

WIRELESS NETWORK TYPE DETECTION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

TECHNICAL FIELD

[0001] The present application relates to the field of communication technology, and in particular, to a wireless network type detection method and apparatus, and an electronic device.

BACKGROUND

[0002] With the development of the mobile Internet, accessing a wireless network through Wi-Fi has become more and more frequent for electronic devices. But at the same time, Wi-Fi security issues have become more and more prominent. Electronic devices may connect to unsecured Wi-Fi hotspots, causing personal information leaks, password leaks, or account theft.

[0003] To facilitate user connections and allow more users to access unsecured Wi-Fi hotspots, most unsecured Wi-Fi hotspots do not set login passwords. Therefore, currently, many security-tool applications will check, after an electronic device connects to Wi-Fi, whether the current Wi-Fi requires a password for connection. If no password is required for connection, the security-tool applications will block the electronic device from accessing the Wi-Fi hotspot, or display a security prompt. However, sometime after connecting to the password-free Wi-Fi hotspot, users are still required to have secondary login verification. The secondary login verification means that although a device does not need a password to connect to a Wi-Fi hotspot, a login screen will pop up on the device when accessing the Internet, requiring the user to enter a username and password to access the Internet.

SUMMARY

[0004] Based on this, the present application provides a wireless network type detection method and apparatus, and an electronic device.

[0004a] According to one aspect, the present application provides a method for detection of a wireless network type performed by an electronic device. The method includes: determining whether a currently connected wireless network requires a password for accessing the Internet through the wireless network based on at least one specified network address; in response to determining that no password is required, accessing the specified

network address; determining whether the currently connected wireless network requires a secondary login verification by determining whether the specified network address can be successfully accessed; determining that the currently connected wireless network is an unsecured network if the currently connected wireless network does not require a password and does not require a secondary password; and providing a security risk warning to a user of the electronic device or automatically blocking access by the electronic device to the currently connected wireless network, if the currently connected wireless network is unsecured network.

[0004b] According to another aspect, the present application provides an electronic device including a processor and a memory. The memory is configured to store an instruction that can be executed by the processor, wherein the processor is configured to: determine whether a currently connected wireless network requires a password for accessing a service through the wireless network based on the specified network address; after determining that no password is required, access at least one specified network address; determine whether the currently connected wireless network requires secondary login verification, by determining whether the specified network address can be successfully accessed; determine that the currently connected wireless network is an unsecured network if the currently connected wireless network does not require a password and does not require a secondary password; and provide a security risk warning to a user of the electronic device or automatically blocking access by the electronic device to the currently connected wireless network, if the currently connected wireless network is unsecured network.

[0005] A wireless network type detection method includes: determining whether a currently connected wireless network requires a password for connection; after determining that no password is required, accessing at least one specified network address based on the specified network address; and determining, by determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0006] Optionally, the determining whether a currently connected wireless network requires a password for connection includes: calling a wireless network password management interface provided by an operating system, obtaining a call result, and determining, based on the call result, whether the currently connected wireless network requires a password for connection.

[0007] Optionally, the specified network address includes a network address of a user-defined API, and the API is used to return specified identification information when the API is accessed; and the determining whether the specified network address can be successfully accessed includes: obtaining an access result of accessing the network address of the API, and determining, based on whether the access result includes the specified identification information, whether the network address of the API can be successfully accessed.

[0008] Optionally, the specified network address includes network addresses of at least two different web pages; and the determining whether the specified network address can be successfully accessed includes: obtaining web page data returned after a network address of each of the web pages is accessed, and determining, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page, so as to determine whether the specified network address of each of the web pages can be successfully accessed.

[0009] Optionally, the page data of the web page includes the network address of the web page; and the determining, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page includes: updating the page data of each of the web pages, where the updating includes deleting the network address included in the page data of each of the web pages or replacing the network address included in the page data of each of the web pages with unified identification data; and comparing updated page data of the web pages to determine whether the page data is the same, and determining, based on a comparison result, whether each accessed web page jumps to the secondary login verification page.

[0010] A wireless network type detection apparatus includes: a connection password determining module, configured to determine whether a currently connected wireless network requires a password for connection; an access module, configured to: after it is determined that no password is required, access at least one specified network address based on the specified network address; and a login verification module, configured to determine, by

determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0011] Optionally, the connection password determining module is further configured to: call a wireless network password management interface provided by an operating system, obtaining a call result, and determining, based on the call result, whether the currently connected wireless network requires a password for connection.

[0012] Optionally, the specified network address includes a network address of a user-defined API, and the API is used to return specified identification information when the API is accessed; and the login verification module is further configured to: obtain an access result of accessing the network address of the API, and determine, based on whether the access result includes the specified identification information, whether the network address of the API can be successfully accessed.

[0013] Optionally, the specified network address includes network addresses of at least two different web pages; and the login verification module is further configured to: obtain web page data returned after a network address of each of the web pages is accessed, and determine, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page, so as to determine whether the specified network address of each of the web pages can be successfully accessed.

[0014] Optionally, the page data of the web page includes the network address of the web page; and the login verification module is further configured to: update the page data of each of the web pages, where the updating includes deleting the network address included in the page data of each of the web pages or replacing the network address included in the page data of each of the web pages with unified identification data; and compare updated page data of the web pages to determine whether the page data is the same, and determine, based on a comparison result, whether each accessed web page jumps to the secondary login verification page.

[0015] An electronic device includes: a processor; and a memory, configured to store an instruction that can be executed by the processor, where the processor is configured to: determine whether a currently connected wireless network requires a password for connection; after determining that no password is required, access at least one specified network address based on the specified network address; and determine, by determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0016] Technical solutions provided in the embodiments of the present application can include the following beneficial effects:

[0017] In the wireless network type detection method in the present application, after determining that the currently connected wireless network does not require a password for connection, the specified network address is further accessed. Whether the specified network address can be successfully accessed is also determined. If the network address can be accessed, it can be determined that the currently connected wireless network is a password-free wireless network. If the network address cannot be accessed, it can be determined that the wireless network requires secondary login verification. In the implementations of the present application, whether a password-free wireless network needs secondary login verification for connection can be accurately determined. Therefore, a user can be accurately warned about a wireless network security risk, reducing the false positive rate and the interruption to the user.

[0018] It should be understood that, the previous general description and the following detailed description are exemplary and explanatory only, and constitute no limitation on the present application.

BRIEF DESCRIPTION OF DRAWINGS

[0019] Accompanying drawings included in the present application constitute a part of the present application, illustrate embodiments consistent with the present application, and together with the description are used to explain principles of the present application.

[0020] FIG 1 is a schematic diagram illustrating connection to a wireless network through Wi-Fi by an electronic device in an exemplary embodiment of the present application;

[0021] FIG 2A is a flowchart illustrating a wireless network type detection method in an exemplary embodiment of the present application;

[0022] FIG 2B is a schematic diagram illustrating a wireless network type detection solution of an electronic device in an exemplary embodiment of the present application;

[0023] FIG 2C is a flowchart illustrating a wireless network type detection method in an exemplary embodiment of the present application;

[0024] FIG 2D is a flowchart illustrating a wireless network type detection method in an exemplary embodiment of the present application;

[0025] FIG 3 is a structural hardware diagram illustrating an electronic device including

a wireless network type detection apparatus of the present application; and

[0026] FIG 4 is a block diagram illustrating a wireless network type detection apparatus in an exemplary embodiment of the present application.

[0027] FIG 5 is a flowchart illustrating an example of a computer-implemented method for determining a wireless network type, according to an implementation of the present disclosure.

DESCRIPTION OF EMBODIMENTS

[0028] Exemplary embodiments are described in detail here, and examples of the exemplary embodiments are illustrated in accompanying drawings. When the following description refers to the accompanying drawings, same numerals in different accompanying drawings indicate the same or similar elements unless otherwise specified. Implementations described in the following exemplary embodiments do not represent all embodiments consistent with the present application. Instead, they are merely examples of apparatuses and methods consistent with some aspects of the present application as set forth in the appended claims.

[0029] The terms used in the present application are merely for the purpose of illustrating specific embodiments, and are not intended to limit the present application. The terms "a", "said" and "the" of singular forms used in the present application and the appended claims of the present application are also intended to include plural forms, unless the context indicates otherwise. It should also be understood that, the term "and/or" used herein indicates and includes any or all possible combinations of one or more associated listed items.

[0030] It should be understood that, although terms such as "first", "second", and "third" are used in the present application to describe various types of information, the information should not be limited by these terms. These terms are merely used to differentiate information of a same type. For example, without departing from the scope of the present application, first information can also be referred to as second information, and similarly, second information can also be referred to as first information. Depending on the context, the word "if" as used here can be interpreted as "when" or "in case that..." or "in response to determining".

[0031] In the embodiments of the present application, Wi-Fi is a technology that allows an electronic device to connect to a wireless local area network (WLAN), and allow terminals such as a personal computer and a handheld device (for example, a PDA or a mobile phone) to wirelessly interconnect with each other.

[0032] A Wi-Fi hotspot is a device that can provide a shared network resource and allow other terminals (for example, a mobile phone and or notebook computer) to connect to a network via a Wi-Fi connection. For example, if wireless network interconnection can be performed via the Wi-Fi connection in an effective coverage area of a radio wave of a wireless router, the wireless router is referred to as a "Wi-Fi hotspot".

[0033] Wi-Fi secondary login verification: although a password is not required when a device is connected to a Wi-Fi hotspot, when accessing the Internet, a login screen will pop up to require the user to enter a username and password. This login connection method is called "Wi-Fi secondary login authentication".

[0034] FIG 1 is a schematic diagram illustrating connection to a wireless network through Wi-Fi by an electronic device in an exemplary embodiment of the present application. When connecting to a wireless network hotspot, the electronic device can access the wireless network without using a password. However, a user needs to enter a username and password when the electronic device accesses the Internet through the wireless network. Therefore, the wireless network is not a password-free Wi-Fi in a practical sense.

[0035] The wireless network type detection solution in the embodiments of the present application, after determining that a currently connected wireless network does not require password for connection, a specified network address can further be accessed. Whether the specified network address can be successfully accessed is also determined. If yes, it can be determined that the currently connected wireless network is a password-free wireless network. If no, it can be determined that the wireless network requires secondary login verification. In the embodiments of the present application, whether a password-free wireless network needs secondary login verification for connection can be accurately determined. Therefore, a user can be accurately warned about a wireless network security risk, reducing the false positive rate and the interruption to the user. The following describes in detail the embodiments of the present application.

[0036] FIG 2A is a flowchart illustrating a wireless network type detection method in an exemplary embodiment of the present application. The wireless network type detection method includes the following steps 202 to 206.

[0037] Step 202: Determine whether a currently connected wireless network requires a password for connection.

[0038] Step 204: After determining that no password is required, based on at least one specified network address, access the specified network address.

[0039] Step 206: Determine, by determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0040] The method in this embodiment can be applied to an electronic device configured with a wireless network module. For example, the method can be applied to an application installed in the electronic device. The application can detect a type of a wireless network that the electronic device accesses, and provide a security risk warning about the wireless network for a user based on a detected type. The electronic device in this embodiment can include a smartphone, a tablet computer, a personal digital assistant, a multimedia player, etc. This type of electronic device is configured with a wireless network module, and can access a wireless network. FIG. 2B is a schematic diagram illustrating a wireless network type detection solution of an electronic device in an exemplary embodiment of the present application.

[0041] When an electronic device connects to a wireless network provided by a router, a gateway device, or another network terminal, the application can determine that the electronic device connects to the wireless network in a plurality of ways, and determine whether a password is required for the access. For example, if the application program has the permission, the electronic device can determine that the electronic device has access to the wireless network Wi-Fi hotspot by directly communicating with the wireless network module, or by reading an interface provided by the wireless network module or by using another method. The application program can also determine whether the accessed wireless network Wi-Fi hotspot requires a password for connection. In another example, the application program may have a permission and an operating system of the electronic device provides an interface, the application program can make the determinations based on a call result of calling the interface. In practical application, the application program can make determinations flexibly based on a plurality of factors such as an operating system used by the electronic device, an operating system permission that an application vendor can obtain, and an interface provided by the operating system.

[0042] In an optional implementation method, the determining whether a currently connected wireless network requires a password for connection includes: calling a wireless network password management interface provided by an operating system, obtaining a call result, and determining, based on the call result, whether the currently connected wireless network requires a password for connection.

[0043] Taking an Android operating system as an example, the operation system provides

a wireless network password management interface for a wireless network module. The application can call the interface, and determine, based on a call result of calling the interface, whether the currently connected wireless network requires a password for connection. The following illustrates code for calling the wireless network password management interface:

```

/**
 * It is determined, by using a WiFiConfiguration.KeyMgmt management
mechanism, whether the currently connected Wi-Fi requires a password for access.
 *
 * @return true: requiring a password for access, false: requiring no
password for access
 */
public static boolean needPassword(Context context) {
    WiFiManager      WiFiManager      =      (WiFiManager)
context.getSystemService(Context.WiFi_SERVICE);
    if (WiFiManager != null) {
        List<WiFiConfiguration>      WiFiConfiguration      =
WiFiManager.getConfiguredNetworks();
        if (WiFiConfiguration != null && WiFiConfiguration.size() > 0) {
            for (WiFiConfiguration configuration : WiFiConfiguration) {
                if (configuration != null && configuration.status ==
WiFiConfiguration.Status.CURRENT) {
                    if
(configuration.allowedKeyManagement.get(WiFiConfiguration.KeyMgmt.NONE)) {
                        return false;
                    } else {
                        return true;
                    }
                }
            }
        }
    }
    //A connection password is required by default.
    return true;
}

```

}

[0044] WiFiManager.getConfiguredNetworks() represents the wireless network password management interface.

[0045] Main logic of the code is to detect: whether WiFiConfiguration.allowedKeyManagement of the Wi-Fi hotspot includes a WiFiConfiguration.KeyMgmt.NONE field. If yes, it is considered that no password is required; or if no, it is considered that a password is required. When no password is required for wireless network connection, the call result includes the KeyMgmt.NONE field.

[0046] Taking an iOS operating system as an example, the iOS operating system provides an API (named NEHotspotNetwork) for obtaining a Wi-Fi list through mainly the following steps: applying to Apple for a permission to develop Network Extension, applying for a description file including Network Extension, configuring Info.plist, configuring entitlements, obtaining Wi-Fi list code implementation by iOS, and obtaining a Wi-Fi list callback.

[0047] After NEHotspotNetwork is called, returned information of NEHotspotNetwork includes: SSID: Wi-Fi name; BSSID: MAC address of a site; signalStrength: Wi-Fi signal strength, with a value ranging from 0.0–1.0; secure: indicates whether a network is secure (a value is false for Wi-Fi requiring no password for access); autoJoined: indicates whether the device automatically connects to the Wi-Fi; justJoined: indicates whether the network is just accessed; and chosenHelper: indicates whether HotspotHelper is selected for the network.

[0048] Therefore, based on security in the call result, it can be determined whether the currently connected wireless network Wi-Fi hotspot requires a password.

[0049] However, after accessing wireless networks without using a password, some networks still require secondary login verification of the user. Therefore, in this embodiment, whether secondary login verification is required is determined by specifying one or more network addresses in advance and accessing the specified network address. Assuming that secondary login verification is required, the user can access the Internet only after entering an account name and password. If the user does not perform secondary login verification, the electronic device cannot obtain desired network data after accessing the Internet. Based on this, in this embodiment, one or more network addresses are specified and the specified network address is accessed. If the specified network address is successfully accessed, it indicates that the accessed wireless network does not require secondary login verification. If the specified network address fails to be accessed, the accessed wireless network requires

secondary login verification.

[0050] In practical use, whether the access is successful can be determined in a plurality of ways. For example, network data corresponding to the specified network address can be pre-configured. After the specified network address is accessed, an access result is obtained, and whether the access is successful is determined based on whether the access result is the same as the pre-configured network data.

[0051] In this embodiment, the specified network address includes a network address of a user-defined API, and the API is used to return specified identification information when accessed.

[0052] The determining whether the specified network address can be successfully accessed includes: obtaining an access result of accessing the network address of the API, and determining, based on whether the access result includes the specified identification information, whether the network address of the API can be successfully accessed.

[0053] In this embodiment, an API can be developed on a server in advance. An application can access a network address of the API, and the network address can be an IP address. If a network is reachable, the specified identification information can be obtained after the API is accessed. If the network is unreachable, the specified identification information cannot be obtained. As such, it can be determined whether the network address of the API can be successfully accessed and whether secondary login verification is required.

[0054] In some other examples, pre-development work may not be performed. The network address can be a network address of a public web page. Page content of the web page can be pre-analyzed and pre-stored. It is determined whether an access result of accessing the web page includes the pre-stored page content, so as to determine whether the access is successful. However, the web page content may change dynamically. Therefore, in this embodiment, network addresses of two or more web pages can be specified, to provide a more reliable determining method. Specifically, the present application provides the following embodiment.

[0055] The specified network address includes network addresses of at least two different web pages; and the determining whether the specified network address can be successfully accessed includes: obtaining web page data returned after a network address of each of the web pages is accessed, and determining, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page, so as to determine whether the specified network address of the web page can be successfully

accessed.

[0056] Two or more existing public web pages, or web pages with relatively simple page content can be selected as the above-mentioned web pages, to reduce data traffic consumption. The network address can include a domain name address or an IP address of the web page. If the network is unreachable, each accessed web page jumps to the secondary login verification page. In this situation, page data of the secondary login verification page is returned, and the returned page data is basically the same. If the network is reachable, after the two or more web pages are accessed, page data of each web page is returned, and the page data of each web page is different. Therefore, in this embodiment, it can be determined, by comparing the page data of the web pages, whether each accessed web page jumps to the secondary login verification page, so as to determine whether the specified network address of each of the web pages can be successfully accessed.

[0057] After access is initiated to a network address, page data returned from the network address can be obtained. The page data includes the network address of the web page. If the network is unreachable, the returned page data includes the page data of the secondary login verification page. In this situation, all page data is the same except for the network address. Based on this, in this embodiment, for improving determining efficiency and accuracy, the determining, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page includes: updating the page data of each of the web pages, where the updating includes deleting the network address included in the page data of each of the web pages or replacing the network address included in the page data of each of the web pages with unified identification data; and comparing updated page data of the web pages to determine whether the page data is the same, and determining, based on a comparison result, whether each accessed web page jumps to the secondary login verification page.

[0058] In this embodiment, after the network addresses in page data are deleted or replaced with the unified identification data, the updated page data of the web pages is compared to determine whether the updated page data is the same. Therefore, comparison efficiency and accuracy can be significantly improved.

[0059] The following describes in detail the present application by using two embodiments.

[0060] FIG 2C is a flowchart illustrating a wireless network type detection method in an exemplary embodiment of the present application. In FIG 2C, an Android operating system is

used as an example. A wireless network password management interface of the operating system, that is, `WiFiManager.getConfiguredNetworks()`, is called and determining is performed based on whether a call result includes a `WiFiConfiguration.KeyMgmt.NONE` field. If not, it is considered that a password is required and a determining result is immediately returned. If yes, it can be further determined whether a currently connected wireless network Wi-Fi hotspot requires secondary login verification.

[0061] Specifically, an API can be developed on a proprietary server, and the API is used to return a simple success flag. An application directly accesses the API. If the success flag can be received, it is considered that the application can directly access the Internet through the currently connected wireless network Wi-Fi hotspot and secondary login verification is not required. Otherwise, it is considered that the secondary login verification is required.

[0062] FIG. 2D is a flowchart illustrating another wireless network type detection method in an exemplary embodiment of the present application. In FIG. 2D, an Android operating system is used as an example. A wireless network password management interface of the operating system, that is, `WiFiManager.getConfiguredNetworks()`, is called and determining is performed based on whether a call result includes a `WiFiConfiguration.KeyMgmt.NONE` field. If not, it is considered that a password is required and a determining result is immediately returned. If yes, it can be further determined whether a currently connected wireless network Wi-Fi hotspot requires secondary login verification.

[0063] Specifically, compared to the development of the API on the proprietary server in FIG. 2C, in this embodiment, addresses of two simple well-known websites (website pages can be as simple as possible to reduce data traffic consumption) can be selected. Assuming that the websites are a website A (the website address is `url_A`) and a website B (the website address is `url_B`), the websites addresses `url_A` and `url_B` are accessed sequentially, and response data returned from the addresses are stored in corresponding records: `response_A` and `response_B`. Finally, content of `response_A` and `response_B` is compared.

[0064] If the currently connected wireless network Wi-Fi hotspot requires secondary login verification, the accessed websites addresses `url_A` and `url_B` both jump to a secondary login verification page, that is, the content of `response_A` and `response_B` both includes page data of the same secondary login verification page. Otherwise, `response_A` and `response_B` represent content of different websites and are definitely different. Therefore, it can be determined whether the current Wi-Fi requires secondary login verification.

[0065] However, since `response_A` and `response_B` include a corresponding network

address, the network address can be replaced with unified identification data before the comparison between response_A and response_B. In this embodiment, the network address is replaced with url_B. Therefore, response_A.replace ("url_A", "url_B") can be executed, that is, the network address in response_A is replaced with url_B, to eliminate a network address difference in the page data, thereby avoiding a misjudgment and increasing determining efficiency and accuracy.

[0066] Corresponding to the foregoing embodiment of the wireless network type detection method, the present application further provides embodiments of a wireless network type detection apparatus and an electronic device that the wireless network type detection apparatus is applied to.

[0067] The embodiment of the wireless network type detection apparatus of the present application can be applied to an electronic device. The apparatus embodiment can be implemented by using hardware, software, or a combination of hardware and software. For example, in a software implementation, the wireless network type detection apparatus is a logical apparatus, and is formed when a wireless network type detection processor of the wireless network type detection apparatus reads a corresponding computer program instruction in a nonvolatile memory and executes the computer program instruction in a memory. In a hardware aspect, FIG. 3 is a structural hardware diagram illustrating an electronic device including a wireless network type detection apparatus of the present application. In addition to a processor 310, a memory 330, a network interface 320, and a nonvolatile memory 340 shown in FIG. 3, in this embodiment, the electronic device where the apparatus 331 is located generally can further include other hardware based on an actual function of the computer device. Details are not repeated here.

[0068] FIG. 4 is a block diagram illustrating a wireless network type detection apparatus in an exemplary embodiment of the present application. The apparatus includes: a connection password determining module 41, configured to determine whether a currently connected wireless network requires a password for connection; an access module 42, configured to: after it is determined that no password is required, access at least one specified network address based on the specified network address; and a login verification module 43, configured to determine, by determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0069] Optionally, the connection password determining module is further configured to:

call a wireless network password management interface provided by an operating system, obtain a call result, and determine, based on the call result, whether the currently connected wireless network requires a password for connection.

[0070] Optionally, the specified network address includes a network address of a user-defined API, and the API is used to return specified identification information when the API is accessed; and the login verification module is further configured to: obtain an access result of accessing the network address of the API, and determine, based on whether the access result includes the specified identification information, whether the network address of the API can be successfully accessed.

[0071] Optionally, the specified network address includes network addresses of at least two different web pages; and the login verification module is further configured to: obtain web page data returned after a network address of each of the web pages is accessed, and determine, by comparing the page data of the web pages, whether each accessed web page jumps to a secondary login verification page, so as to determine whether the specified network address of each of the web pages can be successfully accessed.

[0072] Optionally, the page data of the web page includes the network address of the web page; and the login verification module is further configured to: update the page data of each of the web pages, where the updating includes deleting the network address included in the page data of each of the web pages or replacing the network address included in the page data of each of the web pages with unified identification data; and compare updated page data of the web pages to determine whether the page data is the same, and determine, based on a comparison result, whether each accessed web page jumps to the secondary login verification page.

[0073] An electronic device includes: a processor; and a memory, configured to store an instruction that can be executed by the processor, where the processor is configured to: determine whether a currently connected wireless network requires a password for connection; after determining that no password is required, access at least one specified network address based on the specified network address; and determine, by determining whether the specified network address can be successfully accessed, whether the currently connected wireless network requires secondary login verification.

[0074] For details about implementation processes of functions and purposes of the modules in the apparatus, refer to the implementation processes of corresponding steps in the method, and details are not repeated here.

[0075] An apparatus embodiment basically corresponds to a method embodiment; therefore, for related parts, refer to partial descriptions in the method embodiment. The described apparatus embodiment is merely an example. The modules described as separate parts can or cannot be physically separate, and parts displayed as modules can or cannot be physical modules, that is, can be located in one position, or can be distributed on a plurality of network modules. Some or all of the modules can be selected based on actual requirements to achieve the objectives of the solutions of the present application. A person of ordinary skill in the art can understand and implement the embodiments of the present application without creative efforts.

[0076] Specific embodiments of the present application are described above. Other embodiments fall within the scope of the appended claims. In some situations, the actions or steps recited in the claims can be performed in a different order than in the embodiments and still achieve desirable results. In addition, the processes depicted in the accompanying drawings do not necessarily require the illustrated particular order or sequential order to achieve desirable results. In certain embodiments, multitasking and parallel processing are also possible or can possibly be advantageous.

[0077] Those skilled in the art will readily recognize other embodiments of the present application upon consideration of the present application and practice of the invention as applied here. The present application is intended to cover any variation, use, or adaptation of the present application that conforms to general principles of the present application and that include common general knowledge or a technical means in the art that is not claimed in the present application. The present application and embodiments are considered as mere examples, with the actual scope and spirit of the present application indicated by the following claims.

[0078] It should be understood that the present application is not limited to the precise structures that have been described above and shown in the accompanying drawings, and that various modifications and changes can be made without departing from the scope of the present application. The scope of the present application is limited only by the appended claims.

[0079] The foregoing descriptions are merely preferred examples of the embodiments of the present application, but are not intended to limit this application. Any modification, equivalent replacement, and improvement made without departing from the spirit and principle of the present invention shall fall within the protection scope of the present

invention.

[0080] FIG 5 is a flowchart illustrating an example of a computer-implemented method 500 for determining a wireless network type, according to an implementation of the present disclosure. For clarity of presentation, the description that follows generally describes method 500 in the context of the other figures in this description. However, it will be understood that method 500 can be performed, for example, by any system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. In some implementations, various steps of method 500 can be run in parallel, in combination, in loops, or in any order.

[0081] At 505, a determination is made as to whether a password is required for connecting to a wireless network. In some implementations, the determination is made automatically by a mobile device (such as, a mobile phone, a laptop) when connecting to the wireless network. The wireless network can be a wireless local area network (WLAN). A Wi-Fi hotspot (such as a wireless router) can provide a Wi-Fi connection to the WLAN when the mobile device is in a coverage area of the Wi-Fi hotspot. For example, a user can select the Wi-Fi hotspot on the mobile device to start a Wi-Fi connection to the WLAN. In some implementations, the mobile device can automatically start a Wi-Fi connection to the WLAN when detecting the Wi-Fi hotspot. When requested, the Wi-Fi hotspot can ask the mobile device to provide a password in order to connect the mobile device to the WLAN. In some implementations, the Wi-Fi hotspot can connect the mobile device to the WLAN without a password from the mobile device.

[0082] In some implementations, in response to determining that a password is required for connecting to the wireless network, a determination is made that the connection to the wireless network is a secure connection. In such a situation, a user can input a password on the mobile device to connect to the wireless network. If the mobile device has a stored password for the wireless network, the mobile device can provide the password automatically to connect to the wireless network. Since the connection to the wireless network is determined to be a secure connection, there is no security risk warning about the connection displayed on the mobile device, and the connection to the wireless network is not blocked by, for example, a security application on the mobile device.

[0083] In some implementations, to determine whether a password is required for connecting to a wireless network, a mobile device can call, for example, a wireless network password management interface provided by an operating system of the mobile device. The

mobile device can obtain a call result in response to calling the wireless network password management interface. Then, the mobile device can determine whether a password is required for connecting to the wireless network based on, at least, the call result. For example, if the operating system is an ANDROID operating system, `WiFiManager.getConfiguredNetworks()` can be the wireless network password management interface in the ANDROID operating system. The mobile device can call the interface. Based on, at least, the call result, the mobile device can determine whether `WiFiConfiguration.allowedKeyManagement` of a Wi-Fi hotspot of the wireless network includes a `WiFiConfiguration.KeyMgmt.NONE` field. If the field is included, the mobile device can determine that no password is required for connecting to the wireless network. However, if the field is not included, the mobile device can determine that a password is required for connecting to the wireless network. If the operating system is an APPLE iOS operating system, `NEHotspotNetwork` can be an application program interface (API) in the APPLE iOS operating system. The mobile device can call the API. Based on, at least, a security indicator in the call result, the mobile device can determine whether a password is required for connecting to the wireless network. From 505, method 500 proceeds to 510.

[0084] At 510, in response to determining that no password is required for connecting to the wireless network, data is retrieved from at least one predefined network address through the wireless network. In some implementations, data is retrieved automatically from the at least one predefined network address through the wireless network in response to the determination. For example, for enterprise client applications, a user-defined API can be developed on a proprietary server of the enterprise. The at least one predefined network address can include a network address associated with the user-defined API. The API can be configured to return specified identification information (such as, a “Success” identifier) when the API is accessed. For personal client applications, at least two network addresses, each associated with a different web page, can be predefined. Each web page can be an existing well-known public web page. In some implementations, to reduce data traffic, web pages with simple page content can be used to select the predefined network addresses. From 510, method 500 proceeds to 515.

[0085] At 515, a determination is made as to whether a secondary login verification is required for connecting to the wireless network. The determination is made based on, at least, the retrieved data from the at least one predefined network address. In some implementations, the determination is made automatically by a mobile device. In some implementations,

although a mobile device does not need a password to connect to a Wi-Fi hotspot of the wireless network at step 505, a secondary login verification can exist when the mobile device accesses the Internet through the wireless network. For example, a login screen, requiring a username, a password, or a combination of both, can pop up on the mobile device when the mobile device accesses the Internet through the wireless network. In some cases, the Wi-Fi hotspot of the wireless network can redirect the access request to a secondary login verification page, instead of the at least one predefined network address, if a secondary login verification is required for connecting to the wireless network. In some implementations, the Wi-Fi hotspot can pass the access request to the at least one predefined network address through the wireless network without a secondary login verification from the mobile device.

[0086] In some implementations, when the at least one predefined network address includes the network address associated with the user-defined API, the mobile device can access the network address associated with the user-defined API through the wireless network. The mobile device can obtain a network response to accessing the network address associated with the user-defined API through the wireless network is obtained. Then, the mobile device can determine whether a secondary login verification is required for connecting to the wireless network. The determination is made based on, at least, whether the obtained network response includes specified identification information.

[0087] For example, if the network response includes a “Success” identifier, the mobile device can determine that the access request has reached the network address associated with the user-defined API without a secondary login verification. Therefore, a determination can be made by the mobile device that no secondary login verification is required for connecting to the wireless network. However, if the network response does not include a “Success” identifier, the mobile device can determine that the access request has not reached the network address associated with the user-defined API without a secondary login verification. Therefore, a determination can be made by the mobile device that a secondary login verification is required for connecting to the wireless network.

[0088] In some implementations, when the at least one predefined network address includes at least two network addresses associated with different web pages, the mobile device can access each network address of the at least two network addresses associated with different web pages. For each accessed network address, web page data, including first web page data associated with one of the at least two network addresses and second web page data associated with a different one of the at least two network addresses, is obtained. Then, the

first web page data is compared to the second web page data to determine whether the first web page data matches the second web page data. In response to determining that the first web page data matches the second web page data, the mobile device can determine that a secondary login verification is required for connecting to the wireless network.

[0089] For example, if websites A and B, with web addresses URL_A and URL_B, respectively, are accessed, returned web page data, response_A and response_B, respectively, are obtained and compared. If response_A and response_B are different, the mobile device can determine that the access request has reached both websites A and B without a secondary login verification. Therefore, a determination can be made by the mobile device that no secondary login verification is required for connecting to the wireless network. However, if response_A and response_B are the same, the mobile device can determine that the access request has not reached either website A or B without a secondary login verification. For example, the access request to both websites A and B is redirected to a same secondary login verification page, and as a result, response_A and response_B represent the same content of the secondary login verification page. Therefore, a determination can be made by the mobile device that a secondary login verification is required for connecting to the wireless network.

[0090] In some implementations, comparing the first web page data to the second web page data can include updating the first web page data and the second web page data to remove corresponding network address data or to replace the corresponding network address data with unified identification data, and comparing the updated first web page data to the updated second web page data. For example, if response_A includes URL_A and response_B includes URL_B, a comparison of response_A and response_B will be different if URL_A and URL_B are different, even if a secondary login verification is required for connecting to the wireless network. In such a situation, URL_A in response_A and URL_B in response_B can be deleted before the comparison. In some implementations, URL_A in response_A and URL_B in response_B can be replaced with a same web address before the comparison. For example, URL_A in response_A can be replaced with URL_B, URL_B in response_B can be replaced with URL_A, or URL_A in response_A and URL_B in response_B can be both replaced with URL_C before the comparison.

[0091] In some implementations, in response to determining that no secondary login verification is required for connecting to the wireless network, a determination is made that the connection to the wireless network is not a secure connection. A warning message can be displayed on the mobile device to remind a user of potential security risk of connecting to the

wireless network. In some implementations, a connection to the wireless network is blocked automatically by, for example, a security application on the mobile device in response to the determination that the connection to the wireless network is not a secure connection.

[0092] In some implementations, in response to determining that a secondary login verification is required for connecting to the wireless network, a determination is made that the connection to the wireless network is a secure connection. In such a situation, a user can input a username, a password, or a combination of both on the mobile device to connect to the wireless network. If the mobile device has a stored username, a stored password, or a combination of both for the wireless network, the mobile device can provide the username, the password, or a combination of both automatically to connect to the wireless network. Since the connection to the wireless network is determined to be a secure connection, there is no security risk warning about the connection displayed on the mobile device, and the connection to the wireless network is not blocked by, for example, a security application on the mobile device. After 515, method 500 stops.

[0093] A user can use application software installed on a mobile device to connect to a wireless network through, for example, a Wi-Fi hotspot. Normally, insecure Wi-Fi hotspots do not have login passwords. However, some secure Wi-Fi hotspots also do not have login passwords while implementing a secondary login verification process. As a result, the mobile device cannot differentiate an insecure Wi-Fi hotspot without a login password from a secure Wi-Fi hotspot with a secondary login verification. A security application on the mobile device will treat a secure Wi-Fi hotspot with a secondary login verification the same way as an insecure Wi-Fi hotspot without a login password, hence results in poor user experience when using the security application. The subject matter described in this specification can be used to differentiate an insecure Wi-Fi hotspot without a login password from a secure Wi-Fi hotspot with a secondary login verification. For example, after determining that a Wi-Fi hotspot does not have a login password, another determination is made as to whether the Wi-Fi hotspot without a login password implements a secondary login verification process. As a result, a Wi-Fi hotspot, without a login password and with a secondary login verification, can be accurately identified as a secure Wi-Fi hotspot. In doing so, accurate network security risk of a Wi-Fi connection can be provided to a user, thereby reducing a misjudgment rate of the Wi-Fi connection and disturbance to the user.

[0094] Embodiments and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware,

including the structures disclosed in this specification or in combinations of one or more of them. The operations can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources. A data processing apparatus, computer, or computing device may encompass apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing. The apparatus can include special purpose logic circuitry, for example, a central processing unit (CPU), a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC). The apparatus can also include code that creates an execution environment for the computer program in question, for example, code that constitutes processor firmware, a protocol stack, a database management system, an operating system (for example an operating system or a combination of operating systems), a cross-platform runtime environment, a virtual machine, or a combination of one or more of them. The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing infrastructures.

[0095] A computer program (also known, for example, as a program, software, software application, software module, software unit, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A program can be stored in a portion of a file that holds other programs or data (for example, one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (for example, files that store one or more modules, sub-programs, or portions of code). A computer program can be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0096] Processors for execution of a computer program include, by way of example, both general- and special-purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random-access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be

operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data. A computer can be embedded in another device, for example, a mobile device, a personal digital assistant (PDA), a game console, a Global Positioning System (GPS) receiver, or a portable storage device. Devices suitable for storing computer program instructions and data include non-volatile memory, media and memory devices, including, by way of example, semiconductor memory devices, magnetic disks, and magneto-optical disks. The processor and the memory can be supplemented by, or incorporated in, special-purpose logic circuitry.

[0097] Mobile devices can include handsets, user equipment (UE), mobile telephones (for example, smartphones), tablets, wearable devices (for example, smart watches and smart eyeglasses), implanted devices within the human body (for example, biosensors, cochlear implants), or other types of mobile devices. The mobile devices can communicate wirelessly (for example, using radio frequency (RF) signals) to various communication networks (described below). The mobile devices can include sensors for determining characteristics of the mobile device's current environment. The sensors can include cameras, microphones, proximity sensors, GPS sensors, motion sensors, accelerometers, ambient light sensors, moisture sensors, gyroscopes, compasses, barometers, fingerprint sensors, facial recognition systems, RF sensors (for example, Wi-Fi and cellular radios), thermal sensors, or other types of sensors. For example, the cameras can include a forward- or rear-facing camera with movable or fixed lenses, a flash, an image sensor, and an image processor. The camera can be a megapixel camera capable of capturing details for facial and/or iris recognition. The camera along with a data processor and authentication information stored in memory or accessed remotely can form a facial recognition system. The facial recognition system or one-or-more sensors, for example, microphones, motion sensors, accelerometers, GPS sensors, or RF sensors, can be used for user authentication.

[0098] To provide for interaction with a user, embodiments can be implemented on a computer having a display device and an input device, for example, a liquid crystal display (LCD) or organic light-emitting diode (OLED)/virtual-reality (VR)/augmented-reality (AR) display for displaying information to the user and a touchscreen, keyboard, and a pointing device by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, for example, visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic,

speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's client device in response to requests received from the web browser.

[0099] Embodiments can be implemented using computing devices interconnected by any form or medium of wireline or wireless digital data communication (or combination thereof), for example, a communication network. Examples of interconnected devices are a client and a server generally remote from each other that typically interact through a communication network. A client, for example, a mobile device, can carry out transactions itself, with a server, or through a server, for example, performing buy, sell, pay, give, send, or loan transactions, or authorizing the same. Such transactions may be in real time such that an action and a response are temporally proximate; for example an individual perceives the action and the response occurring substantially simultaneously, the time difference for a response following the individual's action is less than 1 millisecond (ms) or less than 1 second (s), or the response is without intentional delay taking into account processing limitations of the system.

[00100] Examples of communication networks include a local area network (LAN), a radio access network (RAN), a metropolitan area network (MAN), and a wide area network (WAN). The communication network can include all or a portion of the Internet, another communication network, or a combination of communication networks. Information can be transmitted on the communication network according to various protocols and standards, including Long Term Evolution (LTE), 5G, IEEE 802, Internet Protocol (IP), or other protocols or combinations of protocols. The communication network can transmit voice, video, biometric, or authentication data, or other information between the connected computing devices.

[00101] Features described as separate implementations may be implemented, in combination, in a single implementation, while features described as a single implementation may be implemented in multiple implementations, separately, or in any suitable sub-combination. Operations described and claimed in a particular order should not be understood as requiring that the particular order, nor that all illustrated operations must be performed (some operations can be optional). As appropriate, multitasking or parallel-processing (or a combination of multitasking and parallel-processing) can be performed.

CLAIMS

1. A method for detection of a wireless network type performed by an electronic device, the method comprising:

determining whether a currently connected wireless network requires a password for accessing the Internet through the wireless network based on at least one specified network address (202);

in response to determining that no password is required, accessing the specified network address (204);

determining whether the currently connected wireless network requires a secondary login verification by determining whether the specified network address can be successfully accessed (206);

determining that the currently connected wireless network is an unsecured network if the currently connected wireless network does not require a password and does not require a secondary password; and

providing a security risk warning to a user of the electronic device or automatically blocking access by the electronic device to the currently connected wireless network, if the currently connected wireless network is unsecured network.

2. The method according to claim 1, comprising automatically blocking access by the electronic device to the currently connected wireless network, if the currently connected wireless network is unsecured network.

3. The method according to claim 1, comprising providing a security risk warning to a user of the electronic device.

4. The method according to any one of claims 1 to 3, wherein determining whether the currently connected wireless network requires a password for connection comprises:

calling a wireless network password management interface provided by an operating system;

obtaining a call result; and

determining, based on the call result, whether the currently connected wireless network requires the password for connection.

5. The method according to any one of claims 1 to 4, wherein the specified network address comprises a network address of a user-defined API for an enterprise, and the user-defined API is used to return specified identification information when the API is accessed.

6. The method according to claim 5, wherein determining whether the specified network address can be successfully accessed comprises: obtaining an access result of accessing the network address of the user-defined API; the method further comprising

determining, based on whether the access result comprises the specified identification information, whether the network address of the user-defined API can be successfully accessed.

7. The method according to any one of claims 1 to 5, wherein the specified network address comprises network addresses of at least two different web pages.

8. The method according to claim 7, wherein determining whether the specified network address can be successfully accessed comprises:

obtaining a web page data returned after a network address of each of the web pages is accessed, and determining, by comparing the web page data of the web pages, whether each accessed web page jumps to a secondary login verification page, so as to determine whether the specified network address of the web page can be successfully accessed.

9. The method according to claim 8, wherein the web page data of the web page comprises the network address of the web page.

10. The method according to claim 8, wherein determining, by comparing the web page data of the web pages, whether each accessed web page jumps to a secondary login verification page comprises:

updating the web page data of each of the web pages, wherein the updating comprises deleting the network address comprised in the web page data of each of the web pages or replacing the network address comprised in the web page data of each of the web pages with unified

identification data; and

comparing updated web page data of the web pages to determine whether the web page data is the same, and determining, based on a comparison result, whether each accessed web page jumps to the secondary login verification page.

11. An electronic device, comprising:

a processor; and

a memory, configured to store an instruction that can be executed by the processor, wherein the processor is configured to:

determine whether a currently connected wireless network requires a password for accessing a service through the wireless network based on the specified network address (202);

after determining that no password is required, access at least one specified network address (204);

determine whether the currently connected wireless network requires secondary login verification, by determining whether the specified network address can be successfully accessed (206)

determine that the currently connected wireless network is an unsecured network if the currently connected wireless network does not require a password and does not require a secondary password; and

providing a security risk warning to a user of the electronic device or automatically blocking access by the electronic device to the currently connected wireless network, if the currently connected wireless network is unsecured network.

12. The device according to claim 11, wherein the memory comprises a wireless network type detection apparatus that is configured to perform the method according to any one of claims 1 to 10.