

METHOD, APPARATUS, DEVICE, AND STORAGE MEDIUM FOR AUTHENTICATING LOGIN SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present disclosure claims the priority to the Chinese patent application with the filing No. 2024119317680 filed with the Chinese Patent Office on December 26, 2024, and entitled “METHOD, APPARATUS, DEVICE, AND STORAGE MEDIUM FOR AUTHENTICATING LOGIN SYSTEM”, the contents of which are incorporated herein by reference in entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to the technical field of login authentication, specifically to a method, an apparatus, a device, and a storage medium for authenticating login system.

BACKGROUND ART

[0003] With the development of Internet technology, the application of various intelligent devices or systems has become increasingly widespread. Intelligent devices or systems typically provide an administrator account, allowing users to log in to the management program of the intelligent device or system using the administrator account and its corresponding login password, thereby managing the intelligent device or system.

[0004] For security considerations, intelligent devices or systems are usually configured to require the user to change the login password after the first login to the management program, preventing others from accessing the management program using the default password.

[0005] However, in practical applications, users often forget the modified login password and need to retrieve the password or restore the default password before they can log in to the management program again. To enhance the security of device management, the steps and procedures for retrieving the password or restoring the default password are typically designed to be complex, leading to low convenience for users attempting to log in to intelligent devices or systems after forgetting the login password.

SUMMARY

[0006] The objective of the present disclosure is to provide a method, an apparatus, a device, and a storage medium for authenticating login system to improve the convenience of users logging into intelligent devices or systems when they forget the login password.

[0007] The embodiments of the present disclosure provide a method for authenticating login system, including:

[0008] responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information;

[0009] receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

[0010] the to-be-authenticated login password is obtained by parsing the encrypted information.

[0011] In the embodiment of the present disclosure, under the premise of ensuring safety, the convenience of user to login to an intelligent device or system when the user forgets the login password is improved, which is achieved by acquiring the current login password locally in an intelligent device or system and encrypting it, so that the user forwards the encrypted information to the security server for decryption and acquires the corresponding login password.

[0012] In some possible embodiments, before the step of receiving a to-be-authenticated login password input by the user, the method further includes:

[0013] generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string and the security server parses the encrypted information to obtain the to-be-authenticated login password.

[0014] In the embodiments of the present disclosure, a request interface is preset locally in the intelligent device or system and is combined with encrypted information to generate a request string used for requesting the security server, thereby further improving the efficiency of forwarding the encrypted information.

[0015] In some possible embodiments, the step of generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string includes:

[0016] generating a request string based on the encrypted information and the preset request interface, and converting the request string into a graphical recognition code, so that the user, after scanning the graphical recognition code using a carried mobile terminal, forwards the

encrypted information to the security server based on the request string obtained by parsing the graphical recognition code.

[0017] In the embodiments of the present disclosure, by converting the request string into a graphical recognition code for scanning and recognition by a mobile terminal, which then initiates a request to the security server, the flexibility of forwarding the encrypted information is further enhanced.

[0018] In some possible embodiments, the encrypted information is obtained by performing encryption processing on the current login password and a device identifier of the target system; and

[0019] the security server is configured for:

[0020] receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and device identifier; and

[0021] obtaining a registered terminal number bound to the device identifier based on a pre-stored registration information database, and sending the current login password to a target mobile terminal corresponding to the registered terminal number.

[0022] In the embodiments of the present disclosure, a registration information database is set up to manage login passwords for different devices, further improving the flexibility of intelligent device login authentication.

[0023] In some possible embodiments, the encrypted information is obtained by performing encryption processing on the current login password and a target terminal number preset in the target system; and

[0024] the security server is configured for:

[0025] receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and target terminal number; and

[0026] sending the current login password to a target mobile terminal corresponding to the target terminal number.

[0027] In the embodiments of the present disclosure, by locally storing the phone number corresponding to the user (administrator) in the intelligent device or system and encrypting it along with the current login password to forward it to the security server, the security server parses the encrypted information and directly sends the current login password to the mobile terminal corresponding to the phone number, thereby further improving the convenience for users to log in to intelligent devices or systems when they forget the login password.

[0028] In some possible embodiments, the method for authenticating login system further includes:

[0029] responding to an account registration request of the user for the target system, acquiring a to-be-registered terminal number specified by the account registration request, and performing encryption processing on the to-be-registered terminal number and the device identifier of the target system to obtain registration encrypted information; and

[0030] the security server is further configured for:

[0031] receiving the registration encrypted information forwarded by the user, and parsing the registration encrypted information to obtain a corresponding to-be-registered terminal number and device identifier; and

[0032] sending authentication information to the mobile terminal corresponding to the to-be-registered terminal number to perform identity authentication on the to-be-registered terminal number, and after the identity authentication is successfully completed, binding and storing the to-be-registered terminal number and the device identifier in the registration information database.

[0033] In the embodiments of the present disclosure, by authenticating the registration information submitted by the user on the intelligent device through the security server, the security of user registration login accounts is further enhanced.

[0034] In the embodiments of the present disclosure, the step of responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information includes:

[0035] responding to the login password acquisition request of the user for the target system, acquiring a preset login password corresponding to a target account based on the target account specified by the login password acquisition request as the current login password of the target system; and

[0036] performing encryption processing on the target account and the current login password to obtain the encrypted information.

[0037] In the embodiments of the present disclosure, by acquiring a previously preset login password for different users based on the account as the current login password, the current login password is retrieved, login authentication of different users on intelligent devices is achieved by retrieving passwords, thus further improving the convenience for users to log in to intelligent devices or systems when they forget the login password.

[0038] In the embodiments of the present disclosure, the step of responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system includes:

[0039] responding to the login password acquisition request of the user for the target system, and generating a random login password based on a preset random algorithm as the current login password of the target system.

[0040] In the embodiments of the present disclosure, by using a randomly generated login password as the current login password, login authentication for the intelligent device is carried out in the form of a random password, further enhancing the security of logging into the intelligent device or system when users forget the login password.

[0041] In some possible embodiments, the method for authenticating login system further includes:

[0042] resetting the current login password of the target system, after generating the random login password and when a to-be-authenticated login password that is consistent with the random login password is not received within a preset valid duration.

[0043] In the embodiments of the present disclosure, by setting a validity period for the random login password and rendering the current random login password invalid when authentication is not successfully completed within the timeout period, the security of logging into intelligent devices or systems when users forget the login password is further enhanced.

[0044] In some possible embodiments, the method for authenticating login system further includes:

[0045] locking the login account of the user when a number of failed authentication attempts for the to-be-authenticated login password input by the user based on the current login password exceeds a preset threshold.

[0046] In the embodiments of the present disclosure, by locking user accounts that exceed the limit of consecutive authentication failures, the security of logging into intelligent devices or systems when users forget the login password is further improved.

[0047] In some possible embodiments, the step of performing encryption processing on the current login password to obtain the encrypted information includes:

[0048] selecting a target encryption rule from preset multiple encryption rules to perform encryption processing on the current login password, to obtain the encrypted information, and recording an encryption identifier corresponding to the target encryption rule;

[0049] the step of generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string specifically includes:

[0050] generating a request string based on the encrypted information, the encryption identifier, and the preset request interface, so that the user forwards the encrypted information and the encryption identifier to the security server based on the request string; and

[0051] the security server is configured for:

[0052] receiving the encrypted information and the encryption identifier forwarded by the user, acquiring a corresponding target decryption rule based on the encryption identifier, parsing the encrypted information based on the target decryption rule to obtain the corresponding current login password, and feeding back the current login password to the user.

[0053] In the embodiments of the present disclosure, by dynamically selecting an encryption rule to encrypt login passwords and other information, the security of logging into intelligent devices or systems when users forget the login password is further enhanced.

[0054] The embodiments of the present disclosure provide an apparatus for authenticating login system, including:

[0055] a password encryption module, configured for responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information; and

[0056] a login authentication module, configured for receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

[0057] the to-be-authenticated login password is obtained by parsing the encrypted information.

[0058] The embodiments of the present disclosure further provide an electronic device, including a memory, a processor, and a computer program stored on the memory and executable on the processor. The processor, when executing the program, can implement the method described in any embodiment of the first aspect.

[0059] The embodiments of the present disclosure further provide a computer-readable storage medium, wherein the computer-readable storage medium stores the computer program. The computer program, when executed by the processor, can implement the method described in any embodiment of the first aspect.

[0060] The embodiments of the present disclosure further provide a computer program product, wherein the computer program product stores the computer program. The computer program, when executed by the processor, can implement the method described in any embodiment of the first aspect.

BRIEF DESCRIPTION OF DRAWINGS

[0061] In order to more clearly illustrate the technical solutions of the embodiments of the present disclosure, the following will briefly introduce the drawings used in the embodiments of the present disclosure. It should be understood that the following drawings only show some embodiments of the present disclosure, and therefore it should not be regarded as a limitation on the scope. Those ordinary skilled in the art can also obtain other related drawings based on these drawings without inventive effort.

[0062] FIG. 1 is a flowchart of a method for authenticating login system provided by the embodiment of the present disclosure;

[0063] FIG. 2 is an interaction system architecture diagram of a method for authenticating login system provided in the embodiments of the present disclosure;

[0064] FIG. 3 is a structural schematic diagram of an apparatus for authenticating login system provided in the embodiments of the present disclosure; and

[0065] FIG. 4 is a structural schematic diagram of an electronic device provided by the embodiment of the present disclosure.

DETAILED DESCRIPTION OF EMBODIMENTS

[0066] The technical solutions in the embodiments of the present disclosure will be described below with reference to the drawings in the embodiments of the present disclosure.

[0067] It should be noted that similar numerals and letters denote similar terms in the following drawings so that once an item is defined in one drawing, it does not need to be further discussed in subsequent drawings. Additionally, in the description of the present disclosure, the terms "first", "second", and the like are only used for distinguishing descriptions, and cannot be understood as indicating or implying relative importance.

[0068] As shown in FIG. 1, the embodiments of the present disclosure provide a method for authenticating login system, which can include the following steps.

[0069] S1: responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information.

[0070] It should be noted that the method for authenticating login system in the embodiments of the present disclosure can be executed by an intelligent device or system. The intelligent device or system can be any device or system with processing functions, such as a smart wristband, household smart appliances, Internet of Things (IoT) devices, or network devices. The target system refers to the management program within the intelligent device or system.

[0071] Optionally, when a user needs to log in to the management program (target system) of an intelligent device or system but forgets the login password, the user can initiate a request to obtain the login password (i.e., login password acquisition request) to the intelligent device or system. Exemplarily, the user can initiate the login password acquisition request by clicking the "Forgot Password" button through the visual interface of the intelligent device or system.

[0072] After receiving the login password acquisition request of the user, the intelligent device or system obtains the current login password used to log in to the target system from the local. The current login password can be a previously set fixed password or an instantaneously generated random password.

[0073] Then, the current login password is encrypted to obtain encrypted information.

[0074] The encryption process can be implemented using a symmetric encryption algorithm or an asymmetric encryption algorithm (public key and private key) pre-agreed with the security server (e.g., a pre-configured cloud server) so that the security server can parse the encrypted information through a corresponding decryption strategy.

[0075] S2: receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

[0076] the to-be-authenticated login password is obtained by parsing the encrypted information.

[0077] In one possible embodiment, the encrypted information is parsed through a local security decryption program to obtain the to-be-authenticated login password.

[0078] In another possible embodiment, the user forwards the encrypted information to the security server, and the security server parses the encrypted information, thereby obtaining the to-be-authenticated login password.

[0079] It should be noted that after the intelligent device or system generates the encrypted information, the encrypted information can be displayed on the visual interface of the intelligent device or system; optionally, the encrypted information can also be displayed through the Web end (e.g., a management host) connected to the intelligent device or system. Then, the user can obtain the encrypted information through some communication method (e.g., a mobile terminal such as a phone) and forward the encrypted information to the security server, where the security server parses the information and returns the corresponding login password. Exemplarily, the encrypted information can be a string, and the user can send the string to the security server via a URL request from the mobile terminal or Web end to request the security server to parse the string.

[0080] Exemplarily, the security server can use the decryption algorithm corresponding to the encryption algorithm to parse the encrypted information to obtain the current login password, and then feedback the current login password to the user.

[0081] Exemplarily, the security server can directly return the decrypted current login password back through the same path via which the user sent the encrypted information.

[0082] Optionally, the encrypted information can contain a device identifier. Thus, after the security server parses the encrypted information to obtain the current login password and device identifier, the security server can provide feedback on the current login password to the target mobile terminal corresponding to the registration terminal number based on the registered terminal number corresponding to the device identifier.

[0083] Optionally, the encrypted information can also comprise a target terminal number. In this case, after the security server parses the encrypted information to obtain the current login password and target terminal number, the security server can directly send the current login password to the target mobile terminal corresponding to the target terminal number.

[0084] If the user carries the target mobile terminal corresponding to the registered terminal number (target terminal number), once the target mobile terminal obtains the login password returned by the security server, the user, based on the login password, can input the login password into the intelligent device or system for login authentication. At this time, the intelligent device or system receives the login password input by the user (the to-be-authenticated login password) and authenticates the to-be-authenticated login password based on the current login password recorded locally. Exemplarily, if the to-be-authenticated login password is consistent with the current login password, the authentication is successful, and the user is allowed to log in to the target system. Otherwise, the authentication fails, and the user is denied login.

[0085] In the embodiments of the present disclosure, by acquiring the current login password locally on the intelligent device or system and encrypting it, allowing the user to forward the encrypted information to the security server for decryption and obtaining the corresponding login password, the method not only ensures the security of the login password acquisition but also eliminates the need for the intelligent device or system to establish a communication connection with the mobile terminal and the security server to log in to the intelligent device or system, thereby effectively improving the convenience of logging in to the intelligent device or system when the user forgets the login password.

[0086] It should be noted that because the login password is encrypted on the intelligent device or system side and decrypted on the security server side, and ciphertext transmission is used

during the transmission process, the security of the login password during the transmission process is ensured. In addition, to enhance the reliability of encryption and decryption, a public-private key method can be used to perform the encryption and decryption of the login password. Optionally, public key encryption is used on the intelligent device or system side, and private key decryption is used on the security server side. This way, even if the intelligent device or system is cracked, as long as the private key on the security server side is not leaked, the confidentiality of the information during the password retrieval process can still be ensured.

[0087] In some possible embodiments, before the step S2, the method can further include:

[0088] S101: generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string.

[0089] It should be noted that the request string used to request the security server, such as a URL (uniform resource locator), can be generated locally on the intelligent device or system. Exemplarily, the encrypted information can be used as an API parameter and combined with a preset request interface (the request API of the security server) to generate the request string. Then, the user can directly initiate a connection request to the security server using the request string and forward the encrypted information to the security server.

[0090] Exemplarily, the intelligent device or system can display the generated request string, and the user can manually input the request string on the mobile terminal they hold (or use text recognition after taking a photo) to trigger a request to the security server. Alternatively, the intelligent device or system can send the request string to the mobile terminal of the user through wired or wireless methods (such as Bluetooth or hotspot network), thus enabling the mobile terminal of the user to trigger a request to the security server.

[0091] Based on this, by presetting the request interface locally on the intelligent device or system, the request string related to the encrypted information can be generated locally on the intelligent device or system without constructing and generating the request string at the mobile terminal of the user. This further improves the efficiency and reliability of forwarding the encrypted information.

[0092] In some possible embodiments, the step S101 of generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string can include the following step.

[0093] S1011: generating a request string based on the encrypted information and the preset request interface, and converting the request string into a graphical recognition code, so that the user, after scanning the graphical recognition code using a carried mobile terminal,

forwards the encrypted information to the security server based on the request string obtained by parsing the graphical recognition code.

[0094] Optionally, after the intelligent device or system generates the request string related to the encrypted information locally, it can further convert the request string into a graphical recognition code (e.g., QR code) and display it. Since the request string can be a URL string carrying the encrypted information, the user can use their mobile terminal to scan and parse the graphical recognition code, which will automatically connect to the URL corresponding to the graphic recognition code, thereby establishing a direct connection with the security server and sending the encrypted information. Upon receiving the corresponding API request, the security server can extract the encrypted information, parse it, and provide feedback on the login password to the target mobile terminal corresponding to the registered number.

[0095] Based on this, by scanning the recognition code to identify the request string, automatically connecting to the security server, and sending the encrypted information, the flexibility of forwarding the encrypted information is significantly improved, which is beneficial for further enhancing the convenience of retrieving the login password.

[0096] In some possible embodiments, the encrypted information is obtained by performing encryption processing on the current login password and a device identifier of the target system; and

[0097] the security server is configured for:

[0098] receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and device identifier; and

[0099] obtaining a registered terminal number bound to the device identifier based on a pre-stored registration information database, and sending the current login password to a target mobile terminal corresponding to the registered terminal number.

[00100] It should be noted that in scenarios where the intelligent device or system supports only a single user management, the device identifier is bound in a one-to-one relationship with the user, and the security server can parse and manage the login passwords for different intelligent devices or systems using the device identifier.

[00101] Optionally, after the security server parses the encrypted information forwarded by the user, obtaining the corresponding current login password and device identifier, it can look up the registered terminal number bound to the device identifier in the pre-stored registration information database. Based on the registered terminal number, the current login password is sent to the corresponding target mobile terminal. If the user holds the target mobile terminal corresponding to the registered terminal number, the user can retrieve the current login

password feedback from the security server via the target mobile terminal. The registration information database stores information about different device identifiers and their corresponding registered terminal numbers.

[00102] In some possible embodiments, in scenarios where the intelligent device or system supports multiple user management, multiple user accounts can be registered and bound to the same device identifier.

[00103] Optionally, when registering the administrator account, a username (user account) field needs to be added. Based on this, the registration information database can store different device identifiers and their corresponding registered terminal numbers bound to different usernames. Correspondingly, in the process of retrieving the login password, when the user initiates a login password acquisition request for the target system, they need to input the username field. The intelligent device or system then encrypts the username, device identifier, and the corresponding current login password (associated with the username) to generate encrypted information. After parsing and obtaining the username, device identifier, and corresponding current login password, the security server first looks up the registered terminal number information of the corresponding user and device in the pre-stored registration information database based on the username and device identifier, and sends the current login password based on the registered terminal number.

[00104] Thus, by setting up the registration information database to bind and store registration information for different devices and accounts, the system can manage login passwords for different devices and user accounts, further enhancing the flexibility of login authentication for intelligent devices.

[00105] In some possible embodiments, the encrypted information is obtained by performing encryption processing on the current login password and a target terminal number preset in the target system; and

[00106] the security server is configured for:

[00107] receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and target terminal number; and

[00108] sending the current login password to a target mobile terminal corresponding to the target terminal number.

[00109] It should be noted that in some possible embodiments, in addition to encrypting the device identifier and forwarding it to the security server, where the security server determines the target mobile terminal based on the decrypted device identifier, the intelligent device or system can also directly retrieve the pre-stored target terminal number corresponding to the

administrator locally. The target terminal number can then be encrypted along with the current login password, and the encrypted information is forwarded by the user to the security server. After receiving and parsing the encrypted information, the security server can directly send feedback on the current login password to the corresponding target mobile terminal based on the target terminal number.

[00110] In this scenario, the intelligent device or system can locally store one or more target terminal numbers corresponding to the administrator(s). If there are multiple target terminal numbers for different administrators, when the user initiates a login password acquisition request, they can input their user account. The intelligent device or system can then retrieve the target terminal number of the corresponding administrator based on the user account, which will be used to encrypt the current login password. Correspondingly, the current login password can be a randomly generated login password or a preset login password corresponding to the user account input by the user.

[00111] In some possible embodiments, the method for authenticating login system can further include the following steps.

[00112] S3: responding to an account registration request of the user for the target system, acquiring a to-be-registered terminal number specified by the account registration request, and performing encryption processing on the to-be-registered terminal number and the device identifier of the target system to obtain registration encrypted information; and

[00113] the security server is configured for:

[00114] receiving the registration encrypted information forwarded by the user, and parsing the registration encrypted information to obtain a corresponding to-be-registered terminal number and device identifier; and

[00115] sending authentication information to the mobile terminal corresponding to the to-be-registered terminal number to perform identity authentication on the to-be-registered terminal number, and after the identity authentication is successfully completed, binding and storing the to-be-registered terminal number and the device identifier in the registration information database.

[00116] It should be noted that during the user account registration process, an interactive process similar to steps S1 to S2 can be set up. Optionally, when a user needs to register an administrator account for the target system, they can initiate an account registration request on the intelligent device or system and input the desired mobile number (in a scenario where a single device supports multiple user management, the user also needs to input the desired username for registration). The intelligent device or system then retrieves the to-be-registered

terminal number input by the user based on the account registration request submitted by the user, and performs encryption processing on the to-be-registered terminal number and the device identifier of the current intelligent device or system, thus generating registration encrypted information.

[00117] Subsequently, the user forwards the registration encrypted information to the security server through a communication method (e.g., by connecting via a URL request using their mobile terminal). For example, the user can input the registration encrypted information on the mobile terminal or scan a QR code (generated by converting from the registration encrypted information) using the mobile terminal to forward the registration encrypted information to the security server via a URL request.

[00118] The security server, after receiving the registration encrypted information forwarded by the user, parses the registration encrypted information using the corresponding decryption algorithm based on the encryption and decryption protocol predetermined by the intelligent device, thus obtaining the to-be-registered terminal number and the device identifier. Then, exemplarily, the security server can send a random verification code to the corresponding target mobile terminal based on the to-be-registered terminal number and, at the same time, return a verification page for inputting the verification code via the original path of the link through which the user forwarded the registration encrypted information. If the user holds the to-be-registered terminal number corresponding to the target mobile terminal, the user can receive the random verification code through the target mobile terminal, input the verification code on the verification page, and submit the verification code to the security server. Finally, the security server authenticates the identity of the current registered user by comparing the verification code input by the user with the previously generated random verification code for consistency. Upon successful authentication, the security server binds and stores the to-be-registered terminal number requested by the user and the device identifier in the registration information database.

[00119] In the embodiments of the present disclosure, in the step S1, responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information can include the following steps.

[00120] S111: responding to the login password acquisition request of the user for the target system, acquiring a preset login password corresponding to a target account based on the target account specified by the login password acquisition request as the current login password of the target system.

[00121] S112: performing encryption processing on the target account and the current login password to obtain the encrypted information.

[00122] It should be noted that when the intelligent device or system responds to the login password acquisition request of the user for the target system, it can use the login password that has been preset and recorded as the current login password of the target system.

[00123] Optionally, in scenarios where the intelligent device or system supports the management of multiple user accounts, different users can register and set corresponding login passwords for the same intelligent device or system. When the password is forgotten and needs to be retrieved, the user can input their registered username (target account) when initiating the login password acquisition request. The intelligent device or system can then obtain the corresponding preset login password that has been pre-recorded based on the target account and use it as the current login password of the target system. After the password is encrypted and decrypted by the security server, the user can retrieve the previously set login password and use it to log into the target system.

[00124] Based on this, by implementing login authentication for the intelligent device in the form of password retrieval, login authentication for multiple user account management scenarios can be achieved, further improving the convenience of logging into the intelligent device or system when the user forgets the login password.

[00125] In the embodiments of the present disclosure, in the step S1, responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system can include the following steps.

[00126] S121: responding to the login password acquisition request of the user for the target system, and generating a random login password based on a preset random algorithm as the current login password of the target system.

[00127] It should be noted that in the case where the user forgets the password, in addition to logging into the target system through the password retrieval method, it is also possible to log into the target system by obtaining a random password.

[00128] Optionally, when responding to the login password acquisition request of the user for the target system, the intelligent device or system can generate a random login password based on a preset random algorithm, which will serve as the current login password of the target system. In this way, the intelligent device or system does not need to distinguish between different user accounts to retrieve the password but instead uses the random password method to achieve system login authentication, thus further improving the convenience of logging into the intelligent device or system when the user forgets the login password. At the same time, by

generating a random password, the risk of a preset password being cracked or stolen by other users is avoided, thus further enhancing the security of login authentication for the intelligent device or system.

[00129] In some possible embodiments, the method for authenticating login system can further include the following step.

[00130] S4: resetting the current login password of the target system, after generating the random login password and when a to-be-authenticated login password that is consistent with the random login password is not received within a preset valid duration.

[00131] It should be noted that in the scenario where random login passwords are used for login authentication, in order to further enhance the security of the login authentication, an effective login time limit can also be set.

[00132] Optionally, each time a random login password is generated, the timer starts. If the login is not successfully authenticated within the preset valid time, meaning that a to-be-authenticated login password consistent with the current random login password is not received within the preset valid time, the current login password of the target system is reset.

[00133] Resetting the current login password of the target system can include regenerating a random login password and using the new random login password as the current login password, or resetting the current login password of the target system to a preset fixed password. In this case, even if the user obtains the previously generated random login password, they will not be able to pass the authentication of the target system. If the user wishes to continue retrieving the password to log into the system, they must initiate a new request to obtain the login password.

[00134] Based on this, by setting a validity period for the random login password and rendering the current random login password invalid when authentication is not successfully completed within the timeout period, the security of login authentication for the intelligent device or system is further enhanced.

[00135] In some possible embodiments, the method for authenticating login system can further include the following step.

[00136] S5: locking the login account of the user when a number of failed authentication attempts for the to-be-authenticated login password input by the user based on the current login password exceeds a preset threshold.

[00137] It should be noted that in order to prevent brute-force attacks, a login authentication protection strategy can also be set. Optionally, after the user initiates the process of retrieving the password, if a number of failed authentication attempts for the to-be-authenticated login

password input by the user based on the current login password exceeds a preset limit threshold, the login account of the user will be locked.

[00138] Optionally, once the login account of the user is locked, a preset lockout time can be set, for example, three days. During this lockout period, the user will not be able to log into the system using that login account. Additionally, a function to unlock the locked account can be set. After the login account of the user is locked, the user can request authentication and unlock via other higher-level security verification methods (such as manual appeal).

[00139] Based on this, by locking the user account after exceeding the limit of consecutive authentication failures, the occurrence of brute-force attacks can be effectively prevented, thereby further enhancing the security of login authentication for the intelligent device or system.

[00140] In some possible embodiments, in the step S1, performing encryption processing on the current login password to obtain the encrypted information can include:

[00141] selecting a target encryption rule from preset multiple encryption rules to perform encryption processing on the current login password, to obtain the encrypted information, and recording an encryption identifier corresponding to the target encryption rule.

[00142] The step S101, generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string, specifically includes:

[00143] generating a request string based on the encrypted information, the encryption identifier, and the preset request interface, so that the user forwards the encrypted information and the encryption identifier to the security server based on the request string; and

[00144] the security server is configured for:

[00145] receiving the encrypted information and the encryption identifier forwarded by the user, acquiring a corresponding target decryption rule based on the encryption identifier, parsing the encrypted information based on the target decryption rule to obtain the corresponding current login password, and feeding back the current login password to the user.

[00146] It should be noted that during each encryption process, one of the multiple locally preset encryption rules (or algorithms) can also be selected. Then, the user will forward the currently used encryption rule information (encryption identifier) along with the encrypted information to the security server, thus allowing the security server to retrieve the corresponding decryption rule (or algorithm) based on the encryption identifier and perform decryption on the current encrypted information.

[00147] Based on this, by using different encryption rules to encrypt information such as the login password during the process of retrieving the password, the security of logging into the intelligent device or system is further enhanced when the user forgets the login password.

[00148] As shown in FIG. 2, by way of example, the method for authenticating login system in the embodiments of the present disclosure mainly involves the interaction between the following three parts: the intelligent device or system, the mobile phone, and the security server.

[00149] As an example, the method for authenticating login system in the embodiments of the present disclosure can be implemented through the following steps:

[00150] 1. in response to the request to retrieve the password initiated by the user, the program in the intelligent device or system randomly generates a login password, then encrypts the login password and device identifier (or mobile phone number) to obtain an encrypted string;

[00151] 2. the encrypted string is used as an API parameter, and the API parameter is combined with the corresponding request API of the security server to form a request URL string to be sent to the security server;

[00152] 3. the request URL string is converted into a QR code and displayed via the Web interface;

[00153] 4. the user (administrator) uses the mobile phone to scan the QR code;

[00154] 5. after scanning the QR code, the mobile phone automatically connects to the corresponding URL and transmits the corresponding encrypted string to the security server;

[00155] 6. after receiving the corresponding API request, the security server retrieves the encrypted string from the request and decrypts it to obtain the device identifier (or mobile phone number) and the login password;

[00156] 7. the security server notifies the administrator of the login password via a reliable channel. For example: based on the device identifier, the pre-registered mobile phone number is retrieved (or the mobile phone number is directly parsed from the encrypted string), and then a text message is sent to the mobile phone number to inform the login password; or, the login password is orally communicated after confirming the identity of the administrator, etc.;

[00157] 8. after receiving the login password, the administrator uses the login password to log into the intelligent device or system; and

[00158] 9. after receiving the login password input by the administrator, the intelligent device or system compares it with the previously determined login password; if they match, authentication is successful and the administrator is allowed to log into the system; otherwise, login is rejected.

[00159] Referring to FIG. 3, FIG. 3 shows a block diagram of the composition of an apparatus for authenticating login system provided in some embodiments of the present disclosure. It should be understood that the apparatus for authenticating login system corresponds to the method embodiment in FIG. 1 and is capable of executing each step involved in the method embodiment described above. The specific functions of the apparatus for authenticating login system can be referred to in the preceding description. To avoid repetition, detailed descriptions are appropriately omitted here.

[00160] The apparatus for authenticating login system in FIG. 3 includes at least one software function module that can be stored in the memory in the form of software or firmware or embedded in the apparatus for authenticating login system. The apparatus for authenticating login system includes:

[00161] a password encryption module 310, configured for responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, performing encryption processing on the current login password to obtain encrypted information; and

[00162] a login authentication module 320, configured for receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

[00163] the to-be-authenticated login password is obtained by a security server parsing the encrypted information and feeding back after the user forwards the encrypted information to the security server.

[00164] It can be understood that the apparatus embodiment described above corresponds to the method embodiment of the present disclosure, and the apparatus for authenticating login system provided by the embodiments of the present disclosure can implement the method for authenticating login system provided by any method embodiment of the present disclosure.

[00165] It will be clear to those skilled in the field that, for the convenience and brevity of the description, the specific working processes of the apparatus described above can be referred to the corresponding processes in the preceding method embodiments and will not be repeated here.

[00166] As shown in FIG. 4, some embodiments of the present disclosure provide an electronic device 400, and the electronic device 400 includes: a memory 410, a processor 420, and a computer program stored on the memory 410 and executable on the processor 420, wherein the processor 420 reads the program from the memory 410 via a bus 430 and executes the

program, thereby implementing the method included in any embodiment of the method for authenticating login system described above.

[00167] The processor 420 can process digital signals and can include various computational structures, such as a complex instruction set computer architecture, a reduced instruction set computer architecture, or a structure that implements a combination of multiple instruction sets. In some examples, the processor 420 can be a microprocessor.

[00168] The memory 410 can be configured to store instructions executed by the processor 420 or data related to the execution of those instructions. These instructions and/or data can include code for implementing some or all of the functions of one or more modules described in the embodiments of the present disclosure. The processor 420 of the embodiment of the present disclosure can be configured to execute instructions in the memory 410 to implement the method described above. The memory 410 includes dynamic random-access memory, static random-access memory, flash memory, optical storage, or other memory known to those skilled in the art.

[00169] Some embodiments of the present disclosure further provide a computer-readable storage medium, wherein a computer program is stored on the computer-readable storage medium, and the computer program, when executed by a processor, performs the method described in the method embodiment.

[00170] Some embodiments of the present disclosure further provide a computer program product, wherein the computer program product, when executed on a computer, enables the computer to perform the method described in the method embodiment.

[00171] It should be noted that each embodiment described in the summary is progressively elaborated upon, with each embodiment focusing on the differences from the others. The identical or similar parts between the various embodiments can be cross-referenced as needed. For the apparatus-type embodiments, since they are essentially similar to the method embodiments, the description is relatively simple, and the relevant details can be referred to in the description of the method embodiments.

[00172] In the several embodiments provided in the present disclosure, it should be understood that the devices and methods disclosed can be implemented in other ways. The device embodiments described above are merely illustrative. For example, the flowcharts and diagrams in the drawings illustrate possible implementations, architectures, functions, and operations of devices, methods, and computer program products according to multiple embodiments of the present disclosure. At this point, each box in the flowchart or diagram can represent a module, program segment, or part of the code. Each part of the module, program

segment, or code includes one or more executable instructions for implementing the specified logical functions. It should also be noted that in some alternative implementations, the functions indicated in the boxes may occur in a different order than those indicated in the drawings. For example, two consecutive boxes can actually be executed in parallel, and sometimes they can also be executed in reverse order, depending on the functionality involved. It should also be noted that each box in the block diagram and/or flowchart, and the combination of boxes in the block diagram and/or flowchart, can be implemented by specialized hardware systems designed to perform the specified functions or actions, or by a combination of specialized hardware and computer instructions.

[00173] Further, each functional module in each embodiment of the present disclosure can be integrated together to form a separate part, or each module may exist separately, or two or more modules may be integrated to form a separate part.

[00174] The functionality, when implemented as a software functional module and sold or used as a stand-alone product, can be stored in a computer-readable storage medium. Based on this understanding, the technical solution of the present disclosure can essentially be embodied in the form of a software product, which contributes to or includes parts in the prior art. The software product is stored in a storage medium and includes multiple instructions for causing a computer device (which can be a personal computer, server, network device, etc.) to execute all or some of the steps of the methods described in various embodiments of the present disclosure. The aforementioned storage media include various media that can store program code, such as USB drives, external hard drives, read-only memory (ROM), random access memory (RAM), disks, or optical discs.

[00175] The above is only an embodiment of the present disclosure, which is not intended to limit the scope of protection of the present disclosure, and the present disclosure can have various changes and variations for those skilled in the art. Any modification, equivalent substitution, improvement, etc. made within the spirit and principles of the present disclosure shall be included in the scope of protection of the present disclosure. It should be noted that similar numerals and letters denote similar terms in the following drawings so that once an item is defined in one drawing, it does not need to be further discussed in subsequent drawings.

[00176] The above are only specific embodiments of the present disclosure, but the scope of protection of the present disclosure is not limited thereto. Any person skilled in the art can easily envisage changes or substitutions within the technical scope disclosed in the present disclosure, which should be encompassed within the scope of protection of the present

disclosure. Therefore, the scope of protection of the present disclosure shall be stated to be subject to the scope of protection of the claims.

[00177] It is important to note that, in the context, relationship terms such as first and second are used only to distinguish one entity or operation from another entity or operation, without necessarily requiring or implying any such actual relationship or order between those entities or operations. Furthermore, the terms “comprise”, “include”, or any other variations are intended to encompass non-exclusive inclusion. This allows a process, method, item, or device that includes a series of elements to not only include those elements but also include other elements that are not explicitly listed, or elements that are inherent to the process, method, item, or device. In the absence of further limitations, the inclusion of an element specified by the phrase "comprising a..." does not exclude the presence of additional identical elements in the process, method, article, or apparatus that includes the specified element.

INDUSTRIAL PRACTICALITY

[00178] The embodiments of the present disclosure provide a method, an apparatus, a device, and a storage medium for authenticating a login system, which can improve the convenience of users logging into an intelligent device or system when they forget the login passwords while ensuring security.

CLAIMS

1. A method for authenticating a login system, comprising:

responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, and performing encryption processing on the current login password to obtain encrypted information;

receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

the to-be-authenticated login password is obtained by parsing the encrypted information.

2. The method for authenticating the login system according to claim 1, before the step of receiving a to-be-authenticated login password input by the user, further comprising:

generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string and the security server parses the encrypted information to obtain the to-be-authenticated login password.

3. The method for authenticating the login system according to claim 2, wherein the step of generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string comprises:

generating the request string based on the encrypted information and the preset request interface, and converting the request string into a graphical recognition code, so that the user, after scanning the graphical recognition code using a carried mobile

terminal, forwards the encrypted information to the security server based on the request string obtained by parsing the graphical recognition code.

4. The method for authenticating the login system according to claim 2, wherein the encrypted information is obtained by performing encryption processing on the current login password and a device identifier of the target system; and

the security server is configured for:

receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and device identifier; and

obtaining a registered terminal number bound to the device identifier based on a pre-stored registration information database, and sending the current login password to a target mobile terminal corresponding to the registered terminal number.

5. The method for authenticating the login system according to claim 2, wherein the encrypted information is obtained by performing encryption processing on the current login password and a target terminal number preset in the target system; and

the security server is configured for:

receiving the encrypted information forwarded by the user, and parsing the encrypted information to obtain a corresponding current login password and target terminal number; and

sending the current login password to a target mobile terminal corresponding to the target terminal number.

6. The method for authenticating the login system according to claim 4, further comprising:

responding to an account registration request of the user for the target system, acquiring a to-be-registered terminal number specified by the account registration request, and performing encryption processing on the to-be-registered terminal number and the device identifier of the target system to obtain registration encrypted information; and

the security server is further configured for:

receiving the registration encrypted information forwarded by the user, and parsing the registration encrypted information to obtain a corresponding to-be-registered terminal number and device identifier; and

sending authentication information to a mobile terminal corresponding to the to-be-registered terminal number to perform identity authentication on the to-be-registered terminal number, and after the identity authentication is successfully completed, binding and storing the to-be-registered terminal number and the device identifier in the registration information database.

7. The method for authenticating the login system according to claim 1, wherein the step of responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, and performing encryption processing on the current login password to obtain encrypted information comprises:

responding to the login password acquisition request of the user for the target system, acquiring a preset login password corresponding to a target account based on the target account specified by the login password acquisition request as the current login password of the target system; and

performing encryption processing on the target account and the current login password to obtain the encrypted information.

8. The method for authenticating the login system according to claim 1, wherein the step of responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system comprises:

responding to the login password acquisition request of the user for the target system, and generating a random login password based on a preset random algorithm as the current login password of the target system.

9. The method for authenticating the login system according to claim 8, further comprising:

resetting the current login password of the target system, after generating the random login password and when a to-be-authenticated login password that is consistent with the random login password is not received within a preset valid duration.

10. The method for authenticating the login system according to claim 1, further comprising:

locking a login account of the user when a number of failed authentication attempts for a to-be-authenticated login password input by the user based on the current login password exceeds a preset threshold.

11. The method for authenticating the login system according to claim 2, wherein the step of performing encryption processing on the current login password to obtain the encrypted information comprises:

selecting a target encryption rule from preset multiple encryption rules to perform encryption processing on the current login password, to obtain the encrypted information, and recording an encryption identifier corresponding to the target encryption rule;

the step of generating a request string based on the encrypted information and a preset request interface, so that the user forwards the encrypted information to the security server based on the request string comprises:

generating the request string based on the encrypted information, the encryption identifier, and the preset request interface, so that the user forwards the encrypted

information and the encryption identifier to the security server based on the request string; and

the security server is configured for:

receiving the encrypted information and the encryption identifier forwarded by the user, acquiring a corresponding target decryption rule based on the encryption identifier, parsing the encrypted information based on the target decryption rule to obtain the corresponding current login password, and feeding back the current login password to the user.

12. An apparatus for authenticating a login system, comprising:

a password encryption module, configured for responding to a login password acquisition request of a user for a target system, acquiring a current login password of the target system, and performing encryption processing on the current login password to obtain encrypted information; and

a login authentication module, configured for receiving a to-be-authenticated login password input by the user, authenticating the to-be-authenticated login password based on the current login password, and determining whether to allow the user to log in to the target system according to an authentication result, wherein

the to-be-authenticated login password is obtained by parsing the encrypted information.

13. An electronic device, comprising a memory, a processor, and a computer program stored in the memory and executable on the processor, wherein when the processor executes the program, the method for authenticating the login system according to any one of claims 1 to 11 is capable of being implemented.

14. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and the computer program, when run by a

processor, performs the method for authenticating the login system according to any one of claims 1 to 11.