Sierra Victor MSP 2 Mobile Phone Security and Privacy 20230117

17 January 2023

Good day all,

This is a message from Sierra Victor on **Mobile Phone Security & Privacy (MSP).**

1. INTRODUCTION.

Security and privacy are highly dynamic and fast-paced research areas due to rapid technological advancements. Mobile security and privacy are no exception. For example, 10 or 15 years ago, research in mobile security was mainly concerned about securing the Global System for Mobile Communications (GSM) network and communications. Since mobile phones become user programmable (i.e., the device supports third-party software), the scope for security and privacy research extends to studying the security of such third-party software and associated privacy risks (e.g., whether third-party software will result in the leakage of user data). It is also in the user's interest to ensure both confidentiality and integrity of the data that is stored on and made accessible via these devices. This is the focus of this program. Specifically, in this program, we will be presenting the state-of-the-art advances in mobile device security and privacy. Such devices (e.g., Android, iOS, Apple, and Windows devices) are, in fact, “minicomputers,” with processing, communication, and storage capabilities. In addition, these devices often include additional sensing capabilities from the built-in camera, GPS, barometer, accelerometer, and gyro sensors. It should be noted that the modern-day mobile devices are generally more powerful than the IBM Deep Blue supercomputer of 1997.

2. THREATS TO MOBILE SECURITY.

Mobile threats can be broadly categorized into application-, web-, network-, and physical-level threats, as discussed in the following section.

2.1 Application-Level Threats.

Application-level threats appear to be the most widely discussed threats in the literature. As mobile devices can execute downloadable applications (apps), it is clear that apps can be a target vector to breach the security of the device and the system it connects to (e.g., a corporate network). The threats can be due to malicious applications (malware), particularly those downloaded from a third-party app store, as well as vulnerable apps. Malware can, for instance, inject code into the mobile device in order to send unsolicited messages; allow an adversary the ability to remotely control the device; or ex filtrate user data, such as contact lists, email, and photos, without the user's knowledge or permission. For example, in a recent work, mobile security researchers demonstrated that it is possible to ex filtrate data from Android devices using inaudible sound waves. In the rush to reduce the time-to-market, applications are usually designed with functionality rather than security in mind. Hence it is not surprising that there are a large number of applications that contain security loopholes that can be exploited by an attacker. In another recent work, Chen et al. (2016) discussed how a botnet master issues commands, via multiple message push services, to remotely control mobile devices infected by malware. While vulnerable apps may not be developed with a malicious intent, they can result in significant security and privacy risks to the users.

2.2 Web-Level Threats.

While these threats are not specific to mobile devices the security and privacy risks to mobile devices due to web-level threats are real. One key web-level threat is phishing, which uses email or other social media apps to send an unwitting user links to a phishing website designed to trick users into providing sensitive information such as user credentials. When combined with social engineering, phishing is one of the top seven security threats identified by Kaspersky Lab for the 2015 and 2016 years.

2.3 Network Level Threats.

One of the distinct features of mobile devices is the ability to connect. Typical connection supported by currently mobile devices include cellular/mobile networks, local wireless networks, and near field-communication (NFC). Security of the connection at the network level is another active research area.

2.4 Physical-Level Threats.

Finally, physical security of mobile devices is equally important, if not more so. Since mobile devices are typically small and portable, these devices can be easily stolen or misplaced. A lost or stolen device could be used to gain access to user data stored on the device or as an entry point into the user's corporate network.

The rest of this program is organized as follows:

- The use cases of mobile devices within an organization's context and their security implications from a practitioner's perspective are presented in Chapters 2 through 5.
- Chapters 6 and 7 explain how malware and vulnerabilities can be identified using state-of-the-art techniques.
- Chapter 8 examines the effectiveness of existing anti malware Android apps.
- Chapter 9 focuses on mobile forensics.
- Chapter 10 presents a security framework on Internet of Things (or IoT for short) security protocols.
- Chapter 11 introduces the common security models for generic privacy requirements.
- Finally, preliminary experimental results on the implementation of cryptographic algorithms on mobile devices are presented in Chapter 12.

Controlling Access to your Device.

To access your device you'll need to prove you're allowed to use it – typically by using your password, PIN code, or fingerprint. Once you've unlocked it, you'll have access to any online accounts associated with it (e.g. iCloud, Google, Microsoft Live) and securing these accounts is just as important as securing the device itself.

When buying a new device or upgrading your contract, look for the following features:

- Devices that can be unlocked in different ways. Many devices can now be unlocked using biometrics (such as a fingerprint or face recognition).
- Online accounts that support 'two-factor authentication'. This is where you'll need to enter a code from an app (or text message) on your phone in order to log into your account. This makes it significantly harder to break into your account if your password is compromised.

- Devices that reduce your reliance on passwords. Look for devices that let you make purchases or download apps using a biometric (such as a fingerprint) rather than typing your password each time. This makes it easier to use the device and is often more secure

Make sure that you…

- Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock). CyberStreetwise has some good advice on passwords. If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess.
- Secure any linked online accounts. Strong passwords are one of the best defences against many threats you'll face on the Internet, so set a strong password and turn on twofactor authentication. Don't re-use passwords across devices or accounts. You can use a password manager to help you remember different passwords for all your accounts.
- Set up security questions that are hard to guess. Security questions are often used when requesting new passwords from your service provider. Ensure that your answers can't be easily guessed by people that know you, or gleaned from information you've posted on your social media accounts.
- Follow the manufacturer's guidance. This will include important information about securing your device and online services.

We will continue in our next message on **Mobile Phone Security & Privacy (MSP)** with **Mobile Security: A Practitioner's Perspective.**

Thank you for listening or reading this message. Please feel free to use and distribute as needed. Our messages are not by any means intended to assist anyone in any unlawful action, but rather to equip you with the necessary theoretical background in order to assist yourself, local armed forces or police in stabilizing a SHTF situation or any other daily threats on your life or rights as a law abiding citizen. Please contact any admin on any Sierra Victor group for our previous material or search us on Youtube.

We wish you well.

Sierra Victor