~~METHOD AND DEVICE FOR VERIFYING USER BEHAVIOUR IN MOBILE SCENARIO~~
METHOD AND DEVICE FOR AUTHENTICATION VIA USER BEHAVIOR IN MOBILE SCENARIOS

TECHNICAL FIELD

[0001] The present disclosure relates to the field of network security technology, and particularly to a method and device for authentication via user behavior in mobile scenarios.

BACKGROUND

[0002] With the popularity of smartphones, tablet computers, and other portable devices, smart portable terminals have been deeply rooted in people's lives. People desire for more convenient work or life environments using mobile terminals, and particularly via a combination of online and offline technologies. During interactive processes, authentication via user behavior may be used to ensure the safety of the processes. On the other hand, people want the processes to become more convenient. Thus, developers are looking for more flexible and safer authentication solutions using user behavior for better user experience.

SUMMARY

[0003] Accordingly, the present disclosure provides a method of authentication via user behavior. The method is implemented by a mobile device. The method may include performing an authentication via user behavior for an application transaction process and suspending the application transaction process before the authentication is successful; acquiring the latest radio frame from a beacon and determining a distance parameter based on the radio frame after the authentication

is initialized; determining whether a specified distance condition is satisfied for the beacon and the mobile device based on the distance parameter, and in response to a determination that the specified distance condition is satisfied for the beacon and the mobile device, determining that the authentication is successful and resuming the application transaction process that was suspended previously.

[0004] The present disclosure further provides a device for authentication via user behavior. The device is implemented by a mobile device. The device may include an application processing unit configured to perform an authentication via user behavior for an application transaction process and suspend the application transaction process before the authentication is successful; a data processing unit configured to acquire the latest radio frame from a beacon and determine a distance parameter based on the radio frame after the authentication is initialized; a distance authentication unit configured to determine whether a specified distance condition is satisfied for the beacon and the mobile device, where in response to a determination that the specified distance condition is satisfied for the beacon and the mobile device, the application processing unit determines that the authentication is successful and resumes the application transaction process that was suspended previously.

[0005] The present disclosure can perform user authentication via behavior conveniently, quickly achieve execution of the transaction process, and avoid excessive manual operations, thus being widely applicable in a variety of offline interactive processes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is a diagram of an illustrative scheme that enables authentication via user behavior in accordance with implementations of the present disclosure.

[0007] FIG. 2A is an example block diagram showing a hardware structure of a mobile terminal in accordance with implementations of the present disclosure.

[0008] FIG. 2B is another example block diagram showing a logic structure of a device for authentication via user behavior in accordance with implementations of the present disclosure.

[0009] FIG. 3 is a flowchart of an illustrative process for authentication via user behavior in accordance with implementations of the present disclosure.

[0010] FIG. 4 is another flowchart of an illustrative process for authentication via user behavior in accordance with implementations of the present disclosure.

[0011] FIG. 5 is a diagram showing a structure of a radio frame in accordance with implementations of the present disclosure.

DETAILED DESCRIPTION

[0012] The present disclosure provides a technical solution for convenient and safe authentication via user behavior. FIG. 1 shows a system which includes a beacon 10, a mobile terminal 20, and a server 30. In the present disclosure, the mobile terminal 20 may include a mobile phone, a tablet computer, a personal digital assistant and other mobile computing devices. A mobile phone is used as an example hereinafter for illustration. The beacon 10 may include a wireless beacon that supports a variety of short-range wireless technology. A relatively popular Bluetooth beacon is used as an example hereinafter for illustration.

[0013] In implementations, the present disclosure provides a device for authentication via user behavior. The device may be implemented by the mobile device 20. As illustrated in FIG. 2A and 2B, in implementations, the mobile phone 20 may include a processor 21, RAM 22, nonvolatile memory 23, a Bluetooth chip 24, and an internal bus 25. Apparently, the mobile phone 20 may further include various other hardware components. For simplicity of description, they are not repeated herein. In implementations, the device for authentication via user behavior may be implemented by computer software. Apparently, this does not preclude implementations using other techniques. The processor 21 may read computer instructions from the nonvolatile memory 23 to the RAM 22 and run the computer instructions. Then, a running result forms the device on a logical level.

[0014] In these instances, on the logical level, the device for authentication via user behavior may include an application processing unit, a data processing unit, and a distance authentication unit. Referring to FIG. 3, operations implemented by the device may include the following.

[0015] At step 301, the application processing unit 214 may perform the authentication via user behavior for an application transaction process and suspend the application transaction process before the authentication is successful.

[0016] At step 302, the data processing unit may acquire the latest radio frame from the beacon and determine a distance parameter based on the radio frame after the authentication is initialized.

[0017] At step 303, the distance authentication unit may determine whether a physical distance between the beacon and the mobile device meets a specified distance condition based on the distance parameter.

[0018] At step 304, the application processing unit may determine that the authentication is successful and resume the application transaction process that was suspended previously in response to a determination that the specified distance condition is fulfilled.

[0019] Detailed implementations are provided below with respect to the technical solutions described above.

[0020] An owner of the Bluetooth beacon 10 may be a service provider (e.g., a unit or an individual). The owner may communicate with a user of the mobile terminal 20 via the Bluetooth beacon 10 in a convenient and secure manner. As an example, the owner of the Bluetooth beacon 10 is a hotel, and the Bluetooth beacon 10 is deployed in the hotel lobby, for example, at a position near the front desk. A user with the mobile terminal 20 may want to check into the hotel. According to hotel's regulations, the user generally has to register personal information. Currently, this registration is manually processed. For example, the user needs to show her/his identity card, and may also need to fill out some basic information. Hotel staffs need to scan the identity card to register the user and may input the basic information of the user. The whole process is relatively cumbersome and has low efficiency.

[0021] Referring to a process as illustrated in FIG. 4, in implementations, the user may efficiently check into the hotel using the mobile phone 20. To provide better user experience, the hotel and the user need to take some preparation work. For the hotel, the hotel may deploy the Bluetooth beacon 10 in an appropriate location (e.g., the front desk), and register an identity of the Bluetooth beacon 10 in an application server. For example, a hotel staff may install a client terminal on a computing device of the front desk, and the client terminal may communicate with the mobile phone

20. Suppose the name of the client terminal is "Check-in Hotel." The hotel may apply for a service account and transmit a corresponding relationship between the identity of the Bluetooth beacon 10 (which is abbreviated as “beacon identifier” hereinafter) and the service account to the application server. The application server may store the corresponding relationship for use in transactions generated in subsequent processes. For the mobile phone 20 of the user, the user may download a mobile App for registration from the application server. Suppose that the name of the mobile App is "Check-in." In these instances, the mobile App Check-in is an implementation of the device for authentication via user behavior. Before the user uses Check-in, the user may save various types of information required for hotel registration via a configuration interface of Check-in. For example, the information may include a scanned image (or photo) ID card, an ID number, a phone number, a place of work, a gender, a name, a title of an invoice, etc. The information may even include credit card information (used to complete a pre-authorized check-in).

[0022] After the above work is completed, the user with the mobile phone 20 may efficiently and safely check into the hotel. As mentioned earlier, the Bluetooth beacon 10 is deployed in the lobby near the front desk. To declare the existence, the Bluetooth beacon 10 may broadcast radio frames (e.g., beacon frames) in a predetermined frequency. When the user with the mobile phone 20 enters the lobby of the hotel, the mobile phone 20 may receive the beacon frame from the Bluetooth beacon 10. In the present disclosure, the mobile phone 20 may process the radio frames that the Bluetooth beacon 10 broadcasts.

[0023] As mentioned earlier, the user may check into the hotel using the mobile App Check-in. The user may click an icon of Check-in to initialize the mobile App and

then select a function of "registration" to trigger authentication via user behavior. Before the authentication via user behavior is performed successfully, the mobile App Check-in may not transmit registration information of the user to other devices, which amounts to temporarily suspending the process of check-in operation, because the mobile App Check-in may not determine which hotel the user selects at the current stage. In other words, the mobile App Check-in may not know the other end of the transaction. In an exemplary embodiment, the mobile App may output on the interface a notification that the user is close to the Bluetooth beacon 10 to guide the user to place the mobile phone 20 near the Bluetooth beacon 10 in the lobby of the hotel. During the process that the user with the mobile phone 20 moves towards the Bluetooth beacon 10, operations from the step 302 to the step 304 may be executed in a loop until the check-in process is completed or timeout.

[0024] At step 302, the distance parameter may not necessarily be a physical distance parameter in a strict sense. In an exemplary embodiment, the distance parameter may be a received signal strength of the radio frame. Generally, the received signal strength may well indicate a physical distance between a receiver (i.e., the mobile phone 20) and a transmitter (i.e., the Bluetooth beacon 10). That is, the closer the distance between the transmitter and the receiver is, the stronger the received signal strength of the receiver is. By the same token, the specified distance condition may not necessarily be a condition indicating a real physical distance. Correspondingly, the specified distance condition may be a condition indicating a signal strength threshold. For example, the specified distance condition may refer to whether the received signal strength is greater than or equal to the specified signal strength. In other words, developers may obtain a specified signal strength from

various experiments. The specified signal strength is generally relatively strong, which corresponds to a relatively short physical distance, such as 10 centimeters. When the received signal strength is greater than the specified signal strength, this indicates that the physical distance between the mobile phone 20 and the Bluetooth beacon 10 is less than or equal to 10 centimeters.

[0025] In some implementations, when the mobile phone 20 receives the latest Beacon frame, the mobile phone 20 may obtain the received signal strength of the radio frame (e.g., RSSI) via an internal Bluetooth component. When the received signal strength is greater than or equal to the specified signal strength, the step 303 may determine that the physical distance between the mobile phone 20 and the Bluetooth beacon 10 meets the specified distance condition. In contrast, when the received signal strength is less than the specified signal strength, this means that the physical distance between the mobile phone 20 and the Bluetooth beacon 10 fails to meets the specified distance condition. This indicates that the mobile phone 20 is not close enough to the Bluetooth beacon 10. The process will return to the step 302 to repeat the operation. Apparently, to avoid repeated cycles, a timer may be used to initiate a predetermined time period (e.g., 30 seconds) when the authentication via behavior is initiated. When the timer expires, the authentication will be terminated.

[0026] It is worth noting that, in the foregoing implementation, the specified distance condition is designed by developers according to actual needs to ensure that the user is close to the Bluetooth beacon 10 enough, which is a basis for whether the user is close enough to the Bluetooth beacon 10. When the user places the mobile phone 20 close enough to the Bluetooth beacon 10, from a standpoint of

Check-in, its desire that the user's action of placing the mobile phone 20 close enough to the Bluetooth beacon 10 has been performed by the user who clearly indicates his/her desire to check in. At this point, Check-in may execute the application transaction process that was suspended previously and further communicate with the opposite end (i.e., "Check-in hotel") of a transaction corresponding to the beacon for transaction. In implementations, the beacon identifier of the Bluetooth beacon 10 may be further obtained from the beacon frame at step 303. When the application transaction process is processed, the beacon identifier and the pre-stored transaction information or transaction instructions may then be sent to the application server. The application server completes the application transaction process between the beacon and a transaction terminal corresponding to the beacon.

[0027] During further execution of the application transaction process in this implementation, Check-in may transmit the pre-stored information in the mobile phone 20 for the user registration to the application server, which may then transmit to a computing device of the hotel. Specifically, Check-in may transmit the information for the user registration and the beacon identifier of the Bluetooth beacon to the application server at the same time. The application server may determine a corresponding hotel account based on the beacon identifier, and then transmit the information for the user registration to the computing device of the hotel, which runs a hotel version of Check-in. The reception staff may obtain the information for user registration after the mobile phone of the user is scanned (i.e., placing the mobile phone 20 near the Bluetooth beacon 10), which may include the scanned images of ID cards. Thus, the registration of the user is prepared efficiently.

[0028] The hotel version of Check-in may return a confirmation message to the application server after receiving the information for user registration. The application server may transmit a message to the mobile phone 20 to notify the user that the information of user registration is transmitted successfully. Accordingly, the user may know that the information for user registration has been received by the hotel. The loop between the step 302 and the step 304 is then terminated. As illustrated from the above description, the user may provide registration information to check into the hotel using the application Check-in without any tedious manual operations. The reception staff may not perform tedious operations such as scanning ID cards and inputting the registration information. The implementation is a significant improvement with respect to cost and efficiency.

[0029] In the above example, the specified distance condition may be designed by developers of mobile applications. In some other implementations of the present disclosure, an implementation that can be more widely and easily adopted for various scenarios is provided. In these instances, the specified distance condition may refer to whether a received signal strength is greater than or equal to a specified signal strength. The specified signal strength refers to a signal strength obtained from a beacon frame at a specified location at the step 302. The specified signal strength is specified by a terminal associated with the beacon. Specified signal strengths of beacons with different specifications may be different in a location specified by a beacon frame. FIG. 5 is a diagram showing a format of a beacon frame in accordance with implementations of the present disclosure. The specified signal strength has a reserved position on the beacon frame and occupies a byte length. A corresponding signal strength may be input on this position, for example, 0x2B or

0x3C, and so on. An owner or a developer of the Bluetooth beacon 10 may perform configurations thereof based on needs.

[0030] This design apparently has a better universality. Bluetooth chips used by different Bluetooth beacons may be different, and may support different Bluetooth standards. Thus, a same signal strength may correspond to different receiving distances for different beacons. For example, a beacon A adopts a Bluetooth chip having a high transmitting power. Suppose that the received signal strength of the beacon A at 20 centimeters is X. Beacon B adopts a Bluetooth chip having a low transmitting power. Suppose that the received signal strength of the beacon B at 20 centimeters is 0.8X. Beacon C adopts a Bluetooth chip having a lower transmitting power. Suppose that the received signal strength of the beacon C at 20 centimeters is 0.7X. In the previous implementation, suppose that the specified signal strength is fixed at X. When the mobile phone 20 is close to the beacon A and the distance is 20 centimeters, the operation for scanning phones may succeed. However, when the mobile phone 20 is close to the beacon B or C and the distance is 20 centimeters, the operation for scanning phones cannot succeed. In these instances, the user may move the mobile phone closer to the beacon B or C to complete the operation for scanning phones. From another perspective, as for more short-range wireless technologies (e.g., ZigBee), power differences among different beacons are even greater. Thus, adoption of fixed specified signal strengths is generally not effective.

[0031] In these instances, beacons generate beacon frames with specified signal strengths. Thus, different specified signal strengths may be configured for different beacons. The specified signal strengths may be changed to achieve the same physical distance. Suppose that 10 centimeters are the distance that is generally accepted by

users. Accordingly, the specified signal strength of beacon A is X, the specified signal strength of beacon B is 0.8X, and the specified signal strength of beacon C is 0.7X. This design is easily adopted to ensure good user experience with respect to scanning phones. No matter what kind of mobile phone is used and what kind of short-range wireless technology is adopted by the hotel, the user may complete the operation of scanning phones at a relative accurate distance.

[0032] The processing operations described above may be implemented by applications associated with mobile terminals. For example, a consumer may group-buy or other means to buy a movie ticket online. Currently, ticket sellers generally send an authentication code to the mobile phone 20 such that a user may get a ticket using the authentication code. For example, the authentication code is sent to a social network terminal (e.g., TradeManager) of the user. The user may get the ticket from cinema staffs after arriving at the cinema. The staff manually checks whether the authentication code is legitimate. Alternatively, the user may get the ticket using a ticket machine by entering the authentication code. Apparently, these methods are cumbersome since the length of the code is usually a dozen or more. Based on the technical aspect of the present disclosure, developers of TradeManager may consider the design of Check-in and develop a simple ticket function to help users to get tickets efficiently.

[0033] Like the previous implementation, the Bluetooth beacon 10 may be deployed next to the ticket machine. The relationship between the beacon identifier of the beacon and the ID of the ticket machine is bound in the application server. TradeManager may be modified to add a ticket function for the user. The user selects the authentication code to initiate the function and authentication via user

behavior. The transaction process is suspended until the user successfully gets the ticket. The operations 302 to 304 may be executed. After the authentication is successful, TradeManager may continue to execute the ticket operation. TradeManager may proceed the transaction interaction with the ticket machine via the application server. During the interaction for the translation, TradeManager may transmit the beacon identifier of the Bluetooth beacon 10 and the authentication code stored in TradeManager to the application server, and the application server may identify the ticket machine based on the beacon identifier and transmit the authentication code to the ticket machine. The ticket machine may verify the authentication code after receiving the authentication code. The ticket machine may further provide the ticket to the user after authentication is successful. Throughout the process, the user may get the ticket without inputting the authentication code.

[0034] In the previous examples, after the authentication is successful, subsequent interactions may include transmitting the transaction information stored on the mobile phone 20 to a corresponding terminal of the beacon (e.g., a computing device of the hotel or the ticket machine). Other applications may also be supported by the implementations of the present disclosure. Taking an example of Check-in, the registration information may further include information of a user account that the user registers on the application server. After the user is ready to leave the hotel, the user may pay bills using Check-in. In the process, the hotel staff may transmit the bill information corresponding to the user account to the application server, and the application server transmits the bill information to the mobile phone 20. After the user receives the bill and determines the bill is correct, the user may initiate the authentication via behavior and a payment process by

selecting a function "Confirming Payment" of Check-in. The payment process is suspended until the user authentication is successful. Then, the operations 302 to 304 may be executed. In step 304, Check-in may proceed with the payment process if the authentication via behavior is successful. During this process, Check-in may transmit a confirmation message of the payment to the application server, and the confirmation message may include a serial number of the bill. The application server may proceed with the payment based on the confirmation message and notify results of the payment to parties of the current payment transaction. Unlike the previous implementations, in this implementation, a transaction instruction is transmitted with the beacon identifier, together with the transaction information that is transmitted in the previous implementations.

[0035] As can be seen from the above implementations, efficient authentication and external transaction interaction may be achieved. On the one hand, an object of the current transaction interaction is confirmed based on authentication via user behavior. On the other hand, authentication via user behavior enables the user to process application transactions more efficiently. This solution can be widely used in other areas. For example, when users apply for bank cards or membership cards, operations similar to those described above may enable the user to complete the registration of personal information quickly.

[0036] The foregoing is only preferred implementations of the present disclosure only, and it is not intended to limit the present application. Within the theories and principles of the present disclosure, any modifications, equivalent replacement, or improvement are also within the scope of protection of the present disclosure.

CLAIMS

What is claimed is:

1. A method comprising:

under control of one or more processors of a mobile device,

initiating an authentication via user behavior for an application transaction process and suspending the application transaction process before the authentication is successful;

acquiring a latest radio frame from a beacon and determining a distance parameter based on the radio frame after the authentication is initialized;

determining whether a specified distance condition is satisfied for the beacon and the mobile device; and

in response to a determination that the specified distance condition for the beacon and the mobile device is satisfied:

determining that the authentication is successful, and

resuming the application transaction process that was suspended previously.

2. The method of claim 1, wherein the resuming the application transaction process that was suspended previously comprises:

transmitting information to a server to enable the server to complete the application transaction process between the beacon and a transaction terminal corresponding to the beacon, wherein the information includes an identity of the beacon that is acquired from the radio frame, and transaction information and a transaction instruction that is pre-stored.

3. The method of claim 1, wherein the distance parameter comprises a received signal strength, and the specified distance condition comprises whether the received signal strength is greater than or equal to a specified signal strength.

4. The method of claim 3, further comprising:

prior to the acquiring of the latest radio frame from the beacon after the authentication is initialized,

acquiring the specified signal strength from the radio frame in a specified location.

5. The method of claim 3, wherein a receiving distance corresponding to the received signal strength is not greater than 20 centimeters.

6. The method of claim 1, wherein the beacon includes a Bluetooth beacon, and the radio frame includes a beacon frame.

7. The method of claim 1, further comprising:

re-acquiring the latest radio frame from the beacon and continuing subsequent processing if the specified distance condition is not satisfied.

8. A device comprising:

one or more processors;

memory;

an application processing unit stored in the memory and executable by the one or more processors to initiate an authentication via user behavior for an application transaction process, and suspend the application transaction process before the authentication is successful;

a data processing unit stored in the memory and executable by the one or more processors to acquire a latest radio frame from a beacon, and determine a distance parameter based on the radio frame after the authentication is initialized; and

a distance authentication unit stored in the memory and executable by the one or more processors to determine whether a specified distance condition is satisfied for the beacon and the mobile device, wherein the application processing unit further determines that the authentication is successful, and resumes the application transaction process that was suspended previously in response to a determination that the specified distance condition is satisfied for the beacon and the mobile device.

9. The device of claim 8, wherein the resuming the application transaction process that was suspended previously comprises:

transmitting information to a server to enable the server to complete the application transaction process between the beacon and a transaction terminal corresponding to the beacon, wherein the information includes an identity of the beacon that is acquired from the radio frame, and transaction information and a transaction instruction that is pre-stored.

10. The device of claim 8, wherein the distance parameter comprises a received signal strength, and the specified distance condition comprises whether the received signal strength is greater than or equal to a specified signal strength.

11. The device of claim 10, wherein a data processing unit configured to:

prior to the acquiring of the latest radio frame from the beacon after the authentication is initialized,

acquire the specified signal strength from the radio frame in a specified location.

12. The device of claim 10, wherein a receiving distance corresponding to the received signal strength is not greater than 20 centimeters.

13. The device of claim 8, wherein the beacon includes a Bluetooth beacon, and the radio frame includes a beacon frame.

14. The device of claim 8, wherein the distance authentication unit is configured to re-acquire the latest radio frame from the beacon and continue subsequent processing if the specified distance condition is not satisfied.