Mobile Systems and Communications

CIS4020-N-BF1-2018

The Threats and defences for Mobile Applications (Apps).

Thomas Ruddock

Q5114161

Word Count: 4328

Tutor: Dr Naumen Israr

Teesside University

Contents

1 Introduction 4
2 Description of the area of Research 4
3 Research findings and solutions 5
3.1 Market Share 6
3.1.1 Small Solution 6
3.2 Security Models 6
3.2.1 IOS Security Model 7
3.2.2 Android Security Model 7
3.3 Security Threats for IOS and Android App Stores 8
3.3.1 IOS Apple App Store 8
3.3.2 Android Play Store 8
3.4 Online APK files 8
3.4.1 Small Solution 9
3.5 Root Access 9
3.5.1 Android Rooting 9
3.5.2 IOS Jail Breaking 9
3.6 Security threats and attacks from pre-installed app 9
3.6.1 Facebook 9
3.6.2 Twitter 9
3.6.3 Email 10
3.6.4 Text messages 10
3.6.5 Internet (Chrome, Firefox, etc) 10
3.6.6 Small solution 10
3.7 Security threats from pre-installed software 10
3.7.1 Bluetooth 10
3.7.2 Wi-Fi 10
3.8 Malicious Software 11
3.8.1 Small Solution 11
3.9 Solution 11
4 Conclusion 11
5 Reflection 11
5.1 Technological developments next 5 years 11
5.2 What went well/what did not 11
5.3 How might I go about doing it differently in the future 11
5.4 What has been learned from the experience 12
5.5 How this knowledge / experience might be applied in the future 12
5.6 Does what I find answer the question of what was intended to research 12

5.7 What needs work 12

6 References 13

7 Proposal form as an appendix 15

1 Introduction

In this research paper, there will be five main sections and subsections within them to keep the structure flowing to the end. This paper will talk about the rising effort of black hat hackers that are trying to infiltrate the general public's personal mobiles devices. Through shady websites which allow users to download apk files and malicious apps from the play store for Android and the app store for IOS. The paper will include the description of the area for this research. Also, research findings with the current state of the technology, hardware, and solutions which users can take to prevent these threats from happening. It will then have a conclusion of these findings all concentrated into this section after that will be the reflection which will be my views on the developments of these threats and fixes in the future. All references used for this paper will be cited within the paper and a full Harvard reference at the end of the paper.

One of the fundamental reasons for choosing this topic is the higher increase of mobile phone users worldwide in 2018 is 4.57 Billion mobile phone users and estimated to rise to 4.78 Billion in 2020, Statista (2018) provided information for the visit. Seeing the numbers from a credible statistic organisation, it is inevitable that hackers will try to access these devices for malicious intent. For this reason I would like to inform the older generations about these threats which they have might not have known about, for example my parents often gets tricked with phishing emails and had to tell them about these scams and get them to tell me about any email or text message about winning prizes to make sure they are or not scams, but most are. Even though I have knowledge about these threats the older generations don't. It is estimated that around £10 Billion is lost from the victims of scams each year in the UK and 43% of older people which is almost 5 million people aged over 65 are believed to have been targeted by scammers, Neighbourhood watch (2018) provided information for the visit.

2 Description of the area of Research

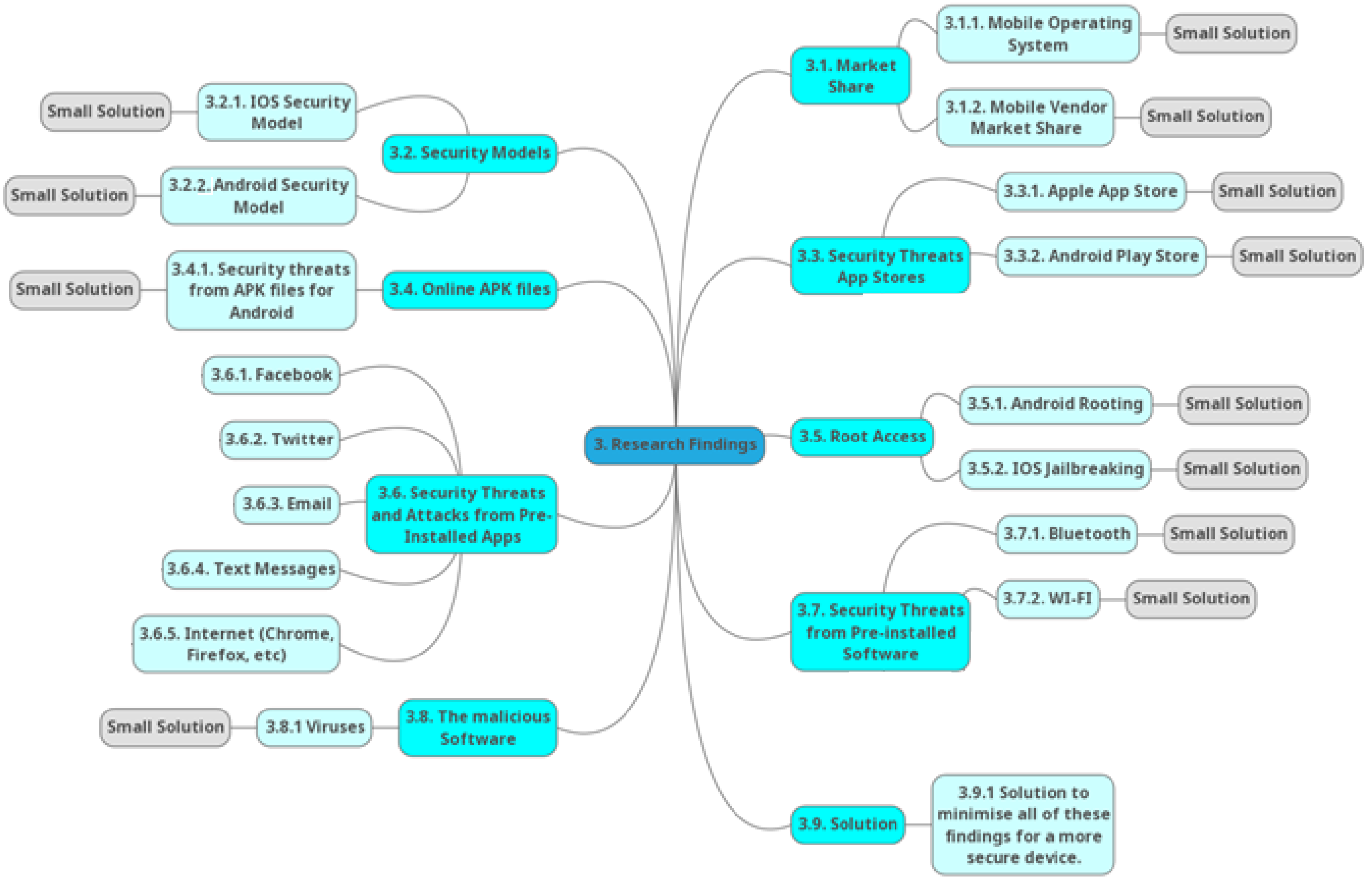
This section of the paper will present all the areas of research which will be more fleshed out in section 3 research findings. All the topics to be researched will have a small solution at the end of the sub-section in section 3, and it includes:

- Market Share
- Security models for IOS and Android
- Security threats to the mobile OS app stores
- Online APK files
- Root Access (Android/ Jailbreak (IOS)
- Security threats and attacks from pre-installed apps and software
- And the malicious software that is used.

These will help keep the users safe and less likely to have data stolen, money stolen or other sensitive information.

3 Research findings and solutions

The mind map below will show the structure of this section, the centre of the map in section 3. Research findings then have lines coming off to the sub-sections, which also have sub-sections under them and all have a small solution on each sub-section which gives the user a way to secure certain sections of the device. At the end of the section is 3.9 Solution this sub-section will have a solution which will cover all the threats presented, some solutions can be setting changes, anti-virus apps, and Googling for information for example, you don't recognise a number calling you can search the number online and will give the user information about it, for example, the location of the caller, and comments from other people who have had this call and found out they are scammers and will give the number a negative review.


3. Research Findings
3.1. Market Share
3.1.1. Mobile Operating System
Small Solution
3.1.2. Mobile Vendor Market Share
Small Solution
3.2. Security Models
3.2.1. IOS Security Model
Small Solution
3.2.2. Android Security Model
Small Solution
3.3. Security Threats App Stores
3.3.1. Apple App Store
Small Solution
3.3.2. Android Play Store
Small Solution
3.4. Online APK files
3.4.1. Security threats from APK files for Android
Small Solution
3.5. Root Access
3.5.1. Android Rooting
Small Solution
3.5.2. IOS Jailbreaking
Small Solution
3.6. Security Threats and Attacks from Pre-Installed Apps
3.6.1. Facebook
3.6.2. Twitter
3.6.3. Email
3.6.4. Text Messages
3.6.5. Internet (Chrome, Firefox, etc)
3.7. Security Threats from Pre-installed Software
3.7.1. Bluetooth
Small Solution
3.7.2. WI-FI
Small Solution
3.8. The malicious Software
3.8.1 Viruses
Small Solution
3.9. Solution
3.9.1 Solution to minimise all of these findings for a more secure device.

3.1 Market Share

The market share for Mobile Operating System and Mobile Vendor Market shares are a very fundamental issue, because of these the hackers will have a better chance on gathering user's data because the higher the shares the more likely they will get sensitive data from unexpected users. Below will be two tables one for the vendor market shares worldwide and mobile operating system shares worldwide all data for these tables are sourced from StatCounter (2018).

Table 1. Mobile Operating System Market Share Analysis

Operating System	Nov 2017	Nov 2018
Android	73.11%	72.35%
IOS	20.34%	24.44%
Windows	0.71%	0.39%

Just from looking at the table above it shows Android has been most dominant in the mobile OS market and because of that it is targeted more. For example, among the new malware attack vectors, Android continues to be the most targeted mobile OS, Symantec (2018).

Table 2. Mobile Vendor Market Share Analysis

Mobile Vendor	Nov 2017	Nov 2018
Samsung	31.88%	28.24%
Apple	20.34%	24.44%
Huawei	5.06%	6.31%
Xiaomi	4.38%	7.83%
Oppo	3.34%	4.23%
LG	3.52%	3.07%
Motorola	2.54%	3.02%
Lenovo	2.86%	2.15%
Mobicel	1.33%	3.42%
Unknown	7.46%	5.27%

Just by looking at the table above shows that Samsung and Apple are the two top devices both with different operating systems and most of the other vendors are using Android this shows all different types of Android versions that are used, for example, Lollipop, Marshmallow, KitKat, etc. All the OS versions have different security and update at different times. Symantec (2018).

3.1.1 Small Solution

Make sure to research what main OS you want to buy from, either IOS or Android and make sure to check the underlining version of the OS if you choose Android, once you have picked out the phone you want or already have to make sure to get a newer version of the device and make sure "Download updates automatically" is turned on, to keep the security up to date. Some vendors have been known to delay OS updates for many months, J. Gold (2016) provided information for the visit.

3.2 Security Models

For this I will talk about the security models and framework that the OS controlled by, each one of these sections can be their own research paper, but in these two-sub sections will be the basics and it will show the difference between the two operating systems.

3.2.1 IOS Security Model

Just by researching “IOS security model” there is much writing on this topic including Apple themselves, most of my information will be from Apple and will be highly accurate. Let’s start off with the security architecture diagram also known as a framework, this shows how the hardware and software communicate with each other, Image below.

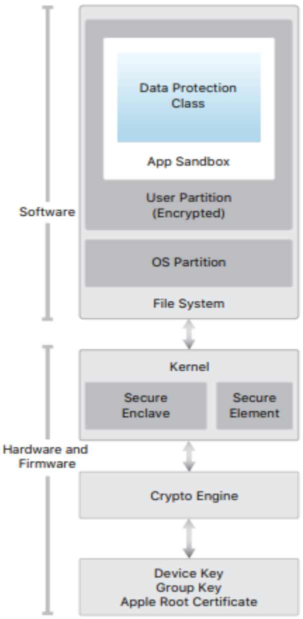


Figure 3. Security Architecture

The system security of the IOS is designed so both the hardware and software are secure across all components of the IOS device and not just mobile devices. Apple has over 11 security procedures each with multiple procedures inside to keep features safe. Which are the System Security, Encryption and Data Protection, App Security, Network Security, Apple Pay, Internet Services, User Management, Device Controls, Privacy Controls, Security Certifications and Programs and finally Apple security bounty which helps white hat hackers discover flaws in the code and Apple will pay the white hat hacker money for finding these security holes, which end up developing the software and hardware much more secure, Apple (2018) provided information for the visit.

Because of the way Apple has built is OS from the ground up it is extremely hard to hack the software and hardware directly, which is why hackers aim for the user and not the device.

3.2.1.1 Small Solution

This is exceedingly hard to achieve a solution for this as the solutions are always being implemented into the new security update from the manufacturer. Therefore, the most invaluable advice just keeps the devices secure with a password, touch ID and keep checking for updates for the devices and Applications which are downloaded.

3.2.2 Android Security Model

Again, just by researching “Android security model” there is a lot of writing on this topic including Android. Most of the information used will be from Android making the information very accurate. The image below will show the reader the Android software stack which represents the framework, image below.

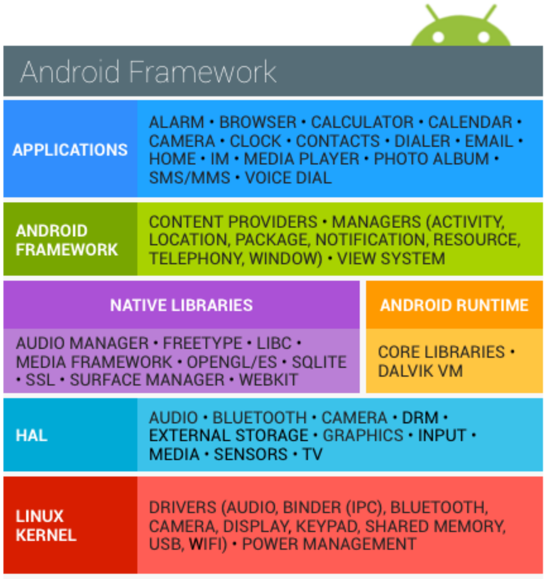

Android Framework
APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL
ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM
NATIVE LIBRARIES
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT
ANDROID RUNTIME
CORE LIBRARIES • DALVIK VM
HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV
LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Figure 4. Android Software Stack

The image shows where all the features of the device are located and will allow the user to understand how it works. Android which was created by Google has several security procedures as well for stock Android which is different in every phone, for example, the Pixel has different security procedures than Samsung, even though they both running on Android. So, some vendor may vary. Stock Android has over 12 security services and security overviews which is the very basic information about them. They include Google Pay, Android Updates, Application services, Verify Apps, Safety Net, Safety Net Attestation, Android Device Management, Design review, penetration testing and code review, open source and community review, incident response and monthly security updates.

3.2.2.1 Small solution

Do the same as section 3.2.1.1, keep devices updated.

3.3 Security Threats for IOS and Android App Stores

In this section, there will be three sub-sections about the legitimate app stores from Android and ISO since they maintain the most sizeable percentage as the market.

3.3.1 IOS Apple App Store

From the start of the App store from Apple, they were known as a brick wall, because of its closed developer ecosystem and very stringent security. This has been reasonably successful in preventing any kind of malicious IOS apps from sneaking their way past security measures and getting onto the app store and user phones. But in recent times from 2015, there was a massive weakness in Apple's current security model, this happened in China and Apples did confirm that 39 malware-infected Applications have been discovered and deleted from the China App store, the hackers where stealing sensitive user and device information. Because of this news, independent researchers promptly discovered the number of infected apps where upwards to 344 apps then went to 4,000 apps and these apps were downloaded by hundreds of millions of devices, Drapeau (2016) provided information for this visit.

The way the hackers were able to get this done was to get legitimate developers in China to download an illicit copy of Apples XCode development toolkit from a local server instead of using Apple official servers. Because of this application were submitted to the China App Store under the developers own trusted credential all the apps were assumed to be safe without checking the code. Drapeau (2016) provided information from this visit.

3.3.1.1 Small Solution

Because of Apple's new security model, it is practically impossible to get malicious apps through the code checking in 2018. But if you want to be extra safe check the rating of the app, the comments to see if people think it is questionable and do a Google search to see if others have issues with the app you might download onto the device.

3.3.2 Android Play Store

Android has not been known for the most adequate security compared to Apple, but the security has been getting betting, through the years. But very recently there has been a large security threat in the Google Play store where 145 Android Apps where removed, this happened after researchers discovered they were infected by malicious Windows-executable files, Wong (2018) provided information from this visit. The apps discovered where published between October and November of 2017. Even a couple of the apps had over 1,000 installations and high ratings. The researchers expected that the Android apps were most likely infected with the Windows malware because the developers developed the applications on a compromised Windows machine.

3.3.2.1 Small Solution

Even though Google deleted the infected apps from the Play Store and many people have already downloaded them, the best thing to do is keep mobile devices safe from these types of apps is to patch the operating systems with the latest fixes and download and keep the anti-virus up to date and scan the devices every other day and or scan apps when downloading.

3.4 Online APK files

Unlike Apple Android will let any device to download anything from the internet, most of the apps people download are unauthorised apps from the Android play store, But by doing this is can harm your device and steal sensitive data, people that use these types of APK files will know what they are doing, by turning off the device security setting to allow unauthorised apps to be installed, they know there is a chance the file they are downloading from internet sites can damage the device and the data, most people who do this will scan the file to check if there is unhidden malicious virus or code waiting to get on the device. But why do people download these apps, mostly because they have illegal content, for example, Kodi and an illegal site where people can watch, stream and download movies, sports, tv shows, and live channels, all of this for free of one download. Even though it is illegal to use these kind sites, many people take advantage of these settings on Android devices and can cause harm.

3.4.1 Small Solution

If you plan of downloading APK files from the internet, make sure you have scanned the files and done some online research to see if other people have had problems with the APK, if they have, don't download, and make sure you have the option turned off, so automatic downloads don't happen when browsing on other internet sites.

3.5 Root Access

Rooting for Android and Jailbreaking for IOS is the same concept but done in alternative ways. It allows the user to access and modify system code allowing the phone to do what the user wants from changing designs, making it run faster, allows to install any app good and bad ones like hacking commands, can access the lasts OS updates without waiting for the update to appear, ditching the factor skins of the device and a lot more features.

3.5.1 Android Rooting

While rooting an Android device is popular amongst some advanced Android users, there is an extremely significant risk, mainly in corporate settings and the device will lose its warranty and if the device bricks itself the user can't get it fixed from the manufacturer. When using a rooting device, it can introduce malware onto the device during the process. These types of malware will place the data of the device at risk, which includes gaining access to personal information like contacts, emails, credentials, passwords and other data. Hawarth (2015) provided information for this visit.

3.5.1.1 Small Solution

If you have already rooted the device and you don't know how anything works, factory reset the device and will go back to factory settings to be the safest, but if you want to keep the extra features and freedom make sure all files installed are scanned for malware.

3.5.2 IOS Jail Breaking

IOS Jailbreaking is the same as Rooting for the android devices just done in different ways, the same reasons are used it's my phone, I want these apps, don't like the look of the layout, etc. It lets the user control the device by modifying the system code.

3.5.2.1 Small Solutions

The solutions are the same as the Android rooting solutions in section 3.5.1.1. Just make sure you scan all files and know what you are doing. But if you don't know what to do try buying an Android device with gives the user more freedom compared to the Apple devices.

3.6 Security threats and attacks from pre-installed app

This section will talk about the security threats which can be found when using a pre-installed app from the manufacturer or App stores, it will include the main Applications people using like Facebook, Twitter, Email, text messages, and Internet browsers. The solutions for these will be at the end of the sub-section.

3.6.1 Facebook

Facebook is the biggest social network site and will be targeted because of that they are mostly scams instead of malware, but both can be found for example on 25 September 2018, Facebook was hacked and 50 Million Accounts where compromised and had their personal data stolen including names, contact information, gender, relationship status, and location check-ins, O'Connell (2018) provide information for this visit. There are several scams that are active in 2018 from "see who's viewed your profile" scam which steals data when clicked, the "see who's blocked you" scam which also steals your data. They are lots and lots of the scams on Facebook, but most of them are easy to spot if you know about them and most people don't, and their ego causes them to want to click on the click bait titles and links.

3.6.2 Twitter

Twitter also has a big issue with scammers, and they use private messages to get people to click a link which says "is it you in this picture" etc. just titles which you would want to click on. Most of the social media networking sites all have similar types of scams.

3.6.3 Email

Everyone knows about the email scams, which mostly go straight into our spam folder, but some get through like you won this click to claim your prize, and the classic email is the African royal prince scam trying to collect money from uninformed people on these issues. One in 10 scams were through emails, and 4 million people scammed each year in 2014 in the UK, citizens advice (2014) Provided information for this visit.

3.6.4 Text messages

Text Messages have scams in as well, since most people mobile numbers can be found online or have been sold to advertisers and companies which have been hacked and mobile numbers sold on the dark web, most people will have had a scam through the text messaging app which is pre-installed on devices form service providers and manufacturers. Most SMS scams are pretending to be the user’s bank or Credit Card Company asking for login details, password and security passwords. Don’t reply to these texts as the will likely to try again and don’t click on any link provide and block the number.

3.6.5 Internet (Chrome, Firefox, etc)

The internet is the easiest to get hacked, malware and scams from, as it depends on what sites you site, maybe from a Facebook, Twitter or email link which can help the hackers gather data from the victims. Make sure to scan the mobile device if any of these things happen as it might catch the malware early and do no damage.

3.6.6 Small solution

All the sub-sections above can be stopped by keep on checking the most recent scams, which are in season from the scammers or hackers as they move to different types once they have been found out. Keep the device updated and scan device every couple of days, make sure to block the people when this happens so you might not get tricked from the same person.

3.7 Security threats from pre-installed software

This section will be talking about the pre-installed software also known as the devices features, the main security threats which come from Bluetooth and Wi-Fi. There is a lot of pre-installed features from all mobile devices, but I believe that Bluetooth and Wi-Fi are the most important to keep your devices safe and secure.

3.7.1 Bluetooth

When Bluetooth was released over 10 years ago, there were many security threats compared to 2018, Bluetooth is used to connect a mobile device to a large array of devices like audio equipment, navigation, and other electronics through the internet of things (IoT). There are a lot of different threats to current devices, for example, eavesdropping where a hacker connects to the Bluetooth signal. Denial of Service is where the malicious attacker can crash the mobile device by blocking calls and can drain the device's battery.

3.7.1.1 Small solution

The best way to prevent hackers from gaining access to the data of the device is to turn off Bluetooth when not using it and make sure all device has the current Bluetooth updates.

3.7.2 Wi-Fi

Mobile device security is always on the rise every year. Kaspersky Lab discovered that almost 3.5 million pieces of malware were on more than 1 million user’s devices. There are a lot of threats to devices through the Wi-Fi the device is connected to, for example, data leakage which uses malware. Another threat is using an unsecured Wi-Fi signal when in public, by exploiting the open signal you could be joining a hacker’s hotspot and they can be sniffing packets and try to brute force their way into the mobile device. They can also use network spoofing where the hacker sets up a fake access point which makes it look real and the device joins the signal which can harm the device as the hacker can have easy access to the data. Another one will be phishing attack by sending the victim fake links which look real and the device will be infected with malware, other ways can be spyware and broken cryptography. Kaspersky Lab (N/A) provided information for this visit.

3.7.2.1 Small solution

The best way to protect from these threats is to use 4G when in public and only access public Wi-Fi like Starbucks when the user plans on not doing anything significant like banking.

3.8 Malicious Software

Since most of this paper has already been talking a malicious software, malware, scams, and viruses. I guess most people already know about them which are developed, coded and bought by black hat hackers to attack, damage and steal data, which can get them some money and don't plan on getting caught when doing so. Malicious software can include, Trojan horse, worm, botnets, rootkit and many more, which all can be bought of the dark web.

3.8.1 Small Solution

Keep the device up to date, keep using anti-virus and scan full device regularly and scan all apps, files mainly anything which needs to be downloaded or viewed.

3.9 Solution

We have gone through all of the research for this section and all sub-sections have small solutions, so the reader can go to what they want, this section though will be a black sheet for all of these combined, Let's start of keeps your mobile device up to date, keep all apps up to date, scan the device frequently, turn off feature and setting when not in use, research current scams for social media and use common sense. All of these will keep your device a lot more secure than not doing them, but as my lecturer said the best security for a device is to have it turned off and inside a concrete block. Meaning your device will never be 100% secure no matter how hard the user tries.

4 Conclusion

In conclusion, we have discovered there is a large number of ways for hackers to penetrate security systems for both Android and IOS devices, and ways for the user to help and prevent these attacks from happing to their devices. Through the years of development of this hardware and software, the security keeps on getting better and better, and so does the hackers have new ways to take advantage of these facts. Because the users that don't know much about security or the threats to their data, they believe the devices are already secure and don't need to take constant action to keep the device secure through first and third-party updates and apps. Though this report we have found out that most if not all attacks can be minimised if the user knows how to do these steps from researching the current hacks, scams, data breaches and to making sure applications are updated when needed.

5 Reflection

This section will talk about the reflection of the report, and it will discuss the technological development in the next 5 years, what went well and what did not go well, how might I go about doing it differently in the future, what have I learned from the experience, how the knowledge and experience might be applied in the future, Does what I found answer the question of what was intended to research then finally what needs more work. All section will be quick and straight to the point.

5.1 Technological developments next 5 years

In the next 5 years, I expect the technology to be so far ahead of where we are now, that will need an updated security software to be compatible with these future devices.

5.2 What went well/what did not

The structure of the report and headings helped with research a lot and very easy to find figures about the topics. The main things which did not go well is the finding of academic research papers for these types of topics, and the information is outdated even if it a couple years out.

5.3 How might I go about doing it differently in the future

If picking the same topic make sure to find more papers, articles, etc. To help with the analysis but stick word count for each section as I have run over. Also, make sure to do the report over a long period of time and not to cram it in within a few weeks.

5.4 What has been learned from the experience

It is harder to find relevant academics papers than I have previously thought, and time management has been very important, which I wished I have used when writing this report.

5.5 How this knowledge / experience might be applied in the future

The experience of writing this research report has shown me the ways of researching, analysis and writing a good report. When my future master's research paper has started, it will help me throughout the process and improve my skills in the report writing.

5.6 Does what I find answer the question of what was intended to research

Yes, it shows current and past threats to mobile security through applications.

5.7 What needs work

More researching, data gathering and analyses of the data this report is not the best I could have done if I started sooner and spent more time of the paper.

6 References

- Android (N/A) *Security.* Available at: https://source.android.com/security (Accessed: 18 December 2018).
- Apple (2018) *iOS Security.* Available at: https://www.apple.com/business/resources/docs/iOS_Security_Overview.pdf (Accessed: 18 December 2018).
- Citizen advice (2014) *Four Million people scammed each year.* Available at: https://www.citizensadvice.org.uk/about-us/how-citizens-advice-works/media/press-releases/four-million-people-scammed-each-year/ (Accessed: 18 December 2018).
- Drapeau, P. (2016) *The Apple App Store Incident: Trouble in Paradise*. Available at: https://www.darkreading.com/application-security/the-apple-app-store-incident-trouble-in-paradise-/a/d-id/1324016 (Accessed: 18 December 2018).
- He, D., Chan, S., Guizani, M. (2015). Mobile Application Security: Malware Threats and Defenses. *IEEE Wireless Communications*, 133, 138-144.
- Howarth, F. (2015) *Is Rooting Your Phone Safe? The Security Risks of Rooting Devices*. Available at: https://insights.samsung.com/2015/10/12/is-rooting-your-phone-safe-the-security-risks-of-rooting-devices/ (Accessed: 18 December 2018).
- J. gold associates (2017) *Android in the Business Environment: Is It Safe?. Available at:* http://jgoldassociates.com/White_Papers/Android_in_the_Business_Environment_Whitepaper.pdf (Accessed: 18 December 2018).
- Kaspersky (N/A) *Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future has in Store.* Available at: https://www.kaspersky.co.uk/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (Accessed: 25 October 2018).
- Kaspersky lab (N/A) *Top 7 mobile security threats: smart phones, tablets, & mobile internet devices – what the future has in store.* Available at: https://www.kaspersky.co.uk/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (Accessed: 18 December 2018).
- Mahmood, S., Amen, B., Nabi, R.M. (2016). Mobile Application Security Platforms Survey. *International Journal of Computer Applications,* 133, 40-46.
- Medium. (2018) *Android vs iOS: Which Platform is More Secure in 2018*. Available at: https://medium.com/@AppInventiv/android-vs-ios-which-platform-is-more-secure-in-2018-33b3108270d (Accessed: 18 December 2018).
- Neighbourhood watch. (2015) *Scams & Older People.* Available at: https://www.ourwatch.org.uk/crimes-archive/scams-older-people/ (Accessed: 18 December 2018).
- O'Connell, B. (2018) *Top 7 Facebook Scams to Watch Out for in 2018*. Available at: https://www.thestreet.com/technology/cybersecurity/facebook-scams-14746513 (Accessed: 18 December 2018).
- Pike, J. (2017) *10 Threats to Mobile Security*. Available at: https://metova.com/10-threats-to-mobile-security/ (Accessed: 18 December 2018).
- SearchSecurity (N/A) *How best to find and fend off malicious mobile apps.* Available at: https://searchsecurity.techtarget.com/securityschool/How-best-to-find-and-fend-off-malicious-mobile-apps (Accessed: 25 October 2018).
- Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., Glezer, C. (2010). Google Android: A Comprehensive Security Assessment. *IEEE Security & Privacy,* 8, 2.
- Sirvastava, S. (2017) *Benefits of iOS vs. Android App Development*. Available at: https://appinventiv.com/blog/ios-vs-android-app-development-a-2018-lookout (Accessed: 18 December 2018).
- StatCounter Global Stata. (2018) *Mobile Operating System Market Share Worldwide*. Available at: http://gs.statcounter.com/os-market-share/mobile/worldwide# (Accessed: 18 December 2018).
- StatCounter Global Stata. (2018) *Mobile Vendor Market Share Worldwide.* Available at: http://gs.statcounter.com/vendor-market-share/mobile (Accessed: 18 December 2018).

- Statista. (2018) *Number of mobile phone users worldwide from 2015 to 2020 (in billions) Available at:* https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ (Accessed: 18 December 2018).
- Symantec. (2017) *Internet Security Threat Report (ISTR) 2018.* Available at: https://www.symantec.com/security-center/threat-report (Accessed: 18 Dec. 2018).
- Webroot Smarter Cybersecurity (N/A) *A review of Bluetooth attacks and how to secure your mobile device.* Available at: https://www.webroot.com/hk/en/resources/tips-articles/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices (Accessed: 18 December 2018).
- Wu, L., Du, X., Fu, X. (2014). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications Magazine,* 52, 3.
- Wylie, W. (2018) *Mobile App Security Threat Forces Google Play Store to Remove 145 Android Apps*. Available at: https://securityintelligence.com/news/mobile-app-security-threat-forces-google-play-store-to-remove-145-android-apps/ (Accessed: 18 December 2018).

7 Proposal form as an appendix

Mobile & Wireless Technologies

Report Proposal

Name: Thomas Ruddock

Working Title: The Threats and defences for Mobile Applications (Apps).

Report Outline

Introduction

This report will identify the current threats to smartphones and how to defend from it. It will show what hackers are using to get onto victim's smartphone devices and gather sensitive information and how the companies and users can minimise or even prevent these from happing to their devices.

Background on the topic

The reason for doing this report is the recent exposure from play store apps illegally using permissions to gather phone numbers, user's locations and receive SMS messages. Because of these apps sneaking through the play store and breaching the security policies, the users can't trust the app stores and will need to carry out procedures to secure their smartphone and information from these hackers.

Sub sections about the paper (bullet points)

- Abstract
- Introduction
- Why smartphones are targeted
- Security threats to mobiles through applications
    - Attacks (phishing, gps tagging, camera hacking, etc)
- How to defend against these attacks
- Conclusion
- References

References:

- He, D., Chan, S., Guizani, M. (2015) 'Mobile Application Security: Malware Threats and Defenses', IEEE Wireless Communications, pp. 138-144.
- SearchSecurity (N/A) *How best to find and fend off malicious mobile apps.* Available at: https://searchsecurity.techtarget.com/securityschool/How-best-to-find-and-fend-off-malicious-mobile-apps (Accessed: 25 October 2018).
- Kaspersky (N/A) *Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future has in Store.* Available at: https://www.kaspersky.co.uk/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (Accessed: 25 October 2018).