EPiC Series in Computing

Volume 82, 2022, Pages 92–101

Proceedings of 37th International Conference on Computers and Their Applications

Mobile Devices Vulnerabilities

Melissa M Schneider [1], MD Minhaz Chowdhury[1] and Shadman Latif[2]
[1] East Stroudsburg University, East Stroudsburg, PA, USA
[2] American International University, Dhaka, Bangladesh
mschneide8@live.esu.edu, mchowdhur1@esu.edu, Sadmanxp@gmail.com

Abstract

With the increase in popularity of mobile devices for personal and business reasons, they have become even more attractive targets to malicious actors. There are many vulnerabilities with any mobile device, though some environments, features, and operating systems are at higher risk than others for certain attacks. This paper discusses such vulnerabilities, including the elements that allow them, methods of exploiting them, and one might combat attacks on mobile devices.

1 Introduction

Over the years, cell phones and other mobile de-vices have increased in popularity. Not only do most people own and use mobile devices, but increasingly they are replacing traditional internet use on a desktop or laptop environment. Because of this, threats against traditional computers have been adapted to target mobile devices. In a world where users regularly manage their emails, financial accounts, and other crucial aspects of their lives on their phones and tablets, mobile security is as essential as desktop security. However, mobile security is often overlooked by users, leaving their devices vulnerable in situations that awareness of common threats could potentially prevent.

There can be measures placed to counteract threats without relying on the users' knowledge. Such security measures can be implemented on many different levels. For example, when developing any product, the developer or security engineer considers how to make their product "user proof", thus preventing unwanted behavior from being possible. In the case of mobile security, this task is made increasingly difficult with the rampant popularity of apps requiring potentially unreasonable permissions and utilizing device re-sources in a way that interferes with the privacy and usability of the device. Additionally, preventing users from being fooled by trojanized and phishing apps is generally outside of developer control, especially due to such apps being available on markets like the Google Play Store for Android. Because of these challenges along with the rising popularity of mobile threats, mobile security awareness and solutions are crucial today.

The remainder of this paper is organized as follows: Section 2 discusses varying mobile security threats, including mobile malware, software vulnerabilities, data leakage in corporate setting, vulnerabilities of mobile apps. Section 3 presents the conditions that contribute to such vulnerabilities.

Section 4 presents few state-of-the-art methodologies and protocols to minimize these vulnerabilities. In Section 5, the paper concludes with a re-statement of the importance of mobile security.

2 List of Mobile Device Vulnerabilities

In this section, groups of mobile device vulnerabilities are described. The first group is the group of software that exploits mobile software, called malwares (Types of mobile malware). The second group is the type of vulnerabilities that are not from maliciously intended software. Third is the vulnerabilities common in corporate settings (data leakage). The fourth group is not a software intended to exploit the mobile devices but the vulnerabilities of the installed software itself.

2.1 Types of mobile malware

While the following is not an exhaustive list, it gives some examples of mobile malware and its effects.

Madware: The word Madware is a combination of the word's malware and adware. When applications contain advertisements, the software is often tracking information about the user based on data gathered from their usage of the app, and potentially other applications on the device due to per-missions or malicious elements. As such, madware can be considered a form of spyware since it collects personal information which it may sell to third-party data collectors for further targeting.

Cryptomining: Cryptomining refers to installing malware onto a device with the intent for it to function as blockchain entries to cryptocurrencies. This type of mobile malware serves to benefit the attacker while the device it is installed on, has its resources depleted. Cryptomining can cause quickly depleting battery life, slow processing speed, and over-load of the device causing it to crash unexpectedly. Because Cryptomining malware can be hidden within apps, a user may suspect the problem is a non-malicious result of a software or hardware defect, allowing their device to remain infected.

Trojans: Trojans, as the name suggests, are things that masquerade as something desirable, while under the surface waits for malicious actors ready to wreak havoc. In this case, the malicious actors are the attackers and their software that intends to infect devices. Trojans can be disguised as an app but are particularly dangerous when they mimic the apps of financial institutions. When a user attempts to log in into a trojanized app, the attackers gain valid credentials to the targeted institutions. In addition to the funds in the targeted institution being vulnerable, the user's identity as well as any other of the user's accounts across the web using similar, or likely the same, password and username are vulnerable in this scenario.

Ransomware: Ransomware is malware characterized by the at-tacker encrypting the user's data and requiring to be paid a lump sum, often in cryptocurrency, to release the data. While this type of attack is more frequent on desktop systems, ransomware has been known to affect mobile devices as well.

Ghost Push: Ghost Push is a family of malware targeting An-droid devices that gains supreme privileges over a device, and allows the software to download un-wanted apps, allow ads, and effectively take over. This malware drains the battery and can be used to spy on the user. While this virus has not been in the news since 2017, at the height of its reign it was infecting "over 600,000 Android devices daily" and was discovered in 2015 (*'Ghost Push' Malware Threatens Android Users*, n.d.). It can be surmised that the Android OS has a long period to patch the vulnerabilities exploited by the malware. However, a user is choosing not to update their devices may have prevented them from being protected even after the vulnerability was patched, thus leaving themselves and others without the update exposed. This contributed to the extension of the malwares' viability.

Keyloggers: Keyloggers are normally thought to be found on desktop computers rather than mobile devices, like some of the other threats listed. However, keyloggers can similarly affect mobile devices, by "logging", or saving, information typed in by the user in hopes of collecting the login credentials, bank account information, and credit card numbers. This type of attack is hard to detect because it is not software that the user interacts with directly but instead runs in the background.

Bots: On a mobile device, a bot is "malware that runs automatically once installed on a mobile device" (*Mobile Botnets Taking over Smartphones – BullGuard*, n.d.). Without antivirus to block them, bots can take over a device completely and give control to malicious commands received remotely. According to BullGuard, mobile bots were first discovered in 2001, and any operating system can be targeted. With many infected devices in a botnet, at-tackers can collect a lot of data and potentially "launch an attack over an entire network". Bots are yet another type of malware that can be transmitted through emails, trojanized apps, and embedded into websites.

2.2 Mobile Device Attacks

There are mobile device vulnerabilities that can be exploited without using any malware. These vulnerabilities include but not limited to the vulnerabilities resulting from social engineering attack (example: phishing attack), man-in-the-middle attack and the vulnerabilities of the host computer software (example: browser vulnerabilities and operating system vulnerabilities).

In the Social engineering attack, the goal of the attacker is to gain access to a given system. Though this is thought to be a technical task, often an attacker will instead use social engineering to trick or deceive an authorized user, resulting in the interception of valid credentials. Phishing, a social Engineering attack, is the practice of sending fraudulent emails appearing to be from a trusted source with the intent to collect personal information. For example, a user may receive an email that appears to be from Netflix asking them to verify payment information so that their account will remain active. While briefly, it may seem to be legitimate, after further inspection one may notice spelling and grammar errors in the text, slight differences in the logo, or a misspelled, misleading email address as the sender; for example, "nettflix" or "netflics" may appear in the address of a phishing email.

Mobile devices are susceptible to phishing emails. For instance, the size of the screen and the typical format of mobile browsers can be taken advantage of by URL padding. To phish using URL padding, malicious actors start their fake-login screen's URL with a legitimate one – PhishLabs uses the example of m.facebook.com in Figure 1, the address for Facebook's legitimate mobile site and follows it with hyphens or various miscellaneous characters before finally listing the true domain

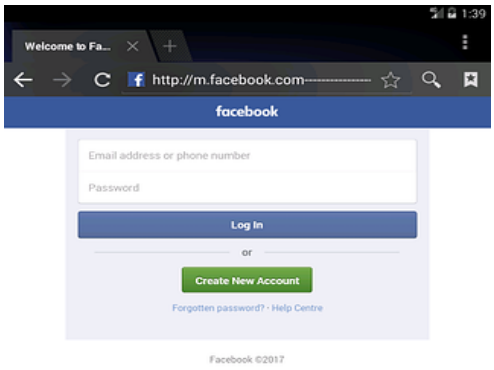

Figure 1: PhishLabs using m.facebook.com

(Hassold, 2017). Since mobile browsers can only show a limited amount of the URL at once, users may not notice the discrepancy until it is too late, if ever. Phishing attacks can also be carried out

through texting. This subset of phishing is sometimes referred to as smishing, a combination of SMS and phishing (Smishing attack). The consequences of a phishing attack can affect many aspects of an individual's life or an organization's business.

In the man in the middle attack, a third-party intercept and possibly alters communications between two parties who believe they are communicating with each other without their knowledge are referred to as "man-in-the-middle attacks". One example of a mobile man-in-the-middle attack involves public Wi-Fi access points. An attacker may install the compromising access point in a public place where individuals spend a lot of time, like an airport or coffee shop (Hassold, 2017). In other instances, an attacker may install an access point that impersonates a legitimate one in a public space, but outside the range of the authentic point's range. Both methods rely on a culture of constant smartphone use and desire to connect to Wi-Fi. Man-in-the-middle mobile attacks are hard to spot from a user perspective since free public Wi-Fi is common, and even if the user knows the SSID for an authentic source, the second approach will prevent them from noticing that there could be a fraudulent access point.

2.3 Corporate Mobile Device Vulnerability: Data Leakage

The context of mobile security in respect to companies is slightly different than discussed in the rest of this paper. The concern arises with the popularity of BYOD, Bring Your Own Device programs, which pose many security risks. One concern is that personal devices used for company functions require capabilities for remote wipes in the event of a lost device or employment termination. Another is fraternizing between personal and work-related data on the device. Although many apps can be granted permission to access the de-vice's content, this is not always appropriate when company information is stored. Because of the concern of this data leakage, many enterprise solutions create containers, or sandbox, environments that effectively separate business from personal functions to prevent the inappropriate breach of company information.

2.4 Mobile App and Software Vulnerabilities

In this section, vulnerabilities relating to the nature of apps and software are discussed as follows:

Trojanized Apps: The concerned issues of mobile security are malware "distributed as trojanized apps", un-secure storage and data leakage, security of communications, device updates, secure coding practices, and more (Seacord, 2015). Apps acting as malware can be downloaded right from an app store, or in the case of Android products, from a third party using a browser. Further, even apps from trusted sources can store data in a way that creates vulnerabilities to the user. Another concern is permissions granted to each app. In many cases, authentic apps, as well as "trojanized" ones, ask for per-missions that put the confidentiality and accessibility of devices at risk.

Permissions Abuse: There are ap-plications who record phone numbers, IMSI codes, ICC-ID numbers, and location information to their server (Enck et al., 2019). In the case of location information, the contributors found that the apps were reporting this information to advertising servers without informing the users.

Researchers at UC Berkley found that many application permissions can be dangerous. In their study, they found that 93% of free apps and even 82% of paid apps have at least one permission they deem dangerous (A. Felt et al., 2011). Additionally, they state that a request to connect to the internet is one of these because it creates the possibility for these apps to leak user data. This study found that "97% of the 225 applications that ask for ACCESS_FINE_LOCATION also request INTER-NET permission," and that "94% and 78% of the respective applications that request READ_CONTACTS and READ_CALENDAR also request the INTERNET permission". This study also characterizes permissions to write to storage, access location, read phone state, wake lock, write settings, and get

tasks as potentially dangerous, and showed that the number of re-quests from free and paid apps was comparable in many cases.

Figure 2, taken from (A. Felt et al., 2011), shows some of this study's data on applications requesting dangerous permissions. This study found that applications acting as malware request more dangerous permissions than non-malicious ones, an average of 6.18 com-pared to 3.46, almost double.

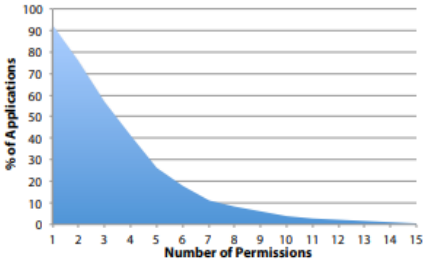

Figure 2: Applications requesting dangerous permissions.

However, since many apps do request many permissions, this begs the question of which ones may indicate a malicious application. Another group of researchers analyzed the data reported in the study, to look for similar characteristics among the 11 applications that were found to contain malware (A. P. Felt et al., 2011). It was found that 73% of malicious apps compared to only 4% of non-malicious apps request SMS messaging permissions. Further, 73% also re-quested to read the phone's state, giving IMEI access compared to 33% of non-malicious applications in the data set. To combat these threats, Security and Privacy-aware mobile App Recommendation software can be implemented, as purposed (Zhu et al., 2014). An example of the framework is shown in Figure 3, taken from (Zhu et

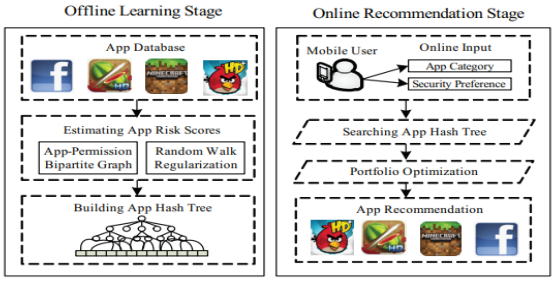

Figure 3: A security framework example

al., 2014). This framework could be useful to aid users in making informed decisions about installing any software onto their devices. Just by adding such a feature, the idea that security should be considered would be introduced and lead users to be-come more curious about what permissions they have given to certain apps, and how they are used.

Browser Exploits: Browser Exploits take advantage of vulnerabilities in operating systems or other software to breach browser-related security.

Client-Side Vulnerabilities: Client-side vulnerabilities are vulnerabilities residing in the software provided by legitimate sources. 60% of vulnerabilities are on the client-side (Technologies, 2019). In some cases, insecure inter-process communication can lead to third-party interception of messages on Android devices. However, security errors are not limited to Android. According to Positive Technologies, "errors in security mechanisms were the cause of 74 percent of vulnerabilities in iOS applications and 57 percent of vulnerabilities in Android applications". In 2018, it was found that developers for iOS did not restrict custom keyboard use, which can potentially prevent Apple from stopping the software from logging and transmitting keystrokes if network access is allowed by the user.

3 Conditions Contributing to Mobile Vulnerability

In this section, conditions that contribute to mobile vulnerabilities are discussed within the context of the threats that may take advantage of them.

3.1 Attacking known vulnerabilities

As mobile devices have become more popular, the monetary value of the information stored on them has grown. For hackers and security professionals, this value is a motivating factor to find vulnerabilities, whether they be hardware, operating system, or specific software-based. When found by security professionals, these vulnerabilities are patched and publicized. On the other hand, hackers may exploit the vulnerability, and potentially share the information with other malicious actors, or keep it secret. Regardless, the longer a system exists, the more vulnerabilities will be discovered, giving at-tackers more ammo as time goes on. Even when known vulnerabilities are patched, users are not protected unless they update their devices as soon as the patch is available. Since many users neglect to understand the crucial reasons behind such updates, they may hold off and leave themselves vulnerable unknowingly.

3.2 Permissions Abuse

Permissions abuse is categorized by software re-questing permissions not essential to the functionality of the program or application, specifically with intentions to use device resources and collect information about the user. For instance, over the years there has been controversy about the permissions required by apps like Facebook and Messenger, including the ability to change the state of network connectivity, send outgoing calls, read text messages, read call logs, contact data, and more. Although these permissions are indicative of features on the app, it is also possible that they can be abused without the knowledge of the user in a worst-case scenario. While one may deduce legitimate reasons for such data collection, it seems increasingly unnecessary as the list goes on, and some such apps have been found to save this in-formation in persistent records. While apps like this at least inform the user of the range of permissions, others access devices without giving such notice. One study on real-time security monitoring on smartphones found that countless apps access location, device ID, network status, and more without ever informing the user (Enck et al., 2019). Without the user having a way to detect this, their security is breached, and malicious attackers can exploit their devices.

4 Consequences of Mobile Security Flaws

According to Positive Technologies, in 2019 vulnerabilities causing high risk were found in 38% of IOS applications and 43% of Android applications, with 89% of vulnerabilities being able to be exploited remotely via malware (Technologies, 2019). Vulnerabilities in legitimate apps are one concern since the user may feel comfortable giving feature-related per-missions to the authentic source. However, vulnerabilities open doors for malicious actors to attempt to gain access to the device as well.

In McAfee's 2019 Q1 report, detection of trojan apps in the FakeApp malware family grew every month in 2018, ending the year between 60,000 and 70,000 detections in December alone (Samani & Davis, 2019). Malware like this may send text messages without user consent, download hidden malicious apps, and display ads that disrupt the use of the device, and are often spread by preying on the popularity of the app it is mimicking. McAfee also reported a rise in trojan apps disguised as legitimate banking applications. This can be attributed to attackers subverting Google's security

methods to prevent malware. Even though upon the installation of the application is found to run accordingly, the trojan downloads the malicious software afterward to bypass security measures.

Kaspersky's 2018 report showed a doubling of mobile malware attacks compared to the previous year, although they showed a drop in malware files itself, presuming that mobile malware is becoming more directed and difficult to detect (Kaspersky Lab, 2019). The company also found an increase in Cryptomining attacks to five times the amount and detected 1.6 times the amount of trojan banking apps compared to 2017 as well. The report names RiskTool (malware that conceals files and modifies processes), various forms of Trojans such as Droppers (used to bypass security), SMS, and Banker, and Adware among the highest distribution of new mobile threats, accounting for more than 90% (Chebyshev, 2019).

5 State-of-the-Art Measures Against Mobile Device Vulnerabilities

The Lightweight Data Sharing Scheme (LDSS) algorithm, proposed in (Li et al., 2018), can solve the security issues of data sharing problems using mobile cloud. The algorithm ensures privacy preservation.

The communication between two mobile devices can be made secure, even though one de-vice gets compromised by an attacker, by using privacy-preserving mutual authentication protocol for mobile internet environment (Wu et al., 2018). The security is ensured by using two-key generation, Paillier homomorphic encryption and zero-knowledge proofs. The protocol follows three steps. In the first step, a server containing all IDs (identity label) generates all system parameters. In the second step, user registers with the server using two de-vices (a master device and a secondary device) by sending the identity level of the user to the server (S generates two key shares and a key pair for security). In the last step, known as mutual authentication step, the user communicates with the server using his/her devices two devices.

Touch dynamics biometrics can also be used for a secured authentication process on a mobile device. From the raw data of bio-metric information, feature extraction process selects the necessary features (two types of features extracted: basic features and extended features) and stores the formatted data. Authentication model is built by classifying these features, using classifiers. One-class classifier overperforms two-class classifier. It is showed in (Teh et al., 2020) that using their proposed authentication method as an additional authentication factor, certain unauthorized access can be hardened and thus the security of the concerned mobile device can be established.

An alternative biometric based method, continuous face-based authentication method can be used to harden unauthorized access to mobile devices (Samangouei et al., 2015). Facial attributes can be classified and can be used as feature vectors for the identification process.

Traditional host-based IDS (intrusion detection system), example snort, fails to identify certain malwares. A new approach named net-work-based mobile malware monitor (N3M), that uses random forest machine learning algorithm, can be used to differentiate between malware and benign/authorized software (Watkins et al., 2018).

There are interdisciplinary concepts that can be applied compensating or minimizing mobile device vulnerabilities. For example, feature selection method used for reducing feature dimensions of cyber security dataset (Ahsan et al., 2021) can be used to select mal features of emails (against social engineering attack). Computational trust can be used trust the activity of another connecting device (M. M. Chowdhury et al., 2018) (M. M. Chowdhury & Nygard, 2017) (Krishna Kambhampaty, Maryam Alruwaythi, Md Minhaz Chowdhury, 2019) (M. Chowdhury & Nygard, 2018) (Md Minhaz Chowdhury, 2017).

6 Conclusion

In this paper, different types of mobile vulnerabilities are identified and explained in de-tail and elaborated with specific examples. Such information is beneficial in educating mobile users to improve their awareness of using these devices and their apps (applications installed in the mobile devices) to handle these vulnerabilities. Mobile security is an ever-evolving, crucial aspect of information security. With the sheer volume of smartphones, tablets, and other IoT devices only increasing, one can assume the number of attacks targeting them will only continue to increase as well. There are various types of malware, each with varying popularity and relevance today. While some become less viable as time goes on, older systems can still be at risk, especially as vulnerabilities are exposed. Additionally, mobile malware is becoming more difficult to detect by users, leaving unprotected devices at high risk. Many attacks plaguing mobile devices today rely on tricking users to download their malicious software, connect to their fraudulent networks, or enter credentials. The strength of these attacks relies on the attacker's ability to appear authentic, and in many cases, users may not notice anything suspicious. To combat this, users should question any requests for their credentials, be hesitant about public network connections, and download applications from trusted sources only, using caution in reviewing permissions granted to the application.

References

Ahsan, M., Gomes, R., Chowdhury, M. M., & Nygard, K. E. (2021). Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector. *Journal of Cybersecurity and Privacy*, *1*(1), 199–218.

Chebyshev, V. (2019). Mobile Malware Evolution: 2018 - Securelist. *Securelist*, 1–20. https://securelist.com/mobile-malware-evolution-2018/89689/.

Chowdhury, M. M., & Nygard, K. E. (2017). Deception in cyberspace: An empirical study on a con man attack. *IEEE International Conference on Electro Information Technology*, 410–415.

Chowdhury, M. M., Nygard, K. E., Kambhampaty, K., & Alruwaythi, M. (2018). Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm. *Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017*, 25–30.

Chowdhury, M., & Nygard, K. E. (2018). Machine learning within a con resistant trust model. *Proceedings of the 33rd International Conference on Computers and Their Applications, CATA 2018*, *2018-March*.

Enck, W., Gilbert, P., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2019). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010*, 393–407.

Felt, A., Greenwood, K., & Wagner, D. (2011). The effectiveness of application permissions. *WebApps '11: 2nd USENIX Conference on Web Application Development*, 75–86.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the ACM Conference on Computer and Communications Security*, 3–14.

'Ghost Push' Malware Threatens Android Users. (n.d.). Retrieved February 15, 2022, from https://www.pandasecurity.com/en/mediacenter/mobile-security/ghost-push-malware-android/

Hassold, C. (2017). *The Mobile Phishing Threat You'll See Very Soon : URL Padding*. PhishLabs. https://www.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding/

Kaspersky Lab. (2019). *The number of mobile malware attacks doubles in 2018, as*

cybercriminals sharpen their distribution strategies. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies

Krishna Kambhampaty, Maryam Alruwaythi, Md Minhaz Chowdhury, K. N. (2019). Trust and its Influence on Technology. *The Midwest Instruction and Computing Sym-Posium 2019*.

Li, R., Shen, C., He, H., Gu, X., Xu, Z., & Xu, C. Z. (2018). A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. *IEEE Transactions on Cloud Computing*, *6*(2), 344–357.

Md Minhaz Chowdhury, K. E. N. (2017). An Empirical Study on Con Resistant Trust Algorithm for Cyberspace. *The 2017 World Congress in Computer Sci-Ence, Computer Engineering, & Applied Computing*

Mobile botnets taking over smartphones – BullGuard. (n.d.). Retrieved February 15, 2022, from https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-botnets.aspx

Samangouei, P., Patel, V. M., & Chellappa, R. (2015, December 16). Attribute-based continuous user authentication on mobile devices. *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015*.

Samani, R., & Davis, G. (2019). McAfee Mobile Threat Report Mobile Malware Continues to Increase in Complexity and Scope. *McAfee*.

Seacord, R. C. (2015). Mobile device security. *MobileDeLi 2015 - Proceedings of the 3rd International Workshop on Mobile Development Lifecycle*, 1–2.

Technologies, P. (2019). *Mobile Application Security Threats and Vulnerabilities 2019: Mobile Device Security - Attacks Research*. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/.

Teh, P. S., Zhang, N., Tan, S. Y., Shi, Q., Khoh, W. H., & Nawaz, R. (2020). Strengthen user authentication on mobile devices by using user's touch dynamics pattern. *Journal of Ambient Intelligence and Humanized Computing*, *11*(10), 4019–4039.

Watkins, L., Kalathummarath, A. L., & Robinson, W. H. (2018). Network-based detection of mobile malware exhibiting obfuscated or silent network behavior. *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, *2018-Janua*, 1–4.

Wu, L., Wang, J., Choo, K. K. R., & He, D. (2018). Secure Key Agreement and Key Protection for Mobile Device User Authentication. *IEEE Transactions on Information Forensics and Security*, *14*(2), 319–330.

Zhu, H., Xiong, H., Ge, Y., & Chen, E. (2014). Mobile app recommendations with security and privacy awareness. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 951–960.

Ahsan, M., Gomes, R., Chowdhury, M. M., & Nygard, K. E. (2021). Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector. *Journal of Cybersecurity and Privacy*, *1*(1), 199–218.

Chebyshev, V. (2019). Mobile Malware Evolution: 2018 - Securelist. *Securelist*, 1–20. https://securelist.com/mobile-malware-evolution-2018/89689/.

Chowdhury, M. M., & Nygard, K. E. (2017). Deception in cyberspace: An empirical study on a con man attack. *IEEE International Conference on Electro Information Technology*, 410–415.

Chowdhury, M. M., Nygard, K. E., Kambhampaty, K., & Alruwaythi, M. (2018). Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm. *Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017*, 25–30.

Chowdhury, M., & Nygard, K. E. (2018). Machine learning within a con resistant trust model. *Proceedings of the 33rd International Conference on Computers and Their Applications, CATA 2018*, *2018-March*.

Enck, W., Gilbert, P., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2019). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones.

Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010, 393–407.

Felt, A., Greenwood, K., & Wagner, D. (2011). The effectiveness of application permissions. *WebApps '11: 2nd USENIX Conference on Web Application Development*, 75–86.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the ACM Conference on Computer and Communications Security*, 3–14.

'Ghost Push' Malware Threatens Android Users. (n.d.). Retrieved February 15, 2022, from https://www.pandasecurity.com/en/mediacenter/mobile-security/ghost-push-malware-android/.

Hassold, C. (2017). *The Mobile Phishing Threat You'll See Very Soon : URL Padding*. PhishLabs. https://www.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding/.

Kaspersky Lab. (2019). *The number of mobile malware attacks doubles in 2018, as cybercriminals sharpen their distribution strategies*. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies.

Krishna Kambhampaty, Maryam Alruwaythi, Md Minhaz Chowdhury, K. N. (2019). Trust and its Influence on Technology. *The Midwest Instruction and Computing Sym-Posium 2019*.

Li, R., Shen, C., He, H., Gu, X., Xu, Z., & Xu, C. Z. (2018). A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. *IEEE Transactions on Cloud Computing*, *6*(2), 344–357.

Mobile botnets taking over smartphones – BullGuard. (n.d.). Retrieved February 15, 2022, from https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-botnets.aspx.

Samangouei, P., Patel, V. M., & Chellappa, R. (2015, December 16). Attribute-based continuous user authentication on mobile devices. *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015*.

Samani, R., & Davis, G. (2019). McAfee Mobile Threat Report Mobile Malware Continues to Increase in Complexity and Scope. *McAfee*.

Seacord, R. C. (2015). Mobile device security. *MobileDeLi 2015 - Proceedings of the 3rd International Workshop on Mobile Development Lifecycle*, 1–2.

Technologies, P. (2019). *Mobile Application Security Threats and Vulnerabilities 2019: Mobile Device Security - Attacks Research*. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

Teh, P. S., Zhang, N., Tan, S. Y., Shi, Q., Khoh, W. H., & Nawaz, R. (2020). Strengthen user authentication on mobile devices by using user's touch dynamics pattern. *Journal of Ambient Intelligence and Humanized Computing*, *11*(10), 4019–4039.

Watkins, L., Kalathummarath, A. L., & Robinson, W. H. (2018). Network-based detection of mobile malware exhibiting obfuscated or silent network behavior. *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, *2018-Janua*, 1–4.

Wu, L., Wang, J., Choo, K. K. R., & He, D. (2018). Secure Key Agreement and Key Protection for Mobile Device User Authentication. *IEEE Transactions on Information Forensics and Security*, *14*(2), 319–330.

Zhu, H., Xiong, H., Ge, Y., & Chen, E. (2014). Mobile app recommendations with security and privacy awareness. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 951–960.