

SYSTEMS AND METHODS FOR TWO-FACTOR AUTHENTICATION

Field of the Disclosure

[0001] The present disclosure relates to systems and methods for user authentication and more specifically relates to systems and methods for authenticating users using two-factor authentication.

Background

[0002] The approaches described in this section could be pursued, but are not necessarily approaches that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, the approaches described in this section are not prior art to the claims in this application and are not admitted to be prior art by inclusion in this section.

[0003] Two-factor authentication (2FA) is commonly used for logins and online transactions. 2FA requires a user to provide two separate pieces of evidence to the authentication mechanism. The first factor is typically a knowledge factor, such as a password or a PIN. The second factor is typically a possession factor, where hardware tokens (e.g., ID cards, wireless tags, and USB tokens) or software tokens (e.g., mobile phones) serves as "something that the user possesses." In recent years, software tokens are becoming more popular due to the use of mobile phones.

[0004] However, the various hardware and software tokens are cumbersome to use and require users to carry specialized devices. Similarly, software tokens increase cognitive burdens by forcing the users to remember One-Time Passwords (OTP), which increase the difficulty of adopting 2FA. The existing methods of implementing 2FA also incur significant costs for the service providers, both in terms of costs of devices and data costs. Furthermore, these methods are vulnerable to attacks by malicious actors.

Summary

[0005] Embodiments described herein include a method for two-factor authentication. It should be appreciated that the embodiments can be implemented in numerous ways, such as a process, an apparatus, a system, a device, or a method. Several embodiments are described below.

[0006] In one embodiment, a method of allowing a first device to access a server is disclosed. The method may include an operation to receive a first authentication factor from the first device using the server. The method may further include an operation to authenticate the first authentication factor using the server. The method may also include an operation to automatically authenticate a second authentication factor using the server. The method may include an operation to activate, using the server, recording of a keystroke timing data using the first device and recording of a keystroke typing data using a second device in response to successfully authenticating the first authentication factor. The method may also include an operation to send, using the server, the keystroke timing data from the first device to the second device. The method may include an operation to allow the first device to access the server in response to the server receiving a notification of a successful authentication of the second authentication factor from the second device, wherein the successful notification is generated according to a comparison between the keystroke timing data and the keystroke typing data by the second device.

[0007] In an embodiment, the first authentication factor may include a username and a password. In an embodiment, authenticating the first authentication factor using the server may further include an operation to receive the username and the password from the first device and match the username and the password to an entry in a database implemented on the server. In an embodiment, the first

authentication factor is encrypted.

[0008] In an embodiment, the first device is a computing system. In an embodiment, the method may further include an operation to notify the first device using the server of an authentication error in response to unsuccessfully authenticating the first authentication factor.

[0009] In an embodiment, the keystroke timing data records keystrokes' timestamps based on inputting a randomized code. In an embodiment, the keystroke typing data records signals generated by inputting of the keystrokes on the first device.

[0010] In an embodiment, the signals are audio data signals. In an embodiment, the signals are vibrational signals. In an embodiment, the method may further include an operation to send the randomized code from the first device to the second device using the server. In an embodiment, the method may further include an operation to send an indicator signal from the first device to the second device using the server such that the indicator signal informs the first device to stop recording the keystroke timing data. The indicator signal may also inform the second device to stop recording the keystroke typing data.

[0011] In an embodiment, the second device is implemented on a second device. In an embodiment, the first device is implemented on the second device. In an embodiment, the second device is a computing system. In an embodiment, the second device includes a recording device capable of recording at least one of audio data and vibrational signals.

[0012] In an embodiment, authentication of the second authentication factor further includes an operation to generate a similarity score according to cross-correlating the keystroke timing data and the keystroke typing data using the second device and an operation to compare the similarity score to a pre-determined threshold value.

[0013] In an embodiment, the method may further include an

operation to receive a notification from the second device using the server in response to an unsuccessful authentication of the second authentication factor by the second device in response to the similarity score being lower than the pre-determined threshold. The method may also include an operation to display the random code for approval using the second device. The method may further include an operation to allow the first device to access the server based on approving the displayed random code using the second device.

[0014] In an embodiment, a system for allowing a first device to access a server is disclosed. The system may include the first device communicatively coupled to the server. The system may also include a second device such that the second device is communicatively coupled to the server. The server may receive a first authentication factor from the first device. The server may also authenticate the first authentication factor. The server may further automatically authenticates a second authentication factor by activating recording of a keystroke timing data using the first device and recording of a keystroke typing data using the second device in response to a successful authentication of the first authentication factor. The server may send the keystroke timing data from the first device to the second device such. The first device is allowed access to the server in response to the server receiving a notification of a successful authentication of the second authentication factor from the second device. The successful notification is generated according to a comparison between the keystroke timing data and the keystroke typing data by the second device.

Brief Description of Drawings

[0015] In the drawings:

[0016] FIG. 1 illustrates an exemplary system for implementing 2FA in accordance with an embodiment of the present invention;

[0017] FIG. 2 illustrates an exemplary computer system in accordance with an embodiment of the present invention;

[0018] FIG. 3 illustrates an exemplary system for accessing a server in accordance with an embodiment of the present invention;

[0019] FIG. 4 illustrates an exemplary method for accessing a server in accordance with an embodiment of the present invention;

[0020] FIG. 5 illustrates an exemplary method for authenticating a second authentication factor in accordance with an embodiment of the present invention.

Detailed Description of the Drawings

[0021] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

[0022] In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

[0023] Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to affect the communication.

[0024] Several features are described hereafter that can each be used independently of one another or with any combination of other features. However, any individual feature may not address any of the problems discussed above or might only address one of the problems discussed above. Some of the problems discussed above might not be fully addressed by any of the features described herein.

[0025] FIG. 1 illustrates an exemplary system for implementing 2FA. In FIG. 1, server 104 is communicatively coupled to first device 102 and second device 106. Server 104 may provide various computing services to first device 102 and second device 106. For example, server 104 may be configured to host websites or webpages, or allow access to secure content for example bank accounts, and personal social media accounts.

[0026] Server 104 may be a part of a datacenter with numerous servers. For example, servers in the datacenter may be physically arranged in the datacenter into rooms, groups, rows, and racks. A datacenter may have one or more zones,

which may include one or more rooms of servers. Each room may have one or more rows of servers, and each row may include one or more racks. Each rack may include one or more individual server nodes. Servers in zones, rooms, racks, and/or rows may be arranged into groups based on physical infrastructure requirements of the datacenter facility, which may include power, energy, thermal, heat, and/or other requirements. The data center may have many computing systems distributed through many racks. In an embodiment, server 104 may be similar to the computer system described in FIG. 2.

[0027] First device 102 and second devices 106 may be connected to server 104 through network links and network adapters. In an embodiment, first device 102 and second device 106 may be computing devices, for example servers, desktops, laptops, tablets, and smartphones. In other embodiments, first device 102 may be an Internet of Things (IoT) device, or a smart home security lock, a smart car locking mechanism, or other internet connected security devices. In an embodiment, first device 102 and second device 106 may be similar to the computer system 200 described in FIG. 2. In an embodiment, second device 106 includes a processing circuitry and a recording device. In an embodiment, the recording device may include a microphone, a camera, a gyroscope, an accelerometer, or other specialized device for recording audio or vibrational signals/data.

[0028] In an embodiment, server 104, first device 102, and second device 106 may form a communication network or a part of a communication network. The network represents any combination of one or more local networks, wide area networks, or internetworks coupled using wired or wireless links deployed using terrestrial or satellite connections. Data exchanged over the network, may be transferred using any number of network layer protocols, such as Internet Protocol (IP), Multiprotocol Label Switching (MPLS), Asynchronous

Transfer Mode (ATM), Frame Relay, etc. Furthermore, in embodiments where the network represents a combination of multiple sub-networks, different network layer protocols may be used at each of the underlying sub-networks. In some embodiments, the network may represent one or more interconnected internetworks, such as the public Internet.

[0029] Although only a particular number elements are depicted in FIG. 1, a practical environment may have many more of each depicted element. In addition, the layout of the networking environment described above may change from embodiment to embodiment.

[0030] FIG. 2 illustrates an exemplary computer system in accordance with an embodiment of the present invention. According to one embodiment, the techniques described herein are implemented by one or more special-purpose computing devices. The special-purpose computing devices may be hard-wired to perform the techniques, or may include digital electronic devices such as one or more application-specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs) that are persistently programmed to perform the techniques, or may include one or more general purpose hardware processors programmed to perform the techniques pursuant to program instructions in firmware, memory, other storage, or a combination. Such special-purpose computing devices may also combine custom hard-wired logic, ASICs, or FPGAs with custom programming to accomplish the techniques. The special-purpose computing devices may be desktop computer systems, portable computer systems, handheld devices, network devices or any other device that incorporates hard-wired and/or program logic to implement the techniques.

[0031] Computer system 200 may include a bus 202 or other communication mechanism for communicating information, and a hardware processor 204 coupled with bus 202 for processing information. Hardware processor 204 may be, for example, a

general-purpose microprocessor. In an embodiment, processor 204 may be similar to processing circuitry 102 described above.

[0032] Computer system 200 also includes a main memory 206, such as a random-access memory (RAM) or other dynamic storage device, coupled to bus 202 for storing information and instructions to be executed by processor 204. Main memory 206 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 204. Such instructions, when stored in non-transitory storage media accessible to processor 204, render computer system 200 into a special-purpose machine that is customized to perform the operations specified in the instructions.

[0033] Computer system 200 further includes a read only memory (ROM) 208 or other static storage device coupled to bus 202 for storing static information and instructions for processor 204. A storage device 210, such as a magnetic disk, optical disk, or solid-state drive is provided and coupled to bus 202 for storing information and instructions.

[0034] Computer system 200 may be coupled via bus 202 to a display 212, such as a cathode ray tube (CRT), a liquid crystal display (LCD), plasma display, light emitting diode (LED) display, or an organic light emitting diode (OLED) display for displaying information to a computer user. An input device 214, including alphanumeric and other keys, is coupled to bus 202 for communicating information and command selections to processor 204. Another type of user input device is cursor controller 216, such as a mouse, a trackball, a touch-enabled display, or cursor direction keys for communicating direction information and command selections to processor 204 and for controlling cursor movement on display 212. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y),

that allows the device to specify positions in a plane.

[0035] According to one embodiment, the techniques herein are performed by computer system 200 in response to processor 204 executing one or more sequences of one or more instructions contained in main memory 206. Such instructions may be read into main memory 206 from another storage medium, such as storage device 210. Execution of the sequences of instructions contained in main memory 206 causes processor 204 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions.

[0036] The term "storage media" as used herein refers to any non-transitory media that store data and/or instructions that cause a machine to operate in a specific fashion. Such storage media may comprise non-volatile media and/or volatile media. Non-volatile media includes, for example, optical disks, magnetic disks, or solid-state drives, such as storage device 210. Volatile media includes dynamic memory, such as main memory 206. Common forms of storage media include, for example, a floppy disk, a flexible disk, hard disk, solid-state drive, magnetic tape, or any other magnetic data storage medium, a CD-ROM, any other optical data storage medium, any physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, NV-RAM, or any other memory chip or cartridge.

[0037] Storage media is distinct from but may be used in conjunction with transmission media. Transmission media participates in transferring information between storage media. For example, transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus 202. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

[0038] Various forms of media may be involved in carrying one or

more sequences of one or more instructions to processor 204 for execution. For example, the instructions may initially be carried on a magnetic disk or solid-state drive of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 200 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector can receive the data carried in the infra-red signal and appropriate circuitry can place the data on bus 202. Bus 202 carries the data to main memory 206, from which processor 204 retrieves and executes the instructions. The instructions received by main memory 206 may optionally be stored on storage device 210 either before or after execution by processor 204.

[0039] Computer system 200 also includes a communication interface 218 coupled to bus 202. Communication interface 218 provides a two-way data communication coupling to a network link 220 that is connected to a local network 222. For example, communication interface 218 may be an integrated service digital network (ISDN) card, cable modem, satellite modem, or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 218 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 218 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

[0040] Network link 220 typically provides data communication through one or more networks to other data devices. For example, network link 220 may provide a connection through local network 222 to a host computer 224 or to data equipment

operated by an Internet Service Provider (ISP) 226. ISP 226 in turn provides data communication services through the worldwide packet data communication network now commonly referred to as the "Internet" 228. Local network 222 and Internet 228 both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 220 and through communication interface 218, which carry the digital data to and from computer system 200, are example forms of transmission media. In an embodiment, network 220 may contain or may be a part of cloud 102 described above.

[0041] Computer system 200 can send messages and receive data, including program code, through the network(s), network link 220 and communication interface 218. In an embodiment, computer system 200 may receive code for processing. The received code may be executed by processor 204 as it is received, and/or stored in storage device 210, or other non-volatile storage for later execution.

[0042] FIG. 3 illustrates an exemplary system for accessing a server in accordance with an embodiment of the present invention. For the purposes of illustrating clear examples, FIG. 3 will be discussed in relation to FIG. 1 and FIG. 2.

[0043] Referring now to FIG. 3, computer device 306 is communicatively coupled to server 104. In an embodiment, computer device 306 includes first authentication module 302 and second authentication module 304.

[0044] In an embodiment, computer device 306 may be similar to computer system 200 described in FIG 2. Similarly, computer device 306 may be a laptop, desktop, smartphone, smartwatch, IoT device, smart security device or some other form of personal computer. In an embodiment, computing device 306 may be a specialized device including specialized processing circuitry and a recording device.

[0045] In an embodiment, first authentication module 302 and

second authentication module 304 may be software modules implemented on computer device 302 as parts of an authentication application executing on computer device 306. In another embodiment, first authentication module 302 and second authentication module 304 may be implemented on separate devices each of which is communicatively coupled to server 104. For example, first authentication module 302 may be implemented as an application executing on first device 102 and second authentication module 304 may be implemented as an application executing on second device 106 as described with reference to FIG. 1. Similarly, first authentication module 302 and second authentication module 304 may include network protocols and programs, similar to the protocols described in FIG. 1, to connect with server 104. In an embodiment, first authentication module 302 and second authentication module 304 may share access to some resources of computing device 306, for example display, input device RAM, ROM, processor, and storage among others. However, first authentication module 302 and second authentication module 304 may be walled-off from one another for securing the system. For example, first authentication module 302 and second authentication module 304 may be implemented on separate partitions on the storage of computer device 306. In an embodiment, there is no direct exchange of data between first authentication module 302 and second authentication module 304. Similarly, first authentication module 302 and second authentication module 304 may only exchange data via server 104.

[0046] First authentication module 302 may include a variety of applications to allow a user to access server 104. For example, first authentication module 302 may include a web browser implemented on computing device 306 that allows a user to connect to a website hosted on server 104. In an embodiment, first authentication module 302 may maintain an active network connection with server 104, for example in case

of internet-connected devices. In an embodiment, first authentication module 302 may facilitate authentication of a first authentication factor by receiving the first authentication factor from a user through various input devices of computer device 306. These input devices may be similar to input device 214 described above. They may also include devices like fingerprint scanners, retinal scanners, cameras, voice print scanners, and other biometric scanners. In an embodiment, first authentication module 302 may include specialized programs to accept and transmit a variety of first authentication factors, for example, text, audio, videos, images, and biometric scans.

[0047] Second authentication module 304 may include applications that are suited for recording vibrational and audio data using specialized hardware of computer device 306. For example, second authentication module 304 may include or implement programs to control a microphone, camera, accelerometer, or gyroscope of computing device 306. In an embodiment, the accelerometer or gyroscope may be used in recording vibrational data from computer device 306. In an embodiment, second authentication module 306 may also implement programs that utilize processors or processing circuitry to perform complex statistical analysis.

[0048] FIG. 4 illustrates an exemplary method for accessing a server in accordance with an embodiment of the present invention. For the purposes of illustrating clear examples, FIG. 4 will be discussed in reference to FIGS. 1, 2, and 3.

[0049] Referring now to FIG. 4, in an embodiment, prior to accessing a server according to the method described below a user may need to enroll second device 106 by installing a software token on second device 106. This one-time, first-time enrolment is similar to other well-known software or hardware token enrolments methods defined elsewhere and well known in the art.

[0050] At 400, a user may use first device 102 to connect to a server 104 for accessing secure content. For example, first device 102 may be a laptop that the user points to a web address of a website hosted on server 104 by using a web browser executing on the laptop. Server 104 may control access to the website by requiring 2FA from the user. Similarly, a user may attempt to login to server 104 using first authentication module 302 implemented on computer device 306. For example, a user may try to login in to a banking app on their smartphone. In an embodiment, user may be attempting to unlock an IoT security device. For example, user may be attempting to unlock an Internet-connected smart door locking mechanism with a built-in fingerprint scanner.

[0051] At step 402, server 104 receives a first authentication factor from first device 102. In an embodiment, the first authentication factor may be communicated to server 104 from first device 102 over network link 220. The first authentication factor may include a username and an associated password such that the combination of username and password is unique to the user. The user may input the username and password by using input device 214. Input device 214 may be a mechanical keyboard connected to first device 102. Similarly, input device 214 may be a virtual keyboard displayed on display 212 of computer device 306. In an embodiment, the first authentication factor may be a facial scan, a retinal scan, a fingerprint scan, a voice scan, or some other unique identifying feature linked to a particular biological trait of the user. For example, the user may scan a finger at the Internet-connected door locking mechanism or the user may use a fingerprint scan or username and password typed on a virtual keyboard to login into a banking app installed on their smartphone.

[0052] In an embodiment, the first authentication factor is sent to server 104 from first authentication module 302 implemented

on computer device 306. In an embodiment, the first authentication factor is encrypted at the source before being transmitted to server 104 to prevent malicious actors like hackers, crackers, and other cyber-criminals from accessing the user's private data. Similarly, the first authentication factor may be communicated to server 104 along a secured or encrypted communication link between first device 102 and server 104.

[0053] At step 404, server 104 authenticates the first authentication factor. For example, if the first authentication factor is a username and a password, authenticating the first authentication factor may involve server 104 checking the username and password transmitted by first device 102 or first authentication module 302 to a previously authenticated stored copy of the username and password. Similarly, server 104 may authenticate other forms of first authentication factors, for example fingerprint scans. In an embodiment, the user login details (for example username and password) are stored in a secure database by server 104. In an embodiment, server 104 successfully authenticates the first authentication factor based on whether the transmitted first authentication factor matches the stored first authentication factor on server 104. If server 104 fails to authenticate the first authentication factor, then server 104 may send a notification to first device 102 or first authentication module 302 of unsuccessful authentication. In an embodiment, the notification may be in the form of a pop-up display on a browser or a re-direct to a different webpage informing the user of the error, or other audio-visual signals for example indicator lights, beeps etc. Server 104 may allow the user to try to login again by re-entering and re-transmitting the first authentication factor. In an embodiment, server 104 may limit the number of unsuccessful login attempts by the user.

[0054] At step 406, in response to successfully authenticating the first authentication factor, server 104 automatically tries to authenticate a second authentication factor by activating recording of keystroke timing data using first device 102 and recording of keystroke typing data using second device 106. In an embodiment, server 104 activates recording of keystroke timing data using first authentication module 302 and recording of keystroke typing data using second authentication module 306.

[0055] In an embodiment, the keystroke timing data is keystrokes' timestamps associated with the user inputting a randomized code using first device 102. For example, a browser implemented on first device 102 or as a part of first authentication module 302 may record a set of timestamps of the user's keystrokes on input device 214 using a script on the webpage hosted on server 104 or a browser extension activated when the user visits the webpage. The randomized code may be entered in response to first device 102 prompting the user after receiving a notification of successful authentication of first authentication factor from server 102.

[0056] In an embodiment, the randomized code is any combination of alphanumeric characters, ASCII characters, or other characters that user is able to input using input device 214, for example a mechanical keyboard, or a virtual keyboard implemented as a part of first authentication module 302, or an alphanumeric keypad attached to an Internet-connected smart door locking mechanism. Persons having ordinary skill in the art will appreciate that the length of the randomized code may vary among different embodiments. For example, some embodiments may require a 4-character code, while others may require a 6-character code. There is a direct relationship between the length of the randomized code and the time taken for server 104 to allow access to first device 102. Similarly, there is an inverse relationship between the length of the

randomized code and the security of the system. For example, a longer randomized code may result in an increase in the time for server 104 to allow access to first device 102 or first authentication module 302. However, the longer randomized code may also improve overall system security. In an embodiment, the user may choose to specify a level of security that affects the length of the randomized code or may directly specify the length of the code according to the user's preferences.

[0057] In an embodiment, second device 106 may be adjacent or near first device 102 to facilitate automatic authentication of second authentication factor. For example, the distance between first device 102 and second device 106 may be between zero and ten meters. Persons skilled in the art will appreciate that distance between first device 102 and second device 106 may vary between embodiments. The distance may depend upon the sensitivity, power, and quality of recording devices included in second device 106.

[0058] In an embodiment, the keystroke typing data records signals generated by inputting of the keystrokes. In an embodiment, the keystroke typing data may be audio data, for example, the noise generated by a user inputting the keystrokes on a mechanical keyboard. Similarly, the keystroke typing data may be vibrational data, for example, the vibrations generated by a user while typing on a virtual keyboard. Furthermore, keystroke typing data may be beeps or other pre-programmed noises, for example when a user is entering a randomized code on a keypad included with an Internet-connected smart door locking mechanism. In an embodiment, second device 106 or second authentication module 304 may include specialized hardware or software to distinguish keystroke typing data from background noise. The process then moves to step 408.

[0059] At step 408, server 104 sends keystroke timing data from

first device 102 to second device 106. In an embodiment, server 104 may send keystroke timing data from first authentication module 302 to second authentication module 304. In an embodiment, keystroke timing data is encrypted at the source before being transmitted to server 104 to prevent malicious actors like hackers, crackers, and other cyber-criminals from accessing the user's private data. Similarly, the keystroke timing data may be communicated to second device 106 along a secured or encrypted communication link between first device 102, server 104, and second device 106. The process then moves to step 410. In an embodiment, server 104 may send the randomized code from first device 102 to second device 106. In an embodiment, server 104 may send an indicator signal from first device 102 to second device 106. The indicator signal may inform second device 106 to stop recording the keystroke typing data. Thus, the indicator signal may deactivate second device 106 recording the audio or vibrational data. In an embodiment, the indicator signal controls the recording device or specialized code for operating recording device.

[0060] At step 410, first device 102 is allowed to access server 104 in response to the server receiving a notification of a successful authentication of the automatic second authentication factor from the second device such that the successful notification is generated according to a comparison between the keystroke timing data and the keystroke typing data by the second device. The comparison between the keystroke timing data and the keystroke typing data by the second device is discussed in reference to FIG. 5 below.

[0061] In an embodiment, the second factor authentication is independent of any interaction between the user and second device 106. For example, upon successful authentication the user is allowed to access the website hosted on server 104 from a web browser executing on a laptop, or the user is

allowed to access their bank account on the banking application implemented on a smartphone or open an Internet-connected smart locking mechanism.

[0062] FIG. 5 illustrates an exemplary method for authenticating a second authentication factor in accordance with an embodiment of the present invention. For the purposes of illustrating clear examples, FIG. 5 will be discussed with reference to FIGS. 1, 2, 3, and 4.

[0063] Referring now to FIG. 5, the keystroke timing data is compared to the keystroke typing data by second device 106 or second authentication module 304 depending upon the embodiment. At step 502, second device 106 or second authentication module 304 generate a similarity score according to cross-correlating the keystroke timing data and the keystroke typing data. The similarity score is a measure of whether the keystroke timing data and the keystroke typing data originate from inputting the randomized code on the same source. In other words, similarity score measures whether the two recordings recorded the same event. In an embodiment, computing the similarity score may include three steps: noise reduction, energy level extraction, and cross-correlation.

[0064] In an embodiment, noise reduction involves reducing background noise. The environment where a user attempts to access a server may have various kinds of noise, such as other users' typing on their computers, people's talking, and background music. A user's keystroke typing data may be covered up or subsumed by such noise. In an embodiment, second device 106 or second authentication module 304 may implement a high pass filter to prune the ambient noise and extract the keystroke typing data.

[0065] In an embodiment, energy level extraction refers to extracting the energy levels associated with the keystroke typing data, especially if the data is vibrational data. In an embodiment, the acoustic signal of one keystroke usually

involves three peaks: touch peak (when user first makes contact with the typing surface of a key), hit peak (when the user presses the key), and release peak (when the user releases the key). In an embodiment, for second device 106 located relatively further away from the source of keystroke typing data or when the environment is noisy, the touch peak and release peak are inconspicuous while the hit peak remains clear and therefore may serve as a landmark of a keystroke. In an embodiment, the hit peak is highlighted by transforming the signal sequence into its energy level in time windows. For example, the energy levels of keystroke typing data may be calculated using windowed discrete Fourier transform (DFT) and taking the sum of all DFT coefficients.

[0066] In an embodiment, cross-correlation is defined as a standard measure of similarity between two time series. In an embodiment, second device 106 or second authentication module 304 may calculate a similarity score by normalizing a cross-correlation of the keystroke timing data and energy levels extracted from keystroke typing data. After generating the similarity score the process moves to block 504. Persons having ordinary skill in the art will appreciate that there are several well-known statistical techniques for correlating time series and such techniques vary among various embodiments.

[0067] At block 504, the similarity score is compared to a pre-determined threshold value by second device 106. The pre-determined threshold value is the lowest value below which, a match between the keystroke timing data and keystroke typing data is not accepted as successful factor authentication by server 104. In an embodiment, the pre-determined threshold value may be determined by server 104. In an embodiment, the pre-determined threshold value may be determined by second device 106 or second authentication module 304. In an embodiment, second device 106 or second authentication module

304 can alter the pre-determined-threshold value based on the quality of recording of keystroke typing data received by second device 106 or second authentication module 304. Persons skilled in the art would appreciate that different embodiments may have different pre-determined threshold values. For example, pre-determined threshold values may be higher for banking smartphone applications as compared to those for Internet-connected door locking mechanisms. If the similarity score exceeds the pre-determined threshold value then the process moves to step 510.

[0068] At step 510, as described previously, server 104 receives a notification of successful authentication of second authentication factor from second device 106. The process then moves to step 512.

[0069] At step 512, as described previously, server 104 allows access to first device 102.

[0070] If the similarity score does not exceed the pre-determined threshold value, then the process moves to block 514. For example, a user may attempt to access server 104 from first device 102 in an abnormal environment with abnormal conditions such as the keyboard being soundless, or the surroundings being too noisy, automatic authentication of second authentication factor may fail. Therefore, at step 514, server 104 receives a notification of unsuccessful authentication of second authentication factor from second device 106. The process then moves to step 516.

[0071] At step 516, server 104 allows access to first device 102 if a user manually approves the randomized code that was input earlier by the user as displayed on the second device. In an embodiment, server 104 may send the randomized code from first device 102 to second device 106, which is then verified by the user. For example, second device 106 or second authentication factor 304 may display the randomized code on display 212. In an embodiment, the user may reject the displayed code, as it

may not match the randomized code. A mismatch between the displayed code and randomized code may indicate a hack or cyberattack and the user may initiate a change in their first authentication factor to protect themselves.

[0072] In the foregoing specification, embodiments of the invention have been described with reference to numerous specific details that may vary from implementation to implementation. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. The sole and exclusive indicator of the scope of the invention, and what is intended by the applicants to be the scope of the invention, is the literal and equivalent scope of the set of claims that issue from this application, in the specific form in which such claims issue, including any subsequent correction. Any definitions expressly set forth herein for terms contained in such claims shall govern the meaning of such terms as used in the claims.

What is claimed is:

1. A method of allowing a first device to access a server comprising:
receiving a first authentication factor from the first device using the server;
authenticating the first authentication factor using the server;
automatically authenticating a second authentication factor using the server, wherein authenticating the second authentication factor further comprises:
activating, using the server, recording of a keystroke timing data using the first device and recording of a keystroke typing data using a second device in response to successfully authenticating the first authentication factor;
sending, using the server, the keystroke timing data from the first device to the second device; and
allowing the first device to access the server in response to the server receiving a notification of a successful authentication of the second authentication factor from the second device, wherein the successful notification is generated according to a comparison between the keystroke timing data and the keystroke typing data by the second device;
wherein the keystroke timing data is keystrokes' timestamps associated with inputting a length-randomized code using the first device.
2. The method as defined in claim 1, wherein the first authentication factor comprises a username and a password.
3. The method as defined in claim 2, wherein authenticating

the first authentication factor using the server further comprises:

receiving the username and the password from the first device; and

matching the username and the password to an entry in a database implemented on the server.

4. The method as defined in claim 1, wherein the first authentication factor is encrypted.
5. The method as defined in claim 1, wherein the first device is communicatively coupled to the server by utilizing at least one networking technology of a group consisting: Wired networking, Wi-Fi, Bluetooth, Near Field Communication, and Infrared.
6. The method as defined in claim 1, wherein the first device is at least one of a group consisting of: personal computer, laptop, desktop, Internet of Things related device, smartphone, and tablet.
7. The method as defined in claim 1 further comprising notifying the first device, using the server, of an authentication error in response to unsuccessfully authenticating the first authentication factor.
8. The method as defined in claim 1, wherein the keystroke typing data records, using the second device, signals generated by inputting of the keystrokes.
9. The method as defined in claim 8, wherein the signals are audio data signals.
10. The method as defined in claim 8, wherein the signals are

vibrational signals.

11. The method as defined in claim 1 further comprising:
sending the length-randomized code from the first device
to the second device using the server.
12. The method as defined in claim 1 further comprising:
sending an indicator signal from the first device to the
second device using the server, wherein the
indicator signal informs the first device to stop
recording the keystroke timing data and wherein the
indicator signal informs the second device to stop
recording the keystroke typing data.
13. The method as defined in claim 1, wherein the second
device is communicatively coupled to the server by
utilizing at least one networking technology of a group
consisting: Wired networking, Wi-Fi, Bluetooth, Near
Field Communication, and Infrared.
14. The method as defined in claim 1, wherein the second
device is at least one of a group consisting of: personal
computer, laptop, desktop, Internet of Things related
device, smartphone, and tablet.
15. The method as defined in claim 13 or claim 14, wherein the
second device comprises a recording device capable of
recording at least one of audio data and vibrational
signals.
16. The method as defined in claim 8, wherein authentication
of the second authentication factor further comprises:
generating a similarity score according to cross-
correlating the keystroke timing data and the

keystroke typing data using the second device; and
comparing the similarity score to a pre-determined
threshold value using the second device.

17. The method as defined in claim 14 further comprising:
receiving a notification of an unsuccessful
authentication of the second authentication factor
at the server from the second device based upon the
similarity score being lower than the pre-determined
threshold;
displaying the length-randomized code for approval using
the second device; and
allowing the first device to access the server based on
approving the displayed length-randomized code using
the second device.
18. A system for allowing a first device to access a server
comprising:
the first device communicatively coupled to the server;
a second device, wherein the second device is
communicatively coupled to the server;
wherein the server:
receives a first authentication factor from the
first device;
authenticates the first authentication factor;
automatically authenticates a second authentication
factor by:
activating recording of a keystroke timing data
using the first device and recording of a
keystroke typing data using the second
device in response to a successful
authentication of the first authentication
factor;
send the keystroke timing data from the first

device to the second device; and
wherein the first device is allowed access to the server
in response to the server receiving a notification
of a successful authentication of the second
authentication factor from the second device,
wherein the successful notification is generated
according to a comparison between the keystroke
timing data and the keystroke typing data by the
second device ;
wherein the keystroke timing data records keystrokes'
timestamps based on inputting a length-randomized
code.

19. The system as defined in claim 18, wherein the first authentication factor comprises a username and a password.
20. The system as defined in claim 18, wherein the first authentication factor is encrypted.
21. The system as defined in claim 18 further comprising notifying the first device , using the server, of an authentication error in response to unsuccessfully authenticating the first authentication factor.
22. The system as defined in claim 18, wherein the keystroke typing data records signals generated by inputting the keystrokes using the first device.
23. The system as defined in claim 18, wherein the signals are audio data signals.
24. The system as defined in claim 18, wherein the signals are vibrational signals.

25. The system as defined in claim 18, wherein the second device comprises a recording device capable of recording at least one of audio data and vibrational signals.
26. The system as defined in claim 18, wherein authentication of the second authentication factor further comprises: generating a similarity score according to cross-correlating the keystroke timing data and the keystroke typing data using the second device; and comparing the similarity score to a pre-determined threshold value.
27. The system as defined in claim 26 further comprising: receiving a notification from the second device using the server in response to an unsuccessful authentication of the second authentication factor by the second device based upon the similarity score being lower than the pre-determined threshold; displaying the length-randomized code for approval using the second device; and allowing the first device to access the server based on approving the displayed length-randomized code using the second device.
28. A method of allowing a computer system to access a server comprising: receiving a first authentication factor, using the server, from a first authentication module implemented on the computer system; authenticating the first authentication factor using the server; automatically authenticating a second authentication factor using the server comprising:

activating recording of a keystroke timing data
using the first authentication module and
recording of a keystroke typing data using a
second authentication module in response to
successfully authenticating the first
authentication factor;
sending the keystroke timing data from the first
authentication module to the second
authentication module; and
allowing the computer system to access the server in
response to the server receiving a notification of a
successful authentication of the second
authentication factor from the second authentication
module, wherein the notification is generated
according to a comparison between the keystroke
timing data and the keystroke typing data by the
second authentication module;
wherein the keystroke timing data is keystrokes'
timestamps associated with inputting a length-
randomized code using the first device.

29. A system for allowing a computer system to access a
server comprising:
the computer system, wherein the computer system is
communicatively coupled to the server;
wherein the server:
receives a first authentication factor from the
computer system;
authenticates the first authentication factor;
automatically activates recording of a keystroke
timing data and recording of keystroke typing
data using the computer system in response to a
successful authentication of the first
authentication factor; and

wherein the computer system accesses the server in response to the server receiving a notification of successful authentication of the second authentication factor from the computer system and wherein the notification is generated based on the comparison between the keystroke timing data and the keystroke typing data by the computer system; wherein the keystroke timing data records keystrokes' timestamps based on inputting a length-randomized code.