Why are certain authentication requirements bad?

Preamble

I came across this draft paper from Princeton University about SIM hijacking attacks. After reading through the paper, I thought it helpful to share some aspects of the paper that has wider applications than just SIM hijacking attacks.

Background

While the adoption of second factor authentication (2FA) continues to grow, a significant portion of web services support SMS as an accepted second factor. Furthermore, SMS validation is performed by some web services in place of the password (e.g. WhatsApp, Shopee).

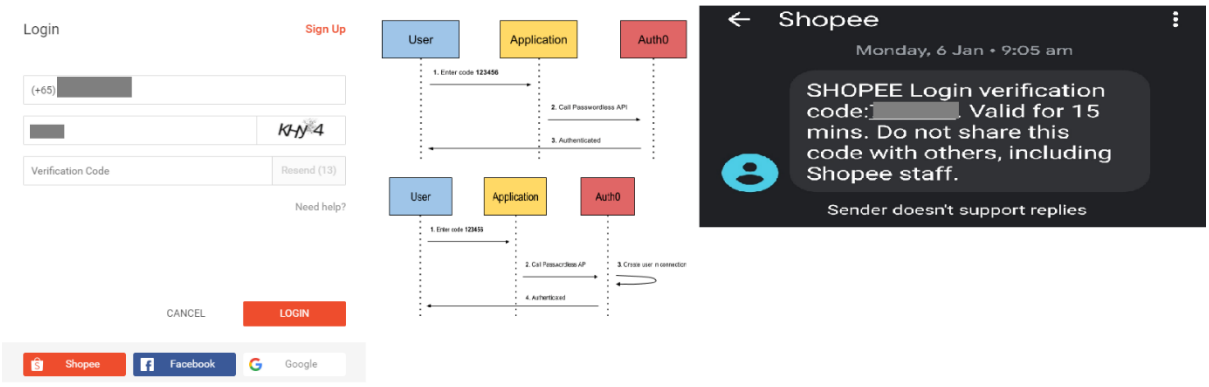

Figure 1: SMS Verification is one of the authentication mechanisms in sites like Shopee

As mentioned in a Princeton University paper, weaknesses in authenticating the identity of a remote user by telcos allow the mobile phone number to the ported to a malicious user's SIM (also known as SIM hijacking or SIM swapping). These methods of authenticating are also use in other areas where other service providers (other than telcos) attempts to verify the identity of a caller via phone (e.g. reporting a lost credit card via phone).

Four weak information requirements

In this article, we will go through four different pieces of information that service providers use for remote identity verification and provide scenarios on how a third-party can "fulfil" the requirement without being the valid owner of that information. The article will conclude with some measures you can take to protect yourself .

a) Last payment method

When asked about the last payment method, there are two ways of getting the "correct answer". The first is to guess the answer correctly. This may be easier than imagined. Practical intuition will allow an attacker to guess this answer with a significant chance of getting it correct. As an example, let's say we are asked this question with relation to a bank credit card account. It is no stretch of imagination to say that the most likely payment method will be either the use of another account in the bank to pay off the credit card or the submission of a cheque to pay off the bill. Unless the service provider has some form of "speed bump", where a delay is implemented for all requests of the same kind, an attacker can guess the answer again. Even considering all supported payment types, the number of possible values rarely exceed 20.

Secondly, some service providers allow unauthenticated payments **to** the victim. For example, a prepaid mobile number can be topped up by an attacker by simply providing the mobile number.

b) Usage information

While the paper only referred to outgoing and incoming calls, other service providers may depend on something similar such as transaction history. For cases where last outgoing call was the information required, a bit of social engineering is required (and dependent on victim behaviour). For some victims, a simple missed call from an attacker is sufficient to trigger a return call from the victim – causing the last outgoing call to be to the attacker. For other victims, a certain pretext is needed to induce a call. In the paper, telcos sometimes requested the last incoming calls as verification information. No social engineering is necessary in such a case – an attacker can call the victim just before the SIM hijacking.

Other types of usage information can also be created or induced by an attacker. For example, unauthenticated deposits to a stored value account (e.g. Grabpay) is sometimes permitted and will generate an incoming log in the transaction history.

c) Last 4 digits of credit card

While the perception is that credit card information is well protected, this applies to the entirety of the credit card information (full 16 digits and card verification value). Receipts often contain the last four digits of a payment card, since Primary Account Number truncation (to comply with PCI DSS) permits display of last 4 numbers. These receipts may be found in the rubbish bin, in intercepted or hacked emails and other less secured places.

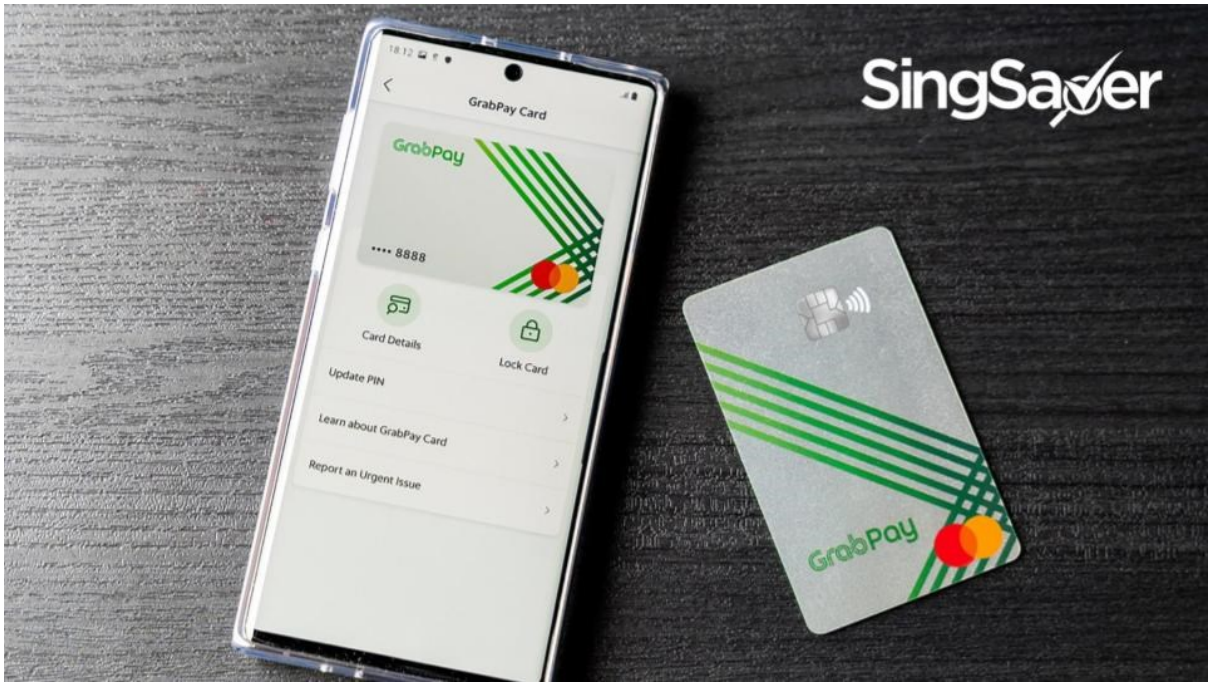

Figure 2: Last 4 digits of a credit card is not considered sensitive information

d) Personal information questions

Information that is personal to the victim is commonly used as a "security" question to perform verification. There are two forms of attacks against this. The first is the limited number of likely answers to the question. Questions that fall into this category include "What is your favourite cartoon

character?" (for a certain age group, statistics would limit the likely answers to a small group) and "Where were you born?" (people would be often near the city of birth). The second attack is finding out the probable answer through research. According to research by Ariel Rabkin, 16% of "personal" information were publicly disclosed on social networks. For example, the victim may publish their date of birth. Even if the victim did not publish the date of birth directly, an attacker can use other information such as birthday greetings from other people as well as stated year of graduation to guess the date of birth. Other information (e.g. maiden name) can be deduced from public records. Data brokers (e.g. WhitePages, MyLife.com, BeenVerified) may also contain data of varying levels of accuracy.

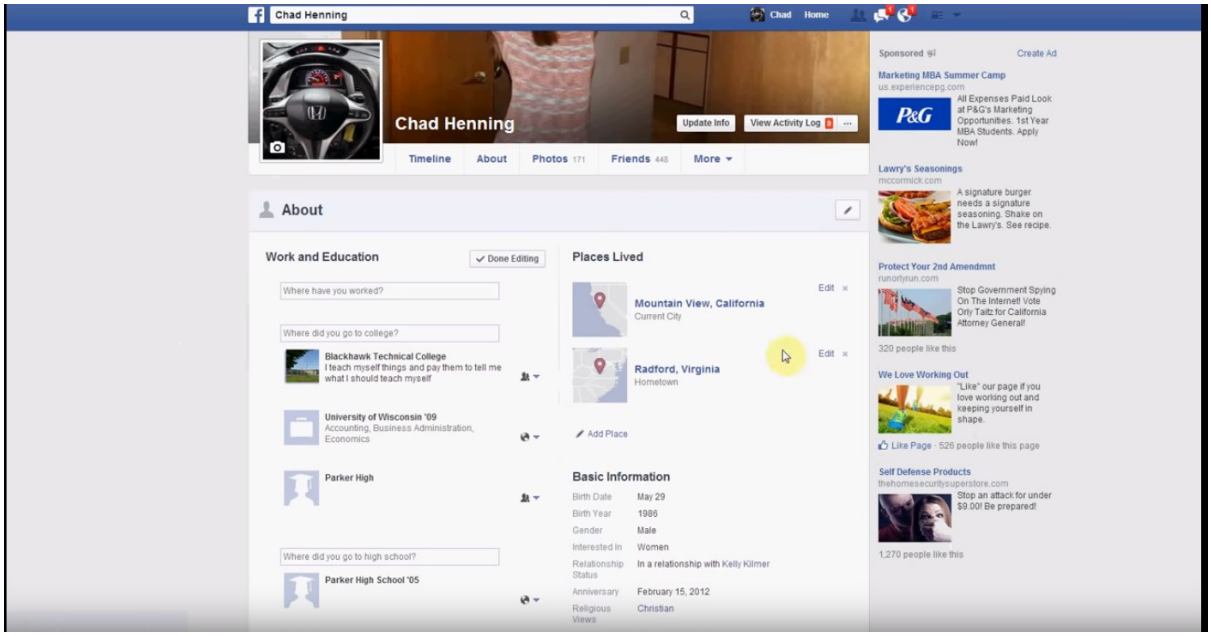

Figure 3: Facebook presents a trove of personal information (source: Youtube)

All these attacks do not include weaknesses of a service provider to vishing (phishing via phone). In the paper, the following apparent non-compliance to security protocol was observed:

- AT&T disclosed the month of the activation and last payment date to the unvalidated attacker
- AT&T allowed repeated guessing and provided feedback on whether the guess was getting closer or further away from the correct answer
- Tracfone and US Mobile did not perform authentication checks

Fortunately for Singapore residents, the procedure of most telecommunication operators (e.g. TPG, Starhub) is to require face-to-face presentation of identification before the telco will give a physical replacement SIM card to the requestor.

What can we do about it?

The following are recommendations you, as an individual, can take.

If your service provider (e.g. Twitter in 2018) uses weak authentication requirements such as the above, we generally can:

1. Move mobile service to one which is harder to SIM swap
2. Remove mobile numbers as a recovery number from those service providers

3. Consider moving to a better service provider 😊

The following are more detailed steps on how to perform these tasks:

Secure Google account

1. Set up a protected Google account (if you are not already using one) to use as a registered email and phone number
2. Get a US number via Skype, NexMo, Twilio or other means.
3. Sign up for Google Voice using the US number.
4. Configure Google account so that it is on the Advanced Protection Program(APP). This will require a Google account and an Android phone (Android 7 and later) or other compatible security keys.
5. Remove all recovery emails, phone numbers and security questions from the account, if any

Remove unnecessary fallback mechanisms

1. Facebook – Remove recovery phone numbers, enable PGP encryption for email notifications, enable second factor authentication as a requirement.
2. WhatsApp – enable two-step verification, use a phone number that is more difficult to SIM swap
3. Passwords – set up complex and long passwords for all accounts. If a password manager (e.g. LastPass) is used and supports it, use a security key as a second factor authentication requirement.
4. Set up two-factor authentication for all online services that support it. A security key is preferred, otherwise use Google Authenticator.
5. Remove recovery emails and phone numbers if you can.
6. Change recovery emails and phone numbers to the US Google Voice account for those services that require a phone number.

References:

I. List of 140 websites and methods of authentication: https://www.issms2fasecure.com/dataset
II. List of sites that support security keys: https://www.dongleauth.info/
III. Princeton university draft paper: https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf
IV. Protective steps against SIM swapping: https://www.vice.com/en_us/article/zm8a9y/how-to-protect-yourself-from-sim-swapping-hacks
V. Google Advanced Protection: https://medium.com/revissolutions/an-introduction-to-google-advanced-protection-90de57d61fc0
VI. Preventing and Responding to a SIM swap attack: https://medium.com/mycrypto/what-to-do-when-sim-swapping-happens-to-you-1367f296ef4d (note: estimated 51 minute read)
VII. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43783.pdf
VIII. OccupyTheWeb. (2019). *Linux basics for hackers: getting started with networking, scripting, and security in Kali.*
IX. Passwordless Authentication with SMS https://auth0.com/docs/connections/passwordless/guides/sms-otp