Donna Petitti
COMP.4631

Security Threats in Mobile Apps

[Abstract]

The mobile app market is booming as the increasing number of smartphone users also increases. With this, comes harmful threats and attackers seeking out to achieve personal information from users for their own benefit. This paper discusses various threats and responses to help avoid security issues to protect users.

INTRODUCTION

There are over 6.3 billion smartphone users in the world, causing the mobile app industry to thrive. With the growth of mobile apps, security threats are also increasing with interest. There is a worry for vulnerabilities in these applications and the safety of its users is being risen as a cause for concern. These emerging threats are real and can inflict serious damage.

MOBILE DEVICES

Two of the most popular operating systems for mobile devices consist of Android and iOS. However, the process of developing on each system is vastly different. Android apps are mainly built using Java and Kotlin, whereas iOS apps are being built with Swift. Development with swift requires a lot less writing code, making it easier to complete projects faster than apps made for android phones. Although this is beneficial, iOS development is platform-limited, meaning it is not available cross-platform. Also, the requirements for launching an application in iOS are much higher.

There are many uses of mobile devices and communications, almost every person carries one in their pocket. An application for every activity of human life exists. There are apps for emails, bank transactions, messages, and other sensitive data transfers. Some applications may need to connect to the web or other devices to function. Thus, smartphones are engineered to be able to connect to various subjects such as the internet, PC, or other mobile devices using a wireless network. This is to allow convenience for the usability of the smartphone however, with this convenience comes the possibility of malicious attackers or software can invade someone's device in various paths.

THREATS

Mobile devices contain a lot of private information such as address books, calling history, location information, passwords, emails, etc. These are all assets that can be targeted for an attack. Some threats can be caused by attackers and threats caused by user unawareness or intention some of which consist of the following:

I. Malware

Malware is intrusive software that is designed to damage and destroy the product that it is targeting. It can alter or expose private information that is within the smartphone device. An example of a malware attack consists of miner cryptocurrency mining malware that has been reported infecting Android-based smartphones. This attack infects the device to mine a type of cryptocurrency and send the funds to a single wallet.

II. Wireless Network Attack

Wireless Network attacks use penetration and intrusion acts that target wireless networks to pose serious threats. An attacker can corrupt, block or modify information on the wireless network by eavesdropping, spoofing, or sniffing. An example of this is Bluejacking, which allows someone to be able to send unsolicited messages to another device via Bluetooth.

III. Break-in

Break-in is done when an attacker can gain partial or full control over the target's device by using flaws of code, code injection, or abuse of logic error.

IV. Phishing

Phishing is the act of posing as legitimate institutions to obtain sensitive information from the targeted individual. This can be accomplished through various forms such as email, SMS, and messenger.

V. Loss

This is regarding the act of physically losing or misplacing a mobile device. If in the wrong hands, the attacker is may now have access to all personal information stored on that mobile device.

USER RESPONSE

Not only can it affect an individual, but these threats can also have severe repercussions on employees and companies. What can users do to help avoid security threats to their mobile

devices? Individuals along with companies need to know that it's essential to stay on top of these security risks and what they can do to avoid something dangerous from impacting themselves and others.

First off is to be educated on the types of risks there are out there so that when encountered by something that looks suspicious, you will be able to detect and predict a harmful attack before it happens.

Keeping personal information hidden and secure is another task to help prevent risk. This can be done with many actions, some of which include, updating passwords constantly, not using the same password for every account, using not easily guessable passwords, keeping the system up-to-date, and many more. Using a VPN is also another method that can be done to help secure private information that will allow others to not access the network you are using. Finally, only using secure and trusted apps and websites when sharing personal data and information.

DEVELOPER RESPONSE

There are practices that an app developer should also consider when creating an app to protect their users. Trust is very important when considering the user base because they want to use an app that protects their personal information rather than putting themselves at risk. Here are some areas developers can be cautious of to protect their users:

I. Write Secure Code

Ensuring that the code does not have bugs or other vulnerabilities makes it more difficult for an attacker to get access and break into the application. Security of the app should be thought about upon day one of developing an app. Making it as tough as possible to break through will detour attackers from pursuing targeting an app.

II. Encrypt Data

Data encryption transforms information into another form so make it only accessible to a secret key. Making an app so that any unit of data exchanged with it is encrypted will make it more difficult for an attacker to access private information on the chance the information is stolen because they do not have access to the secret key.

III. Care for Libraries

Libraries make it easier for a programmer to find shortcut methods to create code. However, some can be insecure to use within the app that is being developed. A library has the potential to contain a security flaw that would then allow attackers to execute malicious code which could crash a system.

IV. Testing

Constantly performing tests allows the developer to find any problems within their code. This makes it so that you're always aware of any issues that arise before an attacker can find them first.

CONCLUSION

Mobile apps take part in a huge portion of everyday life, and we need to ensure the safety and quality of them for our users due to their daily growth of them. Several threats can be avoided by putting in both the effort of the user as well as the developer of the app. Security is a huge concern for many people as sharing personal information can have negative impacts on many aspects of life. Continuing to practice the best security measures is how everyone can protect themselves from these worrisome threats.

REFERENCES

[1] App. “Differences between Android and IOS in App Development.” *Yeeply*, 16 June 2020, https://en.yeeply.com/blog/creating-apps-differences-android-ios/.

[2] Hussain, Jordan. “5 Key Differences between Android and IOS App Development by Michael Kelly.” *Irish Tech News*, 30 May 2019, https://irishtechnews.ie/differences-in-android-and-ios-app-development/#:~:text=While%20Android%20apps%20are%20built,apps%20made%20for%20Android%20phones.

[3] Jeon W., Kim J., Lee Y., Won D. (2011) A Practical Analysis of Smartphone Security. In: Smith M.J., Salvendy G. (eds) Human Interface and the Management of Information. Interacting with Information. Human Interface 2011. Lecture Notes in Computer Science, vol 6771. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21793-7_35

[4] KnowBe4. “What Is Phishing?” *Phishing*, https://www.phishing.org/what-is-phishing.

[5] Meserve, Casey. “What Is Mobile Malware? - Definition from Whatis.com.” *SearchMobileComputing*, TechTarget, 21 Dec. 2018, https://www.techtarget.com/searchmobilecomputing/definition/mobile-malware#:~:text=Examples%20of%20mobile%20malware%20attacks&text=Miner%20cryptocurrency%20mining%20malware%20was,funds%20to%20a%20single%20wallet.

[6] Tripwire Guest AuthorsFeb 14, 2018Security Awareness. “Top 10 Mobile App Security Best Practices for Developers.” *The State of Security*, 15 Feb. 2018, https://www.tripwire.com/state-of-security/security-awareness/top-mobile-app-security-best-practices-developers/.

[7] “Types of Wireless Network Attacks.” *Logsign*, https://www.logsign.com/blog/types-of-wireless-network-attacks/#:~:text=Commonly%20known%20as%20wireless%20network,with%20the%20traffic%20of%20information.

[8] “What Is Malware? - Definition and Examples.” *Cisco*, Cisco, 24 Feb. 2022, https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.

[9] "Wireless Attacks and Their Types." *ExamCollection*, https://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html.