User Authentication Security

Jianhe Zhang

***Abstract*—User authentication is widely used in people's daily life. The security of authentication profoundly affects the security of personal information and property. In this study, we will do research on three aspects: user authentication on SIM card swap, security and privacy risks of phone number recycling, and research on passwords of mainstream websites. We will use experiments to explore and verify the existence of security vulnerabilities and try to come up with solutions.**

I. Introduction

User authentication has made extensive inroads. People can use several methods to verify their identity (e.g. email, smart phone verification code, hardware keys and applications). But there are still applications rely on insecure authentication methods, or even inconsistently enforce their authentication policy.

This research will be divided into the following three parts:

(1) SIM Card Swap: Phone-based passcodes are frequently used as one of authentication factors in multi-factor authentication (MFA) scheme and as an account recovery mechanism. SIM swapping increases the risk of user information leakage. The attacker takes advantage of insecure MFA and swap victim's SIM card, and hijack their social platform accounts or email accounts.

(2) Phone Number recycling: After phone numbers were canceled, they will be recycled and reused by the phone carrier. If the number of the phone numbers is large enough, no user will assign a same number. However, users are inevitably assigned phone numbers that have been used. Attacker can assign a large number of phone numbers to get the recycled numbers, and try to login main streams victims may have registered, then attacker can swindle victims' friends and family members.

(3) Password of mainstream websites: Nowadays, password is a common user authentication method. To prevent password leakage, websites often encourage users to use stronger passwords. For this purpose, the main requirements for passwords on mainstream websites are blocklists, password composition rules / policies (PCPs) and strength meters. However, most websites uses common PCP such as *3Class8* do not achieve its purpose. And the combination of blocklists and strength meters performs better than sigle PCP requirement.

II. Background

A. User Authentication

User authentication is the process of verifying a user's identify. To authenticate, the user typically proves her identity by providing one of the following credentials: something she knows (e.g., a password or PIN), something she has (e.g., her phone), or something she is (e.g., her fingerprint)[1]. Now we can use hardware security keys, one-time passcodes sent via telephone, as well as password complexity guidelines.

B. Factor Authentication

Factor authentication(FA) is a security enhancement that requires users to provide credentials for authentication. In recent days, websites use Multi-factor authentication(MFA), like 2-FA, it requires users type their password and authenticate on their phone (e.g., OTPs and accept on phone application).

C. SIM cards

Wireless service to a mobile device is tied to that device's SIM card. Wireless carriers keep track of the mapping between phone numbers and SIMs to ensure that calls, messages, and data connections are routed to the correct customer. Generally, the mapping from a phone number to a SIM is one-to-one relationship: a phone number can only be associated with a single SIM at any given point in the time and vice versa.

If users want to change their devices, they can easily remove their existing SIM card and insert it into the new device. Or they can also purchase a new inactive SIM card and migrate the service over to the new SIM before inserting it into the new device.

D. Phone Numbers

1) Phone Number in the United States: In the United States, telephone numbers are formatted and geographically assigned according to the North American Numbering Plan (NANP). All NANP phone numbers are of the 10-digit format:

$$NPA - NXX - XXXX$$

The number plan area (NPA) code, or area code, comprises the first three digits. The first digit can be in range[2,9], while the second and third digits can be in range [0,9].

The central office (exchange) code (NXX) comprises the next three digits. The first digit can be in range [2,9], while the second and third digits can be in range [0,9].

2) Phone Number in China: In China, telephone numbers or Mobile Directory Number (MDN) are composed by four parts:

$$MDN = CC + MAC + H_0H_1H_2H_3 + ABCD$$

Totally 13 numbers. CC is country code (e.g., China is 86), MAC is mobile access code, H0H1H2H3 is Home Location Register (HLR) identifier and ABCD are allocated by each HLR.

Because make calls from within the country do not need CC, so we ignore that. MAC are different from operators (e.g., 133 is a number section of China Telecom, 186 is a number section of China Unicom). HLR is a static database stores local users' information. Currently, the total number of the MDN is more than 5 billion.

III. Content

A. SIM Card Swap

B. Attack Step

The step of SIM card swap attack is:

1) Attacker get user's private information (e.g., phone number, birthday and address) from several ways (e.g., phishing site, underground market).
2) After attacker accumulates enough information, he will pretend to be the victim and send SIM card swap requests to the carrier.
3) After the attack succeed, attacker can login victim's account and change the password. The victim's device will not link the Internet.

1) Attack Simulation: To simulate this attack, we designed a client-server model for attack. And the step is shown as Fig.1[1].

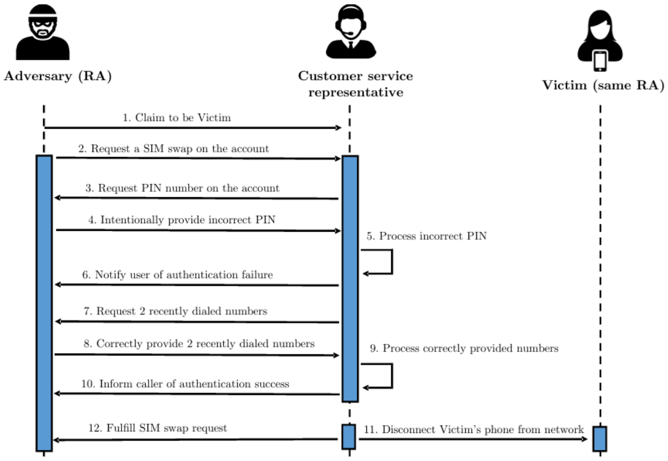

Adversary (RA)
Customer service representative
Victim (same RA)
1. Claim to be Victim
2. Request a SIM swap on the account
3. Request PIN number on the account
4. Intentionally provide incorrect PIN
5. Process incorrect PIN
6. Notify user of authentication failure
7. Request 2 recently dialed numbers
8. Correctly provide 2 recently dialed numbers
9. Process correctly provided numbers
10. Inform caller of authentication success
11. Disconnect Victim's phone from network
12. Fulfill SIM swap request

Fig. 1: SIM swap model

In the addition verification information, we choose 2 recently dialed numbers as figure shows. Other verification information (e.g., last payment, fingerprint, birthday and credit card number) can also be used in addition verification behind the failure of PIN authentication.

In our simulation, the additional verification information is too weak and the attacker can easily induce victim to do calls to attacker. And during the attack, the victim has no way of knowing that his SIM card is being swapped. All the victim will know is his device cannot connect to network.

C. Phone Number Recycling

Attack Simulation

Due to the limitations of the composition and number of phone numbers, when the phone number is abandoned by the original user, the carrier will reclaim the number and reassign it to the new user. The website where the original user registered cannot detect whether the phone number is no longer in use or the owner has changed, resulting in the leakage of the user's information along with the migration of the phone number.

We use the client-server system built in section SIM card swap. User can use his phone number to register website. And user can cancel his phone number, and it will return to the number pool.

The step of the attack is:

1) User register the website
2) User canceled his phone number
3) Attacker register an amount of phone number
4) Attacker try to login the website

D. Passwords of Mainstream Websites

Simulation

To test the validation of PCPs, blacklists and strenth meter, we design a program to simulate the password website. And we can input password then get the strenth of the password use the combination of these methods.

IV. Result

In the section of SIM card swap attack, we notice that easy-to-known information cannot perform as the verification information. Meanwhile, carrier can perform particular information (e.g., password, PIN, fingerprint and face) as verification information.

For phone number recycling attack, the probability depend on the number of recycled number and the total number. The high percentage of recycled number will lead to high risk of attack. And the serial numbers are more likely to be attacked.

In password section, we find that The effectiveness of PCPs in improving password strength is limited, users tent to choose easy-to-remember string as password (e.g., birthday, name and special word). PCPs have problem on filtration common password. And users tend to capitalize the first letter and add special symbol to create password satisfied PCPs.

Blocklists and strenth meter effectively increase the power of the password. It

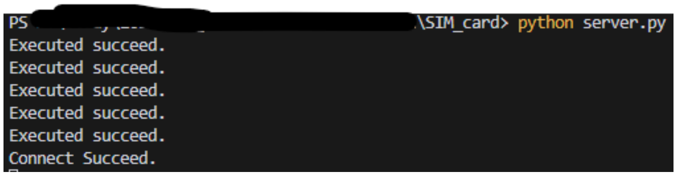
With the increasing of the number of iterations, the algorithm continues to converge and ultimately obtains the optimal solution. It improves the strength of the password. However, the mainstream websites uses PCPs (e.g. 3Class8, 4Class8 and 3Class10) as the threshold.

V. Experiment

The code is published at My Github Repository.

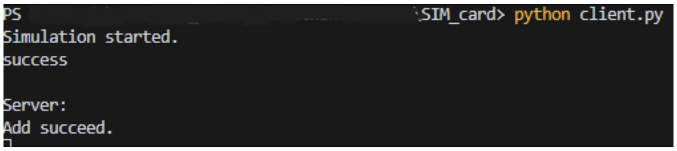
A. Preliminary

Before we start simulation, we need to start the server and client like the figure below:



```
PS [redacted] \SIM_card> python server.py
Executed succeed.
Executed succeed.
Executed succeed.
Executed succeed.
Executed succeed.
Connect Succeed.
```

Fig. 2: Start Server



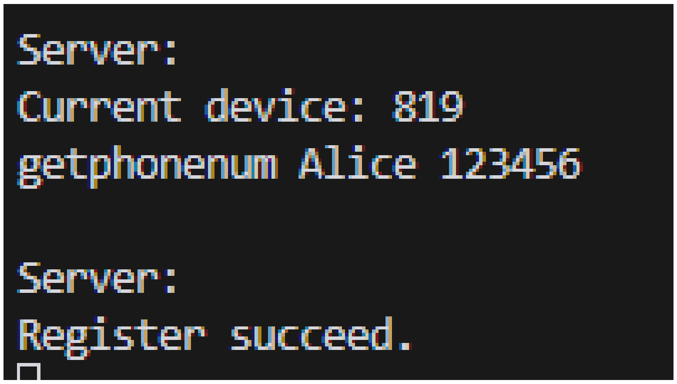
```
PS [redacted] SIM_card> python client.py
Simulation started.
success

Server:
Add succeed.
```

Fig. 3: Start Client

After we start server, it will connect to Postgresql and create databases to store information. Client will connect to the server and automatically create a device.

B. SIM Card Swap

Firstly, we start two client. Two clients register their phone numbers.

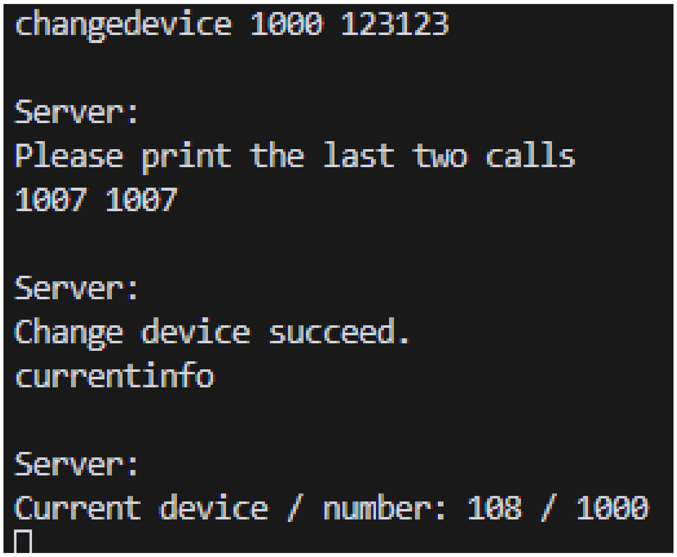


```
Server:
Current device: 819
getphonenum Alice 123456

Server:
Register succeed.
```

Fig. 4: Register Phone Number

The Alice's device / number is 819 / 1000, and Bob's device / number is 438 / 1007

We use Alice victim, Bob as attacker. We assume that Bob knows the last two calls of Alice (From Alice to Bob), then Bob use another phone (client) call server for SIM swap. Bob type wrong PIN and the server call for last two calls. Then Bob answer it successfully, then the device changed successfully.

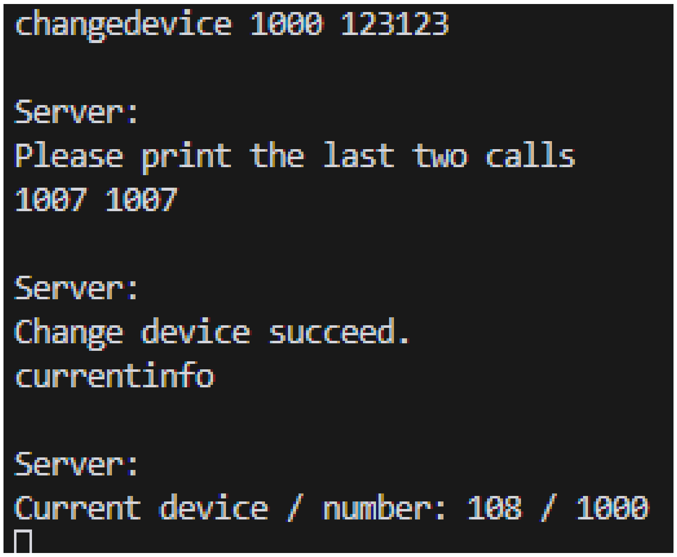


```
changedevice 1000 123123

Server:
Please print the last two calls
1007 1007

Server:
Change device succeed.
currentinfo

Server:
Current device / number: 108 / 1000
```

Fig. 5: SIM Swap

C. Phone Number Recycling

In this experiment, we use some phone number to register website then cancel the phone number. The step shows at Fig.6.



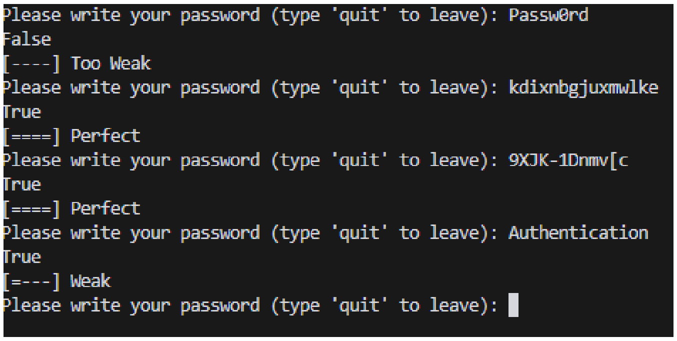
```
changedevice 1000 123123

Server:
Please print the last two calls
1007 1007

Server:
Change device succeed.
currentinfo

Server:
Current device / number: 108 / 1000
```

Fig. 6: Login Website

After user cancels the number, attacker registers an amount of phone number and login the website through phone-PIN mode. If the attacker login the website, the attack is succeed.

D. Password Polices

After starting the program, we can type a string to test the strength of the password. Normally, the program uses zxcvbn (A password strength meter lib) and blocklist (100k-most-used-password-NCSC) as the threshold. A sample shows below.



```
Please write your password (type 'quit' to leave): Passw0rd
False
[----] Too Weak
Please write your password (type 'quit' to leave): kdixnbgjuxmwlke
True
[====] Perfect
Please write your password (type 'quit' to leave): 9XJK-1Dnmv[c
True
[====] Perfect
Please write your password (type 'quit' to leave): Authentication
True
[=---] Weak
Please write your password (type 'quit' to leave):
```

Fig. 7: Password strength

VI. Future work

SIM swap attack and phone number recycle attack is more common in the United States. Chinese carriers perform different ways to authentication, different population base and different step after phone number recycled. Blocklists and strength meter for password are tend to detect English-based password, not for Chinese-based password (e.g., pinyin password). In the future's study, researchers can consider do more indigenous research, and develop new methods on Chinese authentication security.

References

[1] Kevin Lee et al. “The Research-Practice Gap in User Authentication”. AAI29255940. PhD thesis. USA: Princeton University, 2022. ISBN: 9798351480480.