment of the present disclosure;

[0008] FIGURE 1C is a simplified block diagram of a communication system for the protection of sensitive data, in accordance with an embodiment of the present disclosure;

[0009] ;FIGURE 2 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0010] FIGURE 3 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0011] FIGURE 4 is a block diagram illustrating an example computing system that is arranged in a point-to-point configuration in accordance with an embodiment;

[0012] FIGURE 5 is a simplified block diagram associated with an example ARM ecosystem system on chip (SOC) of the present disclosure; and

[0013] FIGURE 6 is a block diagram illustrating an example processor core in accordance with an embodiment.

[0014] The FIGURES of the drawings are not necessarily drawn to scale, as their dimensions can be varied considerably without departing from the scope of the present disclosure.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

EXAMPLE EMBODIMENTS

[0015] FIGURE 1A is a simplified block diagram of a communication system 100a for the protection of sensitive data, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1A, an embodiment of communication system 100a can include an electronic device 102a, cloud services 104, and a server 106. Electronic device 102a can include a processor 110, memory 112, a hypervisor layer 114, one or more applications 116a and 116b, and a security module 118a. Memory 112 can include secured memory 120.

Security module 118a can include a whitelist 122 and a blacklist 124. Cloud services 104 and server 106 can each include a network security module 126a. Network security module 126a can include whitelist 122 and blacklist 124. Electronic device 102a, cloud services 104, and server 106 may be in communication using network 108. Hypervisor layer 114 is a hypervisor layer or level below the operating system level of electronic device 102a.

[0016] Communication system 100a can be configured monitor read attempts to secured memory 120 at hypervisor layer 114. When application 116a (or 116b) tries to read information in secured memory 120, security module 118a can determine if application 116a (or 116b) is trusted. For example, security module 118a can use whitelist 122 to determine if application 116a (or 116b) is trusted and blacklist 124 to determine if application 116a (or 116b) is untrusted. In an example, security module 118a can communicate with network security module 126a to determine if application 116a (or 116b) is trusted or untrusted. For example, whitelist 122 and blacklist 124 may be located in network security module 126a. If application 116a (or 116b) is untrusted, then the read request can be denied.

[0017] Turning to FIGURE 1B, FIGURE 1B is a simplified block diagram of a communication system 100b for the protection of sensitive data, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1B, an embodiment of communication system 100b can include an electronic device 102b, cloud services 104, and server 106. Electronic device 102b can include processor 110, memory 112, hypervisor layer 114, one or more applications 116a and 116b, and a security module 118b. Security module 118b can include a trusted application module 128. Cloud services 104 and server 106 can each include a network security module 126b. Network security module 126b can include a network trusted application module 138. Electronic device 102b, cloud services 104 and server 106 may be in communication using network 108.

[0018] Communication system 100b can be configured monitor read attempts to secured memory 120 at hypervisor layer 114. When application 116a (or 116b) tries to read information in secured memory 120, security module 118b can determine if application 116a (or 116b) is trusted. For example, security module 118b can use trusted application module 128 to determine if application 116a (or 116b) is trusted or untrusted. Security module 118b can be configured to use one or more algorithms or other means to determine if application 116a (or 116b) is trusted or untrusted. In an example, security module 118b can

communicate with network security module 126b to determine if application 116a (or 116b) is trusted or untrusted. For example, network security module 126b may use network trusted application module 138 to determine if application 116a (or 116b) is trusted or untrusted. Network security module 126a and 126b can be configured to use one or more algorithms or other means to determine if application 116a (or 116b) is trusted or untrusted. If application116a (or 116b) is not trusted, then the read request can be denied.

[0019] Turning to FIGURE 1C, FIGURE 1C is a simplified block diagram of a communication system 100c for the protection of sensitive data, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1C, an embodiment of communication system 100c can include an electronic device 102c, a cloud services 104, and server 106. Electronic device 102c can include processor 110, memory 112, hypervisor layer 114, a security module 118c, one or more trusted processes 132, one or more untrusted processes 134, and a payment module 136. Memory 112 can include secured memory 120. Secured memory 120 can include payment data 130. Cloud services 104 and server 106 can each include a network security module 126c. Network security module 126c can include network trusted application module 138. Network trusted application module 138 can include whitelist 122 and blacklist 124. Electronic device 102c, cloud services 104 and server 106 may be in communication using network 108.

[0020] Communication system 100c can be configured monitor read attempts to secured memory 120 at hypervisor layer 114. For example, payment module 136 may receive PoS payment data such as credit card information. The PoS payment data can be stored in payment data 130 in secured memory 120. At hypervisor layer 114, security module 118c can communicate with hypervisor layer 144 and allow trusted process 132 to access payment data 130 in secured memory 120 and deny untrusted process 134 access to payment data 130 in secured memory 120. In an example, security module 118c can communicate with network security module 126c to determine if an application or process is trusted or untrusted. If the application or process is not trusted, then the read request can be denied. In an example, only if the application or process is trusted, then access to secured memory 120 is allowed. Payment module 136 can include a payment terminal, a point of sale terminal, or some other means that can interface with payment cards or other methods of facilitating electronic funds transfers.

[0021] Elements of FIGURES 1A-1C may be coupled to one another through one or more interfaces employing any suitable connections (wired or wireless), which provide viable pathways for network (e.g., network 108, etc.) communications. Additionally, any one or more of these elements of FIGURES 1A-1CB may be combined or removed from the architecture based on particular configuration needs. Communication systems 100a-100c may include a configuration capable of transmission control protocol/Internet protocol (TCP/IP) communications for the transmission or reception of packets in a network. Communication systems 100a-100c may also operate in conjunction with a user datagram protocol/IP (UDP/IP) or any other suitable protocol where appropriate and based on particular needs.

[0022] For purposes of illustrating certain example techniques of communication systems 100a-100c, it is important to understand the communications that may be traversing the network environment. The following foundational information may be viewed as a basis from which the present disclosure may be properly explained.

[0023] Modern point-of-sale (PoS) devices are quite complex and can perform many different tasks. Apart from simply being a cash register, they may include inventory management, warehousing, financial information management, etc. and many PoS devices engage in networking and cloud computing. This brings a number of information security risks to the POS infrastructure.

[0024] One the major problems with current PoS devices is bank card information leak. Standards require PoS data to be encrypted when stored on a hard drive or transmitted through the network but the data is often completely unprotected in the volatile memory, such as random access memory (RAM), of the PoS device. Furthermore the data might remain in a RAM for some time after card data processing is finished. This gives malicious operators an opportunity to steal the data by searching through the RAM of PoS device.

[0025] PoS RAM scrapers are malicious programs that search memory of PoS systems for bank card information. The PoS RAM scrappers can steal payment data, such as credit data from the RAM of PoS systems. This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to home servers.

[0026] A communication system for the protection of PoS data, as outlined in FIGURES 1A–1C, can resolve these issues (and others). Communication systems 100a-100c may be configured to monitor pages that have confidential information to monitor 'READ' attempts to the pages. For example, when confidential information is read/accessed by an untrusted processes/modules, the system can allow or deny the read/access as well as detect the process responsible for read/access. In a specific example, permissions to read or access to all the pages with confidential information is set to a deny permission. When an application or process tries to read the pages with confidential information, a violation occurs and an analysis of where the read request originated can be performed. Once the application or process that originated the read request is determined, the system can determine if the application or process is trusted. If the application or process is not trusted, then the read request can be denied.

[0027] Turning to the infrastructure of FIGURES 1A-1C, communication systems 100a-100c in accordance with an example embodiment is shown. Generally, communication systems 100a-100c can be implemented in any type or topology of networks. Network 108 represents a series of points or nodes of interconnected communication paths for receiving and transmitting packets of information that propagate through communication systems 100a-100c. Network 108 offers a communicative interface between nodes, and may be configured as any local area network (LAN), virtual local area network (VLAN), wide area network (WAN), wireless local area network (WLAN), metropolitan area network (MAN), Intranet, Extranet, virtual private network (VPN), and any other appropriate architecture or system that facilitates communications in a network environment, or any suitable combination thereof, including wired and/or wireless communication. .

[0028] In communication systems 100a-100c, network traffic, which is inclusive of packets, frames, signals, data, etc., can be sent and received according to any suitable communication messaging protocols. Suitable communication messaging protocols can include a multi-layered scheme such as Open Systems Interconnection (OSI) model, or any derivations or variants thereof (e.g., Transmission Control Protocol/Internet Protocol (TCP/IP), user datagram protocol/IP (UDP/IP)). Additionally, radio signal communications over a cellular network may also be provided in communication systems 100a-100c. Suitable

interfaces and infrastructure may be provided to enable communication with the cellular network.

[0029] The term "packet" as used herein, refers to a unit of data that can be routed between a source node and a destination node on a packet switched network. A packet includes a source network address and a destination network address. These network addresses can be Internet Protocol (IP) addresses in a TCP/IP messaging protocol. The term "data" as used herein, refers to any type of binary, numeric, voice, video, textual, or script data, or any type of source or object code, or any other suitable information in any appropriate format that may be communicated from one point to another in electronic devices and/or networks. Additionally, messages, requests, responses, and queries are forms of network traffic, and therefore, may comprise packets, frames, signals, data, etc.

[0030] In an example implementation, electronic devices 102a-102c, cloud services 104, and server 106 are network elements, which are meant to encompass network appliances, servers, routers, switches, gateways, bridges, load balancers, processors, modules, or any other suitable device, component, element, or object operable to exchange information in a network environment. Network elements may include any suitable hardware, software, components, modules, or objects that facilitate the operations thereof, as well as suitable interfaces for receiving, transmitting, and/or otherwise communicating data or information in a network environment. This may be inclusive of appropriate algorithms and communication protocols that allow for the effective exchange of data or information.

[0031] In regards to the internal structure associated with communication systems 100a-100c, each of electronic devices 102a-102c, cloud services 104, and server 106 can include memory elements for storing information to be used in the operations outlined herein. Each of electronic devices 102a-102c, cloud services 104, and server 106 may keep information in any suitable memory element (e.g., random access memory (RAM), read-only memory (ROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), application specific integrated circuit (ASIC), etc.), software, hardware, firmware, or in any other suitable component, device, element, or object where appropriate and based on particular needs. Any of the memory items discussed herein should be construed as being encompassed within the broad term 'memory element.' Moreover, the

information being used, tracked, sent, or received in communication systems 100a-100c could be provided in any database, register, queue, table, cache, control list, or other storage structure, all of which can be referenced at any suitable timeframe. Any such storage options may also be included within the broad term 'memory element' as used herein.

[0032] In certain example implementations, the functions outlined herein may be implemented by logic encoded in one or more tangible media (e.g., embedded logic provided in an ASIC, digital signal processor (DSP) instructions, software (potentially inclusive of object code and source code) to be executed by a processor, or other similar machine, etc.), which may be inclusive of non-transitory computer-readable media. In some of these instances, memory elements can store data used for the operations described herein. This includes the memory elements being able to store software, logic, code, or processor instructions that are executed to carry out the activities described herein.

[0033] In an example implementation, network elements of communication systems 100a-100c, such as electronic devices 102a-102c, cloud services 104, and server 106, may include software modules (e.g., security modules 118a-118c, network security module 126, trusted application module 128, and payment module 136) to achieve, or to foster, operations as outlined herein. These modules may be suitably combined in any appropriate manner, which may be based on particular configuration and/or provisioning needs. In example embodiments, such operations may be carried out by hardware, implemented externally to these elements, or included in some other network device to achieve the intended functionality. Furthermore, the modules can be implemented as software, hardware, firmware, or any suitable combination thereof. These elements may also include software (or reciprocating software) that can coordinate with other network elements in order to achieve the operations, as outlined herein.

[0034] Additionally, each of electronic devices 102a-102c, cloud services 104, and server 106 may include a processor that can execute software or an algorithm to perform activities as discussed herein. A processor can execute any type of instructions associated with the data to achieve the operations detailed herein. In one example, the processors could transform an element or an article (e.g., data) from one state or thing to another state or thing. In another example, the activities outlined herein may be implemented with fixed logic or programmable logic (e.g., software/computer instructions executed by a processor) and

the elements identified herein could be some type of a programmable processor, programmable digital logic (e.g., a field programmable gate array (FPGA), an EPROM, an EEPROM) or an ASIC that includes digital logic, software, code, electronic instructions, or any suitable combination thereof. Any of the potential processing elements, modules, and machines described herein should be construed as being encompassed within the broad term 'processor.'

[0035] Each of electronic devices 102a-102c can be a network element and include, for example, desktop computers, laptop computers, mobile devices, personal digital assistants, smartphones, tablets, or other similar devices. Cloud services 104 is configured to provide cloud services to electronic devices 102a-102c. Cloud services may generally be defined as the use of computing resources that are delivered as a service over a network, such as the Internet. Typically, compute, storage, and network resources are offered in a cloud infrastructure, effectively shifting the workload from a local network to the cloud network. Server 106 can be a network element such as a server or virtual server and can be associated with clients, customers, endpoints, or end users wishing to initiate a communication in communication system 100a-100c via some network (e.g., network 108). The term 'server' is inclusive of devices used to serve the requests of clients and/or perform some computational task on behalf of clients within communication systems 100a-100c. Although security module 118a is represented in FIGURE 1A as being located in electronic device 102a, security module 118b is represented in FIGURE 1B as being located in electronic device 102b, and security module 118c is represented in FIGURE 1C as being located in electronic device 102c, this is for illustrative purposes only. Security modules 118a-118c could be combined or separated in any suitable configuration. Furthermore, security modules 118a-118c could be integrated with or distributed in another network accessible by electronic devices 102a-102c such as cloud services 104 or server 106.

[0036] Turning to FIGURE 2, FIGURE 2 is an example flowchart illustrating possible operations of a flow 200 that may be associated with the protection of sensitive data, in accordance with an embodiment. In an embodiment, one or more operations of flow 200 may be performed by security module 118a-118c and network security module 126. At 202, data is received at an electronic device. At 204, the system determines if the data includes sensitive information. If the data does not include sensitive information, then the data is

stored in unsecured memory, as in 206. If the data does include sensitive information, then the data is stored in a secured area of memory, as in 208. At 210, read access to the secured area is monitored.

[0037] Turning to FIGURE 3, FIGURE 3 is an example flowchart illustrating possible operations of a flow 300 that may be associated with the protection of sensitive data, in accordance with an embodiment. In an embodiment, one or more operations of flow 300 may be performed by security module 118a-118c and network security module 126. At, 302, an application attempts to read data stored in memory. At 304, the system determines if the data is stored in a secured area of memory. If the data is not stored in a secured area of memory, then the application is allowed to read the data, as in 308. If the data is stored in a secured area of memory, then the system determines if the application is a trusted application, as in 306. If the application is a trusted application, then the application is allowed to read the data, as in 308. If the application is not a trusted application, then the application is not allowed to read the data, as in 310.

[0038] FIGURE 4 illustrates a computing system 400 that is arranged in a point-to-point (PtP) configuration according to an embodiment. In particular, FIGURE 4 shows a system where processors, memory, and input/output devices are interconnected by a number of point-to-point interfaces. Generally, one or more of the network elements of communication system 10 may be configured in the same or similar manner as computing system 400.

[0039] As illustrated in FIGURE 4, system 400 may include several processors, of which only two, processors 470 and 480, are shown for clarity. While two processors 470 and 480 are shown, it is to be understood that an embodiment of system 400 may also include only one such processor. Processors 470 and 480 may each include a set of cores (i.e., processor cores 474A and 474B and processor cores 484A and 484B) to execute multiple threads of a program. The cores may be configured to execute instruction code in a manner similar to that discussed above with reference to FIGURES 1-3. Each processor 470, 480 may include at least one shared cache 471, 481. Shared caches 471, 481 may store data (e.g., instructions) that are utilized by one or more components of processors 470, 480, such as processor cores 474 and 484.

[0040] Processors 470 and 480 may also each include integrated memory controller logic (MC) 472 and 482 to communicate with memory elements 432 and 434. Memory elements 432 and/or 434 may store various data used by processors 470 and 480. In alternative embodiments, memory controller logic 472 and 482 may be discreet logic separate from processors 470 and 480.

[0041] Processors 470 and 480 may be any type of processor and may exchange data via a point-to-point (PtP) interface 450 using point-to-point interface circuits 478 and 488, respectively. Processors 470 and 480 may each exchange data with a chipset 490 via individual point-to-point interfaces 452 and 454 using point-to-point interface circuits 476, 486, 494, and 498. Chipset 490 may also exchange data with a high-performance graphics circuit 438 via a high-performance graphics interface 439, using an interface circuit 492, which could be a PtP interface circuit. In alternative embodiments, any or all of the PtP links illustrated in FIGURE 4 could be implemented as a multi-drop bus rather than a PtP link.

[0042] Chipset 490 may be in communication with a bus 420 via an interface circuit 496. Bus 420 may have one or more devices that communicate over it, such as a bus bridge 418 and I/O devices 416. Via a bus 410, bus bridge 418 may be in communication with other devices such as a keyboard/mouse 412 (or other input devices such as a touch screen, trackball, etc.), communication devices 426 (such as modems, network interface devices, or other types of communication devices that may communicate through a computer network 460), audio I/O devices 414, and/or a data storage device 428. Data storage device 428 may store code 430, which may be executed by processors 470 and/or 480. In alternative embodiments, any portions of the bus architectures could be implemented with one or more PtP links.

[0043] The computer system depicted in FIGURE 4 is a schematic illustration of an embodiment of a computing system that may be utilized to implement various embodiments discussed herein. It will be appreciated that various components of the system depicted in FIGURE 4 may be combined in a system-on-a-chip (SoC) architecture or in any other suitable configuration. For example, embodiments disclosed herein can be incorporated into systems including mobile devices such as smart cellular telephones, tablet computers, personal digital assistants, portable gaming devices, etc. It will be appreciated that these mobile devices may be provided with SoC architectures in at least some embodiments.

[0044] Turning to FIGURE 5, FIGURE 5 is a simplified block diagram associated with an example ARM ecosystem SOC 500 of the present disclosure. At least one example implementation of the present disclosure can include the protection of sensitive data features discussed herein and an ARM component. For example, the example of FIGURE 5 can be associated with any ARM core (e.g., A-7, A-15, etc.). Further, the architecture can be part of any type of tablet, smartphone (inclusive of Android™ phones, iPhones™), iPad™, Google Nexus™, Microsoft Surface™, personal computer, server, video processing components, laptop computer (inclusive of any type of notebook), Ultrabook™ system, any type of touch-enabled input device, etc.

[0045] In this example of FIGURE 5, ARM ecosystem SOC 500 may include multiple cores 506-507, an L2 cache control 508, a bus interface unit 509, an L2 cache 510, a graphics processing unit (GPU) 515, an interconnect 502, a video codec 520, and a liquid crystal display (LCD) I/F 525, which may be associated with mobile industry processor interface (MIPI)/ high-definition multimedia interface (HDMI) links that couple to an LCD.

[0046] ARM ecosystem SOC 500 may also include a subscriber identity module (SIM) I/F 530, a boot read-only memory (ROM) 535, a synchronous dynamic random access memory (SDRAM) controller 540, a flash controller 545, a serial peripheral interface (SPI) master 550, a suitable power control 555, a dynamic RAM (DRAM) 560, and flash 565. In addition, one or more example embodiments include one or more communication capabilities, interfaces, and features such as instances of Bluetooth™ 570, a 3G modem 575, a global positioning system (GPS) 580, and an 802.11 Wi-Fi 585.

[0047] In operation, the example of FIGURE 5 can offer processing capabilities, along with relatively low power consumption to enable computing of various types (e.g., mobile computing, high-end digital home, servers, wireless infrastructure, etc.). In addition, such an architecture can enable any number of software applications (e.g., Android™, Adobe® Flash® Player, Java Platform Standard Edition (Java SE), JavaFX, Linux, Microsoft Windows Embedded, Symbian and Ubuntu, etc.). In at least one example embodiment, the core processor may implement an out-of-order superscalar pipeline with a coupled low-latency level-2 cache.

[0048] FIGURE 6 illustrates a processor core 600 according to an embodiment. Processor core 600 may be the core for any type of processor, such as a micro-processor, an

embedded processor, a digital signal processor (DSP), a network processor, or other device to execute code. Although only one processor core 600 is illustrated in Figure 6, a processor may alternatively include more than one of the processor core 600 illustrated in Figure 6. For example, processor core 600 represents one example embodiment of processors cores 474a, 474b, 484a, and 484b shown and described with reference to processors 470 and 480 of FIGURE 4. Processor core 600 may be a single-threaded core or, for at least one embodiment, processor core 600 may be multithreaded in that it may include more than one hardware thread context (or "logical processor") per core.

[0049] FIGURE 6 also illustrates a memory 602 coupled to processor core 600 in accordance with an embodiment. Memory 602 may be any of a wide variety of memories (including various layers of memory hierarchy) as are known or otherwise available to those of skill in the art. Memory 602 may include code 604, which may be one or more instructions, to be executed by processor core 600. Processor core 600 can follow a program sequence of instructions indicated by code 604. Each instruction enters a front-end logic 606 and is processed by one or more decoders 608. The decoder may generate, as its output, a micro operation such as a fixed width micro operation in a predefined format, or may generate other instructions, microinstructions, or control signals that reflect the original code instruction. Front-end logic 606 also includes register renaming logic 610 and scheduling logic 612, which generally allocate resources and queue the operation corresponding to the instruction for execution.

[0050] Processor core 600 can also include execution logic 614 having a set of execution units 616-1 through 616-N. Some embodiments may include a number of execution units dedicated to specific functions or sets of functions. Other embodiments may include only one execution unit or one execution unit that can perform a particular function. Execution logic 614 performs the operations specified by code instructions.

[0051] After completion of execution of the operations specified by the code instructions, back-end logic 618 can retire the instructions of code 604. In one embodiment, processor core 600 allows out of order execution but requires in order retirement of instructions. Retirement logic 620 may take a variety of known forms (e.g., re-order buffers or the like). In this manner, processor core 600 is transformed during execution of code 604, at least in terms of the output generated by the decoder, hardware registers and tables

utilized by register renaming logic 610, and any registers (not shown) modified by execution logic 614.

[0052] Although not illustrated in FIGURE 6, a processor may include other elements on a chip with processor core 600, at least some of which were shown and described herein with reference to FIGURE 6. For example, as shown in FIGURE 6, a processor may include memory control logic along with processor core 600. The processor may include I/O control logic and/or may include I/O control logic integrated with memory control logic.

[0053] Note that with the examples provided herein, interaction may be described in terms of two, three, or more network elements. However, this has been done for purposes of clarity and example only. In certain cases, it may be easier to describe one or more of the functionalities of a given set of flows by only referencing a limited number of network elements. It should be appreciated that communication systems 100a-100c and their teachings are readily scalable and can accommodate a large number of components, as well as more complicated/sophisticated arrangements and configurations. Accordingly, the examples provided should not limit the scope or inhibit the broad teachings of communication system 10 as potentially applied to a myriad of other architectures.

[0054] It is also important to note that the operations in the preceding flow diagrams (i.e., FIGURES 2 and 3) illustrate only some of the possible correlating scenarios and patterns that may be executed by, or within, communication systems 100a-100c. Some of these operations may be deleted or removed where appropriate, or these operations may be modified or changed considerably without departing from the scope of the present disclosure. In addition, a number of these operations have been described as being executed concurrently with, or in parallel to, one or more additional operations. However, the timing of these operations may be altered considerably. The preceding operational flows have been offered for purposes of example and discussion. Substantial flexibility is provided by communication systems 100a-100c in that any suitable arrangements, chronologies, configurations, and timing mechanisms may be provided without departing from the teachings of the present disclosure.

[0055] Although the present disclosure has been described in detail with reference to particular arrangements and configurations, these example configurations and arrangements may be changed significantly without departing from the scope of the present disclosure.

Moreover, certain components may be combined, separated, eliminated, or added based on particular needs and implementations. Additionally, although communication systems 100a-100c have been illustrated with reference to particular elements and operations that facilitate the communication process, these elements and operations may be replaced by any suitable architecture, protocols, and/or processes that achieve the intended functionality of communication systems 100a-100c.

[0056] Numerous other changes, substitutions, variations, alterations, and modifications may be ascertained to one skilled in the art and it is intended that the present disclosure encompass all such changes, substitutions, variations, alterations, and modifications as falling within the scope of the appended claims. In order to assist the United States Patent and Trademark Office (USPTO) and, additionally, any readers of any patent issued on this application in interpreting the claims appended hereto, Applicant wishes to note that the Applicant: (a) does not intend any of the appended claims to invoke paragraph six (6) of 35 U.S.C. section 112 as it exists on the date of the filing hereof unless the words "means for" or "step for" are specifically used in the particular claims; and (b) does not intend, by any statement in the specification, to limit this disclosure in any way that is not otherwise reflected in the appended claims.

OTHER NOTES AND EXAMPLES

[0057] Example C1 is at least one machine readable medium having one or more instructions that when executed by at least one processor, cause the at least one processor to monitor, by a security module, access to data in a secured area of memory at a hypervisor level, receive a request from a process to the data in the secured area, and deny the request if the process is not a trusted process.

[0058] In Example C2, the subject matter of Example C1 can optionally include where the one or more instructions that when executed by the at least one processor, further cause the at least one processor to set a permission to read the data in the secured area of memory to a deny permission.

[0059] In Example C3, the subject matter of any one of Examples C1-C2 can optionally include where the one or more instructions that when executed by the at least one

processor, further cause the at least one processor to determine if the process is a trusted process.

[0060] In Example C4, the subject matter of any one of Examples C1-C3 can optionally include where the one or more instructions that when executed by the at least one processor, further cause the at least one processor to allow the request if the process is a trusted process or is included in a whitelist.

[0061] In Example C5, the subject matter of any one of Examples C1-C4 can optionally include where the electronic device is a point of sale device.

[0062] In Example A1, an electronic device can include a security module, where the security module is configured to monitor access to data in a secured area of memory at a hypervisor level, receive a request from a process to the data in the secured area, and deny the request if the process is not a trusted process.

[0063] In Example, A2, the subject matter of Example A1 can optionally include where the security module is further configured to set a permission to read the data in the secured area of memory to a deny permission.

[0064] In Example A3, the subject matter of any one of Examples A1-A2 can optionally include where the security module is further configured to determine if the process is a trusted process.

[0065] In Example A4, the subject matter of any one of Examples A1-A3 can optionally include where the security module is further configured to allow the request if the process is a trusted process or is included in a whitelist.

[0066] In Example A5, the subject matter of any one of Examples A1-A4 can optionally include where the electronic device is a point of sale device.

[0067] Example M1 is a method including monitoring access to data in a secured area of memory at a hypervisor level, receiving a request from a process to the data in the secured area, and denying the request if the process is not a trusted process.

[0068] In Example M2, the subject matter of Example M1 can optionally include setting a permission to read the data in the secured area of memory to a deny permission.

[0069] In Example M3, the subject matter of any one of the Examples M1-M2 can optionally include determining if the process is a trusted process.

[0070] In Example M4, the subject matter of any one of the Examples M1-M3 can optionally include allowing the request if the process is a trusted process or is included in a whitelist.

[0071] In Example M5, the subject matter of any one of the Examples M1-M4 can optionally include where the electronic device is a point of sale device.

[0072] Example S1 is a system for protecting data, the system including a security module configured to monitor access to data in a secured area of memory at a hypervisor level, receive a request from a process to the data in the secured area, and deny the request if the process is not a trusted process.

[0073] In Example S2, the subject matter of Example S1 can optionally include where the system is further configured to set a permission to read the data in the secured area of memory to a deny permission.

[0074] In Example S3, the subject matter of any one of Examples S1-S2 can optionally include where the system is further configured to determine if the process is a trusted process.

[0075] In Example S4, the subject matter of any one of Examples S1-S3 can optionally include where the system is further configured to allow the request if the process is a trusted process or is included in a whitelist.

[0076] In Example S5, the subject matter of any one of Examples S1-S4 can optionally include where the electronic device is a point of sale device.

[0077] Example X1 is a machine-readable storage medium including machine-readable instructions to implement a method or realize an apparatus as in any one of the Examples A1-A5, or M1-M5. Example Y1 is an apparatus comprising means for performing of any of the Example methods M1-M5. In Example Y2, the subject matter of Example Y1 can optionally include the means for performing the method comprising a processor and a memory. In Example Y3, the subject matter of Example Y2 can optionally include the memory comprising machine-readable instructions.

CLAIMS:

1. At least one machine readable medium comprising one or more instructions that when executed by at least one processor, cause the at least one processor to:

monitor, by a security module, access to data in a secured area of memory at a hypervisor level;

receive a request from a process to access the data in the secured area; and

deny the request if the process is not a trusted process.

2. The at least one machine readable medium of Claim 1, further comprising one or more instructions that when executed by the at least one processor, further cause the at least one processor to:

set a permission to read the data in the secured area of memory to a deny permission.

3. The at least one machine readable medium of any of Claims 1 and 2, further comprising one or more instructions that when executed by the at least one processor, further cause the at least a processor to:

determine if the process is trusted process.

4. The at least one machine readable medium of any of Claims 1-3, further comprising one or more instructions that when executed by the at least one processor, further cause the at least one processor to:

allow the request if the process is a trusted process or is included in a whitelist.

5. The at least one machine readable medium of any of Claims 1-4, wherein the electronic device is a point of sale device.

6. An apparatus comprising:

a security module configured to:

monitor access to data in a secured area of memory at a hypervisor level;

receive a request from a process to access the data in the secured area; and

deny the request if the process is not a trusted process.

7. The apparatus of Claim 6, wherein the security module is further configured to:

set a permission to read the data in the secured area of memory to a deny permission.

8. The apparatus of any of Claims 6 and 7, wherein the security module is further configured to:

determine if the process is a trusted process.

9. The apparatus of any of Claims 6-8 wherein the security module is further configured to:

allow the request if the process is a trusted process or is included in a whitelist.

10. The apparatus of any of Claims 6-9, wherein the electronic device is a point of sale device.

11. A method comprising:

monitoring access to data in a secured area of memory at a hypervisor level;

receiving a request from a process to the data in the secured area; and

denying the request if the process is not a trusted process.

12. The method of Claim 11, further comprising:

setting a permission to read the data in the secured area of memory to a deny permission.

13. The method of any of Claims 11 and 12, further comprising:

determining if the process is a trusted process.

14. The method of any of Claims 11-13, further comprising:

allowing the request if the process is a trusted process or is included in a whitelist.

15. The method of any of Claims 11-14, wherein the electronic device is a point of sale device.

16. A system for protecting data, the system comprising:

a security module configured to:

monitor access to data in a secured area of memory at a hypervisor level;

receive a request from a process to the data in the secured area; and

deny the request if the process is not a trusted process.

17. The system of Claim 16, wherein the system is further configured to:

set a permission to read the data in the secured area of memory to a deny permission.

18. The system of any of Claims 16 and 17, wherein the system is further configured to:

determine if the process is a trusted process.

19. The system of any of Claims 16-18, wherein the system is further configured to:

allow the request if the process is a trusted process or is included in a whitelist.

20. The system of any of Claims 16-19, wherein the electronic device is a point of sale device.

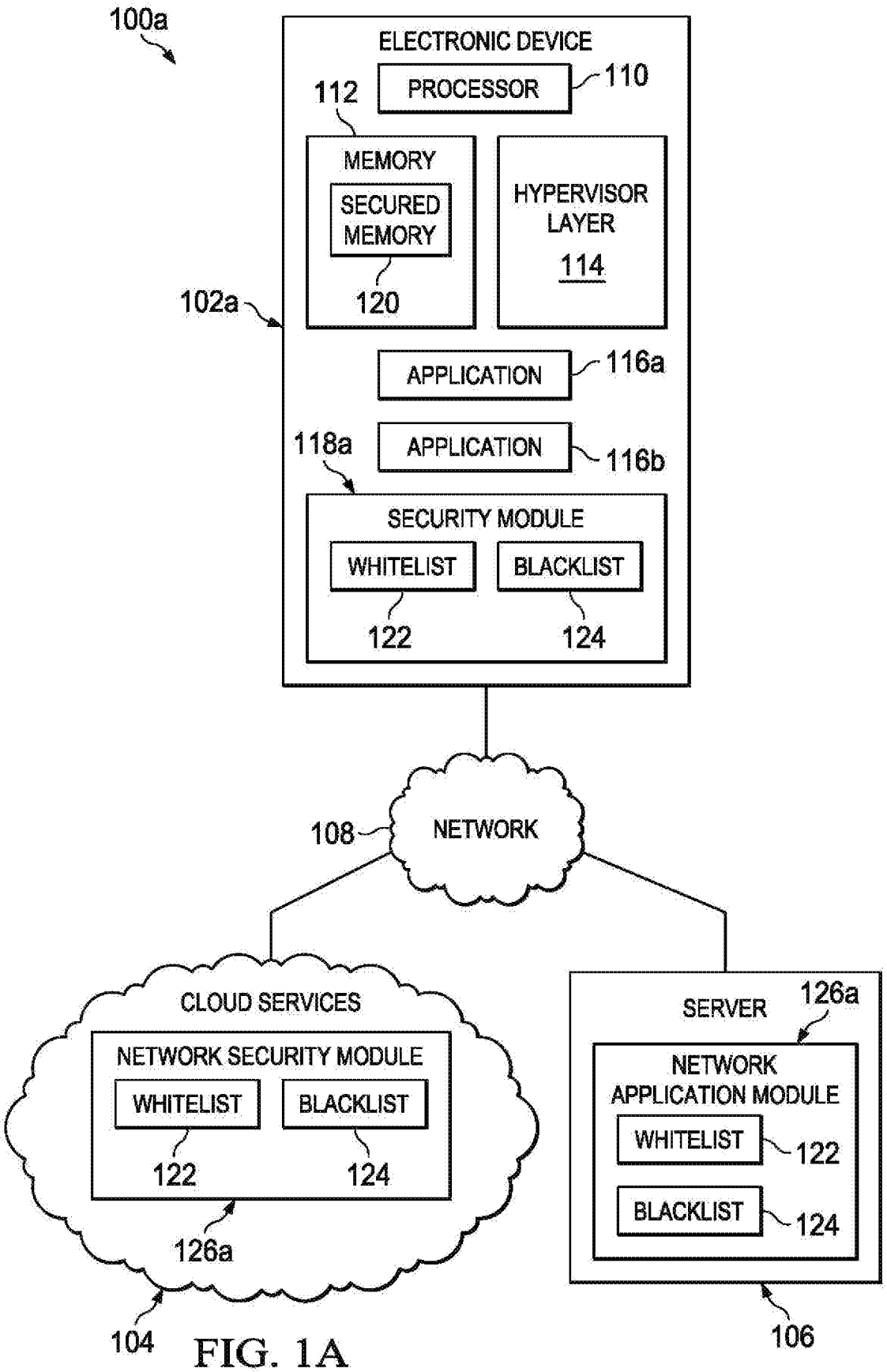

100a
ELECTRONIC DEVICE
PROCESSOR
110
112
MEMORY
SECURED MEMORY
120
HYPERVISOR LAYER
114
102a
APPLICATION
116a
118a
APPLICATION
116b
SECURITY MODULE
WHITELIST
BLACKLIST
122
124
NETWORK
108
CLOUD SERVICES
NETWORK SECURITY MODULE
WHITELIST
BLACKLIST
122
124
126a
104
SERVER
126a
NETWORK APPLICATION MODULE
WHITELIST
122
BLACKLIST
124
106

FIG. 1A

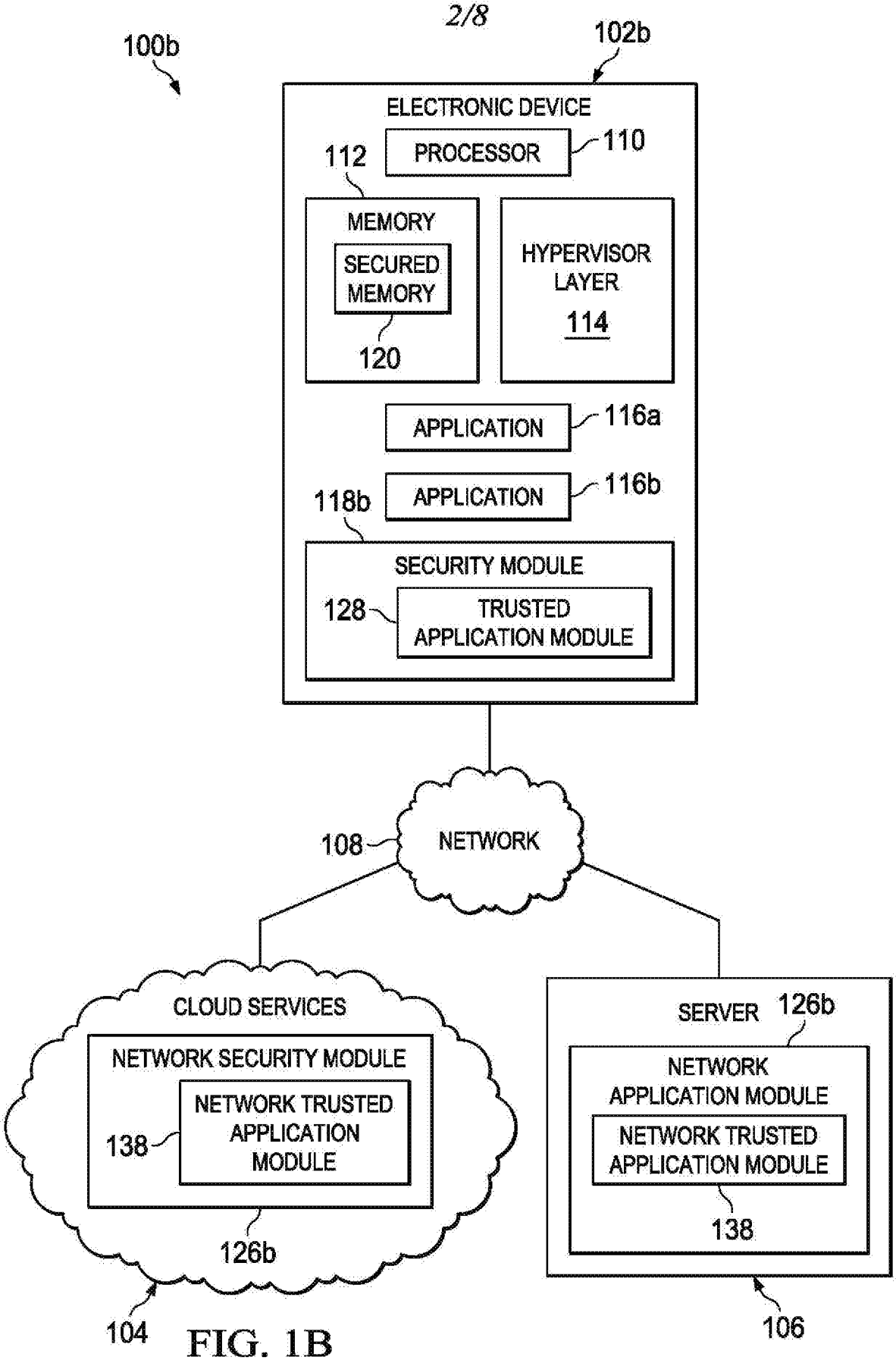

100b
102b
ELECTRONIC DEVICE
PROCESSOR
110
112
MEMORY
SECURED MEMORY
120
HYPERVISOR LAYER
114
APPLICATION
116a
APPLICATION
116b
118b
SECURITY MODULE
128
TRUSTED APPLICATION MODULE
108
NETWORK
CLOUD SERVICES
NETWORK SECURITY MODULE
NETWORK TRUSTED APPLICATION MODULE
138
126b
104
SERVER
126b
NETWORK APPLICATION MODULE
NETWORK TRUSTED APPLICATION MODULE
138
106

FIG. 1B

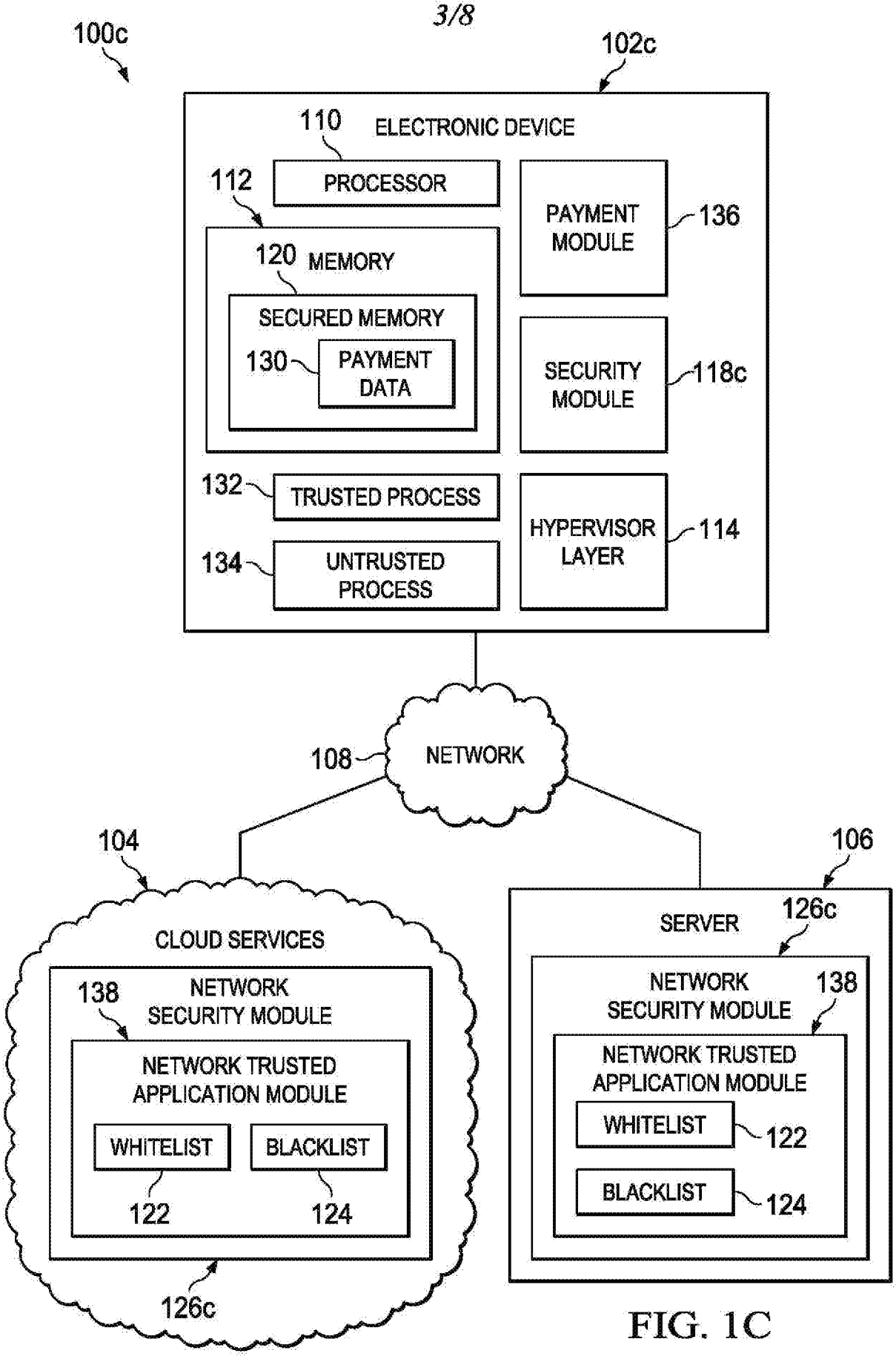

100c
102c
110
ELECTRONIC DEVICE
112
PROCESSOR
120
MEMORY
SECURED MEMORY
130
PAYMENT DATA
PAYMENT MODULE
136
SECURITY MODULE
118c
132
TRUSTED PROCESS
134
UNTRUSTED PROCESS
HYPERVISOR LAYER
114
108
NETWORK
104
CLOUD SERVICES
138
NETWORK SECURITY MODULE
NETWORK TRUSTED APPLICATION MODULE
WHITELIST
BLACKLIST
122
124
126c
106
SERVER
126c
NETWORK SECURITY MODULE
138
NETWORK TRUSTED APPLICATION MODULE
WHITELIST
122
BLACKLIST
124

FIG. 1C

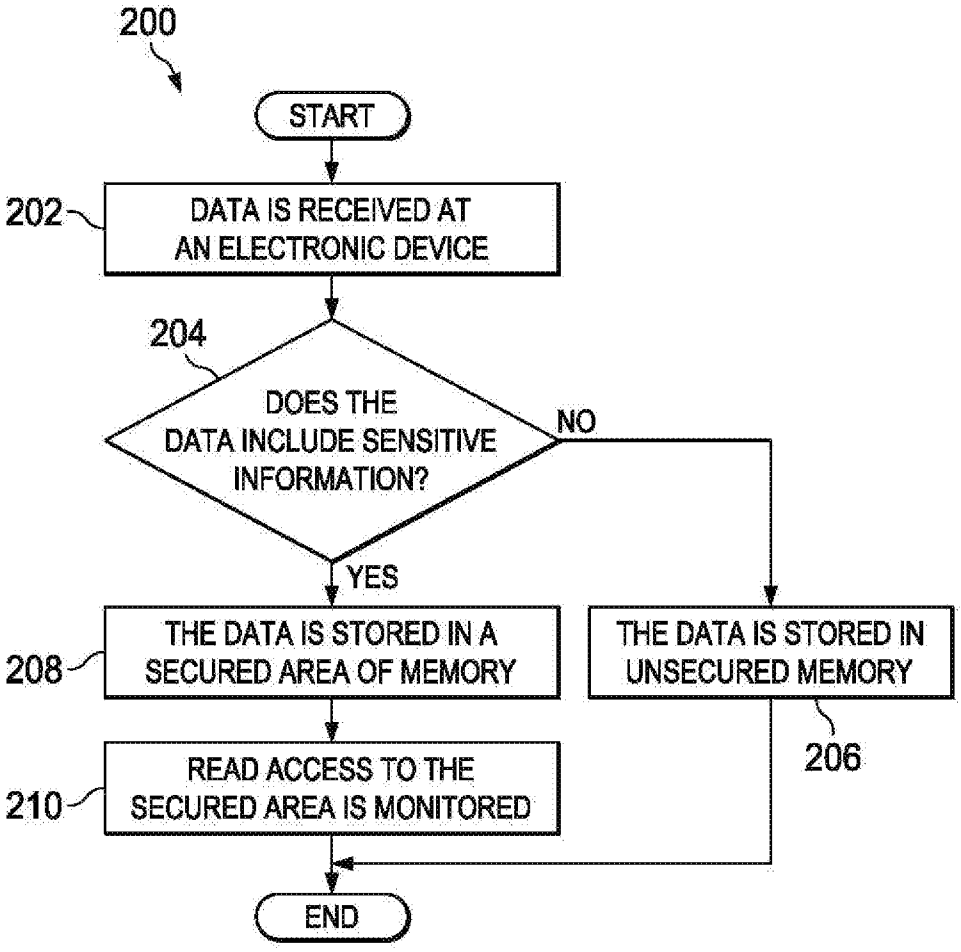

200
START
202
DATA IS RECEIVED AT AN ELECTRONIC DEVICE
204
DOES THE DATA INCLUDE SENSITIVE INFORMATION?
NO
YES
208
THE DATA IS STORED IN A SECURED AREA OF MEMORY
THE DATA IS STORED IN UNSECURED MEMORY
206
210
READ ACCESS TO THE SECURED AREA IS MONITORED
END

FIG. 2

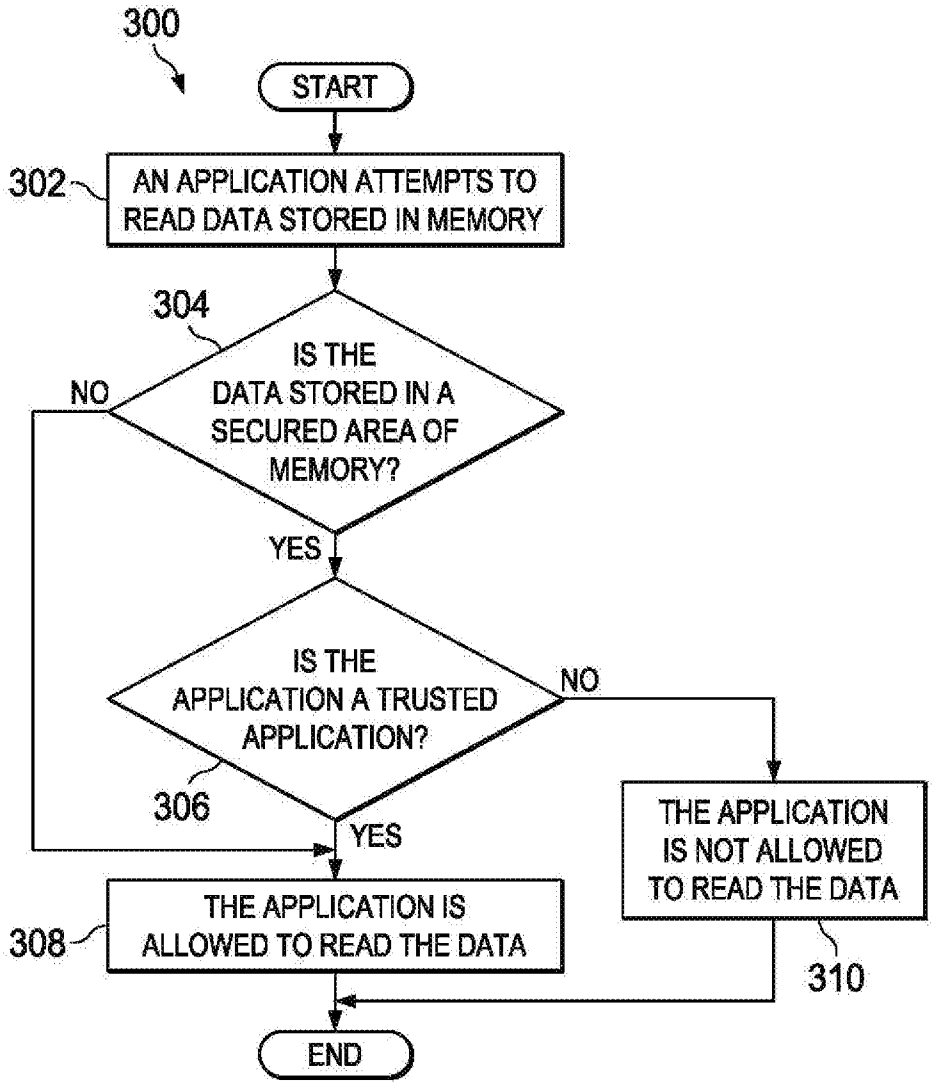

300
START
302
AN APPLICATION ATTEMPTS TO READ DATA STORED IN MEMORY
304
IS THE DATA STORED IN A SECURED AREA OF MEMORY?
NO
YES
IS THE APPLICATION A TRUSTED APPLICATION?
NO
306
YES
THE APPLICATION IS NOT ALLOWED TO READ THE DATA
310
308
THE APPLICATION IS ALLOWED TO READ THE DATA
END

FIG. 3

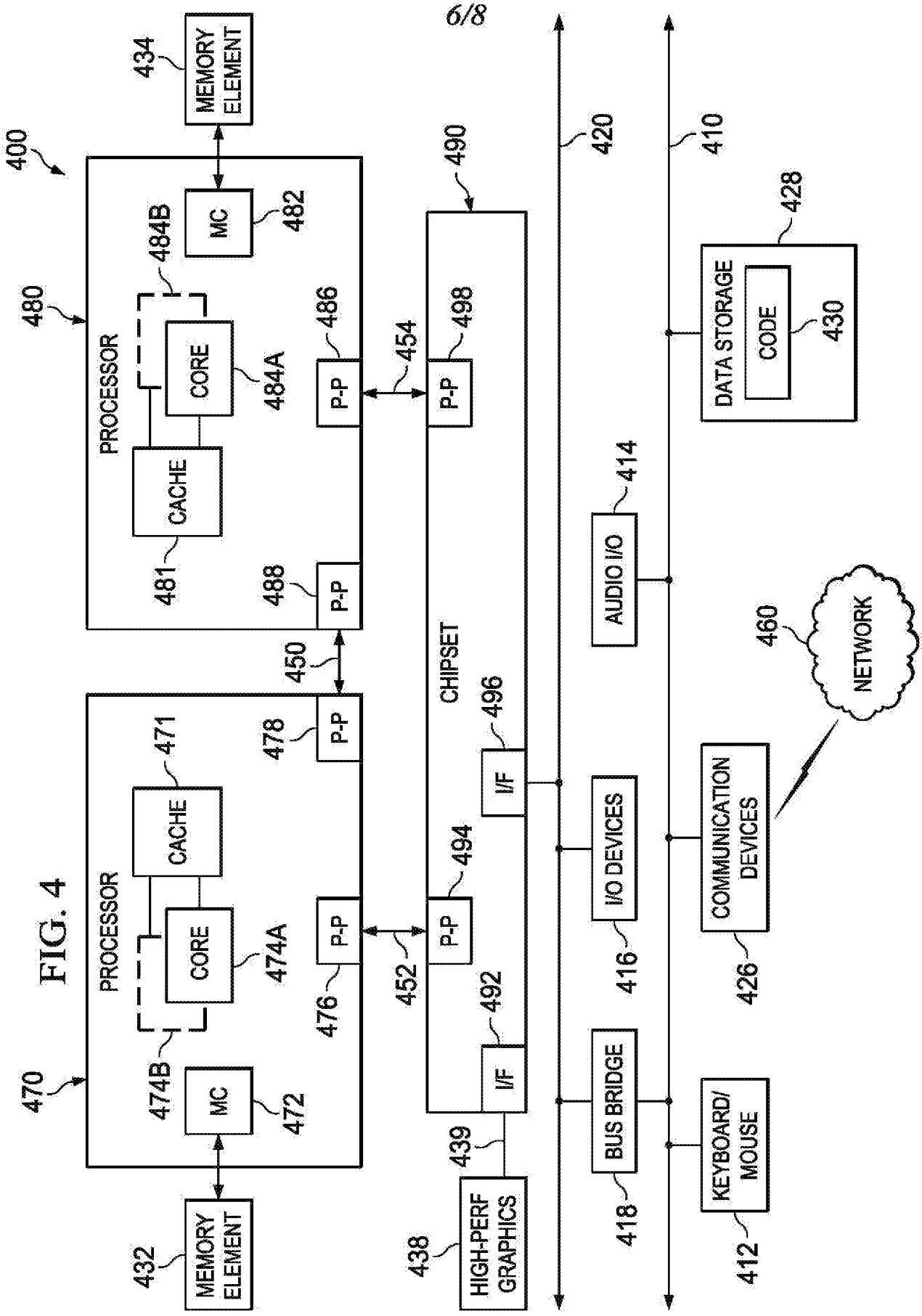
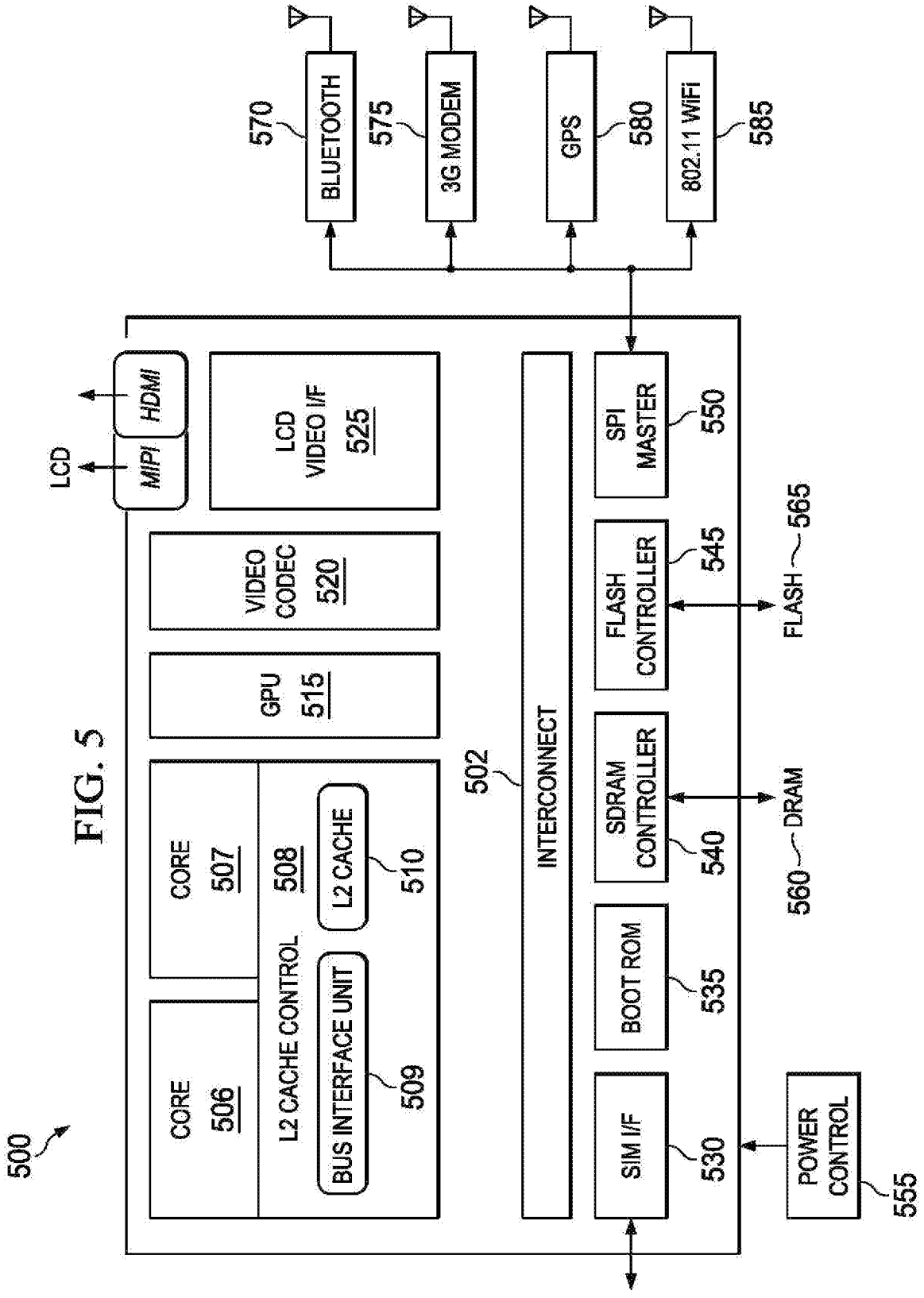

400
434
MEMORY ELEMENT
480
PROCESSOR
484B
MC
482
CORE
484A
CACHE
481
486
P-P
488
P-P
454
450
490
CHIPSET
498
P-P
496
I/F
494
P-P
492
I/F
439
438
HIGH-PERF GRAPHICS
420
410
428
DATA STORAGE
CODE
430
414
AUDIO I/O
460
NETWORK
416
I/O DEVICES
426
COMMUNICATION DEVICES
418
BUS BRIDGE
412
KEYBOARD/ MOUSE
470
PROCESSOR
471
CACHE
474A
CORE
474B
MC
472
476
P-P
478
P-P
452
432
MEMORY ELEMENT

FIG. 4

FIG. 5


500
CORE 506
CORE 507
L2 CACHE CONTROL 508
BUS INTERFACE UNIT 509
L2 CACHE 510
GPU 515
VIDEO CODEC 520
LCD VIDEO I/F 525
LCD
MIPI
HDMI
502
INTERCONNECT
SPI MASTER 550
FLASH CONTROLLER 545
FLASH 565
SDRAM CONTROLLER 540
DRAM 560
BOOT ROM 535
SIM I/F 530
POWER CONTROL 555
570 BLUETOOTH
575 3G MODEM
580 GPS
585 802.11 WiFi

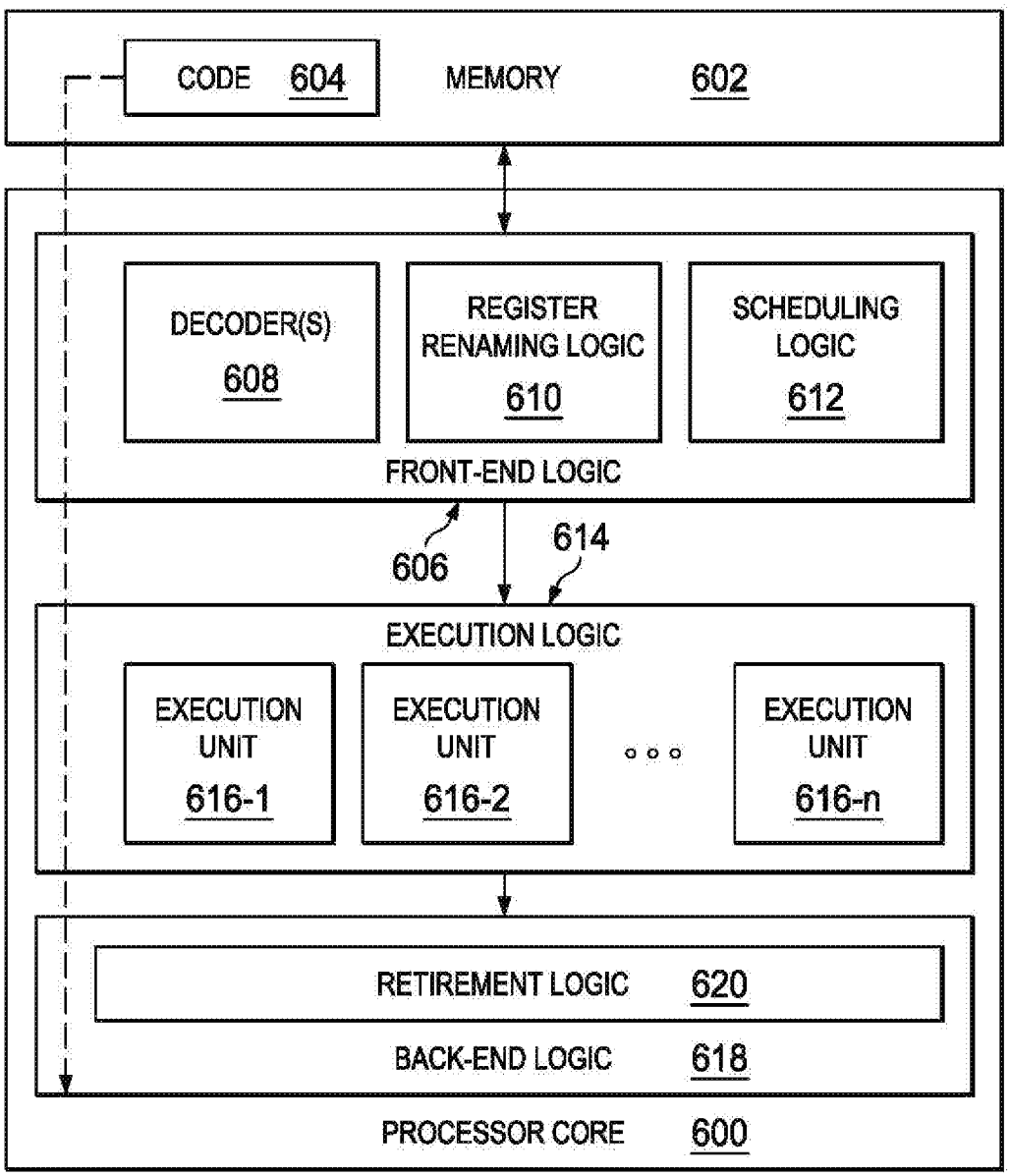

CODE 604
MEMORY 602
DECODER(S) 608
REGISTER RENAMING LOGIC 610
SCHEDULING LOGIC 612
FRONT-END LOGIC
606
614
EXECUTION LOGIC
EXECUTION UNIT 616-1
EXECUTION UNIT 616-2
EXECUTION UNIT 616-n
RETIREMENT LOGIC 620
BACK-END LOGIC 618
PROCESSOR CORE 600

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/033863

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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 29/06; G06F 21/44; G06F 3/06; G07G 1/14; G07G 1/00; G06F 12/14; H04L 9/32; H04W 12/08; G06F 21/31

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
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: memory, secured area, access, allow, deny, whitelist

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015-0106871 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 April 2015 See paragraphs [0037]-[0051], [0060]-[0072] and figures 1, 3.	1-20
A	US 2007-0061596 A1 (NIELS T. FERGUSON et al.) 15 March 2007 See paragraphs [0029]-[0034] and figures 5-6.	1-20
A	US 2014-0351607 A1 (DOV MORAN et al.) 27 November 2014 See paragraphs [0059]-[0074] and figure 3.	1-20
A	US 8984592 B1 (SPRINT COMMUNICATIONS COMPANY L.P.) 17 March 2015 See column 11, line 30 - column 15, line 29 and figure 2.	1-20
A	JP 2014-137821 A (CHOU HUNG-CHIEN) 28 July 2014 See paragraphs [0013]-[0032] and figures 2-3.	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
24 August 2016 (24.08.2016)	**24 August 2016 (24.08.2016)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
LEE, EUN KYU
Telephone No. +82-42-481-3580

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/033863

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015-0106871 A1	16/04/2015	CN 00496746 C	10/06/2009
		CN 100768955 A	10/05/2006
		KR 10-2015-0043954 A	23/04/2015
US 2007-0061596 A1	15/03/2007	CN 101263463 A	10/09/2008
		CN 101263463 B	30/05/2012
		KR 10-1330492 B1	15/11/2013
		KR 10-2008-0049742 A	04/06/2008
		RU 2008110057 A	20/09/2009
		RU 2458385 C2	10/08/2012
		US 8799680 B2	05/08/2014
		WO 2007-035453 A1	29/03/2007
US 2014-0351607 A1	27/11/2014	IL 148834 A	08/03/2007
		IL 148834 D0	12/09/2002
		US 2013-0275771 A1	17/10/2013
		US 8826043 B2	02/09/2014
US 8984592 B1	17/03/2015	None	
JP 2014-137821 A	28/07/2014	AU 2014-100037 A4	13/02/2014
		CA 2839332 A1	15/07/2014
		CN 103927652 A	16/07/2014
		EP 2755178 A1	16/07/2014
		RU 2544798 C1	20/03/2015
		TW 201428651 A	16/07/2014
		US 2014-0201016 A1	17/07/2014