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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/144815 A2

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

(21) International Application Number:
PCT/US2010/038333

(22) International Filing Date:
11 June 2010 (11.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/186,330 11 June 2009 (11.06.2009) US

(71) Applicant *(for all designated States except US):* **PANASONIC AVIONICS CORPORATION** [US/US]; 26200 Enterprise Way, Lake Forest, CA 92630-8400 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only):* **DIERICKX, Michael** [US/US]; 46277 Miner Trail, Temecula, CA 92592 (US).

(74) Agents: STOCKWELL, Davin, **M.** et al; ORRICK HERRINGTON & SUTCLIFFE LLP, 4 Park Plaza, Suite 1600, Irvine, CA 92614-2558 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, **AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, **BJ,** CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

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

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: SYSTEM AND METHOD FOR PROVIDING SECURITY ABOARD A MOVING PLATFORM

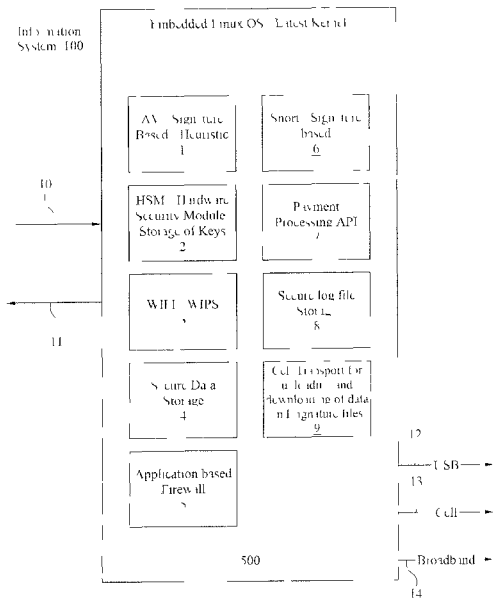


FIG. 1

(57) Abstract: A system for providing network security on a vehicle information system and methods for manufacturing and using same. The security system comprises an all-in-one security system that facilitates security system functions for the vehicle information system. Exemplary security system functions include secure storage of keys used to encrypt and/or decrypt system data, security-related application programming interfaces, a security log file, and/or private data. The security system likewise can utilize antivirus software, anti-spyware software, an application firewall and/or a network firewall. As desired, the security system can include an intrusion prevention system and/or an intrusion detection system. If the information system includes a wireless distribution system, the security system can include an intrusion prevention (and/or detection) system that is suitable for use with wireless network systems. Thereby, the security system advantageously can provide a defense in depth approach by adding multiple layers of security to the information system.

WO 2010/144815 A2

SYSTEM AND METHOD FOR PROVIDING SECURITY BOARD A MOVING PLATFORM

FIELD

[0001] The present application relates generally to network security systems and more particularly, but not exclusively, to security systems suitable for use with vehicle information systems installed aboard passenger vehicles.

BACKGROUND

[0002] Vehicles, such as automobiles and aircraft, often include vehicle information systems for satisfying passenger demand for access to viewing content, such as entertainment, information content, or other viewing content, while traveling.

[0003] Conventional vehicle information (or entertainment) systems typically include overhead cabin video systems or seat-based video systems with individual controls such that viewing content is selectable by the passengers. Handheld (or portable) media devices also can be made available for selecting and presenting the viewing content. The viewing content can include audio and video content that is derived from a variety of content sources. Prerecorded viewing content, such as motion pictures and music, can be provided by internal content sources, such as audio and video players, that are installed aboard the vehicle. The conventional vehicle information systems likewise can include antenna systems for receiving viewing content, such as live television programming and/or Internet content, transmitted from one or more content providers (or sources) that are external to, and/or remote from, the vehicle. As desired, viewing content likewise can be stored within an internal memory system of the portable media devices.

[0004] Conventional vehicle information systems, however, suffer from numerous disadvantages. For example, few conventional vehicle information systems provide robust network security. Those vehicle information systems that do provide security distribute security components across multiple system elements, such as line replaceable units (or LRUs). However, these system elements themselves are insecure. For example, hardware and software applications that process and store commercial transaction information, such as credit card payment data, are distributed throughout current vehicle information systems, exposing sensitive data and placing confidential information at risk. Further, conventional vehicle information systems cannot identify security breaches.

[0005] This application claims priority to United States provisional patent application, Serial No. 61/186,330, filed June 11, 2009. Priority to the provisional patent application is expressly claimed, and the disclosure of the provisional application is hereby incorporated herein by reference in its entirety and for all purposes.

[0006] In view of the foregoing, a need exists for an improved system and method for providing security for vehicte information systems in an effort to overcome the aforementioned obstacles and deficiencies of conventional vehicle information systems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Fig. 1 is an exemplary top-level block diagram illustrating an embodiment of a security system for information systems, wherein the security system is disposed within a single line replaceable unit.

[0008] Fig. 2A is an exemplary block diagram illustrating a selected method by which data can propagate through the security system of Fig. 1.

[0009] Fig. 2B is an exemplary block diagram illustrating an alternative method by which the data can propagate through the security system of Fig. 1, wherein the data is provided to the security system in a wireless manner.

[0010] Fig. 2C is an exemplary block diagram illustrating another alternative method by which the data can propagate through the security system of Fig. 1, wherein the data comprises a security log file for storage in a secure log file storage system.

[0011] Fig. 2D is an exemplary block diagram illustrating another alternative method by which the data can propagate through the security system of Fig. 1, wherein the data comprises payment application data.

[0012] Fig. 2E is an exemplary block diagram illustrating another alternative method by which the data can propagate through the security system of Fig. 1, wherein the data is stored in a secure data storage system.

[0013] Fig. 2F is an exemplary block diagram illustrating another alternative method by which the data can propagate through the security system of Fig. 1, wherein the data comprises secure payment application code.

[0014] Fig. 3A is an exemplary top-level drawing illustrating the information system of Fig. I, wherein the information system comprises a vehicle information system installed aboard an automobile.

{0015] Fig. 3B is an exemplary top-level drawing illustrating the vehicle information system of Fig, 3A, wherein the vehicle information system is installed aboard an aircraft and is configured to communicate with the content system of Fig. 1.

[0016] Fig. 4 is an exemplary detail drawing illustrating one preferred embodiment of a distribution system for the vehicle information systems of Figs. 3A-B.

[0017] Fig. 5A is an exemplary detail drawing illustrating a passenger cabin of a vehicle, wherein the vehicle information system of Figs. 3A-B has been installed.

[0018] Fig. 5B is an exemplary detail drawing illustrating an embodiment of the vehicle information system of Fig. 5A, wherein the vehicle information system is in communication with a personal media device.

[0019] Fig. 6 is an exemplary detail drawing illustrating an alternative embodiment of the security system of Fig. 1, wherein the security system includes a biometric device for preventing unauthorized access to the vehicle information system.

[0020] It should be noted that the figures are not drawn to scale and that elements of similar structures or functions are generally represented by like reference numerals for illustrative purposes throughout the figures. It also should be noted that the figures are only intended to facilitate the description of the preferred embodiments. The figures do not illustrate every aspect of the described embodiments and do not limit the scope of the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

(0021] Since conventional security systems for vehicle information systems are distributed across multiple, insecure system elements and cannot identify security breaches, a security system that provides network security to a vehicle information system and that is disposed within a single system element can prove desirable and provide a basis for a wide range of system applications, such as vehicle information systems for use aboard automobiles, aircraft, ships, buses, trains and other types of conventional passenger vehicles during travel. This result can be achieved, according to one embodiment disclosed herein, by the security system 500 as illustrated in Fig. 1.

[0022] Turning to Fig. 1, the security system 500 can provide network security for an information system 100. The security system 500 is shown as being provided as an integrated security system. In other words, the security system 500 can be disposed within a single system element of the information system 100. The security system 500 advantageously can comprise an all-in-one security system that facilitates security system functions, in whole and/or in part, for the information system 100. Thereby, the security system 500 can provide a defense in depth approach by adding multiple layers of security to the information system 100.

[0023] The security system 500 can provide selected security system functions such as secure storage of keys used to encrypt and/or decrypt system data, storage of security-related application programming interfaces (APIs), storage of a security log file, and/or secure storage for private data, such as user (or passenger) credit card data and/or medical data. The security system 500 likewise can utilize antivirus software, anti-spyware software, an application firewall, and/or a network firewall. As desired, the security system 500 can include an intrusion prevention system (IPS) and/or an intrusion detection system (IDS), If the

information system 100 includes a wireless communication (or distribution) system 320 (shown in Figs. 3A-2B), such as a wireless fidelity (Wi-Fi) network, for example, the security system 500 can include an intrusion prevention system (IPS) and/or an intrusion detection system (IDS) that is suitable for use with wireless network systems. The security system functions described herein are not exhaustive and are provided herein for purposes of illustration only and not for purposes of limitation.

[0024] Exemplary security system functions of the security system 500 are discussed in more detail below with reference to Fig. 1. The security system functions of the security system 500 can comprise any conventional type of security system functions and are shown and described with reference to Fig. 1 for purpose of illustration only and not for purposes of limitation. The security system 500, for example, can include antivirus (and/or anti-malware) software 1 for scanning network traffic, files, and/or other conventional types of data being exchanged with the information system 100. Preferably, the antivirus software 1 is signature-based antivirus software. The antivirus software 1 thereby can be periodically (or regularly) updated, such as at least once a month, for the latest virus signatures. As the data is transmitted through the security system 500, the antivirus software 1 can inspect the data against its virus signature files and thereby allow safe data to propagate and/or prevent malicious code from harming either the security system 500, the information system 100, and/or adjacent peripheral systems, e.g., an In-Flight Entertainment system.

[0025] Alternatively, and/or additionally, the security system 500 advantageously can utilize hardware based encryption. As illustrated in Fig. 1, Hardware Security Module (HSM) 2 of the security system 500 can be provided as an integrated circuit device that stores sensitive information using hardware encryption. For example, the HSM 2 may manage digital keys, accelerate cryptoprocesses in terms of digital signings and provide strong authentication to access critical keys for various software modules or LRUs. The encryption keys thereby can be stored in a secure place to reduce risk exposure. HSM 2 preferably meets and/or exceeds Federal Information Processing Standard (FIPS) level II certification. As desired, the HSM 2 system may handle asymmetric key pairs (and certificates) used in public key cryptography and symmetric keys. HSM 2 is a more robust security solution than conventional security solutions because software encryption-based designs can be utilized to hide information but can be reverse engineered, risking exposure to sensitive data. Software encryption-based designs likewise may present significant risk. For example, the design may be disclosed (or otherwise discovered), and/or some unforeseen event could happen to the limited number of people who know the design.

[0026] If the information system 100 includes a wireless distribution system 320 (Figs. 3A, 3B)$_1$ the security system 500 may include a wireless fidelity (Wi-Fi) device 3. The Wi-Fi device 3 preferably has a built-in access point 368 (shown in Fig. 5B), such as a wireless access point (WAP), that supports wireless communications. Communications for the Wi-Fi device 3, in whole and/or in part, can pass through the wireless access point. Since wireless connectivity typically is deemed insecure, a Denial of Service (DOS) attack could render the information system 100 useless, preventing crew and passengers from communicating. If all wireless communications pass through the access point 368, however, all communication packets can pass through Wireless Intrusion Prevention Software (WIPS) that can block and/or deny all de-auth (DOS) attacks and prevent one or more wireless devices, such as a personal media device 200 (shown in Fig. 5B), from accessing the content distribution system 320.

[0027] The security system 500 alternatively, and/or additionally, can provide secure data storage 4. The secure data storage 4 can be provided in any conventional manner and can include sufficient storage resources for securely storing credit card transactions and/or other sensitive data of any kind in an encrypted format. As desired, the data can be securely stored in accordance with a relevant data security standard. Exemplary security standards may include Payment Card Industry Data Security Standard (PCI DSS) for credit card information and/or Health Insurance Portability and Accountability Act (HIPAA) for medical information. As desired, private data likewise can include personal information protected under applicable law. European personal data privacy laws, for example, protect any type of data, such as name, address, and/or frequent flyer number, that can be used to identify a person.

[0028] As shown in Fig. 1, the security system 500 can include an Application Based Firewall 5. Applications used by the information system 100 typically communicate with each other and transfer data to (and/or from) various locations on the communication (or distribution) system 320. This data can be malformed and/or cause unexpected results, such as buffer overflows and/or remote code execution. Malformed data and/or unexpected results can compromise the information system 100. The application firewall 5 can inhibit malformed data from passing between applications and/or causing unexpected results. Moreover, an Application Based Firewall 5 (or Web Application Firewall) may provide a defense at the network security level for web application attacks capable of being launched on TCP/UDP port 80—a port that must remain open (and vulnerable) due to normal and legitimate web site traffic transmitted on the port. Similar to the antivirus software 1, the Application Based Firewall 5 may receive periodic updates in order to combat the latest web vulnerabilities.

[0029] The intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6 of the security system 500 can identify and/or prevent unauthorized access to the information

system 100 by blocking unwanted data types or fragments. As desired, the IPS/IDS 6 can filter traffic based on data signatures or downloadable rules that may be updated on a regular or ad hoc basis. If a breach occurs, the security system 500 can enable the information system 100 to notify authorized personnel, such as ground control, of the breach and can respond accordingly. In an exemplary embodiment, the IDS/IPS 6 may be configured by adopting a third party open source solution, such as SNORT® provided by Sourcefire, Inc., headquartered in Columbia, MD, In a hard wired environment, the IPS/IDS 6 may be most effective in detecting intrusion if it is configured to operate as the initial input 10 to the security system 500—thereby preventing malicious data packets from entering, and possibly disabling, the security system 500. In a wireless input environment, however, a person of ordinary skill could readily determine that the Wireless Intrusion Prevention System 3 may be the initial point of entry to the security system 500. A WIPS 3 may be capable of preventing unauthorized network access to the security system 500 by wireless devices.

[0030] As desired, the security system 500 can include a payment processing system 7. The payment processing system 7 can be provided as a software (or API) application and/or can process credit card transactions and other types of secure transactions. Preferably, the payment processing system 7 resides within the security system 500, yet remains segmented from the rest of the information system 100 due the sensitivity of the data housed in the payment processing system 7 and the anticipated audits over the handling of the data. The APIs provided by the payment processing system 7 may be capable of being called by other applications and LRUs but the PCI-DSS compliant system preferably is entirely self contained, thereby minimizing the scope of PCI-DSS compliance.

[0031] Fig. 1 shows that the security system 500 has a Secure Log File 8. The Secure Log File 8 can be provided in any conventional manner. All security related events from each line replaceable unit (LRU) 326 (shown in Fig, 4) preferably are stored within the Secure Log File Storage System 8. The Secure Log File Storage System 8 essentially can serve as a central log aggregate for the information system 100.

[0032] Turning briefly to Fig. 2C, for example, a plurality of local LRUs 326 are illustrated as communicating with the security log file 8 over a direct and secure connection 16. Exemplary LRUs 326 can include an Aircraft Interface 312, File Server 314, Media Server 31OA, Content Server 316, Disk Array 318, a user interface system 360, and/or a seat electronics box (SEB) (and/or video seat electronics box (VSEB) and/or premium seat electronics box (PSEB)) 324 without limitation. Exemplary LRUs 326 are shown and described in United States Patent No. 7,675,849, entitled "SYSTEM AND METHOD FOR ROUTING COMMUNICATION SIGNALS VIA A DATA DISTRIBUTION NETWORK,"

and in co-pending United States patent application, entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING TRAVEL," Application Serial No. 12/237,253, filed on September 24, 2008, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes. These LRUs 326 may have a need to generate security log files; however, it may not be feasible to store the log files on the respective local LRUs 326 due to their unsecured nature and/or lack of adequate storage,

[0033] In an effort to secure transmission between LRUs 326 and the secure log file storage 8, each LRU 326 configured to interface with the secure log file 8 may be configured to broadcast a unique identifier to the secure log file 8 receiver system. This interaction may adopt certificate-based authentication that is keyed to either or both of each LRUs IP or MAC address, As security log files are generated over Syslog UDP port 514, the security log files may be written to the secure log file storage 8, which may comprise one or more hard drive, compact flash device, solid state device, and/or any other adequate storage mechanism. As desired, the log files may also be encrypted by using Advanced Encryption Standard (AES) 256 or other adequate encryption means. The security system 500 preferably is configured to provide the security log files stored within the secure log file storage 8 to the remote processing system 15 (shown in Fig. 2F) via a secure Universal Serial Bus (USB) connection 12, a secure cellular communication connection 13, and/or a secure broadband communication connection 14 of the security system 500. Thereby, the processing system 15 can receive information related to any denial of service (DoS) attack, data snooping, and other types of data security incidents detected by the security system 500 and can trace the security risk to its origin and/or identify the attack methodology used for preparing a response to the security incidents.

[0034] Returning to Fig, 1, the security system 500 can receive data and other information 10 from the information system 100 and can provide data and other information 11 to the information system 100. The security system 500 can communicate with the information system 100 in any conventional wired and/or wireless manner, including in the manner set forth below with reference to the communication (or distribution) system 320 (shown in Figs. 3A-B and 4). Preferably, the security system 500 and the information system 100 communicate via a wired communication connect, such as a fiber-optic communication connection, to help ensure secure communications between the security system 500 and the information system **100.**

[0035] The security system 500 likewise can provide secure information to a processing system 15 (shown in Fig. 2F) that is remote from the information system 100. For example, the security system 500 can provide sensitive commercial transaction information, such as

credit card payment data, to the remote processing system 15 for subsequent processing and completion of the commercial transaction. The security system 500 can provide the commercial transaction information to the remote processing system 15 in any conventional manner. An exemplary wireless manner of transmitting the commercial transaction information to the remote processing system 15 can include secure cellular communication connection 13 and/or secure broadband communication connection 14; whereas, a secure Universal Serial Bus (USB) connection is an illustrative manner for transmitting the commercial transaction information to the remote processing system 15 in a wired manner. If installed on an aircraft 390B (shown in Fig. 3B), for example, the information system 100 can comprise a conventional aircraft passenger in-flight entertainment system, such as the Series 2000, 3000, eFX, and/or eX2 in-flight entertainment system as manufactured by Panasonic Avionics Corporation (formerly known as Matsushita Avionics Systems Corporation) of Lake Forest, California, and can include Panasonic Avionics' eXconnect system that supports broadband communications with a terrestrial Earth station.

[0036] The remote processing system 15 can be provided in any suitable manner based, for example, upon the type of data being transmitted. Exemplary remote processing systems 15 are shown and described in co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR MANAGING CONTENT ON MOBILE PLATFORMS," Application Serial No. 11/123,327, filed on May 6, 2005; entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING TRAVEL," Application Serial No. 12/237,253, filed on September 24, 2008, and entitled "SYSTEM AND METHOD FOR PERFORMING REAL TIME DATA ANALYSIS," Application Serial No. 12/638,655, filed on December 15, 2009, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes.

[0037] Fig. I shows that the security system 500 can include a cell transport system 9 for supporting the cellular communication connection 13. Data and signature files thereby can be uploaded to (and/or downloaded from) the security system 500 via the cellular communication connection 13. Although illustrated in Fig. 1 as including the antivirus software 1, the Hardware Security Module (HSM) 2, the wireless fidelity (Wi-Fi) device 3, the secure data storage 4, the Application Based Firewall 5, the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6, the payment processing system 7, the Secure Log File 8, and the cell transport system 9, the security system 500 can include any combination of one or more of the above system components without limitation.

[0038] One manner by which data can propagate through the security system 500 is illustrated in Fig. 2A. Turning to Fig. 2A, the security system 500 is shown as including at least the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6, the antivirus software I, and the Application Based Firewall 5. The intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6 can receive inbound data traffic in any conventional wired and/or wireless manner via the initial input 10 to the security system 500. Receiving the inbound data traffic, the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6 can filter the inbound data traffic based upon data signature information. Thereby, the security system 500 can block any unwanted datatypes and/or data fragments from being transmitted to the information system 100.

J0039] The intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6 is shown as providing the filtered inbound data traffic to the antivirus software 1. The antivirus software 1 can inspect the filtered inbound data traffic against one or more virus signature (and/or malware) files. As desired, the antivirus software 1 likewise can determine a data type for the filtered inbound data traffic. If the filtered inbound data traffic is determined to include a virus (and/or malware) and/or a prohibited data type, the antivirus software 1 blocks the filtered inbound data traffic; otherwise, the antivirus software 1 permits the filtered inbound data traffic o be transmitted to the Application Based Firewall 5. Receiving the filtered inbound data traffic from the antivirus software 1, the Application Based Firewall 5 inspects the filtered inbound data traffic for web applications. In other words, the Application Based Firewall 5 validates the filtered inbound data traffic for web applications, such as Structured Query Language (SQL) injection and/or Cross-site scripting (XSS).

[0040] The filtered inbound data traffic that is validated by the Application Based Firewall 5 can be provided to the information system 100 via the output 11 of the security system 500. Alternatively, and/or additionally, the validated inbound data traffic can be provided to the remote processing system 15 (shown in Fig. 2F) via the secure Universal Serial Bus (USB) connection 12, the secure cellular communication connection 13, and/or the secure broadband communication connection 14 of the security system 500 in the manner set forth in more detail above with reference to Fig. 1. Although shown and described as comprising an exemplary arrangement of the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6, the antivirus software 1, and the Application Based Firewall 5 with reference to Fig. 2A for purposes of illustration only, the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6, the antivirus software 1, and the Application Based Firewall 5 can be provided in any suitable arrangement. The security system 500 likewise can include a greater and/or lesser number of security component modules.

[0041] If the information system 100 includes a wireless distribution system 320 (Figs. 3A, 3B), for example, the security system 500 shown in Fig. 2A can further include a wireless fidelity (Wi-Fi) device 3 as illustrated in Fig. 2B. The wireless fidelity (Wi-Fi) device 3 can be provided in the manner set forth in more detail above with reference to Fig. 1 and is shown as being disposed between the initial input 10 to the security system 500 and the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6. The wireless fidelity device 3 thereby can receive and inspect inbound wireless data traffic for denial of service (DoS) attacks, data snooping, and other types of wireless data security risks. Advantageously, the wireless fidelity device 3 can block any unwanted inbound wireless data traffic and can provide the wanted inbound wireless data traffic to the intrusion prevention system (IPS) and/or intrusion detection system (IDS) 6, the antivirus software 1, and the Application Based Firewall 5 for further inspection, such as filtering and/or validation, in the manner discussed in more detail above with reference to Fig. 2A. The processed inbound data traffic thereby can be provided to the information system 100 via the output 11 of the security system 500 and/or to the remote processing system 15 (shown in Fig. 2F) via the secure Universal Serial Bus (USB) connection 12, the secure cellular communication connection 13, and/or the secure broadband communication connection 14 of the security system 500 in the manner described above.

[0042] Turning to Fig. 2D, the security system 500 is illustrated as including the Hardware Security Module (HSM) 2. The Hardware Security Module 2 is provided in the manner discussed in more detail above with reference to Fig. 1. The information system 100 is shown, at A, as receiving payment application information, media content, public key infrastructure (PKl) authentication data, and/or any other relevant type of inbound data traffic. If the inbound data traffic includes a request for encryption/decryption key information, the information system 100, at B, can provide the request to the Hardware Security Module 2 via the initial input 10 to the security system 500. At C, the Hardware Security Module 2 can responds to the request by providing the requested encryption/decryption key information to the information system 100 via the output 11 of the security system 500. The information system 100 thereby can provide, at D, the requested encryption/decryption key information to a third-party application that requires the encryption/decryption key information for encrypting and/or decrypting the inbound data traffic.

[0043] Fig. 2E illustrates an exemplary embodiment of the secure data storage 4 for securely storing credit card transactions, personal identifiable information (PII), and/or other types of sensitive data in the manner discussed in more detail above with reference to Fig. 1. The secure data storage 4 can receive the sensitive data from the information system 100 via the initial input 10 of the security system 500 and/or from the remote processing system 15

(shown in Fig. 2F) via the secure Universal Serial Bus (USB) connection 12, the secure cellular communication connection 13, and/or the secure broadband communication connection 14 of the security system 500. Upon receiving the sensitive data, the secure data storage 4 can securely store the sensitive data, preferably in an encrypted format, and can provide the stored sensitive data upon receiving proper authorization. The secure data storage 4 thereby can provide the stored sensitive data to the information system 100 via the output 11 of the security system 500 and/or to the remote processing system 15 (shown in Fig. 2F) via the secure Universal Serial Bus (USB) connection 12, the secure cellular communication connection 13, and/or the secure broadband communication connection 14 of the security system 500 in the manner set forth in more detail above.

[0044] Turning to Fig. 2F, the security system 500 is illustrated as including the payment processing system 7. The payment processing system 7 preferably is provided in the manner discussed in more detail above with reference to Fig. 1 and provides secure payment application code storage. As illustrated in Fig. 2F, the payment processing system 7 exchange payment application data with the information 100 via the initial input 10 and the output 11 of the security system 500. The payment processing system 7 likewise can exchange payment application data with the remote processing system 15 via the secure Universal Serial Bus (USB) connection 12, the secure cellular communication connection 13, and/or the secure broadband communication connection H of the security system 500 in the manner set forth in more detail above. Thereby, payment software applications, such as application programming interfaces (APIs) and other payment application code, used in the payment application process can be securely stored within the security system 500, wherein other applications and/or LRUs 326 can access the software applications stored within the payment processing system 7.

[0045] Storage of the software applications within the payment processing system 7 advantageously segments the payment software applications and/or the payment application data from the remainder of the information system 100. With reference to the Payment Card Industry (PCI) standard, for example, processing of payment application data can be subject to audit. By maintaining the payment software applications and/or the payment application data within the payment processing system 7, performance of audits can be facilitated because the payment information is segmented. Thereby, only the security system 500, rather than the entire information system 100, requires examination during an audit, minimizing the scope of the information system 100 that is subject to compliance under the PCI standard.

[0046] Although the information system 100 can be disposed in a fixed location, such as a building, the information system i00 likewise can advantageously be applied in mobile system applications. Turning to Figs. 3A-B, the information system 100 is shown as comprising a

vehicle information system 300 that can be configured for installation aboard a wide variety of vehicles 390. Exemplary types of vehicles can include an automobile 390A (shown in Fig. 3A), an aircraft 390B (shown in Fig. 3B), a bus, a recreational vehicle, a boat, and/or a locomotive, or any other type of passenger vehicle without limitation. If installed on an aircraft 390B as illustrated in Fig. 3B, for example, the vehicle information system 300 can comprise a conventional aircraft passenger in-flight entertainment system, such as the Series 2000, 3000, eFX, and/or eX2 in-flight entertainment system as manufactured by Panasonic Avionics Corporation (formerly known as Matsushita Avionics Systems Corporation) of Lake Forest, California.

[0047] As shown in Figs. 3A-B, the vehicle information system 300 comprises at least one conventional content source 310 and one or more user (or passenger) interface systems 360 that communicate via a real-time content distribution system 320. Each content source 310 can be provided in the manner set forth in United States Patent No. 7,715,783, entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING INTERNATIONAL TRAVEL," and in the co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR DOWNLOADING FILES," Application Serial No. 10/772,565, filed on February 4, 2004; entitled "SYSTEM AND METHOD FORMANAGING CONTENT ON MOBILE PLATFORMS," Application Serial No. 11/123,327, filed on May 6, 2005; entitled "PORTABLE MEDIA DEVICE AND METHOD FOR PRESENTING VIEWING CONTENT DURING TRAVEL," Application Serial No. 11/154,749, filed on June 15, 2005; entitled "SYSTEM AND METHOD FOR INTERFACING A PORTABLE MEDIA DEVICE WITH A VEHICLE INFORMATION SYSTEM," Application Serial No. 12/210,624, filed on September 15, 2008; entitled "PORTABLE USER CONTROL DEVICE AND METHOD FOR VEHICLE INFORMATION SYSTEMS," Application Serial No. 12/210,689, filed on September 15, 2008; entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING TRAVEL," Application Serial No. 12/237,253, filed on September 24, 2008; and entitled "SYSTEM AND METHOD FOR PRESENTING ADVERTISEMENT CONTENT ON A MOBILE PLATFORM DURING TRAVEL," Application Serial No. 12/245,521, filed on October 3, 2008, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes.

[0048] The content sources 310 can include one or more internal content sources, such as server system 310A, that are installed aboard the vehicle 390 and/or remote (or terrestrial) content sources 310B that can be external from the vehicle 390. The server system 310A can

be provided as an information system controller for providing overall system control functions for the vehicle information system 300 and/or at least one media (or file) server system 310A, for storing viewing content 2 10, such as preprogrammed viewing content and/or downloaded viewing content 210D, as desired. The server system 310A can include, and/or communicate with, one or more conventional peripheral media storage systems (not shown), including optical media devices, such as a digital video disk (DVD) system or a compact disk (CD) system, and/or magnetic media systems, such as a video cassette recorder (VCR) system or a hard disk drive (HDD) system, of any suitable kind, for storing the preprogrammed content and/or the downloaded viewing content 210D.

[0049] The viewing content 2 10 can comprise any conventional type of audio and/or video viewing content, such as stored (or time-delayed) viewing content and/or live (or real-time) viewing content, in the manner set forth in the above-referenced United States Patent No. 7,715,783, entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING INTERNATIONAL TRAVEL," and in the above-referenced co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR DOWNLOADING FILES," Application Serial No. 10/772,565, filed on February 4, 2004; and entitled "PORTABLE MEDIA DEVICE AND METHOD FOR PRESENTING VIEWING CONTENT DURING TRAVEL," Application Serial No. 11/154,749, filed on June 15, 2005. Exemplary viewing corrtentUO can include television programming content, music content, podcast content, photograph album content, audiobook content, and/or movie content without limitation.

[0050] As desired, the viewing content 210 can include geographical information in the manner set forth in United States Patent No. 6,661,353, entitled "METHOD FOR DISPLAYING INTERACTIVE FLIGHT MAP INFORMATION," which is assigned to the assignee of the present application and the disclosure of which is hereby incorporated herein by reference in its entirety and for all purposes. Alternatively, and/or additionally, to entertainment content, such as live satellite television programming and/or live satellite radio programming, the viewing content likewise can include two-way communications, such as real-time access to the Internet 310C (shown in Fig. 3B) and/or telecommunications in the manner set forth in United States Patent No. 5,568,484, entitled "TELECOMMUNICATIONS SYSTEM AND METHOD FOR USE ON COMMERCIAL AIRCRAFT AND OTHER VEHICLES," which is assigned to the assignee of the present application and the disclosure of which is hereby incorporated herein by reference in its entirety and for all purposes. The exemplary viewing content as shown and described herein are not exhaustive and are provided herein for purposes of illustration only and not for purposes of limitation.

[0051] Being configured to distribute and/or present the viewing content 210 provided by one or more selected content sources 310, such as a content system 400, the vehicle information system 300 can communicate with the content sources 310 in real time and in any conventional manner, including via wired and/or wireless communications. The vehicle information system 300 and the terrestrial content source 310B, for example, can communicate in any conventional wireless manner, including directly and/or indirectly via an intermediate communication system 370, such as a satellite communication system 370A. The vehicle information system 300 thereby can receive download viewing content 210D from a selected terrestrial content source 310B and/or transmit upload viewing content 210U, including navigation and other control instructions, to the terrestrial content source 310B. As desired, the terrestrial content source 310B can be configured to communicate with other terrestrial content sources (not shown). The terrestrial content source 310B is shown in Fig. 3B as providing access to the Internet 310C. Although shown and described as comprising the satellite communication system 370A for purposes of illustration, the communication system 370 can comprise any conventional type of wireless communication system, such as a cellular communication system (not shown) and/or an Aircraft Ground Information System (AGIS) communication system (not shown).

[0052] To facilitate communications with the terrestrial content sources 310B, the vehicle information system 300 can include an antenna system 330 and a transceiver system 340 for receiving the viewing content from the remote (or terrestrial) content sources 310B as shown in Figs. 3A-B. The antenna system 330 preferably is disposed outside the vehicle 390, such as an exterior surface 394 of a fuselage 392 of the aircraft 390B. The antenna system 330 can receive viewing content 210 from the terrestrial content source 310B and provide the received viewing content 210, as processed by the transceiver system 340, to a computer system 350 of the vehicle information system 300. The computer system 350 can provide the received viewing content 210 to the media (or content) server system 310A and/or to one or more of the user interfaces 360, as desired. Although shown and described as being separate systems for purposes of illustration, the computer system 350 and the media server system 310A can be at least partially integrated.

[0053] The vehicle information system elements, including the content sources 310 and the user interface systems 360, are shown in Figs. 3A-B as communicating via the content distribution system 320. Fig. 4 illustrates an exemplary content distribution system 320 for the vehicle information system 300. The content distribution system 320 of Fig. 4 couples, and supports communication between a headend system 310H, which includes the content sources 310, and the plurality of user interface systems 360. The distribution system 320 as

shown in Fig. 4 is provided in the manner set forth in United States Patent No. 7,675,849, entitled "SYSTEM AND METHOD FOR ROUTING COMMUNICATION SIGNALS VIA A DATA DISTRIBUTION NETWORK," and in United States Patent Nos. 5,596,647, 5,617,331, and 5,953,429, each entitled "INTEGRATED VTDEO AND AUDIO SIGNAL DISTRIBUTION SYSTEM AND METHOD FOR USE ON COMMERCIAL AIRCRAFT AND OTHER VEHICLES," which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes. Alternatively, and/or additionally, the distribution system 320 can be provided in the manner set forth in the co-pending United States patent application "OPTICAL COMMUNICATION SYSTEM AND METHOD FOR DISTRIBUTING CONTENT ABOARD A MOBILE PLATFORM DURING TRAVEL," Serial No. 12/367,406, filed February 6, 2009, which is assigned to the assignee of the present application and the disclosure of which is hereby incorporated herein by reference in its entirety and for all purposes.

[0054] The content distribution system 320, for example, can be provided as a conventional wired and/or wireless communication network, including a telephone network, a local area network (LAN), a wide area network (WAN), a campus area network (CAN), personal area network (PAN) and/or a wireless local area network (WLAN), of any kind. Exemplary wireless local area networks include wireless fidelity (Wi-Fi) networks in accordance with Institute of Electrical and Electronics Engineers (IEEE) Standard 802.11 and/or wireless metropolitan-area networks (MANs), which also are known as WiMax Wireless Broadband, in accordance with IEEE Standard 802.16. Preferably being configured to support high data transfer rates, the content distribution system 320 may comprise a high-speed Ethernet network, such as any type of Fast Ethernet (such as I00Base-X and/or 100Base-T) communication network and/or Gigabit (such as 1000Base-X and/or 1000Base-T) Ethernet communication network, with a typical data transfer rate of at least approximately one hundred megabits per second (100 Mbps). To achieve high data transfer rates in a wireless communications environment, free-space optics (or laser) technology, millimeter wave (or microwave) technology, and/or Ultra-Wideband (UWB) technology can be utilized to support communications among the various system resources, as desired.

[0055] As desired, the distribution system 320 likewise can include a network management system (not shown) provided in the manner set forth in co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR IMPROVING NETWORK RELIABILITY," Application Serial No. 10/773,523, filed on February 6, 2004, and entitled "SYSTEM AND METHOD FOR IMPROVING NETWORK RELIABILITY," Application

Serial No. 11/086,510, filed on March 21, 2005, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes.

[0056] As illustrated in Fig. 4, the distribution system 320 can be provided as a plurality of area distribution boxes (ADBs) 322, a plurality of floor disconnect boxes (FDBs) 323, and a plurality of seat electronics boxes (SEBs) (and/or video seat electronics boxes (VSEBs) and/or premium seat electronics boxes (PSEBs)) 324 being configured to communicate in real time via a plurality of wired and/or wireless communication connections 325. The distribution system 320 likewise can include a switching system 321 for providing an interface between the distribution system 320 and the headend system 310H. The switching system 321 can comprise a conventional switching system, such as an Ethernet switching system, and is configured to couple the headend system 310H with the area distribution boxes 322. Each of the area distribution boxes 322 is coupled with, and communicates with, the switching system 321.

[0057] Each of the area distribution boxes 322, in turn, is coupled with, and communicates with, at least one floor disconnect box 323. Although the area distribution boxes 322 and the associated floor disconnect boxes 323 can be coupled in any conventional configuration, the associated floor disconnect boxes 323 preferably are disposed in a star network topology about a central area distribution box 322 as illustrated in Fig. 4. Each floor disconnect box 323 is coupled with, and services, a plurality of daisy-chains of seat electronics boxes 324. The seat electronics boxes 324, in turn, are configured to communicate with the user interface systems 360. Each seat electronics box 324 can support one or more of the user interface systems 360.

[0058] The switching systems 321, the area distribution boxes (ADBs) 322, the floor disconnect boxes (FDBs) 323, the seat electronics boxes (SEBs) (and/or video seat electronics boxes (VSEBs) and/or premium seat electronics boxes (PSEBs)) 324, the antenna system 330, the transceiver system 340, the content source 310, the server system 310A, the headend system 310H, video interface systems 362 (shown in Figs. 5A-B), audio interface systems 364 (shown in Figs. 5A-B), user input systems 366 (shown in Figs. 5A-B), and other system resources of the vehicle information system 300 preferably are provided as line replaceable units (LRUs) 326. The use of LRUs 326 facilitate maintenance of the vehicle information system 300 because a defective LRU 326 can simply be removed from the vehicle information system 300 and replaced with a new (or different) LRU 326. The defective LRU 326 thereafter can be repaired for subsequent installation. Advantageously, the use of LRUs 326 can promote flexibility in configuring the content distribution system 320 by permitting ready modification

of the number, arrangement, and/or configuration of the system resources of the content distribution system 320. The content distribution system 320 likewise can be readily upgraded by replacing any obsolete LRUs 326 with new LRUs 326.

[0059] As desired, the floor disconnect boxes 323 advantageously can be provided as routing systems and/or interconnected in the manner set forth in the above-referenced United States Patent No. 7,675,849, entitled "SYSTEM AND METHOD FOR ROUTING COMMUNICATION SIGNALS VIA A DATA DISTRIBUTION NETWORK." The distribution system 320 can include at least one FDB internal port bypass connection 325A and/or at least one SEB loopback connection 325B. Each FDB internal port bypass connection 325A is a communication connection 325 that permits floor disconnect boxes 323 associated with different area distribution boxes 322 to directly communicate. Each SEB loopback connection 325B is a communication connection 325 that directly couples the last seat electronics box 324 in each daisy-chain of seat electronics boxes 324 for a selected floor disconnect box 323 as shown in Fig. 4. Each SEB loopback connection 325B therefore forms a loopback path among the daisy-chained seat electronics boxes 324 coupled with the relevant floor disconnect box 323.

[0060] Returning to Figs. 3A-B, the user interface systems 360 are provided for selecting viewing content 210 and for presenting the selected viewing content 210. As desired, the user interface systems 360 can comprise conventional passenger interfaces and can be provided in the manner set forth in the above-referenced co-pending United States patent application, entitled "PORTABLE MEDIA DEVICE AND METHOD FOR PRESENTING VIEWING CONTENT DURING TRAVEL," Application Serial No. 11/154,749, filed on June 15, 2005, as well as in the manner set forth in the co-pending United States patent application, entitled "SYSTEM AND METHOD FOR PRESENTING HIGH-QUALITY VIDEOTO PASSENGERS ON A MOBILE PLATFORM," Application Serial No. 60/673,171, filed on April 19, 2005, the disclosure of which is hereby incorporated herein by reference in its entirety and for all purposes.

[0061] Fig. 5A provides a view of a passenger cabin 380 of a passenger vehicle 390, such as the automobile 390A (shown in Fig. 3A) and/or the aircraft 390B (shown in Fig. 3B), aboard which the vehicle information system 300 has been installed. The passenger cabin 380 is illustrated as including a plurality of passenger seats 382, and each passenger seat 382 is associated with a selected user interface system 360, Each user interface system 360 can include a video interface system 362 and/or an audio interface system 364. Exemplary video interface systems 362 can include overhead cabin display systems 362A with central controls, seatback display systems 362B or armrest display systems (not shown) each with

individualized controls, crew display panels, and/or handheld presentation systems. The audio interface systems 364 can be provided in any conventional manner, including an overhead speaker system 364A, the handheld presentation systems, and/or headphones coupled with an audio jack provided, for example, at an armrest 388 of the passenger seat 382. A speaker system likewise can be associated with the passenger seat 382, such as a speaker system 364B disposed within a base 384B of the passenger seat 382 and/or a speaker system 364C disposed within a headrest 384C of the passenger seat 382. In a preferred embodiment, the audio interface system 364 can include an optional noise-cancellation system for further improving sound quality produced by the audio interface system 364.

[0062] The video interface systems 362 and the audio interface systems 364 can be installed at any suitable cabin surface, such as a seatback 386, wall 396, ceiling, and/or bulkhead, or an armrest 388 of a passenger seat 382 in any conventional manner including via a mounting system 363 provided in the manner set forth co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR MOUNTING USER INTERFACE DEVICES," Application Serial No. 11/828, 193, filed on July 25, 2007, and entitled "USER INTERFACE DEVICE AND METHOD FOR PRESENTING VIEWING CONTENT," Application Serial No. 11/835,371, filed on August 7, 2007, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes.

[0063] As shown in Fig. 5A, the user interface system 360 likewise can include an input system 366 for permitting the user (or passenger) to communicate with the vehicle information system 300, such as via an exchange of control signals 220. For example, the input system 366 can permit the user to enter one or more user instructions 230 for controlling the operation of the vehicle information system 300. Illustrative user instructions 230 can include instructions for initiating communication with the content source 310, instructions for selecting viewing content 210 for presentation, and/or instructions for controlling the presentation of the selected viewing content 210. If a fee is required for accessing the viewing content 210, payment information likewise can be entered via the input system 366.

[0064] The input system 366 can be provided in any conventional manner and typically includes one or more switches (or pushbuttons), such as a keyboard or a keypad, and/or a pointing device, such as a mouse, trackball, or stylus. As desired, the input system 366 can be at least partially integrated with, and/or separable from, the associated video interface system 362 and/or audio interface system 364. For example, the video interface system 362 and the input system 366 can be provided as a touchscreen display system. The input system 366 likewise can include one or more input ports (not shown) for coupling a peripheral input device

(not shown), such as a full-size computer keyboard, an external mouse, and/or a game pad, with the vehicle information system 300.

[0065] Preferably, at least one of the user interface systems 360 includes a wired and/or wireless access point 368, such as a conventional communication port (or connector), for coupling a personal media device 200 (shown in Fig. 5B) with the vehicle information system 300. Passengers (not shown) who are traveling aboard the vehicle 390 thereby can enjoy personally-selected viewing content during travel. The access point 368 is located proximally to an associated passenger seal 382 and can be provided at any suitable cabin surface, such as a seatback 386, wall 396, ceiling, and/or bulkhead.

[0066] Turning to Fig. 5B, the vehicle information system 300 is shown as communicating with one or more personal media devices 200. Each personal media device 200 can store the audio and/or video viewing content 210 and can be provided as a handheld device, such as a laptop computer, a palmtop computer, a personal digital assistant (PDA), cellular telephone, an iPod® digital electronic media device, an iPhone® digital electronic media device, and/or a MPEG Audio Layer 3 (MP3) device. Illustrative personal media devices 200 are shown and described in the above-referenced United States Patent No. 7,715,783, entitled "SYSTEM AND METHOD FOR RECEIVING BROADCAST CONTENT ON A MOBILE PLATFORM DURING INTERNATIONAL TRAVEL," and in the above-referenced co-pending United States patent applications, entitled "SYSTEM AND METHOD FOR DOWNLOADING FILES," Application Serial No. 10/772,565, filed on February 4, 2004; entitled "PORTABLE MEDIA DEVICE AND METHOD FOR PRESENTING VIEWING CONTENT DURING TRAVEL," Application Serial No. 11/154,749, filed on June 15, 2005; entitled "SYSTEM AND METHOD FOR INTERFACING A PORTABLE MEDIA DEVICE WITH A VEHICLE INFORMATION SYSTEM," Application Serial No. 12/210,624, filed on September 15, 2008; entitled "MEDIA DEVICE INTERFACE SYSTEM AND METHOD FOR VEHICLE INFORMATION SYSTEMS," Application Serial No. 12/210,636, filed on September 15, 2008; entitled "MEDIA DEVICE INTERFACE SYSTEM AND METHOD FOR VEHICLE INFORMATION SYSTEMS," Application Serial No. 12/210,652, filed on September 15, 2008; and entitled "PORTABLE USER CONTROL DEVICE AND METHOD FOR VEHICLE INFORMATION SYSTEMS," Application Serial No. 12/210,689, filed on September 15, 2008, which are assigned to the assignee of the present application and the respective disclosures of which are hereby incorporated herein by reference in their entireties and for all purposes.

[0067] The illustrated personal media devices 200 each include a video display system 240 for visually presenting the viewing content 210 and an audio system 250 for audibly presenting

the viewing content 210. Each personal media device 200 can include a user control system 260, which can be provided in any conventional manner and typically includes one or more switches (or pushbuttons), such as a keyboard or a keypad, and/or a pointing device, such as a mouse, trackball, or stylus. The personal media devices 200 thereby can select desired viewing content 210 and control the manner in which the selected viewing content 210 is received and/or presented.

[0068] The personal media devices 200 likewise include a communication port (or connector) 270. The communication port 270 enables the personal media devices 200 to communicate with the vehicle information system 300 via the access points 368 of the user interface systems 360. As illustrated with personal media device 200A, the communication port 270 and the access points 368 can supported wireless communications; whereas, support for wired communications between the communication port 270 and the access points 368 via a communication cable assembly 369 is shown with personal media device 200B. When the communication port 270 and the access points 368 are in communication, the vehicle information system 300 supports a simple manner for permitting the associated personal media device 200 to be integrated with the vehicle information system 300 using a user-friendly communication interface.

[0069] When the personal media device 200 and the vehicle information system 300 are in communication, the vehicle information system 300 can perform a plurality of integration tasks simultaneously, enabling the personal media device 200 to become fully integrated with the vehicle information system 300 via a selected access point 368, The system elements of the vehicle information system 300 and the personal media device 200 thereby become interchangeable. The personal media device 200 likewise can receive control signals (or commands) 220 and/or operating power 220P from the vehicle information system 300. Thereby, the personal media device 200 advantageously can become a seamless part of the vehicle information system 300.

[0070] For example, user instructions 230 (shown in Figs. 3A-B) for controlling the operation of the vehicle information system 300 can be provided via the input system 366 of the vehicle information system 300 and/or the user control system 260 of the personal media device 200. In other words, the input system 366 of the vehicle information system 300 and/or the user control system 260 of the personal media device 200 can be used to select viewing content 210 and control the manner in which the selected viewing content 210 is received and/or presented, The selected viewing content 210 can be provided by a relevant content source 310 (shown in Figs. 3A-B) of the vehicle information system 300 and/or by storage media (not shown) disposed within the personal media device 200. A video portion of the

selected viewing content 210 thereby can be presented via the video presentation system 362 of the vehicle information system 300 and/or the video display system 240 of the personal media device 200. The audio presentation system 364 of the vehicle information system 300 and/or the audio system 250 of the personal media device 200 can be used to present an audio portion of the selected viewing content 210. If the video display system 240 of the personal media device 200 is much smaller than the video presentation system 362 of the vehicle information system 300, a passenger may prefer to view the selected viewing content 210 via the larger video presentation system 362.

[0071] When no longer in use and/or direct physical contact with the personal media device 200 is not otherwise required, the personal media device 200 can be stored at the passenger seat 382. For example, the passenger seat 382 can include a storage compartment 389 for providing storage of the personal media device 200. The storage compartment 389 can be provided in any conventional manner and at any suitable portion of the passenger seat 382. As illustrated with passenger scat 382B, the personal media device 200 can be placed in a storage pocket 389B formed in the armrest 388 of the passenger seat 382B. The storage compartment 389 likewise can be provided on the seatback 386 and/or the headrest 384 of the passenger seat 382. Storage compartment 389A of passenger seat 382A, for example, is shown as being formed on the lower seatback 386 of the passenger seat 382A. As desired, the storage compartment 389 can comprise an overhead storage compartment, a door storage compartment, a storage compartment provided underneath the passenger seat 382, or any other type of conventional storage compartment, such as a glove compartment, trunk, or closet, available in the passenger vehicle 390.

[0072] Alternatively, and/or additionally, it may be desired to further enhance the security of the vehicle information system 300 via at least one biometric device 600 as illustrated in Fig. 6. The biometric device 600 can comprise any conventional type of biometric device, such as a face scanner, a hand scanner, a fingerprint scanner, a retina scanner, and/or an iris scanner, can be employed to help prevent unauthorized access to the vehicle information system 300. Advantageously, the biometric device 600 uses human biological characteristics to identify a user rather than relying on username/password-type authentication, which is prone to being forgotten or compromised in any environment. The biometric device 600 can be disposed at any suitable location within a passenger cabin 380 (shown in Figs. 5A-B) of a passenger vehicle 390 (shown in Figs. 5A-B) such as a selected video interface system 362 of the vehicle information system 300 as shown in Fig. 6. Preferably, the selected video interface system 362 comprises a crew panel system 362C that is accessible only by authorized personnel, such as crew members and/or maintenance workers. The biometric device 600

thereby can permit the crew members and other authorized personnel a method of authenticating their respective identities with the vehicle information system—minimizing the risk of unauthorized access that has the potential to undermine all other security objectives.

[0073] The described embodiments are susceptible to various modifications and alternative forms, and specific examples thereof have been shown by way of example in the drawings and are herein described in detail. The described embodiments, however, are not to be limited to the particular forms or methods disclosed, but to the contrary, the present disclosure is to cover all modifications, equivalents, and alternatives.

CLAIMS

What is claimed is:

1. A security appliance suitable for use with vehicle information systems, comprising:

a communication connection for communicating with a vehicle information system; and

a security system for providing at least one security function for the information system,

wherein said security system is associated with a single system element within a distribution system of the vehicle information system.

2. The security appliance of claim 1, wherein said communication connection comprises a wired communication connection.

3. The security appliance of claim 2, wherein said communication connection comprises a fiber optic communication connection.

4. The security appliance of claim 1, further comprising an external communication connection for providing secure information to a processing system that is remote from the information system.

5. The security appliance of claim 4, wherein said external communication connection includes a secure wireless communication connection.

6. The security appliance of claim 5, wherein said external communication connection is selected from a group of wireless communication connections consisting of a broadband communication connection and a cellular communication connection.

7. The security appliance of claim 4, wherein said external communication connection includes a secure wired communication connection.

8. The security appliance of claim 7, wherein said external communication connection includes a Universal Serial Bus communication connection.

9. The security appliance of claim 1, wherein said at least one security function is selected from a group consisting of providing secure storage of keys used to encrypt system data, providing secure storage of keys used to decrypt system data, providing storage of security-related application programming interfaces, providing storage of a security log file, providing secure storage for private data, utilizing antivirus software, utilizing anti-spyware software, providing an application firewall, providing a network firewall, providing an intrusion prevention system, and providing an intrusion detection system.

10. The security appliance of claim 9, wherein the private data is selected from a group consisting of credit card data, medical data, and data that is protected under law.

11. The security appliance of claim 9, wherein the distribution system of the vehicle information system includes a wireless distribution system and wherein said intrusion prevention system and said intrusion detection system is suitable for use with the wireless distribution system.

12. The security appliance of claim 1, wherein the vehicle information system comprises a passenger entertainment system.

13. The security appliance of claim 1, wherein the vehicle information system is installed aboard a passenger vehicle.

14. The security appliance of claim 13, wherein said security system is disposed within a line replaceable unit within the distribution system of the vehicle information system.

15. The security appliance of claim 13, wherein the passenger vehicle is installed aboard an aircraft.

16. A method for providing network security for a vehicle information system, comprising:

providing a communication connection for communicating with the vehicle information system; and

providing at least one security function for the information system via a security system that is associated with a single system element within a distribution system of the vehicle information system.

17. The method of claim 16, wherein said providing said communication connection comprises providing a wired communication connection.

18. The method of claim 17, wherein said providing said communication connection comprises providing a fiber optic communication connection.

19. The method of claim 16, further comprising providing an external communication connection for providing secure information to a processing system that is remote from the information system.

20. The method of claim 19, wherein said providing said external communication connection includes providing a secure wireless communication connection.

21. The method of claim 16, wherein said providing said at least one security function includes providing a selected security function selected from a group consisting of providing secure storage of keys used to encrypt system data, providing secure storage of keys used to decrypt system data, providing storage of security-related application programming interfaces, providing storage of a security log file, providing secure storage for private data, utilizing antivirus software, utilizing anti-spyware software, providing an application firewall, providing a network firewall, providing an intrusion prevention system, and providing an intrusion detection system.

22. The method of claim 21, wherein said providing said intrusion prevention system comprises providing a wireless intrusion prevention system suitable for use with a wireless distribution system of the vehicle information system.

23. The method of claim 21, wherein said providing said intrusion detection system comprises providing a wireless intrusion detection system suitable for use with a wireless distribution system of the vehicle information system.

24. The method of claim 16, further comprising installing the vehicle information and said security system aboard a passenger vehicle.

25. The method of claim 24, wherein said installing the vehicle information and said security system comprises installing the vehicle information and said security system aboard an aircraft.

26. A distribution for a vehicle information system, comprising:

a plurality of line replaceable units; and

a security system for providing at least one security function for the information system, wherein said security system is associated with a selected line replaceable unit.

27. A vehicle information system suitable for installation aboard a passenger vehicle, comprising:

a content source; and

a distribution system for communicating with said content source and including:

a plurality of line replaceable units; and

a security system for providing at least one security function for the information system,

wherein said security system is associated with a selected line replaceable unit.

28. An aircraft, comprising:

a fuselage and a plurality of passenger seats arranged within the fuselage; and

a vehicle information system, said vehicle information system coupled with said fuselage and comprising:

a headend system that provides overall system control functions for the vehicle information system and that includes a content source;

a user interface system that includes a user input system for selecting viewing content available from said content source and a content presentation system; and

a content distribution system that distributes the selected viewing content throughout the vehicle information system,

wherein content distribution system includes a security system characterized by claim 1.

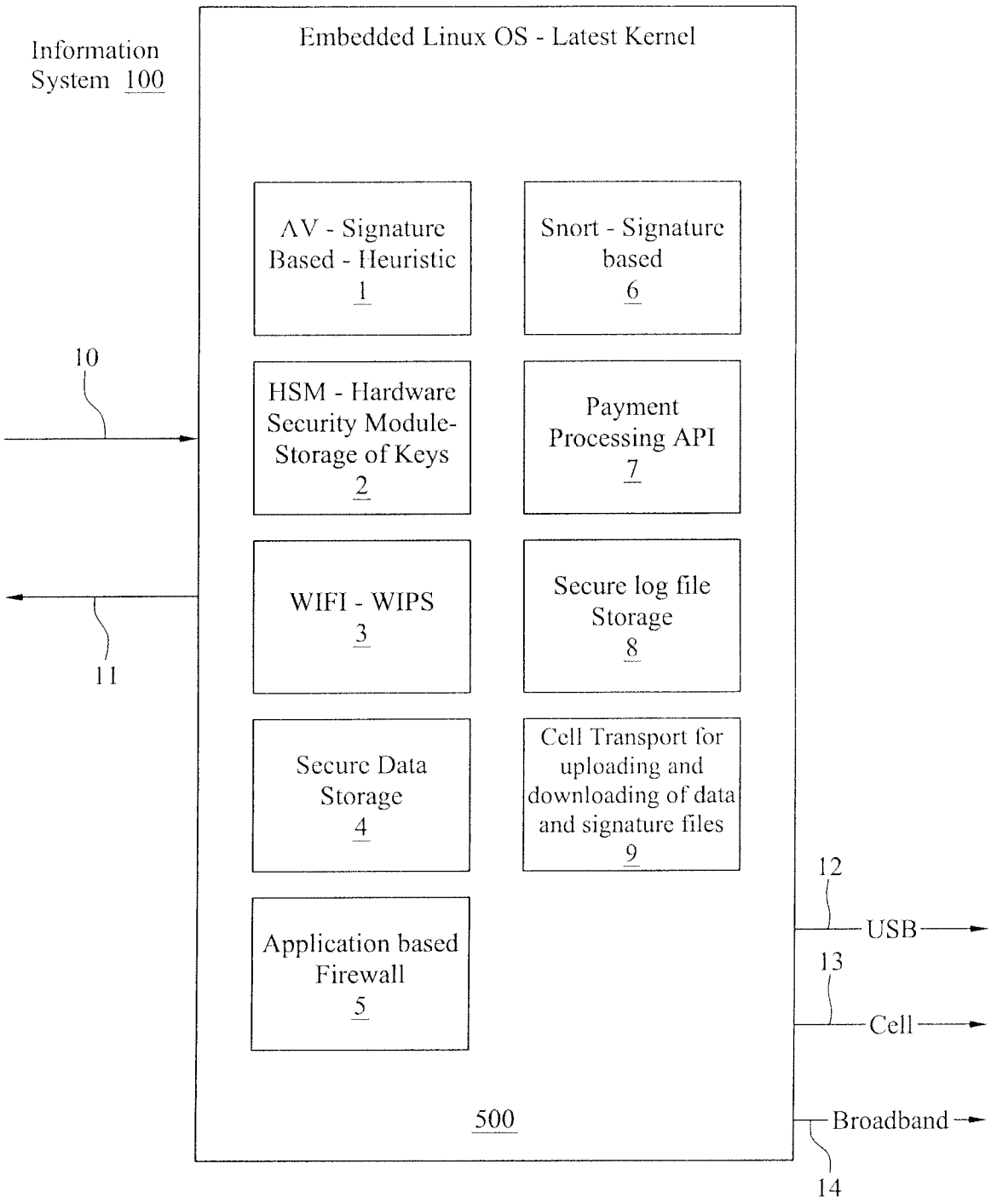

Information System 100
Embedded Linux OS - Latest Kernel
AV - Signature Based - Heuristic 1
Snort - Signature based 6
HSM - Hardware Security Module- Storage of Keys 2
Payment Processing API 7
WIFI - WIPS 3
Secure log file Storage 8
Secure Data Storage 4
Cell Transport for uploading and downloading of data and signature files 9
Application based Firewall 5
500
10
11
12
USB
13
Cell
Broadband
14

FIG. 1

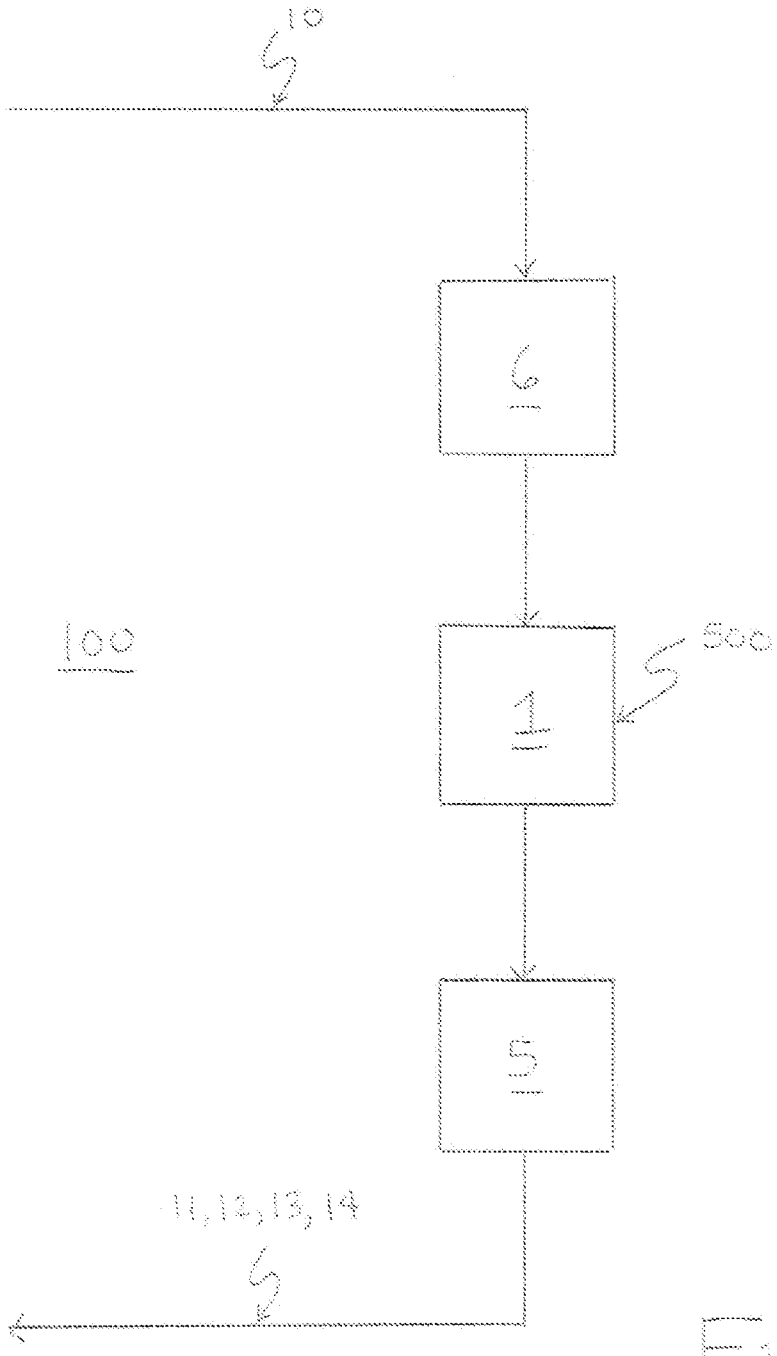


Fig. 2A

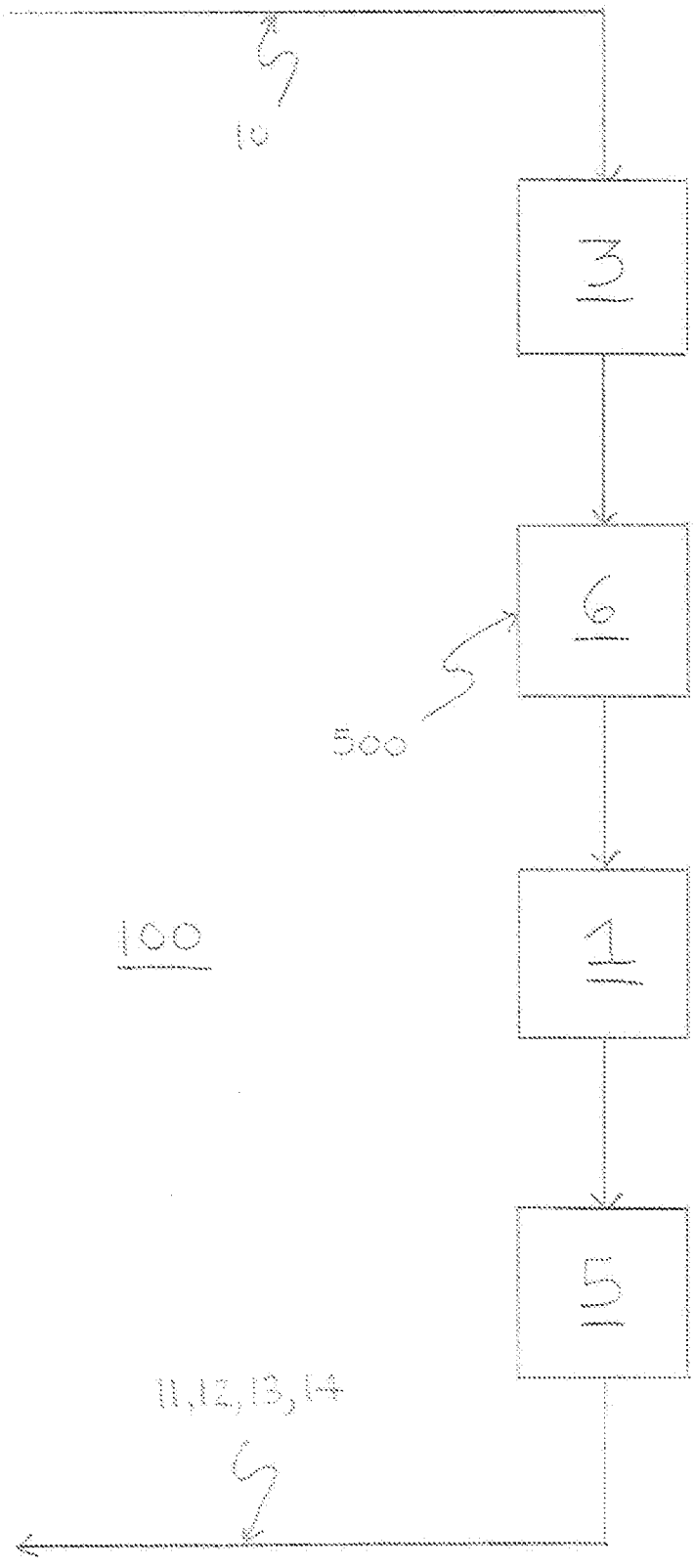


Fig. 2B

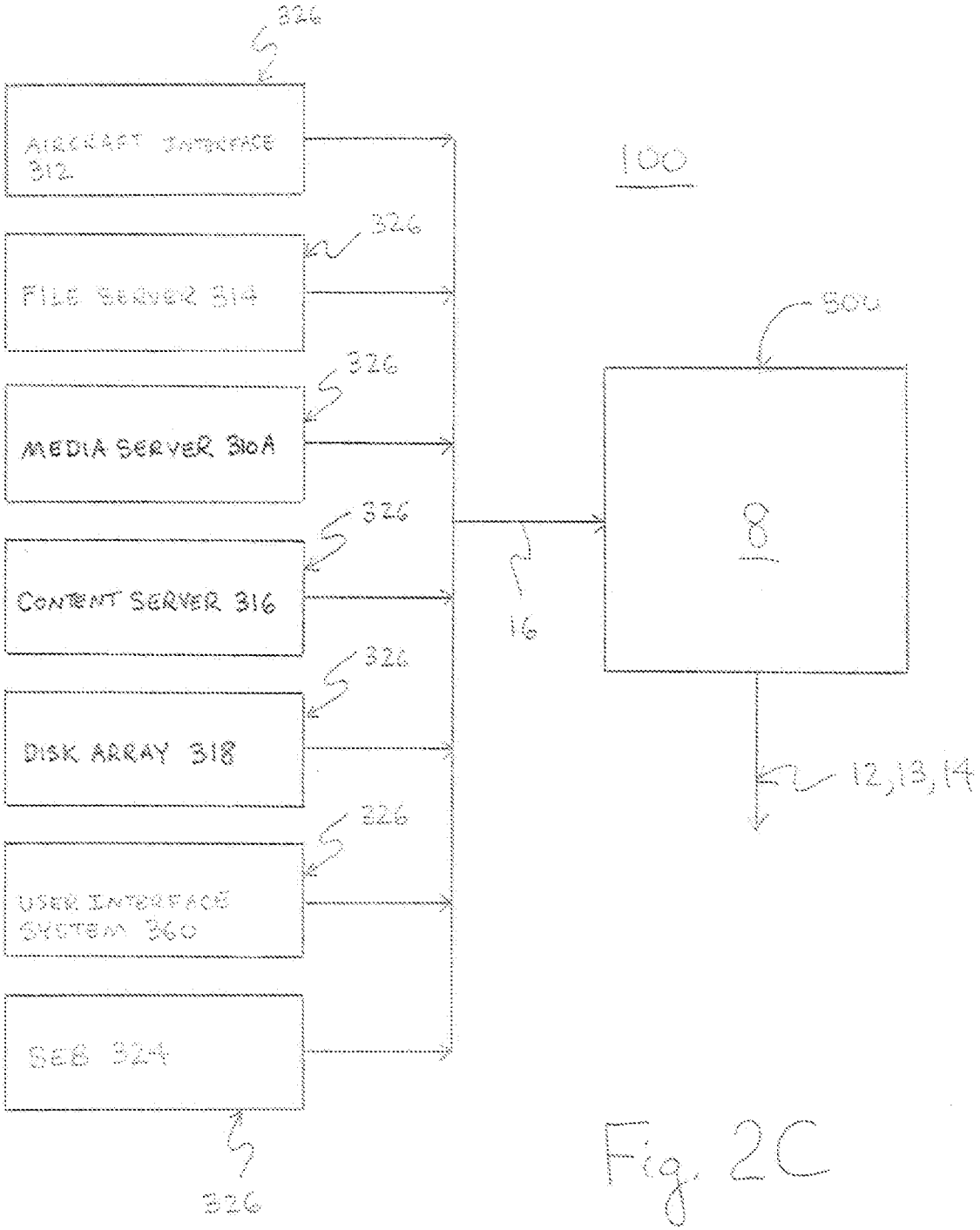

326
AIRCRAFT INTERFACE 312
326
FILE SERVER 314
326
MEDIA SERVER 30A
326
CONTENT SERVER 316
326
DISK ARRAY 318
326
USER INTERFACE SYSTEM 360
SEB 324
326
100
500
8
16
12,13,14

Fig. 2C

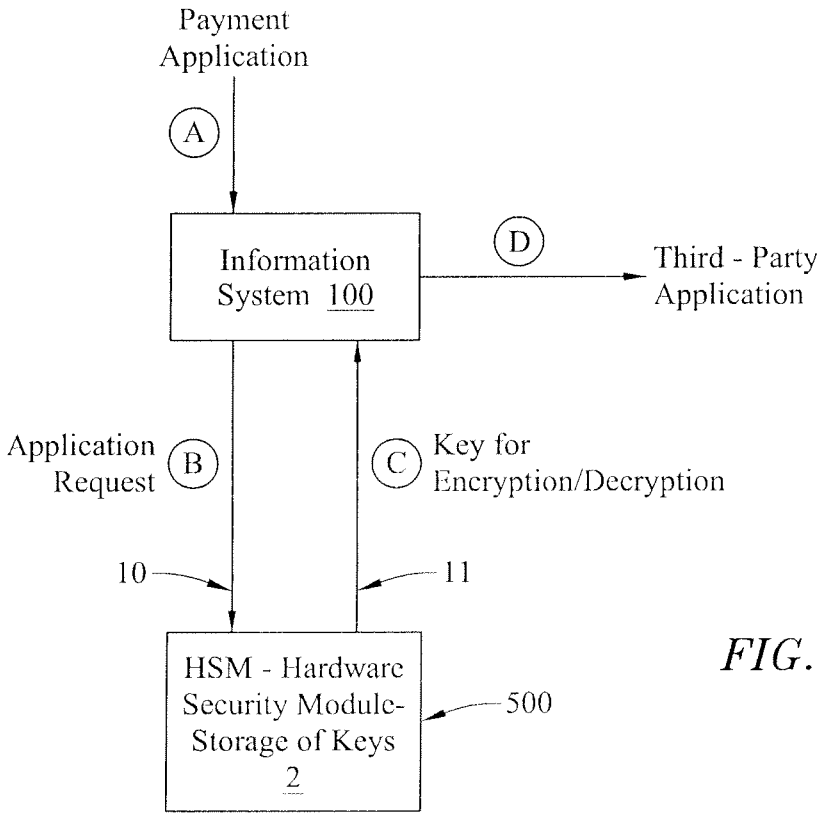

Payment Application
A
Information System 100
D
Third - Party Application
Application Request
B
C
Key for Encryption/Decryption
10
11
HSM - Hardware Security Module- Storage of Keys 2
500

FIG. 2D

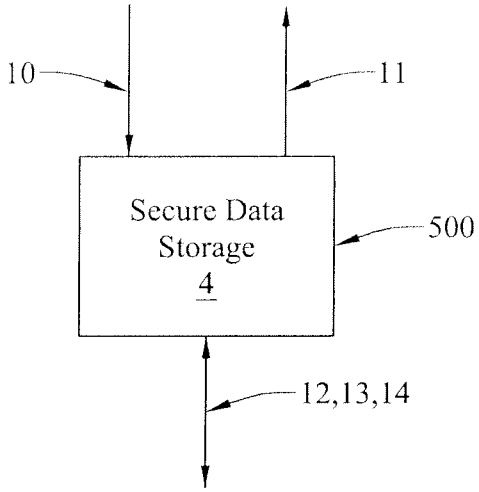


FIG. 2E

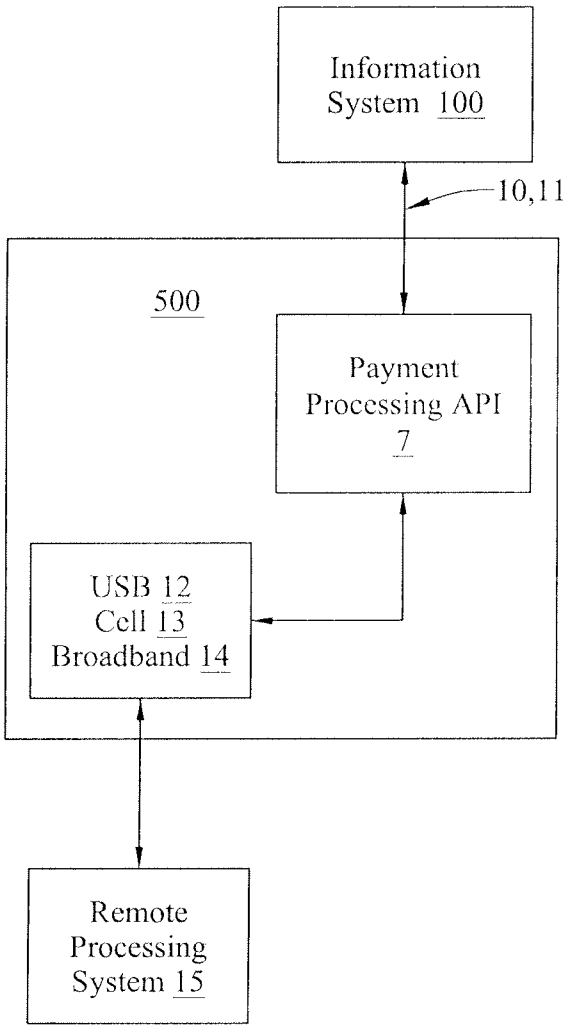
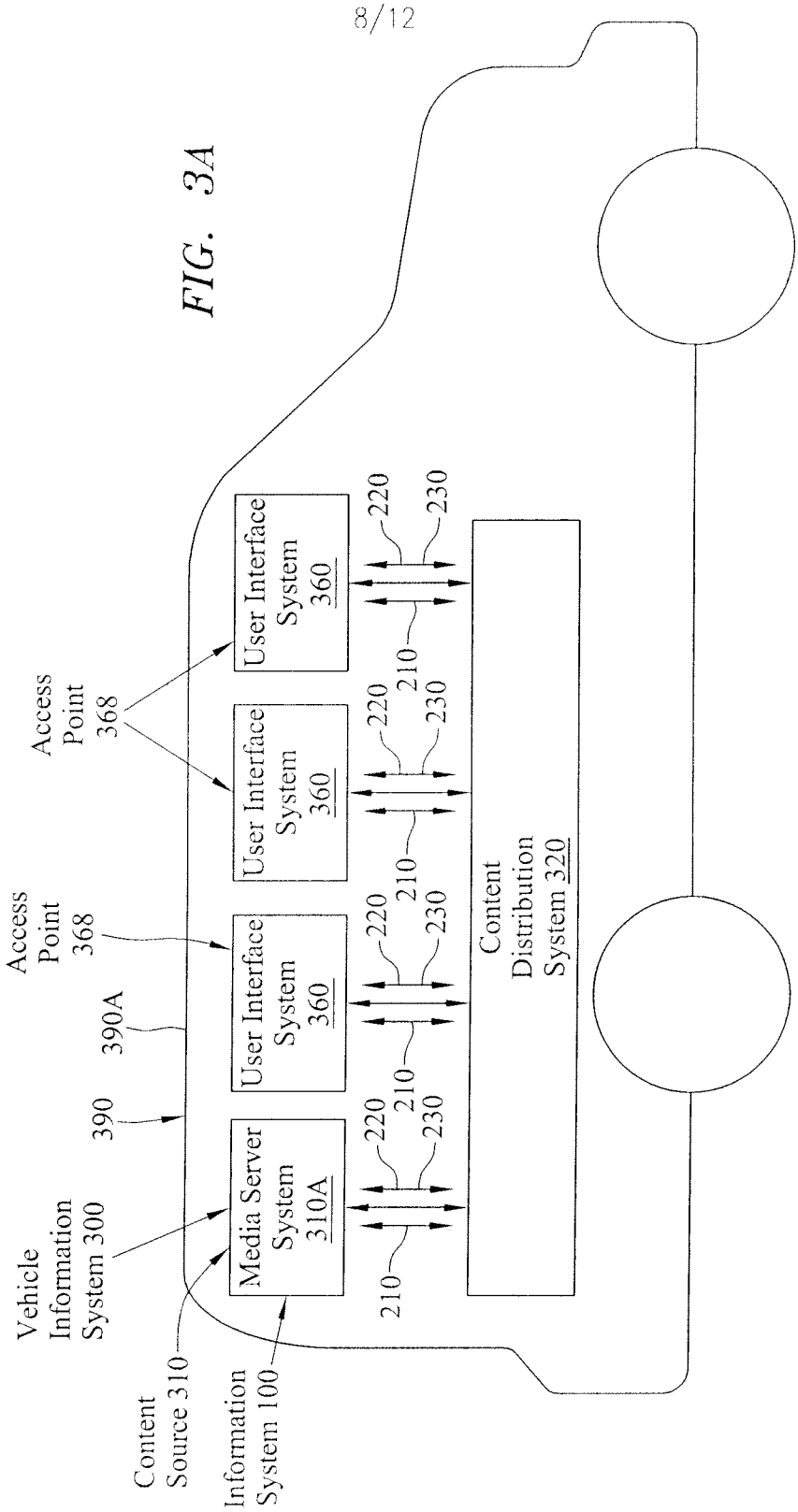

Information System 100
10,11
500
Payment Processing API 7
USB 12
Cell 13
Broadband 14
Remote Processing System 15

FIG. 2F

FIG. 3A


Vehicle Information System 300
Content Source 310
Information System 100
Media Server System 310A
User Interface System 360
User Interface System 360
User Interface System 360
Content Distribution System 320
Access Point 368
Access Point 368
390
390A
210
220
230

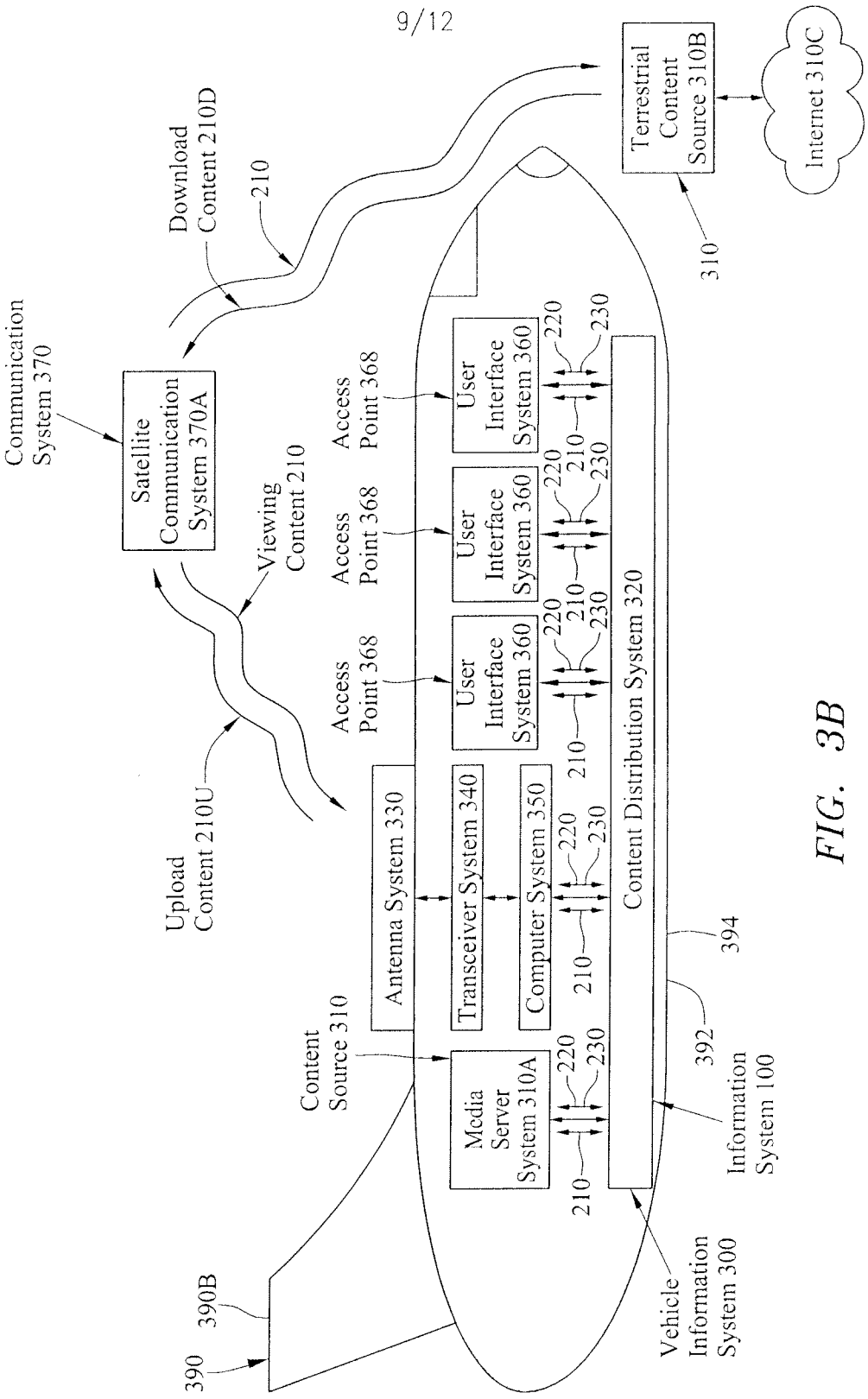

Communication System 370
Satellite Communication System 370A
Download Content 210D
210
Viewing Content 210
Upload Content 210U
Terrestrial Content Source 310B
310
Internet 310C
Access Point 368
User Interface System 360
220
230
210
Content Distribution System 320
Antenna System 330
Transceiver System 340
Computer System 350
Content Source 310
Media Server System 310A
390
390B
Vehicle Information System 300
Information System 100
392
394

FIG. 3B

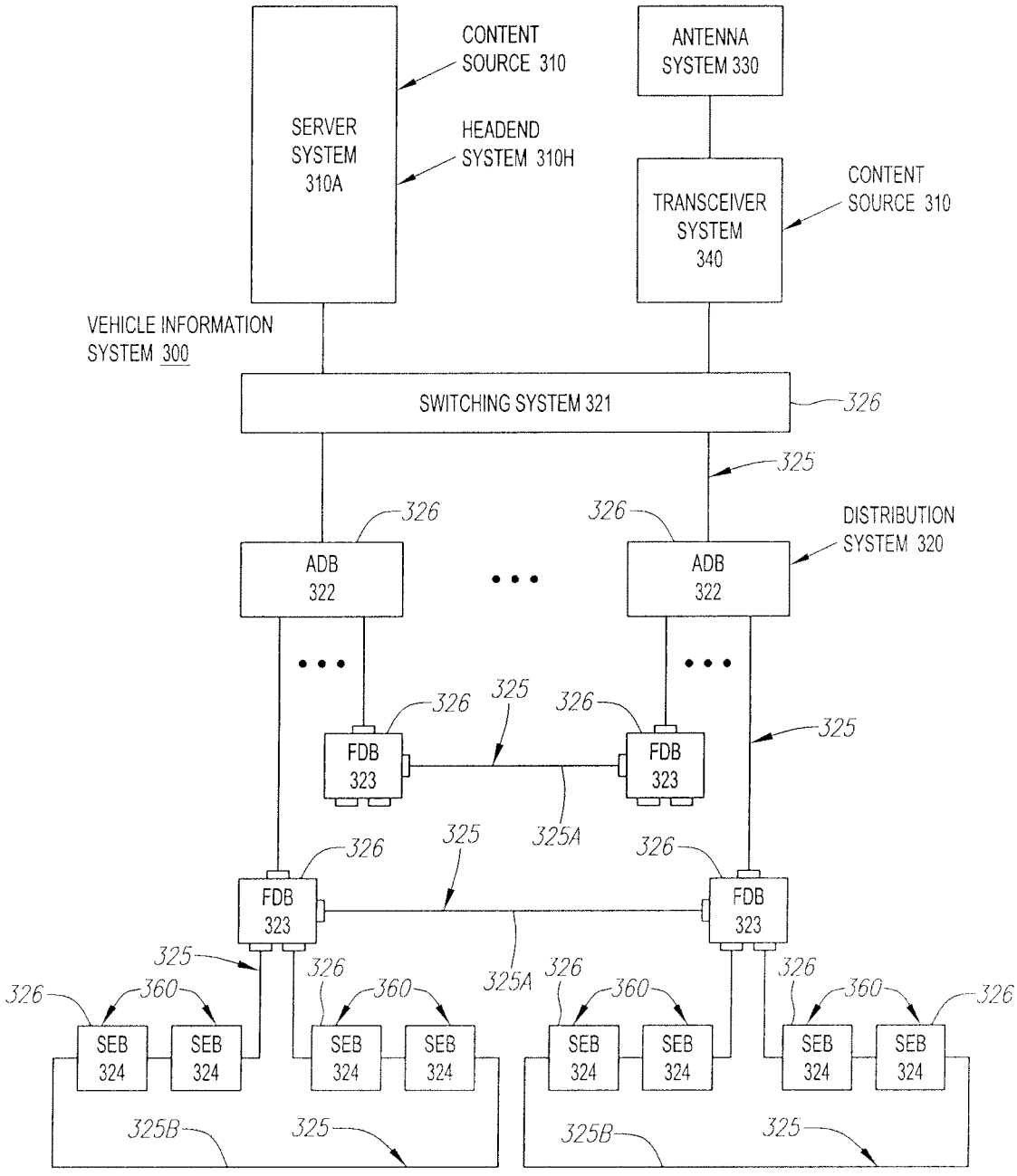

SERVER SYSTEM 310A
CONTENT SOURCE 310
HEADEND SYSTEM 310H
ANTENNA SYSTEM 330
TRANSCEIVER SYSTEM 340
CONTENT SOURCE 310
VEHICLE INFORMATION SYSTEM 300
SWITCHING SYSTEM 321
326
325
DISTRIBUTION SYSTEM 320
ADB 322
FDB 323
325A
SEB 324
360
325B

FIG. 4

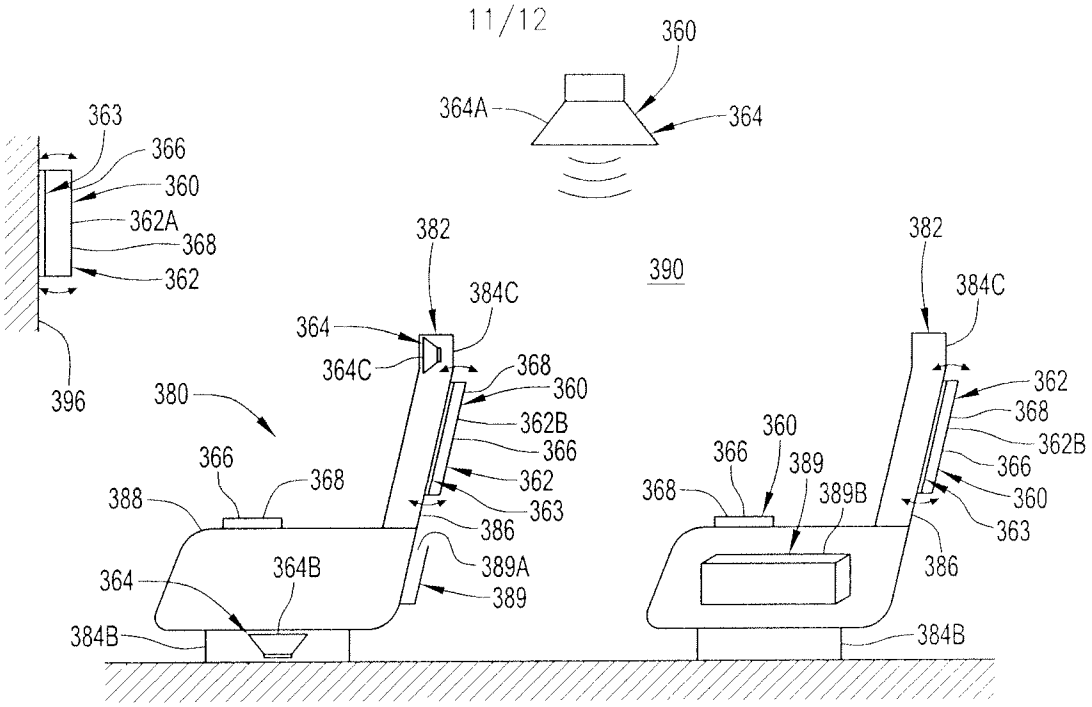

360
364A
364
363
366
360
362A
368
362
396
382
384C
390
364
364C
368
360
380
362B
366
362
363
386
389A
389
388
364B
384B
382
384C
362
368
362B
366
360
363
386
384B
360
366
389
368
389B

FIG. 5A

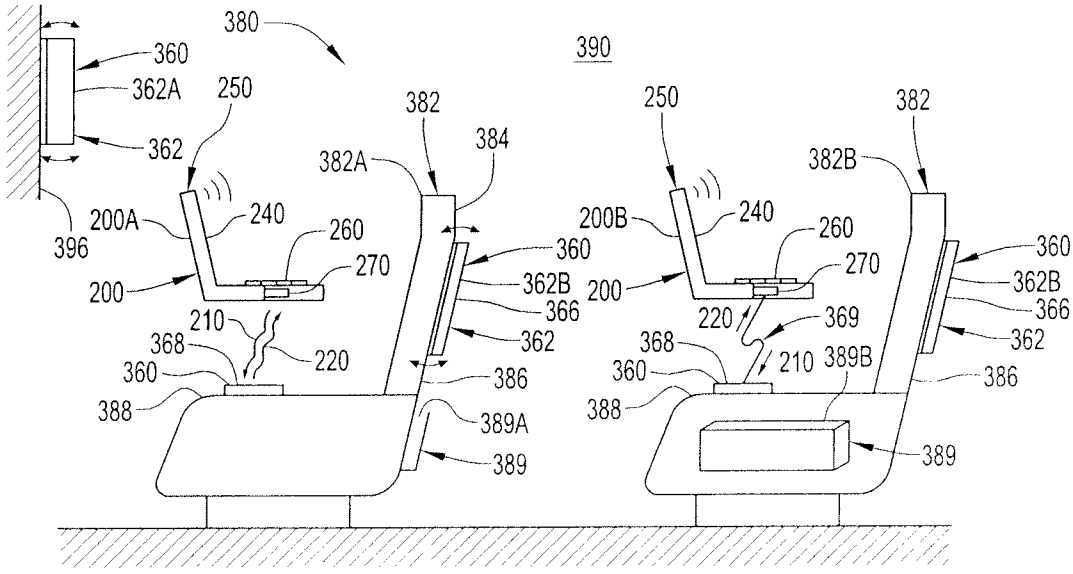

380
390
360
362A
362
396
250
382
384
382A
200A
240
260
270
200
210
220
368
360
388
360
362B
366
362
386
389A
389
250
382
382B
200B
240
260
270
200
220
369
368
210
389B
360
388
360
362B
366
362
386
389

FIG. 5B

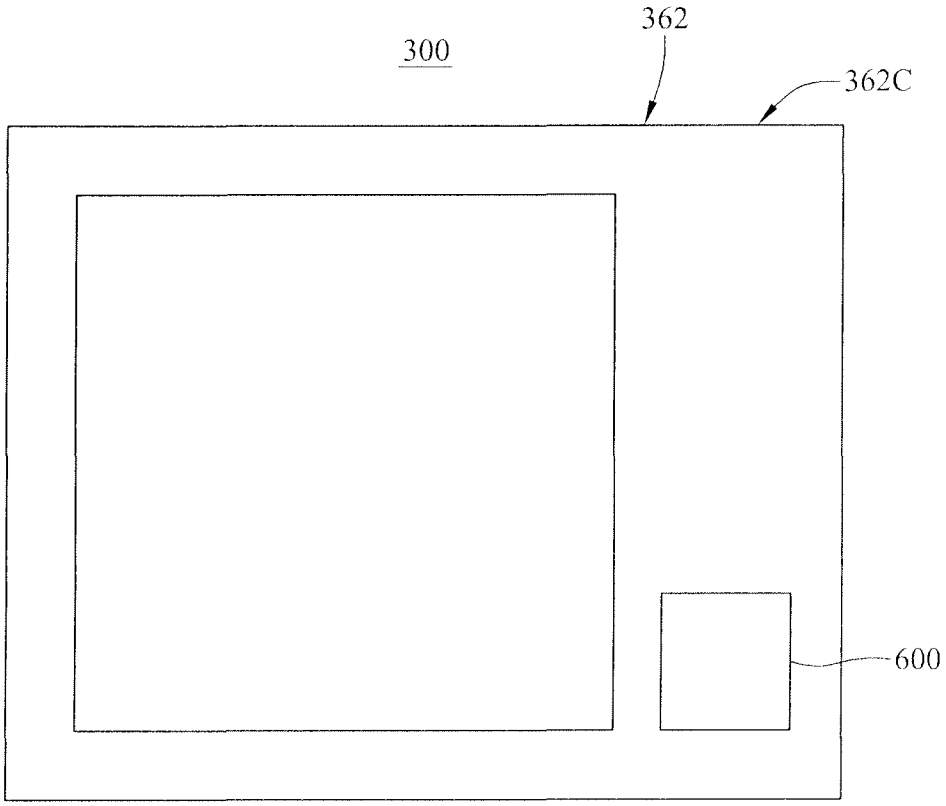


FIG. 6