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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 January 2017 (26.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/015026 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/12* (2009.01)

(21) International Application Number:
PCT/US2016/042090

(22) International Filing Date:
13 July 2016 (13.07.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/805,296 21 July 2015 (21.07.2015) US

(71) Applicant: **MOTOROLA SOLUTIONS, INC.** [US/US]; 1303 E. Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventor: **EYAL, Eilon**; Kibutz Dafna, 12235 Galil Elyon (IL).

(74) Agent: **STETTNER, Derek C.**; Michael Best & Friedrich LLP, 100 East Wisconsin Avenue, Suite 3300, Milwaukee, Wisconsin 53202 (US).

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

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

Published:

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

— *with amended claims (Art. 19(1))*

WO 2017/015026 A1

(54) Title: SYSTEMS AND METHODS FOR MONITORING AN OPERATING SYSTEM OF A MOBILE WIRELESS COMMUNICATION DEVICE FOR UNAUTHORIZED MODIFICATIONS

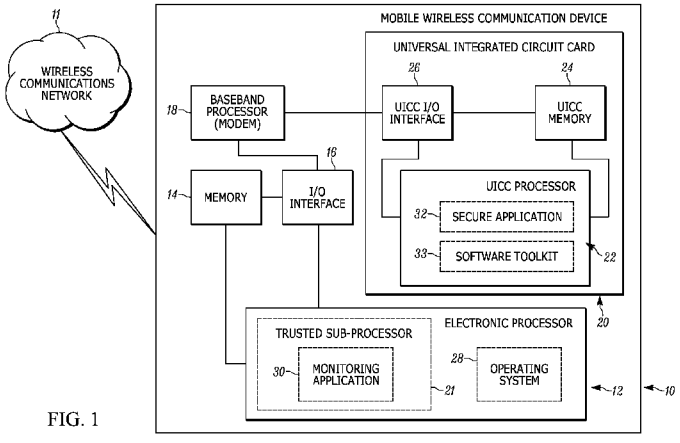

FIG. 1

(57) Abstract: A method and system for securely monitoring an operating system of a mobile wireless communication device for unauthorized modifications. A secure application is provided on universal integrated circuit card of the mobile wireless communication device. The secure application is configured to control the wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network. A monitoring application is provided in a trusted sub-processor of the processor of the mobile wireless communication device. A secure communication link is established between the secure application and the monitoring application. A heartbeat token is generated by the trusted sub-processor, based on a modification status for the operating system and at least one system variable. The secure application receives the heartbeat token, and determines that an unauthorized software modification exists based on the heartbeat token. The secure application activates at least one countermeasure when an unauthorized software modification exists.

SYSTEMS AND METHODS FOR MONITORING AN OPERATING SYSTEM OF A MOBILE WIRELESS COMMUNICATION DEVICE FOR UNAUTHORIZED MODIFICATIONS

BACKGROUND OF THE INVENTION

[0001] Mobile wireless communication devices (e.g., smart telephones, tablet computers, and portable radios) include operating systems that manage hardware and software resources of the mobile wireless communication devices. Operating systems also provide an interface between user applications (e.g., "apps") and the hardware and software resources. Most commonly, operating systems are pre-loaded on mobile wireless communication devices by a wireless service provider, prior to providing the device to an end user (sometime referred to as a "subscriber"). Most operating systems are designed so that they cannot be modified by end users. Restricted-access operating systems are often referred to as "closed" operating systems. Operating systems are closed to improve stability (i.e., reliable and consistent operation of the mobile wireless communication device) and to reduce maintenance problems caused by untested or non-compliant modifications to the operating systems or the use of application software not specifically designed to operate with the operating system. When mobile wireless communications devices are used in environments where security is a concern (e.g., public safety, military, and government), closed operating systems are used to maintain appropriate security.

[0002] Despite the closed nature of the operating systems, it is still possible for end users to modify an operating system using specialized equipment and software (e.g., "jail breaking," and "rooting"). Once an operating system has been modified, unauthorized software can be installed, which can lead to reduced system stability and reduced security.

[0003] Accordingly, there is a need for a method for monitoring an operating system of a mobile wireless communication device for unauthorized modifications.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0004] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed invention, and explain various principles and advantages of those embodiments.

[0005] FIG. 1 is a block diagram illustrating a mobile wireless communication device in accordance with some embodiments.

[0006] FIG. 2 is a block diagram illustrating the internal communications of the mobile wireless communication device of FIG. 1 in accordance with some embodiments.

[0007] FIG. 3 illustrates a method for monitoring an operating system of a mobile wireless communication device for unauthorized modifications in accordance with some embodiments.

[0008] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention.

[0009] The apparatus and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

DETAILED DESCRIPTION OF THE INVENTION

[0010] Some embodiments of the invention include a method for secure monitoring of an operating system of a mobile wireless communication device for unauthorized

modifications. In one embodiment, the method includes providing a secure application on a universal integrated circuit card of the mobile wireless communication device. The secure application is configured to control the wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network. The method further includes providing a monitoring application in a trusted sub-processor of the processor of the mobile wireless communication device. The method further includes establishing a secure communication link between the secure application and the monitoring application. The method further includes the trusted sub-processor generating a heartbeat token based on a modification status for the operating system and at least one system variable. The method further includes the secure application receiving the heartbeat token, and determining that an unauthorized software modification exists based on the heartbeat token. The method further includes the secure application activating at least one countermeasure. Some embodiments of the invention include a system for secure monitoring of the operating system of a mobile wireless communication device for unauthorized modifications. In one such embodiment, the system includes a universal integrated circuit card and an electronic processor. The universal integrated circuit card is configured to control wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network. The electronic processor includes a trusted sub-processor, which is configured to establish a secure communication link between the trusted sub-processor and the universal integrated circuit card. The trusted sub-processor is further configured to generate a heartbeat token based on a modification status for the operating system and at least one system variable. The universal integrated circuit card is further configured to receive the heartbeat token from the trusted sub-processor, determine that an unauthorized software modification exists based on the heartbeat token, and activate at least one countermeasure.

[0011] As illustrated in FIG. 1, the mobile wireless communication device 10 includes an electronic processor 12 (e.g., a microprocessor or another suitable programmable device), a memory 14 (e.g., a computer-readable storage medium), an input/output interface 16, a baseband processor 18 (e.g., a network modem), and a

universal integrated circuit card (UICC) 20. The mobile wireless communication device 10 is capable of terminating and originating voice calls, data information, and text messages over a wireless communications network 11 (e.g., a cellular network or other wireless network). In many of the embodiments described herein, the mobile wireless communication device 10 is a smart telephone. However, in alternative embodiments, the mobile wireless communication device 10 may be a cellular telephone, a smart watch, a tablet computer, a personal digital assistant (PDA), a portable radio, or other device that includes or is capable of being coupled to a network modem or components to enable wireless network communications (such as an amplifier, antenna, etc.) on cellular, land mobile, or other wireless communication networks.

[0012] The electronic processor 12, the memory 14, the input/output interface 16, the baseband processor 18, and the universal integrated circuit card 20, as well as other various modules and components, are coupled by one or more control or data buses to enable communication therebetween. The memory 14 may include a program storage area (e.g., read only memory (ROM) and a data storage area (e.g., random access memory (RAM), and another non-transitory computer readable medium. The electronic processor 12 is connected to the memory 14 and executes computer readable instructions ("software") stored in the memory 14. For example, software for placing and receiving calls, and detecting and reporting unauthorized software modification, as described below, may be stored in the memory 14. The software may include one or more applications, program data, filters, rules, one or more program modules, and/or other executable instructions. The electronic processor 12 includes a trusted sub-processor 21, which provides secure, isolated operating environment within the electronic processor 12. The trusted sub-processor 21 may be implemented as a trusted execution environment, either in hardware, software, or a combination of both. The trusted sub-processor 21 is configured to execute trusted software isolated from the main portion of the electronic processor 12.

[0013] The input/output interface 16 operates to receive user input, to provide system output, or a combination of both. User input may be provided via, for example, a keypad, a touch screen, a scroll ball, buttons, and the like. System output may be

provided via a display device such as a liquid crystal display (LCD), touch screen, and the like (not shown). The input/output interface 16 may include a graphical user interface (GUI) (e.g., generated by the electronic processor 12, from instructions and data stored in the memory 14, and presented on a touch screen) that enables a user to interact with the mobile wireless communication device 10.

[0014] The baseband processor 18 is configured to encode and decode digital data sent and received by a radio transceiver (not shown), and to communicate the data to and from the electronic processor 12 and the universal integrated circuit card 20.

[0015] The universal integrated circuit card (UICC) 20 is a self-contained computer on a chip and includes a UICC processor 22, a UICC memory 24, and a UICC input/output interface 26. The UICC processor 22, the UICC memory 24, and the UICC input/output interface 26, as well as other various modules and components, are connected by one or more control or data buses to enable communication between the modules and components. The UICC memory 24 may include a program storage area and a data storage area. The UICC processor 22 is connected to the UICC memory 24 and retrieves and executes computer readable instructions ("software") stored in the UICC memory 24. The software includes, for example, a software toolkit 33 (e.g., the "subscriber identification module (SIM) Application Toolkit") that enables communication between applications running on the electronic processor 12 and the universal integrated circuit card 20. The UICC memory 24 may also include various access credentials that the mobile wireless communication device 10 may need to communicate using the wireless communications network 11.

[0016] The UICC input/output interface 26 is electrically connected to the baseband processor 18. The UICC processor 22 communicates over this connection with other components of the mobile wireless communication device 10 to send and receive data, including, for example, access credentials for the wireless communications network 11. The universal integrated circuit card 20 is removable from the mobile wireless communication device 10. However, full operation of the mobile wireless communication device 10 requires the presence of the universal integrated circuit card 20 so that the various access credentials in the universal integrated circuit card 20 are

available for authentication processes made prior to or during communications carried out using the wireless communications network 11.

[0017] The electronic processor 12 executes or runs the operating system 28 and the monitoring application 30. The UICC processor 22 runs or executes the secure application 32. In alternative embodiments, the operating system 28, the monitoring application 30, and the secure application 32 may be executed by different processors, or as separate modules from their respective processors. The operating system 28 manages the hardware and software resources of the mobile wireless communication device 10, and serves as an interface between user applications (i.e., "apps") and the hardware and software resources. The monitoring application 30 is configured to operate within the trusted sub-processor 21 of the electronic processor 12. Accordingly, the monitoring application 30 may access the operating system 28, but the operating system 28 may not access or modify the monitoring application 30. The monitoring application 30 monitors the operating system 28 and detects unauthorized modifications to the operating system 28, including, for example, when the security measures of the operating system 28 have been compromised or overridden by "rooting," or "jail breaking." However, it may not be possible for the monitoring application 30 to report the unauthorized modifications that it detects because the monitoring application 30 is isolated, and cannot directly access the baseband processor 18 of the mobile wireless communication device 10. In addition, the operating system 28 cannot be trusted, because the unauthorized modifications to the operating system 28 may include changing the way it receives and responds to commands from software, including the monitoring application 30. For example, the monitoring application 30 may believe that it has successfully reported the unauthorized modification, when in actuality the reporting message has been accepted and subsequently deleted (e.g., by the modified portions of the operating system 28). The monitoring application 30 is configured to communicate with the secure application 32. The secure application 32, in turn, is configured to communicate with the monitoring application 30.

[0018] As illustrated in FIG. 2, the communications between the monitoring application 30 and the secure application 32 take place over a secure communication

link 34. The secure communication link 34 is established securely using suitable network protocols. In one exemplary embodiment, (not shown) the universal integrated circuit card 20 includes a smart card web server (SCWS), which operates to communicate with external components, including, for example, the electronic processor 12, using the bearer independent protocol ("BIP"). The secure communication link 34 may be established using the smart card web server and the hypertext transfer protocol over secure sockets layer ("https"). The secure communication link 34 is secured using a shared key, which is provided by the wireless service provider, and stored in the monitoring application 30 and the universal integrated circuit card 20 when the mobile wireless communication device 10 is initially provisioned. The shared key may be updated when the universal integrated circuit card 20 is replaced. The monitoring application 30 generates a heartbeat token 40, and an OS (operating system) status message 42. The heartbeat token 40 includes the OS status message 42. The OS status message 42 indicates whether the operating system 28 has been modified. The heartbeat token 40 may be transmitted over the secure communication link 34 to the secure application 32.

[0019] FIG. 3 is a flowchart of an exemplary method 100 for monitoring an operating system of a mobile wireless communication device 10 for unauthorized modifications. At block 101, the monitoring application 30 establishes a secure communication link 34 with the secure application 32 on the universal integrated circuit card 20.

[0020] At block 103, the monitoring application 30 generates a heartbeat token 40. The heartbeat token 40 includes the OS status message 42, and one or more system variables, including, for example, the temporary mobile subscriber identity ("TMSI"), the location area identity ("LAI"), and the international mobile subscriber identity ("IMSI"). The temporary mobile subscriber identity is the temporary identifier of the mobile wireless communication device's 10 connection to the wireless communications network 11. The location area identity identifies the current location of the mobile wireless communication device 10. The international mobile subscriber identity is an identifier unique to the mobile wireless communication device 10 across all wireless networks. In some embodiments, a keyed-hash message authentication code algorithm (e.g., HMAC-SHA256) is used to generate a heartbeat token 40,

which includes the OS status message 42, a shared key, the system variables, and a message authentication code.

[0021] At block 105, the monitoring application 30 sends the heartbeat token 40 to the secure application 32 using, for example, an hypertext transfer protocol (HTTP) "put" command. The secure application 32 expects to see a heartbeat token 40 periodically. At block 107, when the secure application 32 has not received a heartbeat token 40 within the determined period, then the secure application 32 activates one or more countermeasures. Countermeasures are described in more detail below. However, when a heartbeat token 40 is received, then the secure application 32 processes the heartbeat token 40 with a keyed-hash message authentication code algorithm, and determines whether the keyed-hash message authentication code is valid at block 111.

[0022] In some embodiments, the secure application 32 uses the message authentication code to determine if the heartbeat token 40 is valid, and the OS status message 42 can be trusted. In alternative embodiments, the check for validity is based on the system variables, to guard against a replay attack. A replay attack occurs when software intercepts a valid message, and continues to send copies of the valid message after the software changes the conditions that generate the valid message. For example, unauthorized software could intercept the heartbeat token 40 containing an OS status message 42 indicating that operating system 28 is unmodified. This unauthorized software could modify the operating system 28, and then replay (i.e., continue sending copies of) the intercepted heartbeat token 40 to the secure application 32, causing the secure application 32 to believe that the operating system 28 is unmodified. The inclusion of system variables in the heartbeat token 40 prevents this type of replay attack. The international mobile subscriber identity value may be altered by unauthorized software, but the international mobile subscriber identity value stored on the universal integrated circuit card 20 cannot be altered by software on the mobile wireless communication device 10. Additionally, both the temporary mobile subscriber identity and the location area identity change over time as the mobile wireless communication device 10 moves or is connected to and disconnected from the wireless communications network 11. In one exemplary

embodiment, the secure application 32 decrypts the heartbeat token 40 and compares the system variables with their current values. When the values match, then the secure application 32 may infer that the heartbeat token 40 is valid and the OS status message 42 can be trusted. In some embodiments, the secure application 32 may require more than one heartbeat token 40 with mismatched system variable values before it infers that the heartbeat token 40 is invalid. Some embodiments use both the message authentication code and the system variable comparisons to determine the validity of the heartbeat token 40. When the secure application 32 determines that the heartbeat token 40 is invalid, then the secure application 32 activates one or more countermeasures at block 109.

[0023] When the secure application 32 determines that the heartbeat token 40 is valid at block 111, it will then check the OS status message 42 at block 113. In some embodiments, the OS status message 42 may consist of a single bit. For example, a value of '0' may indicate that the operating system 28 is unmodified (i.e., the status is 'OK'), while a value of '1' may indicate that the operating system 28 has been modified. In alternative embodiments, the OS status message 42 may be formatted differently, or may contain more information, including, for example, data identifying what modifications were detected and other information, which would be useful in identifying the source or nature of the modifications. When the secure application 32 determines, from the OS status message 42, that the operating system 28 is unmodified, then the process begins again with the generation of another heartbeat token at block 103. When the secure application 32 determines, from the OS status message 42, that the operating system 28 has been modified, then the secure application 32 will activate one or more countermeasures at block 109.

[0024] As noted above, unauthorized modifications to the operating system 28 may result in unstable operation of the mobile wireless communication device 10, compromise the security of the mobile wireless communication device 10, or both. Accordingly, countermeasures may be activated at block 109 of the method 100. In some embodiments, the secure application 32 disables the user-accessible wireless services on the mobile wireless communication device 10, preventing the modified operating system 28 or any unauthorized software from accessing the wireless

communications network 11. To disable the user-accessible wireless services, the secure application 32 blocks cellular communications for everything except the universal integrated circuit card 20. Disabling the user-accessible wireless services prevents the unauthorized software from causing harm to the wireless communications network 11, or transmitting secure data from the mobile wireless communication device 10. In other embodiments, the secure application 32 sends a message to the wireless communications network 11. The message may include the international mobile subscriber identity, or the international mobile equipment identity ("IMEI") for the mobile wireless communication device 10, and an indication that the operating system 28 has been modified. Alternative embodiments may include other types of countermeasures. For example, the secure application 32 may disable other wireless services on the mobile wireless communication device 10 (e.g., Wi-Fi and Bluetooth). Some embodiments include a combination, or all, of the countermeasures described above.

[0025] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings.

[0026] The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0027] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," "has", "having," "includes", "including," "contains", "containing" or

any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by "comprises ... a", "has ... a", "includes ... a", "contains ... a" does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, contains the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially", "essentially", "approximately", "about" or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0028] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and/or apparatus described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used.

[0029] Moreover, an embodiment can be implemented as a computer-readable storage medium having computer readable code stored thereon for programming a computer (e.g., comprising a processor) to perform a method as described and claimed herein. Examples of such computer-readable storage mediums include, but are not limited to,

a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0030] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

Claims

We claim:

1. A method for secure monitoring an operating system of a mobile wireless communication device for unauthorized modifications, the mobile wireless communication device including an electronic processor and a universal integrated circuit card, the method comprising:

providing a secure application in the universal integrated circuit card, the secure application configured to control wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network;

providing a monitoring application in a trusted sub-processor of the electronic processor; and

establishing a secure communication link between the secure application and the monitoring application.

2. The method of claim 1, further comprising generating a heartbeat token based on a modification status and at least one system variable; and receiving, with the secure application, the heartbeat token.

3. The method of Claim 2, wherein generating the heartbeat token includes generating the heartbeat token further based on a message authentication code.

4. The method of Claim 2, wherein generating the heartbeat token includes selecting the at least one system variable from the group consisting of a temporary mobile subscriber identity, a location area identity, and an international mobile subscriber identity.

5. The method of Claim 2, further comprising:

determining, with the secure application, that an unauthorized software modification exists based on the heartbeat token; and

activating, with the secure application, at least one countermeasure.

6. The method of Claim 5, wherein determining that the unauthorized software modification exists includes verifying a message authentication code.

7. The method of Claim 5, wherein activating the at least one countermeasure includes selecting the at least one countermeasure from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

8. The method of Claim 2, further comprising:

determining, with the secure application, that an unauthorized software modification exists when the heartbeat token is not received; and

activating, with the secure application, at least one countermeasure.

9. The method of Claim 8, wherein activating the at least one countermeasure includes selecting the at least one countermeasure from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

10. A system for secure monitoring of an operating system of a mobile wireless communication device for unauthorized modifications, the system comprising:

a universal integrated circuit card configured to control wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network; and

an electronic processor having a trusted sub-processor, the trusted sub-processor configured to establish a secure communication link between the trusted sub-processor and the universal integrated circuit card.

11. The system of claim 10, wherein the trusted sub-processor is further configured to generate a heartbeat token based on a modification status and at least one system variable;

and the universal integrated circuit card is further configured to receive the heartbeat token.

12. The system of Claim 11, wherein the trusted sub-processor is further configured to generate a message authentication code; and wherein generating the heartbeat token includes generating the heartbeat token further based on the message authentication code.

13. The system of Claim 11, wherein the at least one system variable includes at least one selected from the group consisting of a temporary mobile subscriber identity, a location area identity, and an international mobile subscriber identity.

14. The system of Claim 11, wherein the universal integrated circuit card is further configured to determine that an unauthorized software modification exists based on the heartbeat token; and

activate at least one countermeasure.

15. The system of Claim 14, wherein determining that the unauthorized software modification exists includes verifying a message authentication code.

16. The system of Claim 14, wherein the at least one countermeasure includes at least one selected from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

17. The system of Claim 11, wherein the universal integrated circuit card is further configured to determine that an unauthorized software modification exists when the heartbeat token is not received; and

activate at least one countermeasure.

18. The system of Claim 17, wherein the at least one countermeasure includes at least one selected from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

19. A system for secure monitoring of an operating system of a mobile wireless communication device for unauthorized modifications, the system comprising:

a universal integrated circuit card that controls wireless connectivity of the mobile wireless communication device, and communicates with a wireless communications network; and

an electronic processor having a trusted sub-processor, the trusted sub-processor establishes a secure communication link between the trusted sub-processor and the universal integrated circuit card.

AMENDED CLAIMS
received by the International Bureau on 22 November 2016

Claims

We claim:

1. A method for secure monitoring an operating system of a mobile wireless communication device for unauthorized modifications, the mobile wireless communication device including an electronic processor and a universal integrated circuit card, the method comprising:

providing a secure application in the universal integrated circuit card, the secure application configured to disable or block wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network;

providing a monitoring application in a trusted sub-processor of the electronic processor; and

establishing a secure communication link between the secure application and the monitoring application.

2. The method of claim 1, further comprising generating a heartbeat token based on a modification status and at least one system variable; and receiving, with the secure application, the heartbeat token.

3. The method of Claim 2, wherein generating the heartbeat token includes generating the heartbeat token further based on a message authentication code.

4. The method of Claim 2, wherein generating the heartbeat token includes selecting the at least one system variable from the group consisting of a temporary mobile subscriber identity, a location area identity, and an international mobile subscriber identity.

5. The method of Claim 2, further comprising:

determining, with the secure application, that an unauthorized software modification exists based on the heartbeat token; and

activating, with the secure application, at least one countermeasure.

AMENDED SHEET (ARTICLE 19)

6. The method of Claim 5, wherein determining that the unauthorized software modification exists includes verifying a message authentication code.

7. The method of Claim 5, wherein activating the at least one countermeasure includes selecting the at least one countermeasure from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

8. The method of Claim 2, further comprising:

determining, with the secure application, that an unauthorized software modification exists when the heartbeat token is not received; and

activating, with the secure application, at least one countermeasure.

9. The method of Claim 8, wherein activating the at least one countermeasure includes selecting the at least one countermeasure from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

10. A system for secure monitoring of an operating system of a mobile wireless communication device for unauthorized modifications, the system comprising:

a universal integrated circuit card configured to disable or block wireless connectivity of the mobile wireless communication device, and communicate with a wireless communications network; and

an electronic processor having a trusted sub-processor, the trusted sub-processor configured to establish a secure communication link between the trusted sub-processor and the universal integrated circuit card

AMENDED SHEET (ARTICLE 19)

11. The system of claim 10, wherein the trusted sub-processor is further configured to generate a heartbeat token based on a modification status and at least one system variable;

and the universal integrated circuit card is further configured to receive the heartbeat token.

12. The system of Claim 11, wherein the trusted sub-processor is further configured to generate a message authentication code; and wherein generating the heartbeat token includes generating the heartbeat token further based on the message authentication code.

13. The system of Claim 11, wherein the at least one system variable includes at least one selected from the group consisting of a temporary mobile subscriber identity, a location area identity, and an international mobile subscriber identity.

14. The system of Claim 11, wherein the universal integrated circuit card is further configured to determine that an unauthorized software modification exists based on the heartbeat token; and

activate at least one countermeasure.

15. The system of Claim 14, wherein determining that the unauthorized software modification exists includes verifying a message authentication code.

16. The system of Claim 14, wherein the at least one countermeasure includes at least one selected from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

17. The system of Claim 11, wherein the universal integrated circuit card is further configured to determine that an unauthorized software modification exists when the heartbeat token is not received; and

activate at least one countermeasure.

18. The system of Claim 17, wherein the at least one countermeasure includes at least one selected from the group consisting of sending a message to the wireless communications network, and disabling user-accessible wireless services on the mobile wireless communication device.

19. A system for secure monitoring of an operating system of a mobile wireless communication device for unauthorized modifications, the system comprising:

a universal integrated circuit card that disables or blocks wireless connectivity of the mobile wireless communication device, and communicates with a wireless communications network; and

an electronic processor having a trusted sub-processor, the trusted sub-processor establishes a secure communication link between the trusted sub-processor and the universal integrated circuit card.

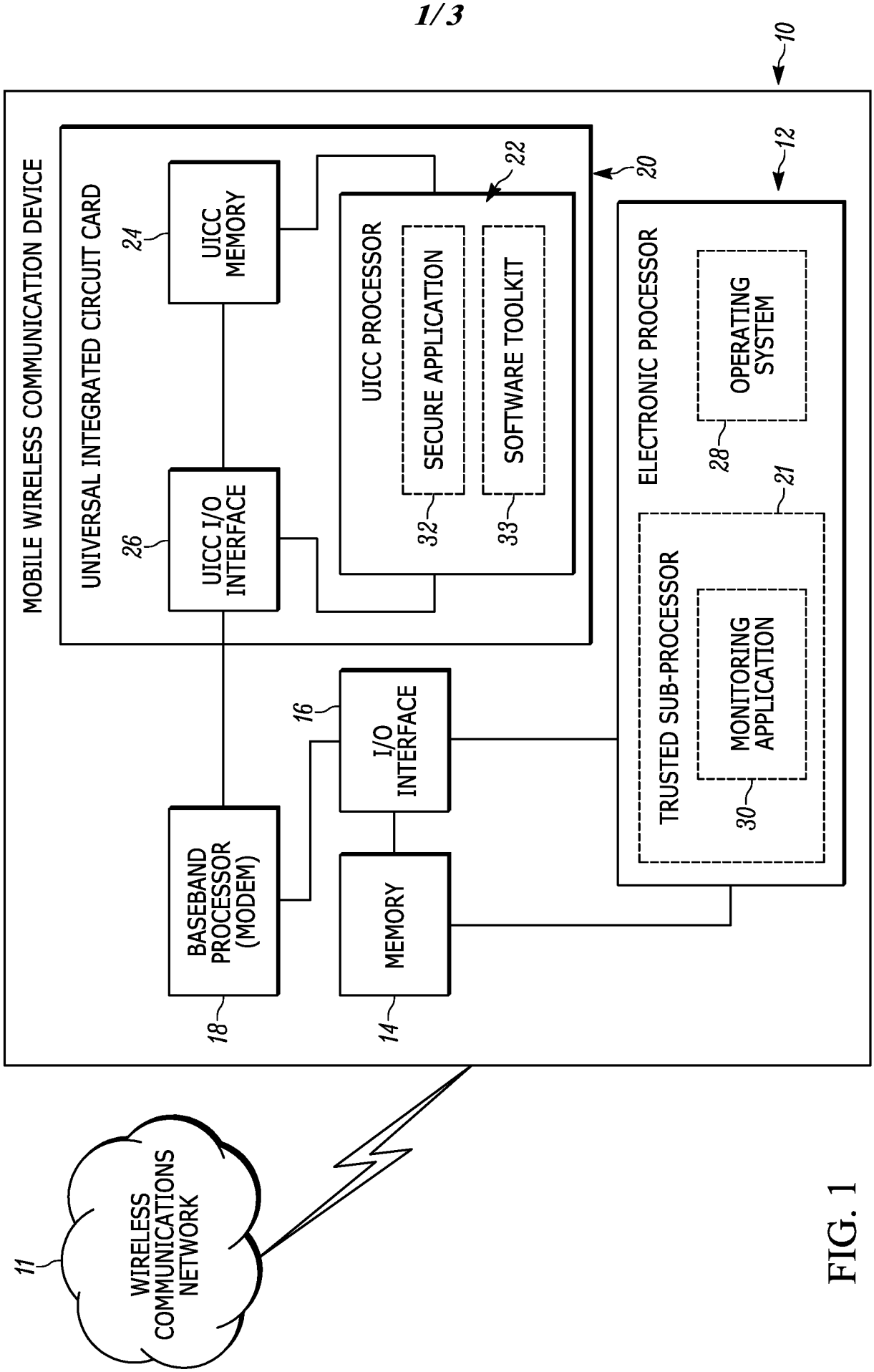
10
MOBILE WIRELESS COMMUNICATION DEVICE
UNIVERSAL INTEGRATED CIRCUIT CARD
20
UICC MEMORY
24
UICC I/O INTERFACE
26
UICC PROCESSOR
22
SECURE APPLICATION
32
SOFTWARE TOOLKIT
33
ELECTRONIC PROCESSOR
12
OPERATING SYSTEM
28
TRUSTED SUB-PROCESSOR
21
MONITORING APPLICATION
30
I/O INTERFACE
16
BASEBAND PROCESSOR (MODEM)
18
MEMORY
14
WIRELESS COMMUNICATIONS NETWORK
11

FIG. 1

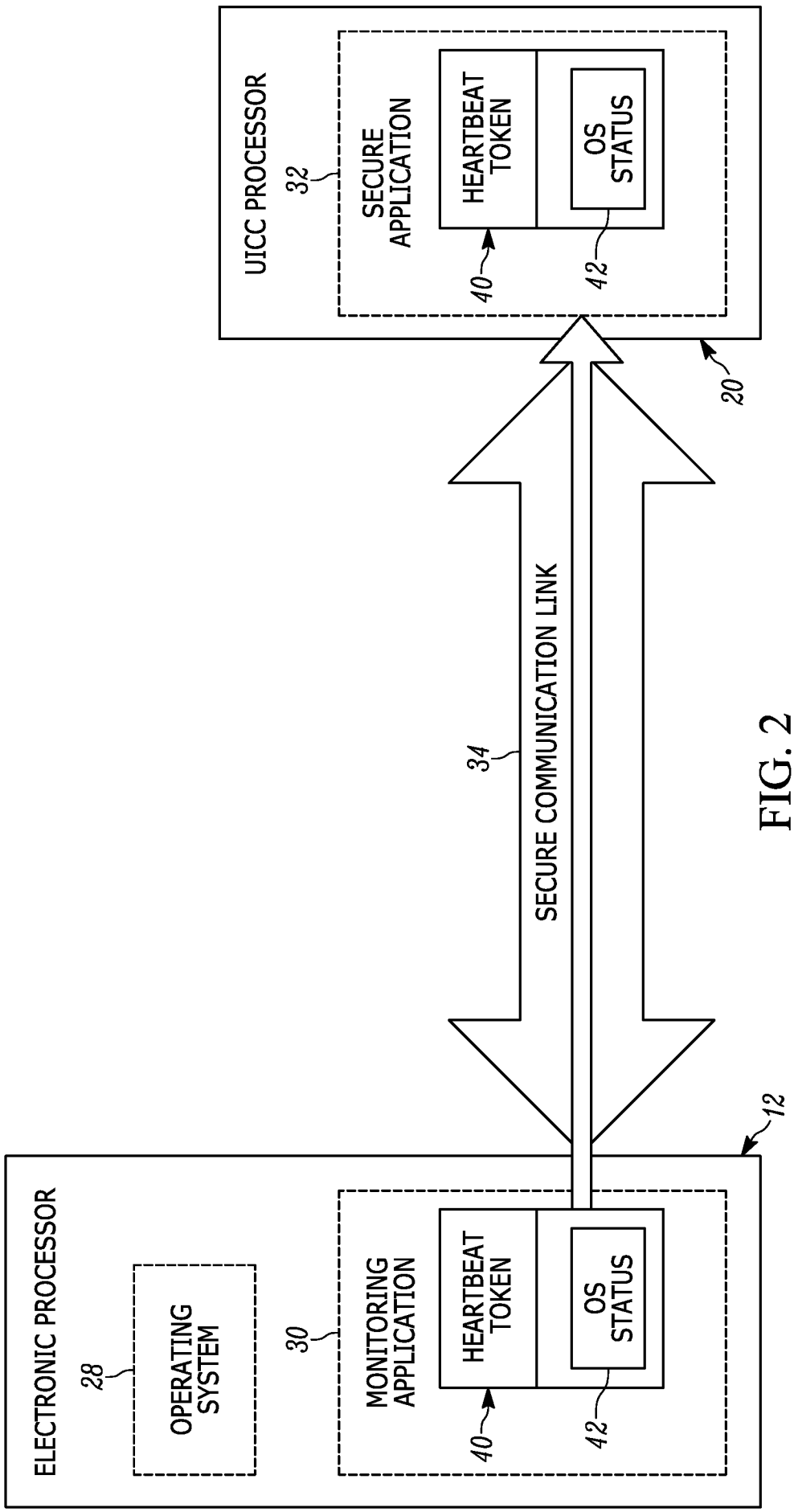
ELECTRONIC PROCESSOR
12
OPERATING SYSTEM
28
MONITORING APPLICATION
30
HEARTBEAT TOKEN
OS STATUS
40
42
SECURE COMMUNICATION LINK
34
UICC PROCESSOR
20
SECURE APPLICATION
32
HEARTBEAT TOKEN
OS STATUS
40
42

FIG. 2

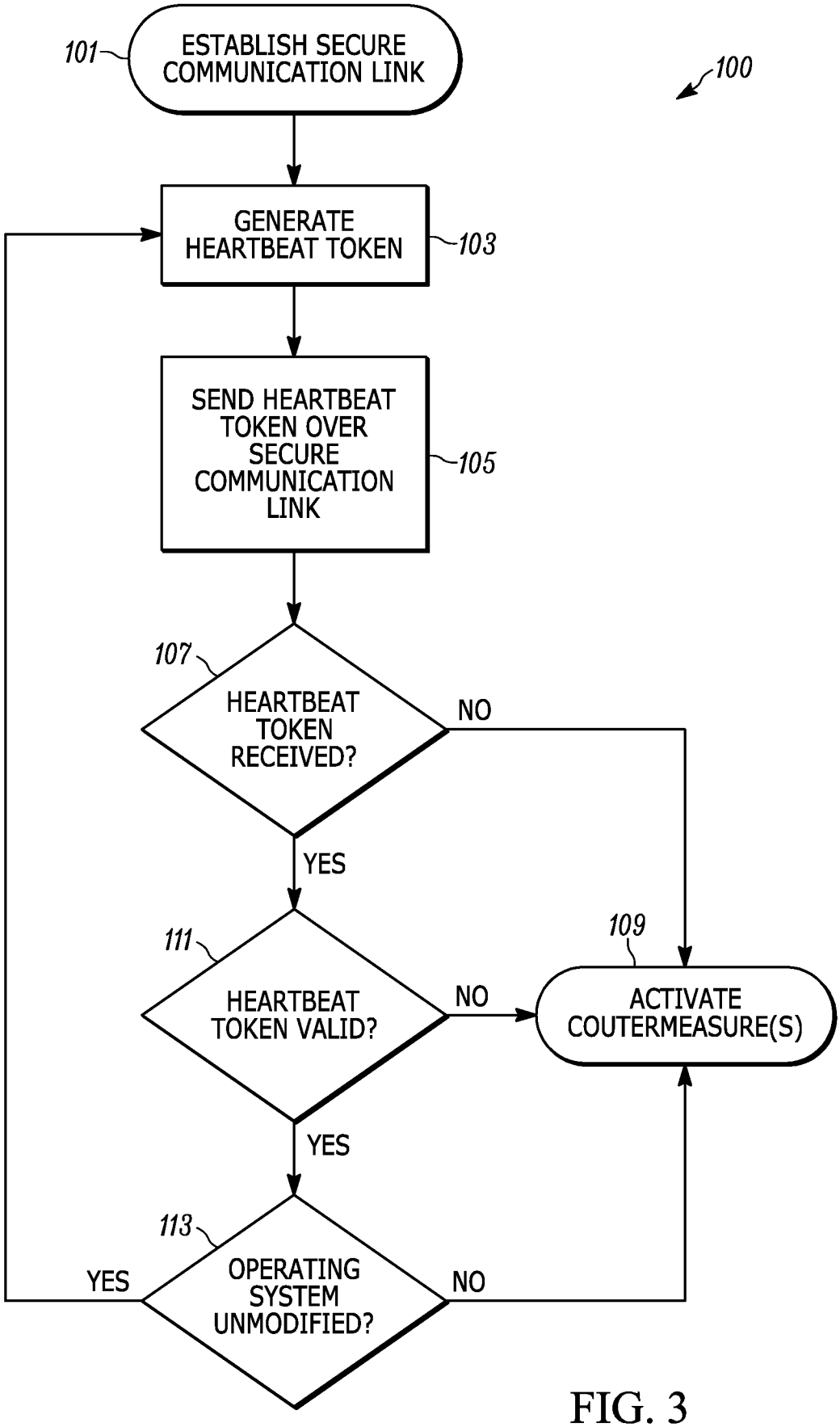
101
ESTABLISH SECURE COMMUNICATION LINK
100
GENERATE HEARTBEAT TOKEN
103
SEND HEARTBEAT TOKEN OVER SECURE COMMUNICATION LINK
105
107
HEARTBEAT TOKEN RECEIVED?
NO
YES
111
HEARTBEAT TOKEN VALID?
NO
109
ACTIVATE COUTERMEASURE(S)
YES
113
OPERATING SYSTEM UNMODIFIED?
YES
NO

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/042090

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/12
ADD.

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 H04W

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/188830 A1 (VISA INT SERVICE ASS [US]) 19 December 2013 (2013-12-19) figures 2,3 paragraph [0007] paragraph [0038] - paragraph [0048] paragraph [0079] - paragraph [0085] paragraph [0097] - paragraph [0098] paragraph [0138] paragraph [0158] - paragraph [0161] claims 1,7,11 -----	1-19
X	US 2012/167162 A1 (RALEIGH GREGORY G [US] ET AL) 28 June 2012 (2012-06-28) paragraph [0269] - paragraph [0270] paragraph [0277] - paragraph [0279] -----	1-19

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
15 September 2016	30/09/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Martínez Cebollada

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/042090

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/297609 A1 (ADAMS NEIL [CA] ET AL) 27 December 2007 (2007-12-27) paragraph [0005] - paragraph [0010] figures 3A,3B -----	1-19
A	US 2014/173733 A1 (FORD DANIEL [US]) 19 June 2014 (2014-06-19) paragraph [0063] claims 1-18 -----	1-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/042090

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013188830 A1	19-12-2013	EP 2862379 A1	22-04-2015
		US 8694795 B1	08-04-2014
		US 2013347064 A1	26-12-2013
		WO 2013188830 A1	19-12-2013
US 2012167162 A1	28-06-2012	US 2012167162 A1	28-06-2012
		US 2015026761 A1	22-01-2015
US 2007297609 A1	27-12-2007	NONE	
US 2014173733 A1	19-06-2014	CA 2835933 A1	17-06-2014
		US 2014173733 A1	19-06-2014