Chapter 16

Mobile Device Security

SYBEX

Overview

- Quick Overview of Mobile Devices
- Mobile Threats and Attacks
- Countermeasures

SYBEX

Overview of Mobile Devices

- **Mobile devices**
  - Mainly smartphones, tablets
  - Sensors: GPS, camera, accelerometer, etc.
  - Mobile hardware
  - Mobile software

SYBEX

Mobile Threats and Attacks

- Data Leakage
- Unsecured Wi-Fi
- Network Spoofing
- Phishing attacks
- Spyware
- Broken cryptography

SYBEX

Device Malware

- **iOS malware: very little**
- **Android malware growth keeps increasing**
- **Main categories:**
  - Trojans
  - Monitoring apps/spyware
  - Adware
  - Botnets

SYBEX

Location Disclosure

- MAC, Bluetooth Addresses, IMEI, IMSI, etc. are globally unique
- Infrastructure based mobile communication
- Peer-to-Peer ad hoc mobile communication

SYBEX

Mobile Access Control

- **Very easy for attacker to control a mobile device if he/she has physical access**
  - Especially if there's no way to authenticate user
  - Tempting target for thieves
  - Theft of mobile devices increasing
- **Need access controls for mobile devices**

SYBEX

Authentication: Categories

- **Authentication generally based on:**
  - Something supplicant knows
    - Password/passphrase
    - Unlock pattern
  - Something supplicant has
    - Magnetic key card
    - Smart card
    - Token device
  - Something supplicant is
    - Fingerprint
    - Retina scan

SYBEX

Password Cracking

- Passwords are the most widely used form of authentication
- Usernames and passwords are a commonly targeted item
- Enumeration may have gathered usernames in some cases
- Password cracking is used to obtain passwords
- Password cracking refers to a group of techniques
- Is an essential skill for penetration testers

SYBEX

What Makes a Password Susceptible to Cracking?

- Passwords that contain letters, special characters, and numbers: stud@52
- Passwords that contain only numbers: 23698217
- Passwords that contain only special characters: &*#@!(%)
- Passwords that contain letters and numbers: meetl23
- Passwords that contain only uppercase or only lowercase: POTHMYDE
- Passwords that contain only letters and special characters: rex@&ba
- Passwords that contain only special characters and numbers: 123@$4
- Passwords of 11 characters or less

SYBEX

An Overview of Malware

- **Malware**
  - Malware is an umbrella term for several forms of bad software
  - Malware has become more destructive and stealthy
  - Has evolved to more readily steal information
  - May be useful, but potentially risky to use during a test

SYBEX

Forms of Malware

- Viruses
- Worms
- Trojan Horses
- Rootkits
- Spyware
- Adware
- Ransomware

SYBEX

Summary

- Mobile devices are increasingly popular
- There are many threats and attacks against mobile devices, (e.g., loss/theft, sensitive information leakage, and location privacy compromise)
- Mobile access control, information leakage protection, and location privacy protection, etc.

SYBEX