MOBILE DEVICE SECURITY

ICTN 6865

BOYD AARON SIGMON
EAST CAROLINA UNIVERSITY

Abstract

Daily usage of mobile devices, such as smartphones and tablets, has surpassed desktop and laptop computers in this day and age. Because of the growing popularity of these pocket-sized computing devices, and the fact that they are almost always full of a person's personal information, attackers now have a number of incentives to try to compromise your mobile device. The purpose of this paper is to discuss some of the most common types of mobile device security threats today, and to provide you with the knowledge of how to protect your mobile device against them.

Table of Contents

1. Introduction

Usage of mobile devices, such as smartphones and tablets, has surpassed desktop and laptop computers in this day and age. These devices are being used for applications like banking, personal digital assistance, remote working, m-commerce, Internet access, entertainment and medical usage [2]. Also, recent innovations in mobile commerce have enabled users to conduct many transactions from their smartphone, such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, processing point-of-sale payments, and even paying at cash registers [8]. Attackers are now targeting these devices because of their lack of security and high probability that they contain sensitive data. In this paper, we will discuss the different mobile device security threats that are present today, as well as discuss the steps that you can take to defend yourself against these threats.

2. Mobile Device Security Threats

Mobile devices are susceptible to many of the same threats as desktop and laptop computers, as well as some additional. Some of the most dangerous threats to mobile devices include theft, malware, phishing attacks, and transmitting data across public Wi-Fi networks. Being aware of these threats and implementing safeguards can prevent you from falling victim to an attack or compromise.

2.1. Mobile Device Theft

Mobile devices are ideal travel companions because they are usually small, easily portable, and extremely lightweight. Because of this, it also makes them very easy to steal or leave behind in airports, airplanes or taxicabs [9]. Also, the devices' mobile nature makes them much more likely to be lost or stolen than other devices, so their data is at increased risk of compromise [7]. In survey by IDG Research and Lookout, 44% of smartphones were stolen because the owner left the phone in a public setting [14].

All of these are reasons are why you should never store sensitive information on your mobile device and make sure your device is password protected. You should also make sure that your device is encrypted and that you have remote wiping capabilities enabled, in case your device is lost or stolen.

2.3. Mobile Device Malware

Much like PCs, mobile devices are also highly vulnerable to malware. A simple task such as just downloading an application or answering an SMS message can be lethal to one's mobile device [1]. Also, downloadable applications introduce many security threats on mobile devices, including both software specifically designed to be malicious as well as software that can be exploited for malicious purposes [2].

To defend against mobile malware, users are encouraged to only download applications from trusted sources, such as the official app stores. Users should also update the software and system updates on their device regularly. Some other defenses include using antivirus software and avoid clicking on links in emails or SMS messages from unknown senders.

2.3. Mobile Device Phishing

Just like the other PC scams, attackers are now using social engineering through mobile apps and SMS text messages to make people click on links [4]. Mobile device users are three times more likely to fall victim of these kinds of phishing attacks than desktop users, because they are less careful and less aware [11]. One of the most popular social engineering attacks on mobile devices is called "smishing". Smishing is another type of phishing when a fake message is sent to the user by text message and asks the user for personal information through web link which is a false website, or a phone number [1]. If you receive a smishing message, it is recommended to contact your cell phone provider and report the incident. Also, users should not click on any links in messages from unknown senders.

2.4. Public Wi-Fi Networks

There are several risks to using public Wi-fi networks with a mobile device. Wireless transmissions are usually not encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit [6]. Also, hackers can exploit weaknesses in these Wi-Fi and cellular data protocols to eavesdrop on data transmission, or to hijack users' sessions for online services, including web-based email [9]. A popular method that attackers use in public settings is hosting fake wireless access points that are designed to trick users into connecting to them. This allows the attacker to easily intercept traffic or direct the user to malicious web pages that may contain malware.

When connecting to public Wi-Fi networks, it is recommended to avoid sending any sensitive information or logging in to any applications that access sensitive data. If you need to access any kind of sensitive data or login into services, you should connect to a trusted VPN to ensure that your transmissions are encrypted. Additionally, you should also enable your local firewall and turn off file sharing to prevent untrusted connections. You should also pay attention to the access points that you are connecting to.

3. Mobile Device Security Defense Techniques

While there are many security risks associated with mobile devices, there are also many ways to mitigate that risk. Most of the risk from the threats listed in the previous chapter can be mitigated by implementing simple security controls, such as password protecting devices, encrypting device data, only installing trusted applications, keeping the system and software up to date, running antivirus, using a VPN connection on untrusted public networks, and having a keen sense of user security awareness.

3.1. Password Protect and Encrypt Mobile Devices

Authentication should be enabled on mobile devices. Devices can be configured to require passwords, PINs, or biometrics to gain access. If using a password or PIN, the password field should be masked to prevent it from being observed by unauthorized users [6]. You should also set an idle time lockout to lock the device after so many seconds of inactivity, and have your device wipe itself after a certain amount of incorrect login attempts. Remote wiping capabilities should also be enabled as well, in case a device is lost or stolen.

To protect you and your company from losing sensitive data, it is recommended to enable encryption on the mobile device to protect data stored directly on the device or memory card. File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools [6].

3.2. Only Install Trusted Apps & Avoid “Jailbreaking”

It is recommended to not install unknown third-party software on your mobile device. One of the best defenses for preventing malware is for users to only download official apps from the app stores [3]. Consumers that load applications to their device only from Google Play, for example, have a 0.1 percent chance of having a potentially harmful application on their device, rather than 0.7 percent for devices that load software from outside of Google [5].

Additionally, it is recommend to not “root” or “jailbreak” the device. This is sometimes used to get access to device features that are locked by default, but can contain malicious code or unintentional security vulnerabilities. Altering the firmware could also prevent the device from receiving future operating system updates, which often contain valuable security updates and other feature upgrades [8]. Also, the ability to keep applications from accessing protected data and to validate applications are both disabled on jailbroken apps [5]. This can cause unwanted exfiltration of data when those controls are disabled.

3.3. Regularly Install System and App Updates

Another critical defense for preventing malware and other attacks is to keep the system and applications up to date. This should be your first line of defense when defending any kind of system. Just like on personal computers, mobile device software and applications contain vulnerabilities that are regularly targeted by attackers and malware. Mobile device companies regularly provide updates to the mobile device operating system, which includes security patches. Check with your device manufacturer for information on how to get the most recent updates [14].

3.4. Install and Run Anti-virus

Malware for mobile devices is on the rise, especially for Android devices. While Android malware currently makes up the majority of mobile malware, iOS devices are not completely immune either [10]. This is why is it is highly recommended to use an antivirus software on your mobile device. Anybody who wants to use a mobile device to access the Internet should install and update antimalware software on their smartphone or tablet. This is especially true for anyone who wants to use such a device for work purposes [12].

3.5. Use VPN when connecting to Untrusted Networks

Public Wi-Fi networks present many security risks to mobile devices because the traffic is usually sent in the clear and unencrypted. When connecting to these networks on your mobile device, you should connect to a trusted VPN connection if you need to access sensitive data, corporate resources, or cloud services. A VPN provides secure access to an organization's network and allows you to get online behind a secure layer that protects your information [13]. Once connected, your traffic will be wrapped in secure tunnel and the routing table on your device will change to make you a part of the trusted VPN network you are connecting to. This will also prevent unwanted users on the public Wi-Fi network from being able to connect to your device. Local firewall software is also recommended to prevent unwanted inbound connections to your device, if you are unable to connect to a VPN.

3.6. User Security Awareness

The last, but most important defense to mobile device security threats, is to provide users with security awareness training. Users are the weakest link in a cyber security attack and should be trained to not click on links in SMS text messages or emails from unknown senders. They should also be trained to only install trusted applications, as well as to keep their device and applications updated, and be cautious of what networks their mobile device is connecting to. A properly trained user can be the difference between whether or not an attack is successful.

4. Conclusion

In conclusion, mobile devices should have the same protections as personal computers. Those protections include putting passwords on devices, encrypting the data on the device, only installing trusted applications, keeping the system and applications updated, installing and running antivirus, connecting to a VPN when using public Wi-Fi networks, and being a security aware user. By following all of the mobile device security defense techniques listed in this paper, you can be assured that you have greatly reduced the risk of having your mobile device compromised.

5. References

[1] Wu, F., Narang, H. and Clarke, D. (2014) An Overview of Mobile Malware and Solutions. Journal of Computer and Communications, 2, 8-17. http://dx.doi.org/10.4236/jcc.2014.212002

[2] Sujithra M and Padmavathi G. Article: Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. *International Journal of*

Computer Applications 56(14):24-29, October 2012. http://research.ijcaonline.org/volume56/number14/pxc3883163.pdf

[3] Shahriar, H., Klintic, T. and Clincy, V. (2015) Mobile Phishing Attacks and Mitigation Techniques. Journal of Information Security, 6, 206-212. http://dx.doi.org/10.4236/jis.2015.63021

[4] Collett, S. (2014, May 21). Five new threats to your mobile device security. Retrieved November 28, 2015, from http://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-device-security.html

[5] Lemos, R. (2015, May 20). How to prevent mobile malware in 3 easy steps. Retrieved November 28, 2015, from http://www.pcworld.com/article/2924195/how-to-prevent-mobile-malware-in-3-easy-steps.html

[6] Cooney, M. (n.d.). 10 common mobile security problems to attack. Retrieved November 28, 2015, from http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

[7] Souppaya, M., & Scarfone, K. (2013, June 1). Guidelines for Managing the Security of Mobile Devices in the Enterprise. Retrieved December 1, 2015, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[8] Ruggiero, P., & Foote, J. (2011). Retrieved December 1, 2015, from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

[9] Poarch, D., Cook, M., & Grahn, A. (2015, June 8). Mobile Device Security in the Workplace: 6 Key Risks & Challenges. Retrieved November 28, 2015, from http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-6-Key-Risks-and-Challenges

[10] 2015 Mobile Threat Report. (2015). Retrieved November 28, 2015, from http://solutions-review.com/dl/2015_Pulse_Secure_Mobile_Threat_Report_TL65.pdf

[11] Kessem, L. (2012, July 25). Rogue Mobile Apps, Phishing, Malware and Fraud - Speaking of Security - The RSA Blog and Podcast. Retrieved December 1, 2015, from https://blogs.rsa.com/rogue-mobile-apps-phishing-malware-and-fraud/

[12] Tittel, E. (2014, February 13). 7 enterprise mobile security best practices. Retrieved December 1, 2015, from http://www.csoonline.com/article/2134384/data-protection/7-enterprise-mobile-security-best-practices.html

[13] Kugler, L. (n.d.). 9 Ways to Keep Your Mobile Devices Secure While Traveling. Retrieved December 1, 2015, from http://www.pcworld.com/article/218671/9_ways_to_keep_your_mobile_devices_secure.html

[14] Lookout. (n.d.). Retrieved December 1, 2015, from https://www.lookout.com/resources/reports/phone-theft-in-america