Mobile Device Security

(3 hours)

Lila Ghemri

Department of Computer Science
Texas Southern University
ghemri_lx@tsu.edu

This work was supported by NSF grants 1241772

Any opinions, findings, conclusions, or recommendations expressed herein are those of the authors and do not reflect the views of the National Science Foundation

Objectives and Prerequisites

- Understand the security and privacy threats to the mobile devices
- Understand the basic strategies and approaches to enhance mobile device security and privacy.
- Mitigations: Device configuration, user authentication, apps certification, data encryption

- Prerequisites:
  - Networking, Databases, Encryption and Operating Systems

Mobile Devices (Wikipedia)

- A **mobile device** (also known as a **handheld computer**) is a small, handheld computing device, typically having a display screen with – screen input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg).[
- A handheld computing device has an operating system (OS), and can run various types of application software, known as apps.
- Most handheld devices are also equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset.
- A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source.
- Smartphones, tablets and PDAs are popular mobile devices.

Physical threats to Mobile Devices

- Mobile devices get lost, stolen or are borrowed, which means that they have No Security
- Physical access to a device no longer requires breaking into a secure facility.
- Mitigation:

The best solution for this problem is to assume that physical access will be granted to untrusted parties.

Secure Data Storage

- Information in many mobile devices is stored locally, including password files and authentication tokens.
- The ability to store sensitive data locally in a secure manner and also keeping it accessible to applications that need it to function properly, is a challenge.

Lila Ghemri

Authentication and keyboards

- Strong authentication : A password that contains a combination of letters (one which should be uppercase), numbers, special characters is now the industry standard.
- This standard is almost impossible to uphold using mobile devices keyboards, which are small and difficult to use, especially non smart mobile phones.

Safe Browsing Environment

- The lack of display space on the mobile device causes some security issues:
  - Difficult to see the entire URL or the URL at all, makes it vulnerable to phishing attacks.
  - Links are followed more frequently on mobile devices than other computing platforms making scamming easier.
  - Mobile devices heavy reliance on URL links makes it difficult to distinguish safe links from compromised ones.

Lila Ghemri

Secure Operating Systems

- Securing the mobile device operating system is the responsibility of the vendor.
- However, oftentimes, securing the system by updates or patches requires a system downtime.
- This can prevent the user from using their device, even to make a simple phone call.
- Consequently, it may discourage vendors and users from making frequent updates to secure the device.

Application Isolation

- Numerous applications reside in the memory of a mobile device.
- These applications require access to different types of data.
- A device should be able to isolate these applications and the data they use.

Information Disclosure

- Sometimes, the data stored on the device is worth more than the device itself.
- The fact that a mobile device has a high likelihood to be lost, stolen or simply to be used by someone else compounds the problem.
- The loss of data residing on the device is a concern as well as the potential access from the device to others networks (private or corporate).

Spyware, Malware and Phishing

- The mobile computing environment with its limited display space requires the presence of links.
- The possibility to access the Internet bring the threats of mobile viruses, worms, Trojans, etc..
- A new attack class is developing in which worms are spread through SMS and messages.
- The lack of space on a mobile device screen makes it impossible to see the full URL of the source web page. The user cannot ascertain the validity of a link before clicking on it, which makes it vulnerable to phishing attacks.

Cross-site Request Forgery (CSRF)

- CSRF is an attack that affects web applications.
- It allows the attacker to access and update a victim’s information, such as email, or password, on a vulnerable application.
- The victim usually clicks on a link that sends them to the destination of their choice, but also sends hidden web request to another application the user is also logged in and extracts or changes information from that application.

Location Privacy/Security

- The use of GPS, location software, to detect the mobile device whereabouts introduces a level of OS security issues that is new for computing platforms.
- The loss of location privacy is now mostly widely accepted by users.

Lila Ghemri

Insecure Device Drivers

- Most applications should *not* have system access to the device.
- However, some applications may require it.
- Many mobile operating systems have built-in a variety of strong security protection schemes against system-level access to the OS.
- Some third-party applications include methods to get around these protections and hence make the whole device more vulnerable.

Risks of Mobile Computing Devices to “traditional” Systems

- Mobile computing devices are of concern because of
  - the data that might be stored on them,
  - and because they may provide access to other services that store or display non-public data.
- This access may be enabled because the mobile device contains passwords or security certificates that identify the device or its user to the email system, Virtual Private Networks (VPNs), or other applications.

Data Security Requirements

- Remove sensitive data from device.

In particular, data items such as Social Security Numbers, credit card numbers, or checking account numbers.

- Restrict the storage of data that is non-public data.
- Password protect your device.

Mobile Phones and Tablets Protection

- Label your device with your name and a phone number where you can be reached to make it easy to return to you if it is lost, even if the battery is dead.
- Configure a passcode to gain access to and use the device.
- Set an idle timeout that will automatically lock the phone when not in use.
- Keep all software up to date, including the operating system and installed "Apps". This helps protect the device from attack and compromise.
- Do not "jailbreak" or "root" your device. "Jailbreaking" and "rooting" removes the manufacturer's protection against malware.

Lila Ghemri

Mobile Phones and Tablets Protection

- Obtain your apps only from trusted sources such as the *Apple iTunes Store*, *Google Play*, or the *Amazon App Store for Android*.
- Enroll your device in “Find my Iphone” or “Find my Phone” or an equivalent service. This will help you locate your device should it be lost or stolen.
- If your device supports it, ensure that it encrypts its storage with hardware encryption.

Mobile Device Managed Environments

- A Mobile device management (MDM) includes software that provides the following functions:
  - software distribution,
  - policy management,
  - inventory management,
  - security management and
  - service management
- It is usually a corporate decision to enroll its devices to a MDM service.

Functions of a MDM Environment

- Establish an authenticated and encrypted connection between an enrolled mobile device and the MDM gateway server enabling all traffic to and from the device network to be redirected through it and the Gateway Server.
- A registered device can interact with the MDM server after it successfully authenticates itself.
- The device management server collects information about the smartphone or tablet and then sends the applicable settings and applications to it

MDM Environment Functions

- MDM allows administrators to enable or disable any functionality of the device;
- decommission inactive devices,
- blacklist and whitelist applications or selectively wipe data from a device as per the mobile policy and the user cannot override it.
- It also supports remote location of any device and provides troubleshooting services to any device.
- The MDM also regularly checks and evaluates for newly published software package distribution.

Suggested Exercise 1

Device Security: Establishing a PIN to your SIM Card:

On iPhone:

1. Select Setting|Phone|SIM PIN
2. Turn on the SIM PIN Option
3. Enter the current PIN(1111, or 0000 or 3436)
4. Select Change PIN
5. Select Settings|General|Passcode Lock
6. Enter your four-digit code

On Windows Mobile phone:

1. Select Start|Setting|Security
2. Select Device Lock
3. Enter your four-digit code

Suggested Exercise 2

Location tracking devices:

Using an example of a location tracking device, study the pros and cons of saving the data in a database, taking into account the user's privacy.

Bibliography

- Guidelines for Securing Mobile Devices at

http://www.stanford.edu/group/security/securecomputing/mobile_devices.html

- **Mobile Device Management** at

http://www.xcubelabs.com/blog/mobile-device-management-enable-manage-and-secure-your-mobile-environment/

- **Mobile Applications Security** H. Dwivedi, C. Clark, D. Thiel McGraw Hill Professional Series, 2010
- **Building Secure software**, by J. Viega and G. McGraw, Addison-Wesley , 2005
- **Lost cellphones added up fast in 2011** http://www.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1
- **Cyber Threats to Mobile Phones** US-CERT Resource Paul Ruggiero and Jon Foote

http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf