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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 March 2025 (20.03.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/056162 A1

(51) International Patent Classification:
H04L 9/00 (2022.01) *H04L 9/40* (2022.01)

(21) International Application Number:
PCT/EP2023/075281

(22) International Filing Date:
14 September 2023 (14.09.2023)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: ASSA ABLOY AB [SE/SE]; P.O. Box 70340, 107 23 Stockholm (SE).

(72) Inventor: KAUFMANN, Martin; Autalerstraße 19a/4, 8042 Graz (AT).

(74) Agent: MURGITROYD & COMPANY; Murgitroyd House, 165-169 Scotland Street, Glasgow Strathclyde G5 8PL (GB).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE,

(54) Title: RELAY ATTACK DETECTION

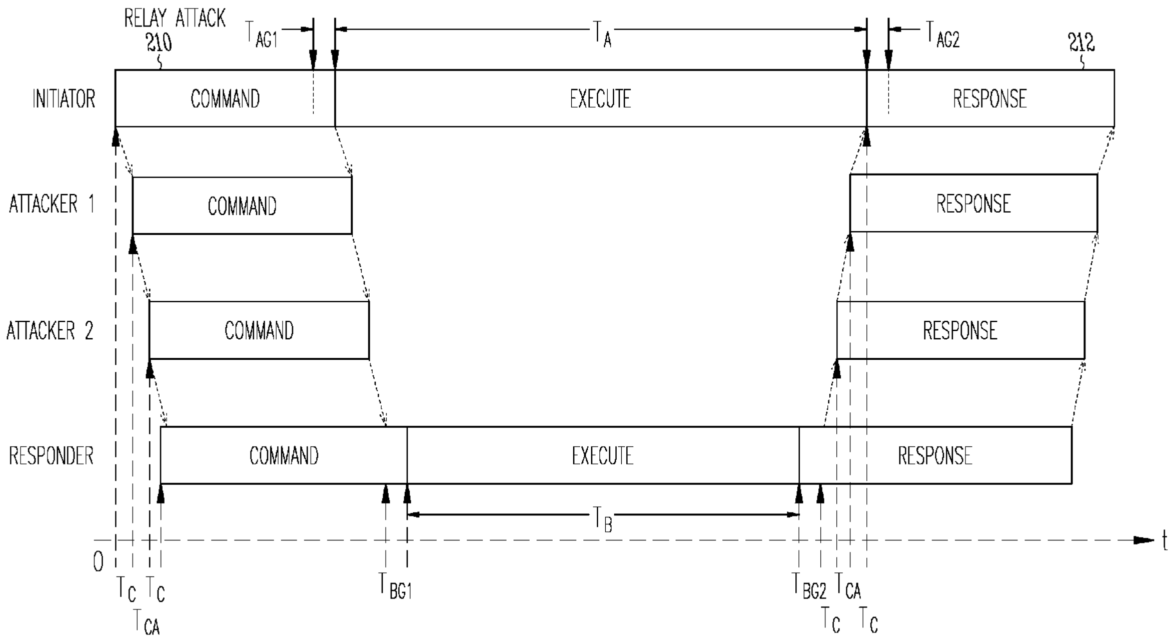

Fig.3

(57) Abstract: An initiator device of an access control system includes physical layer circuitry and processing circuitry operatively coupled to the physical layer circuitry. The processing circuitry is configured to initiate transmission of a command to a responder device, determine a first time measurement of a time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device, receive a response from the responder device that includes a second time measurement of a responder execution time of the command by the responder device, and generate an indication when the first time measurement and second time measurement indicate a relay attack.

[Continued on next page]

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))*

RELAY ATTACK DETECTION

TECHNICAL FIELD

[0001] Embodiments illustrated and described herein generally relate to access control systems and to preventing security breaches in access control systems.

BACKGROUND

[0002] Access control systems grant physical access to an authorized user through a controlled portal such as a secured door. Additionally, remote identity authentication for applications such as mobile online shopping or mobile banking is now a common practice. Remote authentication often involves authentication information being exchanged between a user’s mobile phone and a server performing authentication. Unfortunately, attempts to defeat systems that provide secure authentication often occur. A relay attack is a type of hacking technique that can lead to a security breach of an access control system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] FIG. 1 is an illustration of an example of an access control system structure.

[0004] FIG. 2 is a timing diagram representing an example of a command sent by an initiator device and received by a receiving device.

[0005] FIG. 3 is a timing diagram representing an example of a relay attack involving a command sent by an initiator device received by a receiving device.

[0006] FIG. 4 is a flow diagram of an example of a method of operating an access control system.

[0007] FIG. 5 is a block diagram schematic of portions of an example of a verifier device.

DETAILED DESCRIPTION

[0008] A physical access control system (PACS) provides automatic physical access to an authorized user through a physical access point such as a secured door. Seamless access control systems grant physical access to an authorized user through the controlled portal without requiring intrusive actions of the user such as entering or swiping an access card at a card reader or entering a personal identification number (PIN) or password. The architecture of a PACS may vary significantly based on the application (e.g., a hotel, a residence, an office, etc.), the technology (e.g., access interfaces technology, door type, etc.), and the manufacturer.

[0009] FIG. 1 is an illustration of a basic PACS structure useful for an office application. The Access Credential is a data object, a piece of knowledge (e.g., PIN, password, etc.), or a facet of the person's physical being (e.g., face, fingerprint, etc.) that provides proof of the person's identity. The Credential Device 104 stores the Access Credential when the Access Credential is a data object. The Credential Device 104 may be a smartcard or smartphone. Other examples of Credential Devices include, but are not limited to, proximity radio frequency identification based (RFID-based) cards, access control cards, credit cards, debit cards, passports, identification cards, key fobs, near field communication (NFC) enabled devices, mobile phones, personal digital assistants (PDAs), tags, or any other device configurable to emulate a virtual credential.

[0010] The Credential Device 104 can be referred to as the Access Credential. The Reader device 102 or other verifier device retrieves and authenticates the Access Credential when a Credential Device is used and sends the Access Credential to the Access Controller 106. The Access Controller 106 compares the Access Credential to an Access Control list and grants or denies access based on the comparison, such as by controlling an automatic lock on a door for example.

[0011] The functionality of an Access Controller 106 may be included in the Reader device 102. These Reader devices can be referred to as offline readers or standalone readers. If the unlocking mechanism is included as well, a device is referred to as smart door lock which is more typically used in residential applications. Devices such as smart door locks are often battery powered, and power consumption and battery lifetime can be key parameters for the devices.

[0012] In a PACS, an access sequence consists of four parts: Proof of Presence, Intent Detection, Authentication, and Authorization. The user approaches the door and presents their access credential or credential device. This provides the Proof of Presence and Intent portions of the sequence. The reader device checks the validity of the access credential (the Authentication portion) and sends it to the access controller (e.g., using a local area network or LAN), which grants or denies access (the Authorization portion). As explained above, seamless access is access granted without intrusive actions to show Intent (e.g., presenting a card, entering a password etc.), while maintaining the same level of security as a conventional access system.

[0013] Physical access control systems are susceptible to attempts for unauthorized access such as hacking. A relay attack is a type of hacking technique related to man-in-the middle attacks. In a man-in-the-middle attack, communication between the Access Controller 106 (or Reader device 102) and a Credential Device 104 is initiated by the attacking device, and the attacking device merely relays messages between the two legitimate devices. The Credential Device 104 may be remote from the controlled physical portal, but the Access Controller 106 grants access as if the legitimate Credential Device 104 were present. This may allow access to the holder of the attacking device to the controlled portal.

[0014] FIG. 2 is a timing diagram representing a command sent by an initiator device and received by a responder device. The initiator device may be an interface terminal of a physical access control system (e.g., a Reader Device of a PACS or another type of verifier device) and the responder device may be a Credential Device. The initiator device and the responder device include protocol layer circuitry and processing circuitry. The protocol layer circuitry can include a medium access control (MAC) layer and a physical (PHY) layer. The initiator device transmits a command 210 to the responder device. The command 210 may be included in an authentication protocol communicated between the initiator device and the responder device.

[0015] FIG. 2 shows a time delay or communication time gap T_C between the time the start of the command 210 is sent by the initiator device until it begins to arrive at the responder device. FIG. 2 also shows a time delay or initiator sending time T_{Ag1} between the time the command is signaled to the processing circuitry of the initiator device as being sent and the time the last byte is actually sent by the physical layer circuitry of the initiator device. After the initiator sending time T_{Ag1}, the initiator execution time T_A of executing the command begins.

[0016] FIG. 2 shows another time delay that is a responder receiving time T_{Bg1}, which is the time between the responder device receiving all of the command and the responder device recognizing the command (e.g., by decoding the command data) and an application of the responder device starting to execute the command over the responder execution time T_B. After the responder execution time T_B, FIG. 2 shows a time delay that is the responder sending time T_{Bg2}, which is the time between the protocol layer of the responder device preparing the response data and the protocol layer beginning to send the response 212 to the command 210. FIG. 2 also shows an initiator sending time T_{Ag2} at the initiator device after the initiator execution time T_A. The initiator sending time T_{Ag2} is the time between the initiator device beginning to receive the response data to the time the response 212 is recognized (e.g., by decoding the response data) by the initiator device. There is also a second communication gap T_C between the time that the responder device starts to send the response 212 and the initiator device starts to receive the response data.

[0017] Because of the delays in signaling times and the delay in recognizing the response 212, the time from sending the command to recognizing the response will appear to be an execution time of $T_A + T_{Ag1} + T_{Ag2}$ to the initiator device. It can be seen in FIG. 2 that an expression for the execution time is

$$T_A + T_{Ag1} + T_{Ag2} = T_B + T_{Bg1} + T_{Bg2} + 2(T_C)\ . \qquad (1)$$

The relationship in Equation (1) is true if T_{Ag1}=T_{Bg1} and T_{Ag2}=T_{Bg2}, or if T_{Ag1}, $T_{Bg1,}$ T_{Ag2}, and T_{Bg2} are small enough to be ignored. Solving for the expected communication time gap T_C yields

$$T_C = \{T_A - (T_B + T_{Bg1} + T_{Bg2} - T_{Ag1} - T_{Ag2})\} / 2\ . \qquad (2)$$

[0018] When there is a relay attack, there will be some non-zero time that the command and response pass through the attacking device or devices. The additional devices will add communication gaps T_C to the transmitting and receiving of the command and response. In a perfect relay attack, the attacking device or devices will be as efficient as possible.

[0019] FIG. 3 is a timing diagram representing a command 310 sent by an initiator device, relayed by two attacking devices (ATTACKER 1, ATTACKER 2) in a relay attack, and then received by a responder device. The attacking devices add a communication gap T_C to the sending of the command 310 by the initiator device and the receiving of the command 310 by the responder device. There is also a communication gap T_{CA} between the attacking devices. The communication gap T_{CA} between the attacking devices may be less than the communication T_C. The communication between the attacking devices can be very efficient because the attacking devices can use any proprietary communication protocol. The communication gap T_{CA} is added to the sending of the command 310 by the initiator device and the receiving of the command 310 by the responder device.

[0020] The attacking devices also add the T_C and T_{CA} communication gaps to the sending of the response 312 by the responder device and the receiving of the response 312 by the initiator device. The total time from when the initiator device starts to send the command to when the initiator device recognizes receiving the response 312 to the command is

$$T_A + T_{Ag1} + T_{Ag2} = T_B + T_{Bg1} + T_{Bg2} + 4(T_C) + 2(T_{CA})\ . \qquad (3)$$

[0021] The difference in time between the normal communication and the relay attack communication is $2(T_C) + 2(T_{CA})$. If the communication time gaps are different between directions from initiator to responder and responder to initiator, the time difference may be $(T_{C1} + T_{C2}) + (T_{CA1} + T_{CA2})$. If all the communication time gaps are all the same, the time difference is $4(T_C)$. The difference in communication time for the command 210 and response 212 can be used by the initiator device to detect the relay attack. The initiator device may measure a communication time gap. If the measured communication time gap is greater than a predetermined relay attack detection threshold, then there may be a relay attack.

[0022] To check for a relay attack, the initiator device measures the time from sending the command 210 to receiving the response 212. The responder device sends a value of the responder execution time T_B to the initiator device. In some examples, the initiator device sends a second command to the responder device and the responder device includes the responder execution time T_B in a response to the second command. In some examples, the responder device includes the responder execution time T_B in a response to the first command sent by the initiator device. The processing circuitry of the initiator device uses the received value of the responder execution time and the measured time for sending and receiving the command-response pair to detect a relay attack. For instance, the processing circuitry may calculate a communication time gap between the initiator execution time of $T_A + T_{Ag1} + T_{Ag2}$ and the expected responder response time of $T_B + T_{Bg1} + T_{Bg2}$ and the expected communication gap of $2(T_C)$, or

$$\text{Gap} = (T_A + T_{Ag1} + T_{Ag2}) - (T_B + T_{Bg1} + T_{Bg2} + 2T_C)\ . \quad (4)$$

[0023] If the calculated communication time gap (Gap) is longer than an expected time difference the initiator device may interpret the increase in communication time as a relay attack and take some action, such as denying the access requested, sending an alert message or alert signal to another device in the access control system, suspending communication for a predetermined period of time, etc.

[0024] FIG. 4 is a flow diagram of an example of a method 400 of operating an access control system. At block 405, a command is transmitted from an initiator device of the access control system to a responder device. The initiator device may be a verifier device of the access control system (e.g., a reader device 102 in FIG. 1) and the responder device may be a credential device (e.g., credential device 104 in FIG. 1). The command may be transmitted wirelessly to the responder device according to a wireless communication protocol (e.g., the Bluetooth® protocol) using physical layer circuitry of the verifier device. The responder device may be a smart credential device (e.g., a smartphone or smartcard) storing access credential information. In variations, the interface between the initiator device and the responder device may be a wired interface, and the measurement command can be transmitted according to a wired communication protocol.

[0025] The initiator device may be an authorization-only device that compares the credential information to credential information that is allowed access, or the initiator device may be a combination authorization and control device that evaluates credential information and provides access through a physical portal (e.g., a door) when the credential information meets the criteria for access. In certain examples, the initiator device may be the credential device, and the responder device is the verifier device of the access control system.

[0026] At block 410, the initiator device determines a time duration from the end of sending the command 210 to the start of receiving the response 212 to the command from the responder device. The command 210 may be a measurement command sent by the initiator device specifically to measure the communication time between the initiator device and the responder device.

[0027] At block 415, the initiator device sends a second command to the responder device and receives a value of the responder execution time (T_B) in the response to the command from the responder device. At block 420, the processing circuitry of the initiator device computes a value of the communication time gap between the devices.

[0028] In some examples, the initiator device stores (e.g., in a memory) an expected value for the normal communication time gap. The expected value may be determined from previous measurements and programmed into the initiator device. The processing circuitry of the initiator device may compare the computed communication time gap to the stored expected time. If attacker devices are relaying the command, the computed communication time gap will be longer than the expected time gap, and the initiator device will detect the relay attack.

[0029] According to some embodiments, the processing circuitry of the initiator device computes the difference between the initiator execution time and the responder execution time, and detects a relay attack when the time difference is longer than a predetermined threshold time difference. In certain examples, the time returned by the responder device includes the actual responder execution time (T_B), the responder receiving time (T_{Bg1}), and the responder sending time (T_{Bg2}). The time measured by the initiator device includes the actual initiator execution time (T_B), the initiator sending time (T_{Ag1}), and the initiator receiving time (T_{Ag2}). The time difference computed by the processing circuitry of the initiator device may be the computed communication time gap (Gap) in Equation (4) described previously herein. If the computed time difference is more than a threshold time (e.g., Gap > (T_{Ag1} + T_{Ag2} + threshold)), then the initiator device detects a relay attack.

[0030] At block 425, the processing circuitry of the initiator device generates an indication when the initiator device detects relay attack. The indication may be a signal sent to alarm circuitry of the initiator device or alarm circuitry of a separate device (e.g., an access controller 106 in FIG. 1). In variations, the indication may be a predetermined message transmitted from the verifier device to the separate device. The command 210 may be recurrently transmitted, and the response to the command measured to recurrently check for a relay attack. One or both of the initiator device and the responder device may measure or compute any of the time durations described for the command and use the determined time to detect a relay attack.

[0031] The comparison of the timing measurements is used to decide whether the command 210 is relayed. The timing measurement values may be based on the type of responder device. The behavior of a hardware platform of a responder device may result in using different comparison algorithms. For example, when a command is received on the responder device for some platforms, it is not guaranteed it will be immediately executed. In another example, when a command is executed on the responder device it is not guaranteed that the response will be immediately sent.

[0032] Any communication mechanism that is not restarted or repeated can be used for the command and used in the timing measurements. Conversely, communication mechanism that are restarted or repeated should not be used. This includes error correction (e.g., error correction coding or ECC). If the measurement command includes multiple frames, error correction should be omitted from the first frame of the multi-frame message. Error correction on the first frame may add an additional gap between both timing measurements that can lead to a wrong relay detection. Error correction on the other frames would not cause an incorrect detection using the multi-frame command-response pair.

[0033] The systems, devices, and methods described herein provide a reliable way to detect a relay attack between two devices. Timing measurements for the attack detection are determined and may be shared between the initiator device and the responder device.

[0034] FIG. 5 is a block diagram schematic of various example components of a device 500 (e.g., an embedded device) for supporting the device architectures described and illustrated herein. The device 500 of FIG. 5 could be, for example, a verifier or reader device that authenticates credential information of authority, status, rights, and/or entitlement to privileges for the holder of a credential device. At a basic level, a reader device can include an interface (e.g., one or more antennas and Integrated Circuit (IC) chip(s)), which permit the reader device to exchange data with another device, such as a credential device or another verifier device. One example of credential device is an RFID smartcard that has data stored thereon allowing a holder of the credential device to access a secure area or asset protected by the reader device.

[0035] With reference specifically to FIG. 5, additional examples of a device 500 for supporting the device architecture described and illustrated herein may generally include one or more of a memory 502, a processor 504, one or more antennas 506, a communication port or communication module 508, a network interface device 510, a user interface 512, and a power source 514 or power supply.

[0036] Memory 502 can be used in connection with the execution of application programming or instructions by processing circuitry, and for the temporary or long-term storage of program instructions or instruction sets 516 and/or authorization data 518, such as credential data, credential authorization data, or access control data or instructions, as well as any data, data structures, and/or computer-executable instructions needed or desired to support the above-described device architecture. For example, memory 502 can contain executable instructions 516 that are used by a processor 504 of the processing circuitry to run other components of device 500, to make access determinations based on credential or authorization data 518, and/or to perform any of the functions or operations described herein, such as the method of FIG. 4 for example. Memory 502 can comprise a computer readable medium that can be any medium that can contain, store, communicate, or transport data, program code, or instructions for use by or in connection with device 500. The computer readable medium can be, for example but is not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device. More specific examples of suitable computer readable medium include, but are not limited to, an electrical connection having one or more wires or a tangible storage medium such as a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), Dynamic

RAM (DRAM), any solid-state storage device, in general, a compact disc read-only memory (CD-ROM), or other optical or magnetic storage device. Computer-readable media includes, but is not to be confused with, computer-readable storage medium, which is intended to cover all physical, non-transitory, or similar embodiments of computer-readable media.

[0037] Processor 504 can correspond to one or more computer processing devices or resources. For instance, processor 504 can be provided as silicon, as a Field Programmable Gate Array (FPGA), an Application-Specific Integrated Circuit (ASIC), any other type of Integrated Circuit (IC) chip, a collection of IC chips, or the like. As a more specific example, processor 504 can be provided as a microprocessor, Central Processing Unit (CPU), or plurality of microprocessors or CPUs that are configured to execute instructions sets stored in an internal memory 520 and/or memory 502.

[0038] Antenna 506 can correspond to one or multiple antennas and can be configured to provide for wireless communications between device 500 and another device. Antenna(s) 506 can be coupled to one or more physical (PHY) layers 524 to operate using one or more wireless communication protocols and operating frequencies including, but not limited to, the IEEE 802.15.1, Bluetooth, Bluetooth Low Energy (BLE), near field communications (NFC), ZigBee, GSM, CDMA, Wi-Fi, RF, UWB, and the like. Processor 504 may implement a MAC layer that forms a protocol layer with a physical layer 524. In an example, antenna 506 may include one or more antennas coupled to one or more physical layers 524 to operate using ultra-wide band (UWB) for in band activity/communication and Bluetooth (e.g., BLE) for out-of-band (OOB) activity/communication. However, any RFID or personal area network (PAN) technologies, such as the IEEE 502.15.1, near field communications (NFC), ZigBee, GSM, CDMA, Wi-Fi, etc., may alternatively or additionally be used for the OOB activity/communication described herein.

[0039] Device 500 may additionally include a communication module 508 and/or network interface device 510. Communication module 508 can be configured to communicate according to any suitable communications protocol with one or more different systems or devices either remote or local to device 500. Network interface device 510 includes hardware to facilitate communications with other devices over a communication network utilizing any one of a number of transfer protocols (e.g., frame relay, internet protocol (IP), transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), etc.). Example communication networks can include a local area network (LAN), a wide area network (WAN), a packet data network (e.g., the Internet), mobile telephone networks (e.g., cellular networks), Plain Old Telephone (POTS) networks, wireless data networks (e.g., IEEE 802.11 family of standards known as Wi-Fi, IEEE 802.16 family of standards known as WiMax), IEEE 802.15.4 family of standards, and peer-to-peer (P2P) networks, among others. In some examples, network interface device 510 can include an Ethernet port or other physical jack, a Wi-Fi card, a Network Interface Card (NIC), a cellular interface (e.g., antenna, filters, and associated circuitry), or the like. In some examples, network interface device 510 can include a plurality of antennas to wirelessly communicate using at least one of single-input multiple-output (SIMO), multiple-input multiple-output (MIMO), or multiple-input single-output (MISO) techniques. In some example embodiments, one or more of the antennas 506, communication module 508, and/or network interface device 510 or subcomponents thereof, may be integrated as a single module or device, function or operate as if they were a single module or device, or may comprise of elements that are shared between them.

[0040] User interface 512 can include one or more input devices and/or display devices. Examples of suitable user input devices that can be included in user interface 512 include, without limitation, one or more buttons, a keyboard, a mouse, a touch-sensitive surface, a stylus, a camera, a microphone, etc. Examples of suitable user output devices that can be included in user interface 512 include, without limitation, one or more LEDs, an LCD panel, a display screen, a touchscreen, one or more lights, a speaker, etc. It should be appreciated that user interface 512 can also include a combined user input and user output device, such as a touch-sensitive display or the like. The user interface 512 may include a separate alarm circuit 526 to indicate an alarm condition such as a relay attack or other security breach. Alarm circuit 526 may provide an audio signal to a speaker or may activate a light or present an alarm condition using a display device.

[0041] Power source 514 can be any suitable internal power source, such as a battery, capacitive power source or similar type of charge-storage device, etc., and/or can include one or more power conversion circuits suitable to convert external power into suitable power (e.g., conversion of externally-supplied AC power into DC power) for components of the device 500.

[0042] Device 500 can also include one or more interlinks or buses 522 operable to transmit communications between the various hardware components of the device. A system bus 522 can be any of several types of commercially available bus structures or bus architectures.

ADDITIONAL DISCLOSURE AND EXAMPLES

[0043] Example 1 includes subject matter (such as an initiator device of an access control system) comprising protocol layer circuitry and processing circuitry operatively coupled to the protocol layer circuitry. The processing circuitry is configured to initiate transmission of a command to a responder device, determine a first time measurement of a time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device, receive a response from the responder device that includes a second time measurement of a responder execution time of the command by the responder device, and generate an indication when the first time measurement and second time measurement indicate a relay attack.

[0044] In Example 2, the subject matter of Example 1 optionally includes processing circuitry configured to compute a time difference between the first time measurement and the second time measurement, compare the computed time difference to a specified relay attack detection time gap, and generate the indication when the computed time difference exceeds the relay attack detection time gap.

[0045] In Example 3, the subject matter of one or both of Examples 1 and 2 optionally includes processing circuitry configured to initiate transmission of a second command to the responder device, receive the second time measurement in a response to the second command, compute a time difference between the first time measurement and the second time measurement, and determine whether the time duration indicates a relay attack using the computed time difference.

[0046] In Example 4, the subject matter of one or any combination of Examples 1-3 optionally includes processing circuitry configured to compute a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device, compare the computed communication time gap to a specified relay attack detection time gap, and generate the indication when the computed communication time gap exceeds the specified relay attack detection time gap.

[0047] In Example 5, the subject matter of one or any combination of Examples 1-4 optionally includes processing circuitry configured to compute the first time measurement to include an initiator execution time of the command, an initiator sending time that is a time duration between the protocol layer of the initiator device signaling that the command is sent and a last byte of the command sent by the protocol layer of the initiator device, and an initiator receiving time that is a time after the initiator execution time that the response to the command is recognized; compute a second time duration that includes the responder execution time, a responder receiving time that is a time duration for the responder to recognize the command, and a responder sending time that is a time duration between a protocol layer of the responder device signaling that the response is sent and a last byte of the response sent by the protocol layer of the responder device; compute a time difference between the first time measurement and the second time duration; and generate the indication when the computed time difference indicates a relay attack.

[0048] In Example 6, the subject matter of one or any combination of Examples 1-5 optionally includes processing circuitry configured to initiate transmission of a multi-frame measurement command to the responder device, and determine the time duration as a time from an end of transmitting the multi-frame command to a start of receiving a response to the multi-frame command from the responder device.

[0049] In Example 7, the subject matter of one or any combination of Examples 1-6 optionally includes protocol layer circuitry configured to receive a response to the command from a responder device that is a smart card.

[0050] In Example 8, the subject matter of one or any combination of Examples 1-6 optionally includes protocol layer circuitry configured to receive a response to the command from a responder device that is a smart phone.

[0051] Example 9 include subject matter (such as a method of operating an access control system) or can optionally be combined with one or any combination of Examples 1-8 to include such subject matter; comprising transmitting a command from an initiator device of the access control system to a responder device, determining; using the initiator device, a first time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device; receiving, by the initiator device from the responder device, a responder execution time of a time duration for the responder device to execute the command; generating, using the initiator device, an indication of a relay attack using the first time duration and the responder execution time.

[0052] In Example 10, the subject matter of Example 9 optionally includes computing, by the initiator device, a time difference between the first time duration and the responder execution time; comparing the computed time difference to a specified relay attack detection time gap; and generating the indication of the relay attack when the computed time difference exceeds the relay attack detection time gap.

[0053] In Example 11, the subject matter of one or both of Examples 9 and 10 optionally includes receiving, by the initiator device from the responder device, the responder execution time in response to a following command sent by the initiator device; and using the computed time difference to determine whether the time duration indicates a relay attack.

[0054] In Example 12, the subject matter of Example 11 optionally includes computing, by the initiator device, a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device using the first time duration and the responder execution time; comparing the computed communication time gap to a specified relay attack detection time gap; and generating the indication of the relay attack when the computed communication time gap exceeds the specified relay attack detection time gap.

[0055] In Example 13, the subject matter of one or any combination of Examples 9-12 optionally includes computing, by the initiator device, the first time duration to include an initiator execution time of the command, an initiator sending time that is a time duration between a protocol layer of the initiator device signaling that the command is sent and a last byte of the command sent by the protocol layer of the initiator device, and an initiator receiving time that is a time after the initiator execution time that the response to the command is recognized, a second time duration including the responder execution time, a responder receiving time that is a time duration for the responder to recognize the command, and a responder sending time that is a time duration between a protocol layer of the responder device signaling that the response is sent and a last byte of the response sent by the protocol layer of the responder device, and a difference between the first time duration and the second time duration. The initiator device uses the computed difference to determine whether the time duration indicates a relay attack.

[0056] In Example 14, the subject matter of one or any combination of Examples 9-14 optionally includes detecting, by the responder device, that the command is a multi-frame measurement command; omitting, by the responder device, error correction on the first frame of the multi-frame message; and wherein the determining the time duration includes the initiator device determining a time duration from an end of transmitting the multi-frame command by the initiator device to a start of receiving a response to the multi-frame command from the responder device.

[0057] In Example 15 the subject matter of one or nay combination of Examples 9-14 optionally includes the initiator device being a reader device and the responder device being a smart card.

[0058] In Example 16, the subject matter of one or nay combination of Examples 9-14 optionally includes the initiator device being a verifier device and the responder device being a smart phone.

[0059] Example 17 includes subject matter (or can optionally be combined with one or any combination of Examples 1-16 to include such subject matter) comprising a computer-readable storage medium including instructions that, when executed by processing circuitry of an initiator device of an access control system, cause the initiator device to perform acts including transmitting a command to a responder device, determining a time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device, receiving a responder execution time of a time duration for the responder device to execute the command, and generating an indication of a relay attack using the time duration and the responder execution time.

[0060] In Example 18, the subject matter of Example 17 optionally includes the computer-readable storage medium including instructions that cause the initiator device to perform acts including comparing the computed time difference to a specified relay attack detection time gap, and generating the indication when the computed time difference exceeds the relay attack detection time gap.

[0061] In Example 19, the subject matter of one or both of Example 17 and 18 optionally includes the computer-readable storage medium including instructions that cause the initiator device to perform acts including sending a following command to the responder device, receiving the responder execution from the responder service in a response to the following command, computing a time difference between the time duration and the responder execution time, and determining whether the time duration indicates a relay attack using the computed time difference.

[0062] In Example 20, the subject matter of one or any combination of Examples 17-19 optionally includes the computer-readable storage medium including instructions that cause the initiator device to perform acts including computing a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device, comparing the computed communication time gap to a specified relay attack detection time gap, and generating the indication of the relay attack when the computed communication time gap exceeds the specified relay attack detection time gap.

[0063] These non-limiting Examples can be combined in any permutation or combination. The above detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show, by way of illustration, specific embodiments in which the invention can be practiced. The above description is intended to be illustrative, and not restrictive. For example, the above-described examples (or one or more aspects thereof) may be used in combination with each other. Other embodiments can be used, such as by one of ordinary skill in the art upon reviewing the above description. The Abstract 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 the above Detailed Description, various features may be grouped together to streamline the disclosure. This should not be interpreted as intending that an unclaimed disclosed feature is essential to any claim. Rather, the subject matter may lie in less than all features of a particular disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment, and it is contemplated that such embodiments can be combined with each other in various combinations or permutations. The scope should be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

WHAT IS CLAIMED IS:

1. An initiator device of an access control system, the device comprising:

protocol layer circuitry; and

processing circuitry operatively coupled to the protocol layer circuitry and configured to:

initiate transmission of a command to a responder device;

determine a first time measurement of a time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device;

receive a response from the responder device that includes a second time measurement of a responder execution time of the command by the responder device; and

generate an indication when the first time measurement and second time measurement indicate a relay attack.

2. The initiator device of claim 1, wherein processing circuitry is configured to:

compute a time difference between the first time measurement and the second time measurement;

compare the computed time difference to a specified relay attack detection time gap; and

generate the indication when the computed time difference exceeds the relay attack detection time gap.

3. The initiator device of claim 1, wherein processing circuitry is configured to:

initiate transmission of a second command to the responder device;

receive the second time measurement in a response to the second command;

compute a time difference between the first time measurement and the second time measurement; and

determine whether the time duration indicates a relay attack using the computed time difference.

4. The initiator device of claim 1, wherein processing circuitry is configured to:

compute a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device;

compare the computed communication time gap to a specified relay attack detection time gap; and

generate the indication when the computed communication time gap exceeds the specified relay attack detection time gap.

5. The initiator device of claim 1, wherein processing circuitry is configured to:

compute the first time measurement to include an initiator execution time of the command, an initiator sending time that is a time duration between the protocol layer of the initiator device signaling that the command is sent and a last byte of the command sent by the protocol layer of the initiator device, and an initiator receiving time that is a time after the initiator execution time that the response to the command is recognized;

compute a second time duration that includes the responder execution time, a responder receiving time that is a time duration for the responder to recognize the command, and a responder sending time that is a time duration between a protocol layer of the responder device signaling that the response is sent and a last byte of the response sent by the protocol layer of the responder device;

compute a time difference between the first time measurement and the second time duration; and

generate the indication when the computed time difference indicates a relay attack.

6. The initiator device of claim 1, wherein processing circuitry is configured to:

initiate transmission of a multi-frame measurement command to the responder device; and

determine the time duration as a time from an end of transmitting the multi-frame command to a start of receiving a response to the multi-frame command from the responder device.

7. The initiator device of any one of claims 1-6, wherein the protocol layer circuitry is configured to receive a response to the command from a responder device that is a smart card.

8. The initiator device of any one of claims 1-6, wherein the protocol layer circuitry is configured to receive a response to the command from a responder device that is a smart phone.

9. A method of operating an access control system, the method comprising:

transmitting a command from an initiator device of the access control system to a responder device;

determining, using the initiator device, a first time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device;

receiving, by the initiator device from the responder device, a responder execution time of a time duration for the responder device to execute the command; and

generating, using the initiator device, an indication of a relay attack using the first time duration and the responder execution time.

10. The method of claim 9, including:

computing, by the initiator device, a time difference between the first time duration and the responder execution time;

comparing the computed time difference to a specified relay attack detection time gap; and

generating the indication of the relay attack when the computed time difference exceeds the relay attack detection time gap.

11. The method of claim 9, including:

receiving, by the initiator device from the responder device, the responder execution time in response to a following command sent by the initiator device; and

using the computed time difference to determine whether the time duration indicates a relay attack.

12. The method of claim 11, including:

computing, by the initiator device, a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device using the first time duration and the responder execution time;

comparing the computed communication time gap to a specified relay attack detection time gap; and

generating the indication of the relay attack when the computed communication time gap exceeds the specified relay attack detection time gap.

13. The method of claim 9, including:

computing, by the initiator device:

the first time duration to include an initiator execution time of the command, an initiator sending time that is a time duration between a protocol layer of the initiator device signaling that the command is sent and a last byte of the command sent by the protocol layer of the initiator device, and an initiator receiving time that is a time after the initiator execution time that the response to the command is recognized;

a second time duration including the responder execution time, a responder receiving time that is a time duration for the responder to recognize the command, and a responder sending time that is a time duration between a protocol layer of the responder device signaling that the response is sent and a last byte of the response sent by the protocol layer of the responder device; and

a difference between the first time duration and the second time duration; and

using, by the initiator device, the computed difference to determine whether the time duration indicates a relay attack.

14. The method of claim 9,

detecting, by the responder device, that the command is a multi-frame measurement command;

omitting, by the responder device, error correction on the first frame of the multi-frame message; and

wherein the determining the time duration includes the initiator device determining a time duration from an end of transmitting the multi-frame command by the initiator device to a start of receiving a response to the multi-frame command from the responder device.

15. The method of any one of claims 9-14, wherein the initiator device is a reader device and the responder device is a smart card.

16. The method of any one of claims 9-14, wherein the initiator device is a verifier device and the responder device is a smart phone.

17. A computer-readable storage medium including instructions that, when executed by processing circuitry of an initiator device of an access control system, cause the initiator device to perform acts comprising:

transmitting a command to a responder device;

determining a time duration from an end of sending the command to the responder device to a start of receiving a response to the command from the responder device;

receiving a responder execution time of a time duration for the responder device to execute the command; and

generating an indication of a relay attack using the time duration and the responder execution time.

18. The computer-readable storage medium of claim 17, including instructions that cause the initiator device to perform acts including:

computing a time difference between the time duration and the responder execution time;

comparing the computed time difference to a specified relay attack detection time gap; and

generating the indication when the computed time difference exceeds the relay attack detection time gap.

19. The computer-readable storage medium of claim 17, including instructions that cause the initiator device to perform acts including:

sending a following command to the responder device;

receiving the responder execution from the responder service in a response to the following command;

computing a time difference between the time duration and the responder execution time; and

determining whether the time duration indicates a relay attack using the computed time difference.

20. The computer-readable storage medium of any one of claims claim 17-19, including instructions that cause the initiator device to perform acts including:

computing a communication time gap between a time the command is sent by the initiator device to a time the command is received by the responder device;

comparing the computed communication time gap to a specified relay attack detection time gap; and

generating the indication of the relay attack when the computed communication time gap exceeds the specified relay attack detection time gap.

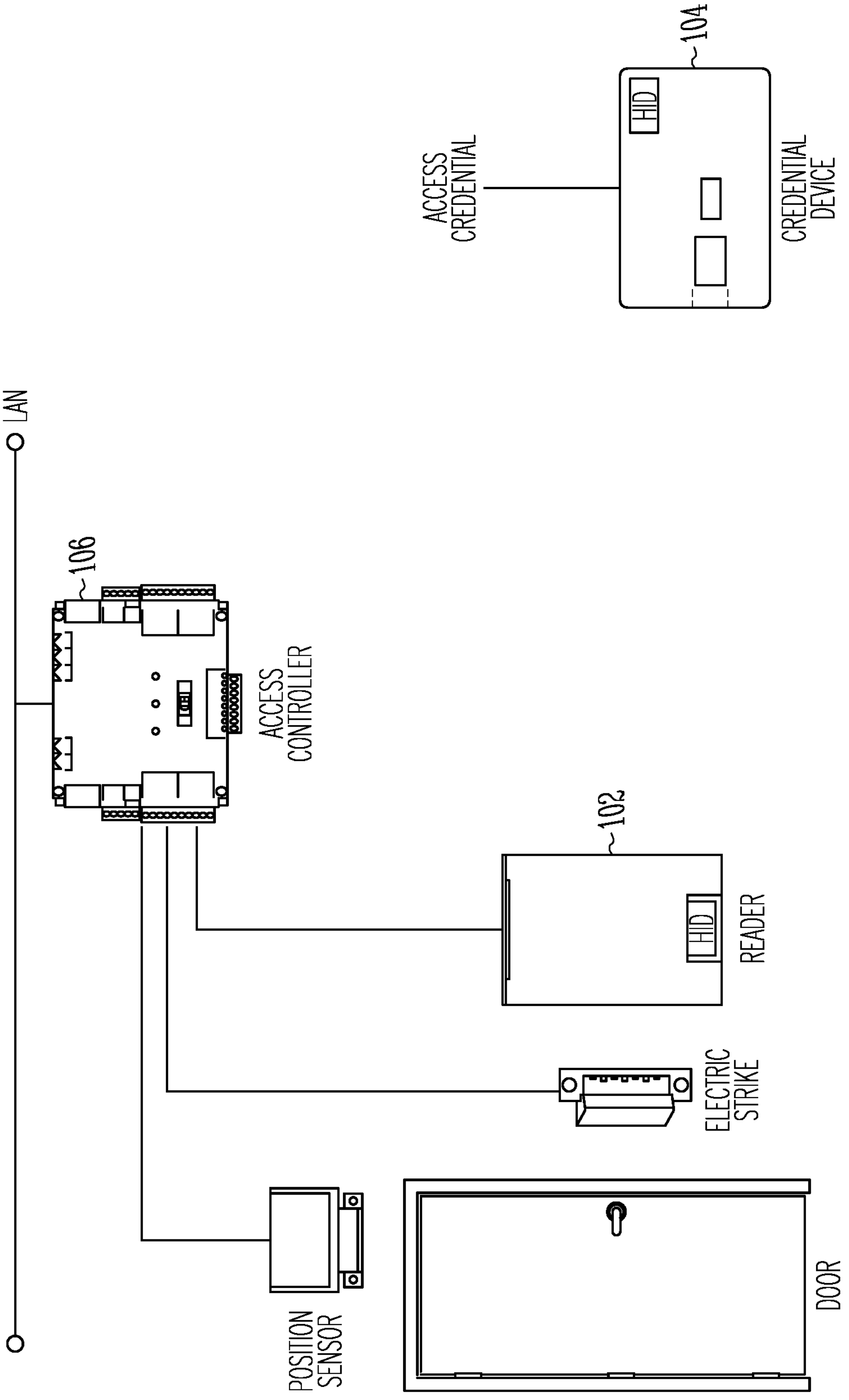
LAN
106
ACCESS CONTROLLER
102
HID
READER
ELECTRIC STRIKE
POSITION SENSOR
DOOR
ACCESS CREDENTIAL
104
HID
CREDENTIAL DEVICE

Fig. 1

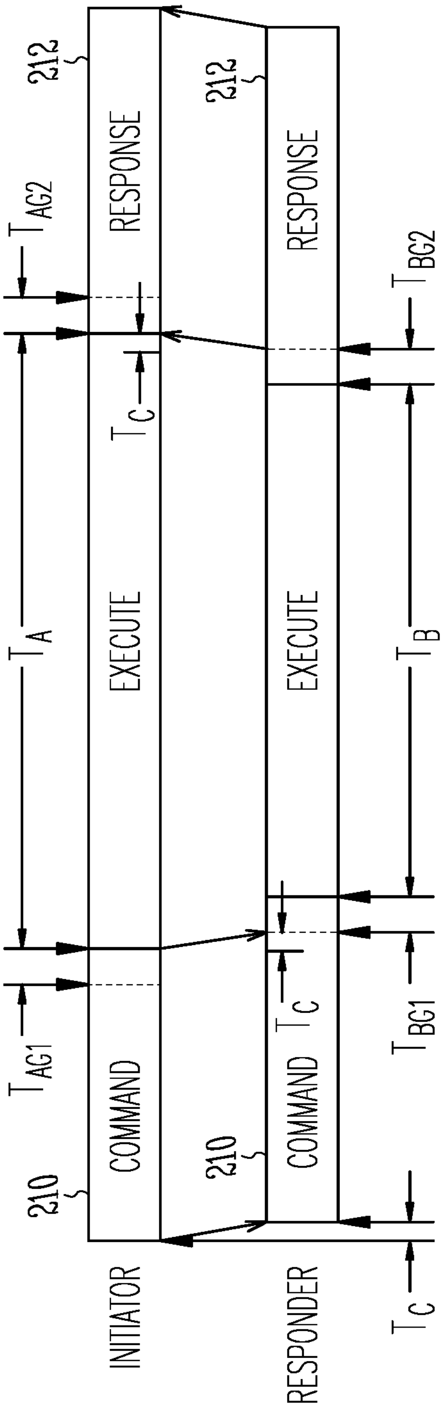
INITIATOR
RESPONDER
210
210
COMMAND
COMMAND
EXECUTE
EXECUTE
RESPONSE
RESPONSE
212
212
T_{AG1}
T_A
T_{AG2}
T_C
T_C
T_C
T_{BG1}
T_B
T_{BG2}

Fig.2

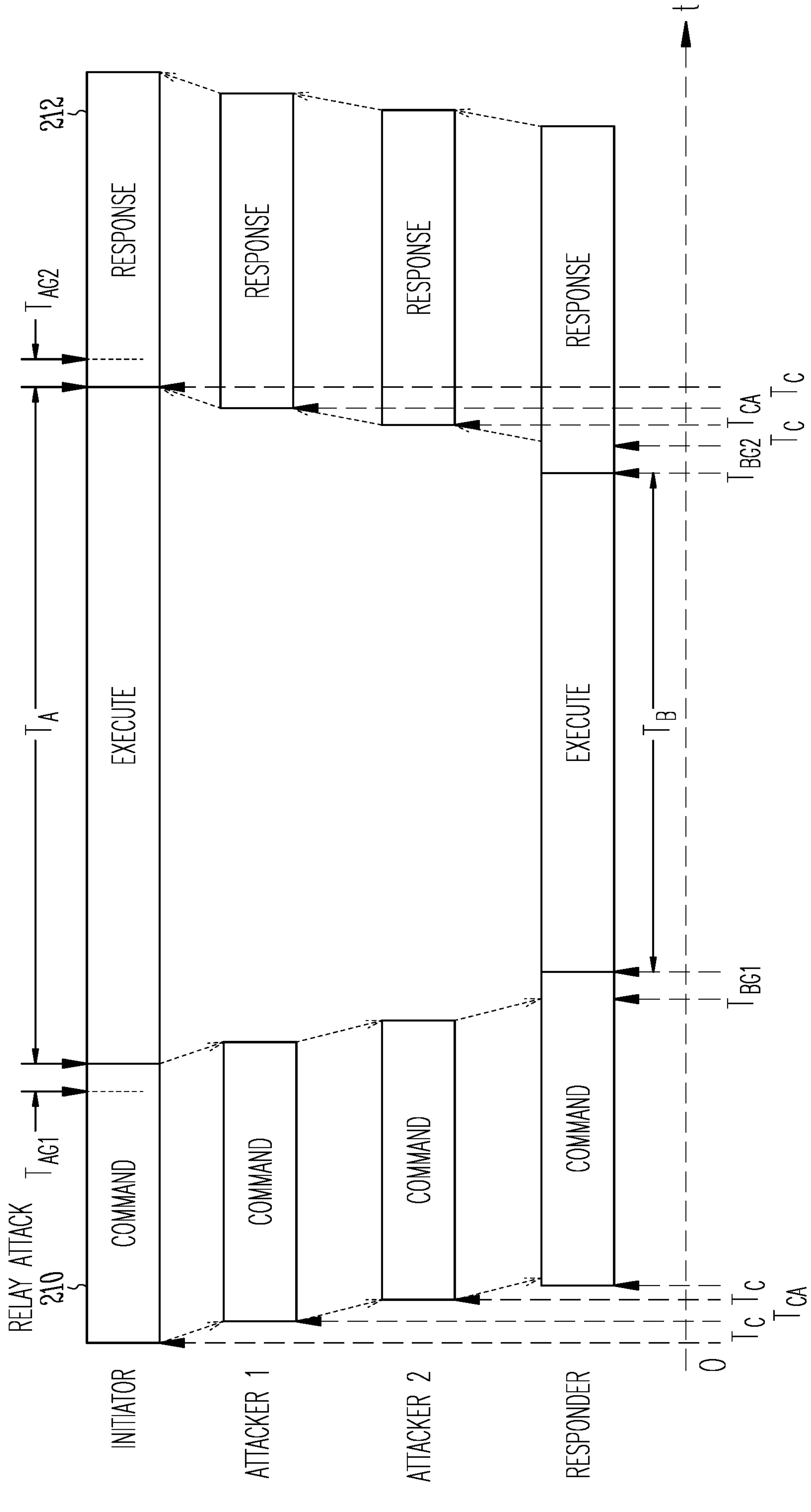
RELAY ATTACK
210
212
INITIATOR
ATTACKER 1
ATTACKER 2
RESPONDER
COMMAND
EXECUTE
RESPONSE
COMMAND
RESPONSE
COMMAND
RESPONSE
COMMAND
EXECUTE
RESPONSE
T_{AG1}
T_A
T_{AG2}
T_B
T_{BG1}
T_{BG2}
T_C
T_{CA}
T_C
T_C
T_{CA}
T_C
T_C
T_C
0
t

Fig. 3

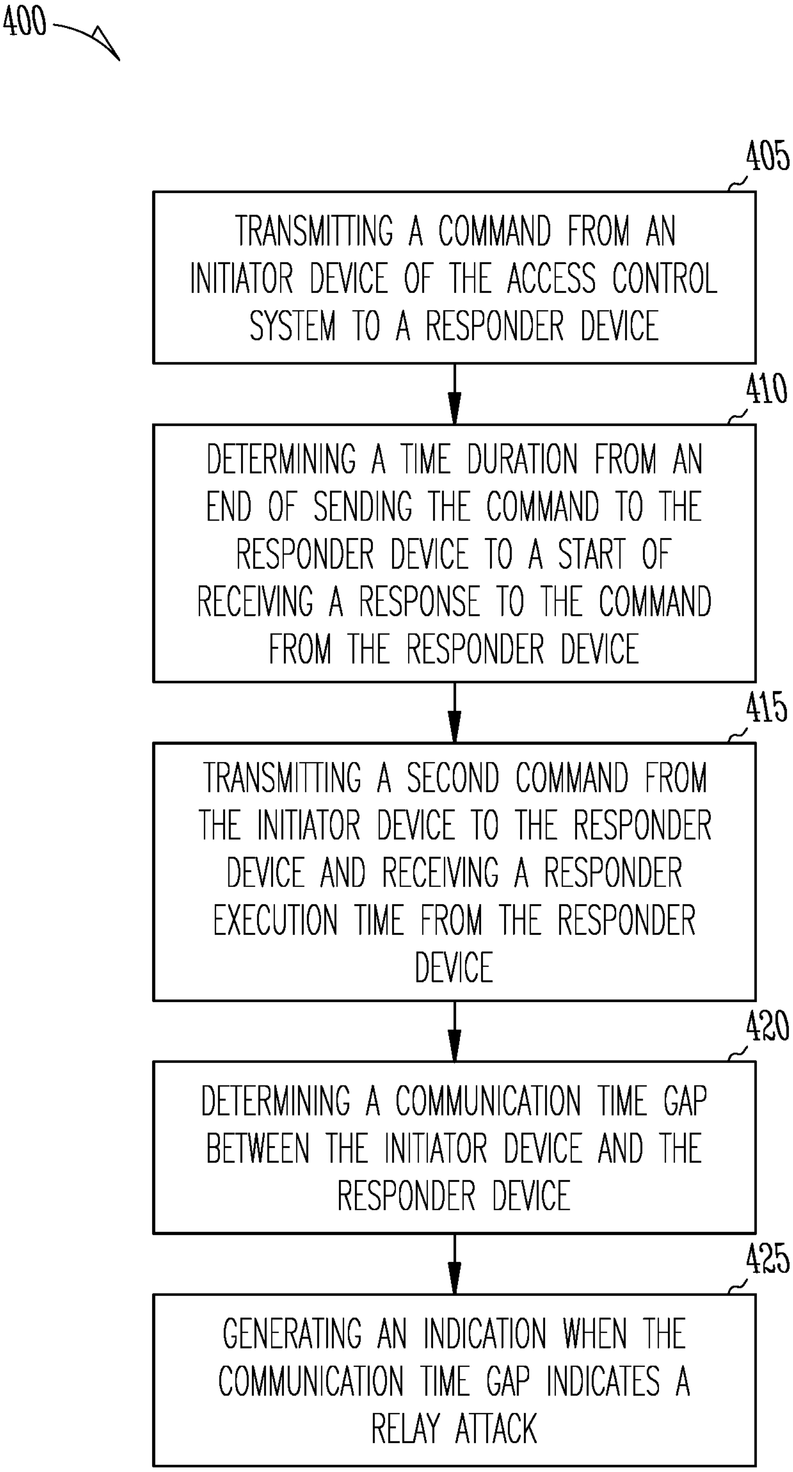
400
405
TRANSMITTING A COMMAND FROM AN INITIATOR DEVICE OF THE ACCESS CONTROL SYSTEM TO A RESPONDER DEVICE
410
DETERMINING A TIME DURATION FROM AN END OF SENDING THE COMMAND TO THE RESPONDER DEVICE TO A START OF RECEIVING A RESPONSE TO THE COMMAND FROM THE RESPONDER DEVICE
415
TRANSMITTING A SECOND COMMAND FROM THE INITIATOR DEVICE TO THE RESPONDER DEVICE AND RECEIVING A RESPONDER EXECUTION TIME FROM THE RESPONDER DEVICE
420
DETERMINING A COMMUNICATION TIME GAP BETWEEN THE INITIATOR DEVICE AND THE RESPONDER DEVICE
425
GENERATING AN INDICATION WHEN THE COMMUNICATION TIME GAP INDICATES A RELAY ATTACK

Fig.4

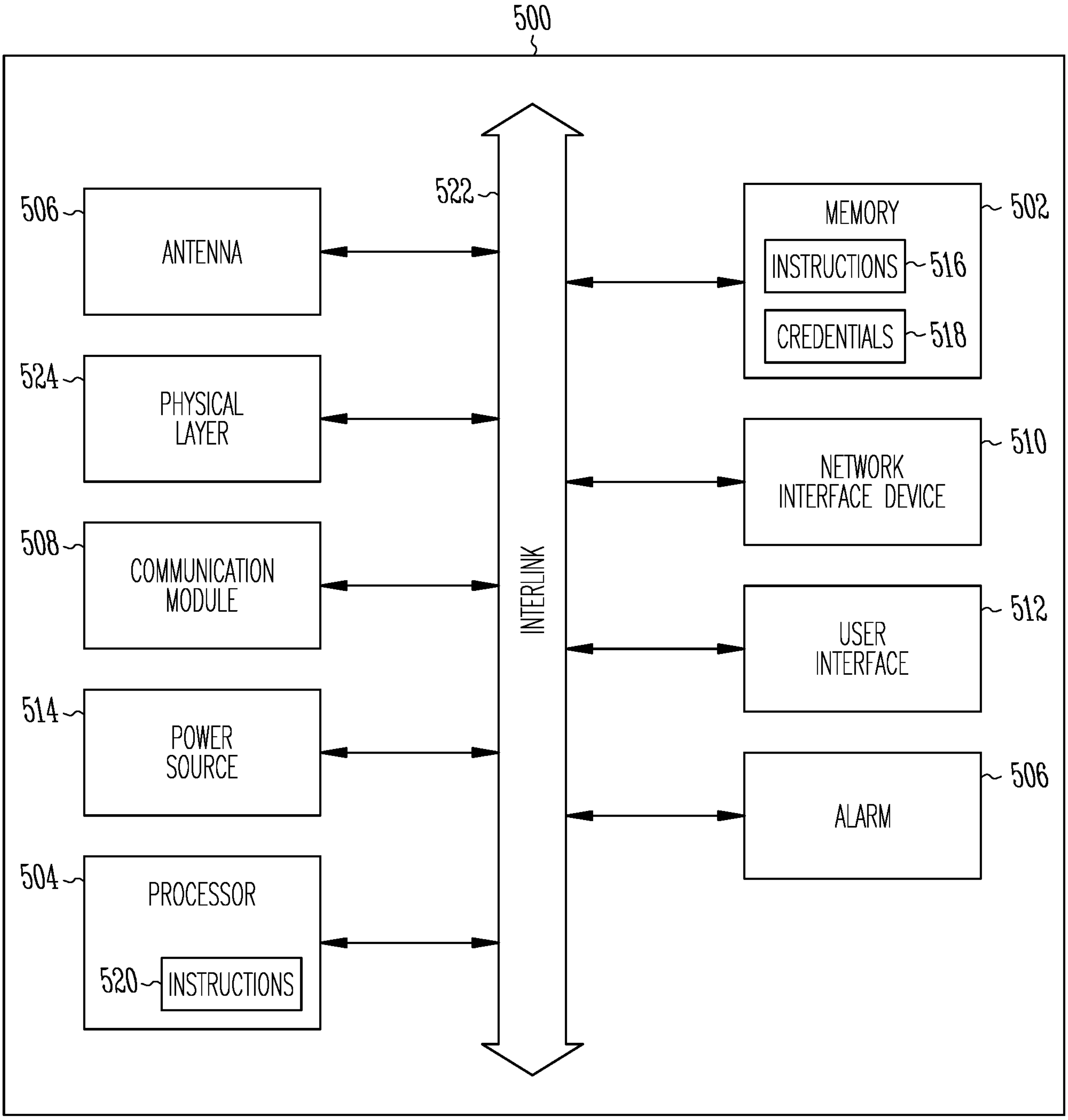
500
506
ANTENNA
522
INTERLINK
MEMORY
INSTRUCTIONS
516
CREDENTIALS
518
502
524
PHYSICAL LAYER
NETWORK INTERFACE DEVICE
510
508
COMMUNICATION MODULE
USER INTERFACE
512
514
POWER SOURCE
ALARM
506
504
PROCESSOR
520
INSTRUCTIONS

Fig.5

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2023/075281

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/00 H04L9/40

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)

G07C 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	US 11 449 691 B2 (ASSA ABLOY AB [SE]) 20 September 2022 (2022-09-20) abstract column 2, line 46 - column 7, line 62; figures 2,3 -----	1-20
A	US 2023/224709 A1 (LERCH MATTHIAS [US] ET AL) 13 July 2023 (2023-07-13) paragraph [0002] - paragraph [0012] -----	1-20

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 6 March 2024	Date of mailing of the international search report 18/03/2024
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 Raposo Pires, João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2023/075281

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 11449691 B2	20-09-2022	CN 116171556 A	26-05-2023
		EP 4200726 A1	28-06-2023
		JP 2023538095 A	06-09-2023
		KR 20230070216 A	22-05-2023
		US 2022058353 A1	24-02-2022
		US 2022414355 A1	29-12-2022
		WO 2022037817 A1	24-02-2022
US 2023224709 A1	13-07-2023	NONE	