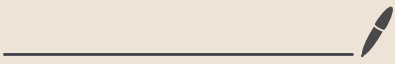
Chapter 17

Hacking Mobile Platforms



Mobile Platform Attack Vectors

- 3G, 4G, 5G, Bluetooth, WiFi, Wired

OWASP - Top 10 Mobile Risks

- Improper Platform usage
- Insecure data storage
- Insecure communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorisation
- client Code Quality
- Code tampering
- Reverse Engineering
- Extraneous Functionality

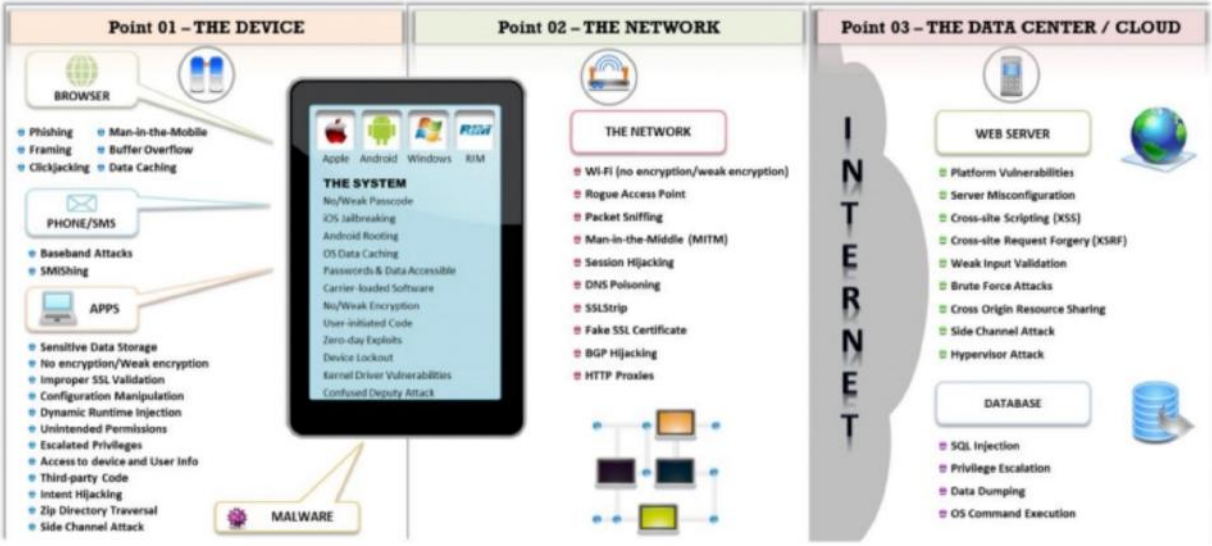


Figure 17.2: Anatomy of a mobile attack

- Browser (framing):
  - Web page integrated to another webpage using iFrame
  - attacker embeds malicious web page for clickjacking.
- Data Caching
  - Store info as cache for better response.
  - access sensitive info from cache.

- User initiated Code
  - trick to install malicious app to install malicious code to exploit user's browser, cookie, security permissions.

- SSL Strip
  - type of MITM attack
  - exploit SSL/TLS vulnerabilities.
  - downgrades connection to HTTP (No encrypt)

---

bluesnarfing - steal info via bluetooth

bluebugging - gain control via bluetooth

Agent Smith Attack

- installs malicious app to produce huge volumes of ads on victim's device through financial gain

SimJacker (Sim-Card Attack)

- Vulnerability in SIM card's S@T browser, Pre installed software on SIM cards.
- capture location, monitor calls, auto-open links, Perform DoS attacks.

Hacking Android OS

Android Device Administration - API

- System level administration for device
- creates security aware applications.

Android rooting

- attain privileged control with android subsystem

Process:

1. exploit device firmware vulnerability
2. Copy SU binary to Current Process path.
   (/system/xbin/su)
3. Grant executable pomission - chmod.

Benefits

- run privileged commands

- Modify, delete system files.
- remove manufacture application (bloatware)
- Wifi & bluetooth tethering
- Install apps on SD card.

Disadvantages

- Void phone's warranty
- Poor Performance
- Malware Infection
- Bricking device.

Methods

1. PC → KingoRoot (USB debugging)
2. KingoRoot.apk (unknown source installation)
3. TunesGo Root
4. One Click Root

5. SuperSU

Blocking WiFi Access

- NetCut is a WiFi killing application
- Identify target device & block access to WiFi

Identifying attack Surfaces

- Drozer tool to discover vulnerabilities, attack surfaces.
- Fetch Package Information
- Identify Attack Surface
- Launch Activities.

zANTI - Spoof MAC address, create malicious WiFi hotspot, hijack Session.

Network Spoofer - change websites on someone's computer from android phone. (redirection)

LOIC

- Low Orbit Ion Cannon
- perform Dos / DDoS attacks on target
- perform UDP, HTTP, TCP flood attacks

DroidSheep

- perform web session Hijacking / sidejacking
- listens for HTTP packets via (802.11)
- extracts session IDs from packets to reuse
- captures using libpcap library of supports OPEN network, WEP, WPA, WPA2 networks.

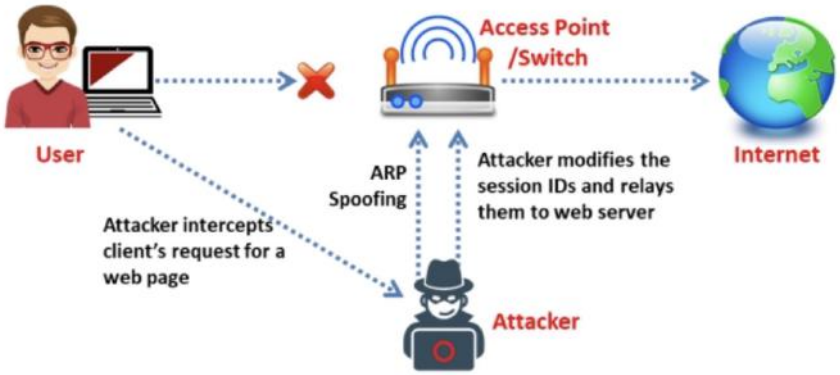


Figure 17.24: Example of Session Hijacking attack with DroidSheep

Orbot Proxy

- Proxy app to privately use Internet
- uses Tor to encrypt Internet traffic
- hide identity while performing attacks.

Phonesploit

- ADB (Android Debug Bridge) is a command line tool to communicate with target android device

- if target enabled debugging (TCP:5555), Perform - screen capture, dump info, Port forwarding, install/uninstall, turn WiFi on/off

Android based Sniffers

FaceNiff - sniff, intercept web session profiles (WEP/WPA-PSK/WPA2-PSK/OPEN)

Android PCAP

Man-in-the-Disk

- Perform MITD when proper security is not given to external storage.
- leads to installation of malicious apps.

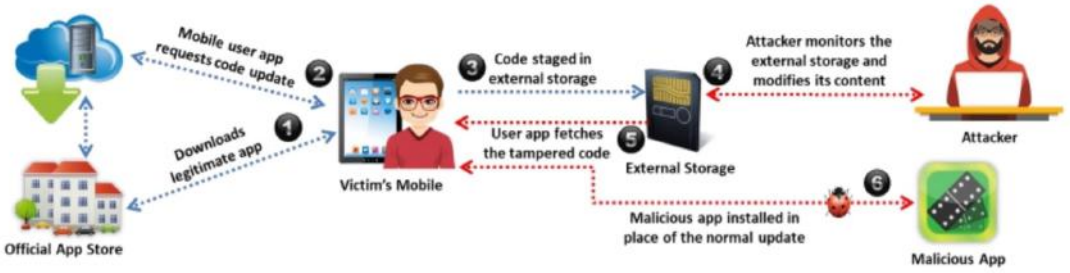


Figure 17.29: Man-in-the-disk attack

Spearphone Attack

- records loudspeaker data without privilege
- eavesdrop loudspeaker voice by exploiting hardware based motion sensor.

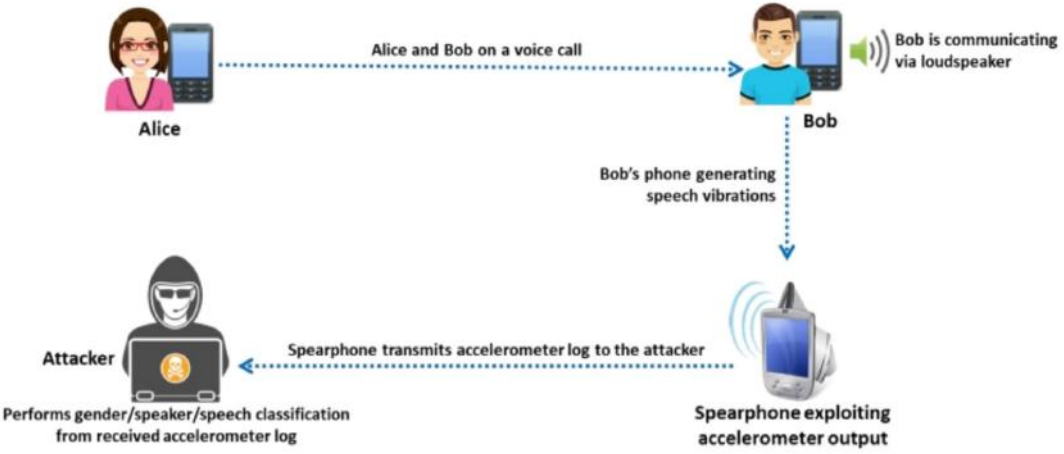


Figure 17.30: Spearphone attack

Other Techniques

- Advanced SMS Phishing.
- Bypass SSL Pinning — MITM
  (reverse engineering, hooking)
- Tap 'n Ghost attack.
  (NFC, Rx electrodes — Touchscreen)
  - Tag based Adaptive Play (TAP)
  - Ghost Touch Generator
- Android Trojans
  - GuStuff (banking)
  - xHelper

Hacking Tools

- csplort (Pentesting)
- Fing (networking)

Secure Android device

- enable screen locks
- download only from official stores
- No apk from Internet
- Update OS
- Never root devices.

Security Tools

- Kaspersky Antivirus
- Find My device / where's my droid
- Xray (Security Vulnerabilities)
- online Android analyser (analyse APK files)

Hacking iOS

Types of Jail Breaking

- Userland Exploit (only user)
- iBoot Exploit (user + iboot level)
- Bootrom exploit (")

Techniques

- Untethered Jailbreaking (Kernel Patch)
- Semi-tethered Jailbreaking (No Kernel Patch)
- Tethered Jailbreaking (No " ")
- Semi-untethered Jailbreaking (without computer)

Tools used:

- Cydia (find, install software package)
- Hexxa Plus (install themes, tweaks, apps)
- Apricot (web based mirror OS)

Spyzie

- hack SMS, call logs, chats, GPS
- attack remotely in invisible mode.

Network Analyser Pro

- discover LAN device addresses, names.

iOS Trust Jacking

- read messages, emails & capture sensitive info from remote location.
- exploits "iTunes Wifi Sync" feature.

iOS Malware

- Clicker Trojan Malware
- Trident (spyware)

Hacking Tools

- Elcomsoft Phone breaker
  - logical & Over the Air acquistion
  - break encrypted backups
  - obtain, analyse backups
- Fing (Network Scanner)

Secure iOS devices

- Use passcode
- disable Javascript, add ons
- don't Jailbreak / root device
- Find My iphone
- Enable Jailbreak detation.
- regularly update device.

Mobile Device Management

- platform for over the air / wired distribution of application & data & setting.
- helps System admin. to deploy & manage Software application.

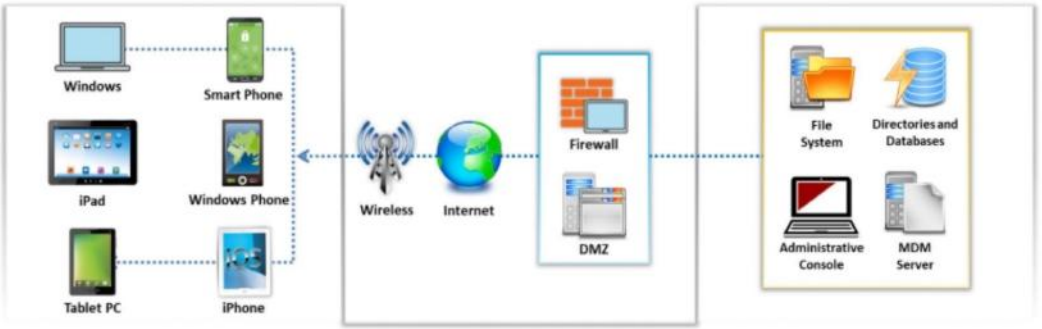


Figure 17.65: Schematic of Mobile Device Management (MDM)

- IBM MaaS 360
- Citrix Endpoint Management

Mobile Security Guidelines and Tools

- identify & protect sensitive data.
- handle password credentials securely
- Implement AAA properly
- keep backend API, platform secure
- Prevent unauthorised access to paid-for
- ensure secure distribution of apps
- Don't load too many applications
- Perform security assessment
- securely wipe/delete data.

Source Code Analysis Tools

z3A Advanced App Analysis

(identifies Security, Privacy risks)

Reverse Engineering Tools

APKtool (form, rebuild modifications)

Promon Shield (App repacking detector)

Protection Tools

Lookout Personal (Security threat, loss, theft)

Zimperium zIPS (intrusion prevention)

BullGuard Mobile Security (antivirus)

Malware Bytes (Android — Malware, Ransomware)

Mobile Pentesting Tools

- ImmuniWeb (ML to augument, accelerate Manual mobile pentesting of iOS)
  - Zero False positive SLA
  - threat aware risk scoring
  - Remediation Guidelines
  - CVE, CWE, CVSSv3 scores