
C|EH
Certified Ethical Hacker
Module 17
Hacking Mobile Platforms

Module Objectives

Module Objectives

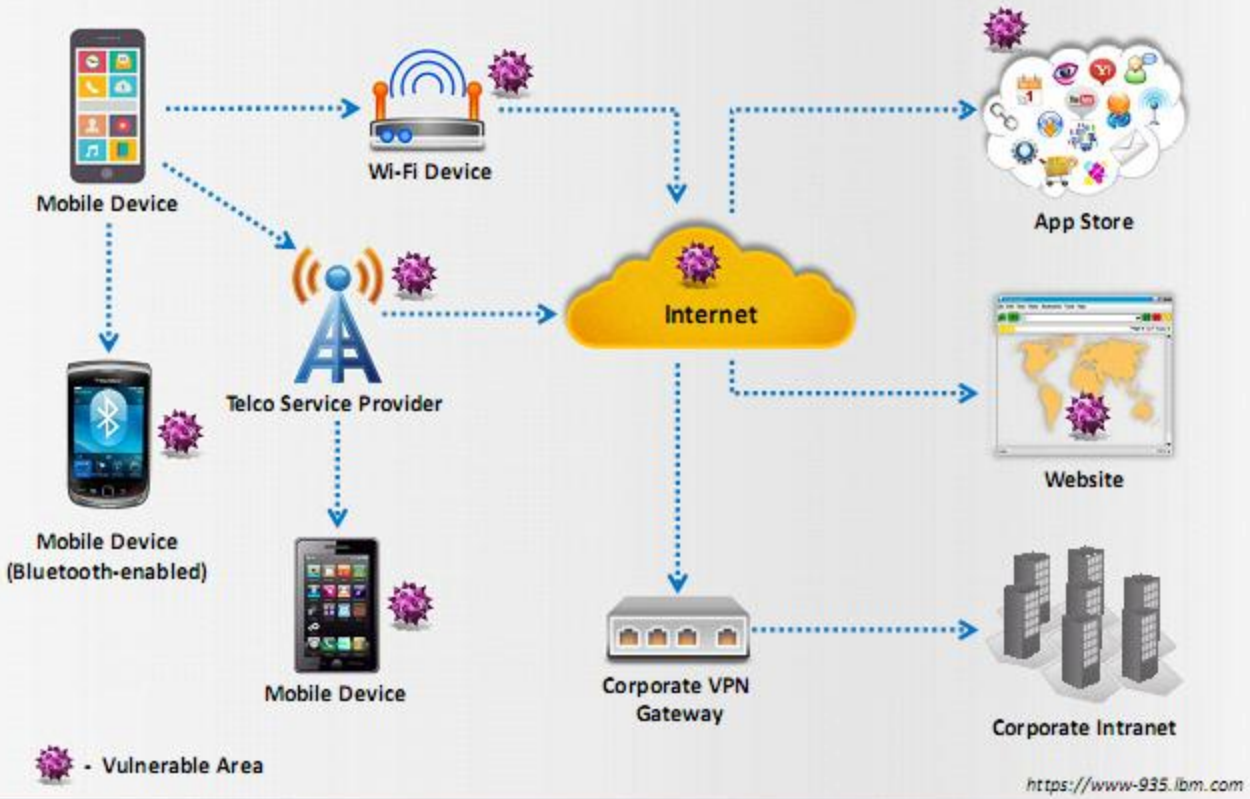
- Understanding Mobile Platform Attack Vectors
- Understanding various Android Threats and Attacks
- Understanding various iOS Threats and Attacks
- Understanding various Mobile Spyware
- Understanding Mobile Device Management (MDM)
- Mobile Security Guidelines and Security Tools
- Overview of Mobile Penetration Testing

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

Vulnerable Areas in Mobile Business Environment

- Smartphones offer **broad Internet** and **network connectivity** via varying channels, such as 3G/4G, Bluetooth, Wi-Fi, or a wired computer connection
- Security threats may arise in different places along these varying paths while **transmitting data**



OWASP Top 10 Mobile Risks - 2016

M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Client Code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

https://www.owasp.org

Anatomy of a Mobile Attack

Point 01 – THE DEVICE

BROWSER

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching

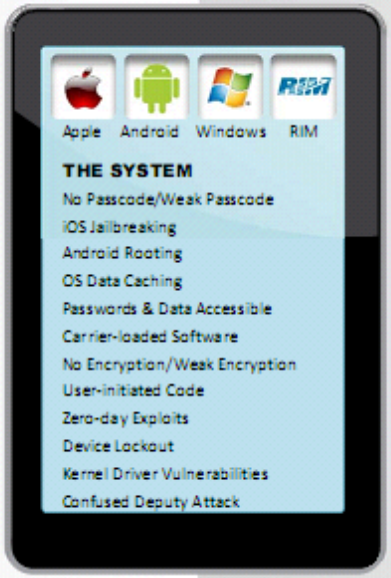
PHONE/SMS

- Baseband Attacks
- SMIShing

APPS

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Validation
- Configuration Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to device and User Info
- Third-party Code
- Intent Hijacking
- Zip Directory Traversal
- Side Channel Attack

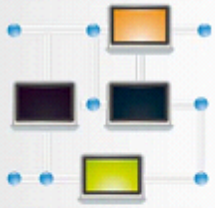
MALWARE



Point 02 – THE NETWORK

THE NETWORK

- Wi-Fi (no encryption/weak encryption
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS Poisoning
- SSLStrip
- Fake SSL Certificate
- BGP Hijacking
- HTTP Proxies



Point 03 – THE DATA CENTER / CLOUD

INTERNET

WEB SERVER

- Platform Vulnerabilities
- Server Misconfiguration
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks
- Cross Origin Resource Sharing
- Side Channel Attack
- Hypervisor Attack

DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

https://www.nowsecure.com

How a Hacker can Profit from Mobile when Successfully Compromised

Surveillance

- Audio
- Camera
- Call logs
- Location
- SMS messages

Financial

- Sending premium rate SMS messages
- Stealing Transaction Authentication Numbers (TANs)
- Extortion via ransomware
- Fake antivirus
- Making expensive calls

Data Theft

- Account details
- Contacts
- Call logs
- Phone number
- Stealing data via app vulnerabilities
- Stealing International Mobile Equipment Identity Number (IMEI)

Botnet Activity

- Launching DDoS attacks
- Click fraud
- Sending premium rate SMS messages

Impersonation

- SMS redirection
- Sending email messages
- Posting to social media

1,598,196
Malicious installation packages

108,073
Mobile ransomware Trojans

19,748
Mobile banking Trojans

https://www.sophos.com

https://securelist.com

Mobile Attack Vectors and Mobile Platform Vulnerabilities

Mobile Attack Vectors

Malware
- Virus and rootkit
- Application modification
- OS modification

Data Exfiltration
- Extracted from data streams and email
- Print screen and screen scraping
- Copy to USB key and loss of backup

Data Tampering
- Modification by another application
- Undetected tamper attempts
- Jail-broken device

Data Loss
- Application vulnerabilities
- Unapproved physical access
- Loss of device

Mobile Platform Vulnerabilities and Risks

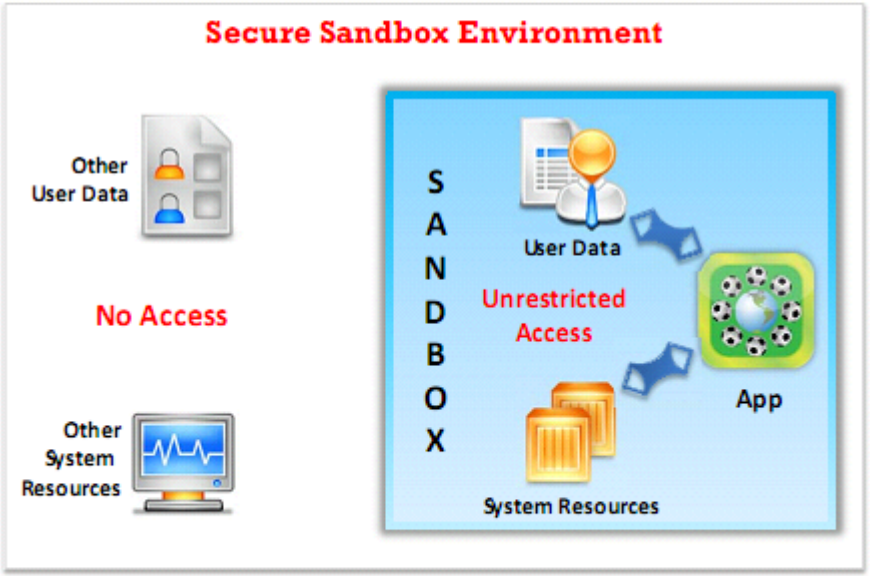
01 Malicious Apps in Stores	07 Mobile Application Vulnerabilities
02 Mobile Malware	08 Privacy Issues (Geolocation)
03 App Sandboxing Vulnerabilities	09 Weak Data Security
04 Weak Device and App Encryption	10 Excessive Permissions
05 OS and App Updates Issues	11 Weak Communication Security
06 Jailbreaking and Rooting	12 Physical Attacks

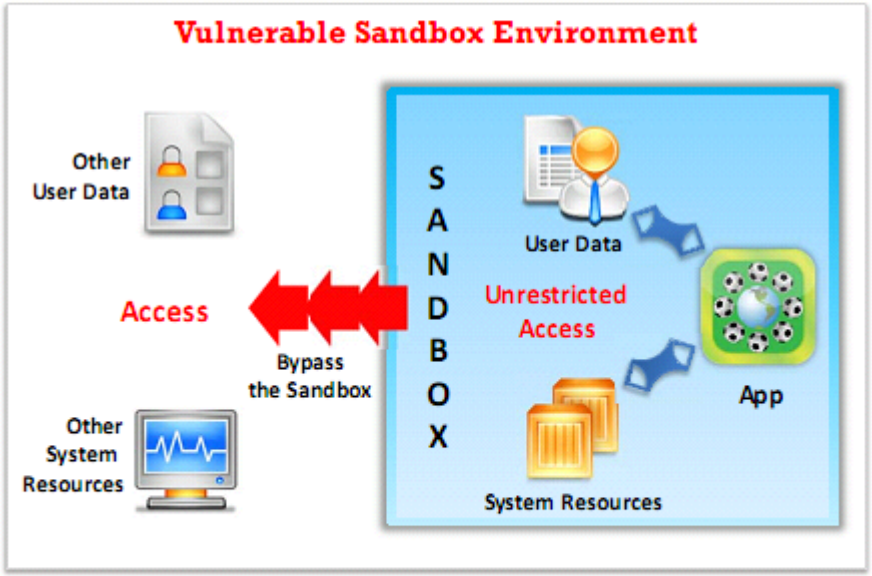
Security Issues Arising from App Stores

1. Insufficient or **no vetting of apps** leads to malicious and fake apps entering app marketplace
2. App stores are common target for attackers to **distribute malware and malicious apps**
3. Attackers can also **social engineer users** to download and run apps outside the official app stores
4. Malicious apps can **damage other applications** and data, and send your sensitive data to attackers

App Sandboxing Issues

- Sandboxing helps **protect systems and users** by limiting the resources the app can access to the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox





Mobile Spam

Unsolicited text/email messages sent to mobile devices from known/ unknown phone number/email IDs

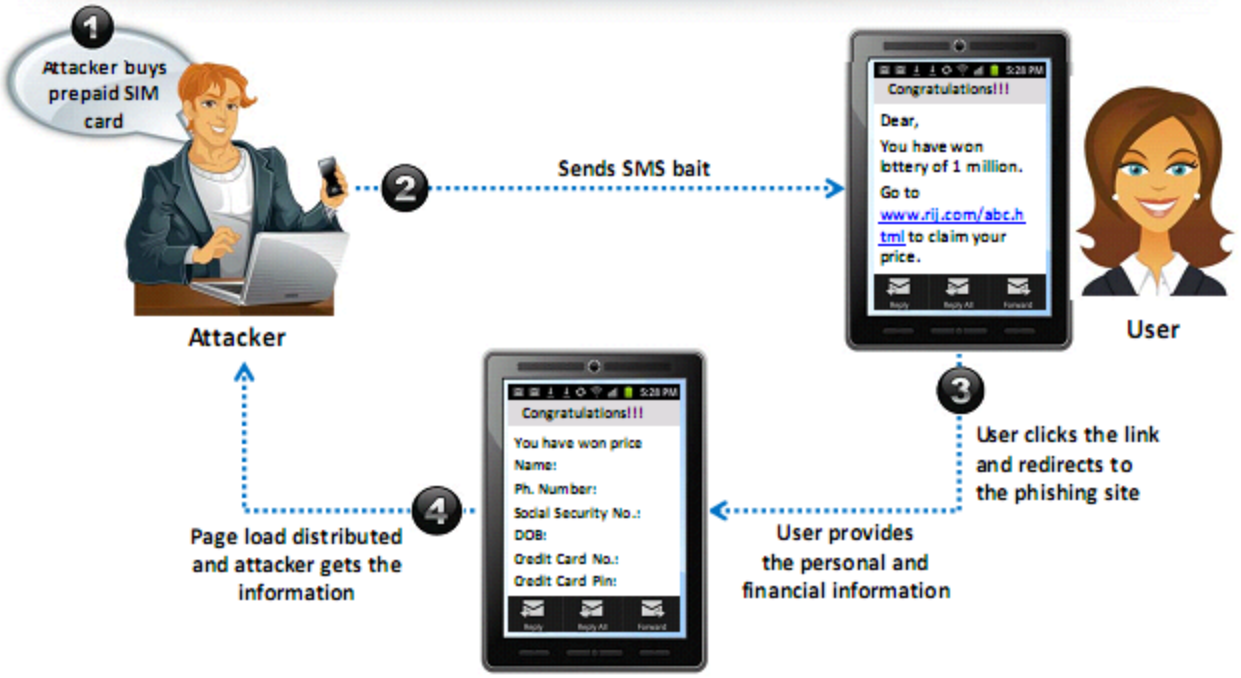
Spam messages contain advertisements or malicious links that can trick users to reveal confidential information

Significant amount of bandwidth is wasted by Spam messages

Spam attacks are done for financial gain

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

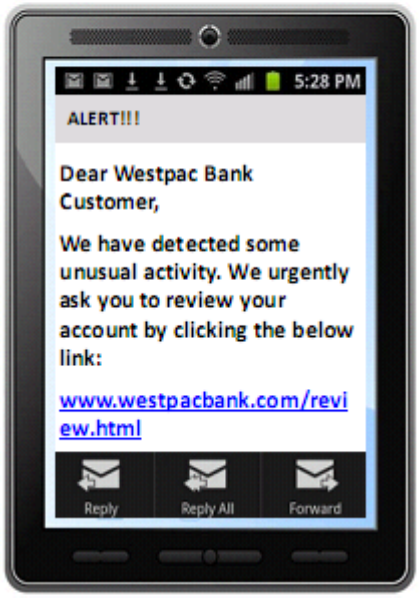
- SMS Phishing is the act of trying to **acquire personal and financial information by sending SMS** (Instant Message or IM) containing deceptive link

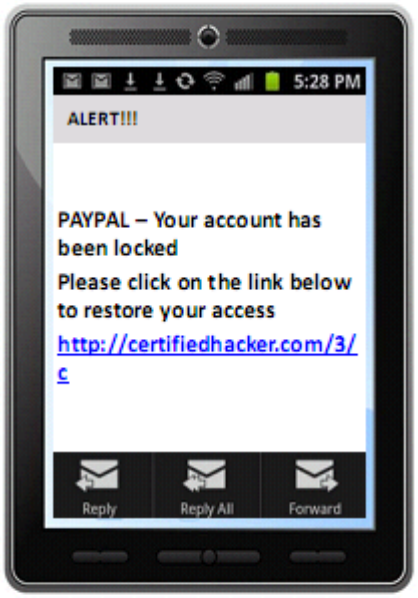


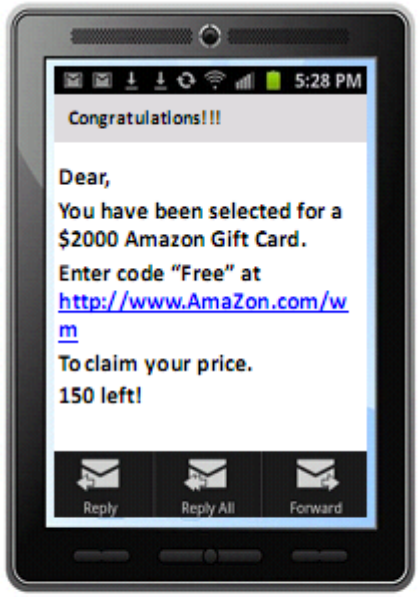
Why SMS Phishing is Effective?

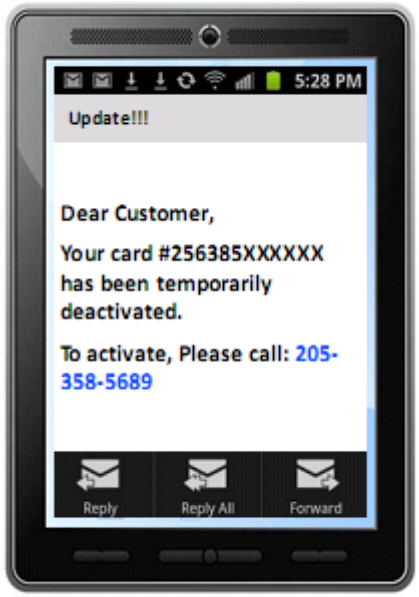
- Most of the consumers **access the Internet** through a mobile
- **Easy to set up** a mobile phishing campaign
- Difficult to **detect and stop** before they cause harm
- Mobile users are **not conditioned** to receiving spam text messages on their mobile
- No **mainstream mechanism** for weeding out spam SMS
- Most of the mobile **anti-virus** does not check the SMS

SMS Phishing Attack Examples



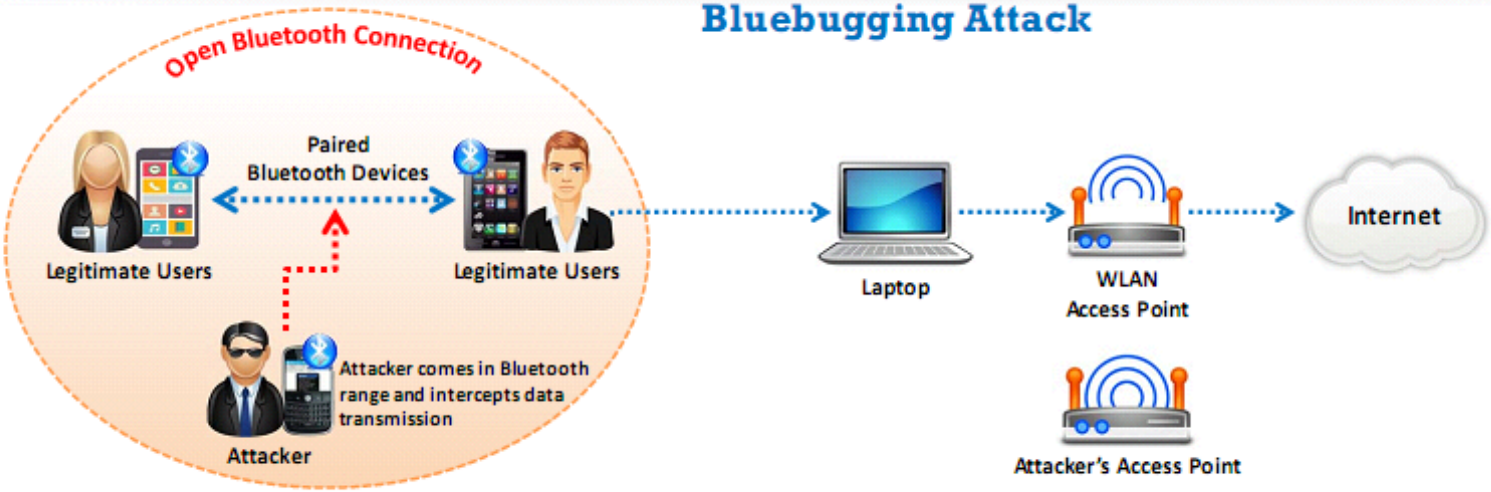






Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- Mobile **device pairing on open connections** (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to **eavesdrop** and **intercept data transmission** using techniques such as;
  - Bluesnarfing (Stealing the information via Bluetooth)
  - Bluebugging (Gaining control over the device via Bluetooth)
- Sharing **data from malicious devices** can infect/breach data on the recipient device



Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

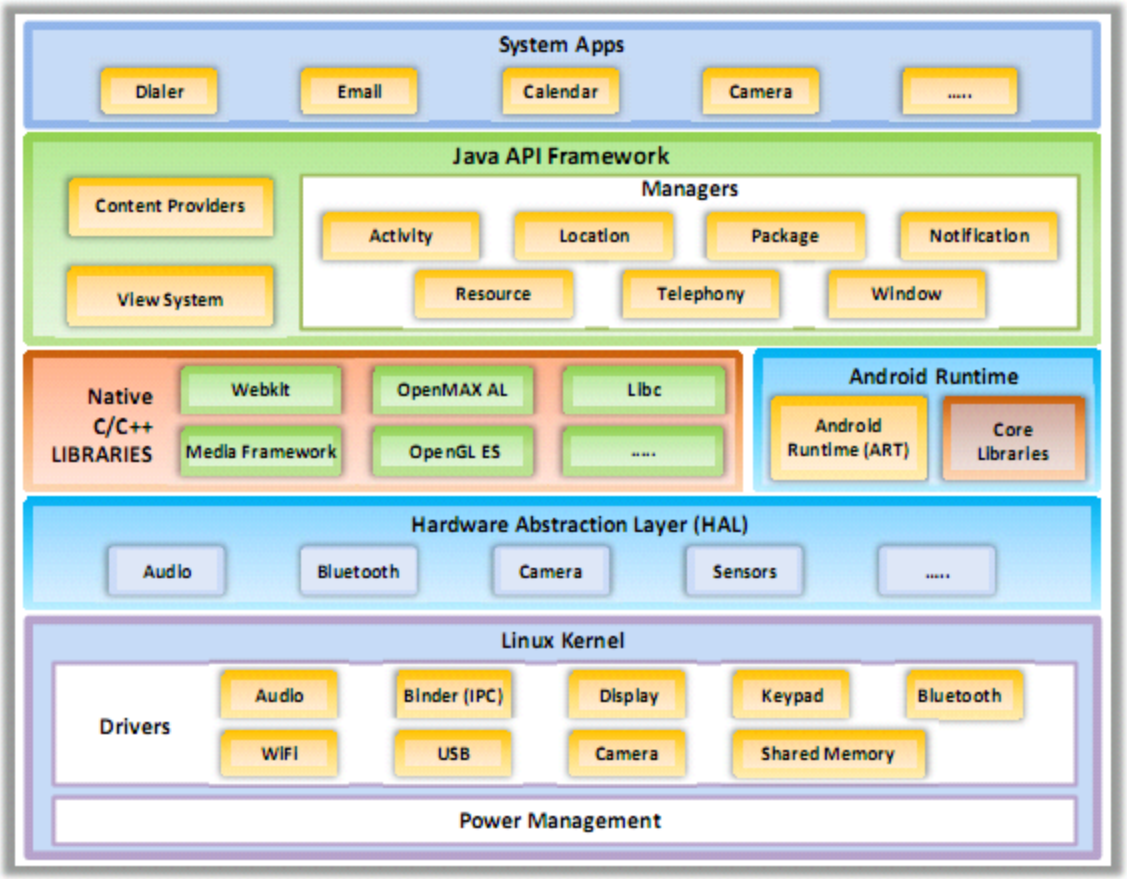
Android OS

- Android is software environment developed by **Google for mobile devices** that includes an operating system, middleware, and key applications

Features

- Application framework **enabling reuse** and **replacement** of components
- Provides a variety of **pre-build** UI components
- Integrated browser based on the **open source Blink and WebKit engine**
- **Media support** for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- **Rich development environment** including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the **Eclipse IDE**

https://developer.android.com

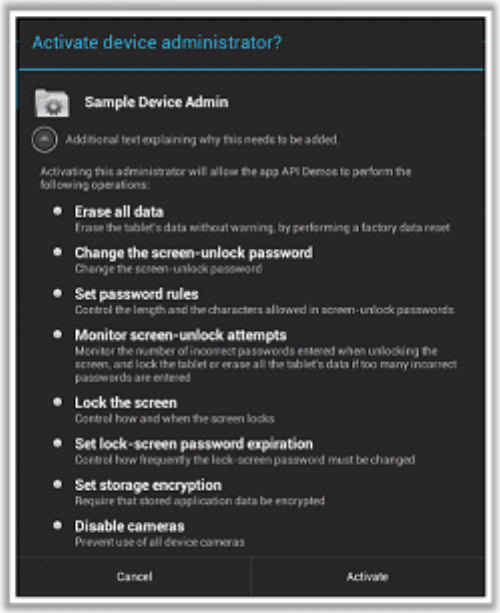


Android Device Administration API

- The Device Administration API introduced in Android 2.2 provides **device administration features** at the system level
- These APIs allow developers to create **security-aware applications** that are useful in enterprise settings, in which IT professionals require rich control over employee devices

Policies Supported by the Device Administration API

- Password enabled
- Minimum password length
- Alphanumeric password required
- Complex password required
- Minimum letters required in password
- Minimum lowercase letters required in password
- Minimum non-letter characters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password
- Minimum uppercase letters required in password
- Password expiration timeout
- Password history restriction
- Maximum failed password attempts
- Maximum inactivity time lock
- Require storage encryption
- Disable camera
- Prompt user to set a new password
- Lock device immediately
- Wipe the device's data



https://developer.android.com

Android Rooting

- Rooting allows Android users to **attain privileged control** (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities 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 the user-installed applications to **run privileged commands** such as:

- Modifying or **deleting system files**, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer- installed applications (**bloatware**)
- Low-level access to the hardware that are typically unavailable to the devices in their **default configuration**
- **Wi-Fi** and **Bluetooth** tethering
- Install applications on **SD card**

Rooting also comes with many **security** and other **risks** to your device including:

- Voids your phone's **warranty**
- Poor **performance**
- **Malware** infection
- **Bricking** the device

Rooting Android Using KingoRoot

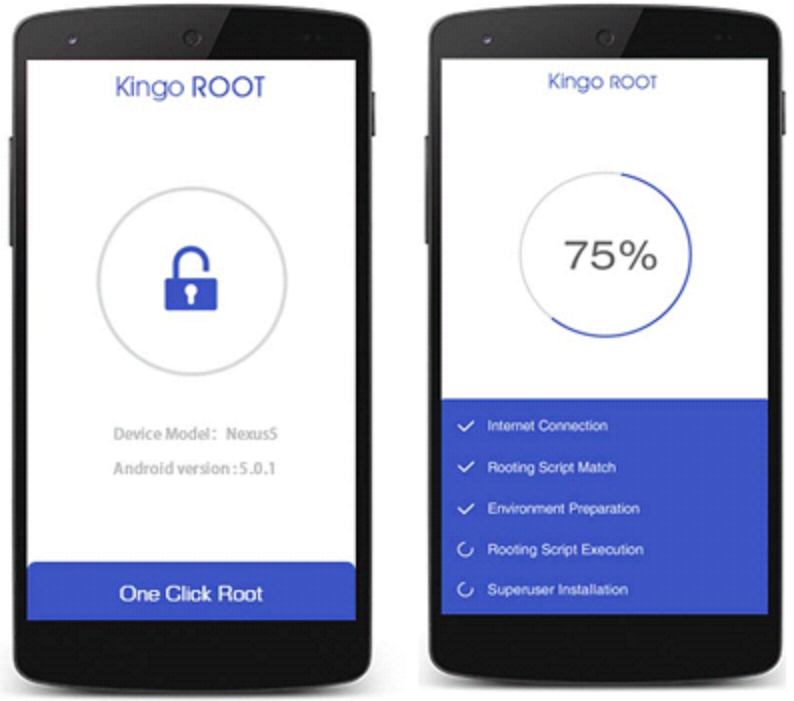
KingoRoot

Android Rooting With PC

- Download KingoRoot Android (PC Version) and install it on your desktop
- Run the tool and connect the device to the computer with USB cable
- Enable the USB debugging mode on android device
- Now the tool will install the latest drivers on your PC
- You will see a new screen on your desktop with your device name and "ROOT" button
- Click on ROOT to root your device

Android Rooting Without PC

- Enable installation from unknown sources in android device
- Download KingoRoot.apk on your Android from play store
- Install and launch KingoRoot
- Press "One Click Root" on the main interface of the app
- Wait for few seconds until root result appears on the display
- Attempt multiple times in case of failed rooting or you can try PC version

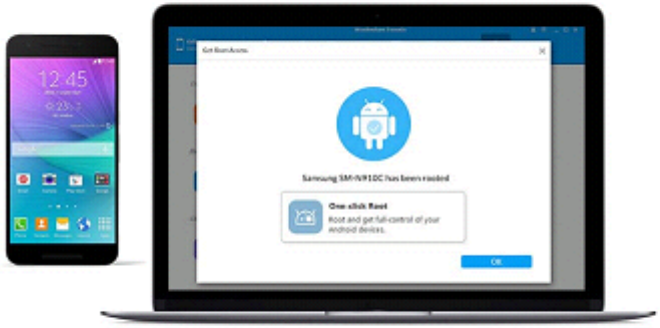


https://www.kingoapp.com

Android Rooting Tools

TunesGo

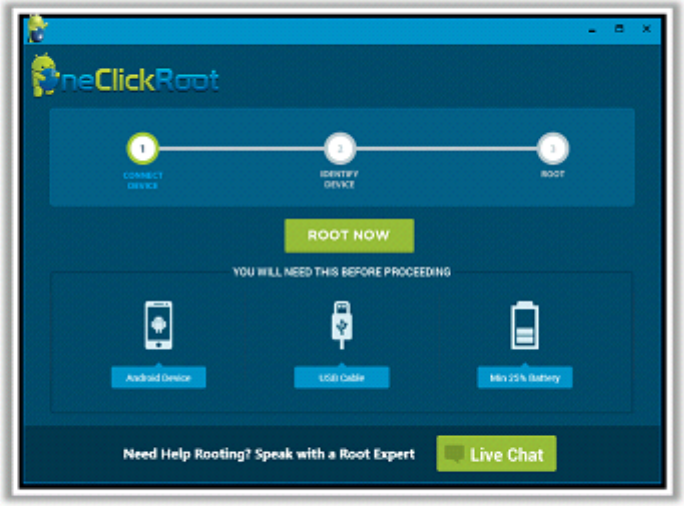
TunesGo - Root Android tool has an advanced android root module that recognize and analyze your Android device and choose the appropriate Android-root-plan for it automatically



https://tunesgo.wondershare.com

One Click Root

One Click Root is an android rooting tool that offers features like gaining access to more apps, Install apps on SD card, preserve battery life, Wi-Fi and Bluetooth tethering, etc.



https://www.oneclickroot.com

- **Unrevoked**
  http://www.unrevoked.com
- **MTK Droid**
  https://androidmtk.com
- **Superboot**
  http://www.galaxynexusforum.com
- **Superuser X [Root]**
  http://www.ksharkapps.com
- **Root Uninstaller**
  https://play.google.com

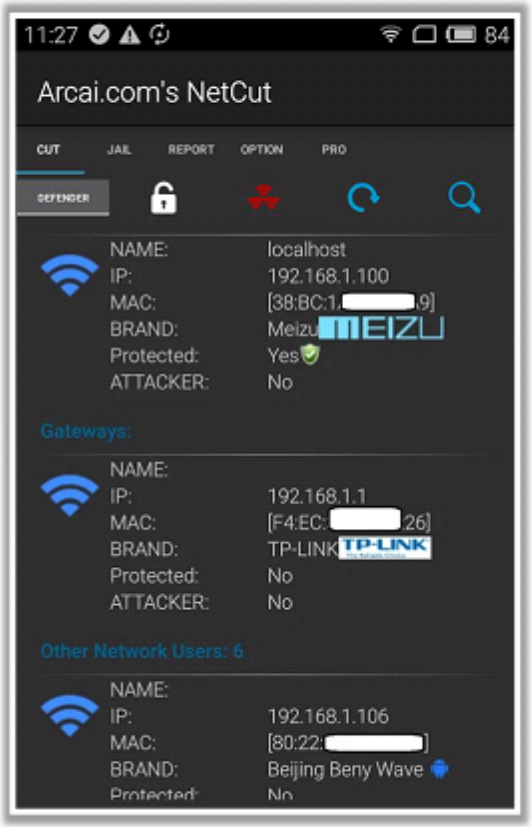
Blocking Wi-Fi Access using NetCut

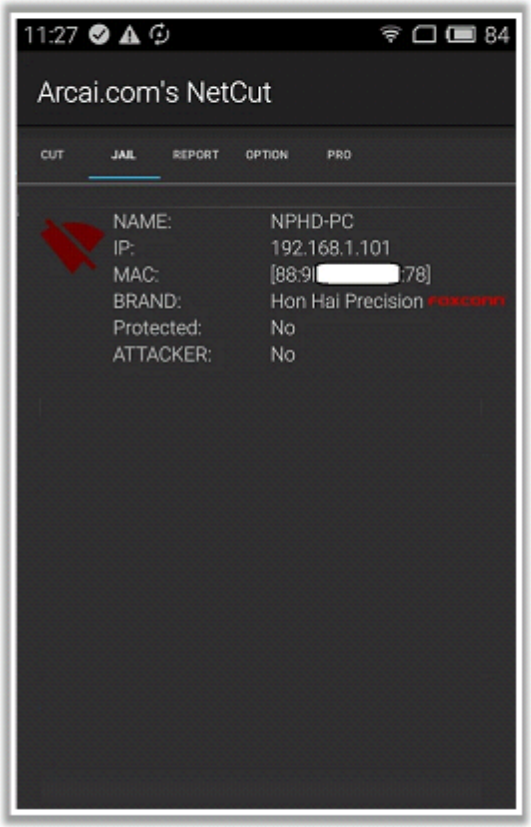
NetCut is a Wi-Fi killing application that allows the attackers to identify the target devices and block the access of Wi-Fi to the victim devices in a network

Steps to Block Wi-Fi Access

- **Step 1:** Download and install NetCut android application on your device
- **Step 2:** Launch the NetCut app in the mobile
- **Step 3:** After opening, it automatically scans for all the devices accessing the Wi-Fi network and displays the list under CUT tab on the interface
- **Step 4:** Identify the target device and tap on it to block the Wi-Fi access to the device. The Wi-Fi propagation symbol on the left of the blocked device name turns red from blue. You can confirm this by navigating to the JAIL tab on the interface, where the list of blocked devices will be displayed

Note: This tool works only on rooted devices



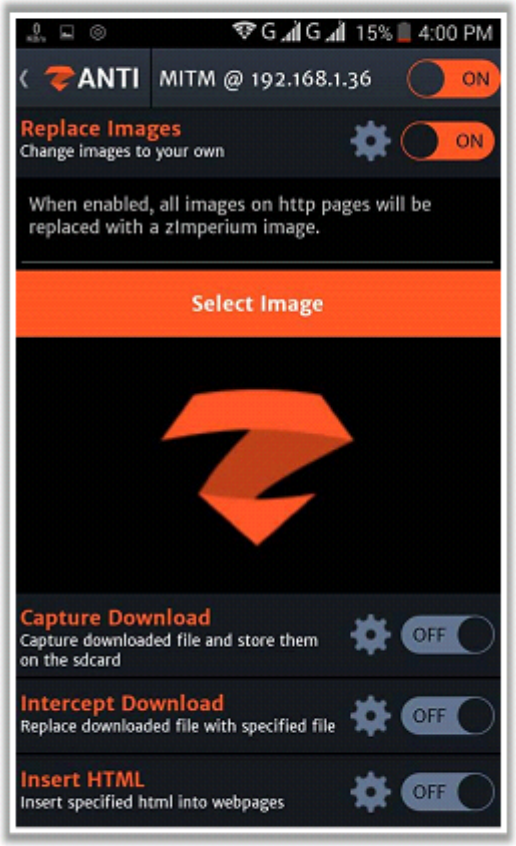


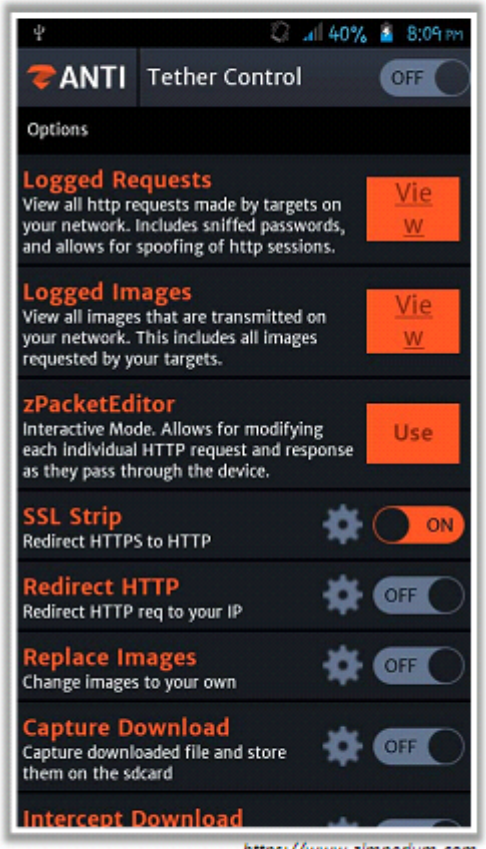
http://www.arcai.com

Hacking with zANTI

zANTI is an android application which allows you to perform following attacks:

- Spoof MAC Address
- Create malicious Wi-Fi hotspot
- Scan for open ports
- Exploit router vulnerabilities
- Password complexity audits
- Man-in-Middle attack
- DoS Attack





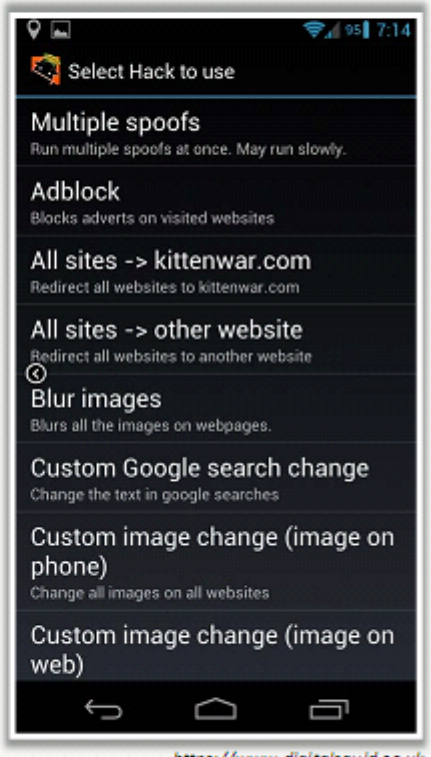
https://www.zimperium.com

Hacking Networks Using Network Spoofer

- Network Spoofer lets you **change websites** on other people's computers from an Android phone

Features:

- Flip pictures upside down
- Flip text upside down
- Make websites experience gravity
- Redirect websites to other pages
- Delete random words from websites
- Replace words on websites with others
- Change all pictures to Trollface
- Wobble all pictures / graphics around a bit



https://www.digitalsquid.co.uk

Launching DoS Attack using Low Orbit Ion Cannon (LOIC)

Low Orbit Ion Cannon (LOIC) is a mobile application that allows the attackers to perform DoS/DDoS attacks on the target IP address. This application can perform UPD, HTTP or TCP flood attacks

Steps to Launch DoS Attack

Step 1: **Download and install** LOIC android application from Android Play Store

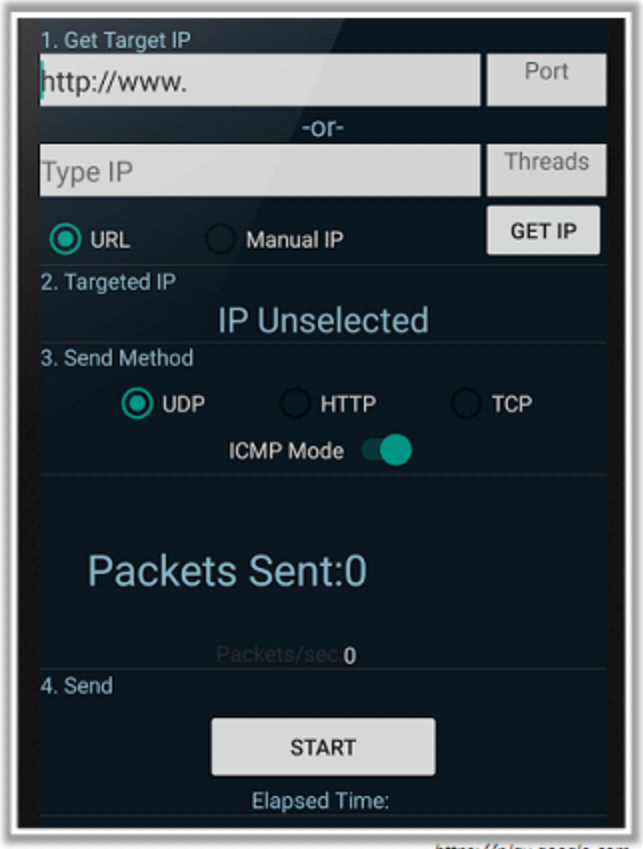
Step 2: **Launch** the **LOIC** application

Step 3: Enter the target IP address or the URL in **GET Target IP** field and click **GET IP** button

Step 4: Select the DoS attack method by selecting any of **UDP**, **HTTP**, **TCP** radio buttons under **Send Method** option

Step 5: Enter the port and number of threads. Numbers must be a positive whole number

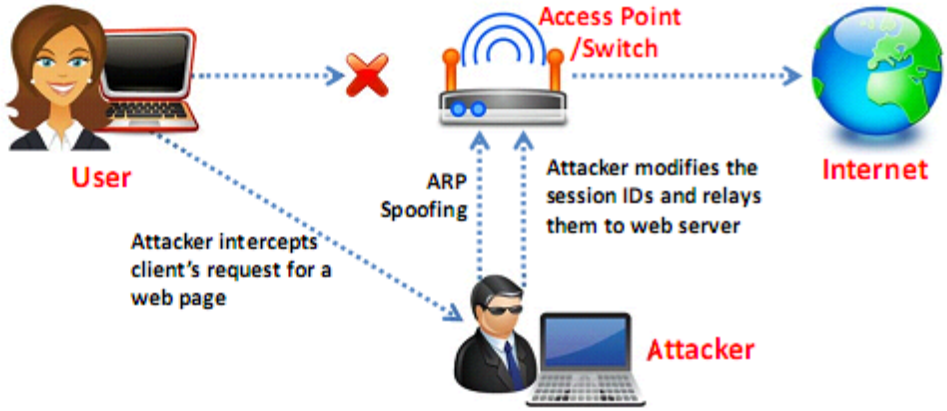
Step 6: Click on **START** button at the bottom of the interface to **launch the DoS attack**

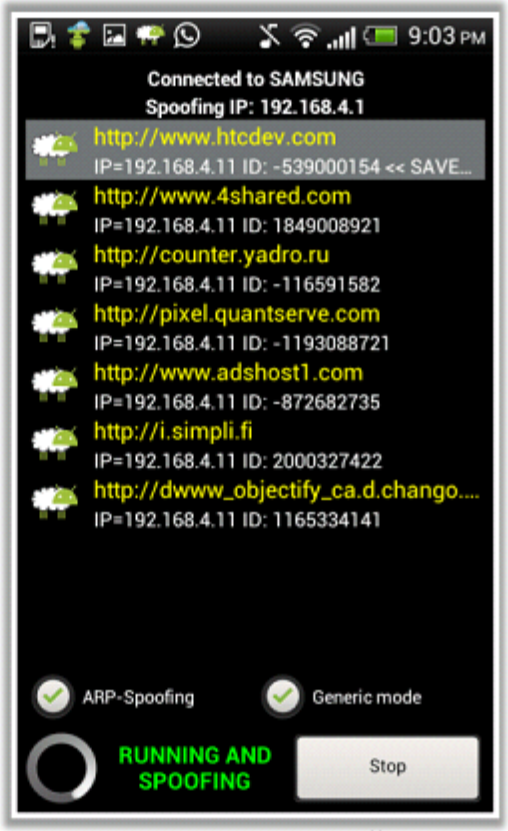


https://play.google.com

Performing Session Hijacking Using DroidSheep

- DroidSheep is a simple Android tool for web session hijacking (sidejacking)
- It listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets in order to reuse them
- DroidSheep can capture sessions using the libpcap library and supports: OPEN Networks, WEP encrypted networks, WPA and WPA2 (PSK only) encrypted networks

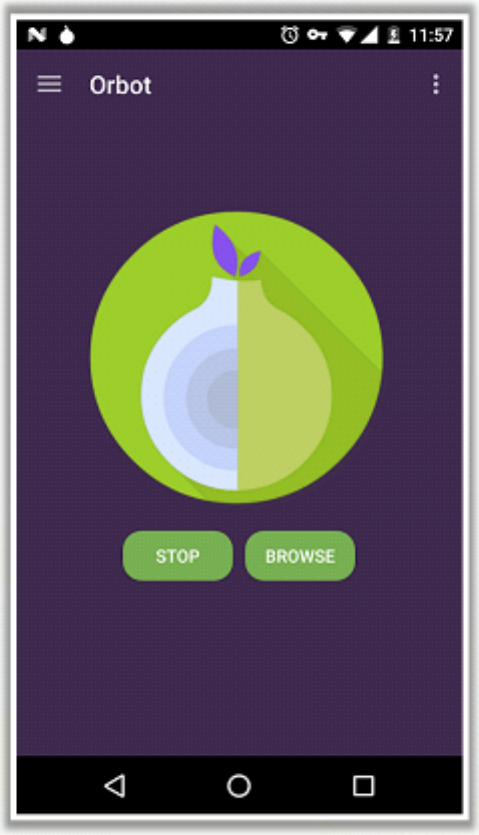


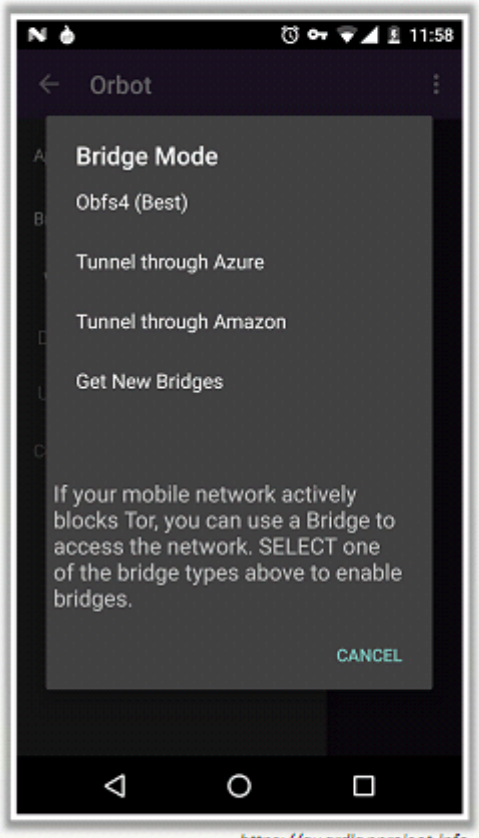


http://droidsheep.org

Hacking with Orbot Proxy

- Orbot is a proxy app that empowers other apps to use the **internet more privately**
- It uses Tor to **encrypt your Internet traffic** and then hides it by bouncing through a series of computers around the world
- Attackers can use this application to **hide their identity** while performing attacks or surfing through the **target web applications**



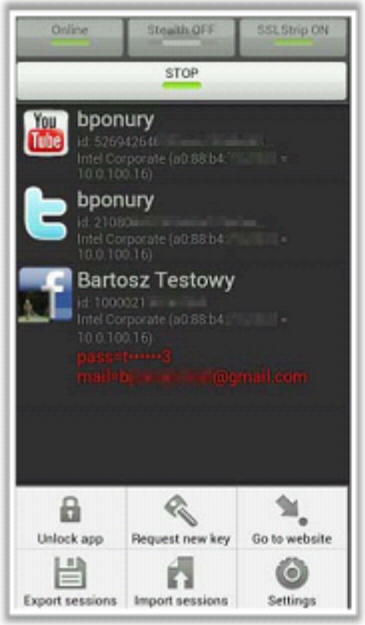


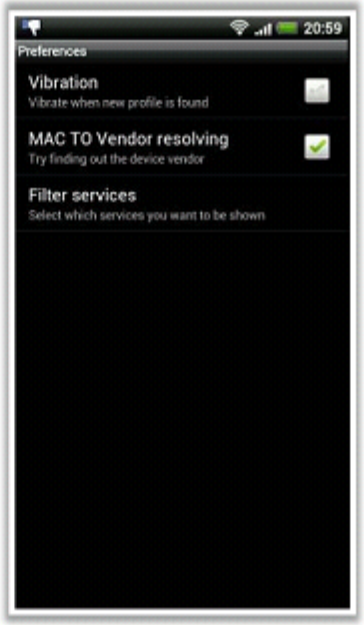
https://guardianproject.info

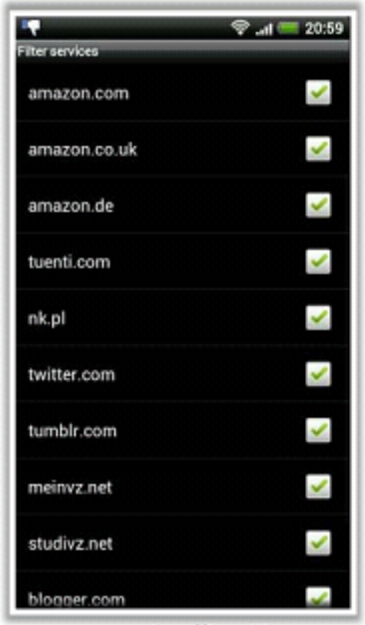
Android-based Sniffers

FaceNiff

- FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi that your mobile is connected to
- It is possible to hijack sessions only when Wi-Fi is not using EAP, but it should work over any private networks (Open/WEP/WPA-PSK/WPA2-PSK)







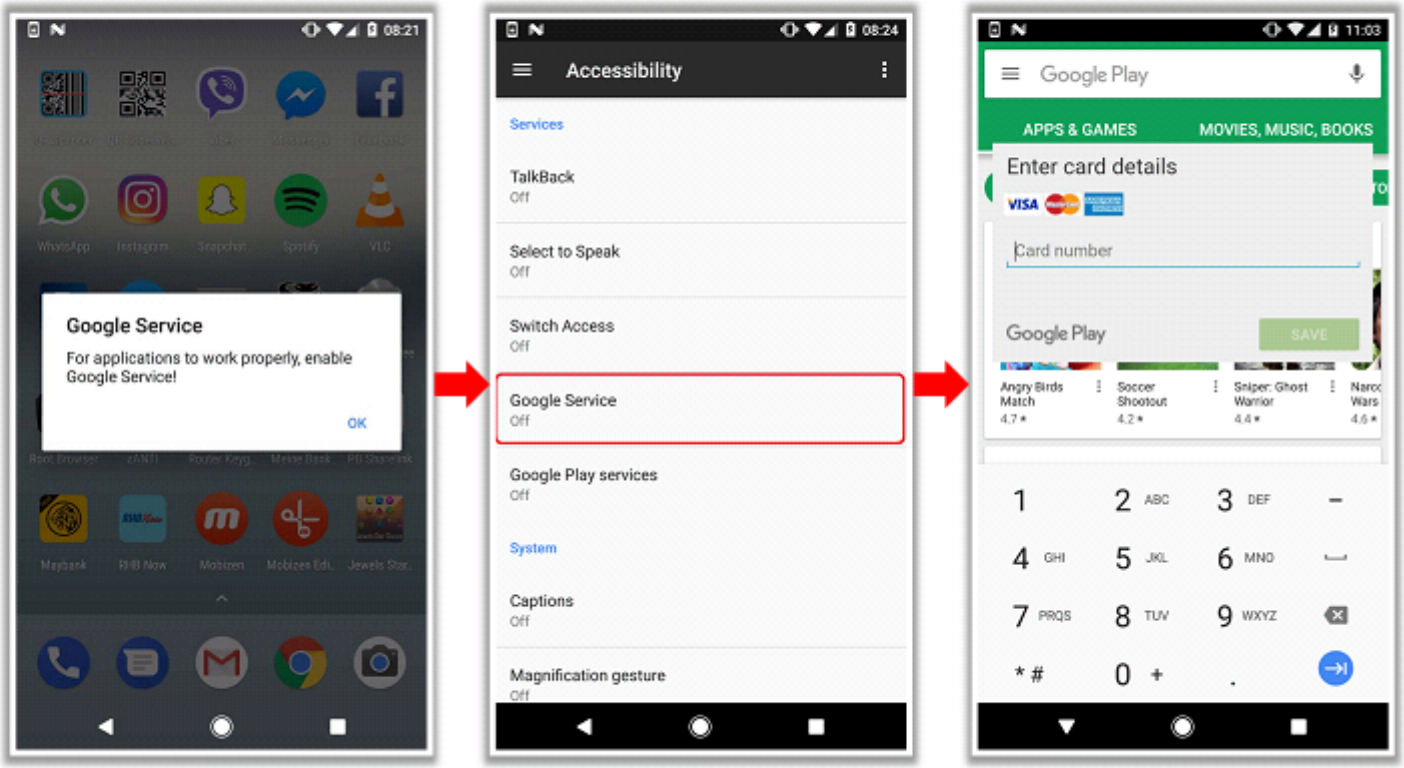
http://faceniff.ponury.net

- **Packet Sniffer** — *https://play.google.com*
- **tPacketCapture** — *http://www.taosoftware.co.jp*
- **Android PCAP** — *https://www.kismetwireless.net*
- **Wicap. Sniffer Demo [ROOT]** — *https://play.google.com*
- **Testeldroid** — *https://play.google.com*

Android Trojans

BankBot (Android/Spy.Banker.LA)

- **BankBot** is a banking Trojan that is comprised of sophisticated techniques in code obfuscation, payload dropping and infection mechanism affecting android accessibility service
- This Trojan spreads by Jewels Star Classic android game application and after installing the app, the user will be tricked to enable malicious service and enter the credit card details



Android Trojans (Cont'd)

SpyDealer

- SpyDealer is a spying Trojan that ex-filtrates the private and sensitive data from 40 android applications including WeChat, Facebook, WhatsApp, Skype, Line, Viber, QQ, Tango, Telegram, Sina Weibo, Tencent Weibo, etc.
- It employees exploits from a commercial rooting app "Baidu Easy Root" to gain root privilege
- It abuses the Android Accessibility Service feature
- It extracts information like phone number, IMEI, IMSI, SMS, MMS, contacts, accounts, phone call history, location, and connected Wi-Fi information, etc.

```
String pkgName = this.m_service.m_cont.getPackageName();
String cmd = "settings put secure enabled_accessibility_services " + (String.valueOf(pkgName) + "/"
        + pkgName + ".MobileService") + "\n" + "settings put secure accessibility_enabled 1";
while(Build$VERSION.SDK_INT >= 18) {
    if(!this.isAccessibilitySettingsOn(this.m_service.m_cont) && ((this.CheckAccessibility(this
            .m_service.m_wifi)) || (this.CheckAccessibility(this.m_service.m_3g))) && (this.
            m_service.CheckSu())) {
        this.m_service.RootCmd(cmd);
    }
```

- Android/Trojan.AsiaHitGroup
- GhostCtrl malware
- Triada
- AndroRAT
- ZitMo (ZeuS-in-the-Mobile)

Securing Android Devices

- Enable screen locks for your Android phone for it to be more secure
- Never root your Android device
- Download apps only from official Android market
- Keep your device updated with Google Android antivirus software

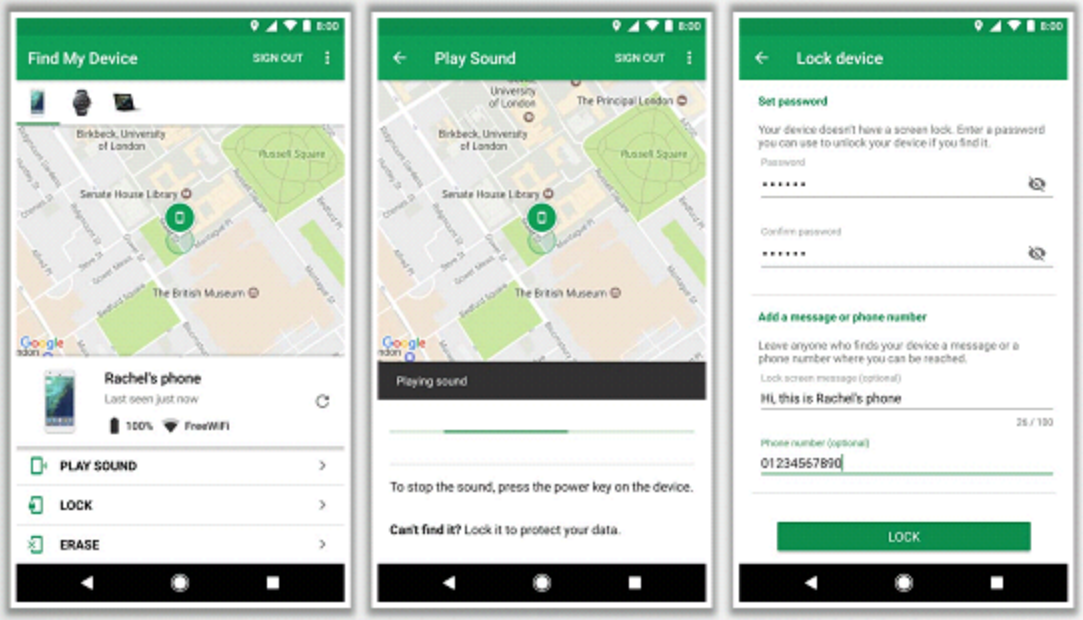
- Do not directly download Android package files (APK)
- Update the operating system regularly
- Use free protector Android app like Android Protector where you can assign passwords to text messages, mail accounts, etc.
- Customize your locked home screen with the user's information

Android Security Tool: Find My Device

- Find My Device helps you easily **locate a lost Android device**, and keeps your information safe and sound while you look

To find, lock or erase a lost or stolen device:

- Go to https://www.google.com/android/find and sign in to your Google Account
- If you have more than one device, click the **lost device** at the top of the screen
- The device gets a **notification**
- On the map, see about where the device is
- Pick what you want to do. If needed, first click **Enable lock & erase**
  - **Play sound:** Rings your device at full volume for 5 minutes
  - **Lock:** Locks your device with your PIN, pattern, or password
  - **Erase:** Permanently deletes all data on your device



https://www.google.com

Android Security Tools

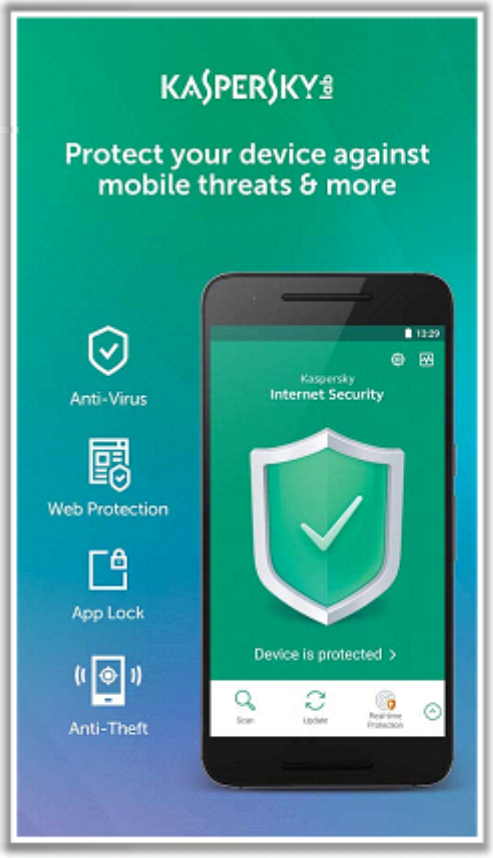
Kaspersky Mobile Antivirus: AppLock & Web Security

- Kaspersky mobile antivirus is a android security software focusing on anti-theft and virus protection for mobile and tablet devices

Features

- Antivirus protection
- Background check
- App Lock
- Find my phone
- Anti-Theft
- Anti-Phishing
- Call blocker
- Web filter
- Android 8 Support
- Antivirus Database Expansion

https://my.kaspersky.com



Avira Antivirus Security
https://www.avira.com

Avast Antivirus & Security
https://www.avast.com

McAfee Mobile Security & Lock
https://www.mcafeemobilesecurity.com

Lookout Security & Antivirus
https://www.mylookout.com

Sophos Mobile Security
https://www.sophos.com

Android Vulnerability Scanner

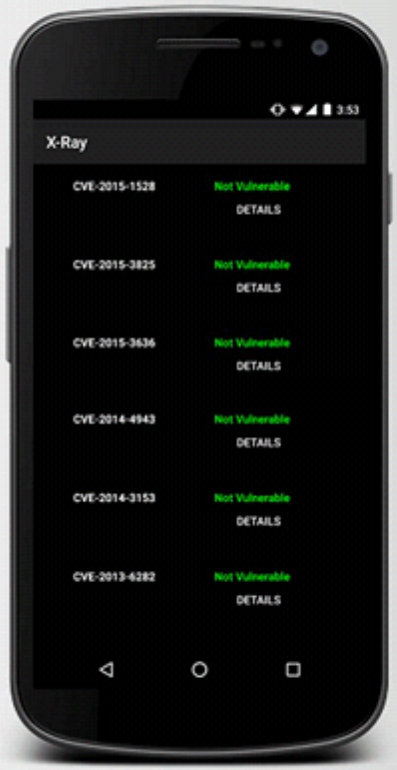
X-Ray

X-Ray scans your Android device to determine whether there are **vulnerabilities** that **remain unpatched** by your carrier

It presents you with a **list of vulnerabilities** that it is able to identify and allows you to check for the presence of each vulnerability on your device

X-Ray is **automatically updated** with the ability to scan for new vulnerabilities as they are discovered and disclosed

https://labs.duo.com



Threat Scan
http://free.kaspersky.com

Norton Halt exploit defender
https://community.norton.com

Shellshock Scanner – Zimperium
https://www.zimperium.com

Hackode
http://www.ravikumarpurbey.com

BlueBorne Vulnerability Scanner by Armis
https://www.armis.com

Android Device Tracking Tools

Find My Phone

http://findmyphone.mangobird.com

Where's My Droid

http://wheresmydroid.com

Prey Anti Theft: Find My Android & Mobile Security
https://preyproject.com

iHound
http://ihoundgps.com

Mobile Tracker for Android
https://play.google.com

Tech Expert
https://protection.sprint.com

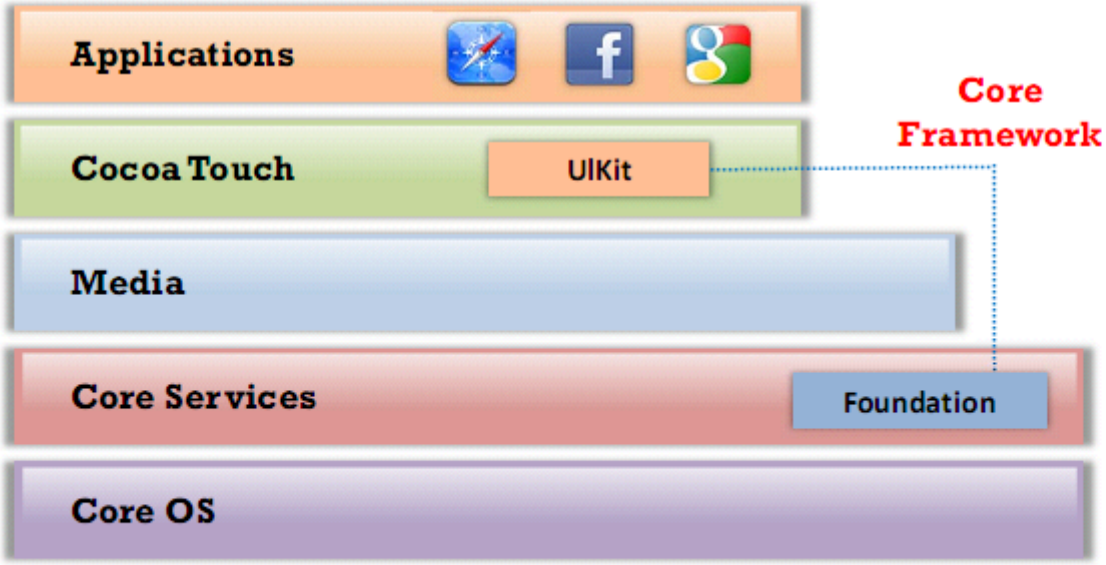
GadgetTrak Mobile Security
http://www.gadgettrak.com

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

Apple iOS

- iOS is **Apple's mobile operating system**, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV
- The user interface is based on the concept of **direct manipulation**, using **multi-touch** gestures



Jailbreaking iOS

- Jailbreaking is defined as the process of **installing a modified set of kernel patches** that allows users to run third-party applications not signed by the OS vendor
- Jailbreaking provides **root access to the operating system** and permits downloading of third-party applications, themes, extensions on iOS devices
- Jailbreaking **removes sandbox restrictions**, which enables malicious apps to access restricted mobile resources and information

Jailbreaking, like rooting, also comes with many security and other risks to your device including

1. Voids your phone's warranty
2. Poor performance
3. Malware infection
4. Bricking the device

Types of Jailbreaking

Userland Exploit

A userland jailbreak **allows user-level access** but does not allow iboot-level access

iBoot Exploit

An iboot jailbreak allows **user-level access** and **iboot-level access**

Bootrom Exploit

A bootrom jailbreak allows **user-level access** and **iboot-level access**

Jailbreaking Techniques

Untethered Jailbreaking

- An untethered jailbreak has the property that if the user turns the device off and back on, the device will start up completely, and the **kernel will be patched** without the help of a computer – in other words, it will be jailbroken after each reboot

Semi-tethered Jailbreaking

- A semi-tethered has the property that if the user turns the device off and back on, the device will start up completely, it will **no longer have a patched kernel**, but it will still be **usable for normal functions**. To use jailbroken addons, the user need to start the device with the help of the **jailbreaking tool**

Tethered Jailbreaking

- With a tethered jailbreak, if the device starts back up on its own, it will **no longer have a patched kernel**, and it may get stuck in a partially started state; in order for it to start completely and with a patched kernel, it essentially must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on

Jailbreaking iOS 11.2.1 Using Cydia

- Cydia is a software application for iOS that **enables a user to find and install software packages** (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad

Steps to Jailbreak iOS 11.2.1 using Cydia

01 On your iPhone or iPad, open the **Safari browser**

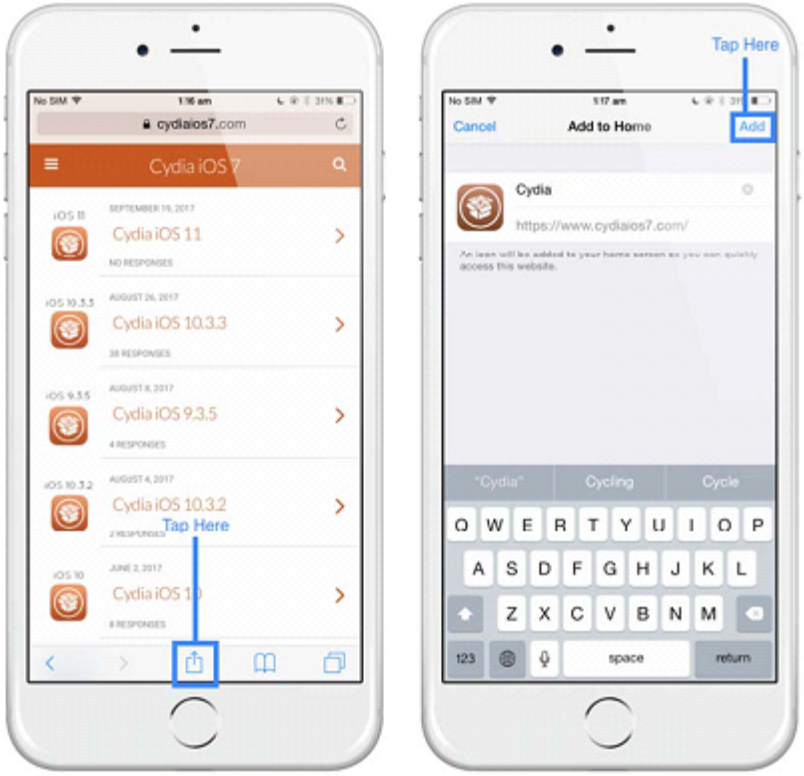
02 From the address bar, go to **cydiaios7.com**

03 Locate the **UP arrow** on the web page, top right on the iPad and bottom center on the iPhone screen, and tap on it

04 When the new page loads, tap **Add to Home Screen**

05 Now type **Cydia** into the box for naming the app icon. Tap the **Add** button and close Safari browser

06 Look on your home screen for the **Cydia** icon



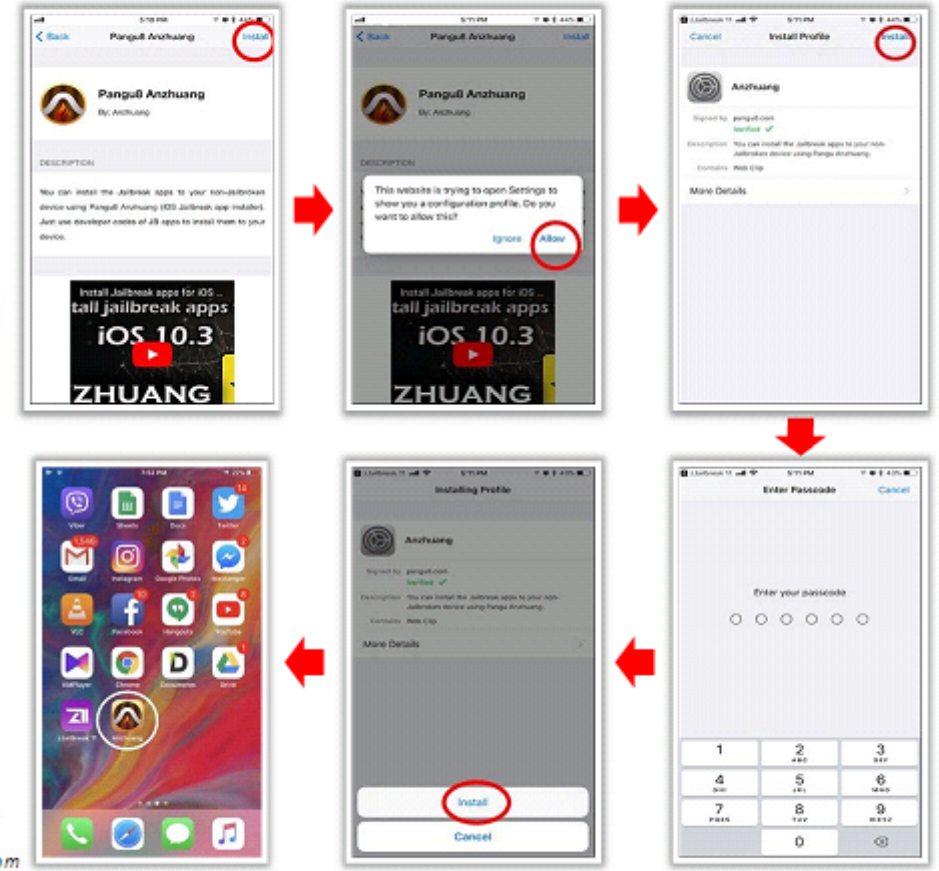
https://www.cydiaios7.com

Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang

- Pangu Anzhuang is a simple application which allows you to **install jailbreak apps** for iOS 11.2.1 - iOS 10.2 versions
- Pangu Anzhuang is **online jailbreak app** installer for latest iOS versions

Steps to Install Pangu Anzhuang

1. Download **zJailbreak** app
2. Open the **zJailbreak** app. Go to **Pangu8 Anzhuang** app available under jailbreak clicking on it
3. Click on **"Install"** and then Click **"Allow"** to popup message
4. Again Click on **"Install"** from the popup screen and Enter your regular **passcode**
5. Now Tap on **"Install"** → **"Done"**. It will begin to install Anzhuang app to your device
6. Once you complete the Installation process, Anzhuang icon will be appeared on your **home screen**

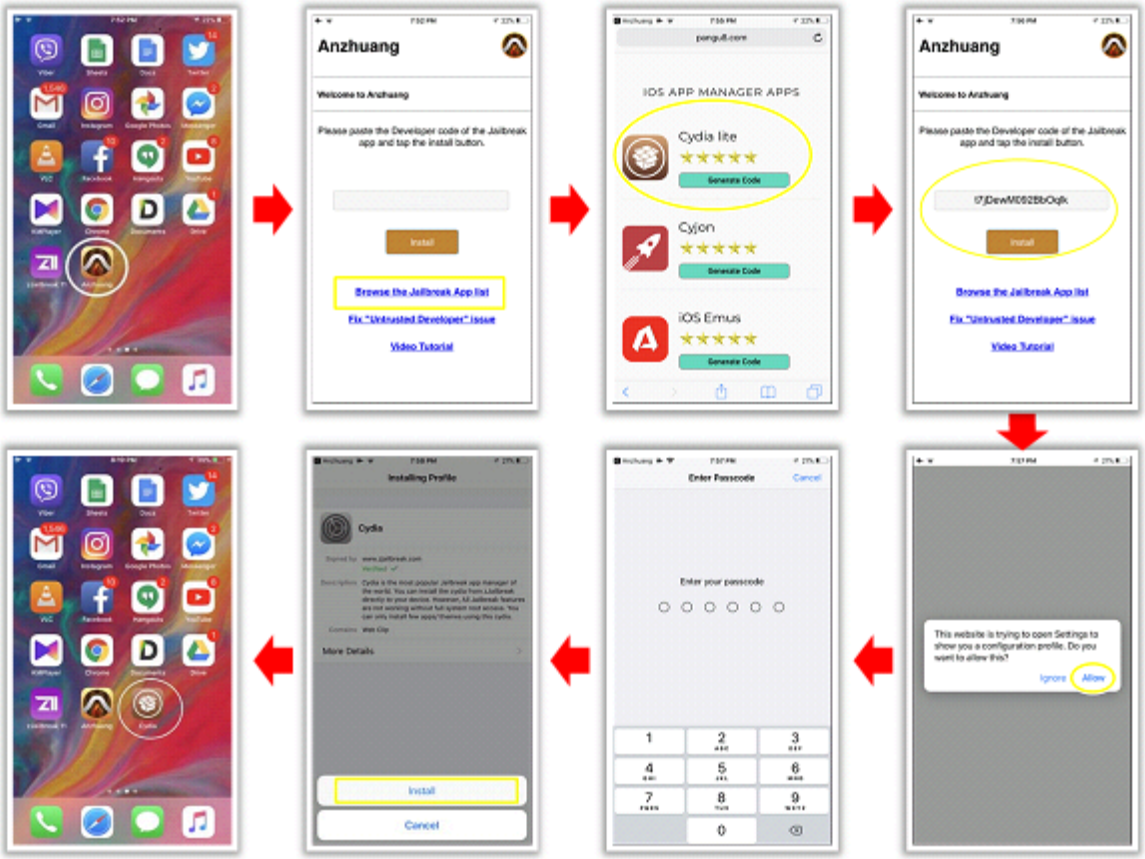


http://pangu8.com

Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang (Cont'd)

Steps to Install Cydia Jailbreak Apps

1. Open the Pangu8 Anzhuang app. Tap on "Browse the Jailbreak App list" to copy the app code
2. Click on the "App managers" Then you need to click on "Generate Code" in Cydia lite icon
3. Go back to Anzhuang App and Paste the Code and Tap on "Install"
4. Click "Allow" to popup message and tap on "Install"
5. It will ask your passcode. Enter it and then tap on "Install" → "Done"
6. Finally you can see the jailbreak app icon on your home screen



Jailbreaking Tools

Keen Jailbreak

- Keen Jailbreak is an **unofficial Semi-tethered tool** that was released for iOS 11 beta versions
- It is compatible to jailbreak following devices:
  - Phone 7 & 7 Plus, iPhone 6S & 6S Plus, iPhone 6 & 6 Plus
  - iPhone SE / iPhone 5s, iPod Touch 6G
  - iPad Mini 2 / iPad Mini 3 / iPad Mini 4
  - iPad Air /iPad Air 2 /iPad Pro

http://pangu8.com

- **Yalu** — http://pangu8.com
- **Velonzy** — http://pangu8.com
- **Pangu9 Jailbreak** — https://pangu9.net
- **TaiG** — https://www.taigjailbreak.org
- **Pangu** — http://en.pangu.io

iOS Trojans

AceDeceiver

- This Trojan exploits design flaws in Apple's DRM (Digitals Rights Management) mechanism
- Fair Play Man-in-the-Middle technique is used to spread pirated IOS app

Spy/MobileSpy!iPhoneOS

- This malware allows an attacker to eavesdrop all incoming and outgoing calls, SMS, URLs and GPS position are logged to a remote server on the infected iOS device
- Installation of this spyware requires a jailbroken iPhone

Aliases

- Spyware:WinCE/BopSmiley.A
- SPR/MobileSpy
- SPR/RetinaX.A

- DualToy trojan
- KeyRaider
- XcodeGhost
- AdThief/Spad
- Trapsms

Guidelines for Securing iOS Devices

1. Use passcode lock feature for locking iPhone
2. Use iOS devices on a secured and protected Wi-Fi network
3. Do not access web services on a compromised network
4. Deploy only trusted third-party applications on iOS devices
5. Disable Javascript and add-ons from web browser
6. Do not store sensitive data on dient-side database
7. Do not open links or attachments from unknown sources
8. Change default password of iPhone's root password from alpine
9. Do not jailbreak or root your device if used within enterprise environments
10. Configure Find My iPhone and utilize it to wipe a lost or stolen device
11. Enable Jailbreak detection and also protect access to iTunes AppleID and Google accounts, which are tied to sensitive data
12. Regularly update your device OS with security patches released by Apple

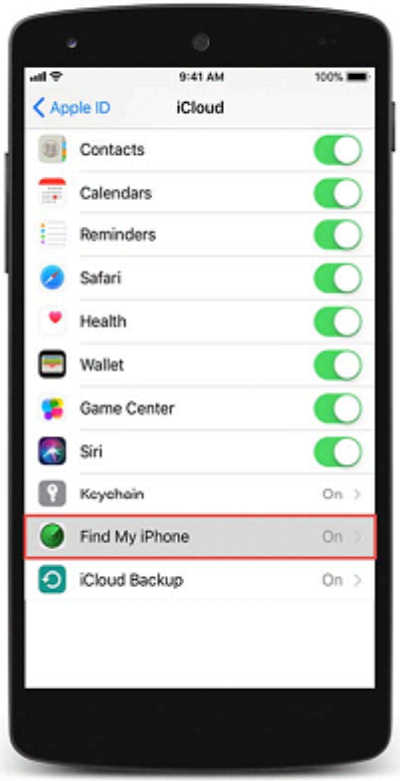
iOS Device Tracking Tools

Find My iPhone

- Find My iPhone helps you **locate and protect your Apple device** if it's ever lost or stolen
- It helps you **locate your missing device on a map**, **remotely lock it**, play a sound, display a message, and remotely erase all the data on it

How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods

- Start at your **Home** screen
- Tap **Settings** → **[your name]** → **iCloud**. If you're using iOS 10.2 or earlier, go to **Settings** → **iCloud**
- Scroll to the bottom and tap **Find My iPhone**
- Slide to turn on **Find My iPhone** and **Send Last Location**



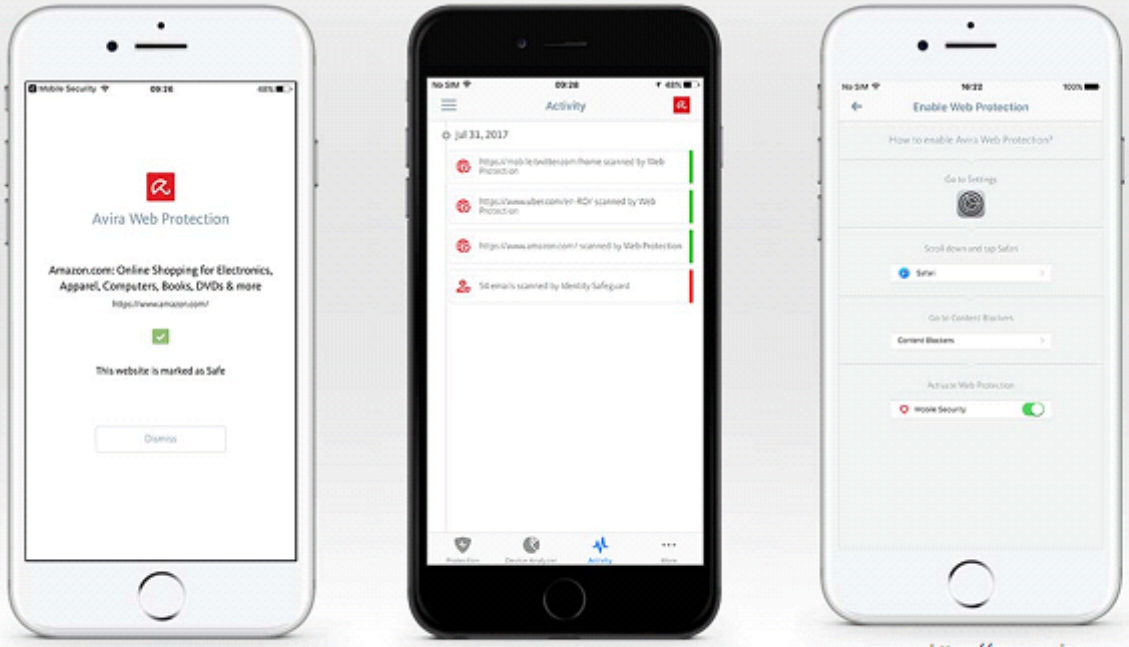
https://support.apple.com

- **Phonty** — https://phonty.com
- **SpyBubble** — https://thespybubble.com
- **GadgetTrak** — http://www.gadgettrak.com
- **iLocalis** — http://ilocalis.com
- **GPS Tracker by FollowMee** — https://itunes.apple.com

iOS Device Security Tools

Avira Mobile Security

This tool provides features like web protection, identity safeguarding, identifies Phishing websites that target you personally, securing emails, tracking your device, identifying activities, organizing device memory, and backing up all your contacts, etc.



https://www.avira.com

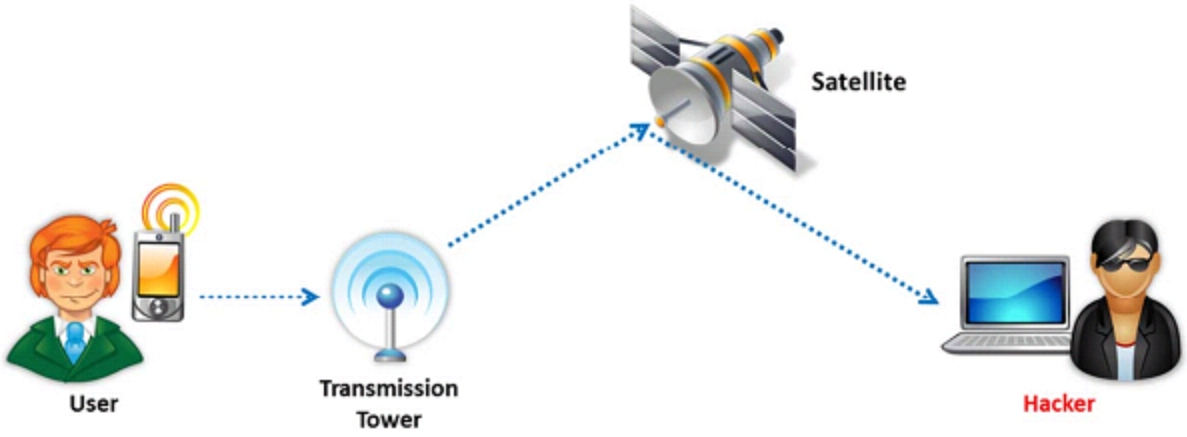
- **Norton Mobile Security**
  https://us.norton.com
- **LastPass Password Manager**
  https://www.lastpass.com
- **Lookout for iOS**
  https://www.mylookout.com
- **SplashID Safe Password Manager**
  https://www.splashid.com
- **Webroot SecureWeb Browser**
  https://www.webroot.com

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

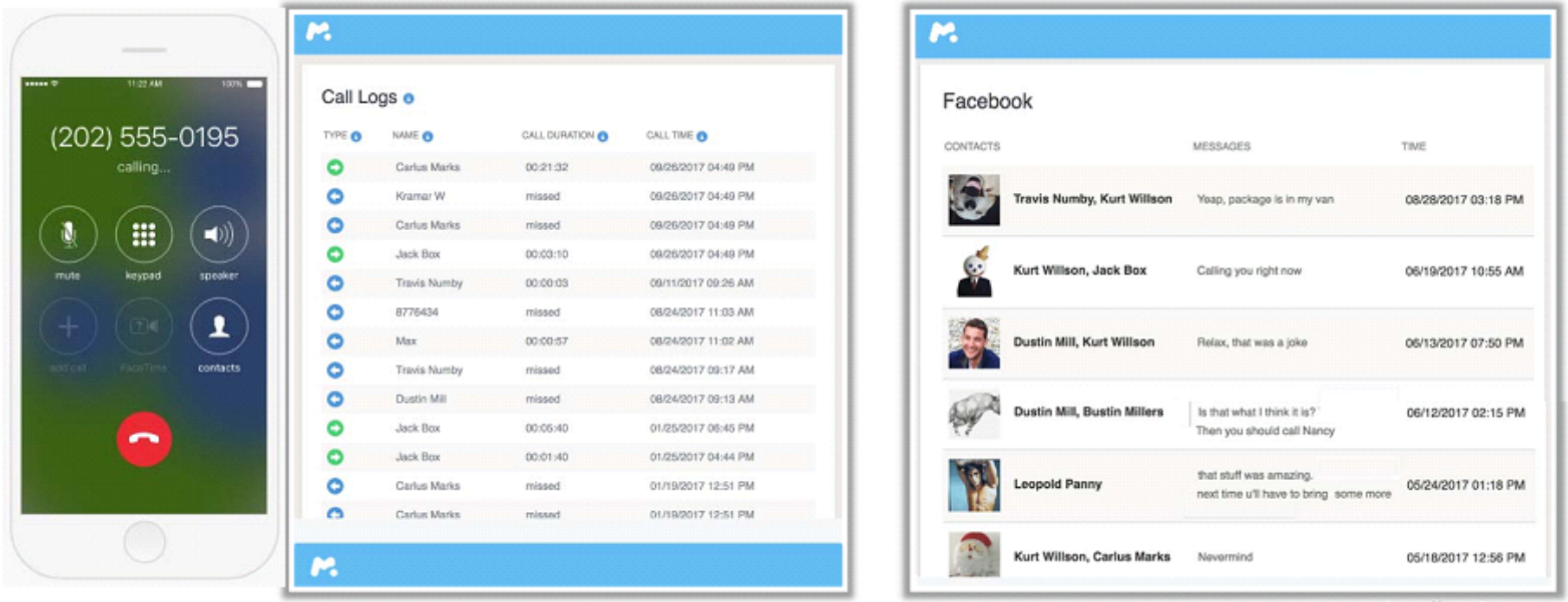
Mobile Spyware

- Mobile spyware is a software tool that **gives you full access to monitor a victim's phone**
- It **secretly records all activity** on the phone such as Internet use, text messages, phone calls, etc.
- Then you can **access the logged information via the software's main website**, or you can also get this tracking information through SMS or email



Mobile Spyware: mSpy

- mSpy is a **mobile monitoring** and **spying application** which runs on the target device to log all activities including call log history, GPS location, calendar updates, text messages, emails, web history, instant messenger chats, keystrokes, etc.



Mobile Spywares

FlexiSPY

FlexiSPY silently **monitor all communications**, locations and user behavior of a smartphone from any web browser

https://www.flexispy.com

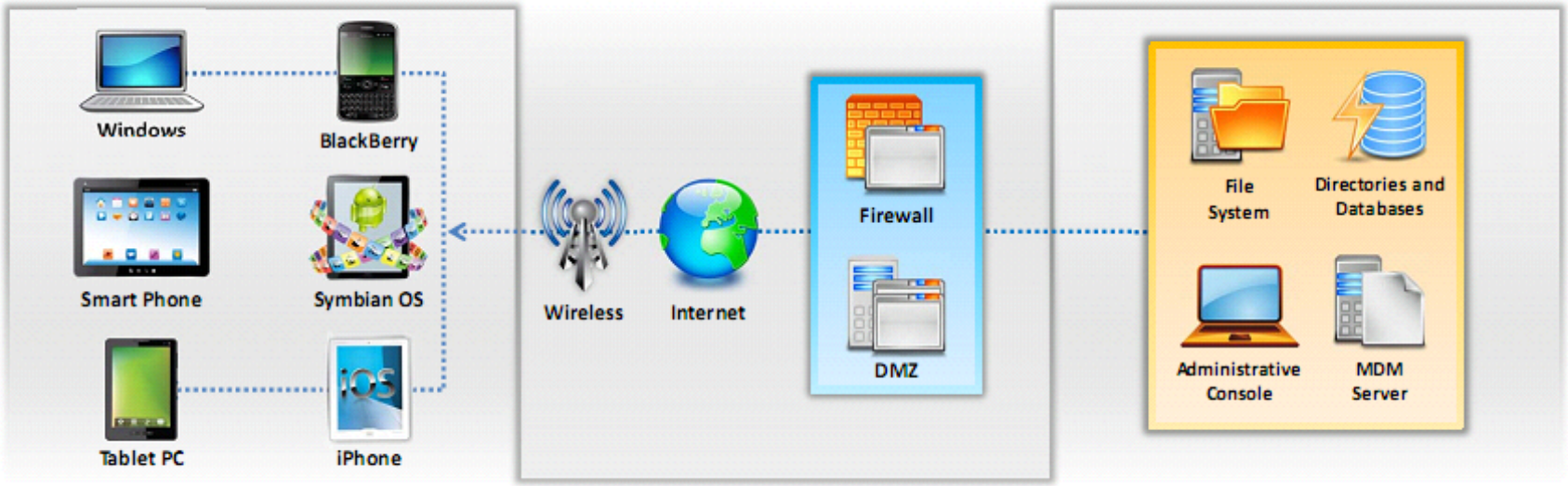
- **Spyera**
  https://spyera.com
- **Highster Mobile**
  http://www.highstermobi.com
- **TeenSafe**
  https://www.teensafe.com
- **MobiStealth**
  http://www.mobistealth.com
- **TheTruthSpy**
  http://thetruthspy.com

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

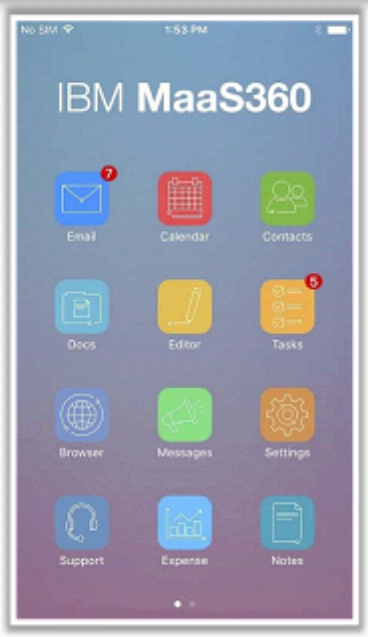
Mobile Device Management (MDM)

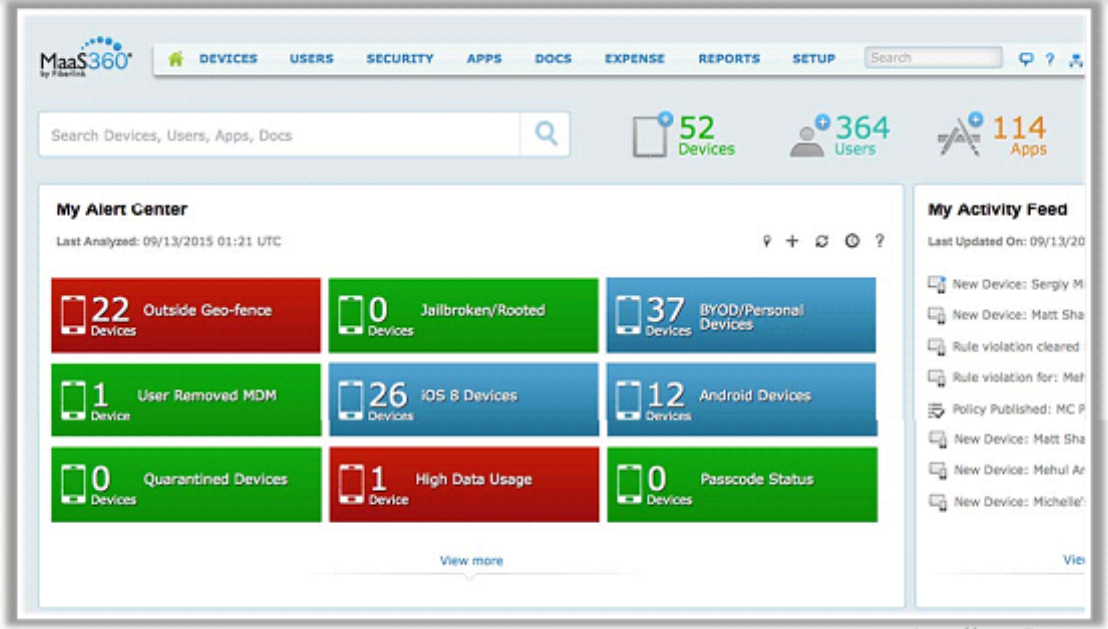
- Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution of applications**, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.
- MDM helps in implementing **enterprise-wide policies** to reduce support costs, business discontinuity, and security risks
- It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and supports mobile devices



Mobile Device Management Solution: IBM MaaS360

- MaaS360 supports the complete **mobile device management (MDM) lifecycle** for smartphones and tablets including iPhone, iPad, Android, Windows Phone, BlackBerry, and Kindle Fire
- As a **fully integrated cloud platform**, MaaS360 simplifies MDM with rapid deployment and comprehensive visibility and control that spans across mobile devices, applications, and documents



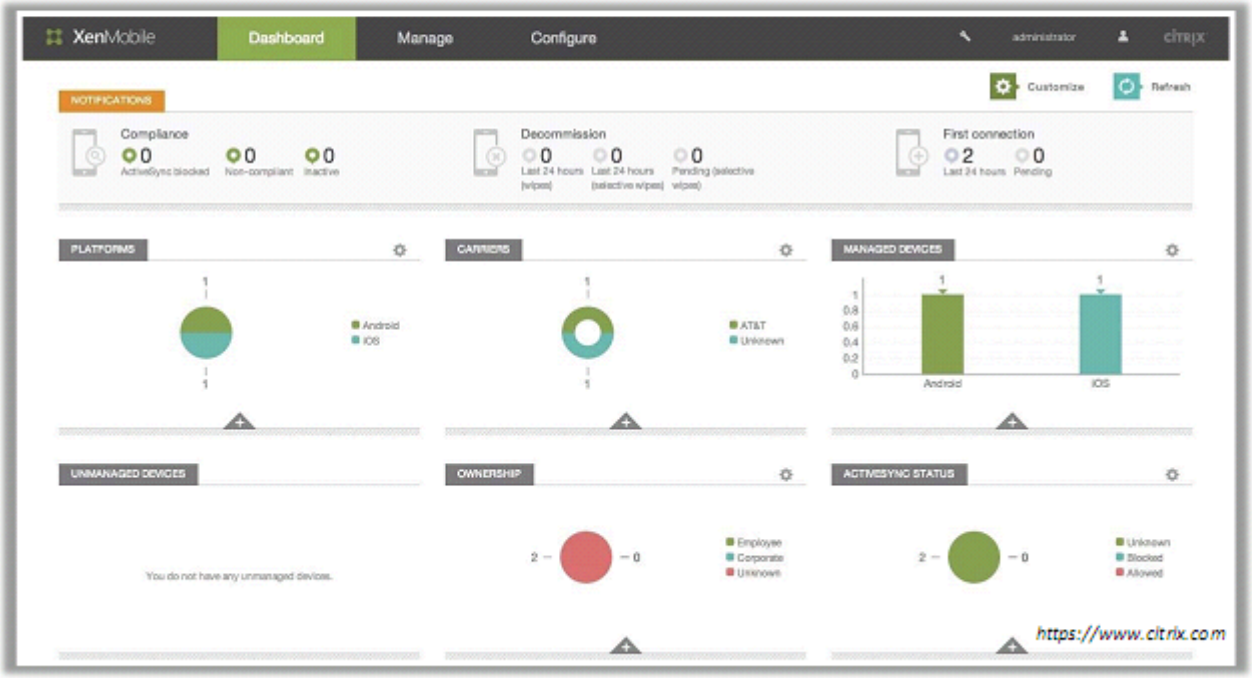


https://www.ibm.com

Mobile Device Management Solutions

XenMobile

Citrix XenMobile contains mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), secure network gateway, and enterprise-grade mobile productivity apps in one comprehensive **enterprise mobility management solution**



VMware AirWatch
https://www.air-watch.com

Sicap Device Management Centre
https://www.sicap.com

SOTI MobiControl
https://www.soti.net

MobiLock Pro
https://mobilock.in

ManageEngine Mobile Device Manager Plus
https://www.manageengine.com

Bring Your Own Device (BYOD)

- Bring your own device (BYOD) refers to a policy allowing an employee to bring their **personal devices** such as laptops, smartphones, and tablets at **workplace** and use them for accessing organization's resources as per their access privileges
- BYOD policy allows employees to use the devices that they are **comfortable with** and **best fits his/her preferences** and work purposes

BYOD Benefits

1. Increased productivity
2. Employee satisfaction
3. Work flexibility
4. Lower costs

BYOD Risks

01 Sharing **confidential data** on unsecured network

02 Data leakage and **endpoint security issues**

03 Improperly **disposing device**

04 Support of many **different devices**

05 Mixing personal and **private data**

06 Lost or **stolen devices**

07 Lack of awareness

08 Ability to bypass organizations **network policy rules**

09 Infrastructure issues

10 Disgruntled employees

BYOD Policy Implementation

01 Define your requirements

02 Select device of your choice and build a technology portfolio

03 Develop policies

04 Security

05 Support

BYOD Security Guidelines

For Administrator

- Secure organization's data centers with **multi-layered protection systems**
- **Educate your employees** about the BYOD policy
- Make it clear who owns what apps and data
- Use **encrypted channel** for data transfer
- Make it clear what apps will be allowed or banned
- **Control access** based on the need-to-know
- Do not allow jailbroken and **rooted devices**
- Apply **session authentication** and **timeout policy** on access gateways

For Employee

- Use **encryption mechanism** to store data
- Maintain a **dear separation** between the business and personal data
- Register devices with a **remote locate** and wipe facility if **company policy permits**
- Regularly update your device with **latest OS** and **patches**
- Use **anti-virus** and **data loss prevention** (DLP) solutions
- Set a **strong passcode** to the device and change it quite often
- Set **passwords for apps** to restrict others from accessing them

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

General Guidelines for Mobile Platform Security

1. Do not load too many **applications** and avoid auto-upload of photos to **social networks**
2. Perform a **Security Assessment** of the Application **Architecture**
3. Maintain **configuration** control and **management**
4. **Install** applications from trusted application **stores**
5. Securely **wipe or delete** the data disposing of the device
6. Do not share the information within **GPS-enabled apps** unless they are necessary
7. Disable wireless access such as **Wi-Fi** and **Bluetooth**, if not in use
8. Never connect two separate networks such as **Wi-Fi** and **Bluetooth** simultaneously

General Guidelines for Mobile Platform Security (Cont'd)

- Use passcode
- Update OS and Apps
- Enable remote management and use remote wipe services
- Do not allow Rooting or Jailbreaking
- Encrypt storage

- Perform periodic backup and synchronization
- Filter e-mail-forwarding barriers
- Configure Application certification rules
- Harden browser permission rules
- Design and implement mobile device policies

Mobile Device Security Guidelines for Administrator

01 Publish an **enterprise policy** that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise

02 Publish an enterprise policy for **cloud**

03 Enable **security measures** such as antivirus to protect the data in the datacenter

04 Implement policy that specifies what levels of **application and data access** are allowable on consumer-grade devices, and which are prohibited

05 Specify a **session timeout** through **Access Gateway**

06 Specify whether the **domain password** can be cached on the device, or whether users must enter it every time they request access

07 Determine the allowed **Access Gateway authentication methods** from the following:

- No authentication
- Domain only
- SMS authentication
- RSA SecurID only
- Domain + RSA SecurID

SMS Phishing Countermeasures

01 Never reply to a **suspicious SMS** without verifying the source

02 Do not click on any **links** included in the SMS

03 Never reply to a SMS that requires **personal and financial information** from you

04 Review the **bank's policy** on sending SMS

05 Enable the "**block texts from the internet**" feature from your provider

06 Never reply to a SMS which urging you to **act or respond quickly**

07 **Never call a number** left in a SMS

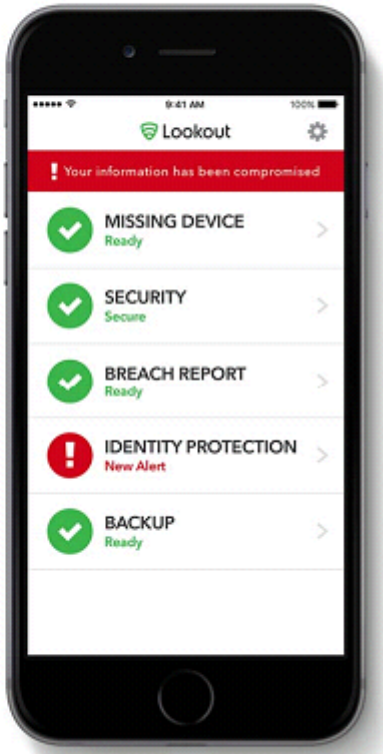
Mobile Protection Tools

Lookout Personal

- Lookout Personal helps to **protect your device** from security threats, loss, and theft

Features

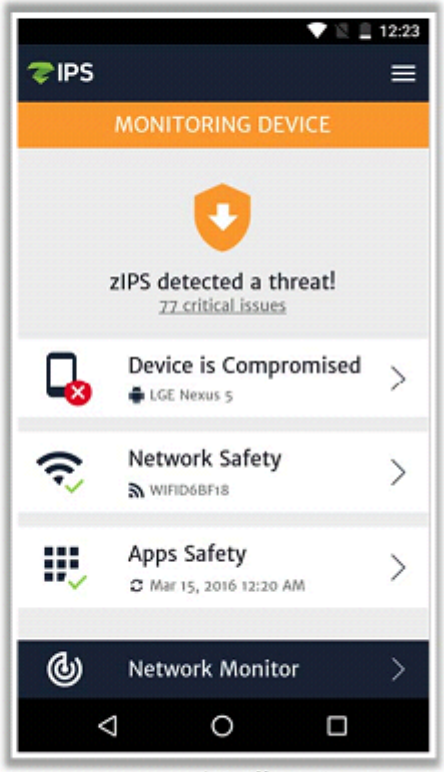
- All-in-one protection
- Mobile threat security
- Identity theft protection
- Breach report
- Theft protection
- Data backup



https://www.lookout.com

Zimperium's zIPS

- Zimperium's zIPS is the mobile **intrusion prevention system app** that provides comprehensive protection for iOS and Android devices against mobile network, device and application cyber attacks
- It can detect both **known and unknown threats** by analyzing the behavior of your mobile device

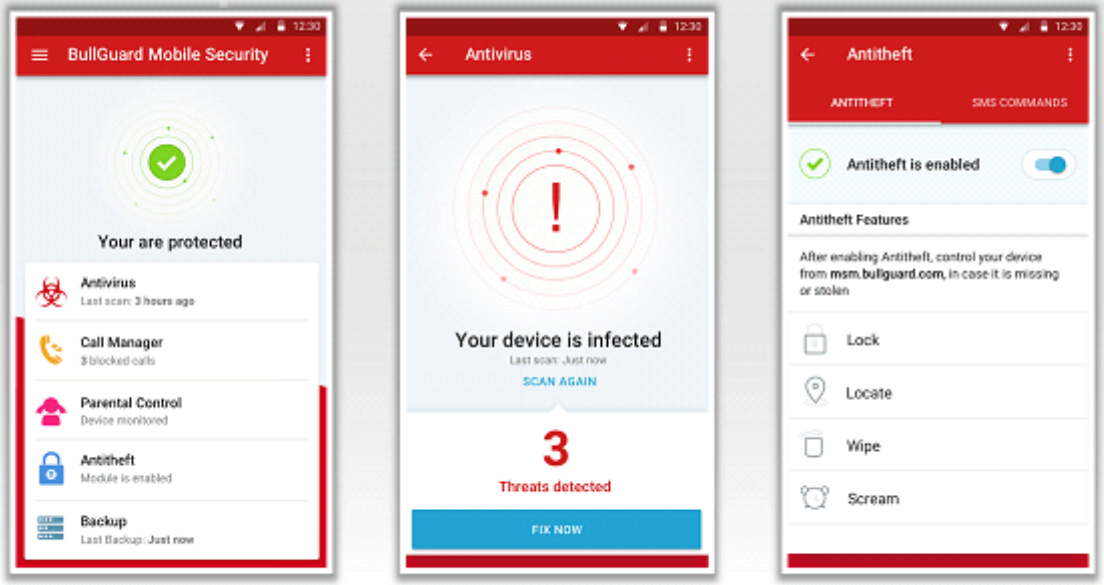


https://www.zimperium.com

Mobile Protection Tools (Cont'd)

BullGuard Mobile Security

- It delivers complete **mobile phone antivirus** against all mobile phone viruses
- It locks, locates and wipes device **remotely if lost or stolen**
- It blocks **unwanted calls** and **SMS messages**



https://www.bullguard.com

- **McAfee Mobile Security**
  https://www.mcafee.com
- **Kaspersky Internet Security for Android**
  https://my.kaspersky.com
- **AVG AntiVirus Pro for Android**
  https://www.avg.com
- **F-Secure Mobile Security**
  https://www.f-secure.com
- **Avast Mobile Security**
  https://www.avast.com

Mobile Anti-Spyware

Malwarebytes for Android

- Malwarebytes Anti-malware mobile tool is an **protection against malware, ransomware**, and other growing threats to Android devices

Features

- Detects and removes adware and malware
- Blocks malware and ransomware automatically
- Conducts privacy audit for all apps
- Safer browsing

https://www.malwarebytes.org

AntiSpy Mobile
http://www.antispymobile.com

FREE Spyware & Malware Remover
https://play.google.com

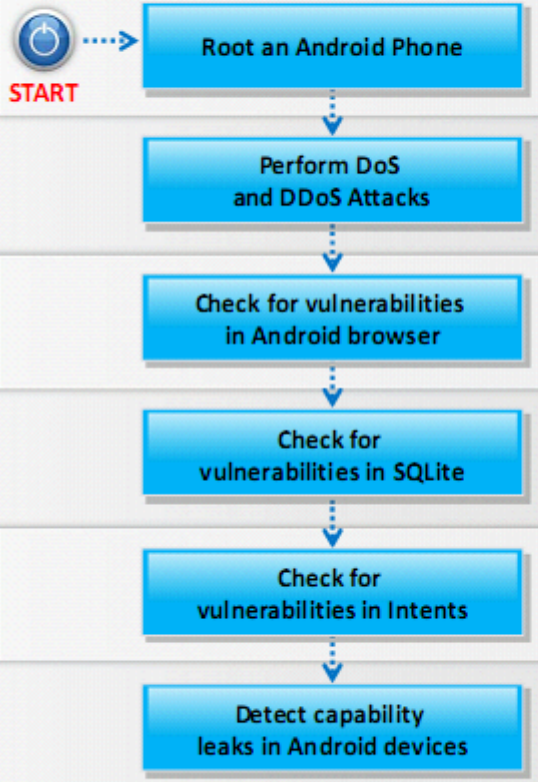
D-Vasive Anti-Spy
https://play.google.com

SpyWare Removal (Anti Spy)
https://play.google.com

Module Flow

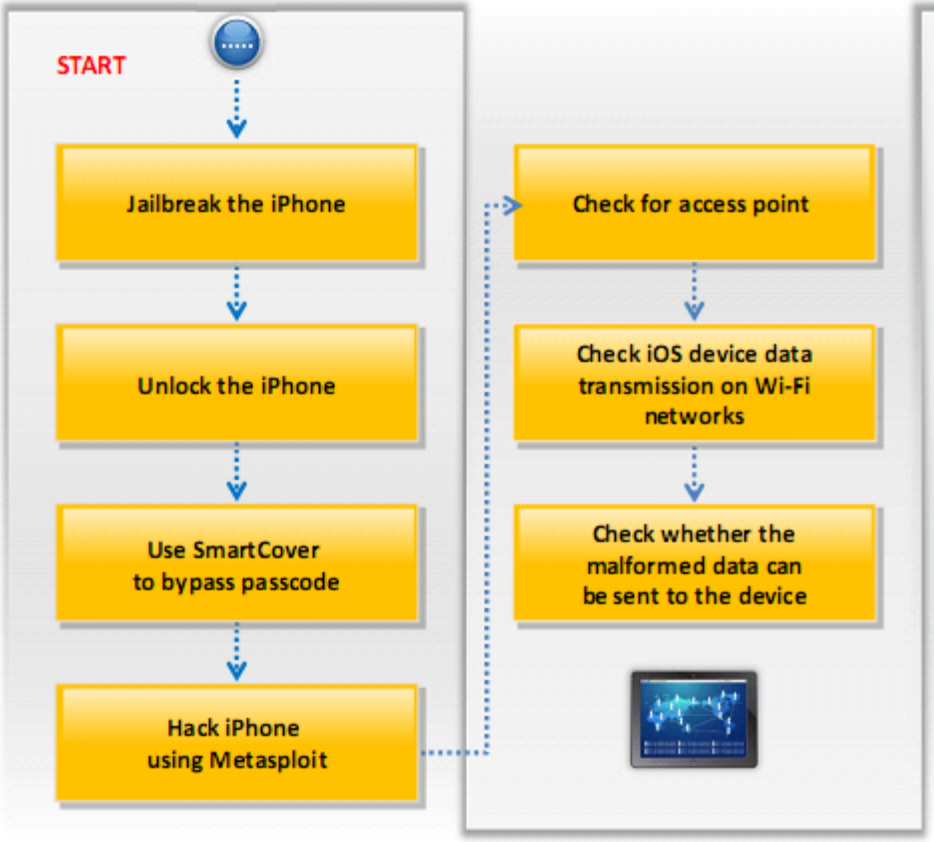
1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Spyware
5. Mobile Device Management
6. Mobile Security Guidelines and Tools
7. Mobile Pen Testing

Android Phone Pen Testing



- Try to Root an Android Phone to gain the administrative access to the Android devices using tools such as **Kingo Android ROOT**, **TunesGo Root Android Tool**, etc.
- Use tool **LOIC**, **AnDOSid** to perform DoS and DDoS attacks on Android phone
- Check whether **cross-application-scripting error** is present in the android browser which allows hackers to easily hack the Android device and try to break down the web browser's sandbox using infected java script code
- Check whether email password is stored as **plain text in the SQLite database** and also check whether Skype on Android uses unencrypted SQLite database to store contacts, profile information and instant message logs
- Try to **exploit Android Intents** to obtain the user's private information
- You can use **apset** tool to detect application's communication vulnerabilities
- Use tool **Co Checker**, **IntentFuzzer**, etc. to detect capability leaks in Android devices

iPhone Pen Testing



- Try to Jailbreak the iPhone using tools such as **Cydia**, **Anzhuang**, etc.
- Unlock the iPhone using tools such as **iPhoneSimFree**, etc.
- Hold the power button of an iOS operating device till the **power off message** appears. Close the smart cover till the screen shuts and open the smart cover after few seconds. Press the cancel button to **bypass the password code security**
- Use the Metasploit tool to exploit the vulnerabilities in iPhone. Try to send **malicious code** as payload to the device to gain access to the device
- Setup an **access point** with the same name and encryption type
- Perform **man-in-the-middle/SSL stripping attack** by intercepting wireless parameters of iOS device on Wi-Fi network. Send malicious packets on Wi-Fi network using **Cain & Abel** tool
- Use **social engineering techniques** such as sending emails, SMS to trick the user to open links that contain malicious web pages

Mobile Pen Testing Toolkit: Hackode

Hackode: The hacker's Toolbox is an application for penetration tester, Ethical hackers, IT administrator and Cyber security professional to perform different tasks like reconnaissance, scanning for exploits, etc.

- Google Hacking and Google Dorks
- Whois, Ping, and Traceroute
- DNS lookup, MX Records, DNS Dig
- Exploits and Security Rss Feed

https://play.google.com

Module Summary

- Focus of attackers and malware writers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls
- Sandboxing helps protect systems and users by limiting the resources the app can access to the mobile platform
- Android is a software stack developed by Google for mobile devices that includes an operating system, middleware, and key applications
- Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- Jailbreaking provides root access to the operating system and permits download of third-party applications, themes, extensions on iOS devices
- Mobile Device Management (MDM) provides a platform for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.
- Mobile protection tools protect your device from security threats, loss, and theft