25th of August

Information Security Report

Contents

1.Introduction:

a) Significance of mobile phone security :

Since our mobile phones have a great number of personal data such as official name, phone number, address, your workplace, date of birth, etc…, it is really important to secure our device from any security attacks, information disclosure by all attackers. In addition, our devise has been significantly convenient to improve our daily life, such as these devices can be used to pay, access to buildings, and these devices are already part of our life. If our devices are compromised by some unauthorised people, there are no way to get lost devices found even though there is some apps to find lost or stolen devices. Moreover, since most people use a smart phone, the idea of compromising data have already spread, and which makes unauthorized people include attackers easier to compromise data.

b) Purpose of this report:

This article deeply explains the importance of mobile devices security discussing real-world security incidents and issues with four sections (apps, operating systems, mobile device user behaviour, and a physical threat to a mobile phone) and specific detail of mobile devices that I currently use. In addition, privacy analysis, which describes a policy for an app we usually use in our life and how information is collected in apps are discussed. As for the mitigation of these security issues are provided in part 5 of this report discussing how to prevent our mobile devices and personal information from a security breach and being collected by applications. These mitigations will be useful for all those people who use applications on the phone to protect.

c) These days, the mobile device is getting used in the wide-area by a great number of people in the world. However, the more people use mobile devices and developing application and new functions such as new operating systems or new password managing systems, the more vulnerabilities and security incidents might increase, and mobile device users should be able to know how to prevent their devices from being attacked by unauthorized people. Whether personal user input has been collected by companies created apps should be fully discussed and pursued by many

articles and experts to understand and prevent the third party to be able to use user personal information. In order to improve security understanding for users, knowing how to prevent issues are significant not only protect our devices but also the total amount of loss associated with these security attacks could decrease.

d) Since this article only covers security incidents on smartphone and other incidents associated with phone operating systems and applications there are some limitations, especially for other security areas.

2. Context establishment

a) a brief description of information assets

i) Device Hardware

The apple technical specification. (n.d.) explained

Chipset: iphone 7 use A10 fusion chip, 32GB of memory.

Display: When it comes to screen, Retina HD display, 5.5 inch(diagonal) wide screen LCD multi-touch display with IPS technology, 1920-by-1080-pixcel resolution at 401 ppi 1300:1 contrast ratio (typical)

According to GSMARENA (2019) Wide color display (ps3) 625 cd/m2 max brightness (typical)

Dual-domain pixels for wide viewing angles

Fingerprint-resistant oleophobic coating

Support for display of multiple languages and characters simultaneously

Camera: 12MP camera f/1.8 aperture Digital zoom up to 5x

SIM: Nano SIM

Power and battery:

Built-in rechargeable lithium-ion battery

Charging via USB to computer system or power adapter

Communication component:

Face time audio, video formats supported : HEVC, H.264, MPEG-4 part2, and Motion JPEG.

Audio Playback:

audio formats supported: AAC_LC, HE_AAC, stero speaker

Active noise cancellation with dedicated mic.

Headphones: EarPods wit lightning Connector

ii) Software

Operating System: IOS 12

IOS 12 is faster than the previous version in terms of swipe to camera, keyboard display, launch under a heavy workload.

3D Touch, Siri will suggest useful app shortcuts to help the user by notifying messages when it is needed. Moreover, According to the Kelly (2018) The IOS try to help user healthier balance using a smartphone, new screen time features will tell us how much time we spent on specific apps and screen time and how much they lost battery. Also, Siri is more often used in other apps.

Preinstalled apps:

Camera, photos, Heath, Messages, Phone, Facetime, Mail, Music Wallet, safari, Maps, Calendar, itunes store, App store, Notes, Contacts, books, Home, Weather, Reminders, Clock, Stocks, Calculator, Voice Memos, Compass, Podcast, Watch, Tips, Find my phone, Find my friends, Setting, Files, Measure.

Facebook, Linked in, Line, Instagram, youtube, Uber, Didi, BBc news, twitter, Evernote, Slack, QUT apps, Google maps, Oulook, google drive, music, lime =, olacabs, smartnews, My translink, Netflix, gmail.

iii) Data:

25.8 GB out of 32 are used as it is now, more than one quarter is used by Apps, such as Music and game apps, but mostly numbers of music occupy great part.

Next used data is photos, about 3.86GB is used, followed by Media like news apps, and other SNS.

All other use of data is as follow below:

Line: 767.1MB

Google: 474.9 MB

Facebook 335.6 MB

Messenger 332.9MB

Youtube 289.MB

Netflix 216.2 MB

b) An overview of your use of the devices

i) Level of criticality of all items/applications and data.

A chipset of smartphones is a significant factor regarding a device's speed include use of applications, set up applications, and other great of part of the operating system. In other words, the ability of smartphones depends on which chipset attached to it. In the case of the iPhone 7, it uses A10 fusion chip with 32 GB whereas, the latest model use A12 Bionic chip with 64-bit architecture.

Concerning memory of the smartphone, the more memory it has, the more user can add data to their own devices, in other words, user can add more and more applications, photos, videos, etc... Memory is critical part considering the smoothness of use of a smartphone.

iPhone 7 has either 32 GB or 128Gb.

The battery length of the iPhone series is inferior to other company devices. Some smartphone is heavily used more than 24hours without any charging, whereas iPhone 7 can only keep used within 24 hours.

Some preinstalled apps play an important role in using iphone7, like Maps, facetime, calendar, camera, clocks, etc… Those items are potentially used in our daily life to help our society. People no longer need to bring a small camera, moreover, people no longer need to bring a clocks.

Not only preinstalled apps but also some other apps could also often be used to increase the efficiency of our life. For example, Translink, transit, google maps, those are all apps used for finding bus timetable and appropriate bus lines to plan our small trip easily.

In terms of data importance, as discussed in 2.a, mostly apps occupy a quarter of data use. Each apps stores data on its app itself. For example, the music app store several songs, line or Facebook messenger store several texts respectively. Once it is exposed, that might be unfixable forever, and once those are all deleted without any backups, the lost data might not be able to recover as it used to be. In addition to the photo, all photo is also difficult to recover once it is deleted. However, in the case of exposed of apple ID, it could lead not only

to loss of data, but it could lead to compromise the stolen data for purchasing, reused by an unauthorized user.

The Sensitivity of the data (CIA)

As discussed above, being exposed to critical data from our smartphones could be compromised variously by unknown people, such as phishing emails, unauthorized disclosure, etc…

If a password has been stolen and unauthorized people rewrite the password, users cannot access their account and also, an unauthorized person could buy apps or pay without any permission. This is a compromising of availability and integrity. However the possibility of losing passwords is not high, but still, there is some chance.

Moreover, a person might have some photos that they do not want it to be exploited, such as private or confidential photos. Once the photo data is stolen or exposed to the public, it might be considered that confidentiality is compromised.

ii) The apps I often use are google maps, line(message application), Instagram, Facebook, mostly SNS. In contrast, apps I rarely use are a calendar, setting, other games. I found that I tend to use SNS rather than other apps.

3. Risk assessment

3.a **Title**: EVERYTHING WE KNOW ABOUT FACEBOOK'S MASSIVE SECURITY BREACH

Author: Louise Matsakis and Issile Lapowsky

Reference details (if online article, give URL and date accessed):

Matsakis, L**.** and Lapowsky, I.(2018, September 28). *EVERY THING WE KNOW ABOUT FACEBOOK'S MASIVE SECURITY BREACH.* Retrieved from:

https://www.wired.com/story/facebook-security-breach-50-million-accounts/

Date accessed: August 18, 2019.

Brief Summary: EVERYTHING WE KNOW ABOUT FACEBOOK'S MASSIVE SECURITY BREACH is an in-depth article describing massive data breach took place by Facebook on the 25th of

September in 2018. Besides, how Facebook corresponded to the massive data branch after the attack are described in each process.

Information asset: According to the article, approximately 50 million user accounts are breached associated with the attack and also attackers could have seen any profiles of victims. Whether stole data are compromised or not is unclear so far. Besides, all applications that use Facebook accounts might have been affected.

Security issue: **Threat**: This security incident is an external threat caused by deliberated human action who tried to attack a Facebook account to breach information. The attacker took advantage of multiple Facebook's vulnerabilities and earlier than the week, one hacker deleted Mark Zuckerberg's account from Facebook. As a result, a great number of personal information has been breached. Not only Facebook affected, but also many apps that use Facebook's authentication have been affected. The attack would compromise security goal confidentiality since the attacker utilized Facebook's vulnerabilities.

Vulnerability: There were some vulnerabilities and bugs found in the Facebook application. The first one is where a third company wrongly attempts to use a then-legitimate quiz app (Matsakis.L, n.p.) that allows an attacker to take over accounts. Moreover, up to 14 million user account has been publicly posted and anyone could access the accounts.

Security incident/attack: The article illustrates how 50 million Facebook accounts have been exposed by the attacker and why explaining the process and vulnerabilities in Facebook rather than as a security incident. Facebook logged out 40 million accounts to prevent from being more affected to reduce victims. This attack should be called an active attack from the attacker using vulnerabilities and bugs and breach 50 million user's accounts. Some researchers said, "This is a complex interaction of multiple bugs".

3.b **Title:** Google researchers discovered serious ios security flaws

Authors: AJ Dellinger

Reference detail: Dellinger, A,J(2019, July 30). *Google researchers discovered serious ios security flaws.* Retrieved from: https://www.engadget.com/2019/07/30/google-project-zero-ios-interactionless-vulnerabilities-apple/

Data accessed: August 20, 2019.

Brief summary: The article explains that Google security researchers found several security vulnerabilities that were fixed in the iOS 12.4 update. The researcher founds so-called

"interactionless" bugs, which allows a hacker to access to other people's phone without any permission.

Information Asset:

The involved asset was iPhone IOS itself, which can be exposed and taken over using just simple applications preinstalled in all iPhones.

Security issue:

Threat: The vulnerability found on IOS could have been compromised by a malicious attacker by sending malicious code through iMessage if some people open the malicious code.

These attacks could have happened if the researchers have not found the bugs, and also could have considered as an external threat, due to attacker could have attacked deliberately. Besides, other vulnerabilities allowed some attackers to leak all data from iPhone memory by reading files.

Vulnerability:

The researchers found there were six vulnerabilities in IOS, and four of the uncovered vulnerabilities could compromise without any interaction between iPhone users. According to the article, Even though after the latest version of 12.4 patched, it still not remediated the bugs. All data stored on iPhone users could have been considered dangerous, even though the user does nothing that is considered dangerous.

Security incident/attack: "Google researchers discovered serious IOS security flaws**"** is an in-depth article describing all the vulnerabilities and potential attacks associated with the bugs. The article describes that those bugs are considered as a potential attack. This would be considered that security goal confidentiality and integrity would be compromised due to an attacker can execute and control IOS using remote applications.

3.c**. Ttile**: The Rise in Mobile phishing Attacks

Author: Elliot Volkman

Reference Detail: Volkman, E.(2019, May 29). *The Rise in Mobile Phishing Attacks*. Retrieved from: https://info.phishlabs.com/blog/rise-mobile-social-engineering-phishing-attacks

Date Accessed: September 29, 2019.

Brief summary: The Rise in Mobile Phishing Attacks is an in-depth website describing typical phishing technics on a smartphone, which the group of the authors has observed and found

through analysis. Besides, the author also describes mobile malware trends by comparing mobile phone operating systems with numbers and percentages.

Information asset:

The involved information assets are username and passwords stolen by phishing through SMS, the user tends not to be aware of malicious SMS due to it is hard to track where it comes from. According to the author's statics, about 74.85% of all mobile OS that is easily be targeted is Android Systems, but IOS is low with 22.94%.

Security issue:

Threat: The process of sending malicious code to SNS randomly should be considered as an external threat, due to attackers send an email with malicious URL especially and once victims clicked the link attacker sent, an attacker could easily access to victim's account. This may offend security goal confidentiality, integrity and availability since user password and username are stolen and the attacker could rewrite the passwords that lead users might not be able to access to original accounts. Moreover, since the phone number is easily exposed in the internet environment.

Vulnerability:

There is no vulnerability in SNS systems, but the user could be vulnerability due to users tend to think SNS is secure and they do not expect to get malicious messages from the attacker. Besides, SMS and text messages do not filter phishing messages, and any messages could be delivered.

Security incident/attack:

The article describes how an attacker lets people click malicious code using SNS. An attacker sends a fake email pretending, such as the account has been deactivated since there was some fraud, and let the user put user name and password. This process of attacks might be considered as an active attack due to attackers send malicious messages.

3.d **Tile**: Watch Out For SIM-Swap Attacks

Author: Anthony Caruana

Reference details:

Caruana, A. (2019, Jun 17). *Watch out For SIM-Swap Attacks*. Retrieved from: https://www.lifehacker.com.au/2019/06/watch-out-for-sim-swap-attacks/

Date accessed: August 23, 2019.

Brief summary:

The Watch Out For SIM-Swap attacks is an in-depth article explaining the possibility of security incidents associated with losing a phone, which is called 'SIM-Swap Attacks'. In addition, detail of the attack and how the attacks are like are illustrated with a real-world example, and also how to prevent the attacks are described.

Information asset:

The consequences of SIM-Swap Attacks reach a great area of all information assets of a smartphone, such as a user name, passwords, phone number, and a number several logs in detail if the stolen user name and passwords are used in wide-ranging. People might not be able to access their original account once it is stolen and compromised by specialists of the attack.

Security issue:

Threat: The SIM-Swap Attack is an attack that occurred in which a smartphone is stolen by attackers somehow, or even phone users leave their phones for just a few minutes. Attackers tend to attempt to send a new update with the stolen SIM cards to some companies to disconnect from the original user to the SIM. This leads the original user who lost a phone not to access their account even though try to send a message or phone call to phone company due to the attackers already changed the system.

The attack would be considered as compromising security goal Confidentiality and Integrity and Availability due to a user could access user's passwords to access to different kinds of accounts, and also user lose accessibility to their original account, also passwords and user name might be changed. This should be considered as an external threat.

Vulnerabilities: There are some vulnerabilities in how people think towards to SIM card system. Smartphone user tends to consider phone numbers are not a significant factor of vulnerabilities when attackers try to compromise. Moreover, users do not set two-factor system or PINs to its account.

Security incident/ attack: The article illustrates the process of SIM-Swap attack and security incidents with the attack. Attackers changed a SIM from stolen mobile devices to update SIM account and attackers can intercept user's phone calls and text messages in order to find information of two-factor user authentication to take over an account. The attack could be considered as an active and theoretical attack.

Conclusion:

This report deeply explains security vulnerabilities and threats associated with mobile devices and also the details of mobile devices such as version, memory, stored data, pre-installed apps, etc, are about iPhone 7 which is the one I currently use. As I proceed with the report of the first part, I found an article that describes vulnerabilities of iPhone operating system IOS version 12.4, which is my iPhone's current version. According to the article 1.a, there were threats and vulnerabilities associated with missive data breach from Facebook. Since I use Facebook apps and have a Facebook account, I would assume that my Facebook account has also been compromised during the incident. This reminds me that we are always in the environment where our personal details easily to be exposed as long as we use application.

According to the article 3.b, there are some vulnerabilities found in the version with iMessage (iPhone's pre-installed app). That means that some attacker could have sent some malicious messages through iMessage apps, and I might have received them before. Besides, if I had clicked the RL from the attacker, my phone could have been taken over by those attackers due to the vulnerabilities. With regard to article 3.c describing security incidents by user behaviour, which is also about iPhone, statically speaking, people tend to think SNS is a secured app.

However, this might leads smartphone users to be in dangerous situations where users are easily compromised by attackers due to lack of knowledge. Obviously, it is really important to know the security issues and processes to prevent attacks. In addition, Android phones have a much more high chance to be attacked by bad people compare to iPhone. In summary, People definitely have to be able to distinguish whether received emails are phishing or legitimate, when attackers say like "you are account has been stolen by fraud, so please log in with your username and passwords" in email, otherwise, attacker easily can compromise all information.

As for the article 3.d, explaining typical attack of mobile devices called SIM-Swap, briefly discuss that if people lost or their smartphone has stolen by bad people, an attacker might swap the SIM card used in the stolen devices to compromise all stored data, phone number, passwords, and username respectively. As I discussed in the above part, the process is extremely simple, which means that after a lost smartphone or noticed

smartphone has stolen, people should immediately correspond to prevent the lost smartphone from being compromised.

To sum up, by searching real-world security incidents, I found that there is a significant number of attacks are being taken place in various parts of our life.

4. Privacy Analysis:

a) Privacy policy Summary

(i) **The name of the app:** Line (Messenger apps mostly used in Japan, Taiwan, Thailand, Indonesia).

Contents described in 4(a) are provided by Line official web site's privacy policy. The privacy policy is available in the link below. The policy describes the reason why the company collects personal information. https://terms.line.me/line_rules

(ii)(iii) **The type of information the app collects and How the information is collected:**

a) Phone number: User's phone number is necessary to authenticate whether the account is reliable or deter unauthorized or fraudulent use or abuse of services. In addition, if users decided to let the apps to enable "Allow Others to Add" feature, a stored phone number is used to add friends who have the user's phone number automatically as a Line friend.

b) Device type, OS type, IP address, cookie data, ad identifier, browser information, language settings: That information is important when the apps want to differentiate between phone type, OS, to adjust the proper setting.

c) Email Address: if users try to access their account from multiple devices, the apps utilize and store registered email account associated with passwords and PIN number.

   The data will be collected s user provide their email address so that makes the account available from different devices.

d) Line Id and Geolocation: If users wish to make other people easy to add via Line ID, The app collects Line ID. If users accept notification from the app asking "Would you allow the app to use your location?" once the user accepts the notification, the apps use the user's GPA and find near people around the user.

e) Payment information: If users choose to buy additional services, such as Line Sicker, Line game, etc…, then Line will ask users to put their bank account or credit card number to proceed the payments. This is how Line store people customer's bank detail.

(iv) **When the information is collected**

- *Phone number*: The app collects and uses user's personal information when they try to create a Line account, and then the app will ask users to provide a phone number.
- the app collects and uses user's personal information when they try to create a Line account, and then the app will ask users to provide a phone number.
- *Device type, OS type, IP address, cookie data, ad identifier, and browser information, language settings*: This information will be obtained by the app if users use the apps. Those data will be automatically collect once the user downloads the apps.
- *Email address*: The data will be collected s user provide their email address so that makes the account available from different devices.
- *Line Id and Geolocation*: The information will be collected once the user accepts the requirements from the app as a notification.
- *Payment information*: When User tries to extend the functionality in the app, and wish extra services, user have to pay either via Credit or credit account.

(v) How relevant the collected information is to your use of the app

a) *Phone number***:** Since the app is an SNS app, in terms of authentication and security reason, collecting user's phone number is a necessary process to the app. If the app could be used by us as with only email accounts, it would be easy for attackers to have many user accounts, which leads to increase security problems, such as fraud, sextortion, and phishing attack. Since phone number is a unique value for all devices, a collecting phone number is important and appropriate.

b) *Device type, OS type, IP address, cookie data, ad identifier, and browser information, language settings*: All those data above are most appropriate to be collected in terms of understanding the languages of each device. In addition, IP address, OS Type, cookie data, are also a significant factor due to differentiate each device from others and have to be able to be used by great numbers of phone type. However, collecting that information is important and relevant for the use of an app.

C) *Email address*: Email is also used when the app wants to send the message to customers and when a user forgets their passwords, the app will send a link to the customer to reset the old passwords. However, there may be some possibility of exposure of emails.

d) *Line ID and Geolocation*: Storing Line ID does not affect users directly due to the ID are kind of unique values that are not used in different purpose except for the use of the app.

However, as for the Geolocation, the stored location data might cause some problems if the data have been exploited by somehow. As an example, an attacker could utilize stolen data for a different reason, such as user can always track where the specific person is or they might even send exploited data to third people. As a summary, collecting and storing geolocation data has to be highly secured.

e) *Payment information*: Payment information is always necessary for sales purpose, otherwise there are no ways to collect money from the user, but having user payment information has high responsibilities and hard to prevent from unauthorized attack.

(VI)How the information is used by the app provider

- *Phone number*: Line use user's phone number to verify who they are, and allow a customer to transfer their account easily just using their phone number**.**
- *Device type, OS type, IP address, cookie data, ad identifier, and browser information, language settings*: Collecting that information enables customers to notify any issues using the app and to improve the customer support.
- *Email address*: This allows users to check their account detail and password as they forgot. In addition, the app notifies the user about important information from the app and updating information.
- *Line ID and Geolocation*: Collecting location allow us to find friends nearby them using function call "Find a person nearby you". In addition, according to the Line privacy policy (2019), "we provide features that utilize geolocation data for your convenience and to improve your user experience." As for using Line ID, also allow a user to find their friends easily.

(Vii)How long the collected information is stored for, and how and where it is stored.

- **How long the collected data is stored:** Line keep retain the collected information from the user as long as the account is active, associated with complying laws and regulations. According to Line privacy policy(2019), there are some possibilities that Line retain stored data after the account stopped if to comply with laws, legal obligations, to provide and complete support, to identify any unauthorized activity such as abuse or fraudulent of accounts.
- **How the collected information is stored:** Line has to implement organizational security standards and technical team to prevent personal information from security attacks and any other disclosure, alternation.

a) **Where the collected data is stored:** All collected data is stored in Japan where Line Corporation located.

(viii) Whether encryption is used for data transmission and/or storage.

Encryption is not used in the Line app according to Line privacy policy (2019).

(ix) Whether collected information is shared, whose information may be shared with, and how the shared information may be used by third parties:

According to the privacy policy website, Line admits that all stored data from the user is not transferred to another third party. As for my opinion, I read some article about the company saying, since 84% of the stock is occupied by Korean, but a high percentage of the user using the app is Japanese. In addition, according to an article, the Korean government officially admitted that as a national government, they store all message, photograph, and all personal information by the app.

(x)**Whether you have access to the information held and, if so how to obtain access to your data:** there are no ways to access to held information due to Line described they never give anybody personal information in the official website.

B) Privacy risk identification

(i)Identify the risks. Which sort of analysis can you perform – quantitative or qualitative? : According to Conner(2019), there are so many apps which steal our data with more than 1000 Android apps. One research found that some apps can even access to all smartphone devices data without any permission, and these apps can gather data from our Wi-Fi connections. One app called Shutterfly is one of the famous photo editing apps, but the app used to collect user's GPS coordinates from user's devices without any permission. In addition, other research found that up to 1,325 apps that collect user device data regardless if people accept permission, and hidden code that gathers user data are used from metadata stored in images and Wi-Fi connections. Furthermore, approximately 13 apps are listed since these apps can rewrite IMEl information to the file. The study found that user's personal data have been collected via a Wi-Fi network and router's MAC address.

Obviously, there are some risks of collecting data from apps. In this analysis, quantitative analysis are utilized to analyse and identify the risks associated with data collection of some apps.

(ii)Risk analysis and evaluates analysed risks:

the process of collecting information by apps, there are about more than 2000 potentially fake apps on Google Play even Line, where most android apps are sold, are used by attackers and it is very hard to detect which one is fake or not and also 20140 potential counterfeit apps are found. 5 researcher from University Sydney has spent two years to analysis more than a million of google play apps as part of security research. This researcher found that the reason of increasing numbers of fake apps on the Google Play is because of Open app system of Google play technically decrease the security level and make the web site relatively easy for attackers to use the web site to publish fake apps publically. The counterfeit app includes some famous apps like Line, free flow and hill climb racing, and that makes the effect more damage. Moreover, the research found that a few counterfeit apps request dangerous access data permissions event though it does not contain any malware.

As examples, the researchers provided some common mistake user often make in terms of data security. First, a common mistake is that some time user download apps on Google Play that only explicitly released on Apple Store. That indicates that if there is an app that only released in one place, not two places, the app has been created by other people and it is intended to be used in unauthorized use.

a common mistake is that using some time download apps inappropriate website, which is not the official web site of the specific app or Google Play Store and Apple store.

assigns treatment priorities with justification: In addition, the researcher also provide some solutions of how to avoid being victims, such as when user try to download app from website, user should check whether the website is authorized or not, and also metadata is also an important factor to detect fake app or not, moreover, to check the numbers of people installed the app is also important due to fake apps tend to have less download numbers compare to official apps.

(iii) Outline any limitations in the process or discuss difficulties you encounter in completing the risk analysis: The risk analysis might have some limitations due to only

three websites cited for the risk analysis and some cited web sites are not officially published.

(C) A Privacy conclusion:

(i) How frequently do I use the app? How is it important to me? What sort of information is involved? : The app I discussed in the risk analysis is called Line, which is a messenger app used widely in Japan, Taiwan, Indonesia, Thailand, etc…
I use the app every day when I contact with my friends and family, as a Japanese, I could tell that the app has been used by most Japanese since around 2014, as far as I know. After smartphones were widely used by a bunch of people, people had to choose either use SNS by phone number or other apps like Line. Then, people end up using the Line app since it is convenient compared to SNS and it is more functional. As one of a user of the app, I have my own Line account and ID, and also provided my phone numbers, email, a password for more convenient use of the app.

(ii)Which assets are at most risk? And vulnerabilities, threats: Line ID, phone numbers, passwords might be exploited easily since there are so many cases that accounts have been hacked by somehow in the app. Besides, as vulnerabilities, since the user can add people via the phone number, every person could send messages to anybody. This is obviously a vulnerability, an attacker could use the function to send malware by sending messages randomly by collected phone number, which is a threat from attackers. I also have some experiences that some unknown people send me a malicious link toward my account somehow. In case if my provided personal information like email, phone numbers, and passwords were exploited from the app, security goal confidentiality is compromised, and if my passwords would have been changed by attackers, which is obviously compromising security goal integrity, and if I could not access to the original account, that is compromising of availability.

(iii) How is this connected to user privacy? How closely does the app privacy policy meet the requirements of Australian Privacy legislation? : In the Australian privacy legislation under part2, “An app must not collect unless the information is necessary for…”It is hard to tell whether Line follow the privacy policy or not by just looking at the official website. Whereas, in principle 6, which is about disclosure of personal information,

Line follow the principle due to, the official document say that they never provide any information collected to third party.

5. Risk Treatment:

5-A: Overview of Security issue from Part I section 3-A.

In section 3-A of the report, some vulnerabilities were found on Facebook on the 25ht of September in 2018, as results that lead security issues being exploited great numbers of user's user name and user's personal information. In addition, 5 million Facebook user has been affected associated with the attack, and there were some chances that the attacker could have compromised the victim's profile that is not supposed to be seen by anyone except the owner user. The attacks would compromise confidentiality due to a bunch of personal information were compromised. Since some of these occurred vulnerabilities were made by a human, it is obvious that the developer always has to be able to care about any security vulnerabilities.

a). Briefly explain what the control measure is how it works.

Having Knowledge of security vulnerabilities as a software developer would be helpful to reduce risks of security vulnerabilities, and having confidence about security also makes communication easier with security experts (Bradbury, 2019). Besides, to check any existed vulnerabilities in the app people work with is also significant in terms of knowing the vulnerabilities. According to the Bradbury(2019), to do security testing using simple testing tools is also essential to reduce any security vulnerabilities.

b) Type and categorize of the control measure.

This is a preventive measure intended to train app developers so that they have enough knowledge to prevent having any security vulnerabilities during the process of making apps, and also how to take advantages of testing security vulnerabilities to prevent issues. These suggested ways are provided by Bradbury to improve developer security idea.

c) Degree and asset of provided protection.

A few experts alert in a situation where application developer does not have experts level of knowledge in security protection. As a solution described above, learning security

vulnerabilities. This would reduce any security vulnerabilities. In addition, constant testing of developing apps would also reduce the likelihood of vulnerabilities.

d) **Limitations or another impact.**

Since Facebook is a huge company, it surely they hire security experts to prevent any issues. However, in some development and management process, Facebook cannot always be in charge of every single process. As a result, sometimes, Facebook needs to rely on the third company, which leads to generating some vulnerabilities even though Facebook does not affect directly.

5-B: Overview of Security issue from Part I section 3-B.

As for the summary of section 3-b in part I, there were several vulnerabilities found on IPhone's OS systems called IOS. Those bugs are named as "Interactionless" by some researchers, which allows attackers attacker to be able to take over someone's phone control without noticing people. Even iPhone users just using the preinstalled app could be used to be compromised by the attacker. How this attack work is attacker just needs to send malicious messages through iMessage and if some user opens the malicious messages, the devices will be taken over. In addition, the researchers also found more vulnerabilities in IOS. However, after the latest patch, the vulnerabilities were not fixed yet. The attacks would compromise security goal availability since, after a phone was taken over, there will be no access and every information will be exposed.

a). Briefly explain what the control measure is how it works.

It is impossible to prevent having security vulnerabilities during the software development process in any software, whereas, still, there are several ways to secure any software, not 100% but mostly secure. According to Segal (2019), there are three common patterns that may get into software. Firstly, insecure coding practices would be the factor, since the developer needs to finish within the limited deadline and developing time, security vulnerabilities tend to be ignored or insufficiently corrected. Secondary, most applications use open-software that has vulnerabilities already, and those vulnerabilities are already known publicly. The last one is that every programming language has some vulnerabilities, which does not tend to be not cared for by less experienced developers. As for some control measures for the vulnerabilities, according to Segal (2019), some efficient ways such as

Shifted-Left security, validation of inputs and Encoding of Outputs, and authentication and session management are introduced.

b) Type and categorize of the control measure.

Those mitigations recommended by Segal are detective measures since all of the mitigation strategies were how to use some convenient tools to detect existed vulnerabilities. Besides, a Whitelisting is provided as one of validation.

c) Degree and asset of provided protection.

In the process of development, using information tools, for instance, OWASP can provide the best education management and guidance for vulnerabilities to make developers easy to identify flaws and learn. Furthermore, limiting concurrent access from the different users could reduce the risk of having vulnerabilities due to help to ensure only legitimate users can access the appropriate application.

d) Limitations or other impacts.

Described mitigation above is intended to be used by the manufacturer to prevent having vulnerabilities in application development. These strategies will efficiently reduce the risk of issues, and also help to develop and maintain easily even after it is released. However, as for the limitations, in order to utilize, users will be required to purchase external software.

5-C: Overview of Security issue from Part I section 3-C.

As for the overview of part, I section c, a risk of mobile phishing attack was described with real-world examples. As an example, some malicious codes have been sent via SNS to retrieve usernames and passwords from an unknown user by attackers and especially, Android phone users tend to be targeted from attackers, with 74.85% of all mobile OS. Besides, some vulnerabilities of smartphone users are also listed, such as users do not care about any malicious messages sent through SMS, because people tend to think that SNS is quite secured. However, for attackers, using SMS to send malicious code is simple since only phone numbers are needed to send. Phone numbers can be easily exploited and it requires some time and process to change phone numbers when the user needs to change. In section part, I c, user behavior is a significant factor to avoid getting involved in any attacks.

a). Briefly explain what the control measure is how it works.

Significant ways to prevent us from receiving strange malicious code via SMS are mainly separated into two parts. The first one is that examine texts from a company like a bank.

This indicates that user first needs to know any bank do not want to send messages often since they do not want customers to fall for smishing attack (SMS attack), and also people need to detect whether the used phone number is legitimate or not. In addition, the user needs to check the actual phone number used by visiting their website, all the phone number should be declared officially. As for the second key, there are some ways to prevent receiving malicious SMS.

b) Type and categorize of the control measure.

This article provides detective measurement explaining how to detect whether received messages are legitimate or not, and with real-world examples. In addition, those are also about preventive measurements since the author describes how to prevent receiving any malicious messages from the attacker.

c) Degree and asset of provided protection.

According to O'Donell (2019), the user needs to be suspicious of strange-looking phone numbers whet they received. If it is too suspicious or threating email, then it would be better to just report the emails to the local authorities and Internet Crime Complaint Center. Besides, O'Donnell provides some advice, which is to enable "block texts from the internet" feature if it is available since most phishing or spam emails are sent via internet text services to hide information of themselves.

d) Limitations or other impacts.

Those advice form O'Donell (2019) should be implemented by smartphone users to avoid to get involved by a malicious attack. These attacks would be avoidable in terms of the way the attacks work with the user's precise use of the SMS. Those do not affect other resources. Those introduced technics will not require any advanced skill or equipment, so they are used by anyone.

5-D: Overview of Security issue from Part I section 3-D.

In the part I section D, the SIM-Swap attack is described with details of the attack, which will occur when SIM-Cards are changed and swapped intendedly by somehow and it only just takes a few minutes to finish the whole process, obviously, for attackers, it will be useful and efficient way to compromise someone's data. The attack causes a significant effect once it is swapped. For example, attackers try to update the stolen SIM's information by visiting

some phone companies so that the disconnect between its original user and the SIM. If attackers attempt the whole process, there are no ways to recover personal information such as phone numbers, and usernames. Furthermore, all messages that are supposed to be sent to the original user are exposed to the attacker. This attack compromises security goal availability and confidentiality since there will be no ways to access to the original account and also, the original user's personal information will be exploited and compromised.

a) Briefly explain what the control measure is how it works.

According to Hesse (2019), it is essential to set up some defenses against SIM-Swap to protect mobile devices from SIM-Swap. The first step in SIM-Swap is based on malicious attack or some phishing tools. It is critical to make sure not click some unknown link. Besides, Hesse (2019) also provided some listed to protect accounts it is self. For instance, creating a PIN that is used when logins and passwords need to change, utilizing two-factor authentication, and using encrypted passwords manager, etc…

b) Type and categorize of the control measure.

This is a preventing control measure to set significant protection for SIM-swap attacks that are intended to swap someone's SIM cards by physically or phishing tools. Hesse (2019) provided some advice and real-world solution in general speaking.

c) Degree and asset of provided protection.

To be more frankly, as it is discussed above, creating a PIN, and using two-factor authentication are significant in terms of preventing the attack. Furthermore, strong answers security recovery questions, which should not be one guessed easily such as date of birth, and just in case of if smartphones are compromised, then the attacker could access other different SNS that are logged in my Facebook account. That indicates that using Facebook account to log in different SNS account help attackers to logged in easily.

d) Limitations or other impacts.

Those control measures provided by Hesse could be utilized by all mobile phone users to prevent mobile devices from SIM-swap attacks. Three control measure discussed above would reduce risk of the attacks and protect from any other security attacks associated with a physical mobile phone, furthermore, those measure does not reduce any external equipment, so these are easily utilized. In addition, those control measure does not introduce any extra risks.

5-E: Overview of Security issue from Part I section 3-E.

As for the overview of Part 4-b, more than 1000 Androids existed apps are revealed that those apps are suspected to steal all user's personal information by using fake apps that imitate existed popular apps. For instance, one app called "Shutterfly" is one of the famous photo editing apps, but it pretty much stores user's GPS location from the user's devices. Furthermore, approximately, more than 1,325 apps would collect user's personal information regardless of asking permission to the user or not, and some information might be stolen once they accept any request from the fake apps including WI-FI connection. As the reasons why those fake apps are still affecting significant damage, which is because of the difficulties of detecting any face apps compare to legitimate apps on the Androids google store. Some researchers provided some common ways to get affected by those attacks.

The user tends to downloads apps that are only released on the App store. Those series of attacks would compromise security goal confidentiality since the user's personal information is stolen unexpectedly by just using apps.

a) Briefly explain what the control measure is how it works.

According to Brown (2019), he provided 7 ways to secure our mobile devices from stealing our personal information and also be warned that some apps we still steal our mobile data event tough user turned off their phone. The first recommended solution is the use of a strong passwords manager, which keeps each different number of passwords to one place with only one encrypted and passwords-protected apps. While letting web browser such as Firefox or Google chrome to store our passwords, it would be better to use some strong passwords manager.

b) Type and categorize of the control measure.

This is the preventive control measure since those security attacks could be prevented by using some developed tools and improved by users with legitimate knowledge of the solution.

These solutions are provided by Brown (2019) with significant solutions against attack using fake apps.

c) Degree and asset of provided protection.

As for the other types of solutions, limiting social media from exposure, which means that even if user appeared on their friends or family members on apps such as Facebook or other SNS, it also causes some security exposure due to those apps are smart enough to make any advertisement that corresponds to what they are interested in. Besides, keeping software updated is also an efficient way to provide well security. That is because, attackers always to try to make another way to attack user's devices, thus user's mobile devices also need to be updated constantly.

d) Limitations or other impacts.

Those measurements should be used by smartphone users to protect their information from the security breach. Those tools are available by anyone who has the phone with intentional and constant care such as keep updating apps or to be more careful especially for the apps that are explicitly established in only one shop such as the App store if it is an iPhone and google store for Android user. As for some limitations, since those solutions heavily depend on user behaviour, users need to commit those efficient solutions precisely.

6 Conclusion

a) **Relate application:** There are different numbers of security risks and vulnerabilities as the numbers of people use a smartphone and other social network services increase these days. Thus, it is essential to prevent our devices and personal information from different types of attacks since even with one vulnerability could compromise personal information.
In part 1 of this report, some security risks associated with a mobile device application, operating systems, devices user, and any risks are discussed. As one of the examples, Facebook was listed to provide a real-world case of a security breach affecting significant damage. Besides, some vulnerabilities were found on the latest IOS version, which could be compromised by attackers with phishing or malicious attacks, and some preinstalled apps were also found that might cause some risks with phone numbers. In part 2 of the report, how mobile apps collect user's personal information or other security data from users were discussed based on Line (messenger apps). As the research proceeds, Line collects several data from user's devices such as Phone number, Device Type, OS type, IP address, cookie data, email address, etc…. According to Line, that collected information is used to improve the customer service quality and to make the use of Line easier. However this collected information is necessary for terms of providing better apps to users, and once the user accepts some notifications from apps, those apps start collecting apps automatically. Thus, the user needs to be serious about some notifications or terms of use of those apps.
b) **Summarizing resulting information:** As some solutions of how to prevent those attacks, some researchers provide several ways. One is that when we try to install apps from websites, it is important to make sure whether those apps are appropriate or not. Use always need to identify how those apps created and who created the apps. Besides, it is also important to check how many times the apps download. As for the how-to prevent any malicious code and phishing, I stared utilizing some solutions some researcher provided, which is, of course, checking phone numbers whether it is valid or not, and setting phone's security system that avoids receiving messages especially from websites were all spam and malicious emails come from. Importantly, all smartphone users include myself should know how to prevent SIM-swap attacks, such as having a strong passwords manager that contains all passwords and having PINs. To sum up, one of the best ways to protect our devices is to know real security attacks and ways of how to solve them.

7 Reference list

Apple. (2019*). iPhone7 Technical specification*. Retrieved fromhttps://www.apple.com/lae/iphone-7/specs/

Caruana, A. (2019, Jun 17). *Watch out For SIM-Swap Attacks*. Retrieved from: https://www.lifehacker.com.au/2019/06/watch-out-for-sim-swap-attacks/

Dellinger, A,J(2019, July 30). *Google researchers discovered serious ios security flaws.* Retrieved from: https://www.engadget.com/2019/07/30/google-project-zero-ios-interactionless-vulnerabilities-apple/

GSMarena. (2019). Full phone specification. Retrieved from https://www.gsmarena.com/apple_iphone_7-8064.php

Kelly, G. (2018). Apple iOS 12 Has 25 Great Secret Features. Retrieved from https://www.forbes.com/sites/gordonkelly/2018/09/18/apple-ios-12-has-25-great-secret-features-iphone-ipad/#762b34fe4048

Matsakis, L**.** and Lapowsky, I.(2018, September 28). *EVERY THING WE KNOW ABOUT FACEBOOK'S MASIVE SECURITY BREACH* . Retrieved from: https://www.wired.com/story/facebook-security-breach-50-million-accounts/

Volkman, E. (2019, May 29). *The Rise in Mobile Phishing Attacks*. Retrieved from: https://info.phishlabs.com/blog/rise-mobile-social-engineering-phishing-attacks

References list for Privacy analysis

Conner, K. (2019, July 16). *Over 1,000 Android apps were found to steal your data. Here's what you can do*. Retrieved from C net: https://www.cnet.com/how-to/over-1000-android-apps-were-found-to-steal-your-data-heres-what-you-can-do/

Lamont, J. (2019, July 8). *Over 1,000 Android apps ignore permissions and steal data: study*. Retrieved from Mobile Syrup: https://mobilesyrup.com/2019/07/08/android-apps-ignore-permissions-steal-data/

Line Privacy Plocily. (2019, May 31). Retrieved from Line : https://terms.line.me/line_rules

Read the Australian Privacy Principles. (2019, July 31). Retrieved from Australia Privacy Principle: https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/

References list for Risk treatment

Bradbury, D. (2019, Jun 24). *Mobile apps riddled with high-risk vulnerabilities, warns report*. Retrieved from naked security: https://nakedsecurity.sophos.com/2019/06/24/mobile-apps-riddled-with-high-risk-vulnerabilities-warns-report/

Hesse, B. (2019, Jun 20). *How To Prevent And Respond To A SIM Swap Scam*. Retrieved from https://www.lifehacker.com.au/2019/06/how-to-prevent-and-respond-to-a-sim-swap-scam/

O'Donnell, A. (2019, September 20). *Protect Yourself From SMiShing (SMS Text Phishing) Attacks* . Retrieved from Lifewire: https://www.lifewire.com/protect-yourself-from-smishing-sms-phishing-attacks-2487626

Segal, E. (2019, August 08). *Secure Coding: How to Prevent Vulnerabilities from Creeping into Your Software*. Retrieved from codemenor: https://www.codementor.io/eddiesegal5/secure-coding-how-to-prevent-vulnerabilities-from-creeping-into-your-software-xn487opv8

An appendix

3.a)

LOUISE MATSAKIS AND ISSIE LAPOWSKY SECURITY 09.28.18 03:03 PM

EVERYTHING WE KNOW ABOUT FACEBOOK'S MASSIVE SECURITY BREACH

FACEBOOK'S PRIVACY PROBLEMS severely escalated Friday when the social network disclosed that an unprecedented security issue, discovered September 25, impacted almost 50 million user accounts. Unlike the Cambridge Analytica scandal, in which a third-party company erroneously accessed data that a then-legitimate quiz app had siphoned up, this vulnerability allowed attackers to directly take over user accounts.

The bugs that enabled the attack have since been patched, according to Facebook. The company says that the attackers could see everything in a victim's profile, although it's still unclear if that includes private messages or if any of that data was misused. As part of that fix, Facebook automatically logged out 90 million Facebook users from their accounts Friday morning, accounting both for the 50 million that Facebook knows were affected, and an additional 40 million that potentially could have been. Later Friday, Facebook also confirmed that third-party sites that those users logged into with their Facebook accounts could also be affected.

"We were able to fix the vulnerability and secure the accounts, but it definitely is an issue that it happened in the first place."

—MARK ZUCKERBERG, FACEBOOK

Facebook says that affected users will see a message at the top of their News Feed about the issue when they log back into the social network. "Your privacy and security are important to us," the update reads. "We want to let you know about recent action we've taken to secure your account." The message is followed by a prompt to click and learn more details. If you were not logged out but want to take extra security precautions, you can check this page to see the places where your account is currently logged in, and log them out.

Facebook has yet to identify the hackers, or where they may have originated. "We may never know," Guy Rosen, Facebook's vice president of product, said on a call with reporters Friday. The company is now working with the Federal Bureau of Investigation to identify the attackers. A Taiwanese hacker named Chang Chi-yuan had earlier this week promised to live-stream the deletion of Mark Zuckerberg's Facebook account, but Rosen said Facebook was "not aware that that person was related to this attack."

"If the attacker exploited custom and isolated vulnerabilities, and the attack was a highly targeted one, there simply might be no suitable trace or intelligence allowing investigators to connect the dots," says Lukasz Olejnik, a security and privacy researcher and member of the W3C Technical Architecture Group.

On the same call, Facebook CEO Mark Zuckerberg reiterated previous statements he has made about security being an "arms race."

"This is a really serious security issue, and we're taking it really seriously," he said. "I'm glad that we found this, and we were able to fix the vulnerability and secure the accounts, but it definitely is an issue that it happened in the first place."

The social network says its investigation into the breach began on September 16, when it saw an unusual spike in users accessing Facebook. On September 25, the company's engineering team discovered that hackers appear to have exploited a series of bugs related to a Facebook feature that lets people see what their own profile looks like to someone else. The "View As" feature is designed to allow users to experience how their privacy settings look to another person.

The first bug prompted Facebook's video upload tool to mistakenly show up on the "View As" page. The second one caused the uploader to generate an access token—what allows you to remain logged into your Facebook account on a device, without having to sign in every time you visit—that had the same sign-in permissions as the Facebook mobile app. Finally, when the video uploader did appear in "View As" mode, it triggered an access code for whoever the hacker was searching for.

> **"There simply might be no suitable trace or intelligence allowing investigators to connect the dots."**
>
> —SECURITY RESEARCHER LUKASZ OLEJNIK

The social network already faces multiple federal investigations into its privacy and data-sharing practices, including one probe by the Federal Trade Commission and another conducted by the Securities and Exchange Commission. Both have to do with its disclosures around Cambridge Analytica.

It also faces the specter of more aggressive regulation from Congress, on the heels of a series of occasionally contentious hearings about data privacy. After Facebook's announcement Friday, Senator Mark Warner (D-Virginia), who serves as vice chairman of the Senate Intelligence Committee, called for a "full investigation" into the breach. "Today's disclosure is a reminder about the dangers posed when a small number of companies like Facebook or the credit bureau Equifax are able to accumulate so much personal data about individual Americans without adequate security measures," Warner said in a statement. "This is another sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users."

Facebook may also face unprecedented scrutiny in Europe, where the new General Data Protection Regulation, or GDPR, requires companies to disclose a breach to a European agency within 72 hours of it occurring. In cases of high risk to users, the regulation also requires that they be notified directly. Facebook says it has notified the Irish Data Protection Commission about the issue.

This is the second security vulnerability that Facebook has disclosed in recent months. In June, the company announced it had discovered a bug that made up to 14 million people's posts publicly viewable to anyone for days. This is the first time in Facebook's history, though, that users' entire accounts may have been compromised by outside hackers. Its response to this vulnerability—and the speed and comprehensiveness of the important disclosures ahead—will likely be of serious importance. Once again, all eyes are on Mark Zuckerberg.

Additional reporting by Lily Hay Newman.

3.b)

Google researchers discovered serious iOS security flaws

The vulnerabilities reportedly would have sold on the black market for up to $5 million.

AJ Dellinger, @ajdell
07.30.19 in Security

69 Comments

488 Shares

Six critical security vulnerabilities that were patched in the iOS 12.4 update released earlier this month were originally discovered by security researchers at Google. Natalie Silvanovich and Samuel Groß, two members of Google's Project Zero bug-hunting team, alerted Apple to the issues. Silvanovich will be laying out the details on several of the bugs and provide a demonstration of exploits in action at the Black Hat security conference set to be held in Las Vegas next week.

The majority of the vulnerabilities discovered by Google were so-called "interactionless" bugs, meaning they can be executed on a remote iOS device without requiring any sort of direct interaction with the phone. An attacker simply has to send malicious code via iMessage and wait for the victim to open it. Because these "interactionless" bugs are in high demand for hackers, the security flaws discovered would have sold on the black market or other seedy parts of the internet for as much as $5 million apiece, according to *ZDNet*.

While Apple largely addressed these significant security flaws with the release of iOS 12.4 on July 22nd, the researchers are holding back on revealing the details of one vulnerability that has not yet been fully patched. Users are advised to keep their phones up to date and download updates as soon as they become available in order to avoid any significant security risks.

3.c)

The Rise in Mobile Phishing Attacks

Posted by Elliot Volkman on May 29, '19

Find me on:

Each year new phishing techniques result in more attacks successfully landing in user inboxes. In most cases, threat actors are no different than anyone else, and follow the hottest trends in an effort to be more relevant. During tax season they may push out tax scams, during elections they may push bogus political-inspired healthcare emails, and there are even Game of Thrones inspired attacks, too.

Regardless of the latest fads, the one major shift in social engineering-based attacks is the technology in play. Fortunately, we don't yet have virtual reality-based attacks plaguing the planet, but with mobile, in particular Android devices, accounting for a majority of online traffic, it's becoming the primary target for threat actors.

The following are the primary findings that our team has observed and analyzed as part of the annual Phishing Trends and Intelligence report:

- In 2018, we observed a significant rise in SMS phishing, particularly targeting the financial industry.
- Most people open and read SMS messages reflexively, and don't expect to receive malicious messages.
- SMS phish are much more difficult for the security community to track and respond to than traditional phishing attacks.
- Mobile-specific phish kits accurately mimic login screens of legitimate mobile apps. In many cases, these kits contain files for both mobile and desktop phishing sites.

Tracking SMS Threats and Visibility

Let's break these down a bit further, starting with how the security community is able to track SMS attacks. Unlike a typical phishing email where it's easy to collect the header and report or forward it to a researcher, SMS attacks are more complicated.

Phone numbers can easily be spoofed, and the routing that leads to a text message landing in your message queue is not accessible. This means that the most common way to report an SMS-based phishing attack is through screenshots, which poses numerous issues, with the largest being that URLs may be truncated.

On top of this, SMS or text message filtering of spam is practically non-existent, which means any kind of malicious or spam will be front and center on a person's phone. This brings us to our next point regarding how users typically interact with text messages.

Mobile Makes a Fool Out of Us

Between a lack of filtering technology and our expectations that mobile devices are relatively secure, most users don't take the extra time to ensure content is safe. You would certainly never click on a malicious email, so how could you get fooled on mobile? Using simple tricks like URL padding, or taking advantage of small screen sizes and how much of a URL you can see, easily trick users into thinking a website is legitimate.

As a result, in the past year we've seen more SMS phishing, particularly for the financial industry. SMS phish are using the same fear tactics as the traditional email-based phishing lures, such as saying there's been fraud on the account and as a result has been deactivated. This, of course, encourages the user to try and reset the password, which then sends off the credentials to a threat actor.

We've also seen more phish kits specifically crafted for mobile-based phish. These phish kits present login screens similar to the bank's legit mobile login. A lot of kits also contain files for both mobile and desktop phishing sites. These kits check for a user-agent in order to determine if the user is on a mobile device, and if so, it will show the mobile version of the site.

Mobile Malware Trends

As Android OS continues to be the primary entry point for mobile traffic, the most prevalent mobile malware specifically targets the operating system. In total, Android makes up 74.85% of all mobile OSs, with iOS significantly behind at 22.94%, and those that follow make up less than a single percent each.

The most active and prevalent mobile trojans in the past year are: BankBot, RedAlert2, and Marcher.

As other mobile banking trojans fall by the wayside, these prevalent ones have seen other incarnations and shifts, too. In the past year, March 2018, we detected a new BankBot variant. BankBot Anubis incorporates ransomware, keylogging, remote access, SMS interception, call forwarding, and lock screen functionality.

The creators also develop more sophisticated methods to obscure command and control (C2) infrastructure, which makes it more difficult to shut down. Criminals behind BankBot Anubis used public Twitter accounts to post tweets containing encoded C2 URLs in an attempt to hide their C2 infrastructure. C2 information could be encoded in images or foreign language characters to avoid suspicion. You can read more about it in our report from late last year.

3.d)

Watch Out For SIM-Swap Attacks

Anthony Caruana
Jun 17, 2019, 9:30am· Filed to: Australian Stories

Share

Image: iStock

SIM-swapping attacks are becoming increasingly common. In these attacks, someone tricks your mobile carrier into porting your number so that you lose control of your phone number. The bad guys can then intercept your calls and text messages in order to capture two-factor authentication requests and then take over your online accounts.

It's a tactic used by identity thieves and those trying to steal valuable online handles. And, it turns out, that it's pretty easy to do.

Our mobile phones are becoming an important identity management device. That's happened over time as online services have been using one-time codes sent to our mobile phones and through authenticator apps and services.

In a sense, our mobile numbers are becoming as important as Tax File Numbers and, if you're from the USA, a Social Security Number, as a form of personal identification. But given mobile numbers can be listed in public directories, they are a pretty easy target for someone to find.

To test out how easy it is to carry out a SIM swap, I ported my son's number from my account with a major carrier to a mail-order pre-paid service. It turns out the process is trivially easy. And the only piece of information that's needed to make the change is the originating account number. No other authentication was requested or needed.

I followed up with the three big carriers about the magnitude of this issue. The response I received from Vodafone is indicative of how easy a SIM swap is and how powerless carriers are to stop it.

> Porting fraud and SIM swap fraud is a concerning issue for all mobile carriers. We can't stress strongly enough the need for customers to be vigilant for online scams.
>
> Unfortunately, if fraudsters obtain the personal details of customers, they can attempt to perform unauthorised number ports or SIM swaps, usually to attempt to gain access to the customer's bank account.
>
> We do everything we can to protect customers from fraud, including recently increased SIM swap security measures and monitoring for suspicious account activity. We strongly encourage our customers to ensure their personal information is kept secure and only provided to known, trusted sources.

A couple of years ago I reported on a low-tech burgulary that had a high tech edge. In that, a friend had some personal documents stolen when their home was robbed. Amongst the stolen documents were some phone bills. The thieves ported the number, ordered a new phone and took over his Google accounts resulting in the loss of years of photos.

My friend ended up getting a new phone number and losing years of photos, emails and other information.

I asked Telstra about SIM swaps as well.

Fiona Hayes, Telstra Retail and Regional Executive, said a "A SIM swap is considered a high risk transaction and therefore a one-time PIN is sent to the customer to ensure enhanced due diligence is undertaken".

So, while some carriers are taking steps, it's not universal. One potential way around this would be to have burner mobile number services. In the US, you can access services like MySudo that give you burner numbers that can be used to authenticate access without giving up your real number but those aren't available here yet.

In the mean time, it's really important to keep your account details well protected. Avoiding paper-based bills that can be stolen from your letterbox is a good place to start. And scanning documents you do receive, storing them securely and shredding the originals is also a good step to take.

SIM-swap attacks are real and surprisingly easy to execute.