

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

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.