Hacking Mobile Platforms

Module 15

Unmask the Invisible Hacker.

The Future of Mobile

C|EH Certified Ethical Hacker

Internet Users Worldwide

Global number of internet users

2013	2016	2025
2.4 Billion	3.4 Billion	5.4 Billion

66% of the world's population (based on an increase of 2-3 billion connected to the Internet)

Using Mobiles with Money

Mobile payment user

2012	2013	2017
200 Million	245 Million	450 Million
transactions	transactions	transactions
$163 Billion	$235 Billion	$721 Billion

2020

50%

of transactions will be made by mobile

The Projected Growth of Mobile Use

Internet connections made via mobile devices

2013	2025
17%	80%

http://www.three.co.uk

Smartphone Adoption Rate

Percentage of UK Population

Tablet Adoption Rate

Percentage of UK Population

Module Objectives

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



Module Flow

1. Mobile Platform Attack Vectors

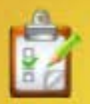
2. Hacking Android OS

3. Hacking iOS

4. Hacking Windows Phone OS

5. Hacking BlackBerry

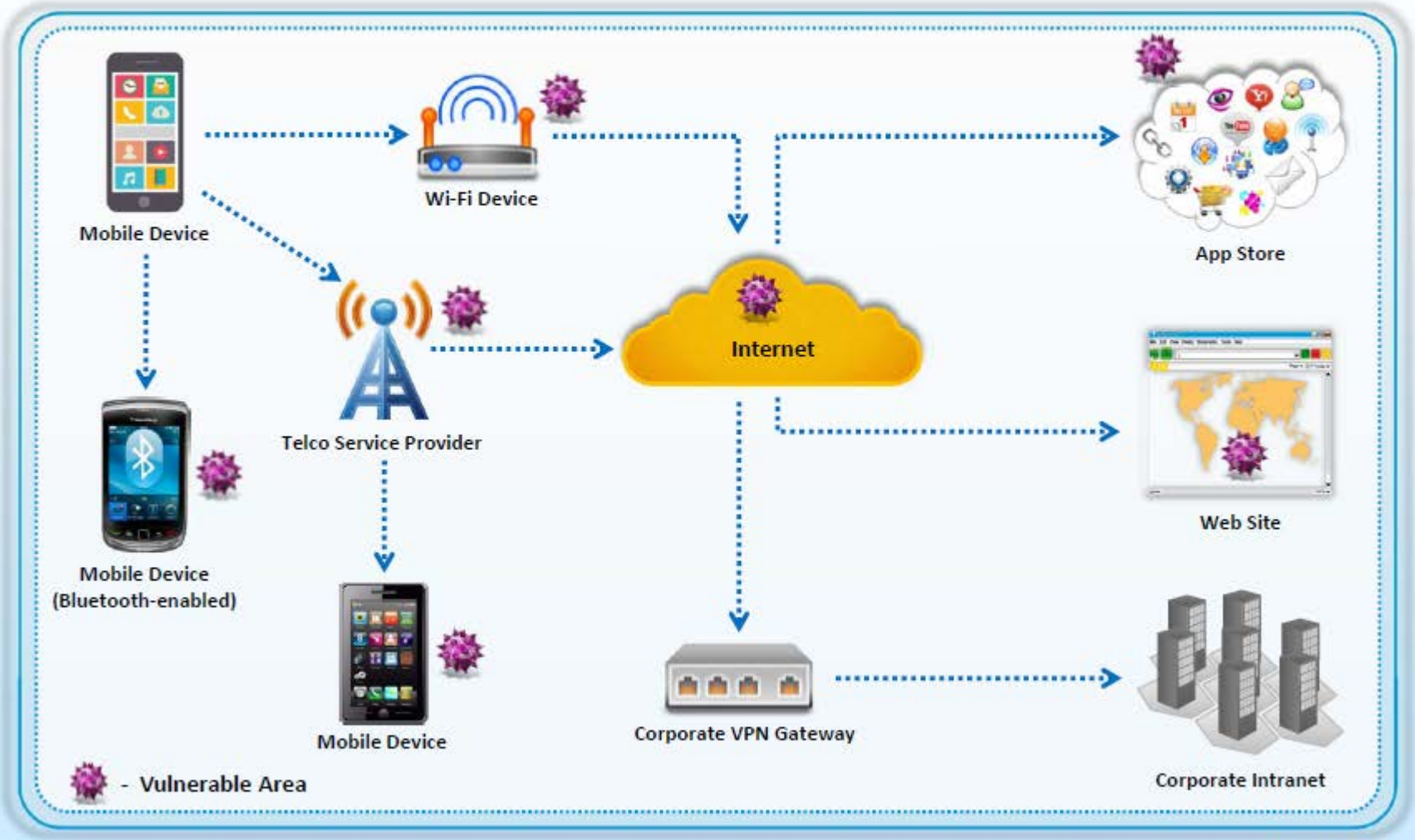
6. Mobile Device Management



7. Mobile Security Guidelines and Tools

8. Mobile Pen Testing

Vulnerable Areas in Mobile Business Environment



https://www-935.ibm.com

OWASP Mobile Top 10 Risks

C|EH Certified Ethical Hacker

01  Weak Server Side Controls

02  Insecure Data Storage

03  Insufficient Transport Layer Protection

04  Unintended Data Leakage

05  Poor Authorization and Authentication

06  Broken Cryptography

07  Client Side Injection

08  Security Decisions Via Untrusted Inputs

09  Improper Session Handling

10  Lack of Binary Protections

https://www.owasp.org

Anatomy of a Mobile Attack

C|EH Certified Ethical Hacker

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
- Config Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to device and User Info

MALWARE

Apple | Android | Windows | RIM

SYSTEM

- No Passcode/Weak Passcode
- iOS Jailbreaking
- Android Rooting
- OS data caching
- Passwords & Data accessible
- Carrier-loaded software
- No Encryption/Weak Encryption
- User-initiated code
- Zero-day exploits

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

Point 03 – THE DATA CENTER

INTERNET

WEB SERVER

- Platform Vulnerabilities
- Server Misconfiguration
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks

DATABASE

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

https://viaforensics.com

How a Hacker can Profit from Mobile when Successfully Compromised

C|EH Certified Ethical Hacker

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

16M

Mobile devices infected worldwide

6 out of the top **20** mobile threats are spyphone apps

14%

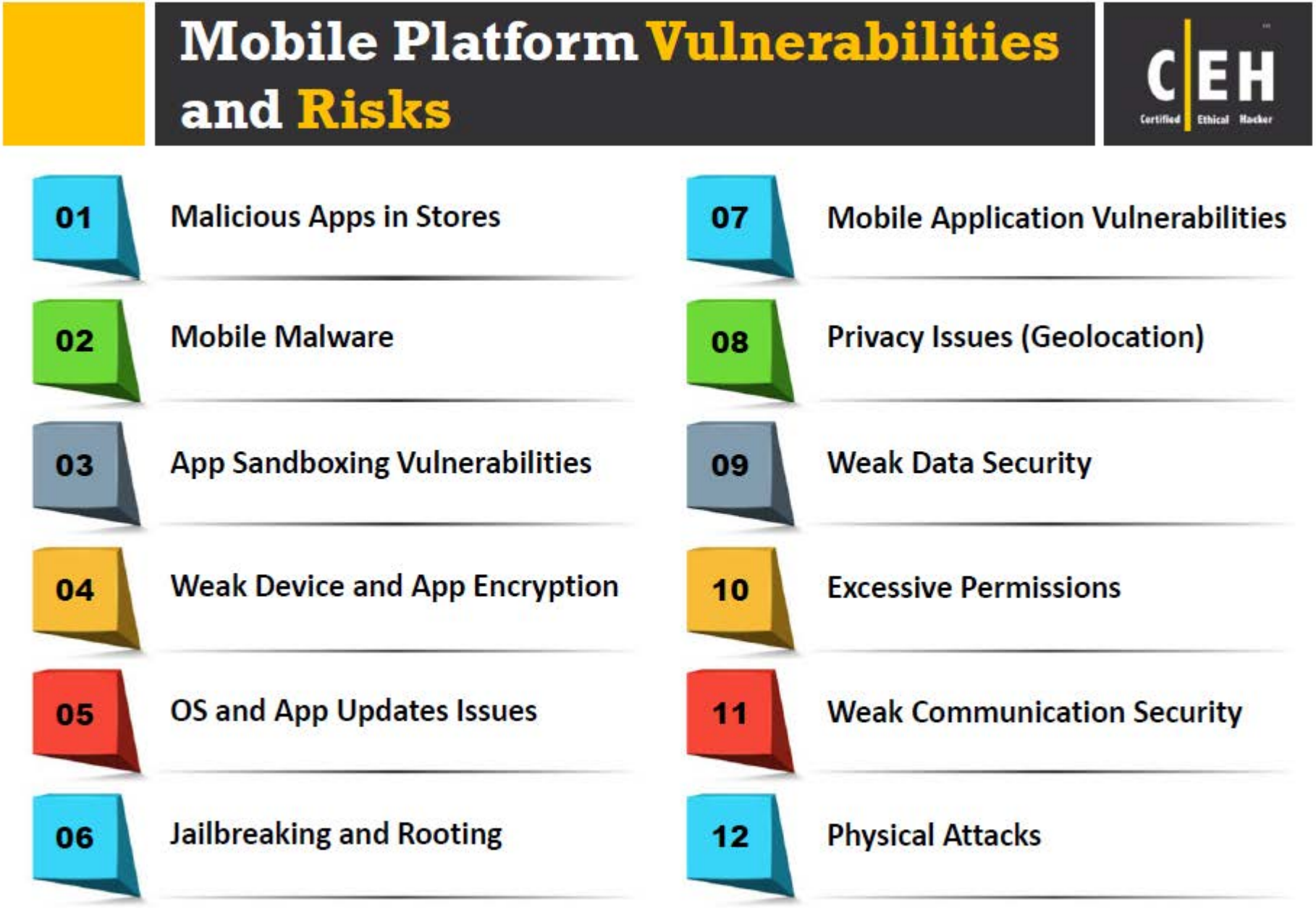
of homes are infected with malware

http://www.sophos.com

http://www.alcatel-lucent.com

Mobile Attack Vectors

Mobile Platform Vulnerabilities and Risks

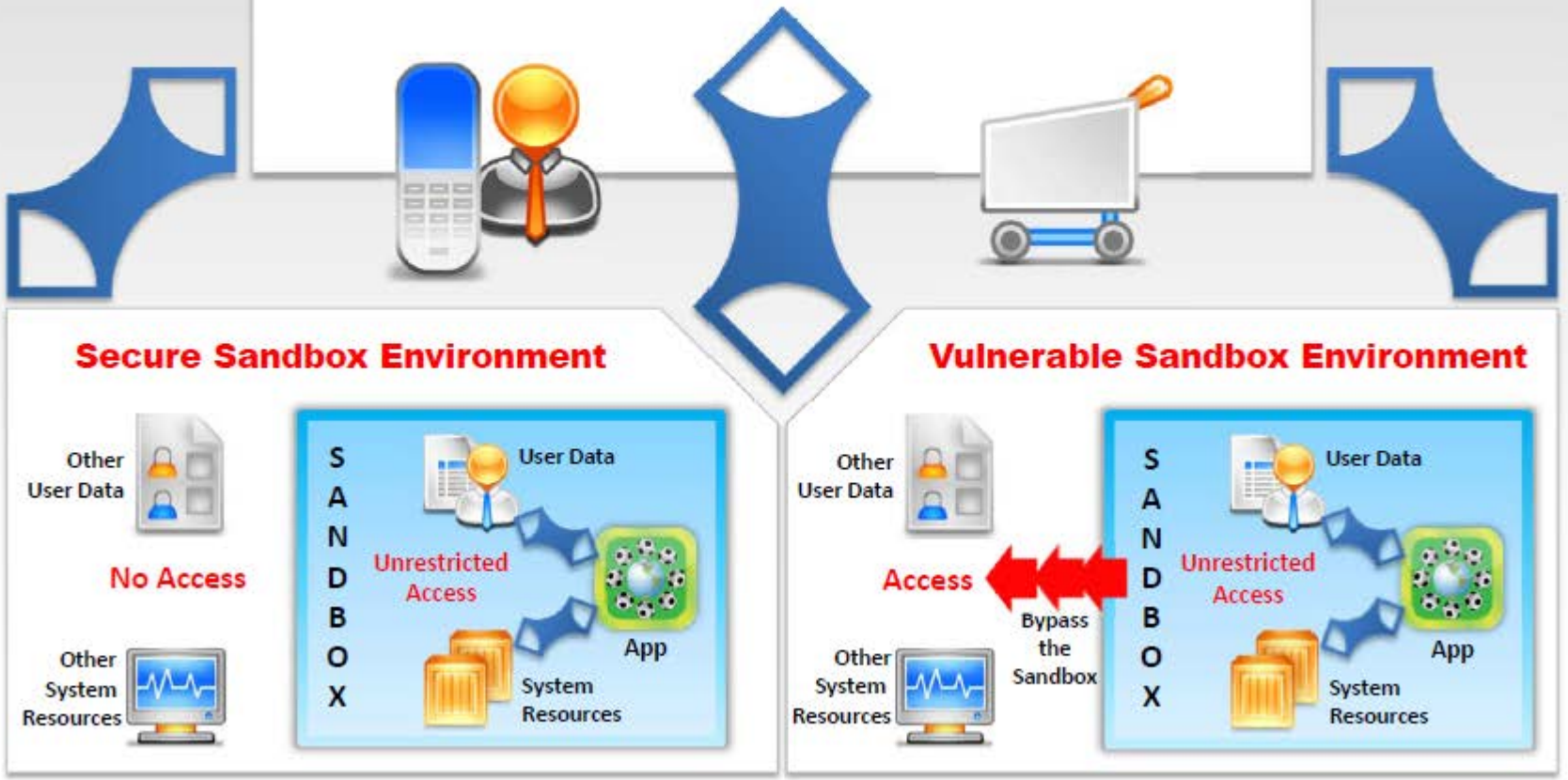


Security Issues Arising from App Stores

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 in the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



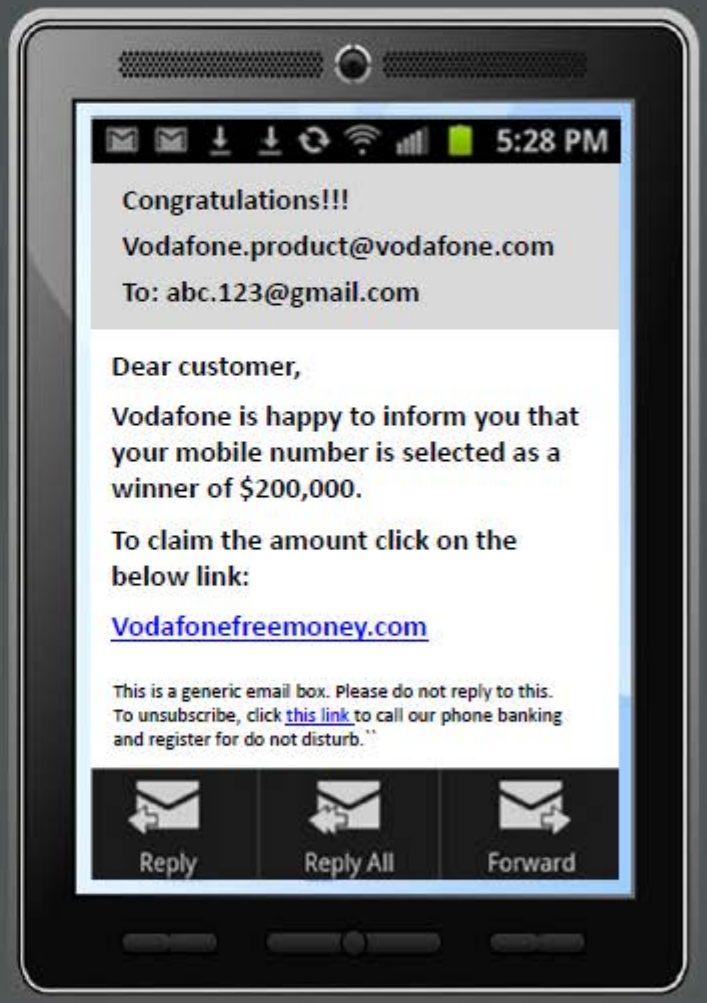
Mobile Spam

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

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

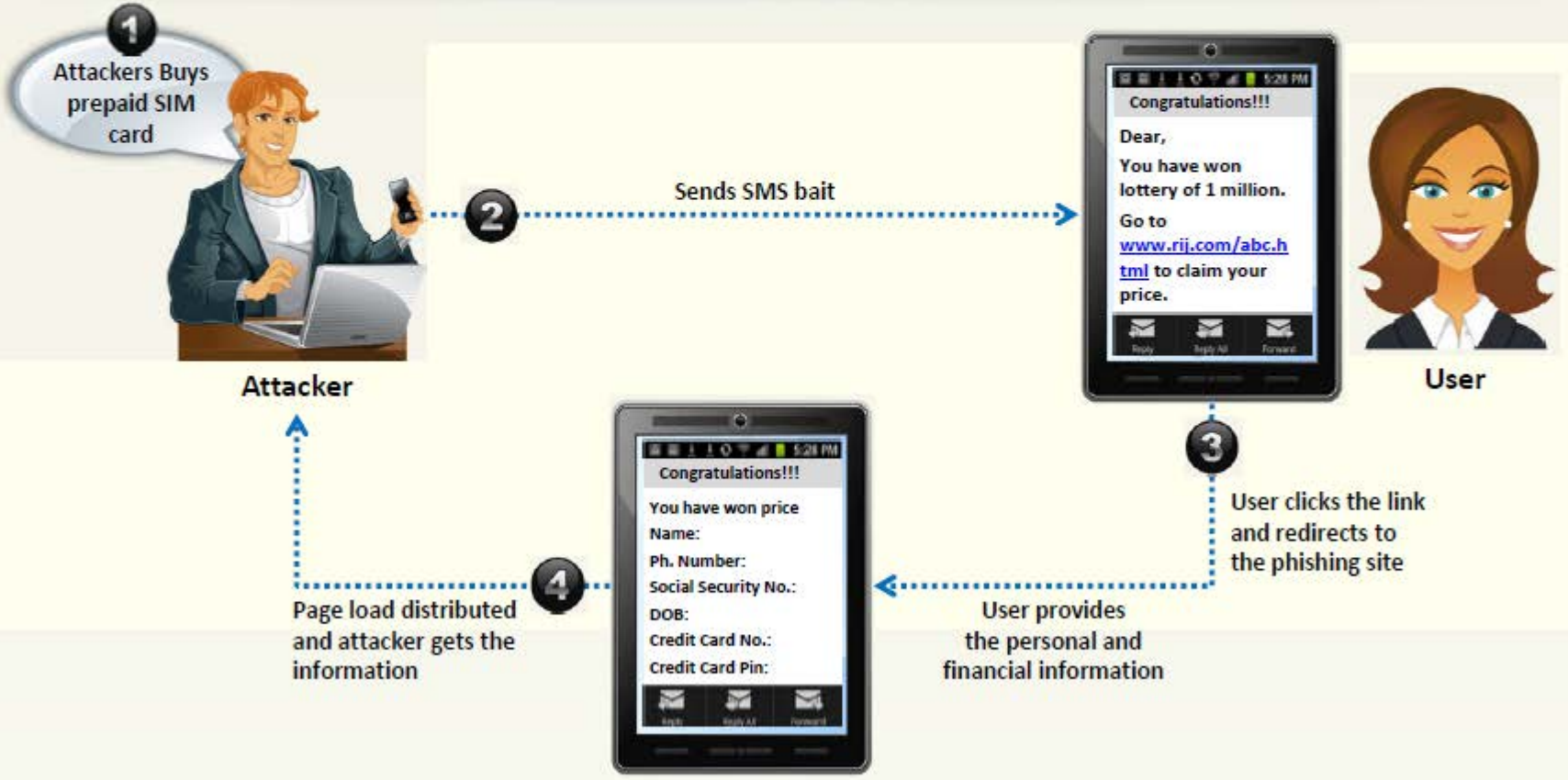
03 Significant amount of bandwidth is wasted by Spam messages

04 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

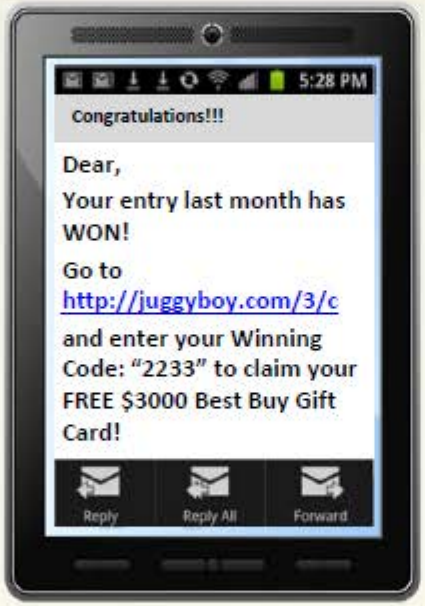


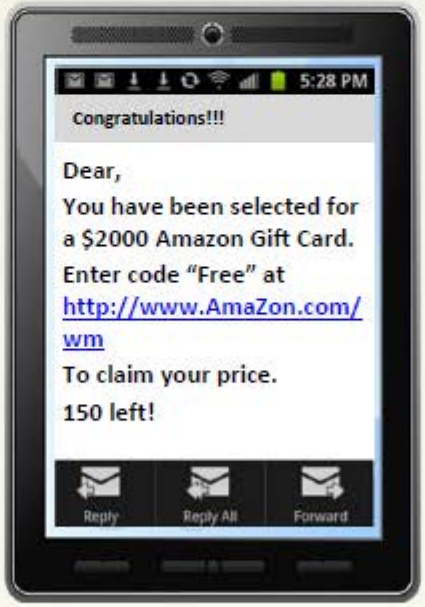
Why SMS Phishing is Effective?

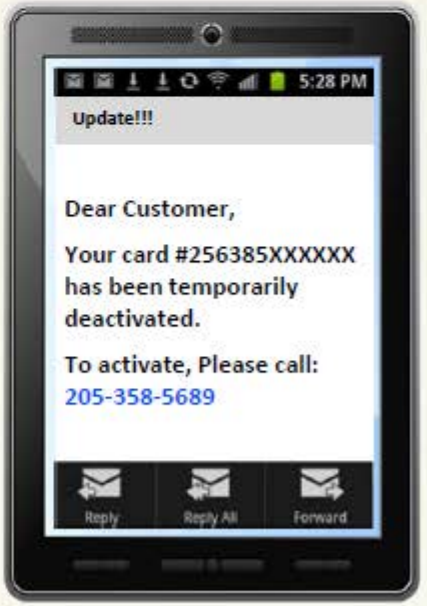
C|EH Certified Ethical Hacker

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

SMS Phishing Attack Examples

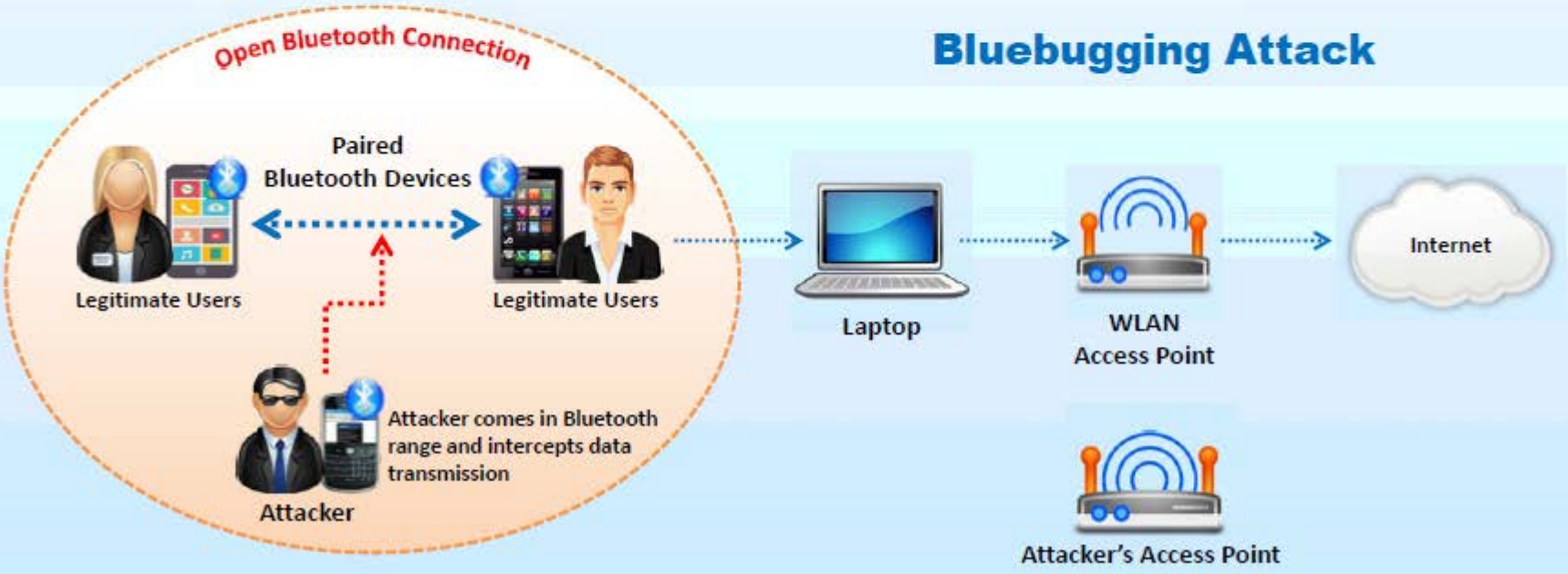




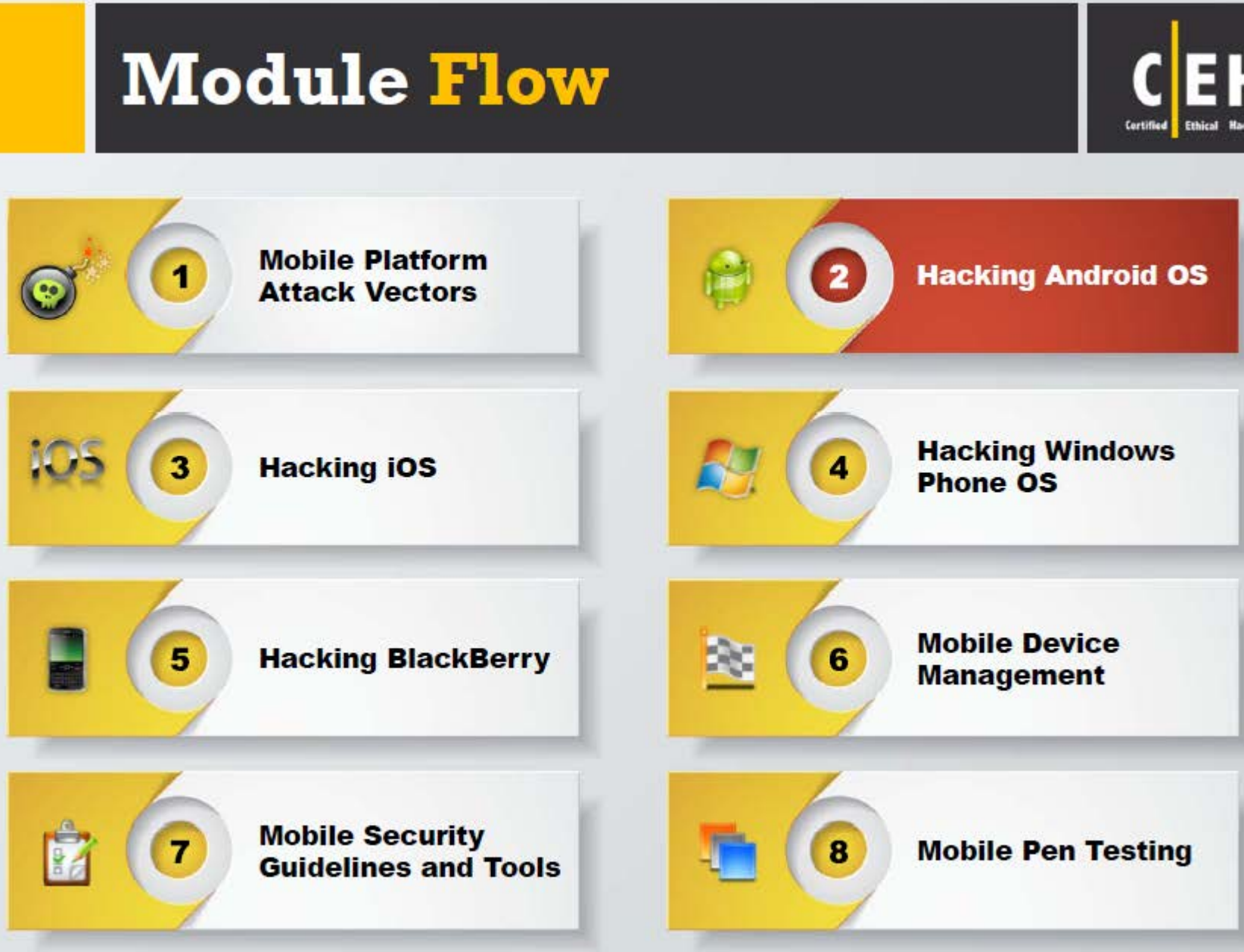


Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- 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



Android OS

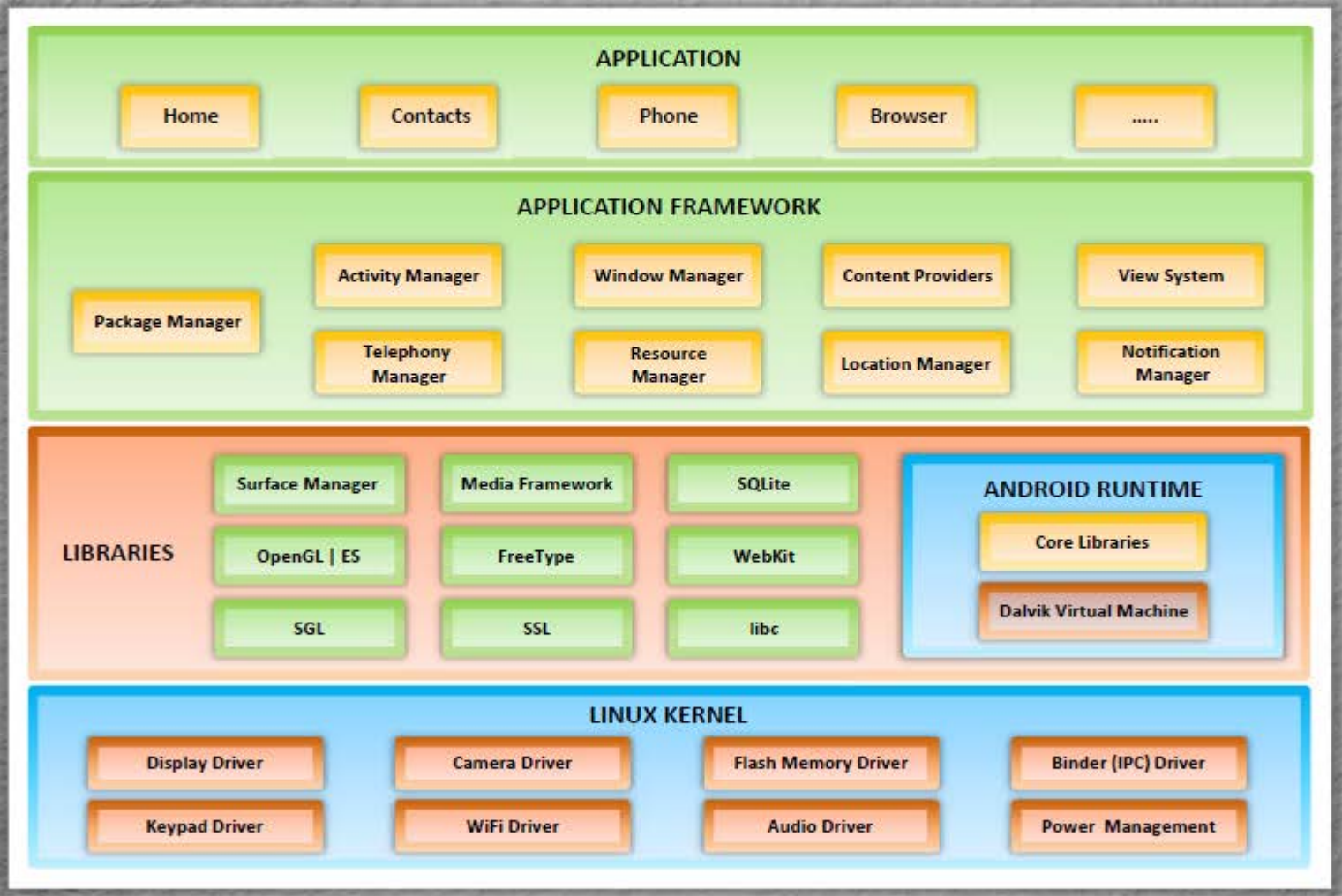
Android is software environment developed by Google for mobile devices that includes an operating system, middleware, and key applications

Features

- Application framework enabling reuse and replacement of components
- Dalvik virtual machine optimized for mobile devices
- Integrated browser based on the open source WebKit engine
- SQLite for structured data storage
- 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

http://developer.android.com

Android OS Architecture



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

http://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**
- Improved **performance**
- **Wi-Fi** and **Bluetooth** tethering
- Install applications on **SD card**
- Better user interface and keyboard

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 Phones Using SuperOneClick

- Plug in and connect your android device to your computer via **USB**
- **Install driver** for the device if prompted
- Unplug and re-connect, but this time select "**Charge only**" to sure that your phone's SD Card is not mounted to your PC
- Go to **Settings** → **Applications** → **Development** and enable **USB Debugging** to put your android into USB Debugging mode
- Run **SuperOneClick.exe** (available in Tools DVD)
- Click on the "**Root**" button
- Wait for some time until you see a "**Running a Su test Success!**" message
- Now check out the **installed apps** in your phone
- Superuser icon means you now have **root access** (reboot the phone if you do not see it)

Rooting Android Phones Using Superboot

C|EH Certified Ethical Hacker

1 Download and extract the **Superboot files**

2 **Put your Android phone in bootloader mode**

- Turn off the phone, **remove the battery**, and plug in the USB cable
- When the battery icon appears onscreen, **pop the battery back in**
- Now tap the **Power button** while holding down the Camera key
- For Android phones with a trackball: Turn off the phone, **press and hold the trackball**, then turn the phone back on

3 **Depending on your computer's OS, do one of the following:**

- **Windows**: Double click "install-superboot-windows.bat"
- **Mac**: Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-mac.sh" followed by "./install-superboot-mac.sh"
- **Linux**: Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-linux.sh" followed by "./install-superboot-linux.sh"

4 Your device has been **rooted**



Android Rooting Tools

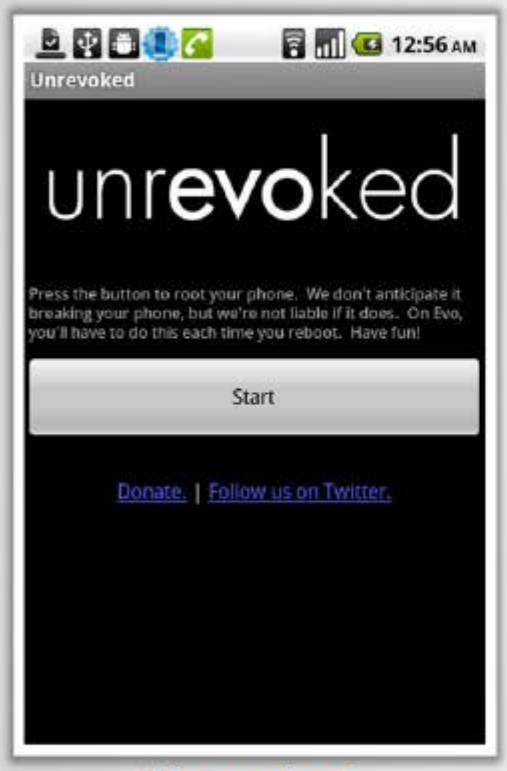
One Click Root

- Download **One Click Root**
- Connect your Android phone or tablet to your computer using your **Micro USB/USB cable**
- Enable **USB Debugging** mode and Install **USB drivers** for your device
- Run One Click Root software then click '**Root Now**'

Kingo Android ROOT

- Download **Kingo Android Root** and install it on your desktop
- Run the tool and **connect the device** to the computer with USB cable
- 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

Android Rooting Tools (Cont'd)



Unrevoked

RescueRoot

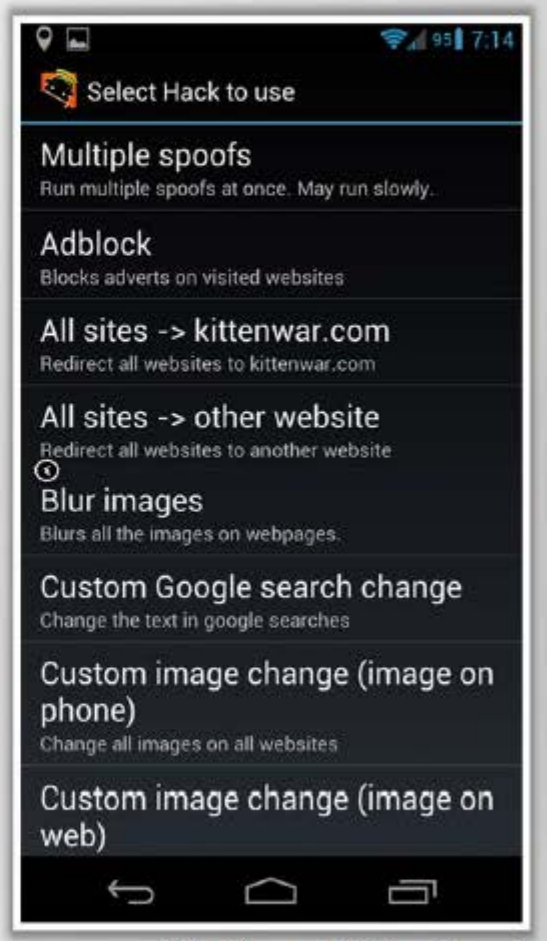
Unlock Root Pro

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



http://www.digitalsquid.co.uk

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

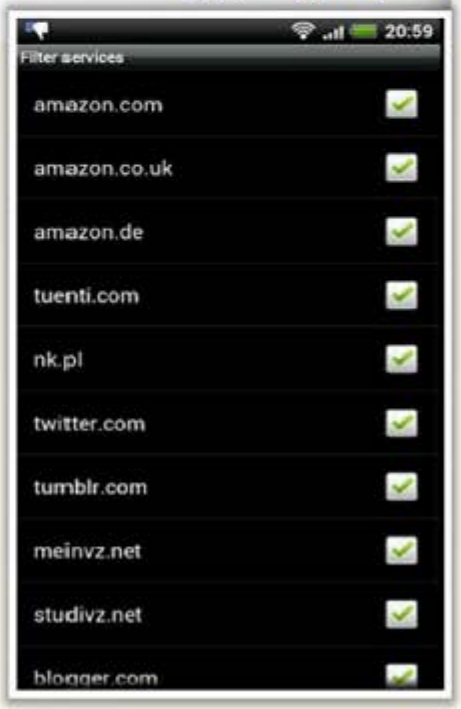
DroidSheep can capture sessions using the libpcap library and supports: OPEN Networks, WEP encrypted networks, WPA and WPA2 (PSK only) encrypted networks

http://droidsheep.de

Android-based Sniffer: 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

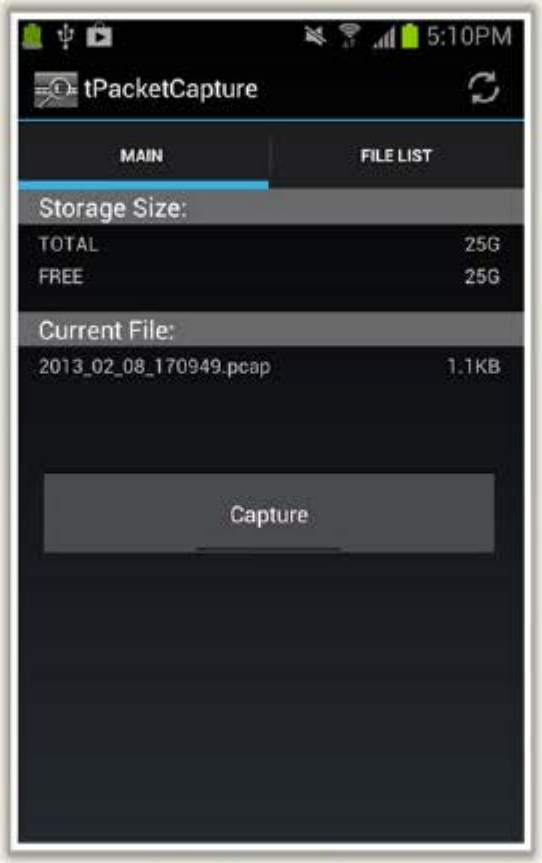


Android-based Sniffers: Packet Sniffer, tPacketCapture, and Android PCAP

Packet Sniffer

https://sites.google.com

tPacketCapture



http://www.taosoftware.co.jp

Android PCAP

http://www.kismetwireless.net

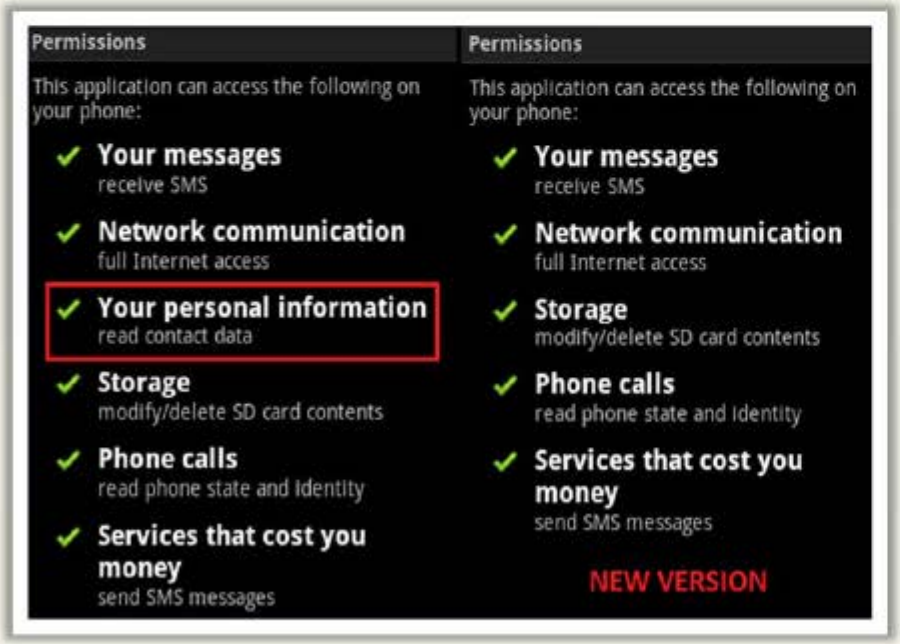
Android Trojan: ZitMo (ZeuS-in-the-Mobile)

- ZitMo is the notorious mobile component of the **Zeus banking Trojan** that circumvents two-factor authentication by intercepting SMS confirmation codes to **access bank accounts**
- The new versions for Android and BlackBerry have now added botnet-like features, such as **enabling cybercriminals** to control the Trojan via SMS commands

Android Trojans: FakeToken and TRAMP.A

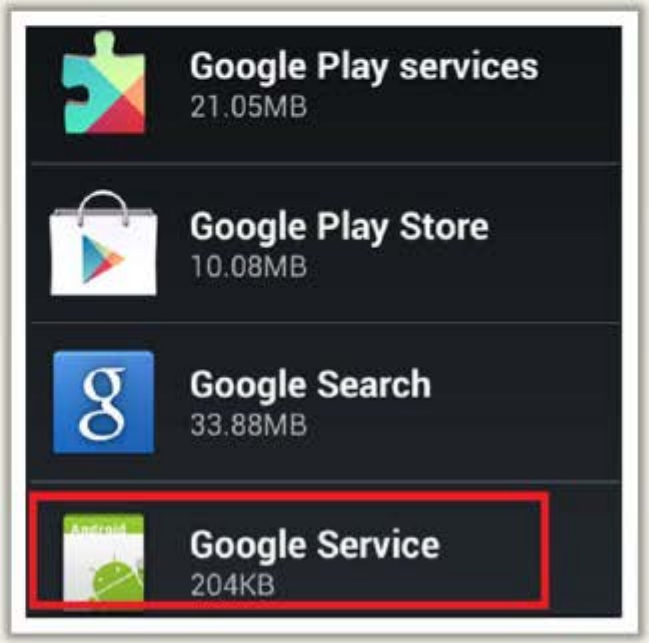
FakeToken

FakeToken **steals both banking authentication factors** (Internet password and mTAN) directly from the mobile device



TRAMP.A

Design to **log the keystrokes** of target android mobile to steal passwords and other sensitive information



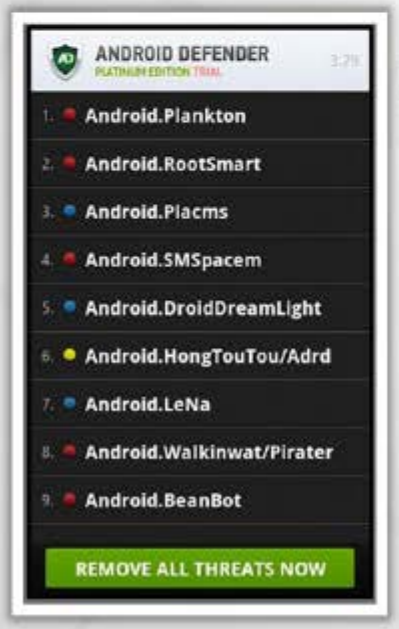
Android Trojans: Fakedefender and Obad

Fakedefender

- Android.Fakedefender is a Trojan horse for Android devices that **displays fake security alerts** in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device

Obad

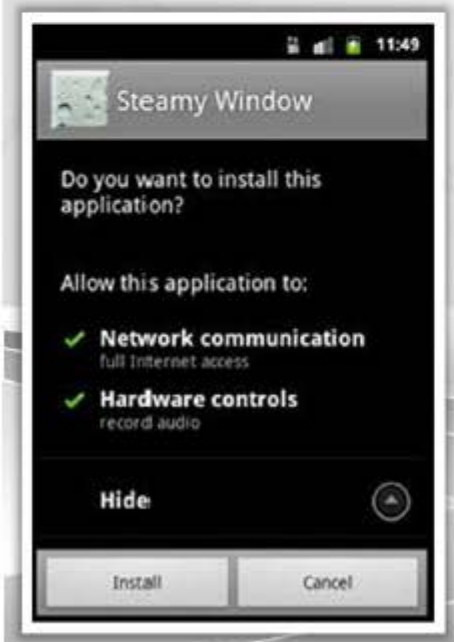
- Obad Trojan is distributed through different methods such as mobile botnet, traditional SMS spam, Google Play fake store, etc.
- It **gains administrator privileges** and uses an exploit to break through the Android operating system's security layer



Android Trojans: FakeInst and OpFake

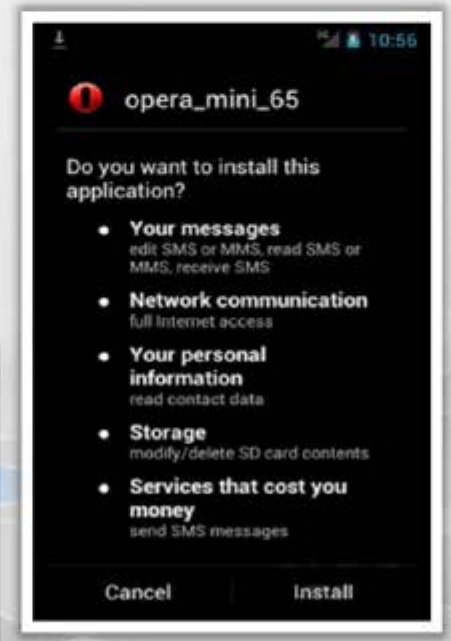
FakeInst

- FakeInst Trojan sends **SMS messages to premium rate phone numbers** or a subscription-based paid service



OpFake

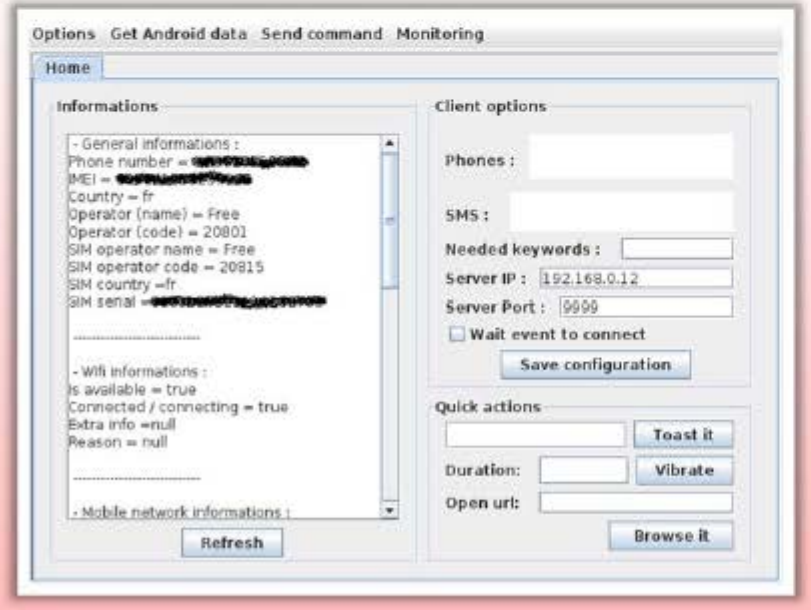
- Android.Opfake is a detection for Trojan horses on the Android platform that send **SMS texts to premium-rate numbers**



Android RAT: AndroRAT and Dendroid

AndroRAT

- AndroRAT allows a remote attacker to **gain control over the device** and steal information from it
- It allows a remote attacker to perform various actions such as **retrieve call log and contact information**, **place a call**, etc.



Dendroid

- Dendroid is a **HTTP RAT** that is marketed as being transparent to the user and firmware interface, having a sophisticated PHP panel, and an application APK binder package
- It **generates a malicious APK file** that can delete call logs, open web pages, etc.

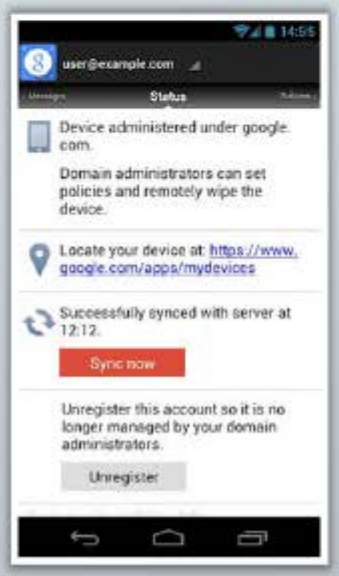
Securing Android Devices

C|EH Certified Ethical Hacker

- ✓ **Enable screen locks** for your Android phone for it to be more secure
- ✗ Do not directly download **Android package files (APK)**
- ✗ Never **root** your Android device
- ✓ Update the **operating system** regularly
- ✓ Download apps only from **official Android market**
- ✓ Use free protector Android app like **Android Protector** where you can assign passwords to text messages, mail accounts, etc.
- ✓ Keep your device updated with **Google Android antivirus software**
- ✓ Customize your **locked home screen** with the user's information

Google Apps Device Policy

1. Google Apps Device Policy app allows Google Apps domain admin to **set security policies for your Android device**
2. It is a device administration app for Google Apps for Business, Education, and Government accounts that makes your **Android device more secure for enterprise use**
3. This app allows IT administrator to **enforce security policies** and remotely wipe your device
4. Additionally, this app allows you to ring, lock, or locate your Android devices through the My Devices page: `https://www.google.com/apps/mydevices`



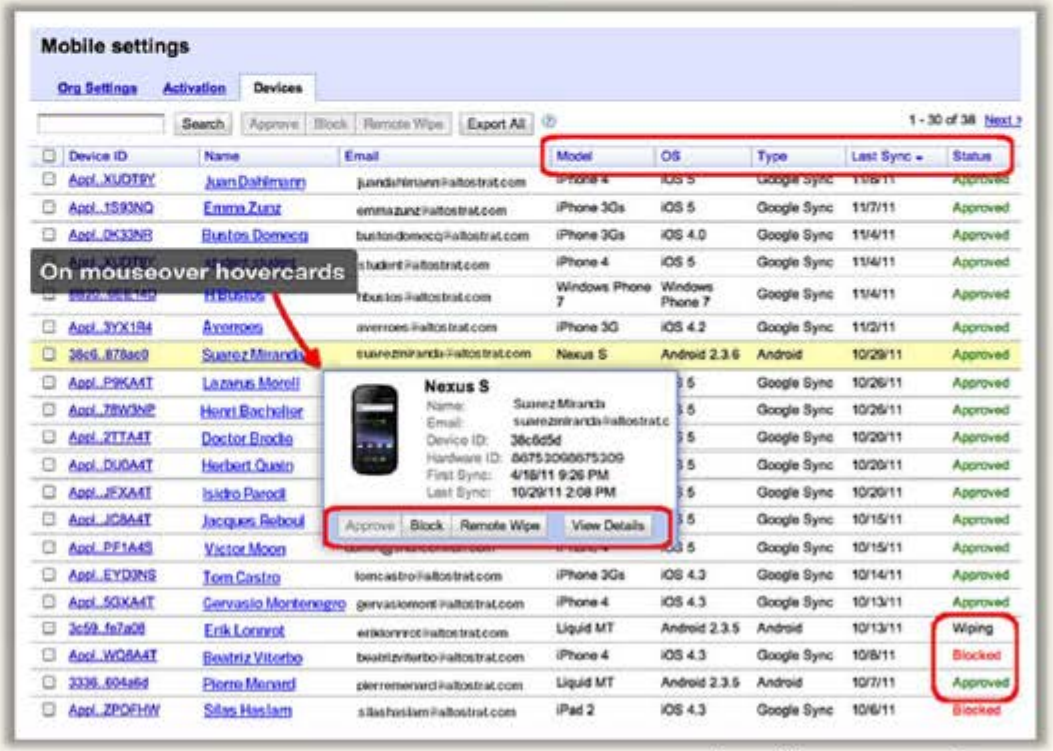
https://play.google.com

Remote Wipe Service: Remote Wipe

- If users have Google Sync installed on a supported mobile device or an Android device with the **Google Apps Device Policy** app, they can use the Google Admin console to remotely wipe the device

To remote wipe a lost or stolen device:

- Sign in to your **Google Admin console**
- Click **Device management** → **Managed devices**
- In the **Devices tab**, hover your cursor over the user whose device you want to wipe
- Click **Remote Wipe** (or **Wipe account**) in the box that appears
- A second box appears asking you to confirm that you want to remotely wipe the device. If you are sure your want to wipe the device, click **Wipe Device** (or **Wipe account**)



http://support.google.com

Android Security Tool: DroidSheep Guard

- DroidSheep Guard **monitors your phones ARP-Table** and **pop-up alerts** in case it detects suspicious entries in the phones ARP-Table
- It can immediately **disable Wi-Fi connection** to protect your accounts
- DroidSheep Guard works with all **ARP-Based attacks**, like DroidSheep and Faceniff

Android Security Tools: TrustGo Mobile Security and Sophos Mobile Security

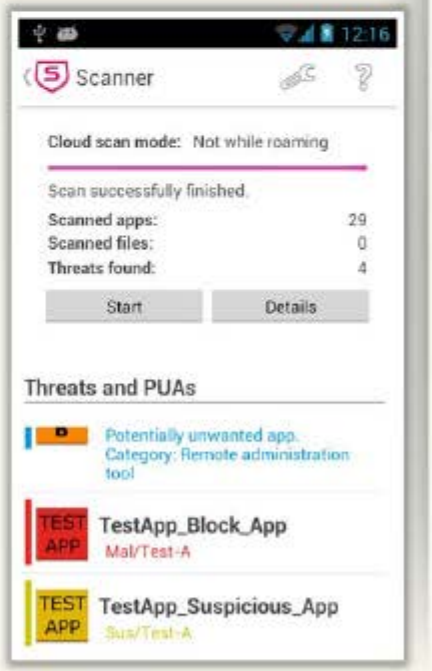
TrustGo Mobile Security

- TrustGo SAFE lets you know which apps are **free from malware** and **risks before you download**

http://www.trustgo.com

Sophos Mobile Security

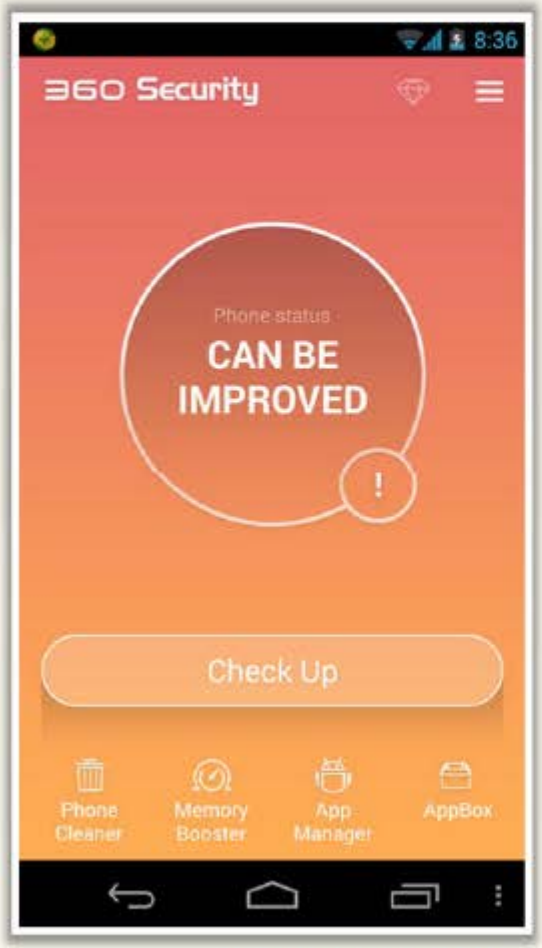
- Sophos Mobile Security protects your Android device **without reducing performance** and helps you **avoid undesirable software**



http://www.sophos.com

Android Security Tools: 360 Security, AVL, and Avira Antivirus Security

360 Security

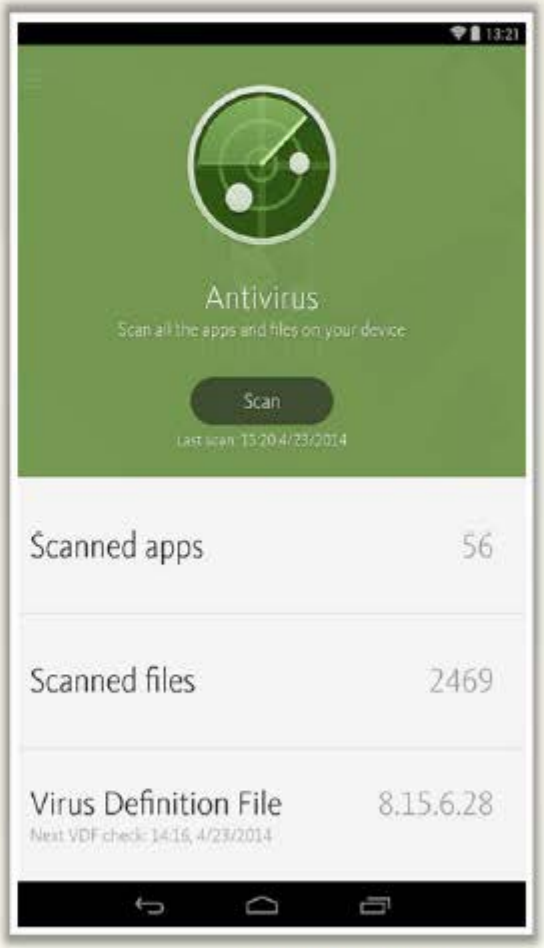


http://www.360safe.com

AVL

http://www.antiy.net

Avira Antivirus Security



http://www.avira.com

Android Vulnerability Scanner: X-Ray

01

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

02

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

03

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

http://www.xray.io

Android Device Tracking Tools

C|EH Certified Ethical Hacker

Find My Phone

http://findmyphone.mangobird.com

Prey Anti-Theft

http://preyproject.com

My AntiTheft

http://myantitheft.com

Wheres My Droid

http://wheresmydroid.com

iHound

https://www.ihoundsoftware.com

GadgetTrak Mobile Security

http://www.gadgettrak.com

Total Equipment Protection App

https://protection.sprint.com

AndroidLost.com

http://www.androidlost.com

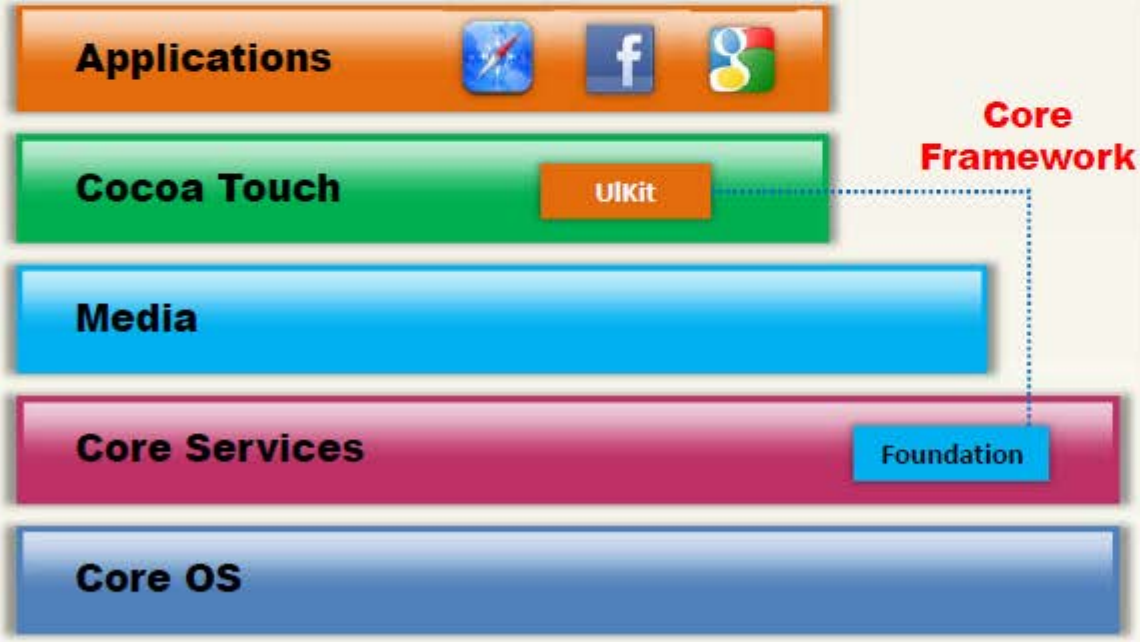
Module Flow

C|EH Certified Ethical Hacker

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Hacking Windows Phone OS
5. Hacking BlackBerry
6. Mobile Device Management
7. Mobile Security Guidelines and Tools
8. 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 an 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

App Platform for Jailbroken Devices: 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

It is a graphical front end to **Advanced Packaging Tool** (APT) and the dpkg package management system, which means that the packages available in Cydia are provided by a **decentralized system of repositories** (also called sources) that list these packages

http://cydia.saurik.com

Jailbreaking Tool: Pangu

Pangu is a jailbreak program and performs an **untethered jailbreak for all devices on iOS 7.1.x**

http://en.pangu.io

Untethered Jailbreaking of iOS 7.1.1/7.1.2 Using Pangu for Mac

CEH Certified Ethical Hacker

1.  Download **Pangu.dmg** application (also available in CEH Tools DVD)

2.  Connect your device running iOS 7.1.1/7.1.2 to your Mac computer via **USB cable** and launch **Pangu.dmg** application

3.  Wait until the device is detected by the Pangu application and then click **Jailbreak** button

4.  A guide will popup asking you adjust your date back in time. Navigate to **Settings** → **General** → **Date & Time** and disable the **Set Automatically** toggle. Press the **date & time** and set the date to **1 June 2014**

5.  Once the date has been adjusted, a **Pangu icon** will appear on your **Springboard**. Tap the icon to launch Pangu app then press **Continue** when prompted to confirm the launch of the application

6.  The Pangu utility will continue with the jailbreak. you will get a prompt to unlock your device once it **reboots**. You will see **Cydia icon** on your device **Home screen**

Jailbreaking Tools: Redsn0w and Absinthe

Redsn0w

- RedSn0w allows you to jailbreak your iPhone, iPod Touch, and iPad running a variety of firmware versions

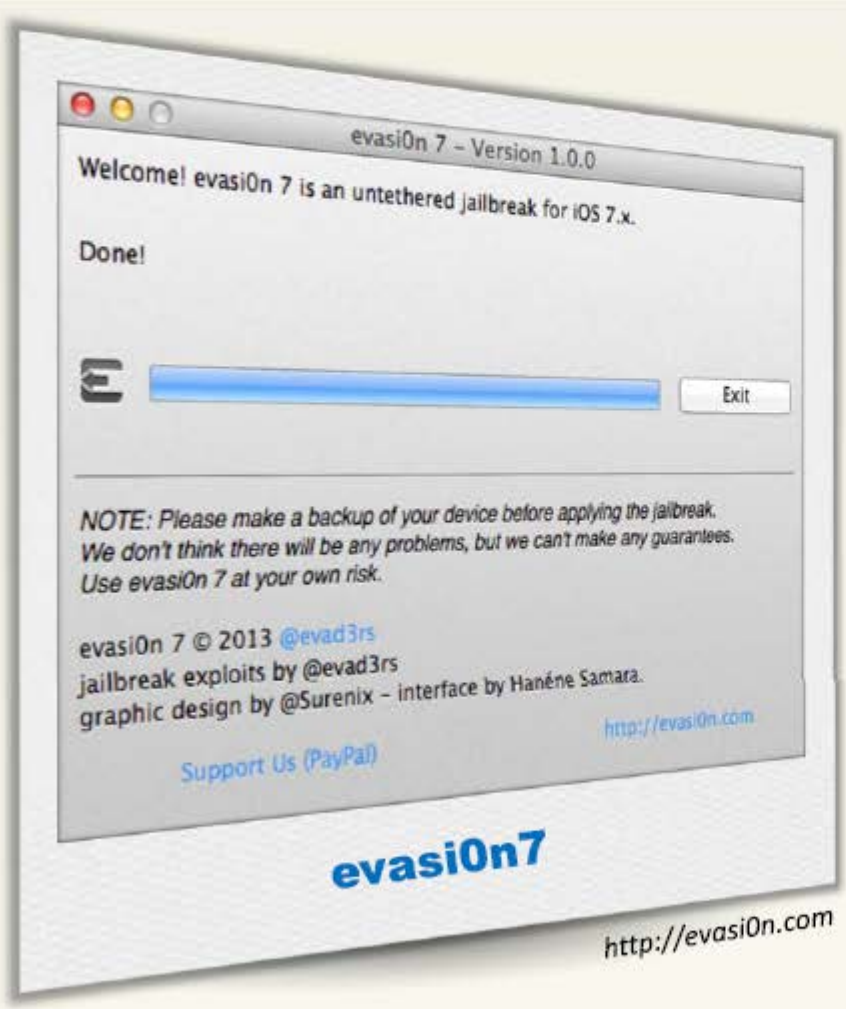
http://redsn0w.info

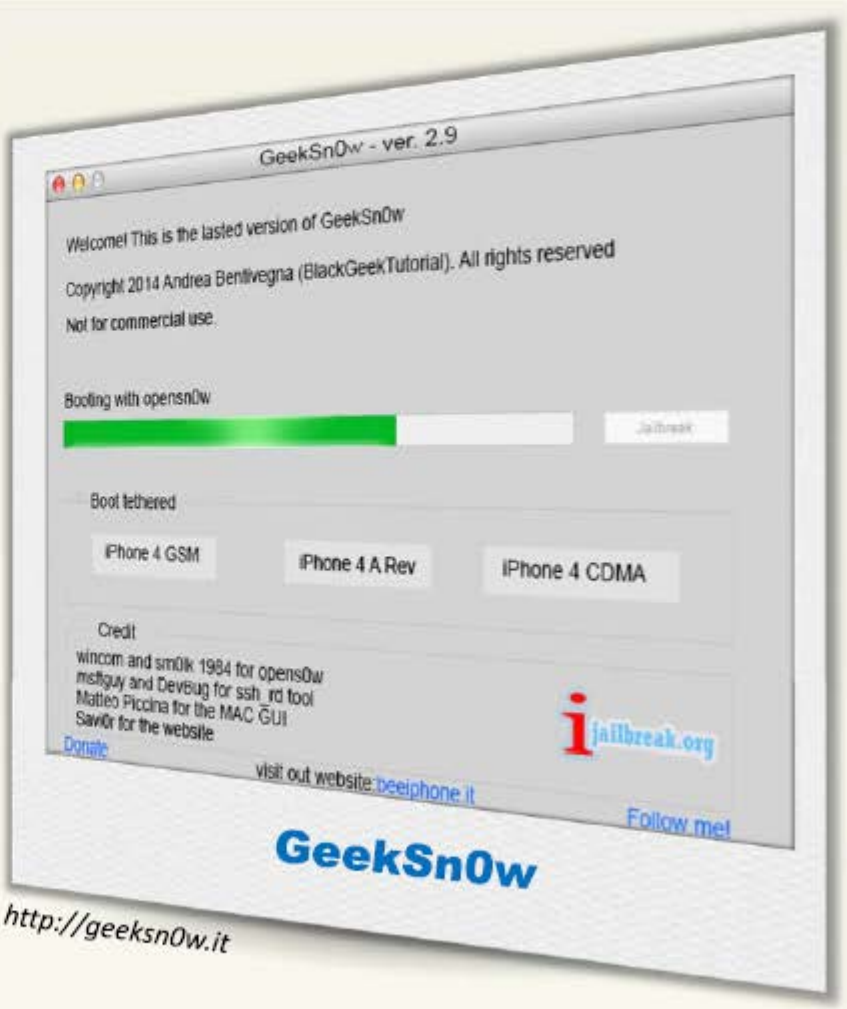
Absinthe

- A jailbreak solution for your iPhone, iPod, iPad, and AppleTV brought to you by Chronic Dev Team

http://greenpois0n.com

Jailbreaking Tools: evasi0n7 and GeekSn0w





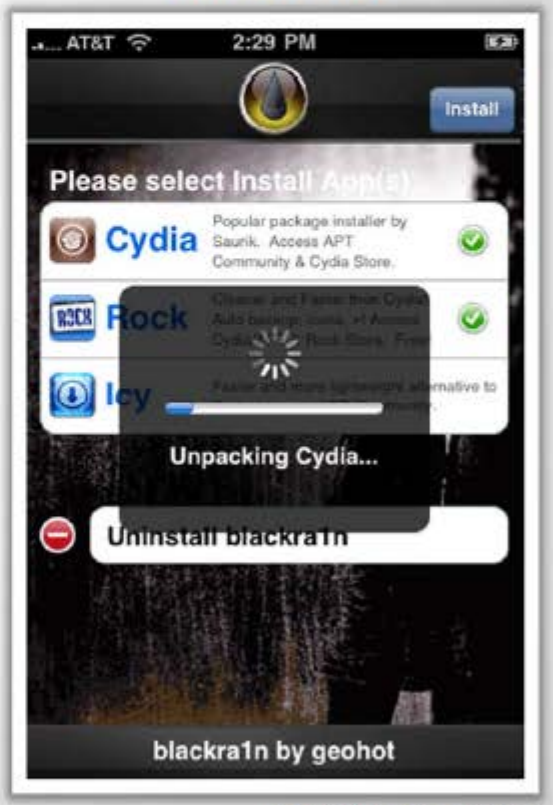
Jailbreaking Tools: Sn0wbreeze and PwnageTool

Jailbreaking Tools: LimeRa1n and Blackra1n

LimeRa1n

http://www.limera1n.com

Blackra1n



http://blackra1n.com

Guidelines for Securing iOS Devices

01 Use **passcode lock** feature for locking iPhone

02 Disable **Javascript** and **add-ons** from web browser

03 Use iOS devices on a **secured** and **protected** Wi-Fi network

04 Do not store sensitive data on **client-side database**

05 Do not access web services on a **compromised network**

06 Do not open **links** or **attachments** from unknown sources

07 Deploy only **trusted** third-party **applications** on iOS devices

08 Change default password of iPhone's **root password** from **alpine**

Guidelines for Securing iOS Devices (Cont'd)

Do not jailbreak or **root your device** if used within enterprise environments

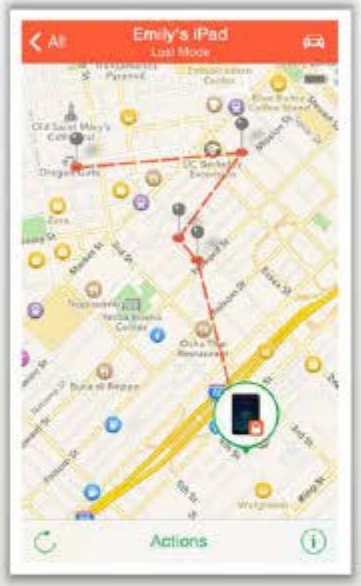
Configure **Find My iPhone** and utilize it to wipe a lost or stolen device

Enable **Jailbreak detection** and also protect access to **iTunes AppleID** and **Google accounts**, which are tied to sensitive data

Disable **iCloud services** so that sensitive enterprise data is not backed up to the cloud (Note that cloud services can back up documents, account information, settings, and messages)

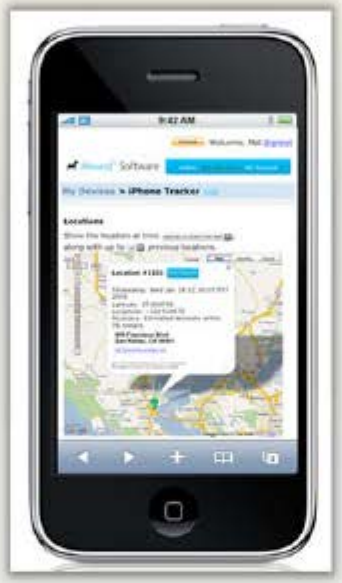
Along with this **follow the common security guidelines** for all the mobile devices outlined in the later slides

iOS Device Tracking Tools



Find My iPhone

https://itunes.apple.com



iHound

https://www.ihoundsoftware.com

GadgetTrak iOS Security

http://www.gadgettrak.com

iLocalis

http://ilocalis.com

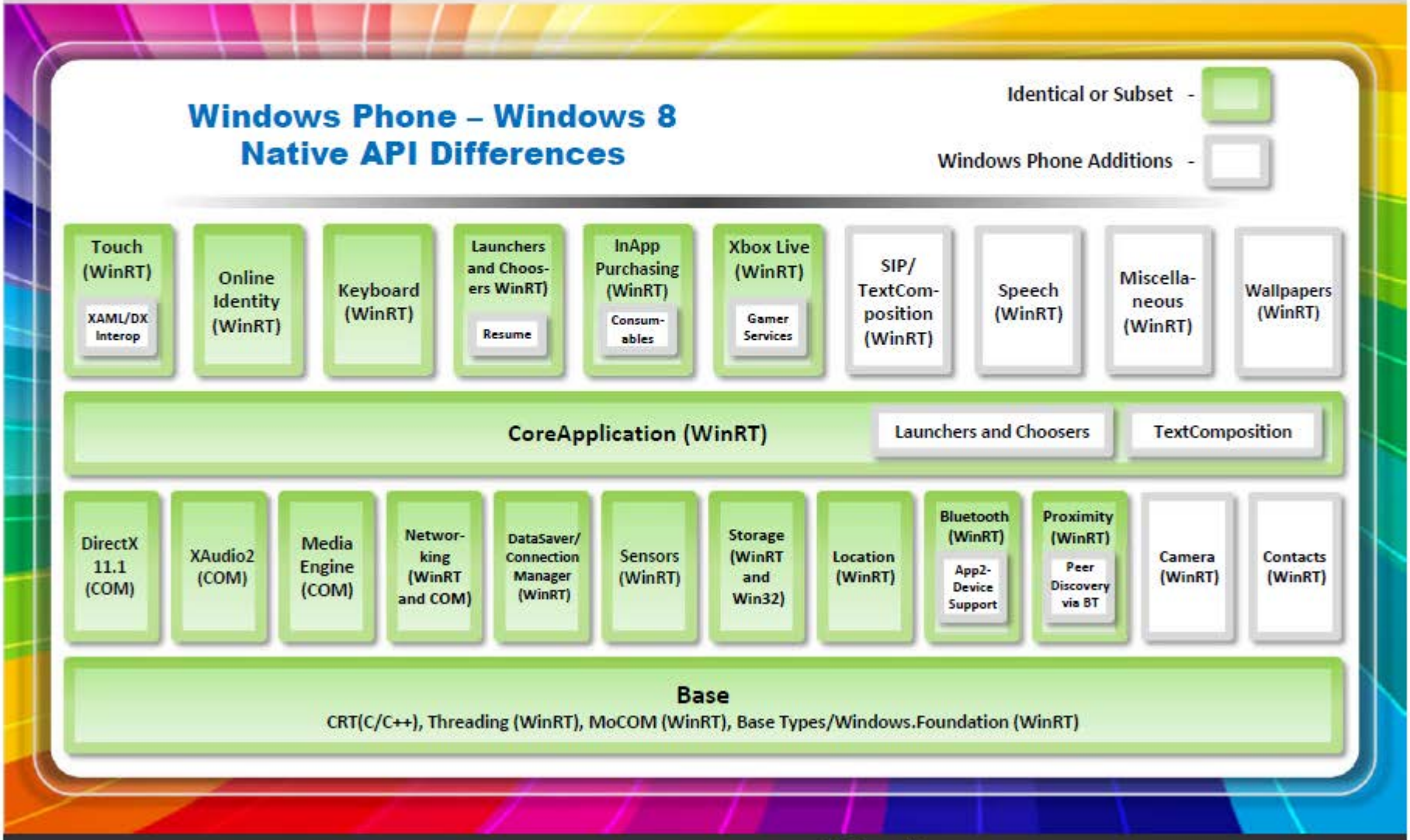
Module Flow

Windows Phone 8

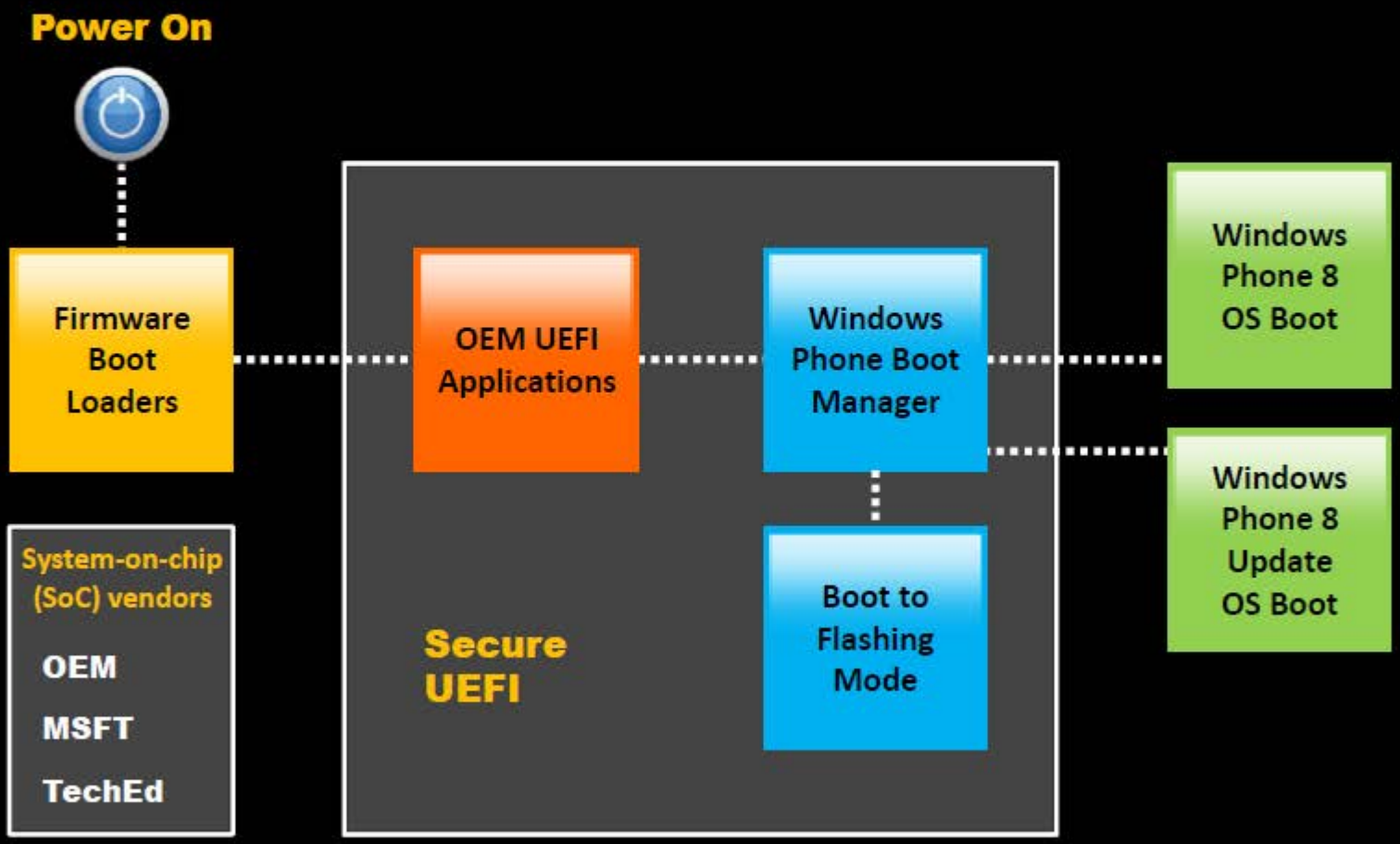
C|EH Certified Ethical Hacker

- It allows devices with larger screens and multi-core processors up to 64
- Trusted shared Windows core and improved support for removable storage
- Core components from Windows 8, including kernel, file system, drivers, network stack, security components, media and graphics support
- Internet Explorer 10, Nokia map technology and background multitasking
- Supports Near field communication (NFC), including payment and content sharing with Windows Phone 8 and Windows 8 machines
- Supports native code (C and C++), simplified porting from platforms such as Android, Symbian, and iOS
- Carrier control and branding of "wallet" element is possible via SIM or phone hardware
- Native 128-bit Bitlocker encryption and remote device management of Windows Phone
- United Extensible Firmware Interface (UEFI) secure boot protocol and Firmware over the air for Windows Phone updates
- Features improved app sandboxing and VoIP and video chat integration for any VoIP or video chat app

Windows Phone 8 Architecture



Secure Boot Process



http://www.uefi.org

Guidelines for Securing Windows OS Devices

Download apps only from trusted sources like **windowsphone.com**

Protect your WP8 **SIM** (Subscriber Identity Module) with a **PIN** (Personal Identification Number)

Setup **passwords** for WP8 **lock** screen and keep your phone updated with WP8 **security updates**

Enable device encryption using **Exchange ActiveSync** (EAS) or **device management policy**

Make sure to **clear** all your **browsing history** from **Internet Explorer**

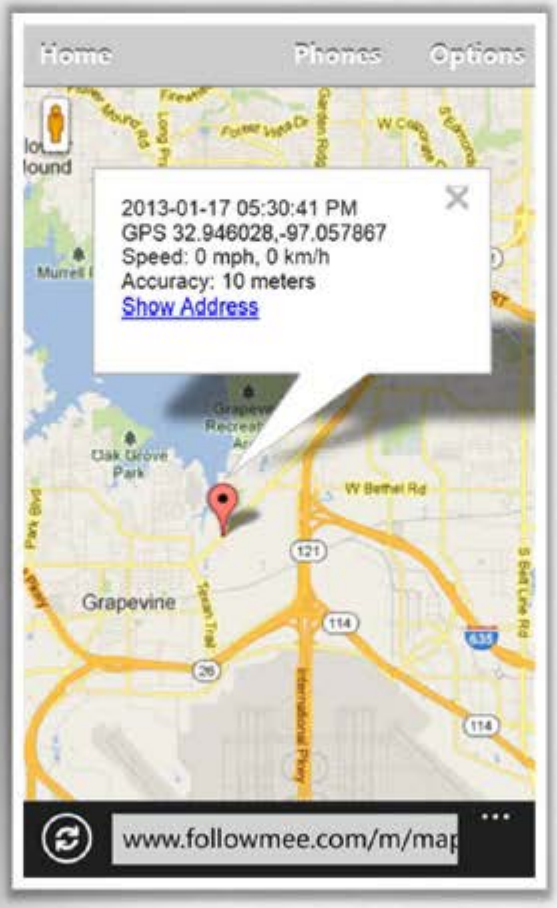
Implement the **chambers concept** for all applications on Windows Phone 8

Try to avoid accessing **password protected** websites in your windows phone while you are in **unsecured Wi-Fi networks**

Implement **trusted Boot and code signing features** on Windows Phone device

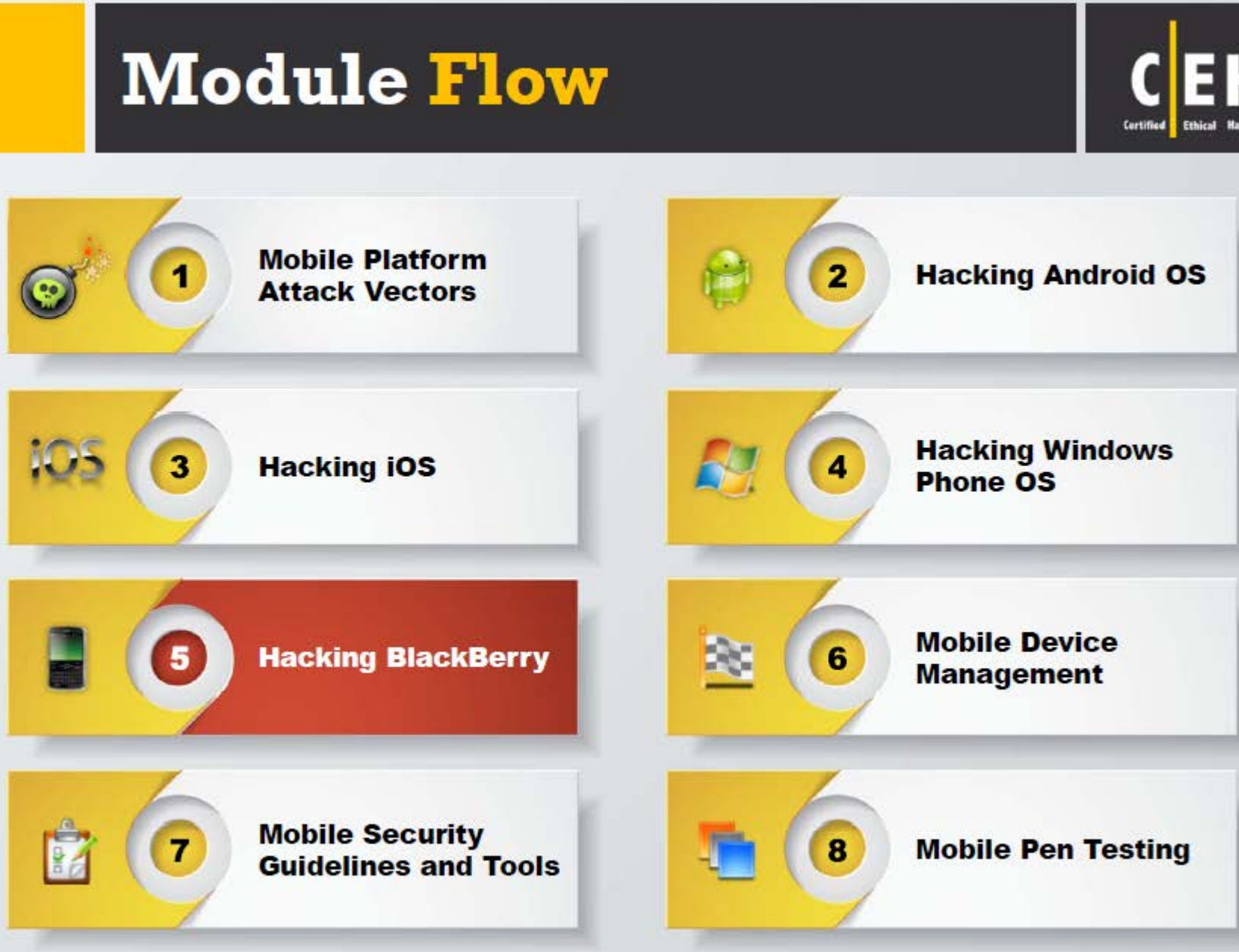
Windows OS Device Tracking Tool: FollowMee GPS Tracker

- GPS Tracker by FollowMee converts your smart phone or tablet into a **GPS tracking device**
- It tracks location of a Windows Phone 8 device, **records locations** (GPS, Wi-Fi, or cellular triangulation) and uploads to a secured server
- Using this app, you can track your **children's movement** daily, follow whereabouts of your **family members** or **employees**
- It supports **multiple mobile platforms**



https://www.followmee.com

Module Flow



BlackBerry Operating System

BlackBerry OS

BlackBerry OS is a proprietary mobile operating system developed by **Research In Motion (RIM)** for its BlackBerry line of smartphones and handheld devices

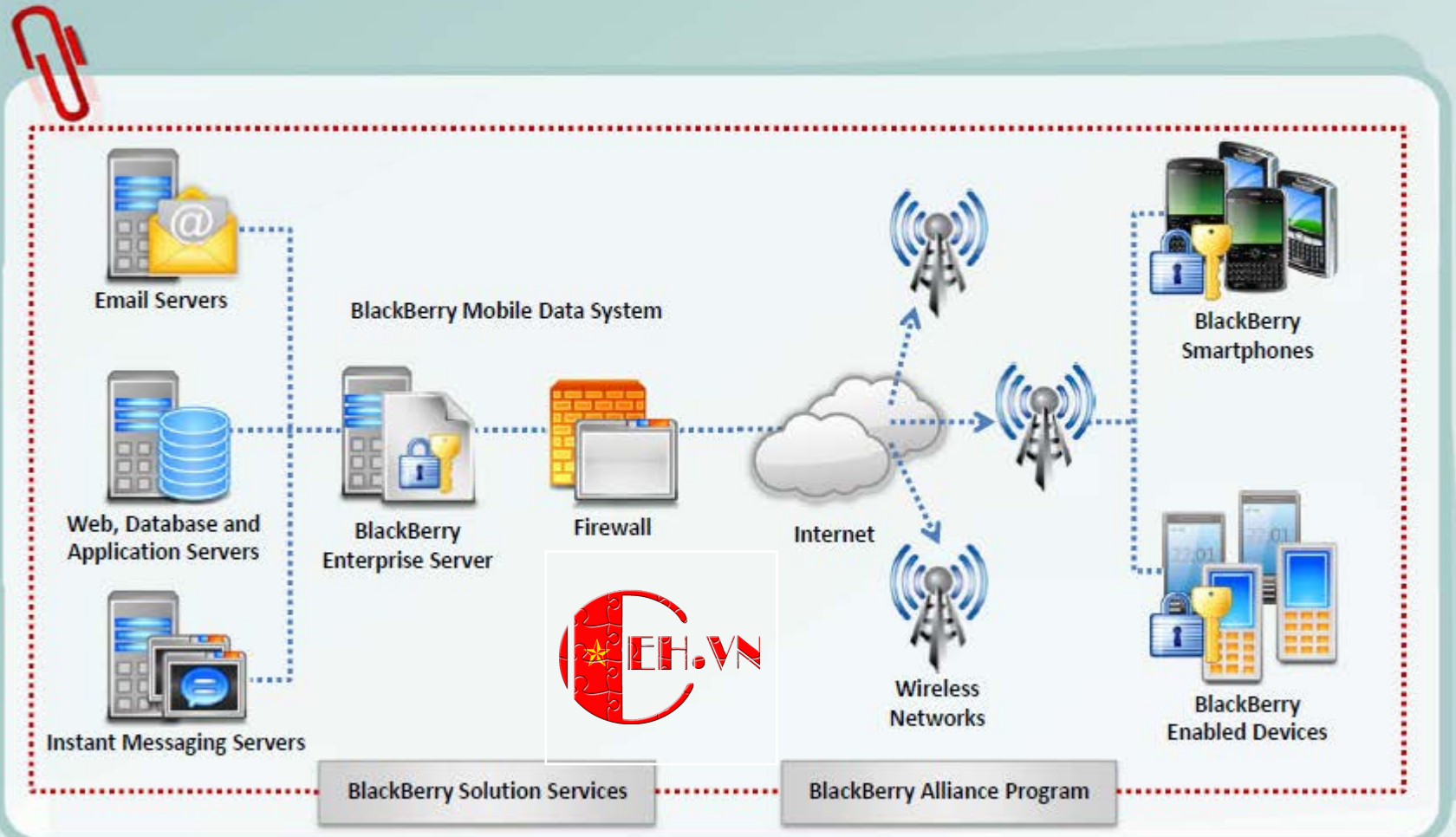
Java Based Application

It includes a Java-based third-party application framework that implements **J2ME Mobile Information Device Profile v2** (MIDP2) and Connected Limited Device Configuration (CLDC), as well as a number of RIM specific APIs

BlackBerry Features

- Native Support for Corporate Email
- BlackBerry Enterprise Server
- BlackBerry Messenger
- BlackBerry Internet Service
- BlackBerry Email Client

BlackBerry Enterprise Solution Architecture



Blackberry Attack Vectors

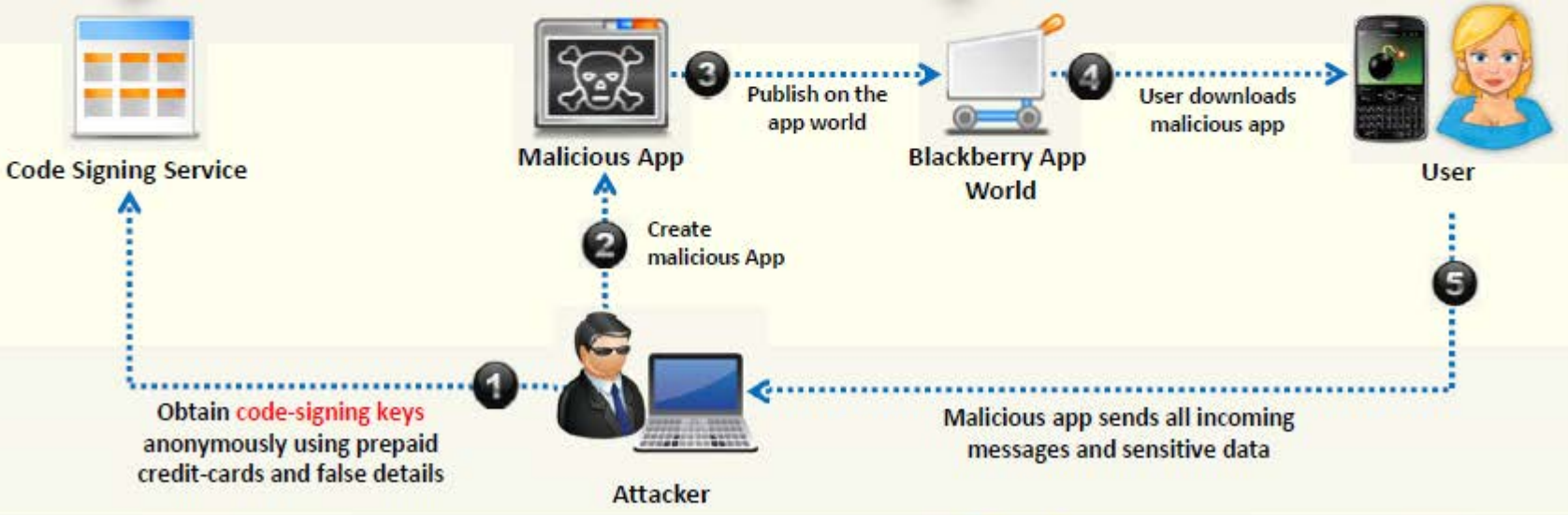
C|EH Certified Ethical Hacker

- Malicious Code Signing
- JAD File Exploits
- Memory and Processes Manipulations
- Email Exploits
- PIM Data Attacks
- Short Message Service (SMS) Exploits
- TCP/IP Connections Vulnerabilities
- Blackberry Malwares
- Telephony Attacks

Malicious Code Signing

- BlackBerry applications must be **signed by RIM** to get full access to the operating system APIs
- If a required signature is missing or the application is altered after signing, the JVM will either **refuse/restrict the API access to the application** or will fail at run-time with an error message

- Attacker can obtain **code-signing keys** anonymously using prepaid credit-cards and false details, sign a malicious application and publish it on the **BlackBerry app world**
- Attackers can also **compromise a developer's system** to steal code signing keys and password to decrypt the encrypted keys



JAD File Exploits and Memory/ Processes Manipulations

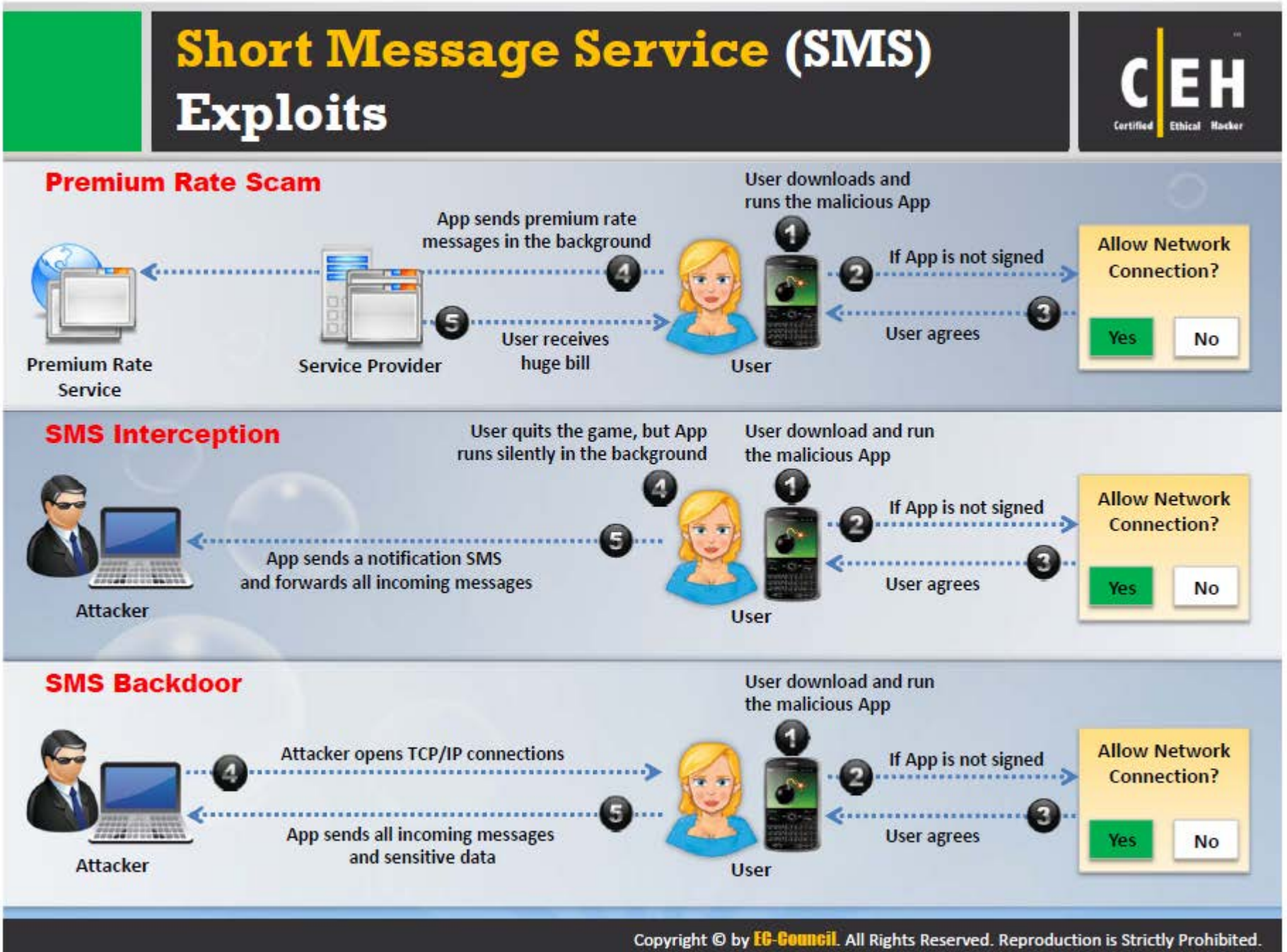
JAD File Exploits

- .jad (Java Application Descriptors) files include the **attributes of a java application**, such as app description, vendor details and size, and provides the URL where the application can be downloaded
- It is used as a standard way to provide **Over The Air (OTA)** installation of java applications on J2ME mobile devices
- Attackers can use specially crafted .jad file with **spoofed information** and trick user to **install malicious apps**

Memory/Processes Manipulations

- Attackers can create malicious applications by creating an **infinite loop**, with a break condition in the middle that will always be false to bypass compiler verification
- It will cause a **denial-of-service (DoS) attack** when the malicious application is run rendering the device unresponsive

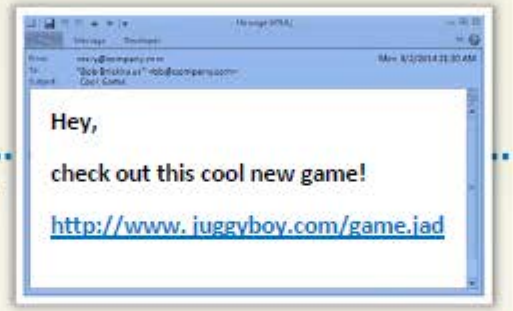
Short Message Service (SMS) Exploits



Email Exploits

Attacker

2 Sends an email to a BlackBerry user



.cod file installs itself as a start-up process with no icon

4

Prompts to download and install the .cod file 3

User

1 Hosts malicious .cod application file on a web server: http://www. juggyboy.com/game.cod along with matching .jad file: http://www. juggyboy.com/ game.jad

Web Server

5

Users Contact List

.cod file enumerates the contact list, and forwards the email to everyone on the list

PIM Data Attacks and TCP/IP Connections Vulnerabilities

PIM Data Attacks

- Personal Information Manager (PIM) data in the PIM database of a BlackBerry device includes **address books**, **calendars**, tasks, and memo pads information
- Attackers can create **malicious signed application** that read all the PIM data and send it to an attacker using different **transport mechanisms**
- The malicious applications can also **delete or modify the PIM data**

TCP/IP Connections Vulnerabilities

- If the device firewall is off, signed apps can **open TCP connections** without the user being prompted
- Malicious apps installed on the device can **create a reverse connection with the attacker** enabling him to utilize the infected device as a TCP proxy and gain access to organization's internal resources
- Attackers can also exploit the reverse TCP connection for backdoors and perform various **malicious information gathering attacks**

Guidelines for Securing BlackBerry Devices

Use **content protection** feature for protecting data on the BlackBerry Enterprise Network

Enterprises should follow a **security policy** for managing BlackBerry devices

Use **password encryption** for protecting files on BlackBerry devices

Maintain a **monitoring mechanism** for the network infrastructure on BlackBerry Enterprise Networks

Use **BlackBerry Protect** or other security apps for securing confidential data

Disable **unnecessary applications** from BlackBerry Enterprise Networks

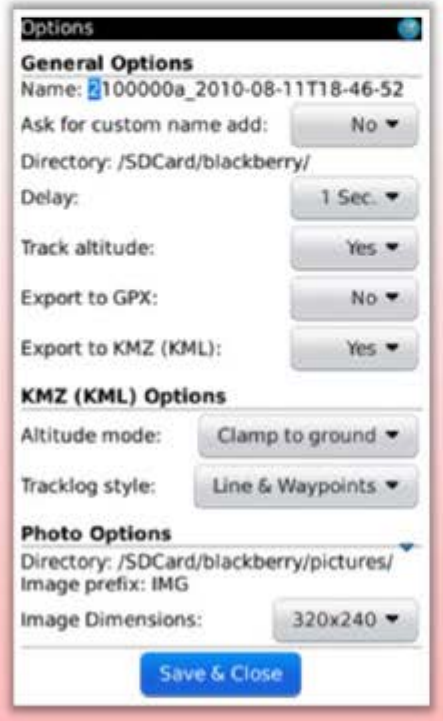
Enable **SD-card/Media card encryption** for protecting data

Provide training on **security awareness and attacks** on handheld devices on BlackBerry Enterprise Networks

BlackBerry Device Tracking Tools: MobileTracker and Position Logic Blackberry Tracker

MobileTracker

http://www.skylab-mobilesystems.com

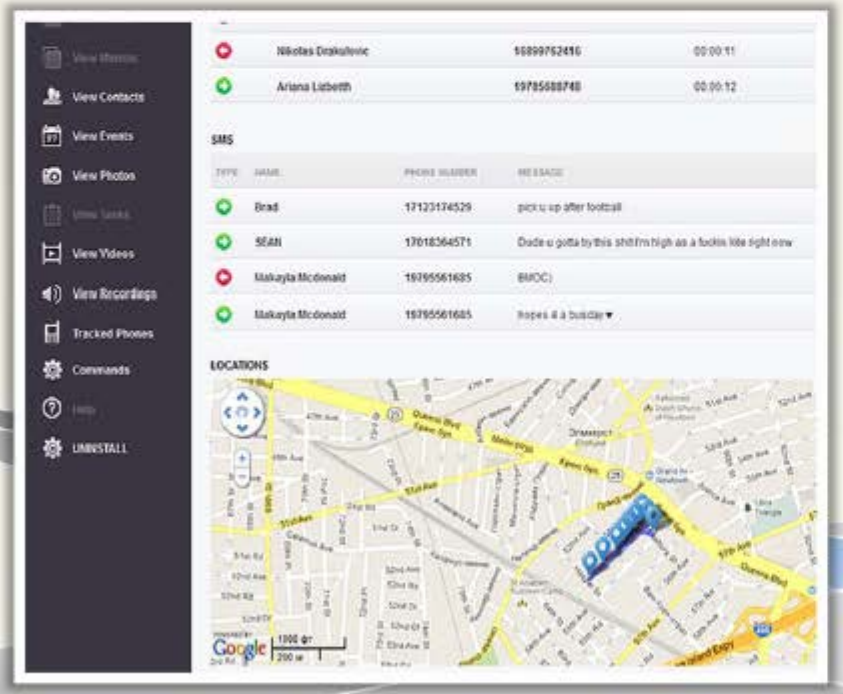


Position Logic Blackberry Tracker

http://www.positionlogic.com

Mobile Spyware: mSpy and StealthGenie

mSpy



http://www.mspy.com

StealthGenie

http://www.stealthgenie.com

Mobile Spyware

Mobile Spy
http://www.mobile-spy.com

SpyBubble
http://www.spybubble.com

Mobistealth
http://www.mobistealth.com

FlexiSPY
http://www.flexispy.com

Highster Mobile
http://www.highstermobile.com

SpyPhoneTap
http://www.spyphonetap.com

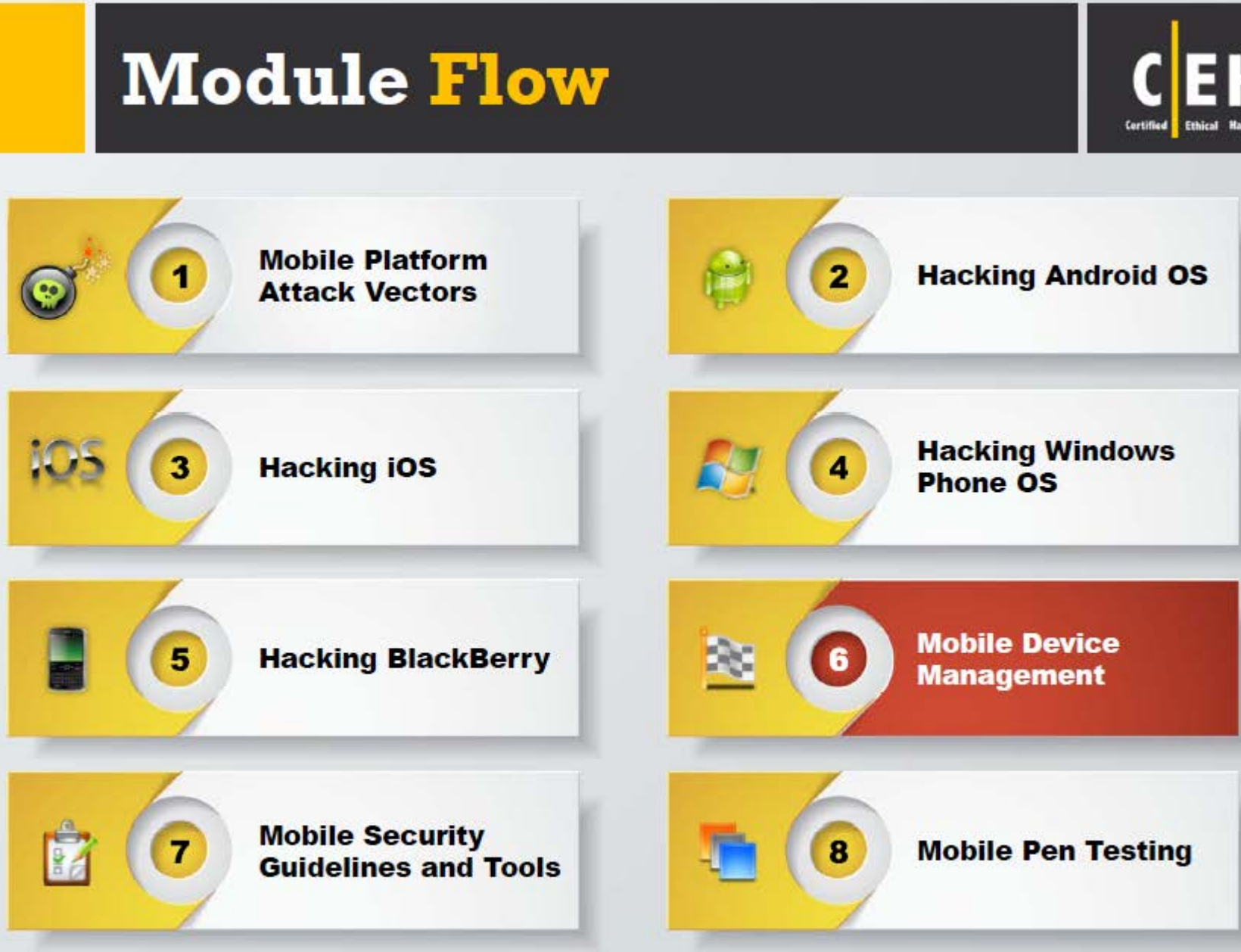
Spyera
http://spyera.com

PhoneSheriff
http://www.phonesheriff.com

My Mobile Watchdog
https://www.mymobilewatchdog.com

SpyToMobile
http://spytomobile.com

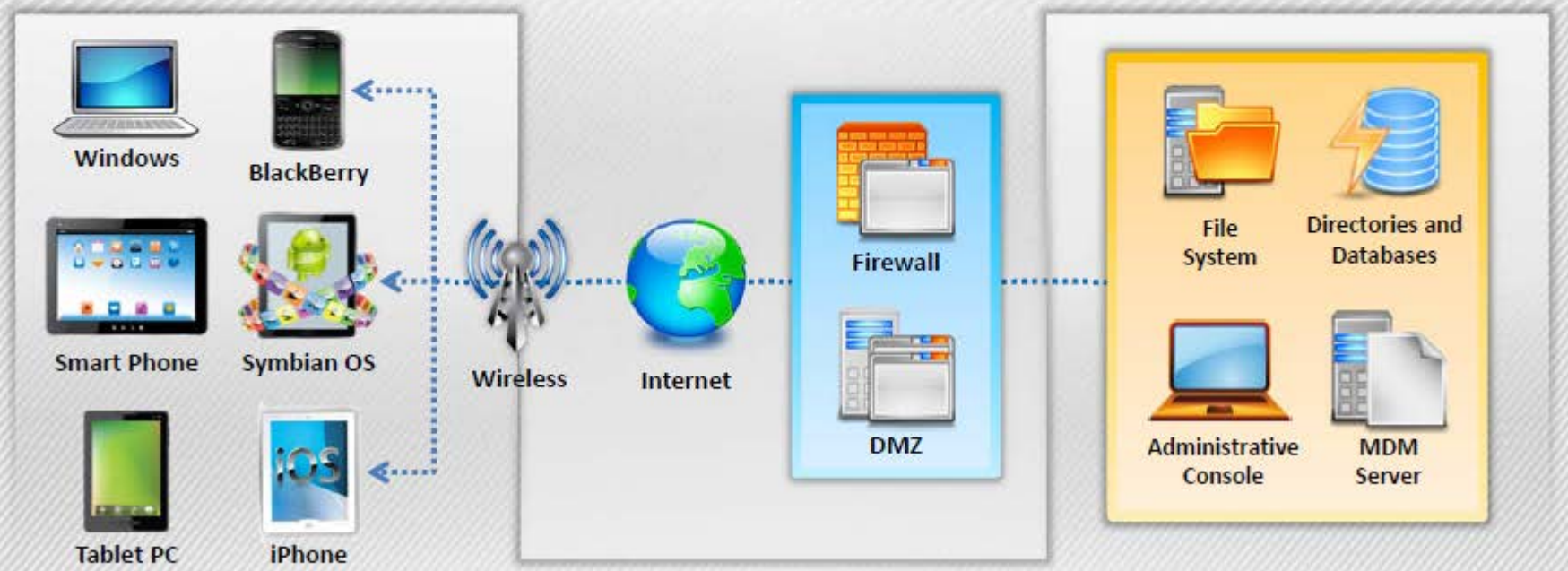
Module Flow



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

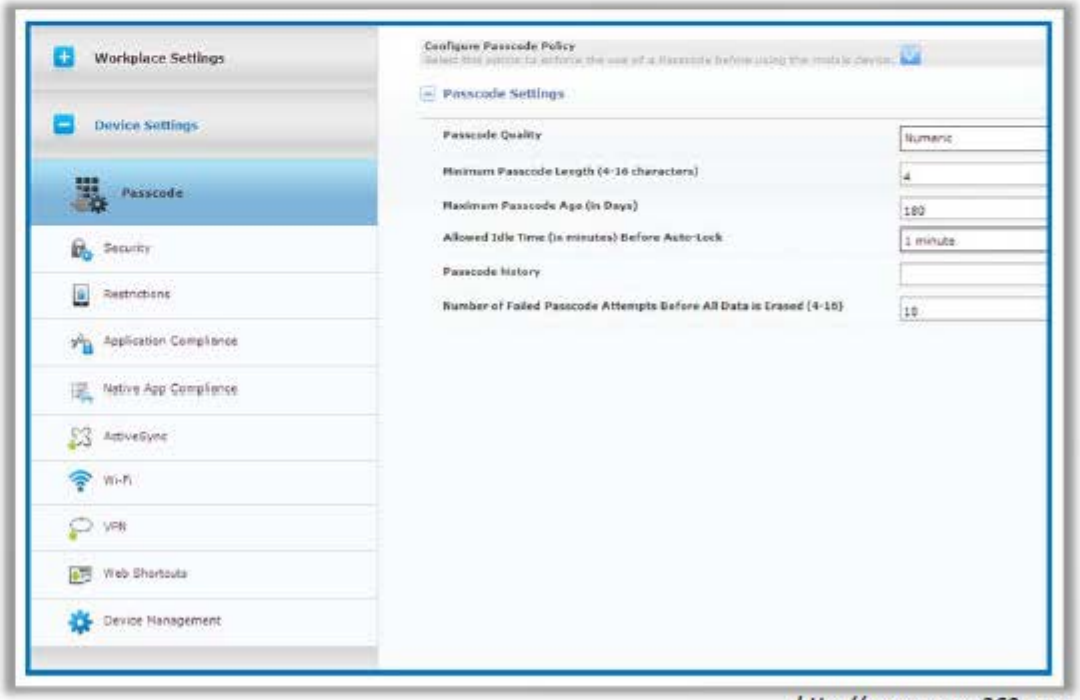
- It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and supports mobile devices
- It can be used to **manage both company-owned and employee-owned (BYOD) devices** across the enterprise



MDM Solution: MaaS360 Mobile Device Management (MDM)

01 MaaS360 supports the complete **mobile device management (MDM) lifecycle** for smartphones and tablets including iPhone, iPad, Android, Windows Phone, BlackBerry, and Kindle Fire

02 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



http://www.maas360.com

MDM Solutions

XenMobile
http://www.citrix.com

Absolute Manage MDM
http://www.absolute.com

SAP Afaria
http://www.sybase.com

Device Management Centre
http://www.sicap.com

AirWatch
http://www.air-watch.com

Good Mobile Manager
http://www1.good.com

MobileIron
http://www.mobileiron.com

Tangoe MDM
http://www.tangoe.com

MobiControl
https://www.soti.net

MediaContact
http://www.device-management-software.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 allow employees to use the devices that they are **comfortable with** and **best fits his/her preferences** and work purposes

BYOD Risks

Sharing confidential data on unsecured network	Data leakage and endpoint security issues
Improperly disposing device	Support of many different devices
Mixing personal and private data	Lost or stolen devices
Lack of awareness	Ability to bypass organizations network policy rules
Infrastructure issues	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**

Make it clear **who owns what apps and data**

Make it clear **what apps will be allowed or banned**

Do not allow **jailbroken and rooted devices**

Educate your employees about the BYOD policy

Use encrypted channel for data transfer

Control access based on the need-to-know

Apply **session authentication and timeout policy** on access gateways

BYOD Security Guidelines for Employee

Use encryption mechanism to store data

Maintain a clear 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

Module Flow

C|EH Certified Ethical Hacker

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

General Guidelines for Mobile Platform Security

Do not load too many **applications** and avoid auto-upload of photos to **social networks**

Securely **wipe or delete** the data disposing of the device

Perform a **Security Assessment** of the Application **Architecture**

Ensure that your **Bluetooth** is "**off**" by default. Turn it on when ever it is necessary

Maintain **configuration** control and **management**

Do not share the information within **GPS-enabled apps** unless they are necessary

Install applications from trusted application **stores**

Never connect two separate networks such as **Wi-Fi** and **Bluetooth** simultaneously

General Guidelines for Mobile Platform Security (Cont'd)

C|EH Certified Ethical Hacker

1 Use Passcode

- Configure a **strong passcode** with maximum possible length to gain access to your mobile devices
- Set an idle **timeout** to automatically lock the phone when not in use
- Enable **lockout/wipe** feature after a certain number of attempts

2 Update OS and Apps

3 Enable Remote Management

- In an enterprise environment, use **Mobile Device Management (MDM) software** to secure, monitor, manage, and support mobile devices deployed across the organization

4 Do not allow Rooting or Jailbreaking

- Ensure your MDM solutions prevent or detect **rooting/jailbreaking**
- Include this clause in your **mobile security policy**

5 Use Remote Wipe Services

- Use **remote wipe services** such as Remote Wipe (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen

6 Encrypt Storage

- If supported, configure your mobile device to encrypt its storage with **hardware encryption**

General Guidelines for Mobile Platform Security (Cont'd)

Perform periodic backup and synchronization	• Use a secure, **over-the-air backup-and-restore tool** that performs periodic background synchronization
Filter e-mail-forwarding barriers	• Filter email/emails by configuring **server-side settings** of the corporate email/emails system • Use **commercial data loss prevention filters**
Configure Application certification rules	• Allow only **signed applications** to install or execute
Harden browser permission rules	• Harden browser permission rules according to **company's security policies** to avoid attacks
Design and implement mobile device policies	• Set a policy that defines the **accepted usage**, **levels of support**, and **type of information access permitted** on different devices

General Guidelines for Mobile Platform Security (Cont'd)

C|EH Certified Ethical Hacker

- Set require passcode to immediately
- Thwart passcode guessing: set erase data to ON
- Enable auto-lock and set to one minute
- Encrypt the device and backups
- Configure wireless to ask to join networks
- Perform regular software maintenance
- Control the location of backups
- Control devices and applications
- Prohibit USB keys
- Encrypt backups
- Prevent local caching of email
- Sandbox application and data

General Guidelines for Mobile Platform Security (Cont'd)

1. Disable the collection of **Diagnostics and Usage Data** under **Settings** → **General** → **About**
2. Apply **software updates** when new releases are available
3. Limit **logging data** stored on device
4. Use **device encryption** and **patch** applications
5. Managed **operating environment**
6. Managed **application environment**
7. Press the **power button** to lock the device whenever it is not in use
8. Verify the **location of printers** before printing sensitive documents
9. Utilize a **passcode lock** to protect access to the mobile device - consider the eight character non-simple passcode
10. Report a **lost or stolen device to IT** so they can disable certificates and other access methods associated with the device

General Guidelines for Mobile Platform Security (Cont'd)

C|EH Certified Ethical Hacker

1. Consider the **privacy implications** before enabling location-based services and limit usage to trusted applications
2. Keep **sensitive data off** of shared mobile devices. If enterprise information is locally stored on a device, it is recommended that this device not be openly shared
3. Ask your IT department how to use **Citrix technologies** to keep data in the data center and keep personal devices personal
4. If you must have sensitive data on a mobile device, use **follow-me data** and **ShareFile** as an enterprise-managed solution
5. (Android) Backup to **Google Account** so that sensitive enterprise data is not backed up to the cloud
6. **Configure location services** to disable location tracking for applications that you do not want to know your location information
7. **Configure notifications** to disable the ability to view notifications while the device is locked for applications that could display sensitive data
8. **Configure AutoFill** - Auto-fill Names and Passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by enterprise policy)

Mobile Device Security
Guidelines for Administrator

C|EH Certified Ethical Hacker

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

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

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

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

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

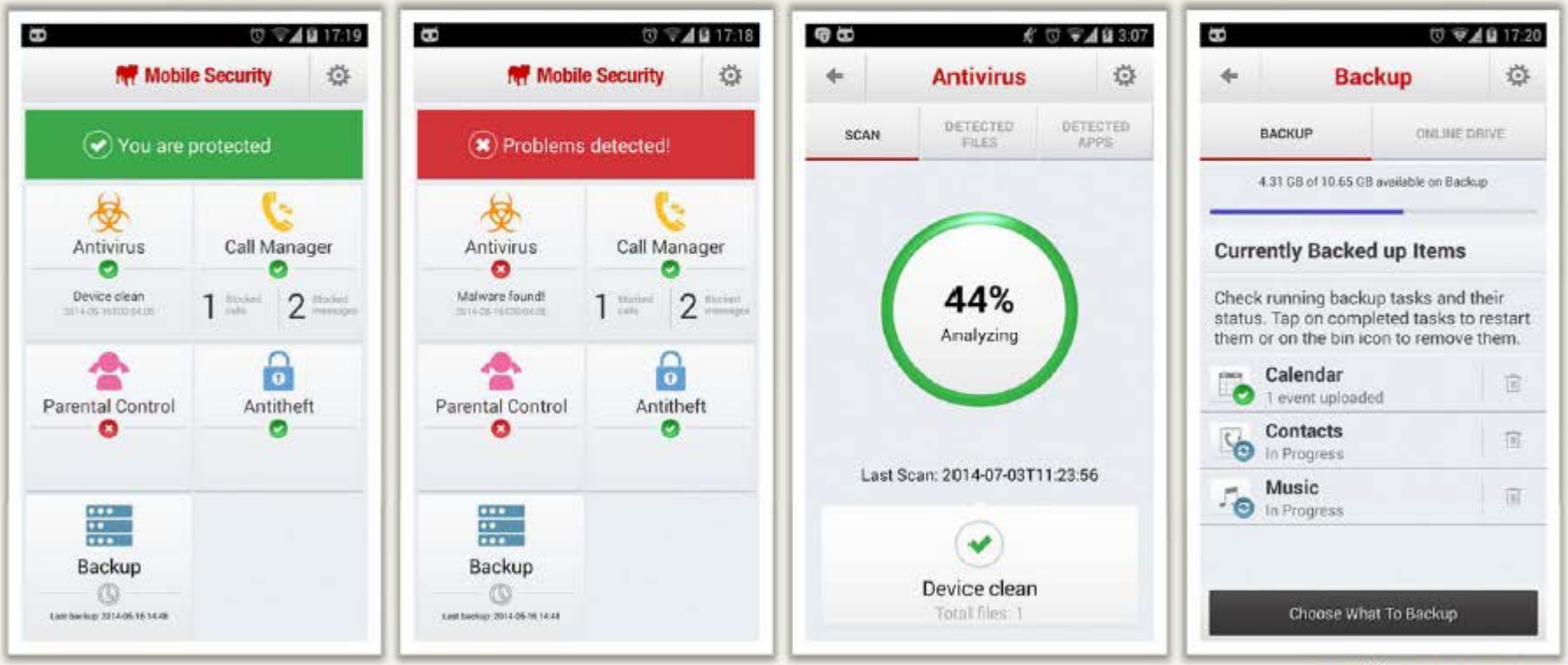
Enable the "**block texts from the internet**" feature from your provider

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

Never call a number left in a SMS

Mobile Protection Tool: 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**



http://www.bullguard.com

Mobile Protection Tool: Lookout

C|EH Certified Ethical Hacker

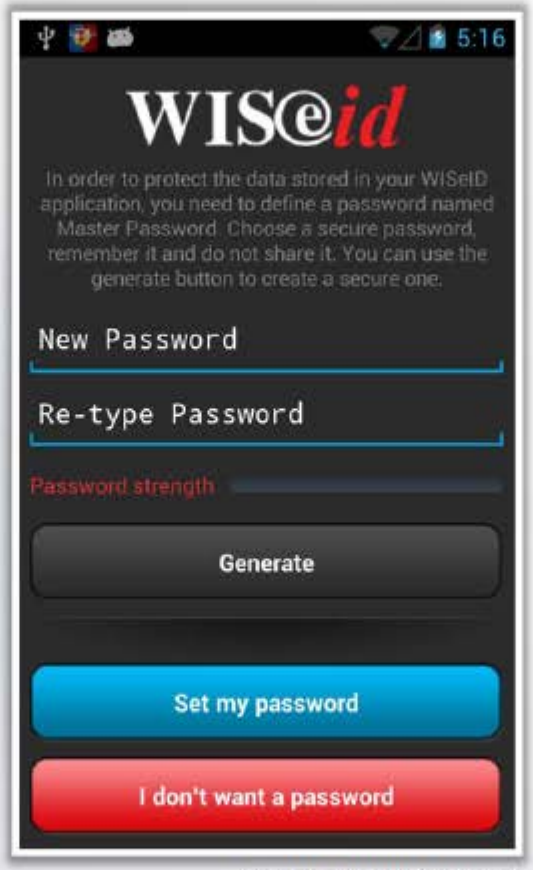
Lookout protects your phone from mobile threats

Security and Privacy	Helps avoid risky behavior, like connecting to an unsecured Wi-Fi network, downloading a malicious app
Backup	Provides safe, secure and seamless backup of your mobile data, automatically over the air
Missing Device	Helps you find your phone if it's lost or stolen
Manage-ment	Allows you to remotely manage your phone

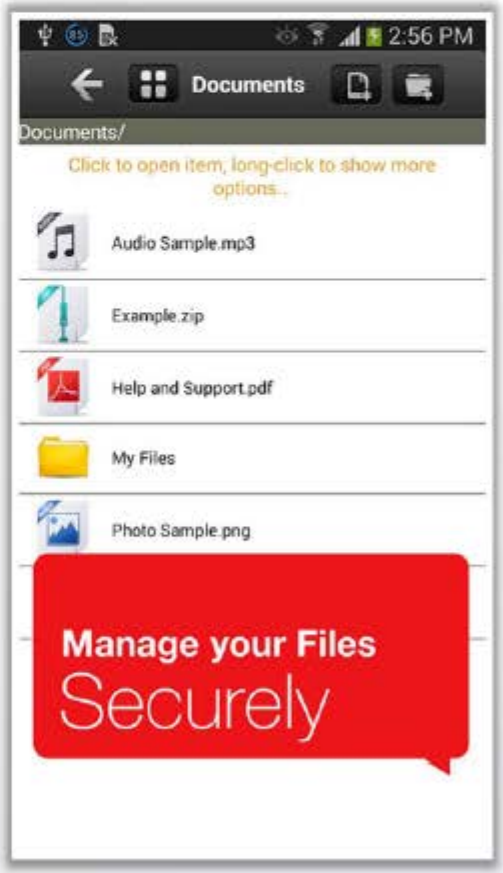
https://www.lookout.com

Mobile Protection Tool: WISeID

- WISeID provides secure and easy-to-use **encrypted storage for personal data**, personally identifiable information (PII), PINs, credit and loyalty cards, notes, and other information
- WISeID allows you to store your web sites, user names and passwords and quickly log on to your **favourite websites** through your mobile device



http://www.wiseid.com



Mobile Protection Tool: zIPS

- zIPS employs machine-learning to **detect abnormal behavior** and isolate your device before any exploit can take place
- zIPS is equipped with a **behavioral analysis engine** to automatically detect and block malicious threats by monitoring how they change the characteristics of the mobile device
- It **scans all mobile applications** and browsers to enhance the security of user device and keeps your whole organization safe from MITM, IPv4 and even IPv6 attacks

ZIMPERIUM MOBILE DEFENSE

https://www.zimperium.com

Mobile Protection Tools

C|EH Certified Ethical Hacker

McAfee Mobile Security
http://home.mcafee.com

AVG AntiVirus Pro for Android
http://www.avg.com

avast! Mobile Security
http://www.avast.com

Norton Mobile Security
http://us.norton.com

ESET Mobile Security
http://www.eset.com

Kaspersky Internet Security for Android
http://www.kaspersky.com

F-Secure Mobile Security
http://www.f-secure.com

Trend Micro™ Mobile Security
http://www.trendmicro.com

Comodo Mobile Security
http://www.comodo.com

Bitdefender Mobile Security
http://www.bitdefender.com

Mobile Anti-Spyware

SeCore Security

http://www.secorelab.com

AntiSpy Mobile

http://www.antispymobile.com

Malwarebytes Anti-Malware Mobile

https://www.malwarebytes.org

Module Flow

Android Phone Pen Testing

C|EH Certified Ethical Hacker

START

Root an Android Phone

- Try to Root an Android Phone to gain the administrative access to the Android devices using tools such as **SuperOneClick**, **Superboot**, **One Click Root**, **Kingo Android ROOT**, etc.

Perform DoS and DDoS Attacks

- Use tool **AnDOSid** to perform DoS and DDoS attacks on Android phone

Check for vulnerabilities in Android browser

- 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 for vulnerabilities in SQLite

- 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

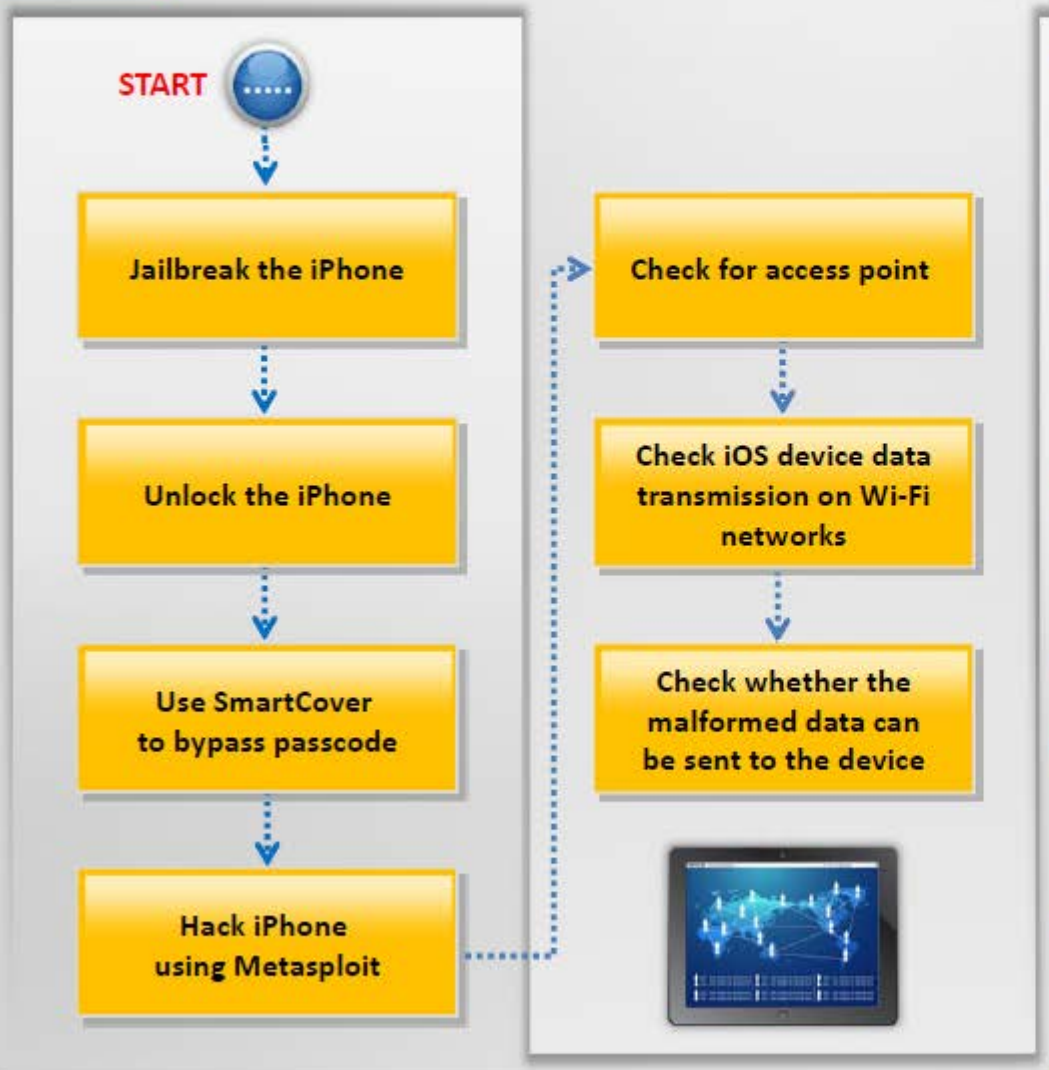
Check for vulnerabilities in Intents

- Try to **exploit Android Intents** to obtain the user's private information
- You can use **ComDroid** tool to detect application's communication vulnerabilities

Detect capability leaks in Android devices

- Use tool **Woodpecker** to detect capability leaks in Android devices

iPhone Pen Testing



- Try to Jailbreak the iPhone using tools such as **Pangu**, **evasi0n7**, **Redsn0w**, **Absinthe**, **Sn0wbreeze**, **PwnageTool**, etc.
- Unlock the iPhone using tools such as **iPhoneSimFree** and **anySIM**
- 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

Windows Phone Pen Testing

START

Try to turn off the phone by sending an SMS

- **Send an SMS** to the phone which turns off the mobile and reboots again

Try to jailbreak Windows phone

- Use **WindowBreak** program to jailbreak/unlock Windows phone

Check for on-device encryption

- Check whether the data on phone can be accessed without **password or PIN**

Check for vulnerability in Windows phone Internet Explorer

- Check whether the **flaw in CSS function** in Internet Explorer allows attackers to gain full access over the phone through **remote code execution**

BlackBerry Pen Testing

- **Perform blackjacking on BlackBerry**
  - Use **BBProxy** tool to hijack BlackBerry connection
- **Check for flaws in application code signing process**
  - Obtain **code-signing keys** using prepaid credit-cards and false details, sign a malicious application and publish it on the **Blackberry app world**
- **Perform email exploit**
  - Send mails or messages to trick a user to download **malicious .cod application file** on the BlackBerry device
- **Perform DOS attack**
  - Try sending malformed **Server Routing Protocol (SRP) packets** from BlackBerry network to the router to cause DOS attack
- **Check for vulnerabilities in BlackBerry Browser**
  - Send **maliciously crafted web links** and trick users to open links containing malicious web pages on the BlackBerry device
- **Search for password protected files**
  - Use tools such as **Elcomsoft Phone Password Breaker** that can recover password protected files, backups from BlackBerry devices

Mobile Pen Testing Toolkit: zANTI

1. zANTI is a comprehensive **network diagnostics toolkit** that enables complex audits and penetration tests

2. It provides **cloud-based reporting** that walks you through simple guidelines to ensure network safety

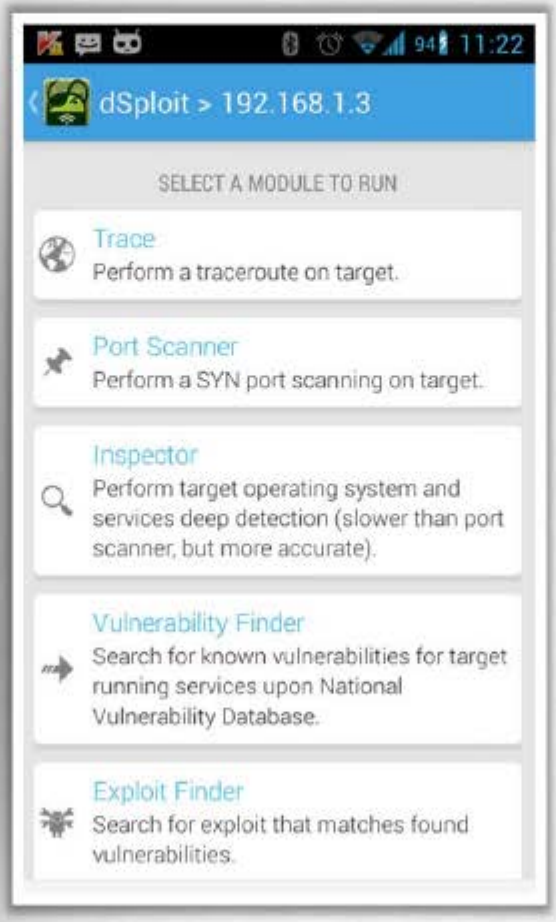
3. It offers a comprehensive range of fully customizable scans to **reveal everything** from authentication, backdoor and brute-force attempts to database, DNS and protocol-specific attacks – including rogue access points

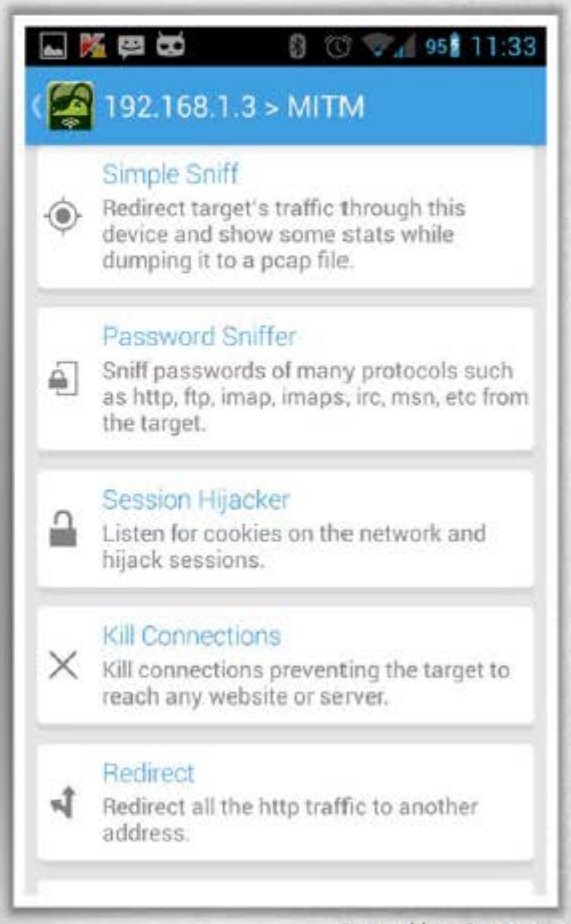
4. It produces an **Automated Network Map** that shows any vulnerabilities of a given target

https://www.zimperium.com

Mobile Pen Testing Toolkit: dSploit

- dSploit is an Android network analysis and penetration suite which aims to offer to IT security experts/geeks the most complete and advanced professional toolkit to **perform network security assessments on a mobile device**
- **Features**
  - Wi-Fi scanning and common router key cracking
  - Deep inspection
  - Vulnerability search
  - MITM multi protocol password sniffing
  - MITM HTTP/HTTPS session hijacking





http://dsploit.net

Mobile Pen Testing Toolkit: Hackode (The Hacker's Toolbox)

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 in 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 an iOS devices
- Attacker can obtain code-signing keys anonymously using prepaid credit-cards and false details, sign a malicious application, and publish it on the Blackberry app world
- 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.