Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6245397, 10 pages
https://doi.org/10.1155/2022/6245397

Research Article

Issues of Clinical Identity Verification for Healthcare Applications over Mobile Terminal Platform

Sultan Ahmad,[1] Hikmat A. M. Abdeljaber,[2] Jabeen Nazeer,[1] Mohammed Yousuf Uddin,[3] Velmurugan Lingamuthu,[4] and Amandeep Kaur[5]

[1]*Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, P.O. Box. 151, Alkharj 11942, Saudi Arabia*
[2]*Department of Computer Science, Faculty of Information Technology, Applied Science Private University, Amman, Jordan*
[3]*Department of Information System, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, P.O. Box. 151, Alkharj 11942, Saudi Arabia*
[4]*Department of Computer Science, School of Informatics and Electrical Engineering, Hachalu Hundesa Campus, Ambo University, Ethiopia*
[5]*University Centre for Research and Development, Department of Computer Science and Engineering, Chandigarh University, Gharuan, Mohali, India*

Correspondence should be addressed to Velmurugan Lingamuthu; velmurugan.lingamuthu@ambou.edu.et

Received 22 February 2022; Revised 15 March 2022; Accepted 19 March 2022; Published 19 April 2022

Academic Editor: Yuanlong Cao

According to recent research, attacks on USIM cards are on the rise. In a 5G setting, attackers can also employ counterfeit USIM cards to circumvent the identity authentication of specified standard applications and steal user information. Under the assumption that the USIM can be replicated, the identity authentication process of common mobile platform applications is investigated. The identity authentication tree is generated by examining the application behavior of user login, password reset, and sensitive operations. We tested 58 typical applications in 7 categories, including social communication and personal health. We found that 29 of them only needed the SMS verification code received by the USIM card to pass the authentication. In response to this problem, it is recommended to enable two-step verification and use USIM anti-counterfeiting methods to complete the verification.

1. Introduction

USIM (Global User Identity Module) [1] is widely used as an identification module for user identity in UMTS (Universal Mobile Telecommunication System) networks and is commonly used in various mobile devices to provide users with authentication services, short message services, etc. Compared with the SIM (Subscriber Identity Module), the USIM Card has been upgraded in application support and security. While the USIM card supports 3G/4G services, it is backward compatible with the 2G network supported by the SIM card. In the increasingly mature 5G network, the USIM card will play a more important role in entity authentication and information exchange.

The promotion of mobile devices and the development of mobile applications complement and promote each other. As of the third quarter of 2019, data from the National Bureau of Statistics show that the number of 4G mobile phone users in my country has increased by 10.1% year-on-year, and mobile Internet access traffic has increased by 34.9% year-on-year [2].

At the same time, 130,000 5G base stations have been built, and 5G communication technology and commercialization have ushered in rapid development. Globally, in

2018, users all over the world downloaded a total of 194 billion mobile applications (Apps), covering financial payment, social communication, travel, entertainment, audio and video applications, etc., of which online financial payment applications have developed rapidly. The number of user downloads has increased by 27.8% compared with 2017 [3, 4]. The subsequent data privacy risks continue to grow. Mobile devices equipped with USIM cards and the applications in them have become a part of people's lives. These applications often have operating rights for sensitive user information and authenticate the logged-in user's identity. When implementing identity authentication, SMS verification code has been widely used as a low-cost, easy-to-implement, and low-threshold verification method for users to learn. As a necessary carrier for receiving SMS verification codes, the USIM card will directly threaten the security of all USIM devices once it can be copied or forged, and it will inevitably pose a considerable threat to the identity authentication process of the App in the device and user privacy [5–7].

1.1. SIM/USIM Security Research Status. When a user uses a mobile device to communicate, the SIM/USIM card in the device needs to be authenticated and connected to the network first. Research shows that although the USIM card uses the MILENAGE algorithm to achieve two-way authentication [8, 9], and the SIM card uses the A3/A8 algorithm to achieve one-way authentication, they all face the possibility of being copied.

1.1.1. SIM/USIM Card Copy Attack. Miškovsky et al. [10] proposed a feasible differential power analysis (DPA) side-channel attack method based on the power signal difference in the USIM authentication process. In the MILENAGE algorithm, the differential power consumption analysis is performed by selecting the f5 function among them. The expected value of the round key used in the authentication parameter calculation and the OPc can be calculated with the help of the Pearson correlation coefficient [11]. Based on this, the attacker can complete the copy of the original USIM card within a few minutes only by using an oscilloscope, a smart card analyzer, and a personal computer and realize the authentication and normal communication with the AuC (Authentication Center) [12–14].

In addition, Saxena and Chaudhari [15] studied the A3/A8 algorithm based on COMP128, combined with the SRES response number of the A3 authentication algorithm to crack the pseudorandom number generator used by AuC, and can extract the customer authentication secret of AuC and SIM card.

A copy of the SIM card is now displayed. Tabassum [16] considered that the COMP128 authentication algorithm used by GSM (Global System for Mobile Communications) enables attackers to successfully extract the authentication key of SIM by brute force cracking and proposed the basic process and common methods for OTA copying of SIM cards. Xie et al. [17] proposed a side-channel attack method called partition attack, which can perform fast power consumption analysis on the divided lookup table structure in COMP128 to extract the authentication key. For CDMA technology, Chen et al. [18] analyzed the look-up table in the CAVE protocol and the cyclic shift operation in the AKA protocol and designed different power analysis methods, which cost a very short time on 8-bit microprocessors and SIM cards. Time can successfully extract the authentication key [19, 20].

In the 5G network environment, the AKA authentication protocol adopted by USIM is consistent with the main process and algorithm parameters of the 3G/4G AKA protocol in the NSA mode [21, 22]. Therefore, the security analysis methods and cracking methods of the USIM card in the 3G/4G environment are still effective in the 5G network [23, 24]. The above research shows that there are a large number of USIM cards that are easy to be copied in the domestic and foreign markets. Attackers only need to spend a few minutes of power consumption data collection time to achieve offline cracking and copying of the target user's USIM card. It only takes a few minutes to tens of minutes to complete the cracking and copying using a personal PC.

In order to deal with the risk of USIM cards being cracked by the abovementioned attack methods, many chip design companies at home and abroad have begun to study various chip protection methods and apply protection technologies to newly designed and taped-out USIM chips. However, compared with the repair of software vulnerabilities, the solution of chip security problems often requires the redesign and development of the chip and the tape out. This is undoubtedly a longer time. For the USIM chip, even if it has been produced with antiattack capability USIM cards, these chips must be widely used.

Operators are still required to carry out a large-scale recall or forced replacement of the issued USIM chips, which is obviously not feasible. This objectively causes a large number of USIM cards that can be copied to be used for a long time and widely in reality [25–27].

1.1.2. SMS Verification Code Application and Security. SMS verification codes have been widely used in authentication links such as logging in to applications on mobile platforms or resetting passwords. As a carrier and bridge for the USIM card to transmit information to the App, it represents the connection between a specific USIM card and the device holder. SMS verification code is essentially a time-based one-time password (TOTP, time-based one-time password) [28], and its architecture is shown in Figure 1.

The authentication and message transmission from MSC (Mobile Switching Center) to UE are often based on GSM or UMTS networks. In practice, attacks against SMS mostly occur during the authentication process between the device and the base station or after the user receives the SMS message. Yubo et al. [29] analyzed various SMS attack vectors and pointed out that installing malware on devices to steal data is a common attack method against SMS security. Kotkar and Game [30] implemented an attack method that allows the device to send SMS messages without user permission and prevents the device from receiving the messages. When the attacker uses the copied USIM card to

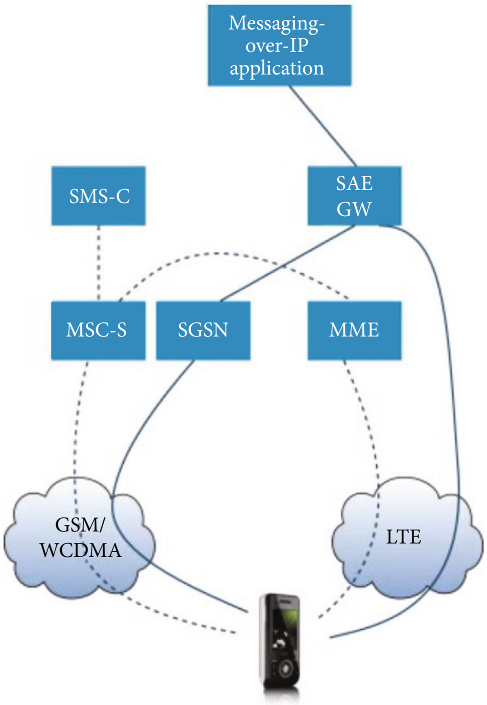

Figure 1: Overall structure of short message service (SMS) [7].

access the base station, he can receive the SMS verification code instead of the original user and complete the authentication process in the App.

1.2. The Main Work and Results of This Article. To avoid the security vulnerabilities or potential hazards of App applications created by the copied USIM card, the current practicable method is to update the App or security patches in a timely manner from the software level to compensate for the security risks caused by the usage of the copied USIM. In this context, this study analyzes and tests common apps in depth, identifying which apps have security issues when the USIM is duplicated and raising the alarm about the need for app updates and technology upgrades.

This article summarizes the general model of authentication for the general process of mobile application identity authentication and focuses on the analysis of possible security problems in the identity authentication strategy in the environment where the USIM card is copied. In an environment that simulates the USIM card being copied by an attacker, this paper studies the identity authentication link of 58 typical applications on the mobile terminal platform was tested, and the real machine test was carried out. The authentication process of application login, reset password, and sensitive operation was observed, and the application login data and jump process were analyzed and studied. The request-response data format and code execution process of these applications in the identity authentication process and finally recorded the use and performance of various security services (such as SMS verification codes) in the environment of copying the USIM card.

The test results found that 29 out of 58 applications have identity authentication services that can be directly bypassed in the environment where the USIM card is copied. Among them, 9 apps can be bypassed directly during password reset and login, 10 apps can be bypassed directly only during password reset, and the remaining 10 apps can be bypassed directly only during login. The test results in this article show that for applications that have identity authentication problems caused by USIM card copy attacks, mobile app developers, and security vendors should use at least two-step authentication and other software protection methods to avoid USIM card copy attacks on mobile applications and security risk.

2. Certification Process for Mobile Applications

Applications need to verify their identity before users perform functions. The identity authentication interfaces provided by various apps usually exist in user login, user reset the password, and performing sensitive operations. This section analyzes the general pattern of mobile application identity authentication and summarizes the users—identity verification tree.

2.1. Functional Scenarios of Identity Authentication. User login authentication: when a user accesses an application, the App needs to identify and authenticate the user's identity. User login usually requires a matching user name and password. The common user name types are usually user-defined strings, mailboxes, user mobile phone numbers, etc. After the password matches the user name, the current user will be allowed to log in. The general user login authentication process is shown in Figure 2. User reset password authentication: in practice, users forget their passwords from time to time, and user the application will also provide a password recovery function. After the user provides the correct user name, the authenticity of the username must be verified in conjunction with other information. The type of username determines the process of verifying identity. When using an email address or mobile phone number as a username, the application will send a verification email or SMS verification code. Only after the user receives the verification information and performs the corresponding operation will the password be allowed to reset, and some applications also adopt two-step verification and other means.

E-mail and mobile phones are an important part of daily life. Private mailbox letters and SMS verification codes are usually owned by individuals. Therefore, it is reasonable for application vendors to use them as necessary information for identity authentication, but some applications do not adopt additional verification methods to ensure current users. The correctness of the identity only guarantees the necessity of verification means. Once an external attacker manages to provide correct verification information, he can also reset the password and have the operation authority of the original user to achieve the purpose of the attack.

User authentication for sensitive operations: if a user performs certain sensitive operations after logging in, such as transferring money or viewing operation history, some applications will require the user to perform additional authentication, usually requiring the user to enter a PIN

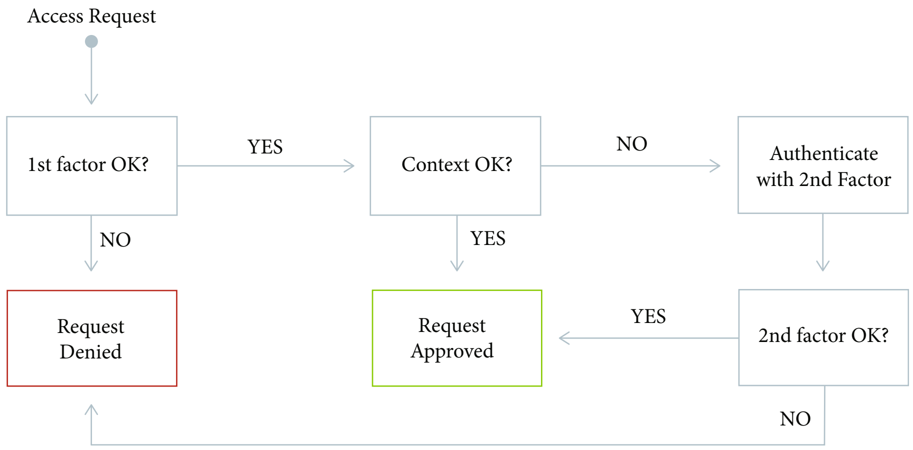

Figure 2: Procedure of authentication for App users logging in [12].

code, SMS verification code, or biometric verification. This measure can better protect the core business data. When personal financial apps involve banking services, it is often recommended that users turn on operation authentication to protect the safety of personal property.

2.2. The User Authentication Tree of the Application. According to the three common authentication processes in applications, this article can summarize the common user authentication trees in mobile applications. In the verification process, in order to achieve login applications, attackers can perform attacks on user login authentication and reset password authentication. In the process of user login authentication, potential logic vulnerabilities in the application can be used to initiate attacks; and in the process of resetting the password, there are many authentication methods involved, which also cause the attacker to have more attack originating points, such as SMS for USIM cards attack methods such as verification code security and email security. At the same time, because some applications have not developed a secondary verification process when resetting the password, the difficulty of the attack faced by the attacker is further reduced. Once the attacker successfully logs in to the application, and the application is not correct and sensitive operations are verified again, the attacker can obtain the response and use authority to steal user information.

3. Application Test of the Mobile Terminal Platform

This section adopts a field test method to examine the behavior of different applications in the certification process and introduces the standard test types and test techniques of mobile applications.

3.1. Mobile Application Testing and Analysis Technology. Common test types: various tests of mobile applications can help improve software quality to ensure long-term stable iterations of software versions. The main classification results of the test target and test method of the mobile application test method are shown in Figure 3.

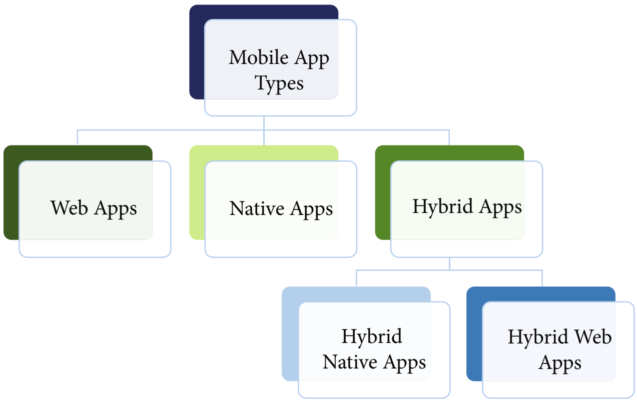

Figure 3: Classification of mobile applications [13].

Among them, functional testing examines the basic services, user interaction, and flexibility of the application. Safety testing, flow testing, power consumption testing, etc. have become necessary testing links in recent years [31]. Automated testing often uses a black box- (white box-) based automation framework to dynamically or statically analyze the product's modular units. In order to adapt to the rapid development and iteration of products, most manufacturers adopt automatic or semiautomatic testing methods.

Test analysis technology: the GUI automation framework API in the literature [32, 33] provides a common interface for the basic system functions of the mobile platform as the basis for other test functions. Testers write scripts through these APIs and use assert statements to test status information.

R&R-based test schemes such as “Reran” [34] and “Versatile” [35] may replace manual test scripts, and such methods can provide fine-grained capture and replay. The automatic input generation (AIG) technology [36] automates the generation process of test cases, which can improve code coverage, detect more errors, and reduce the scale of test programs. In addition, there are error reporting tools [37], equipment flow testing tools, etc.

Table 1: Tested mobile applications.

Category	Application composition
Social communication	WhatsApp, Messenger, Facebook, Instagram, Twitter, Skype, WeChat, Snapchat, Pinterest
Financial payment	Amazon, wish, eBay, Apple store, Walmart, Flipkart, cash, Paypal, Bank Internet Banking
Takeaway	Uber, Zomato, Parkmobile, Waze, UberEats, DoorDash, iFood, are you hungry
Health care	Keep, Nike Training Club, calm, pregnancy
File cloud disk	Dropbox, Google Drive, iCloud, Onedrive
Entertainment video	Youtube, TikTok, Netflix, Amazon Prime Video
Information retrieval	Google Chrome, search, Bing search

The researchers have analyzed the data interaction process and interaction strategy of several typical applications in the traditional test environment. Still, these applications have not been tested and researched in the environment where the USIM card is copied. This article makes up for this shortcoming and proposes to the behaviors and processes of App-like apps are tested to give out the security problems and deficiencies in the identity authentication of these apps and give solutions to them.

3.2. Identity Authentication Process Test for Typical Applications. In this section, in an environment where the attacker already has a copy of the USIM card, study the identity authentication of the test App in the USIM device, and analyze the data request and response results during the jump process of the identity authentication process by executing the identity authentication tree of different applications, observe and record the behavior of the App, and analyze the links that the attacker may bypass.

3.2.1. Test Conditions. Test object: the value of the information contained in the application is one of the main factors that affect the attacker's selection of attack targets. This test selects applications that are more likely to be targeted by the attacker. These applications usually occupy the mainstream market and can have a profound impact on the personal lives of a large number of users. These applications have a high user stickiness, are closely integrated with users' lives, and can access personal privacy and other data, which will be researched and targeted by attackers, and the potential security vulnerabilities of these applications will also lead to more serious data leakage incidents. Therefore, in order to improve the representativeness of the test results, combined with the abovementioned App analysis data, this article covers 7 types of applications in social communication, financial payment, travel delivery, health care, file cloud disk, entertainment video, and information retrieval. Launched the test, each type of application selected a total of 58 typical applications according to the download and usage rankings. The details are shown in Tables 1 and 2. The mobile big data service provider shows that applications such as short video, integrated e-commerce, and mobile payment have developed rapidly. These applications have a high user stickiness, are closely integrated with the user's life, can access personal privacy and other data, and will be subject to research and targeting by attackers, and these applications.

Table 2: Tested mobile platforms.

Index	Information
Model	iPhone XR
System	iOS 12.4.1
Operator	China Unicom
IMEI	357394092794037
ICCID	89860116208410304191
MEID	35739409279403

The potential security breaches will also lead to more serious data breaches. Therefore, in order to improve the representativeness of the test results, combined with the abovementioned App analysis data, this article covers 7 types of applications in social communication, financial payment, travel delivery, health care, file cloud disk, entertainment video, and information retrieval. A total of 58 typical applications are selected according to the ranking of downloads and usage. The details are shown in Tables 1 and 2.

The above 58 applications can access the user's communication content, property status, geographic location and travel trajectory, physical health status, private files, and retrieve information. This information is directly related to user privacy, and the leakage of this information will endanger user data security poses serious personal information security risks. Once these applications cannot guarantee the security of user identity verification, they will pose a greater potential threat to users' lives.

Test environment: the test model information used in this article is as follows.

Apple iOS and Google Android are the main types of mobile device systems. Except for the Apple authentication mechanism represented by iCloud, the remaining 57 apps have the same authentication process on iOS and Android. Therefore, the test results and conclusions of 58 applications of the equipment used in this test are consistent with the tests under different test systems result. Based on the above test conditions, the following prerequisites must be given before the test.

(1) The copied USIM card and the original USIM card are the same to the base station when sending and receiving messages

(2) The username of the target user and the mobile phone number of the USIM card are easy to obtain.

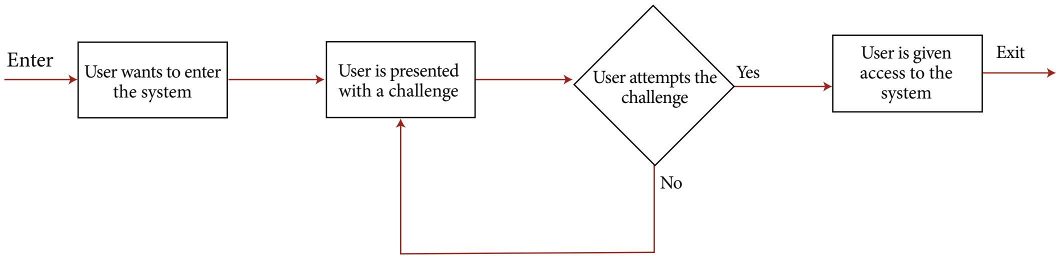
Enter
User wants to enter the system
User is presented with a challenge
User attempts the challenge
Yes
No
User is given access to the system
Exit

Figure 4: General procedure of authentication test [14].

According to the above test conditions, a general method of testing can be proposed

3.2.2. Test Methods. In this section, test the real device based on the verification tree of the mobile application. After downloading each application, use the target phone number or email address to register to complete the general registration process for new users. Then log out to simulate the behavior of an attacker, test the password reset function on the login page, pay attention to the response results of different steps and the links that require SMS verification codes, and record whether the application can be bypassed in password reset and other links. In the test process, use Stream to capture the Http/Https data request and response during the App login process, analyze the data packet fields and control methods, and combine the actual behavior of the App to give the test results. The basic test procedure is shown in Figure 4.

Other test requirements are as follows.

(1) For applications that can use mobile phone number or email to register and log in

In terms of usage, priority is given to using mobile phone to register and log in.

(2) For applications that use SSO services, the authentication logic is the same as that of the identity provider (IdP), and it is preferred not to use SSO services for testing

(3) For applications that do not enable secondary verification by default, keep the original settings for testing. If the application forces two-step verification to be turned on

Do not turn off this function during testing.

This article selects “Do you need SMS verification code,” “Do you need secret information,” “Do you need email verification,” and “Do you verify the current device” as the test indicators in the password reset process. Combining the Http/Https data fields applied during the test and the control functions in the page code, if the user only needs the SMS verification code and does not need to verify the device environment to complete the password reset, it can be considered that the attacker is copying the USIM card environment. You can directly bypass the authentication link of the application, that is, the application is insecure.

3.3. Data Analysis in Identity Authentication of Typical Applications. During the testing process, this article captures and analyzes the request data and response results of the application. This section takes two typical applications of WeChat and Alipay as examples to analyze the format and jump flow of the request and response data in the process of resetting the password. And combined with the application behavior, give the test results of the two in the copied USIM environment.

3.3.1. Data Capture and Analysis in WeChat Login. According to the requirements in Section 3.2.2, this section needs to test the authentication process of WeChat to retrieve the password. Since WeChat can directly use the mobile phone number and SMS verification code to complete the login, when the user selects the “Retrieve Password” function, WeChat will make users taste.

Try to log in directly with your mobile phone number. In this process, Stream1.0.4 is used to capture and analyze Http network traffic. WeChat login process.

After analyzing the server response data, it can be seen that the above three request data correspond to the three stages of “request for password retrieval,” “request for mobile verification code login,” and “request for login application” when the client retrieves the password. The key fields and the code execution process of the response page expand the description of the identity authentication process during the login phase of WeChat.

Request to retrieve the password: when the user requests to retrieve the password on the WeChat login page, the client will initiate a request to support. After the verification is passed, the server responds, and the client jumps to the prompt message page for retrieving the password. At this time, WeChat will prompt the user to log in with a mobile phone. The response data includes the control code of the page, select the function button of “Can receive SMS,” the ican function in the corresponding code will realize the jump to the next page. After confirming on the next page, the go function constructs a request for the mobile phone verification code to log in to the application.

Request mobile phone verification code login: when the user can log in with the SMS verification code, the user will be redirected to the login page using the SMS verification code according to the prompt. Among them, the go function sets the p1 and p2 fields to 1 and assigns rid to the p10 field. The above fields are spliced and used as report data, which is passed as part of the login request in the next stage to the server. At this stage, the client will construct an ap_msg field that contains information about the current device's network environment and system parameters and use the GET method to request the server to send the verification code to the login page.

Request to log in to the application: when the user logs in using the SMS verification code, the 6-digit SMS verification code is required. After the client is authenticated, the reportFunc function uses the characteristics of the Image object of Javascript and realizes the static of the server resources by changing the source link attribute of the object access. Finally, the report data field in the message can tell the identity of the server user and the method used to log in to the application and use the GET method to send it to the server to complete the login.

In summary, in the process of retrieving the password and logging into WeChat, the client uses scan and go functions to complete the application identity authentication process based on the user's existing identity credentials. On the client-side, when the attacker chooses to log in with the SMS verification code during the password reset process. When used, you can copy the USIM card to directly obtain the SMS verification code to complete the login.

3.3.2. Data Analysis in Password Reset. Use the same method as in Section 3.3.1 to analyze password reset process analysis. When logging in to your account, this article chooses to reset the password instead of the SMS verification code to log in. Use Stream to capture the Https data in password.

The above request data packets correspond to the client's request to retrieve the password, send the SMS verification code, and send the reset password, respectively. When resetting the password, the client will repeatedly send to the host of http://abc.com/ the data including the phone model, network environment, operator type, and other device environment parameters, and the data will be returned by the server.

The status code determines whether the current device can continue the next operation. Due to the large amount of Https traffic data in this link, only the three request response processes will be explained below.

4. Identity Authentication Test Results and Analysis of Typical Applications

According to the test requirements and test methods in Section 3, through the process observation and recording of the identity authentication functions such as login and password retrieval of the test application, this section presents the test results and analysis.

4.1. Overview of Test Results. According to records, when resetting the password, 19 of the 58 apps used in the test can be directly used to reset the password through the SMS verification code to complete the login. The remaining 39 apps are attacked due to additional requirements such as confidential information, email verification, and device verification.

Apps cannot be bypassed because the app only provides email verification but not SMS verification. Except for Apple's App store and iCloud, the verification methods for other test applications are SMS verification or email verification. Among the 21 apps that performed secondary verification, 4 adopted additional confidential information, 4 adopted additional email verification, and 13 apps tested the current device environment to remind or warn the original logged-in user of the current attacker. Behavior to prevent attackers from bypassing directly. Some of these 21 applications also use multiple verification methods to ensure product safety.

The test also found that when the attacker can obtain the SMS verification code sent to the user's device, 9 apps can be bypassed during password reset and normal login, and 10 apps are easily bypassed only during password reset. However, there are 10 other applications that can be bypassed only during normal login. Among them, the application names included in each indicator are shown in Table 3.

When at least one verification method is additionally adopted, it is difficult for an attacker to steal user information. However, when logging in normally, the attacker can use the user's mobile phone number to log in, which makes each application default to the original legitimate user who is currently logged in remotely, so no additional verification is performed.

4.2. Application Classification and Index Test Results. For each test indicator, 38 apps provide an interface for SMS verification to reset passwords, and only 4 apps require users to provide confidential information, such as historical orders and purchased product names. For email verification, 4 apps require SMS verification. In the case of, additional email verification is still required, while 22 models only require email verification, and 16 apps will perform environmental testing of newly logged-in devices, etc.

Seven types of applications tested, the proportion of financial applications that are directly bypassed is the least, only 20%. Among the 20 apps in social, health, and entertainment, 11 can be bypassed. In the global mobile application market, applications that directly involve the safety of users' personal property have relatively safe protection measures, while applications that indirectly involve user privacy, such as providing entertainment and personal health information, still have relatively simple identity authentication strategies and are vulnerable to attackers.

4.3. Analysis and Research of Test Results. Combining the test results, this section analyzes the current status and characteristics of the mobile application's identity authentication process from the perspective of the characteristics of the application process, the relationship between the application type and the authentication process.

4.3.1. Differences in SMS Verification Services at Home and Abroad. During the test, it was noticed that most of the apps in India have implemented the service entrance, while many foreign apps only use email addresses and user names for authentication. Further analysis found that all 17 domestic applications provide SMS verification and reset password

Table 3: Comparison between domestic and foreign Apps.

	SMS verification	Reset password services	Directly bypassable
Domestic apps	17	17	6
Foreign apps	41	21	13

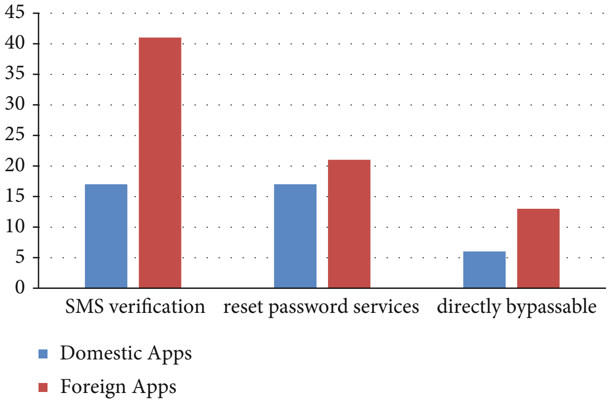

Figure 5: Comparison between domestic and foreign Apps.

services, and 6 of them are deemed to be directly bypassable, while 21 of foreign applications provide SMS verification, and 13 of them can be bypassed, such as shown in Figure 5.

The reason why mobile Internet companies and relevant departments implement SMS verification code services on a large scale is not only because of the low cost and difficulty of operation of SMS verification codes but also the effective supervision of mobile applications. The test also found that foreign apps do not require mobile phone number binding, and even a small number of apps do not have a mobile phone number registration entry.

4.3.2. Lack of Confidential Information. For the test results of each indicator, only 6.9% of applications use secret information as the second step of verification. For different types of confidential information, too high uniqueness may increase the user's operation difficulty, while low uniqueness will appear very fragile in the face of various social engineering methods, as shown in Figure 6.

Secret information required by the application is the last four digits of a random merchant order number in the user's previous orders. This operation is difficult for users who do not frequently use mobile smartphones. The application requires any of the historical orders to be filled in the name of a consignee, and this information is easily leaked by various phishing and retrieval methods. Therefore, the design of confidential information with low user operation difficulty but high uniqueness should become a problem that needs to be considered in the application of the App user identity verification system in the future.

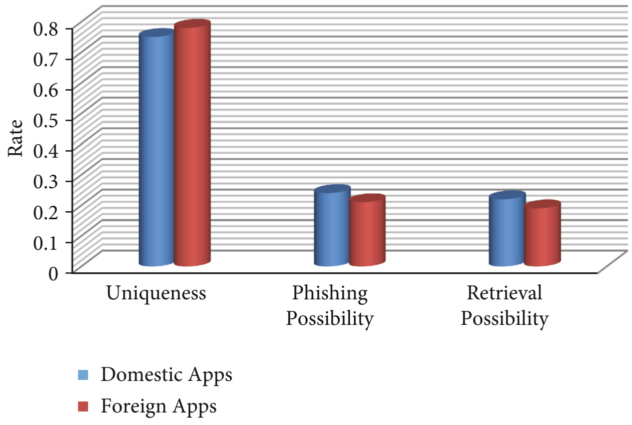

Figure 6: Confidentiality level between domestic and foreign Apps.

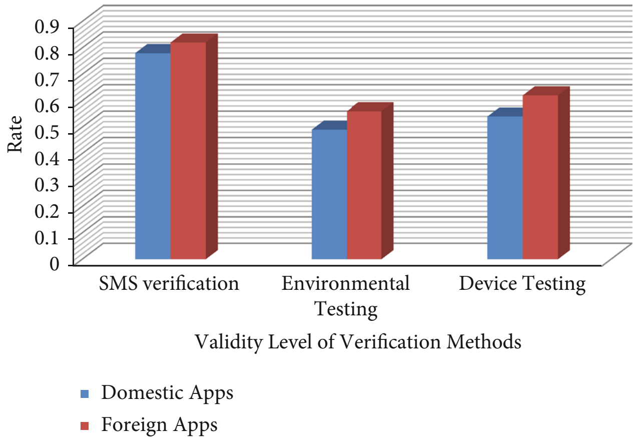

Figure 7: Validity level of verification methods.

Table 4: Verification label validity.

	Validity level of verification methods		
	SMS verification	Environmental testing	Device testing
Domestic apps	0.78	0.49	0.54
Foreign apps	0.82	0.56	0.62

4.3.3. Value Difference of Application Information Type. For different types of applications, having a low bypass ratio only indicates that it has a better security performance in the environment of copying the USIM card, but it does not indicate that it has a strong degree of protection in protecting user information. More retail applications and a small number of payment applications do not require additional identity binding when registering, and the secondary verification function is not mandatory. It can be considered that in the information value evaluation system of users and mobile Internet companies, compared with personal online assets (such as all property, cloud files, etc.), the sensitivity of personal interests, health conditions, and social content is not high.

Making entertainment, health care, and social networking applications have a single verification method, resulting in a higher percentage of bypassable applications for these three types of applications.

4.3.4. Improvement of Equipment Verification Methods. The test found that when resetting the password, 27.6% of the applications will detect the user's device model and environment, such as capturing the current network IP address, geographic location, and machine hardware parameters, and log in frequently with the original device. Information matching and peer recognition of the user who tried to log in before or remind the original device user.

At present, there are three main methods for the verification of new devices: SMS verification, device testing, and environmental testing as shown in Figure 7 and Table 4. The device detection link is one of the two-step verification methods adopted by apps such as Google when they detect a new device login. When an attacker tries to reset the password on a device, the application that the original device logs in will prompt the user whether to allow the operation to occur. Only after the authentication is completed in the device, the user account can request other devices to reset the password. For example, when an attacker tries to reset the password of a target Apple ID on a certain device, Apple requires the ID to log in to other devices for first verification. This can effectively prevent attackers from using the copied USIM card to log in to the application.

5. Conclusion

This paper focuses on the problem of mobile application identity authentication. It first explains the authentication process of mobile applications and describes the general verification tree of mobile applications to identify problematic linkages in the identity authentication strategy; then, when various mobile applications authenticate users, log in to the application. The authentication methods used in resetting passwords and completing sensitive actions may be the same, whereas SMS verification codes and email verification are commonly employed in the process of resetting passwords and login authentication. The USIM card copy attack makes it possible for the attacker to obtain the SMS verification code sent to the original user device, so that the password reset and application login in the verification tree can be used as the starting point of the attack, and user information can be stolen after bypassing the authentication login application.

This article uses real machine testing to simulate the security flaws of password reset and login authentication of various applications after the attacker successfully implements the USIM card copy attack. After analyzing the Https traffic data in the identity authentication process and combining the application behaviors, it is found that a total of 29 of 58 applications face security risks that can be directly bypassed by copying the USIM card. Among them, 9 applications can be used for password reset and login. It is bypassed directly. There are 10 apps that can be bypassed only when the password is reset, and the remaining 10 apps can only be bypassed directly when logging in.

Among them, social communication and entertainment applications are most easily bypassed. Mobile application developers and security personnel should complete and improve the authentication logic of current products, adopt two-step authentication or two-factor authentication to prevent USIM card copy attacks, and implement effective deployment of user data security protection methods.

Data Availability

The data used to support the findings of this study are available from the author upon request (s.alisher@psau.edu.sa).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Sultan Ahmad wrote the paper, Hikmat A. M. Abdeljaber validated the paper, Jabeen Nazeer designed the methodology, Mohammed Yousuf Uddin proofread the paper, Velmurugan Lingamuthu validated the software, and Amandeep Kaur proposed the method.

Acknowledgments

The authors are grateful to the Applied Science Private University, Amman-Jordan, for the full financial support granted to cover the publication fee of this research article.

References

[1] W. F. El-Sadek and M. N. Mikhail, "Universal mobility with global identity (UMGI) architecture," *International Conference on Wireless Networks and Information Systems*, vol. 2009, pp. 389–394, 2009.

[2] B. Mathur and S. M. Satapathy, "An analytical comparison of mobile application development using agile methodologies," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1147–1152, Tirunelveli, India, 2019.

[3] S. Khan, Z. Jiangbin, and A. Wahab, "Design and development of android performance testing tool," in *IEEE Conference on Big Data and Analytics (ICBDA)*, pp. 57–60, Kota Kinabalu, Malaysia, 2020.

[4] V. P. La Manna and F. Pasveer, "Towards a framework for proximity-based hybrid mobile applications," in *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, pp. 176–179, 2018.

[5] G. Dhiman, J. Rashid, J. Kim, S. Juneja, W. Viriyasitavat, and K. Gulati, "Privacy for healthcare data using the byzantine consensus method," *IETE Journal of Research*, pp. 1–12, 2022.

[6] S. Kanwal, J. Rashid, J. Kim, S. Juneja, G. Dhiman, and A. Hussain, "Mitigating the coexistence technique in wireless body area networks by using superframe interleaving," *IETE Journal of Research*, pp. 1–15, 2022.

[7] N. Singh, E. H. Houssein, S. B. Singh, and G. Dhiman, "HSSAHHO: a novel hybrid Salp swarm-Harris hawks optimization algorithm for complex engineering problems," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–37, 2022.

[8] G. Dhiman, A. K. Nagar, S. Vimal, and S. Rho, "Cybertwin-Driven 6G for Internet of Everything (IoE): Architectures," *IEEE Transactions on Industrial Informatics*, 2022.

[9] G. Dhiman, S. Juneja, W. Viriyasitavat et al., “A novel machine-learning-based hybrid CNN model for tumor identification in medical image processing,” *Sustainability*, vol. 14, no. 3, p. 1447, 2022.

[10] V. Miškovsky, H. Kubátová, and M. Novotný, “Speeding up differential power analysis using integrated power traces,” in *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–5, Budva, Montenegro, 2018.

[11] J. Liu, Y. Zhang, and Q. Zhao, “Video stabilization algorithm based on Pearson correlation coefficient,” *International Conference on Advanced Mechatronic Systems (ICAMechS)*, vol. 2019, pp. 289–293, 2019.

[12] K. Kour, D. Gupta, K. Gupta et al., “Smart-hydroponic-based framework for saffron cultivation: a precision smart agriculture perspective,” *Sustainability*, vol. 14, no. 3, p. 1120, 2022.

[13] G. Dhiman, A. Vignesh Kumar, R. Nirmalan et al., “Multimodal active learning with deep reinforcement learning for target feature extraction in multi-media image processing applications,” *Multimedia Tools and Applications*, pp. 1–25, 2022.

[14] K. Prasanna, K. Ramana, G. Dhiman, S. Kautish, and V. D. Chakravarthy, “PoC design: a methodology for proof-of-concept (PoC) development on internet of things connected dynamic environments,” *Security and Communication Networks*, vol. 2021, Article ID 7185827, 2021.

[15] N. Saxena and N. S. Chaudhari, “Secure algorithms for SAKA protocol in the GSM network,” in *2017 10th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1–8, Valencia, Spain, 2017.

[16] K. Tabassum, “An efficient authentication technique for security management against cloning mobile phones,” in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 125–128, Chennai, India, 2017.

[17] H. Xie, K. Lv, and C. Hu, “A partition matching method for optimal attack path analysis,” in *2018 IEEE Intl Conf on parallel & distributed processing with applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, pp. 120–126, 2018.

[18] Z. Chen, L. Zhang, W. Wang, and Z. Wu, “A pre-coded multicarrier M-ary chaotic vector cyclic shift keying transceiver for reliable communications,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 2, pp. 1007–1021.

[19] S. Kranthi Kumar, K. Ramana, G. Dhiman, S. Singh, and B. Yoon, “A novel blockchain and bi-linear polynomial-based QCP-ABE framework for privacy and security over the complex cloud data,” *Sensors*, vol. 21, no. 21, p. 7300, 2021.

[20] G. Dhiman and R. Sharma, “SHANN: an IoT and machine-learning-assisted edge cross-layered routing protocol using spotted hyena optimizer,” *Complex & Intelligent Systems*, pp. 1–9, 2021.

[21] M. Ouaissa, M. Houmer, and M. Ouaissa, “An enhanced authentication protocol based group for vehicular communications over 5G networks,” in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*,, pp. 1–8, Marrakech, Morocco, 2020.

[22] K. Han, M. Ma, X. Li, Z. Feng, and J. Hao, “An efficient handover authentication mechanism for 5G wireless network,” *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 2019, pp. 1–8, 2019.

[23] X. G. Huang, L. Shen, and Y. H. Feng, “A user authentication scheme based on fingerprint and USIM card,” in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1261–1264, Harbin, China, 2008.

[24] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, “LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.

[25] V. K. Gupta, S. K. Shukla, and R. S. Rawat, “Crime tracking system and people’s safety in India using machine learning approaches,” *International Journal of Modern Research*, vol. 2, no. 1, pp. 1–7, 2022.

[26] P. K. Vaishnav, S. Sharma, and P. Sharma, “Analytical review analysis for screening COVID-19 disease,” *International Journal of Modern Research*, vol. 1, no. 1, pp. 22–29, 2021.

[27] R. Kumar and G. Dhiman, “A comparative study of fuzzy optimization through fuzzy number,” *International Journal of Modern Research*, vol. 1, no. 1, pp. 1–14, 2021.

[28] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler, “Sending out an SMS: characterizing the security of the SMS ecosystem with public gateways,” *IEEE Symposium on Security and Privacy (SP)*, vol. 2016, pp. 339–356, 2016.

[29] S. Yubo, Z. Zhiwei, and X. Yunfeng, “Using short message service (SMS) to deploy android exploits,” in *International Conference on Cyberspace Technology (CCT)*, pp. 1–5, Beijing, China, 2014.

[30] C. Kotkar and P. Game, “Prevention mechanism for prohibiting SMS malware attack on android smartphone,” *Annual IEEE India Conference (INDICON)*, vol. 2015, pp. 1–5, 2015.

[31] S. Rinaldi, M. Pasetti, A. Flammini, P. Ferrari, E. Sisinni, and F. Simoncini, “A testing framework for the monitoring and performance analysis of distributed energy systems,” *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 10, pp. 3831–3840, 2019.

[32] W. Squires and P. Centonze, “Cross-platform access-rights analysis of mobile applications,” *IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft)*, vol. 2016, pp. 295-296, 2016.

[33] W. Huang, Z. Chen, W. Dong, H. Li, B. Cao, and J. Cao, “Mobile internet big data platform in China Unicom,” *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 95–101, 2014.

[34] L. Gomez, I. Neamtiu, T. Azim, and T. Millstein, “RERAN: timing- and touch-sensitive record and replay for android,” in *2013 35th International Conference on Software Engineering (ICSE)*, pp. 72–81, San Francisco, CA, USA, 2013.

[35] S. Peng, Z. Peng, Y. Ren, and F. Chen, “Fast intra-frame coding algorithm for versatile video coding based on texture feature,” in *2019 IEEE International Conference on Real-time Computing and Robotics (RCAR)*, pp. 65–68, Irkutsk, Russia, 2019.

[36] Q. Liu and Q. Liu, “Research on automatic generation control system of photovoltaic power station based on adaptive PID control algorithm,” in *2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*,, pp. 231–236, Dalian, China, 2020.

[37] M. Su, Y. Wang, N. Yin, and H. Liu, “The effects of position errors compensation on the other geometric errors in the CNC machine tools,” in *2019 6th International Conference on Information Science and Control Engineering (ICISCE)*, pp. 939–947, Shanghai, China, 2019.