Module - 16
Hacking Mobile Platform

- **ROM :** Modified version of Android operating system
- **AOSP** : Android Open Source Project : Strip Down version of android operating system given to developers and manufacturer so they can customise
- **Firmware** : It is a piece of software that makes the hardware function correctly with the OS
- **Open Source** : Piece of software free to edit
- **Bloatware** : Software or application that are installed on your mobile device that you don't need
- **APK :** file extension for android environment
- **Stock Rom** : ROM that comes stocked with the device
- **CyanogenMod** :
- **Odex** : Files that are a collection of parts from application that are optimized before booting
- **OTA** : Over The Air : We get the updates OTA
- **Recovery and Download Modes :** recovery mode is used to reset the device
- **Bricking :**
- **Jailbreak :** Jailbreak in the iOS World is simply the process of removing some software restriction that apple has imposed on devices, It is done through software exploit.
- **Unlocking :** Unlocking is basically allowing me to get the phone to work in different carrier
- **Kernel :** computer program that manages the input and output request from software and Translates them into instruction for the CPU.
- **Rooting :** Rooting is giving me access at the root level.

Attack Vector :

Malware :

- OS Modification.
- Application Modification
- Viruses, Worms, Rootkits

Data Storage :

- Emails
- Copying
- Encypting the Data storage

Social Engineering :

- Non-Technical
- Manipulation
- Email/MMS/SMS
- Social Networks
- Video Chat

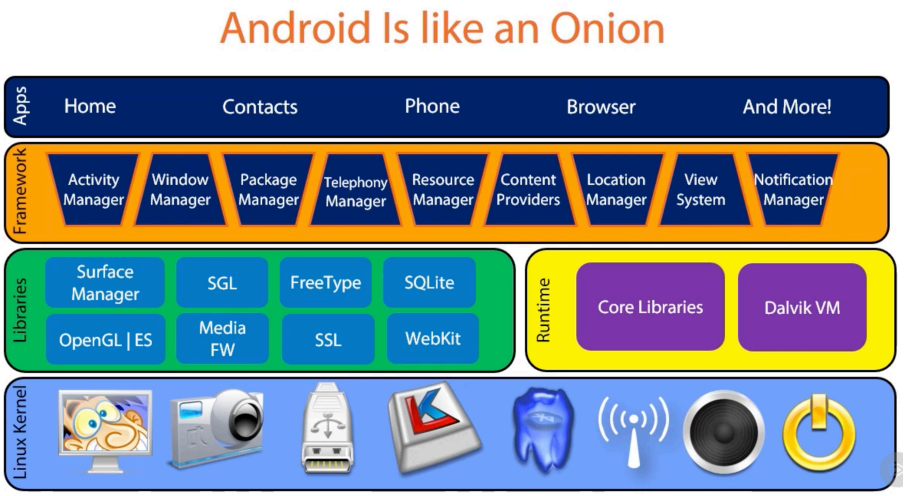
SMS Phishing :

Hacking Android :

Understanding the architecture :

Countermeasures :

- Don't click on any links in any SMS
- Don't Reply any suspicious SMS
- Check your financial companies
- Don't call any number in a suspicious SMS
- Ignore any SMS which are urging you to react quickly
- Derive-by's : When we go to a site and get infected by the virus
- Older Version of Operating Systems



Understanding the Device :

Security Model :

1. Normal 2. Dangerous 3. Signature 4. SignatureOrSystem

Application Modules

1. Activites 2. Content Providers 3. Services 4. Broadcast Receivers

Data Storage :

1. NAND Flash (Non Volatile Storage Mechanism) 2. SD(internal/external) 3.NFC

4. **Android Debug Bridge (ADB) :** Command Line Interface that allows you to communicate with mobile device via USB Cable: Remote Shell, Push/pull commands , Logcat (Logging Information), Install (installing APK files),

Rooting :

- Rooting elevates your privileges
- Run Specialized apps
- Side loading : Sideloading describes the process of transferring files between two local devices

Bootloader :
Bootloader is the first thing that fires off when your device is turned on same as BIOS in PC
Tells the OS to boot, Every device has their own boot loader

Kernel :
Apps to hardware communication channel
Kernel underclock the CPU for Battery saving

Baseband :
Software that allows the correct communication with the radio and the operating system. Many vendors don't update these basebands.
Radio

Recovery :
- Stock recovery
- Custom recovery

Dalvik-Cache & ART :
ART is a new runtime for android

Download Mode :
This mode is also known as Fast-boot mode, gives you the ablitiy to flash images

Attacks :

Decompiling
Disassembly
Repacking

Network Attacks
NFC Attacks
Relay Attack

Data Leakage :
- Internal Files
  App uses UID & GID
- External Storage
  SD Cards
- SQLite
  Android Supported
- Logs
  Designed for Debugging
- URI Scheme
  using web page to access SD
- Insecure content
  Wi-Fi

Malware :

Lock it down

No Side Loading
Updates
Screen locks
Use Legit App stores
Security Apps
Protect the apps

Hacking iOS :

Understanding the Architecture

Understanding the Device

Application security :

- Application code signing certificates
- All application of apple is signed by the apple certificate and if you want to run third party then that should first go to apple and approve a apple certificate.
- Runtime Security
- Extensions
- Apps Groups
- Accessories

Jailbreaking :

Removing restriction via exploit
Custom kernel is used with root access
Allow software that apple blocks
customization / unlocking

Typed of Jailbreaking :

Untethered
No Computer helping out
Tethered
Help, I need Somebody (Computer)
Semi-Tethered
Need a little help from my friend

Exploits :

Userland Exploit : It allows user-level Access bur does not allow iboot level access
iBoot Exploit : allows for jailbreaking it allows for both user-level and iBoot Level access
Bootrom exploit : This allow both user-level and iBoot Level access

Tools :

1. Pwnage 2. Redsn0w 3. Jailbreakme 4. Evasio0n 5. Pangu8

---------- **Hacking Mobile Devices** ----------

App Sandboxing Issue : Sandboxing helps protect systems and users by limiting the resources the app can access to the mobile platform, However malicious application may exploit vulnerabilities and bypass the sandbox.

Mobile Spam :

- Unsolicited text/email messages sent to mobile devices from known/unknown phone number and email IDs
- Spam message contains advertisements or malicious links that can trick users into revealing confidential information
- Significant amount of bandwidth is wasted by spam messages
- Spam attacks are performed for financial gain

SMS Phishing attack (SMSiShing)(Targeted Attack Scan) :

SMS Phishing is the act of trying to acquire personal and financial information by sending SMSs containing deeptive links

Exploiting SS7 Vulnerability :

Signaling System 7 (SS7) is a communication protocol that allow mobile users to exchange communication through another cellular network.
SS7 is a operative depending on mutual trust between operators without any Authentication
Attacker can exploit this vulnerability to perform a man-in-the-middle attack, impeding the texts and calls between communicating devices.

Android Rooting :

Rooting allows android users to attain privilege control (known as "root access") within android subsystems
Rooting process involves exploiting security vulnerabilites in the device firmware and copying the SU Binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the chmod command

Rooting enables all user-installed to run privilege command :
1. Modify or delete system files
2. Removing carrier-or manufacture-installed application (bloatware)
3. Low level access to the hardware
4. Wifi and bluetooth tethering
5. install application on SD CARD

ROOTING also comes with many security and other risks
1. voiding of phone's waranty
2. poor performance
3. Malware infection
4. Bricking of Device

Session hijacking Using DroidSheep :
It listens for HTTP packets ent via a wireless network connection and extract the sessions ID from these packets to reuse them
DroidSheep can capture session using libpcap library and support OPEN network, WEP Encryption and WPA, WPA2(PSK only) encrypted network.

Launching Man-in-the-Disk Attack :

Attackers perform Man in the Disk attack when application donot incorporate proper security measure against ussage of the device's external storage.
This vulnerability lead to the installation of potential malicious apps to the user's devices, thereby blocking access to legitimate apps.

Launching Spearphone attacks :

A Spearphone attack allows android apps to record loudspeaker data without any privileges
Attacker can eavesdrop on loudspeaker voice conversation between remote mobile users by exploiting hardware-based motion sensor i.e accelerometer.

Gustuff Banking Trojan : It is andorid trojan

Jailbreaking is defined as the process of installing a modified set of kernel patches that allows user to run third party applications not signed by the OS vendor.
Jailbreaking provides root access to the OS and permits downloading the third party application,themes and extensions on iOS Devices
Jailbreaking removes sandbox restriction which enables malicious apps to access restricted mobile resources and info.

iOS Trustjacking :

iOS Trustjacking is the vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge
This Vulnerability exploits the "iTunes Wi-Fi Sync" features, where the victim connects their phone to any trusted computer that is already infected by an attacker.

iOS Malware :

1. Clicker Trojan Malware : Automatically open web pages in the backgrounds and click ad links without the user's knowledge

2. Trident : It is Sophisticated Spyware
3. Exodus
4. checkrain
5. AceDeceiver Trojans
6. XcodeGhost
7. KeyRaider

Mobile Device Management :

Mobile Device Management (MDM) provides platform for over-the-air or wired distribution of application and data and configuration settings for all type of mobile devices, including mobile phones, smartphones, Tablet and computers
MDM help in implementing enterprise wide policies, to reduce support cost, business discontinuity, and security risk.
it helps system administrator to deploy and manage software application across all enterprise mobile devices to secure, monitor, manage and support mobile devices.