



(51) International Patent Classification:

H04L 29/08 (2006.01) *H04W 8/22* (2009.01)
H04L 29/06 (2006.01) *H04W 12/08* (2009.01)

(21) International Application Number:

PCT/US2018/036788

(22) International Filing Date:

08 June 2018 (08.06.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/554,829 06 September 2017 (06.09.2017) US

(71) Applicant: **GOOGLE LLC** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).

(72) Inventors: **MADAN, Arjita**; Block 1, DivyaSree Omega Towers, Survey No. 13, Kondapur Village, Hyderabad TS 500 084 (IN). **GWALANI, Sumit**; Block 1, DivyaSree Omega Towers, Survey No. 13, Kondapur Village, Hyderabad TS 500 084 (IN).

(74) Agent: **ISAACS, William O., II**; Johnson, Marcou & Isaacs, LLC, PO Box 691, Hoschton, GA 30548 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) Title: AUDIO SIGNAL BASED IDENTIFICATION

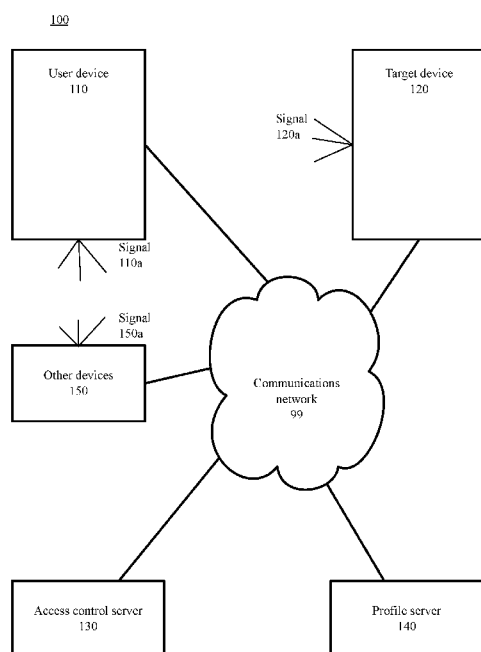


FIG. 1

(57) Abstract: Controlling wireless access to target devices by initiating, by a user device, wireless pairing with a target device. The user device collects, concurrent with the initiating, a wireless signal of at least the target device. One or more computing devices builds a profile for the user device based on the collected wireless signal. The one or more computing devices controls access of the user device to functionality of the target device based on the profile.



AUDIO SIGNAL BASED IDENTIFICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 62/554,829, filed September 6, 2017 and entitled “Audio Signal Based Identification,” the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The technology disclosed herein is related to identification using audio signals collected by user devices. Particular embodiments relate to managing access to functionality based on such audio signals collected via mobile devices.

BACKGROUND

[0003] Identity and access management (IAM) involves controlling access to resources (including e.g., computing resources and physical spaces), including access to functions of those resources. IAM addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

[0004] As of 2016, only thirteen percent of the U.S. adult population does not have a mobile phone. In most places outside the U.S., especially jurisdictions where a landline telecommunications infrastructure was not ubiquitous, more people have mobile phones than have access to landline phones. For example, India has vast non-banking population, many of whom reside in the rural areas and are cut off from access to basic financial services from a trusted source. However, as of 2012, India had nearly a billion mobile phone customers, many of whom access financial services via their mobile phones.

[0005] Throughout the world, mobile computing devices are being used to access functions and services, such as financial services. IAM directed to such access via mobile computing devices is an important aspect of offering such services.

SUMMARY

[0006] The technology described herein includes computer-implemented methods, computer program products, and systems to control wireless access to target devices. In some examples, a user device initiates wireless pairing with a target device. The user device collects, concurrent with the initiating, a wireless signal of at least the target device. One or more computing devices, build a profile for the user device based on the collected wireless signals. The one or more computing devices control access of the user device to functionality of the target device based on the profile.

[0007] In some such examples, the collected signal of a least the target device is an audio frequency signal. In some such examples, collecting further includes collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device. In some such examples, collecting includes collecting a plurality of signals in the frequency band of the wireless signal of the target device.

[0008] In some such examples, the user device determines, concurrent with the initiating, the location of the first user device, and the profile is built further based in the determined location. In some such examples, controlling access includes basing a level of authentication required from the user device on the profile. In some such examples, the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

[0009] These and other aspects, objects, features, and advantages of the example embodiments will become apparent to those having ordinary skill in the art upon consideration of the following detailed description of illustrated example embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Figure 1 is a block diagram depicting an operating environment to control wireless access to target devices, in accordance with certain example embodiments.

[0011] Figure 2 is a block diagram illustrating methods to control wireless access to target devices, in accordance with certain example embodiments.

[0012] Figure 3 is a block diagram illustrating methods to control wireless access to target devices, in accordance with certain example embodiments.

[0013] Figure 4 is a block diagram depicting a computing machine and a module, in accordance with certain example embodiments.

DETAILED DESCRIPTION OF THE EXAMPLE EMBODIMENTS

[0014] In many cases, an organization (such as an enterprise or service provider) may have the need to monitor the risk profile of its members (employees or users) for access to certain services, benefits, or functionality. Audio pairing can be use to connect nearby devices such as mobile phones -- for example to complete a transaction or exchange information between devices. During this pairing, the devices also may share their location information with the server (if online). If sufficient number of devices exist in the environment, which broadcast and receive audio signals, then a footprint of the user can be obtained based on the audio devices that the user interacted with over a certain period.

[0015] The data collected is used to build a risk profile of each user based on factors such as the frequency of pairing, location, authenticity of pairing (for example, does pairing end in a genuine transaction). This approach can be used to modify allowed behavior (for example, prevent too many payment requests from a suspected spammer). The approach is relevant for enterprise applications, allowing an administrator to set rules related to the pairing interactions between enabled users. In an enterprise context, it is possible to control the environment sufficiently to achieve the scenario described in the collection of signals section (for example, there are plenty of devices placed at various locations which emit and receive audio, and there are use cases for users to pair their devices with others).

[0016] Embodiments of the present technology include methods, systems, and computer program products control wireless access to target devices, for example by identifying user devices using audio signals.

Example System Architectures

[0017] Figure 1 is a block diagram depicting a communications and processing operating environment 100 in accordance with certain example embodiments. While each server, system, and device shown in the architecture is represented by one instance of the server, system, or device, multiple instances of each can be used. Further, while certain aspects of operation of the present technology are presented in examples related to Figure 1 to facilitate enablement of the claimed invention, additional features of the present technology, also facilitating enablement of the claimed invention, are disclosed elsewhere herein.

[0018] As depicted in Figure 1, the example operating environment 100 includes network devices 110, 120, 130, 140, and 150; each of which may be configured to communicate with one another via communications network 99. In some embodiments, a user associated with a device must install an application and/or make a feature selection to obtain the benefits of the technology described herein.

[0019] Network 99 includes one or more wired or wireless telecommunications means by which network devices may exchange data. For example, the network 99 may include one or more of a local area network (LAN), a wide area network (WAN), an intranet, an Internet, a storage area network (SAN), a personal area network (PAN), a metropolitan area network (MAN), a wireless local area network (WLAN), a virtual private network (VPN), a cellular or other mobile communication network, a BLUETOOTH® wireless technology connection, a near field communication (NFC) connection, any combination thereof, and any other appropriate architecture or system, that facilitates the communication of signals, data, and/or messages. Throughout the discussion of example embodiments, it should be understood that the terms "data" and "information" are used interchangeably herein to refer to text, images, audio, video, or any other form of information that can exist in a computer-based environment.

[0020] Each network device 110, 120, 130, 140, and 150, can include a communication module capable of transmitting and receiving data over the network 99. For example, each network device can include a server, a desktop computer, a laptop computer, a tablet computer, a television with one or more processors embedded therein and/or coupled thereto, a smart phone, a handheld computer, a personal digital assistant (PDA), or any other wired or wireless processor-driven device.

[0021] User device 110 can be any user device, such as a mobile phone. User device 110 can receive signals, such as signal 120a and signal 150a, from devices within signal range of the user device, such as target device 120 and other devices 150. Target device 120 can be a device similar to user device 110, for example a mobile phone to be used for peer-to-peer payments between user device 110 and target device 120. As another example, target device 120 can be an automated teller machine (ATM) or an information kiosk with which the user device 110 can establish a local communication channel. Other devices 150 can be any device that emits signal 150a. Signal 150 can be energy, such as radio frequency electromagnetic energy or audio energy, compatible with the receiving abilities of user device 110. In general, user device 110, target device 120, and any one or more of zero or more other devices are within a local range of each other, where “local” means the range of signals 110a, 120a, and 150a.

[0022] Profile server 140 can be operated by a financial services company, or, as further example, by a company offering access control services to a financial services company. Access control server 130 can be operated by the financial services company to control access to functions (such as peer-to-peer payments between user device 110 and user device 120) offered by a function server 150 of the financial services company. Control of such access can be based on audio data collected by user devices 110, 120, and 150 based on profiles stored in profile server 140.

[0023] The network connections illustrated are examples and other means of establishing a communications link between the computers and devices can be used. Moreover, those having ordinary skill in the art having the benefit of the present disclosure will appreciate that the network devices illustrated in Figure 1 may have any of several other suitable computer system configurations. For example, computing devices 110 and 120 each may be embodied as a mobile phone or handheld computer and may not include all the components described above.

[0024] In example embodiments, the network computing devices, and any other computing machines associated with the technology presented herein, may be any type of computing machine such as, but not limited to, those discussed in more detail with respect to Figure 4. Furthermore, any modules associated with any of these computing machines, such as modules described herein or any other modules (scripts, web content, software, firmware, or hardware) associated with the technology presented herein may be any of the modules discussed in more detail with respect to Figure 4. The computing machines discussed herein may communicate with one another as well as other computer machines or communication systems over one or more networks, such as network 99. The network 99 may include any type of data or communications network, including any of the network technology discussed with respect to Figure 4.

Example Processes

[0025] The example methods illustrated in the figures are described hereinafter with respect to the components of the example operating environment 100. The example methods also can be performed with other systems and in other environments. The operations described with respect to any of the figures can be implemented as executable code stored on a computer or machine readable non-transitory tangible storage medium (e.g., floppy disk, hard disk, ROM, EEPROM, nonvolatile RAM, CD-ROM, etc.) that are completed based on execution of the code by a processor circuit implemented using one or more integrated circuits; the operations described herein also can be implemented as executable logic that is encoded in one or more non-transitory tangible media for execution (e.g., programmable logic arrays or devices, field programmable gate arrays, programmable array logic, application specific integrated circuits, etc.).

[0026] Referring to Figure 2, and continuing to refer to Figure 1 for context, methods 200 to identify user devices using audio signals are illustrated in accordance with certain example embodiments.

[0027] In such methods 200, a user device 110 initiates wireless pairing with a target device 120 – **Block 210**. In a continuing example, the user device 110 is a mobile phone, and the target device is a particular automatic teller machine (ATM) in a set of two side-by-side ATMs. The user device 110 and the target device ATM 120 have pair multiple times over a month via an audio channel between the user device 110 and the particular ATM 120. The user device 110

use an audio signal to pair with an audio signal broadcast from the target device 120. In some embodiments, the pairing signals are radio frequency signals, such as BLUETOOTH® signals, or other local, near-me, personal, body, or near-field network signals.

[0028] In such methods 200, a user device 110 collects wireless signals, concurrent with initiating, of at least the target device 120 – **Block 220**. In a continuing example, the user device 110 (a mobile phone) and a particular automatic teller machine (ATM) 120 in a set of two side-by-side ATMs (the other being other device 150) have paired multiple times over a month via an audio channel between the first device and the particular ATM. The user device 110 repeatedly collected not only the broadcast of the particular ATM 120, but also collected the broadcast of the nearby ATM 150. In the continuing example, the user device 110 collects signals of both ATMs 120 and 150 concurrent with the initiated pairing of Block 210. In other example, the user device 110 collects only the audio frequency pairing signal of ATM 120. In yet other examples, the user device 110 collects audio signals from other, possibly indeterminate sources in the vicinity. In some examples, the user device 110 collects audio not only within the bandwidth expected for the ATM 120, but also outside that bandwidth.

[0029] The profile server 140, in communication with device 110, builds a profile of the user based on the collected audio signals – **Block 240**. In the continuing example, the data collected by the user device 120 is communicated to the profile server 140 over communication network 99. The audio profile is built by the profile server 140 from data collected by the user device 110 when pairing with the particular given automatic teller machine 120 among a bank of two ATMs serves as part of the profile developed by the profile server 140. That profile includes broadcast audio of the other ATM and background sounds. Such a profile can be treated as unique to the setting. In some embodiments, the profile server 140 builds the risk profile based not only on the collected signals, but on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

[0030] The access control server 130 controls the user's access based on the developed profile – **Block 250**. The user's access can be to network resources (such as devices or data), specific functions of network resources (such as account functions), or to other resources (such as access to restricted physical spaces). In the continuing example, the profile gathered at the

particular ATM can be used by the access control server 130 to control the degree of authentication required over communication network 99. For example, the user may not be required to provide a PIN for the user's regular Friday ATM withdrawal from the particular ATM if an audio environment sufficiently corresponding to the profile is found. In another example, where the bank of ATMs are associated with a record of fraudulent activity, sensing an audio environment sufficiently corresponding to the profile triggers additional authorization steps imposed by the access control server 130.

[0031] Referring to Figure 3, and continuing to refer to prior figures for context, methods 300 to identify user devices using audio signals are illustrated in accordance with certain example embodiments.

[0032] In such methods 300, concurrent with initiating pairing with the target device 120, the user device determines the location of the user device – **Block 330**. In the continuing example, the user device 110 is equipped with a global positioning system (GPS) chip that locates the user device. The user device 110 communicates the collected location data to the profile server 140 via communication network 99. The location information is then used along with the other profile information by the profile server 140 to build the profile (as described in connection with Block 340) that is relied on by the access control server 130 to control access (as described in connection with Block 350).

Other Example Embodiments

[0033] Figure 4 depicts a computing machine 2000 and a module 2050 in accordance with certain example embodiments. The computing machine 2000 may correspond to any of the various computers, servers, mobile devices, embedded systems, or computing systems presented herein. The module 2050 may comprise one or more hardware or software elements configured to facilitate the computing machine 2000 in performing the various methods and processing functions presented herein. The computing machine 2000 may include various internal or attached components such as a processor 2010, system bus 2020, system memory 2030, storage media 2040, input/output interface 2060, and a network interface 2070 for communicating with a network 2080.

[0034] The computing machine 2000 may be implemented as a conventional computer system, an embedded controller, a laptop, a server, a mobile device, a smartphone, a set-top box, a kiosk, a router or other network node, a vehicular information system, one or more processors associated with a television, a customized machine, any other hardware platform, or any combination or multiplicity thereof. The computing machine 2000 may be a distributed system configured to function using multiple computing machines interconnected via a data network or bus system.

[0035] The processor 2010 may be configured to execute code or instructions to perform the operations and functionality described herein, manage request flow and address mappings, and to perform calculations and generate commands. The processor 2010 may be configured to monitor and control the operation of the components in the computing machine 2000. The processor 2010 may be a general purpose processor, a processor core, a multiprocessor, a reconfigurable processor, a microcontroller, a digital signal processor (“DSP”), an application specific integrated circuit (“ASIC”), a graphics processing unit (“GPU”), a field programmable gate array (“FPGA”), a programmable logic device (“PLD”), a controller, a state machine, gated logic, discrete hardware components, any other processing unit, or any combination or multiplicity thereof. The processor 2010 may be a single processing unit, multiple processing units, a single processing core, multiple processing cores, special purpose processing cores, co-processors, or any combination thereof. According to certain embodiments, the processor 2010 along with other components of the computing machine 2000 may be a virtualized computing machine executing within one or more other computing machines.

[0036] The system memory 2030 may include non-volatile memories such as read-only memory (“ROM”), programmable read-only memory (“PROM”), erasable programmable read-only memory (“EPROM”), flash memory, or any other device capable of storing program instructions or data with or without applied power. The system memory 2030 may also include volatile memories such as random access memory (“RAM”), static random access memory (“SRAM”), dynamic random access memory (“DRAM”), and synchronous dynamic random access memory (“SDRAM”). Other types of RAM also may be used to implement the system memory 2030. The system memory 2030 may be implemented using a single memory module or multiple memory modules. While the system memory 2030 is depicted as being part of the computing machine 2000, one skilled in the art will recognize that the system memory 2030 may

be separate from the computing machine 2000 without departing from the scope of the subject technology. It should also be appreciated that the system memory 2030 may include, or operate in conjunction with, a non-volatile storage device such as the storage media 2040.

[0037] The storage media 2040 may include a hard disk, a floppy disk, a compact disc read only memory (“CD-ROM”), a digital versatile disc (“DVD”), a Blu-ray disc, a magnetic tape, a flash memory, other non-volatile memory device, a solid state drive (“SSD”), any magnetic storage device, any optical storage device, any electrical storage device, any semiconductor storage device, any physical-based storage device, any other data storage device, or any combination or multiplicity thereof. The storage media 2040 may store one or more operating systems, application programs and program modules such as module 2050, data, or any other information. The storage media 2040 may be part of, or connected to, the computing machine 2000. The storage media 2040 may also be part of one or more other computing machines that are in communication with the computing machine 2000 such as servers, database servers, cloud storage, network attached storage, and so forth.

[0038] The module 2050 may comprise one or more hardware or software elements configured to facilitate the computing machine 2000 with performing the various methods and processing functions presented herein. The module 2050 may include one or more sequences of instructions stored as software or firmware in association with the system memory 2030, the storage media 2040, or both. The storage media 2040 may therefore represent examples of machine or computer readable media on which instructions or code may be stored for execution by the processor 2010. Machine or computer readable media may generally refer to any medium or media used to provide instructions to the processor 2010. Such machine or computer readable media associated with the module 2050 may comprise a computer software product. It should be appreciated that a computer software product comprising the module 2050 may also be associated with one or more processes or methods for delivering the module 2050 to the computing machine 2000 via the network 2080, any signal-bearing medium, or any other communication or delivery technology. The module 2050 may also comprise hardware circuits or information for configuring hardware circuits such as microcode or configuration information for an FPGA or other PLD.

[0039] The input/output (“I/O”) interface 2060 may be configured to couple to one or more external devices, to receive data from the one or more external devices, and to send data to the one or more external devices. Such external devices along with the various internal devices may also be known as peripheral devices. The I/O interface 2060 may include both electrical and physical connections for operably coupling the various peripheral devices to the computing machine 2000 or the processor 2010. The I/O interface 2060 may be configured to communicate data, addresses, and control signals between the peripheral devices, the computing machine 2000, or the processor 2010. The I/O interface 2060 may be configured to implement any standard interface, such as small computer system interface (“SCSI”), serial-attached SCSI (“SAS”), fiber channel, peripheral component interconnect (“PCI”), PCI express (PCIe), serial bus, parallel bus, advanced technology attached (“ATA”), serial ATA (“SATA”), universal serial bus (“USB”), Thunderbolt, FireWire, various video buses, and the like. The I/O interface 2060 may be configured to implement only one interface or bus technology. Alternatively, the I/O interface 2060 may be configured to implement multiple interfaces or bus technologies. The I/O interface 2060 may be configured as part of, all of, or to operate in conjunction with, the system bus 2020. The I/O interface 2060 may include one or more buffers for buffering transmissions between one or more external devices, internal devices, the computing machine 2000, or the processor 2010.

[0040] The I/O interface 2060 may couple the computing machine 2000 to various input devices including mice, touch-screens, scanners, electronic digitizers, sensors, receivers, touchpads, trackballs, cameras, microphones, keyboards, any other pointing devices, or any combinations thereof. The I/O interface 2060 may couple the computing machine 2000 to various output devices including video displays, speakers, printers, projectors, tactile feedback devices, automation control, robotic components, actuators, motors, fans, solenoids, valves, pumps, transmitters, signal emitters, lights, and so forth.

[0041] The computing machine 2000 may operate in a networked environment using logical connections through the network interface 2070 to one or more other systems or computing machines across the network 2080. The network 2080 may include wide area networks (WAN), local area networks (LAN), intranets, the Internet, wireless access networks, wired networks, mobile networks, telephone networks, optical networks, or combinations thereof. The network 2080 may be packet switched, circuit switched, of any topology, and may use any

communication protocol. Communication links within the network 2080 may involve various digital or an analog communication media such as fiber optic cables, free-space optics, waveguides, electrical conductors, wireless links, antennas, radio-frequency communications, and so forth.

[0042] The processor 2010 may be connected to the other elements of the computing machine 2000 or the various peripherals discussed herein through the system bus 2020. It should be appreciated that the system bus 2020 may be within the processor 2010, outside the processor 2010, or both. According to certain example embodiments, any of the processor 2010, the other elements of the computing machine 2000, or the various peripherals discussed herein may be integrated into a single device such as a system on chip (“SOC”), system on package (“SOP”), or ASIC device.

[0043] Embodiments may comprise a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing embodiments in computer programming, and the embodiments should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment of the disclosed embodiments based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use embodiments. Further, those skilled in the art will appreciate that one or more aspects of embodiments described herein may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as more than one computer may perform the act.

[0044] The example embodiments described herein can be used with computer hardware and software that perform the methods and processing functions described herein. The systems, methods, and procedures described herein can be embodied in a programmable computer, computer-executable software, or digital circuitry. The software can be stored on computer-

readable media. For example, computer-readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays (FPGA), etc.

[0045] The example systems, methods, and acts described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain acts can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different example embodiments, and/or certain additional acts can be performed, without departing from the scope and spirit of various embodiments. Accordingly, such alternative embodiments are included in the scope of the following claims, which are to be accorded the broadest interpretation to encompass such alternate embodiments.

[0046] Although specific embodiments have been described above in detail, the description is merely for purposes of illustration. It should be appreciated, therefore, that many aspects described above are not intended as required or essential elements unless explicitly stated otherwise. Modifications of, and equivalent components or acts corresponding to, the disclosed aspects of the example embodiments, in addition to those described above, can be made by a person of ordinary skill in the art, having the benefit of the present disclosure, without departing from the spirit and scope of embodiments defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

[0047] In the following some examples are described.

[0048] Example 1: A computer-implemented method to control wireless access to target devices, includes initiating, by a user device, wireless pairing with a target device. The user device collects, concurrent with the initiating, a wireless signal of at least the target device. One or more computing devices build a profile for the user device based on the collected wireless signals. The one or more computing devices control access of the user device to functionality of the target device based on the profile.

[0049] Example 2: The method of example 1, wherein the collected signal of at least the target device is an audio frequency signal.

[0050] Example 3: The method of example 1 or 2, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.

[0051] Example 4: The method of at least one of the preceding examples, wherein collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.

[0052] Example 5: The method of at least one of the preceding examples, further comprising determining, by the user device and concurrent with the initiating, the location of the user device, and wherein the profile is built further based in the determined location.

[0053] Example 6: The method of at least one of the preceding examples, wherein controlling access comprises basing a level of authentication required from the user device on the profile.

[0054] Example 7: The method of at least one of the preceding examples, wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

[0055] Example 8: The method of at least one of the preceding examples, wherein the target device comprises an automatic teller machine or an information kiosk.

[0056] Example 9: The method of at least one of the preceding examples, wherein the user device is a smartphone.

[0057] Example 10: The method of at least one of the preceding examples, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

[0058] Example 11: A computer program product, comprising at least one non-transitory computer-readable storage device having computer-executable program instructions embodied thereon that when executed by one or more computers cause the computers to control wireless access to target devices. The computer-executable program instructions comprise: computer-executable program instructions to initiate, by a user device, wireless pairing with a target

device; computer-executable program instructions to collect, by the user device and concurrent with the initiating, a wireless signal of at least the target device; computer-executable program instructions to build, by one or more computing devices, a profile for the user device based on the collected wireless signals; and computer-executable program instructions to control, by the one or more computing devices, access of the user device to functionality of the target device based on the profile.

[0059] Example 12: The computer program product of example 11, wherein the collected signal of a least the target device is an audio frequency signal.

[0060] Example 13: The computer program product of example 11 or 12, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.

[0061] Example 14: The computer program product of at least one of the examples 11 to 13, wherein the collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.

[0062] Example 15: The computer program product of at least one of the examples 11 to 14, further comprising determining, by the user device and concurrent with the initiating, the location of the user device, and wherein the profile is built further based in the determined location.

[0063] Example 16: The computer program product of at least of the examples 11 to 15 wherein controlling access comprises basing a level of authentication required from the user device on the profile.

[0064] Example 17: The computer program product of at least one of the examples 11 to 16, wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

[0065] Example 18: The computer program product of at least one of the examples 11 to 17, wherein the target device comprises an automatic teller machine or an information kiosk.

[0066] Example 19: The computer program product of at least one of the examples 11 to 18, wherein the user device is a smartphone.

[0067] Example 20: The method of at least one of the examples 11 to 19, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

[0068] Example 21: A system to control wireless access to target devices, the system comprising: a storage device; and a processor communicatively coupled to the storage device, wherein the processor executes application code instructions that are stored in the storage device to cause the system to: initiate, by a user device, wireless pairing with a target device; collect, by the user device and concurrent with the initiating, a wireless signal of at least the target device; build, by one or more computing devices, a profile for the user device based on the collected wireless signals; and control, by the one or more computing devices, access of the user device to functionality of the target device based on the profile.

[0069] Example 22: The system of example 21, wherein the collected signal of a least the target device is an audio frequency signal.

[0070] Example 23: The system of example 21 or 22, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.

[0071] Example 24: The system of at least one of the examples 21 to 23, wherein collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.

[0072] Example 25: The system of at least one of the examples 21 to 24 wherein the processor further executes application code instructions that are stored in the storage device to cause the system to determine, by the user device and concurrent with the initiating, the location of the user device, and wherein the profile is built further based in the determined location.

[0073] Example 26: The system at least one of the examples 21 to 26 wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

[0074] Example 26: The system of at least one of the examples 21 to 26, wherein the target device comprises an automatic teller machine or an information kiosk.

[0075] Example 27: The system of at least one of the examples 21 to 26, wherein the user device is a smartphone.

[0076] Example 28: The system of at least one of the examples 21 to 27, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

CLAIMS

1. A computer-implemented method to control wireless access to target devices, comprising:
 - initiate, by a user device, wireless pairing with a target device;
 - collect, by the user device and concurrent with the initiating, a wireless signal of at least the target device;
 - build, by one or more computing devices, a profile for the user device based on the collected wireless signals; and
 - control, by the one or more computing devices, access of the user device to functionality of the target device based on the profile.
2. The method of claim 1, wherein the collected signal of at least the target device is an audio frequency signal.
3. The method of claim 1 or 2, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.
4. The method of at least one of the preceding claims, wherein collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.
5. The method of at least one of the preceding claims:
 - further comprising determining, by the user device and concurrent with the initiating, the location of the user device, and
 - wherein the profile is built further based in the determined location.
6. The method of at least one of the preceding claims, wherein controlling access comprises basing a level of authentication required from the user device on the profile.
7. The method of at least one of the preceding claims, wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

8. The method of at least one of the preceding claims, wherein the target device comprises an automatic teller machine or an information kiosk.
9. The method of at least one of the preceding claims, wherein the user device is a smartphone.
10. The method of at least one of the preceding claims, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

11. A computer program product, comprising:

at least one non-transitory computer-readable storage device having computer-executable program instructions embodied thereon that when executed by one or more computers cause the computers to control wireless access to target devices, the computer-executable program instructions comprising:

computer-executable program instructions to initiate, by a user device, wireless pairing with a target device;

computer-executable program instructions to collect, by the user device and concurrent with the initiating, a wireless signal of at least the target device;

computer-executable program instructions to build, by one or more computing devices, a profile for the user device based on the collected wireless signals; and

computer-executable program instructions to control, by the one or more computing devices, access of the user device to functionality of the target device based on the profile.

12. The computer program product of claim 11, wherein the collected signal of at least the target device is an audio frequency signal.

13. The computer program product of claim 11 or 12, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.

14. The computer program product of at least one of the claims 11 to 13, wherein the collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.

15. The computer program product of at least one of the claims 11 to 14:

further comprising determining, by the user device and concurrent with the initiating, the location of the user device, and

wherein the profile is built further based in the determined location.

16. The computer program product of at least one of the claims 11 to 15 wherein controlling access comprises basing a level of authentication required from the user device on the profile.

17. The computer program product of at least one of the claims 11 to 16, wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

18. The computer program product of at least one of the claims 11 to 17, wherein the target device comprises an automatic teller machine or an information kiosk.

19. The computer program product of at least one of the claims 11 to 18, wherein the user device is a smartphone.

20. The computer program product of at least one of the claims 11 to 19, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

21. A system to control wireless access to target devices, the system comprising:
a storage device; and
a processor communicatively coupled to the storage device, wherein the processor executes application code instructions that are stored in the storage device to cause the system to:
initiate, by a user device, wireless pairing with a target device;
collect, by the user device and concurrent with the initiating, a wireless signal of at least the target device;
build, by one or more computing devices, a profile for the user device based on the collected wireless signals; and
control, by the one or more computing devices, access of the user device to functionality of the target device based on the profile.
22. The system of claim 21, wherein the collected signal of at least the target device is an audio frequency signal.
23. The system of claim 21 or 22, wherein collecting further comprises collecting, by the user device and concurrent with the initiating, audio outside the bandwidth of the wireless signal of the target device.
24. The system of at least one of the claims 21 to 23, wherein collecting comprises collecting a plurality of signals in the frequency band of the wireless signal of the target device.
25. The system of at least one of the claims 21 to 24
wherein the processor further executes application code instructions that are stored in the storage device to cause the system to determine, by the user device and concurrent with the initiating, the location of the user device, and
wherein the profile is built further based in the determined location.
26. The system at least one of the claims 21 to 25 wherein the profile is built further based on one or more of the frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and the time of the pairing initiation.

27. The system of at least one of the claims 21 to 26, wherein the target device comprises an automatic teller machine or an information kiosk.
28. The system of at least one of the claims 21 to 27, wherein the user device is a smartphone.
29. The system of at least one of the claims 21 to 28, wherein the profile server builds the risk profile based collected signals, frequency of pairings between the user device and the target device, the rate of transactions completed after pairing between the user device and the target device, and / or the time of the pairing initiation.

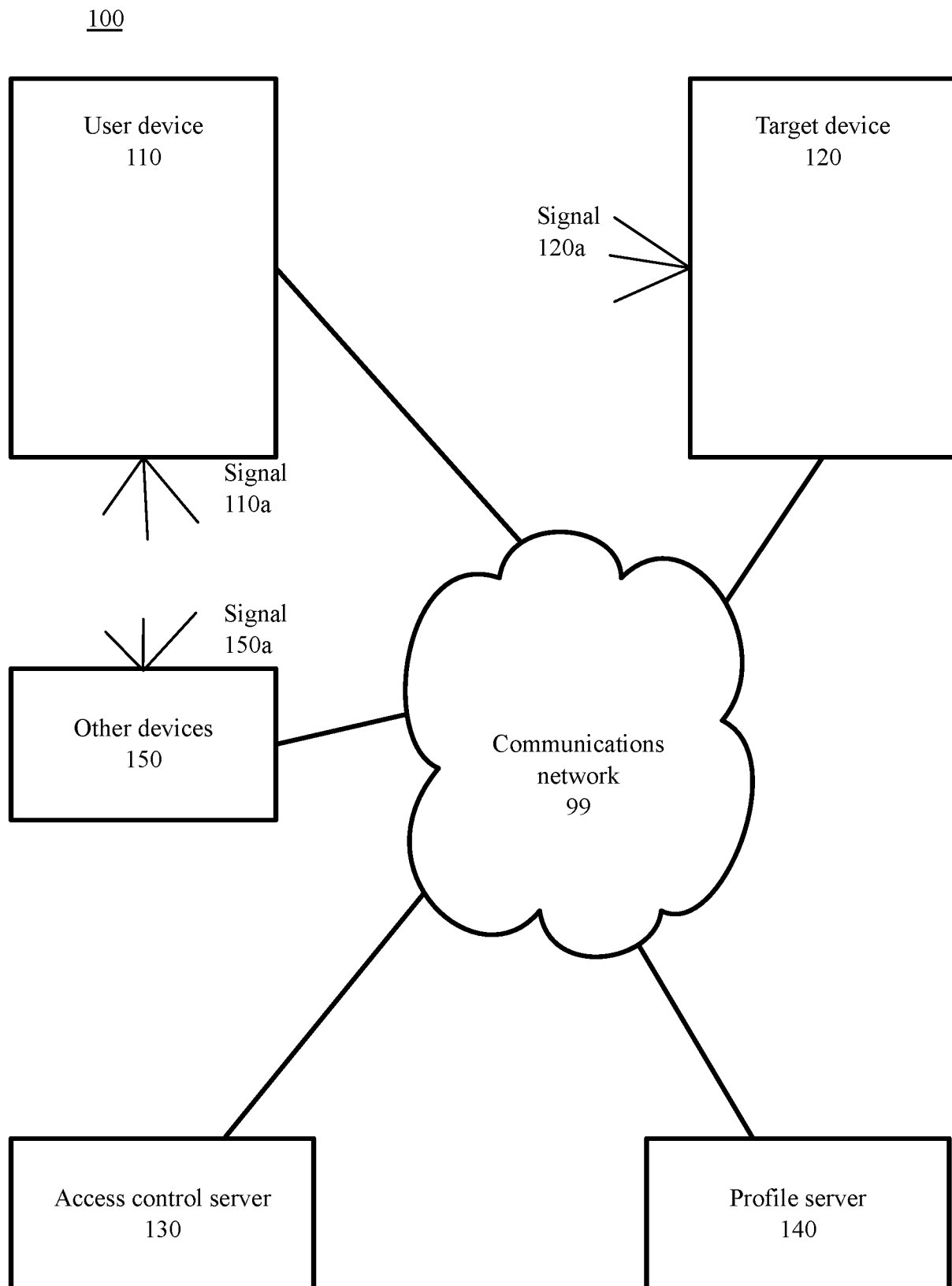


FIG. 1

2/4

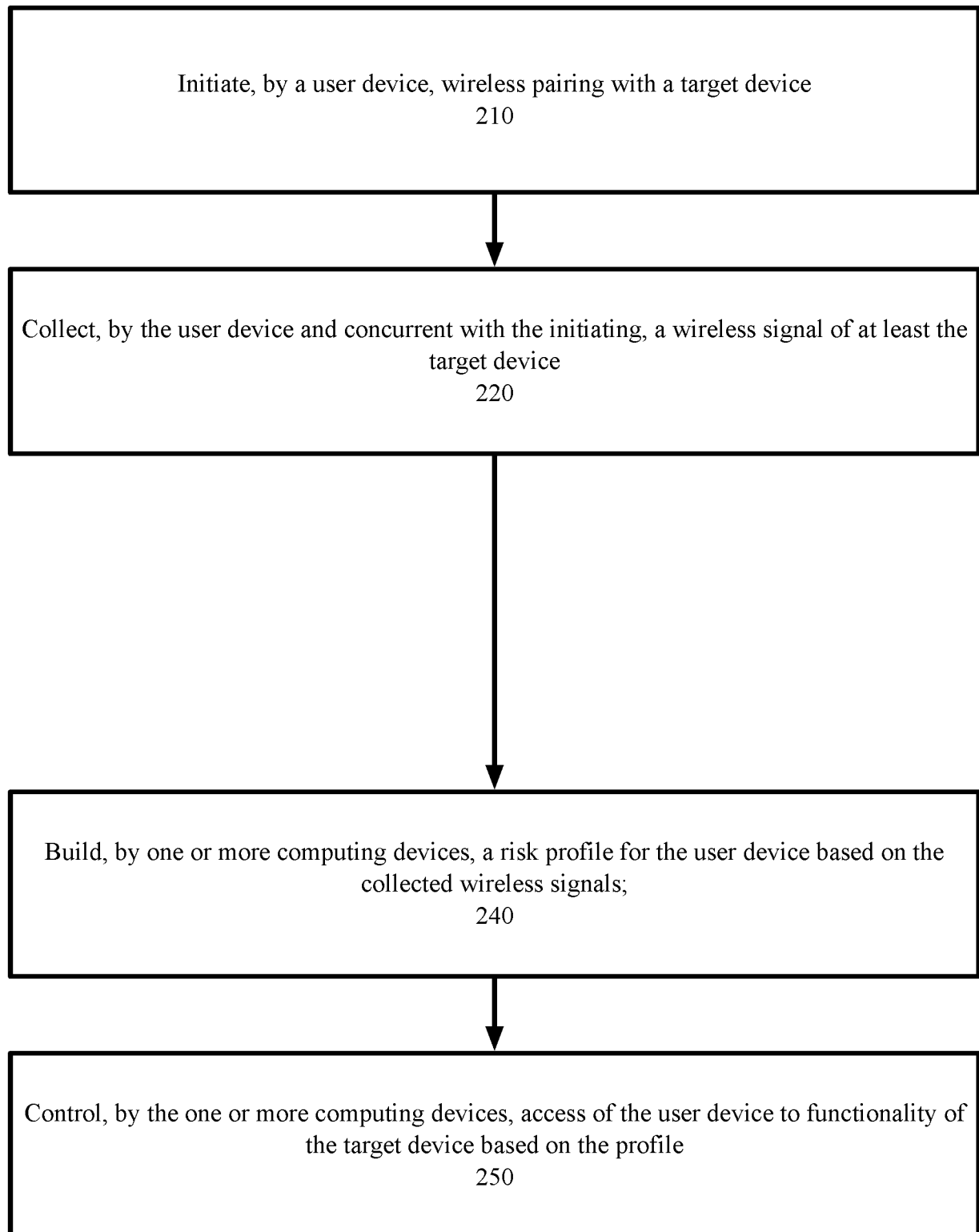
200

FIG. 2

3/4

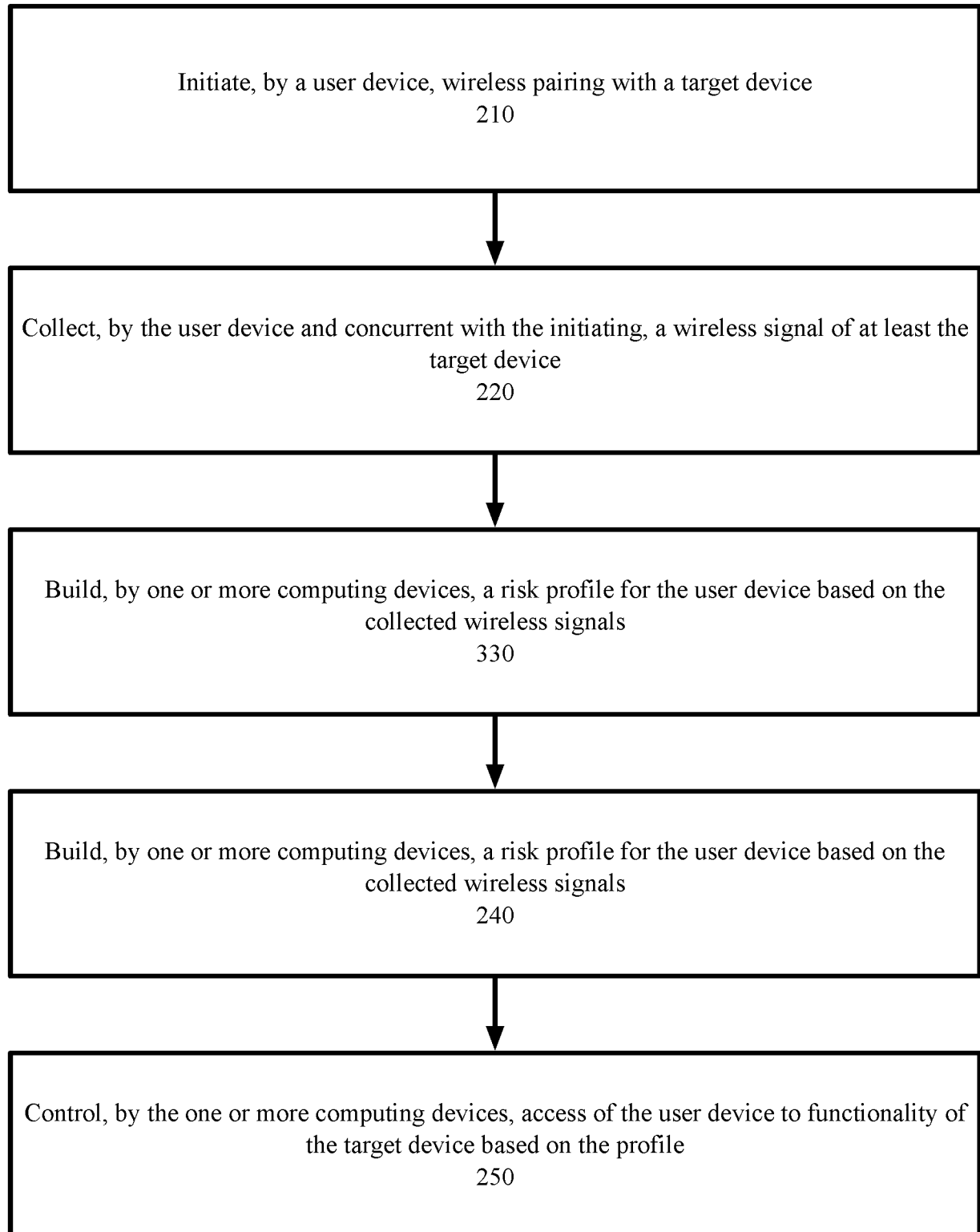
300

FIG. 3

2000

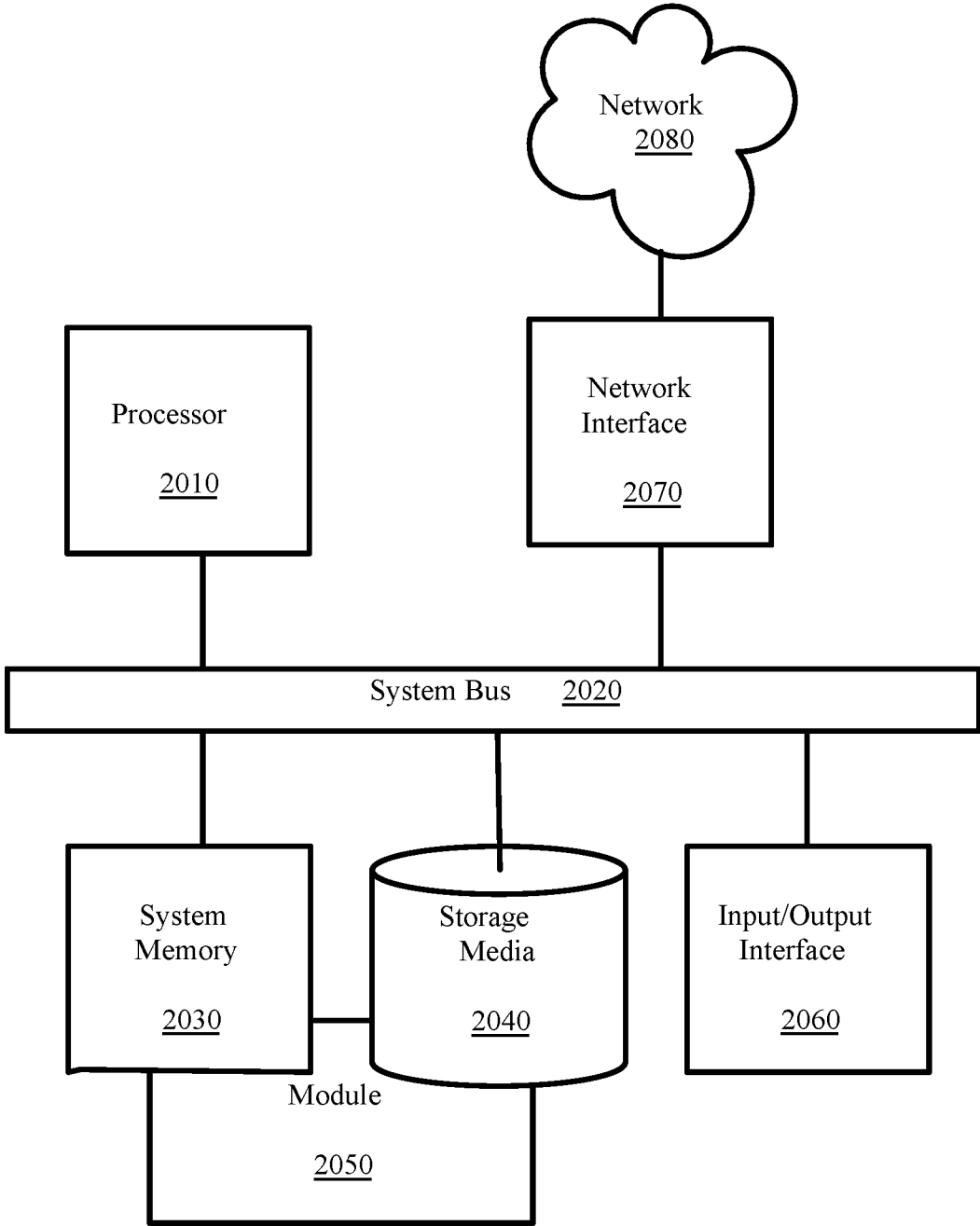


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/036788

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/08 H04L29/06 H04W8/22 H04W12/08
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	IOANNIS AGADAKOS ET AL: "Location-enhanced authentication using the IoT", COMPUTER SECURITY APPLICATIONS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 5 December 2016 (2016-12-05), pages 251-264, XP058306825, DOI: 10.1145/2991079.2991090 ISBN: 978-1-4503-4771-6	1,5-11, 15-21, 25-29
Y	page 2, column 1 - column 2 page 3, column 1 abstract ----- -/--	2-4, 12-14, 22-24



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

11 September 2018

Date of mailing of the international search report

19/09/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Manea, Anda

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2018/036788

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	PARK F S ET AL: "Leveraging Cellular Infrastructure to Improve Fraud Prevention", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2009. ACSAC '09. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 7 December 2009 (2009-12-07), pages 350-359, XP031610280, ISBN: 978-0-7695-3919-5	2-4, 12-14, 22-24
A	paragraph [00iv] -----	1,5-11, 15-21, 25-29