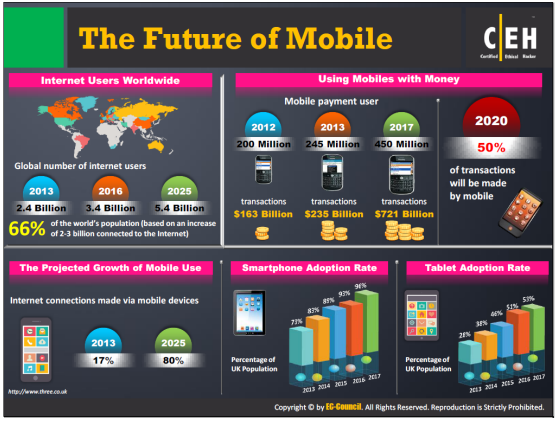
Hacking Mobile Platforms

Module 15

Ethical Hacking and Countermeasures v9

Module 15: Hacking Mobile Platforms

Exam 312-50



With the advancement of mobile technology, mobility has become the key parameter for internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. The report summarized below explains about what the future holds for the world of mobile.

Internet Users Worldwide

World has over **three billion** internet users as of September 2015. This figure shows no signs of slowing down. About **half the world's population** will be able to access the Internet on a regular basis by the year 2018.

The Projected Growth of Mobile Use

As the usage of the Internet grows, so is the number of Internet-enabled mobile devices. By the year 2018, over **50%** of internet users around the world will be using mobile devices to get online and by 2025, the figure is expected to jump up to **80%**.

Mobile Device Adoption Rate

The sales of mobile devices **overtook** that of desktop devices in the U.S back in 2014 itself. It is now just the matter of how much this gap will widen in the future. As of mid-2015, people in U.S.A accessed the internet from a mobile device about **51%** of the times as compared to **42%** from a desktop device.

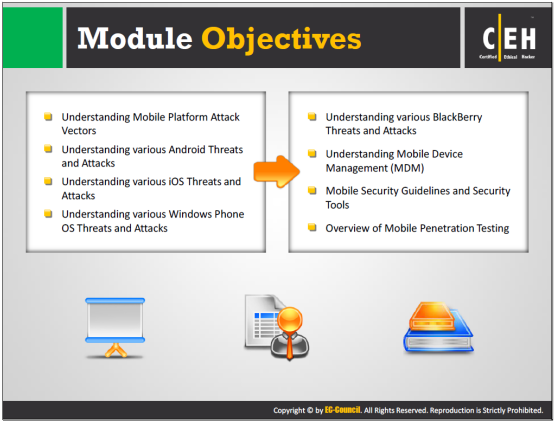
Using Mobiles with Money

Owing to their ubiquity and portability, payments made through a mobile and with a mobile (NFC enabled devices) have gained the maximum momentum. While the payments aided by a mobile device cocked a totally of $52 billion in 2014, it will rise up to $142 billion by the year 2019. The estimated number of mobile transactions by the end of 2015 is 47 billion.

The Internet of Things

The global Internet of Things (IoT) market will witness a net growth of **31.72%** from 2014 to 2019. The number of smart or connected devices will climb up to **17 billion**, creating a net profit of **$14.4 trillion** globally.

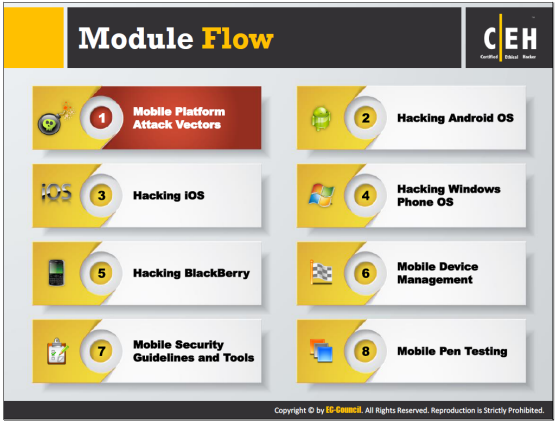
Source: *http://www.three.co.uk*



Mobile devices are replacing desktops and laptops, as they enable the users to access email, Internet, GPS navigation, and the storage of critical data such as contact lists, passwords, calendars, and login credentials. Also, recent developments in mobile commerce have enabled users to perform transactions such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking from their smartphones.

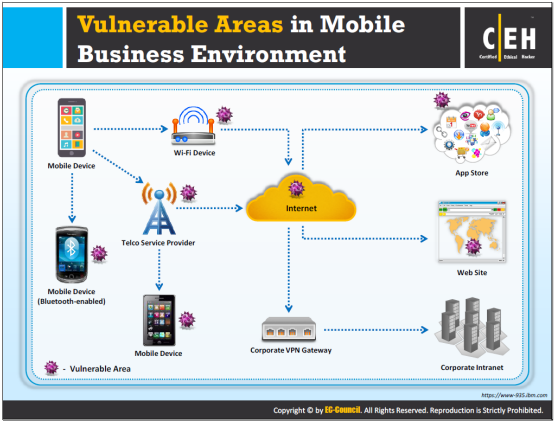
Believing that surfing the internet on mobile devices is safe, many users fail to enable existing security software. However, the popularity of smartphones and their moderately lax security have made them attractive and valuable targets of attackers.

The main objective of this module is to explain the potential threats to mobile platforms and provide guidelines for using mobile devices securely.



Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats exploit critical data, money, and other information from mobile users and sometimes damage the reputation of mobile networks and organizations.

This section discusses current mobile usage statistics, the anatomy of mobile attacks, mobile attack vectors, associated vulnerabilities and risks, security issues arising from app stores, app sandboxing issues, mobile spam, pairing mobile devices on open Bluetooth and Wi-Fi connections, and others.



At present, smartphones are being widely used for both business and personal purposes. Thus, they are a treasure trove for attackers to steal corporate or personal data. Security threats to mobile devices have progressed because of Internet connectivity, use of business and other applications, the different communication mechanisms available, and so on. Apart from those threats specific to mobile devices, they are also susceptible to many of the threats applicable to desktop and laptop computers.

Smartphones today 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.

Source: *https://www-935.ibm.com*

According to OWASP, the top 10 mobile risks include:

- **Weak Server Side Controls**

  Attackers can exploit this vulnerability when an organization reveals a web service or API call used by the mobile app. They exploit insecure code in the exposed web service or API call to launch various attacks on the mobile app service. Attackers inject malicious input or unexpected series of events to the vulnerable endpoint via mobile interface. To overcome this threat, app developers must implement secure coding and configuration practices on the server side of the mobile application.

- **Insecure Data Storage**

  This vulnerability arises when development teams assume that users and malware will not have access to a mobile device's file system and subsequently to sensitive information in the device's data stores. "**Jailbreaking**" or rooting a mobile device bypasses encryption protections. OWASP recommends analyzing platforms' data security APIs and calling them appropriately.

- **Insufficient Transport Layer Protection**

  Often, mobile applications do not protect network traffic using SSL/TLS. This may result in revealing sensitive data and session IDs to intercept. OWASP recommends applying SSL/TLS to transport channels the mobile application uses to transmit sensitive data, session IDs, and so on to the backend API or web service.

- **Unintended Data Leakage**

  Unintended data leakage occurs when a developer unintentionally places sensitive data in a location on the mobile device that is easily accessible by other apps on the device. Unintended data leakage is due to vulnerabilities from the OS, frameworks, compiler environment, new hardware, and so on without a developer's knowledge. It is a significant threat to OSs, platforms, and frameworks; thus it is important to understand how they handle features such as URL caching, browser cookie objects, and HTML5 data storage.

- **Poor Authorization and Authentication**

  Poor or missing authentication schemes allow an attacker to anonymously execute functionality in the mobile app or the backend server that uses it. Weaker authentication is prevalent because of a device's input form factor, which encourages short passwords (four-digit PINs).

  Attackers make use of vulnerabilities such as poor or missing authorization schemes to execute functionality without permission, via an authenticated but lower-privilege user of the mobile app.

  Testers can perform binary attacks against mobile apps to detect poor authentication schemes (by forcing apps to bypass offline authentication, then executing functionality) and poor authorization schemes (e.g., attempting to execute privileged functionality only executable by a higher-privileged user during "offline" mode).

- **Broken Cryptography**

  This vulnerability is a result of weak encryption algorithms or flaws in the encryption process. In broken cryptography, an attacker effectively deciphers the encrypted code. To prevent this type of attack, developers use strong approved encryption algorithms such as AES and 3DES.

- **Client Side Injection**

  Client-side injection results in the execution of malicious code on the mobile device via apps. Generally, attackers inject the app with malicious code in the form of data. To overcome this threat, developers must examine all the input fields of the application and apply appropriate input validation.

- **Security Decisions via Untrusted Inputs**

  Applications use protection mechanisms that depend on input values (such as cookies, environmental variables, and hidden form fields), but these input values can be altered by an attacker to bypass the protection mechanism, making it very hard to detect the changes made. While making security decisions (authentication, authorization, etc.) regarding the input values, attackers can bypass the software's security. To prevent this attack, it is important to validate all inputs and ensure trusted data sources for security decisions.

- **Improper Session Handling**

  Improper session handling occurs when a user shares the session token inadvertently with the attacker during a subsequent transaction between the mobile app and backend servers. To handle sessions appropriately, it is important to ensure that the mobile app code creates, maintains, and destroys session tokens properly during the user's entire mobile app session.

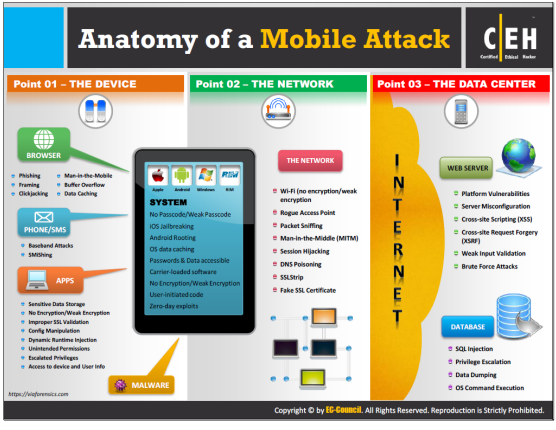
- **Lack of Binary Protections**

  The lack of binary protections in a mobile app exposes it and its owner to a wide variety of technical and business risks if it is insecure, or if it exposes sensitive intellectual property. Lack of binary protections results in an app that can be analyzed, reverse-engineered, and modified very quickly by an adversary.

  To overcome this vulnerability, the application must follow secure coding techniques for components such as jailbreak detection controls, checksum controls, certificate pinning controls, and debugger detection controls.

  In addition, it is important to use static or dynamic analysis techniques to prevent attackers from analyzing and reverse-engineering the app, and to ensure that it is able to detect and react appropriately at runtime to code integrity violations.

Source: *https://www.owasp.org*



Because of extensive usage and implementation of BYOD (bring your own device) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. These attacks can involve the device layer, the network layer, the data center, or a combination of these.

Attackers exploit vulnerabilities associated with the following to launch malicious attacks:

The Device

Vulnerabilities in mobile devices pose significant risks to sensitive personal and corporate data. Attackers targeting the device itself can use various entry points.

Device-based attacks include:

- **Browser-Based Attacks**

  Browser-based points of attack include:

  - **Phishing**

    Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information such as usernames, passwords, credit card details, address, and mobile number. Mobile users are more likely to be victims of phishing sites because of the small size of the devices, which display only short URLs, limited warning messages, scaled-down lock icons, and so on.

- **Framing**

  Framing involves a webpage integrated into another webpage using iFrame elements of HTML. An attacker exploits iFrame functionality used in target website, embeds his/her malicious webpage, and uses clickjacking to steal users' sensitive information.

- **Clickjacking**

  Clickjacking, also known as a user Interface redress attack, is a malicious technique used to trick web users to click something different from what they think they are clicking. As a result, attackers obtain sensitive information or take control of the device.

- **Drive-By Downloading**

  Drive-by downloading is the unintended download of software (probably malicious) from the Internet. Drive-by downloads may take place on visiting a website, viewing an e-mail, or by clicking on a deceptive prompt. Android devices are predominantly vulnerable to this attack.

- **Man-in-the-Mobile (MitMo)**

  Attacker implants malicious code into the victim's mobile device to bypass password verification systems that send OTPs via SMS or voice calls. Thereafter, the malware relays the gathered information to the attacker.

- **Buffer Overflows**

  Buffer overflow is an abnormality whereby a program, while writing data to a buffer, surfeits the intended limit and overwrites the adjacent memory. This results in erratic program behavior, including memory access errors, incorrect results, and crash mobile device.

- **Data Caching**

  Data caches in mobile devices store information that is often required by mobile devices for interacting with web applications, thereby saving scarce resources and resulting in better response time for the client application. Attackers attempt to exploit these data caches to gain sensitive information stored in them.

- **Phone/SMS-based attacks**

  Phone/SMS-based points of attack include:

  - **Baseband attacks**

    Attackers exploit vulnerabilities resident in a phone's GSM/3GPP baseband processor, which sends and receives radio signals to cell towers.

  - **SMiShing**

    SMS phishing (also known as SMiShing) is a type of phishing fraud in which an attacker utilizes Short Message Service (SMS) to send text messages to a victim that

contains a deceptive link of a malicious website or a telephone number. The attacker tricks the victim into clicking the link or calling the phone number and revealing his or her personal information such as social security numbers, credit card numbers, and online banking username and password.

- **RF (Radio Frequency) Attacks**

  Attackers exploit vulnerabilities found on different peripheral communication channels normally used in nearby device-to-device communications.

- **Application-based attacks**

  Application-based points of attack include:

  - **Sensitive Data Storage**

    Some apps installed and used by mobile users employ weak security in their database architecture, which make them targets for attackers to hack and steal sensitive user information stored on them.

  - **No Encryption/Weak Encryption**

    Apps that transmit data unencrypted or weakly encrypted are susceptible to attacks such as session hijacking.

  - **Improper SSL Validation**

    Security loopholes in an application's Secure Socket Layer (SSL) validation process may allow attackers to circumvent the data security.

  - **Config Manipulation**

    Apps may use external configuration files and libraries, modifying those entities or affecting apps' capability of using those results in a configuration manipulation attack. This includes gaining unauthorized access to administration interfaces, configuration stores, and retrieval of clear text configuration data.

  - **Dynamic Runtime Injection**

    Attackers manipulate and abuse the runtime of an application to circumvent security locks, logic checks, access privileged parts of an app, and even steal data stored in memory.

  - **Unintended Permissions**

    Misconfigured apps can at times open doors to attackers by providing unintended permissions.

  - **Escalated Privileges**

    Attackers engage in privilege escalation attacks, which take advantage of design flaws, programming errors, bugs, or configuration oversights to gain access to resources usually protected from an application or user.

- **OS-based attacks**

  Operating system–based points of attack include:

  - **No passcode**

    Many users choose not to set a passcode, or use a weak PIN, passcode or pattern lock, which an attacker could easily guess or crack to compromise sensitive data stored in the mobile.

  - **iOS jailbreaking**

    Jailbreaking iOS is the process of removing security mechanisms set by Apple to prevent malicious code from running on the device. It provides root access to the operating system and removes sandbox restrictions. Thus jailbreaking, like rooting, comes along with many security and other risks to the iOS device including poor performance, malware infection, and so on.

  - **Android rooting**

    Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. Like jailbreaking, rooting can result in the exposure of sensitive data stored in the mobile device.

  - **Passwords and data accessible**

    iOS devices store encrypted passwords and data using cryptographic algorithms that have certain known vulnerabilities. Attackers exploit these vulnerabilities to decrypt the device's keychain, exposing user passwords, encryption keys, and other private data.

  - **Carrier-loaded software**

    Pre-installed software or apps on devices may contain vulnerabilities that an attacker can exploit to perform malicious activities such as delete, modify, or steal data on the device, eavesdrop on calls, and others.

  - **Zero-day exploits**

    It is launching an attack by exploiting a previously unknown vulnerability in a mobile OS or app. The name "zero-day" denotes the immediacy of potential exploitation, in that there are zero days between the time of vulnerability discovery and the first attack.

The Network

Network-based points of attack include:

- **Wi-Fi (weak encryption/no encryption)**

  Some applications fail to encrypt or use weak algorithms to encrypt data in transmission across wireless network. An attacker may intercept data by eavesdropping on the wireless connection. Though many applications use SSL/TLS, which offers protection for

data in transit, attacks against these algorithms are reputed to expose users' sensitive data.

- **Rogue access points**

  Attackers install an illicit wireless access point by physical means, which allows them to access a protected network by hijacking the connections of legitimate network users.

- **Packet sniffing**

  An attacker uses sniffing tools such as Wireshark and Capsa Network Analyzer to capture and analyze all data packets in network traffic, which generally includes sensitive data such as login credentials sent in clear text.

- **Man in the Middle (MITM)**

  Attackers eavesdrop on existing network connections between two systems, intrude into that connection, and thereafter read, modify, or insert fraudulent data into the intercepted communication.

- **SSLStrip**

  SSLStrip is a type of MITM attack in which attackers exploit vulnerabilities in the SSL/TLS implementation on web sites. It relies on the user validating the presence of the HTTPS connection. The attack invisibly downgrades connections to HTTP, without encryption, which is hard for users to detect in mobile browsers.

- **Session hijacking**

  Attackers steal valid session IDs and use them to gain unauthorized access to user and network information.

- **DNS poisoning**

  Attackers exploit network DNS servers, resulting in the substitution of false IP addresses at the DNS level, thereby directing website users to another website of the attacker's choice.

- **Fake SSL certificates**

  Fake SSL certificates represent another kind of MITM attack, in which an attacker issues a fake SSL certificate to intercept traffic on a supposedly secure HTTPS connection.

The Data Center

Data Center has two main points of entry: a web server and a database.

- **Web server-based attacks**

  Web server–based vulnerabilities and attacks include:

  - **Platform vulnerabilities**

    Attackers exploit vulnerabilities in the operating system, server software such as IIS, or application modules running on the web server. Sometimes, attackers can expose

vulnerabilities associated with protocol or access controls by monitoring communication established between a mobile device and a web server.

- **Server misconfiguration**

  Misconfigured web servers may allow an attacker to gain unauthorized access to its resources.

- **Cross-site scripting (XSS)**

  Cross-site scripting (XSS) attacks exploit vulnerabilities in dynamically generated web pages, which enable malicious attackers to inject client-side script into web pages viewed by other users. It occurs when invalidated input data is included in dynamic content sent to the user's web browser for rendering. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests.

- **Cross-Site Request Forgery (CSRF)**

  Cross-Site Request Forgery (CSRF) attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send unintended malicious requests. The victim holds an active session with a trusted site and simultaneously visits a malicious site that injects an HTTP request for the trusted site into the victim user's session, compromising its integrity.

- **Weak Input Validation**

  Web services excessively trust the input coming from mobile applications, depending on the application to perform input validation. However, attackers can forge their own communication to the web server or circumvent the app's logic checks, allowing them to take advantage of missing validation logic on the server to perform unauthorized actions.

  Attackers exploit input validation flaws so that they can perform cross-site scripting, buffer overflow, injection attacks, etc. that lead to data theft and system malfunctioning.

- **Brute-Force Attacks**

  Attackers perform trial and error method in an attempt to guess the valid input to a particular field. Applications, which allow any number of input attempts, are generally prone to this kind of attacks.

- **Database Attacks**

  Database-based vulnerabilities and attacks include:

  - **SQL injection**

    SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a

backend database. SQL injection is a basic attack used either to gain unauthorized access to a database or to retrieve information directly from the database.

- **Data Dumping**

  An attacker causes the database to dump some or all of its data, thereby uncovering sensitive records.

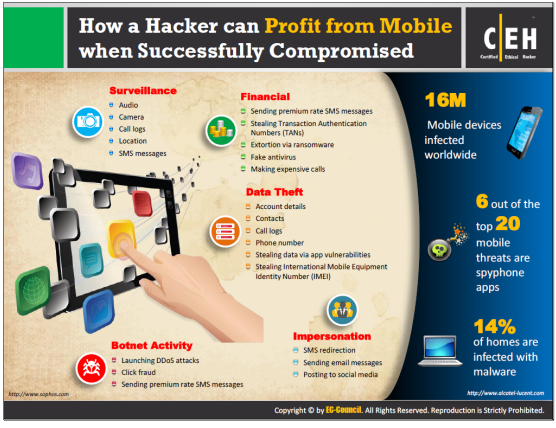
- **OS command execution**

  An attacker injects OS-level commands into a query, causing certain database systems to execute these commands on the server; thereby providing an attacker with unrestricted/root level system access.

- **Privilege escalation**

  This happens when an attack leverages some exploit to gain high-level access, resulting in the theft of sensitive data stored in the database.

Source: *https://viaforensics.com*

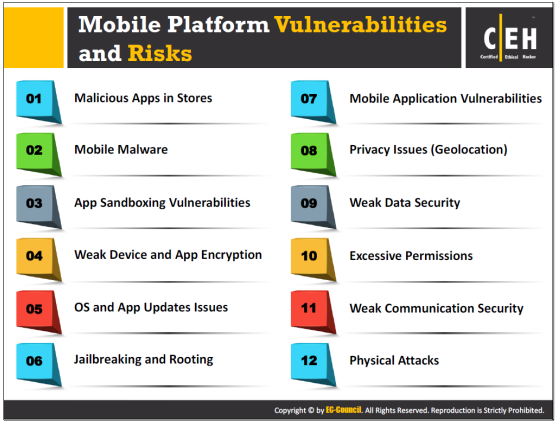


Today, pictures, contact lists, banking apps, social media, email accounts, financial information, business information, and others all reside on our smartphones devices. Thus, smartphones are a treasure trove of information for potential exploitation by attackers. Among all smartphones, Android devices are most likely to be hacked, as they occupy **80%** of the mobile market share.

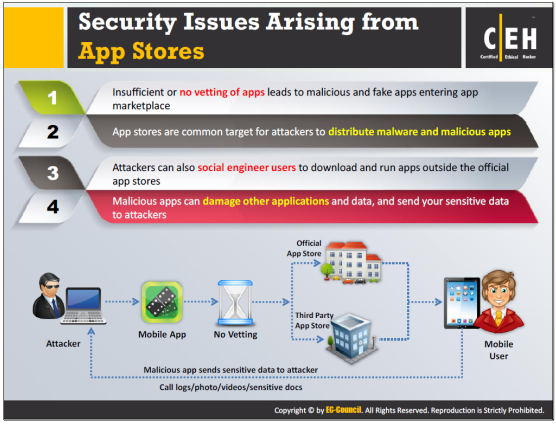
Upon compromising a smartphone, an attacker could spy user activities on mobile, misuse the sensitive information stolen, impersonate the user by posting on social media accounts, or enlisting the device in a botnet (a network of many hacked smartphones).

Source: *http://www.sophos.com, http://www.alcatel-lucent.com*

The enormous usage of mobile devices has grabbed the attention of attackers. Mobile devices access many of the resources that traditional computers use. Apart from that, mobile devices also have some unique features that add new attack vectors and protocols to the mix. All these mobile attack vectors make mobile phone platforms susceptible to malicious attacks both from the network and upon physical compromise. Given in the slide are some of the attack vectors that allow an attacker to exploit vulnerabilities present in mobile OS, device firmware, or mobile apps.

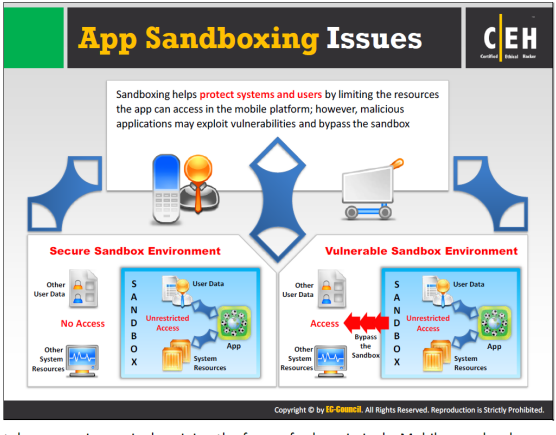


Increased usage of smartphones with ever-evolving technological features has made mobile device security a primary security concern for the IT sector. Mobile devices are becoming privileged targets for cyber criminals because of significant improvements in both mobile Oss and hardware. In addition, the enhancements in smartphone features introduce new types of security concerns. As smartphones are surpassing PCs as preferred devices to access the Internet, manage communications, and so on, attackers are more attracted to research and implement possible attack schemes against mobile platforms to compromise users' security and privacy, or even gain complete control over their devices.



Mobile applications are computer programs designed to run on smartphones, tablets, and other devices. These include text messaging, email, video play, music play, voice recording, and games, among many others. In general, apps are made available via application distribution platforms, which could be official app stores operated by the owner of mobile OS such as Apple's App Store, Google Play app store, and Blackberry App World, or third-party app stores such as Handango, GetJar, and MobiHand.

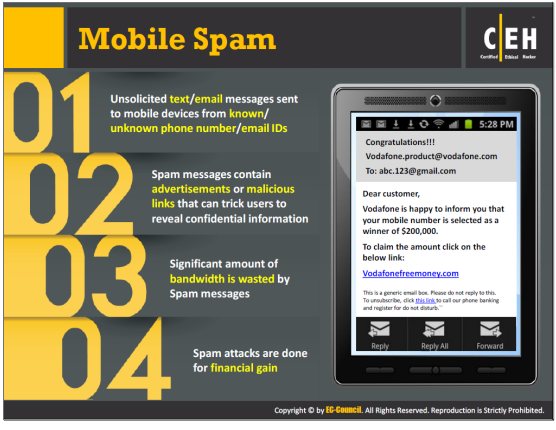
App stores are a common target for attackers to distribute malware and malicious apps. Attacker may download a legitimate app, repackage it with malware, and upload it to a third-party app store, from which users download it, thinking it to be genuine. Malicious apps installed on user systems can damage other applications or stored data, and send sensitive data such as call logs, photos, videos, sensitive docs, and so on to the attacker without users' knowledge. Attacker may use the information gathered to exploit the devices and launch many more attacks. Attackers can also social engineer users to download and run apps outside the official app stores. Insufficient or no vetting of apps usually leads to malicious and fake apps entering the marketplace.



Smartphones are increasingly gaining the focus of cybercriminals. Mobile app developers must understand the threat to security and privacy to mobile devices by running a non-sandboxed app, and should therefore develop sandboxed apps.

App ***sandboxing*** is a security mechanism that helps protect systems and users by limiting resources the app can access to its intended functionality on the mobile platform. Often, sandboxing is useful in executing untested code, or untrusted programs from unverified third parties, suppliers, untrusted users, and untrusted websites. This is to enhance security by isolating an application to prevent intruders, system resources, malware such as Trojans and viruses, and other applications from interacting with the protected app. As sandboxing isolates applications from one another, it protects them from tampering with each other.

A secure sandbox environment provides an application with limited privileges intended for its functionality to restrict it from accessing other users' data and system resources, whereas a vulnerable sandbox environment allows a malicious application to exploit vulnerabilities in the sandbox and breach its perimeter, resulting in the exploitation of other data and system resources.



Nowadays, mobile phones are widely being used for both personal and business purposes. Spam is the generic term for unsolicited messages sent via electronic communication technologies such as SMS (Short Message Service), MMS (Multimedia Message Service), IM (Instant Messaging), and email without having requested them.

Mobile Phone Spam, also known as SMS spam, text spam, or m-spam is any unsolicited message sent in bulk form known/unknown phone number/email IDs that targets a mobile phone.

Messages delivered via spam to mobile phones typically include:

- Attractive commercial messages advertising products/services
- SMS and MMS messages that claim victim has won a prize and asks him/her to place a call to a provided premium rate telephone service number for further details
- Malicious links, which may lure users to divulge sensitive personal or corporate data
- Phishing messages that lures the recipient into revealing personal or financial data such as name, address, date of birth, bank account number, credit card number, etc., that an attacker can later use to commit identity or financial fraud against the recipient

Due to spam messages, a significant amount of bandwidth is wasted. Consequences of mobile spam include financial loss, malware injection, and corporate data breach incidents.

Text messaging is the most prevalent non-voice communication on a mobile phone. Users send and receive some billions of text messages around the world for a day. With that huge number, there is also increase in spam or phishing attacks.

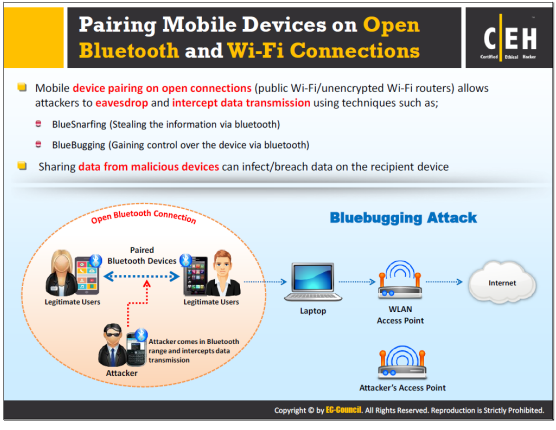
SMS phishing (also known as **SMiShing**) is a type of phishing fraud in which an attacker utilizes **SMS (Short Message Service)** systems to send bogus text messages. Often, these bogus text messages contain a deceptive website URL link or telephone number to lure victims into revealing their personal or financial information, such as social security numbers, credit-card numbers, and online banking username and password. In addition, attackers implement SMiShing to infect victims' mobile phones and associated networks with malware.

Attackers buy a prepaid SMS card using a fake identity. They then send SMS bait to a user. The SMS can seem attractive or scary. For example, it may include a lottery message, gift voucher, online purchase, or notification of account suspension, along with a malicious link or phone number. The user clicks the link, thinking it to be legitimate, and is redirected to an attacker's phishing site, where the user provides the requested information (e.g., name, phone number, date of birth, credit-card number or PIN, CVV code, Social Security number [SNN], email address). The attacker may use the acquired information to perform malicious activities such as identity theft and online purchases, among many others.

Why SMS Phishing is Effective?

- 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



Setting a mobile device's Bluetooth connection "**open**" or in "**discovery**" mode and turning on automatic Wi-Fi connection capability, particularly in public places, greatly increases risk rate. Attackers use this to their advantage to exploit and infect a mobile device with malware such as viruses and Trojans, or compromise unencrypted data being transmitted across untrusted networks. They may lure victims into accepting a Bluetooth connection request from a malicious device, or may perform an MITM attack to intercept and compromise all the data sent to and from the connected devices. Attacker, armed with the information gathered, engage in identity fraud and other malicious activities, thereby putting users at great risk.

Techniques such as "**bluesnarfing**" and "**bluebugging**" help an attacker eavesdrop and intercept data transmission between mobile devices paired on open connections (e.g., public Wi-Fi/unencrypted Wi-Fi routers).

- **Bluesnarfing (Stealing Information via Bluetooth)**

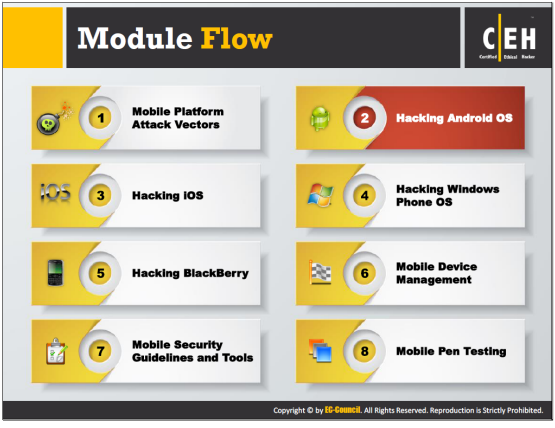
  Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, PDAs, and others. This technique allows an attacker to access victim's contact list, emails, text messages, photos, videos, business data, and so on stored on the device.

  Any device with its Bluetooth connection enabled and set to "discoverable" or "discovery" mode (allowing other Bluetooth devices within range to view the device) may be susceptible to bluesnarfing if the vendor's software contains certain

vulnerability. Bluesnarfing exploits others' Bluetooth connections without their knowledge.

- **Bluebugging (Taking Over a device via Bluetooth)**

  Bluebugging involves gaining remote access to a target Bluetooth-enabled device and use its features without a victim's knowledge or consent. Attackers compromise the target device's security to create a backdoor attack prior to returning control of it to its owner. Bluebugging allows attackers to sniff sensitive corporate or personal data, receive calls and text messages intended for the victim, intercept phone calls and messages, forward calls and messages, connect to the Internet, and perform other malicious activities such as accessing contact lists, photos, and videos.



The number of people using smartphones and tablets is on the rise, as these devices support a wide range of functionalities. Android is the most popular mobile OS because it is a platform open to all applications. Like other operating systems, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This casualness enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on them.

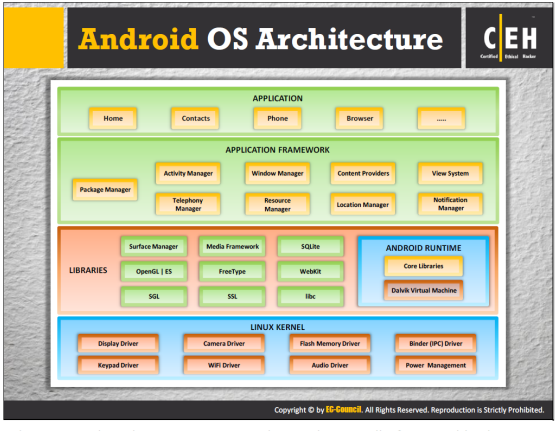
This section discusses the Android OS, its architecture and the associated vulnerabilities. It also covers the process of rooting Android phones, rooting tools and Android Trojans. The section ends with the guidelines for securing Android devices, security controls, and device-tracking tools.

The Android OS relies on the Linux kernel and is an open-source platform.

Additional Features:

- Provides a variety of pre-build UI components such as structured layout objects and UI controls that allow one to build the GUI for the app
- Provides several options to save persistent application data:
  - **Shared Preferences** - Store private primitive data in key-value pairs
  - **Internal Storage** - Private data on the device memory
  - **External Storage** - Public data on the shared external storage
  - **SQLite Databases** - Store structured data in a private database
  - **Network Connection** - Store data on the web with your own network server
- RenderScript provides a platform-independent computation engine that operates at the native level. One can use it to accelerate apps that require extensive computational horsepower.
- Provides rich APIs to let the app connect and interact with other devices over Bluetooth, NFC, Wi-Fi P2P, USB, and SIP, in addition to standard network connections

Source: http://developer.android.com



Android is a Linux-based operating system designed especially for portable devices such as smartphones and tablets. It is a stack of software components categorized into five sections (application, application framework, libraries, Android runtime, and Linux kernel) and four layers.

Applications

All Android applications are at the top layer. Any app developed should fit in this layer. Some of the standard applications that come pre-installed with every Android device include SMSs, Web browsers, contact managers, and calendars. Most Android apps are "written" in Java programming language.

Application Framework

The application framework offers many higher-level services to applications, which developers incorporate in their development.

Application framework blocks include:

- **View System** – for developing lists, grids, text boxes, buttons, and so on
- **Content Providers** – manages data sharing between applications
- **Location Manager** – manages location, using GPS or cell towers
- **Resource Manager** – manages various types of resources used
- **Notification Manager** – helps applications display custom messages in a status bar

- **Activity Manager** – controls the activity life cycle of applications
- **Telephony Manager** – manages all voice calls
- **Package Manager** – keeps track of the applications installed on the device
- **Window Manager** – manages application windows

Libraries

The next layer is the native libraries. Libraries are "written" in C or C++ and are specific to particular hardware. This layer allows the device to control different types of data.

Native libraries include:

- **Surface Manager** – meant for display management
- **Media Framework** – provides media codecs that allows recording and playback of different media formats
- **SQLite** – a database engine used for data storage purposes
- **Open GL | ES** – is a 3D graphics library
- **FreeType** – meant for rendering fonts
- **WebKit** – Web browser engine to display HTML content
- **SGL** – is a 2D graphics library
- **SSL** – meant for Internet security
- **libc** – comprises System C libraries

Android Runtime

Android Runtime includes core libraries and the Dalvik virtual machine

- **Core Libraries**

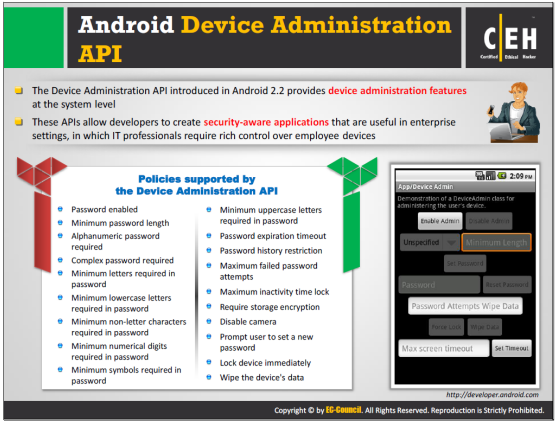
  The set of core libraries allows developers to write Android applications using the Java programming language.

- **Dalvik Virtual Machine**

  Dalvik VM is a type of JVM that helps in executing Android applications designed particularly for Android to run on embedded systems as well as on limited battery power, limited memory, and limited CPU capability. Dalvik VM allows creating multiple instances of Virtual Machine instantaneously that provides security isolation, memory management, and threading support.

Linux Kernel

The Android OS relies on the Linux 2.6 kernel. This layer comprises low-level device drivers such as a display driver, camera driver, Flash memory driver, binder (IPC) driver, keypad driver, Wi-Fi driver, audio driver, and power management for its various hardware components. It also acts as an abstraction layer between the hardware and software stack. Functions of this layer include memory management, power management, security management, and networking.



One can use a device administration ("admin") API to write device admin applications that users install on their devices. The device admin application enforces the desired policies.

Examples of the types of applications that might use the device administration API are:

- Email clients
- Security applications that do remote wipe
- Device management services and applications

Listed below are the policies supported by the Android device administration API:

Policy	Description
Password enabled	Requires that devices ask for PIN or passwords
Minimum password length	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.
Alphanumeric password required	Requires passwords to have a combination of letters and numbers. They may include symbolic characters.
Complex password required	Requires that passwords must contain at least a letter, a numerical digit, and a special symbol. Introduced in Android 3.0.
Minimum letters required in password	The minimum number of letters required in the password for all admins or a particular one. Introduced in Android 3.0.

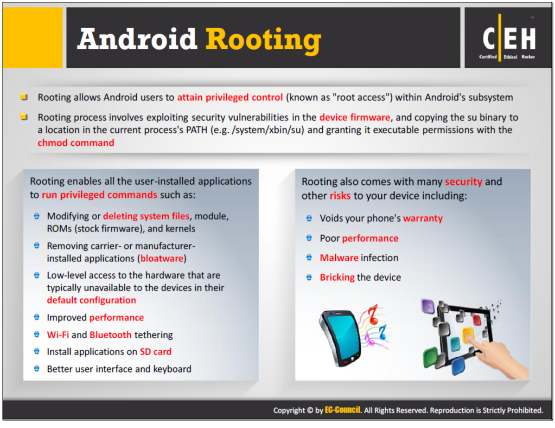
Minimum lowercase letters required in password	The minimum number of lowercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum non-letter characters required in password	The minimum number of non-letter characters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum numerical digits required in password	The minimum number of numerical digits required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum symbols required in password	The minimum number of symbols required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum uppercase letters required in password	The minimum number of uppercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Password expiration timeout	When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration timeout. Introduced in Android 3.0.
Password history restriction	This policy prevents users from reusing the last *n* unique passwords. Typically, you can use this policy in conjunction with setPasswordExpirationTimeout(), which forces users to update their passwords after a specified amount of time has elapsed. Introduced in Android 3.0.
Maximum failed password attempts	Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.
Maximum inactivity time lock	Sets the length of time since the user last touched the screen or pressed a button before the device locks the screen. When this happens, users need to enter their PIN or passwords again before they can use their devices and access data. The value can be between 1 and 60 minutes.
Require storage encryption	Specifies regarding the encryption of storage, if the device supports it. Introduced in Android 3.0.
Disable camera	Specifies the camera disabling feature. Note that this does not have to be a permanent disabling. The camera can be enabled/ disabled dynamically based on context, time, and so on. Introduced in Android 4.0.

TABLE 15.1: List of policies supported by the Android Device Administration API

In addition to supporting the policies mentioned above, the device administration API lets you:

- Prompt user to set a new password
- Lock device immediately
- Wipe the device's data (that is, restore the device to its factory defaults)

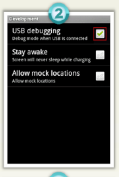
Source: http://developer.android.com



The goal behind rooting Androids is to overcome restrictions imposed by hardware manufacturers and carriers, resulting in the ability to modify or replace system applications and settings, run apps that require admin privileges, remove and replace a device's OS, remove applications pre-installed by its manufacturer or carrier, or perform other operations that are otherwise inaccessible to the typical Android user. One can use tools such as SuperOneClick, Superboot, and Kingo Android ROOT to root Android devices.

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

CEH 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**



Discussed below are a few more Android rooting tools that allow privileged control within Android's subsystem:

One Click Root

One Click Root is Android rooting software that allows rooting an Android smartphone or tablet and provides access to additional features such as gaining access to more apps, Install apps on SD card, preserve battery life, Wi-Fi and Bluetooth tethering, installing custom ROMs, and accessing blocked features.

Kingo Android ROOT

Kingo Android ROOT helps users root their Android devices to:

Features:

- Improve performance
- Preserve battery life
- Access root-only apps
- Remove carrier "bloatware"
- Customizable appearance
- Attain admin level permission

Discussed below are a few more tools with which one can root Android devices:

Unrevoked

Source: *http://unrevoked.com*

Unrevoked is used to flash a custom recovery image to an Android phone. A custom recovery image allows performing advanced tasks on the system partition, such as flashing custom ROMs and accessing a full ("nandroid") backup of your phone. Unrevoked roots the following phones: the HTC Evo, Hero, Wildfire, Desire, and Aria, and the Droid Incredible.

RescueRoot

Source: *http://rescueroot.com*

RescueRoot features a state-of-the-art Android rooting database that contains all of the latest scripts and exploits, all of which are custom matched and optimized for specific phones.

Features:

- Roots most Android devices (Android 1.x, 2.x, 4.0.x and 4.1.x)
- Backup and protects data (saves and encrypts apps, contacts, stored files, text messaging, etc. on your own hard drive)
- Data restoration
- Unroot (restores a phone to its previous unrooted state)

Unlock Root Pro

Source: *www.unlockroot.com*

Unlock Root Pro is software used to root Android devices. Its main function is to obtain the highest possible user privileges so that the user can remove, install, or uninstall any application.

Rooting the device with Unlock Root helps in:

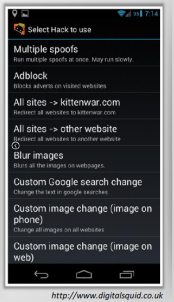
- Overclocking and Underclocking
- Making modifications to improve battery life
- Accessing apps that might require superuser permission
- Removing bloatware such as apps pre-installed by manufacturers or carriers
- Customization
- Flashing ROMs such as CyanogenMod, MIUI
- Gaining access to features for which your carrier would otherwise charge a fee (i.e., Wi-Fi/USB tethering)

Hacking Networks Using Network Spoofer

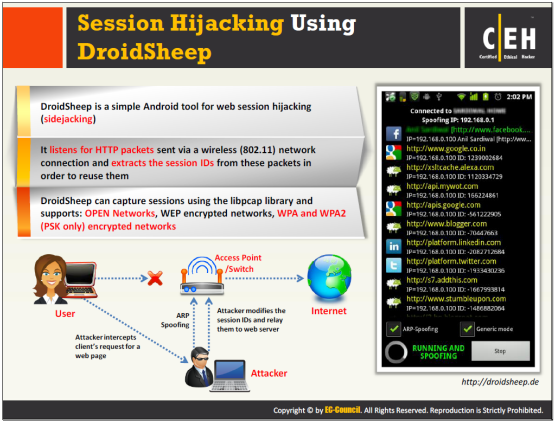
- Network Spoofer lets you **change websites** on other people's computers from an Android phone

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



DroidSheep is a simple Android tool for web session hijacking ("**sidejacking**"), using libpcap and arpspoof. Most web applications use a session ID to verify user identity in the application. They transmit this session ID in subsequent requests in HTTP packets to maintain the user session. Attackers can use DroidSheep to read all packets sent via a wireless network and capture the session ID. Once captured, attackers use the stolen session ID to access the target web app on behalf of the victim.

Source: http://droidsheep.de

Discussed below are a few more Android-based sniffers:

Packet Sniffer

Source: *https://sites.google.com*

Packet Sniffer is an Android app that allows the capture and display Wi-Fi and Bluetooth traffic. To use it, you must be root on your phone and have the "su" command installed.

tPacketCapture

Source: *http://www.taosoftware.co.jp*

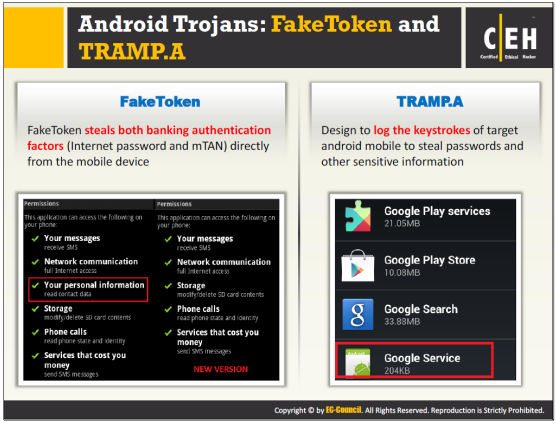
tPacketCapture is software that can capture communication packets on non-Rooted devices. It uses the Android OS VpnService. Attackers store the captured data in PCAP file format, in external storage. It does not access any external servers for packet capturing.

Android PCAP

Source: *http://www.kismetwireless.net*

Android PCAP Capture is a utility for capturing raw 802.11 frames ("Monitor mode," aka "Promiscuous mode"). Attackers view the resulting Pcap file on a computer using Eye P.A., Wireshark, Tcpdump, and similar tools, or online using CloudShark.

ZitMo is a version of the Zeus malware that specifically targets mobile devices. The motive behind this mobile component is to steal online banking details from users. It can intercept two-factor authentication, which banks use to validate account-holder identity during login. Even if a mobile user does not rely on two-factor authentication for banking, ZitMo is capable of forwarding and spying on all SMS messages, making it a valid threat.



Listed below are a few more Android Trojans:

FakeToken

FakeToken is a Trojan horse that opens a back door on a compromised device to steal SMS messages containing mTAN numbers generated by banks to validate online transactions.

When a user enters a key for an online banking transaction, the Trojan returns a randomly generated, fake token number. It then opens a back door on the compromised device, allowing an attacker to:

- Execute arbitrary commands
- Filter SMS messages based on a predefined string and then send them to the C&C server (e.g., SMS messages from an online bank that contain authorization tokens)
- Delete arbitrary SMS messages
- Add a new C&C server
- Send contact lists to the C&C server
- Download and install arbitrary packages

TRAMP.A

Tramp.A silently forwards information about the device to a remote location. Using the package name "**com.android.services**," the app attempts to disguise itself as an official Google service. When installed, it does not create an application shortcut, making it difficult for the user to notice its presence on the device. Searching for Tramp.A under Manage Applications shows the app as a "Google Service," again making it much harder for the user to identify the app.

The app most likely waits for a reboot or an incoming message to activate. On execution, it registers **GCMBroadCastReceiver**. Google Cloud Messaging (GCM) is, as its name suggests, a tool that enables cloud-based messaging. In this instance, GCM is used for remote control and communication (C&C) of the installed app.

The app does not have to be actively running to receive messages, as the GCM system itself will "**awaken**" when the message arrives. It is also difficult to block the device from receiving messages, as the host itself delivers the messages from the cloud.

Once installed, the app harvests data from the affected device, including contact numbers, carrier information, and SMS message details. It is also able to receive and execute the following commands received via GCM:

- Send message
- Block call
- Package name
- Get current location
- Observe
- Contact

Discussed below are a few more Android Trojans:

Fakedefender

Fakedefender deletes all .apk files found in the following folders:

- [EXTERNAL STORAGE MEDIA]/Download
- /mnt/external_sd/Download
- /mnt/extSdCard/Download

Fakedefender creates the following SQLite database file: droidbackup.db. Next, it copies all SMS messages in the device's inbox to the "smstable" table, located in the droidbackup.db file. The Trojan may display a pornographic background image when the device is locked.

Obad

Obad is a Trojan horse for Android devices that opens a back door, steals information, and downloads files. Once installed on the device, Obad variants gain administrator privileges and use an exploit to break through the Android OS's security layer. It collects and sends the following details about the device to a remote C&C server: the Media Access Control (MAC) address and IMEI, the operator name, the time, and root access data. The C&C server also issues commands to the installed application, including sending SMS messages, making the device act as a proxy or remote shell, launching a URL in the mobile browser, downloading and installing additional components, obtaining the contact list, as well as other app-specific details, and sends a file of the compiled data via Bluetooth.

Discussed below are more Android Trojans:

FakeInst

FakeInst masquerades as installers for other (even legitimate) applications; however, when executed, it send SMS messages to premium-rate numbers or subscription-based paid services.

Activities performed by FakeInst:

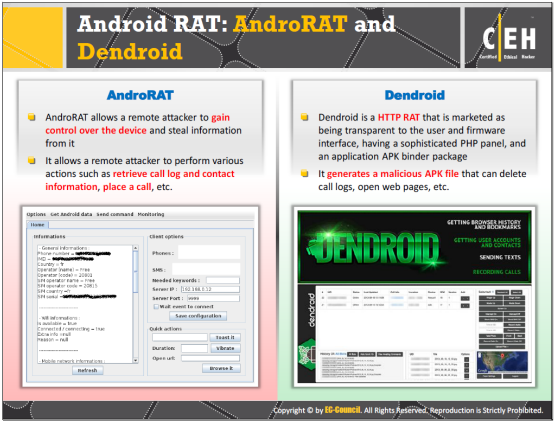
- Steals contacts and pictures
- Tracks victim's location
- Accesses victim's text messages
- Logs victim's keystrokes and passwords
- Sends SMS messages to premium numbers without victims' knowledge, resulting in a very high phone bill
- Installs fake banking applications that look legitimate and steal personal banking information upon login

OpFake

The OpFake malware family includes variants that operate on Android, Symbian, and Windows mobile platforms. All variants essentially send SMS messages to premium-rate numbers.

Attackers disguise the first variant, OpFake.A, as an Opera Mini web-browser updater, to the extent of adding an Opera icon on the menu and displaying a fake download progress bar to make it appear that the application is actually downloading, as well as a fake license.

In addition, OpFake.A also monitors SMS messages and is capable of deleting/moving messages according to their originating phone numbers and message content. Subsequent variants share similar technical details.



Discussed below are a few Android RATs:

AndroRAT

Features:

- Get contacts (and all theirs information)
- Get call logs
- Get all messages
- Location by GPS/Network
- Monitoring received messages in live
- Monitoring phone state in live (call received, call sent, call missed, etc.)
- Take a picture from the camera
- Stream sound from microphone (or other sources)
- Streaming video (for activity-based client only)
- Do a toast
- Send a text message
- Give call

- Open an URL in the default browser
- Vibrate the phone

Dendroid

Dendroid toolkit generates a malicious APK file that offers features like:

- Delete call logs
- Open Web pages
- Dial any number
- Record calls and audio
- SMS intercepting
- Upload photos and videos
- Open an application
- Initiate a HTTP flood (DoS) for a period of time
- Change the command-and-control (C&C) server

Security of Android devices is a major concern, as they are widely attacked. Given below are some of the additional countermeasures that help you to secure your Android devices and the data stored on them from malicious users:

- Enable encryption in your Android device to enhance its security
- Lock your apps that hold private information to prevent others from viewing, using apps such as AppLock
- Prior to installing an app from Google Play, read the required permissions and ensure it makes sense and corresponds to what the app actually does, and go through the comments and rating of that app
- Create multiple accounts if you would like to share your Android tablet with others, to protect each other's privacy
- Enable GPS on your Android device for it to be tracked when lost or stolen
- Use third-party applications such as Lookout Mobile Security, 3CX Mobile Device Manager, or SeekDroid AntiTheft to remotely wipe the confidential data on your Android device when lost or stolen
- Turn off the features given below:
  - "**Visible Passwords**" – prevents displaying passwords on screen

- "**Use Secure Credentials**" – prevents applications from accessing secure certificates and credentials
- "**Wi-Fi**" – to ensure you don't inadvertently connect to a wireless network when you wish not to connect

Note: You can find many of the features discussed above in **Settings → Connections** and in **Settings → More → Security** on most Android devices

Follow the common **security guidelines** for all the mobile devices outlined in the slides below.

Google Apps Device Policy for Android applications enforces security policies on Android devices. It is a device administration app for Google Apps for Business, Education, and Government accounts that make Android devices more secure for enterprise use. Once installed, your administrator can set up security measures such as password protection, so that only you can sign in and wipe the device remotely in the event that you lose it. Some organizations require users to install the Google Apps Device Policy. Failure to install the app could result in blocked email, calendar, and contacts, thus disabling their ability to synchronize on your phone.

This application gives the Google Apps administrator the ability to:

- Require that you have a PIN or password on your device
- Require a password on your device
- Require a screen lock for idle timeout on your mobile device
- Wipe a lost or stolen device

Additionally, the administrator and user have the ability to remotely: reset PIN, ring device, lock device, locate your device, and wipe the device (if your Google Apps administrator has enabled this setting).

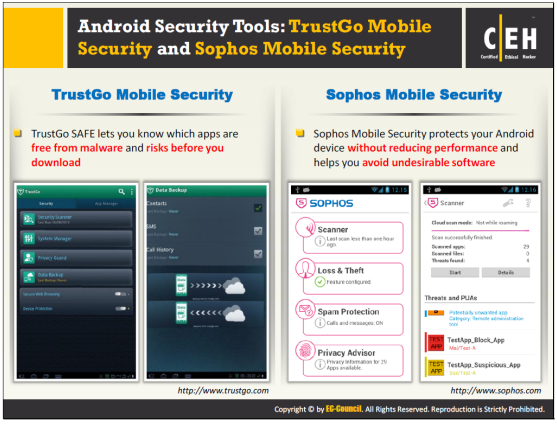
Source: *https://play.google.com*

Remote Wipe Service allows you to reset or erase the information on the lost or stolen device. If users have Google Sync installed on a supported mobile device (including Android) with the Google Apps Device Policy app, they can use the Google Apps control panel to remotely wipe the device.

One can select Remote Wipe when a device is lost or stolen to erase all data on the device and perform a factory reset. All data is erased from the device (and SD card, if applicable), including email, calendar, contacts, photos, music, and the user's personal files.

One can select Wipe account to only delete the Google Apps data from an Android device but keep the user's personal files on their device. Wipe account functions similar to removing an account on Android. It deletes a user's Google Apps account data, such as email, calendar, and contacts from the device's internal storage. This is useful, for example, when a user who owns the device leaves their company.

Source: http://support.google.com



Discussed below are more Android security tools that allow one to secure Android devices:

TrustGo Mobile Security Features:

Source: http://www.trustgo.com

- **Security Scanner** - On-demand or scheduled scans of your mobile phone or tablet and SD card to find and remove viruses, malware, spyware and trojans PLUS risky apps that can steal data.
- **Secure App Search** - Secure App Finder Engine (SAFE) lets you search and download apps that you know are safe. TrustGo alerts before downloading bad and risky apps.
- **Secure Web Browsing** - Gives an instant notification when a site you're browsing is known to be malicious or part of a phishing scheme.
- **System Manager** - Monitor and manage phone's data usage, battery consumption and memory usage.
- **Privacy Guard** - Identify apps that might be hurting your privacy.
- **Data Backup** - Store, backup and restore phone's data securely in the cloud.
- **Device Protection** - Remotely locate the phone (Find My Phone), lock it, set off an alarm, or securely wipe data and personal information if the phone is lost or stolen.
- **Candid Camera Thief ID** - Lock the phone with TrustGo, and anyone who puts in the wrong password 3 times will have their picture taken and emailed to you.

Sophos Mobile Security Features:

Source: *http://www.sophos.com*

- Anti-malware and anti-virus protection
- Loss and theft protection
- Spam protection
- Privacy protection and security

Discussed below are a few more Android security tools:

360 Security

Source: *http://www.360safe.com*

360 Security is designed to protect your Android phone against the latest viruses, malware, system vulnerabilities, and privacy risks. It also cleans application caches and junk files running in the background, and boosts your Android phone.

Features:

- **Phone Checkup** – Performs virus scans, vulnerability scans, trash cleanups and memory optimization.
- **Phone Cleaner** – Cleans trash files, uninstalls residual, private usage history and useless APKs.
- **Accelerator & Power saver** – Manages background apps, to make your phone run faster and save power.
- **System vulnerabilities fixing** – Clears vulnerabilities rooted in mobile with verified hot fixes.
- **Stop the Bad Guys** – Keeps your device away from threats.
- **Call and SMS Blocker** – Blocks unwanted phone calls.
- **Data Usage** – Saves mobile data by providing a Data Usage Monitor and a Mobile Data Firewall.

AVL

Source: http://www.antiy.net

AVL is antivirus software produced by Antiy Labs that is applicable for Android system. It displays the mobile antivirus engine of AVL SDK, which provides the basic functionality of virus scan to protect the Android system and its applications.

AVL SDK Mobile provides configuration options of detection switches, which scan malicious codes on smart phones at different levels, through which it is possible to balance its scan speed and detection capability.

AVL SDK Mobile can detect and analyze different file formats such as APK, SIS, SISX, XAP, and CAB. It can also detect different executable files such as DEX, ELF, EPOC, and PE.

Avira Antivirus Security

Source: http://www.avira.com

Avira Antivirus Security is an Android security app focusing on anti-theft and virus protection for mobile and tablet devices. It is designed to help users find their device, step by step, in the case of loss or theft. It also protects the device against virus or malware attacks.

Features:

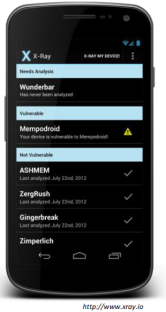
- Keeps the mobile device malware-free
- Helps to find a lost/misplaced cell phone
- Protects data from theft
- Blacklists unwanted contacts
- Doesn't drain your battery
- Automatically scans apps and updates for malware
- Tracks phone's location on a map
- Remotely lock/wipe your cell
- Triggers a loud sound, even if the device is in silent mode
- Checks whether you or your contacts' email have been hacked
- Blocks and unblocks calls and SMSs from any number

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 help you track and find the location of an Android device in case it is lost, stolen, or misplaced. Below is a list of widely used Android device tracking tools.

Find My Phone

Source: *http://findmyphone.mangobird.com*

Find My Phone is an anti-theft, device recovery app for Android that helps you find your lost, stolen, or misplaced mobile phone or tablet.

Features:

- If your phone is lost, send it a text message and Find My Phone will reply to you with its current address, and a Google Maps link to your phone's location
- Text your phone and have it ring at maximum volume (even if it is on silent) to locate by ear
- Find out how much battery is remaining
- Get notified if somebody changes your SIM card
- Remotely wipe your phone

Prey Anti-Theft

Source: http://preyproject.com

Prey lets you keep track of your laptop, phone, or tablet if it is stolen or missing. It supports geolocation. You can remotely control your Android phone and tablet online.

Features:

- Find your phone on a map through geolocation using both GPS and Wi-Fi triangulation
- Lock your device from any unwanted intruder
- Trigger a loud alarm remotely even if your phone is put on silent
- Display a tailored alert message on the screen
- Gather the network information that your device is connected to (for accurate pinpointing)

My AntiTheft

Source: http://myantitheft.com

My AntiTheft helps to track and recover your lost or stolen property (computers, smartphones and tablets). It ensures the protection of your personal identity and data as well as provides the best tracking and location solutions to recover lost or stolen devices.

Its features include Device Lockdown, Tracking, Spy Camera, Audible Alarm, Wipe, Tamper Proof, Google Account Integration, and Web Control Panel.

Where's My Droid

Source: http://wheresmydroid.com

Where's My Droid is an Android device tracking tool that allows you to track your phone from anywhere, either with a text messaged attention word or through the online control center known as Commander.

Features:

- Find phone by making it ring/vibrate
- Find phone using GPS location
- GPS Flare - Location alert on low battery
- Passcode protection to prevent unauthorized app changes
- Notification of changed SIM card or phone number
- Stealth Mode hides incoming text with attention word

iHound

Source: https://www.ihoundsoftware.com

iHound uses the GPS and Wi-Fi, 3G, or Edge signals built into your devices to determine its location. Using the app and iHound software's unique tracking website, you can:

Features:

- Track the location of your device
- Remotely Lock Your Phone
- Remotely Wipe Private Information
- Set up Geofencing Location Alerts

GadgetTrak Mobile Security

Source: *http://www.gadgettrak.com*

GadgetTrak Mobile Security helps mitigate the risk of mobile device loss or theft, allowing you to track its location, back up data, and wipe the device remotely.

Features:

- **Locate & Find** – Advanced hybrid positioning (uses combination of GPS, Wi-Fi positioning, and cell tower triangulation) and device alarm
- **Data Protection** – Secure encrypted backup and remote data wipe
- **Security** – SIM change detection and tamper proof

Total Equipment Protection App

Source: *https://protection.sprint.com*

Total Equipment Protection App enables you to locate your phone if lost or theft. It provides backup of photos and videos, wipe data, built-in antivirus security, and others.

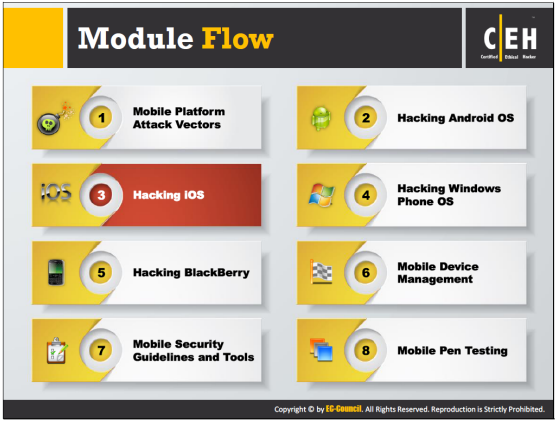
AndroidLost.com

Source: *http://www.androidlost.com*

AndroidLost.com allows you to remotely control your Android phone via the Internet or by SMS.

Features:

- Lock the phone
- Wipe the phone
- Remote control alarm
- View location of phone on the map
- Notifies if SIM card is changed
- Erase SD (secure digital) card



iOS is a mobile operating system developed by Apple. Apple does not license iOS for installation on non-Apple hardware. The company has increased its product range by including mobile phones, tablets, smartwatches, and other mobile devices. The increase in use of Apple devices has grabbed the attention of attackers. The design flaws in iOS make it vulnerable to malicious apps, hidden network profiles, man-in-the-middle attacks, and others. Attackers hack the iOS to gain root-level access to these devices.

This section deals with introduction to Apple iOS jailbreaking iOS; the types, tools, and techniques of jailbreaks; guidelines for securing secure iOS devices; and iOS device tracking tools.

iOS manages the device hardware and offers various technologies required to implement native apps.

At the highest level, iOS acts as an intermediary between apps you create and the underlying hardware. Apps communicate with the underlying hardware via a set of well-defined system interfaces. The iOS architecture comprises of four layers (Cocoa Touch, Media, Core Services, and Core OS). The lower-level layers contain fundamental services and technologies, whereas the higher-level layers build upon the lower layers, provide more sophisticated services and technologies.

Discussed below are the layers of iOS:

- **Cocoa Touch**

  This layer contains key frameworks that help in building iOS apps. These frameworks define the appearance of app, offers basic app infrastructure, and supports key technologies such as multitasking, touch-based input, push notifications, and many high-level system services.

- **Media**

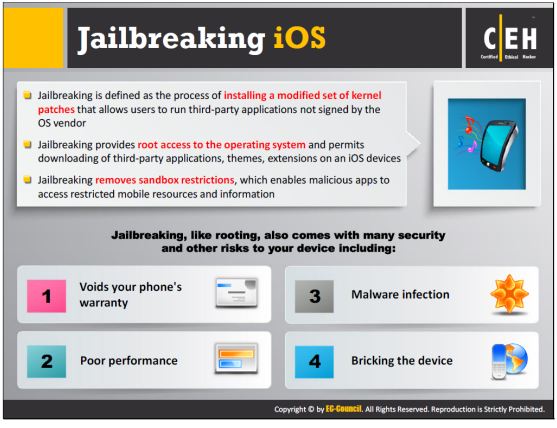
  This layer contains the graphics, audio, and video technologies that enable multimedia experiences in apps.

- **Core Services**

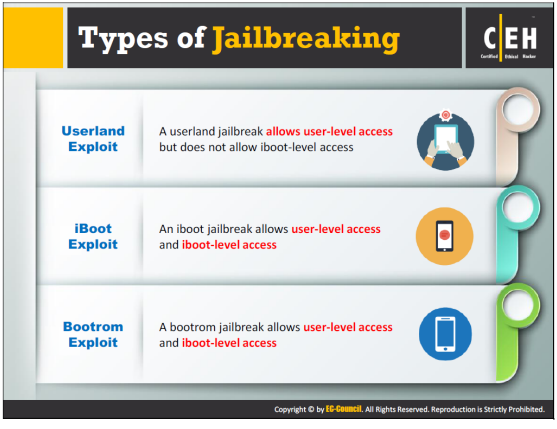
  This layer contains fundamental system services for apps. Key among these services are Core Foundation and Foundation frameworks (defines the basic types that all apps use). Individual technologies that support features such as social media, iCloud, location, and networking also belong to this layer.

- **Core OS**

  This layer contains low-level features on which most other technologies are built. Frameworks in this layer are useful when dealing explicitly with security or communicating with an external hardware accessory.



Jailbreaking iOS is the process of bypassing user limitations as set by Apple, such as modifying the OS, attaining admin privileges, and installing unofficially approved apps via "side loading." You can accomplish jailbreaking simply by modifying iOS system kernels. A reason for jailbreaking iOS devices such as iPhone, iPad, and iPod Touch is to expand the feature set restricted by Apple and its App Store. Jailbreaking provides root access to the operating system and permits downloading of third-party applications, themes, and extensions that are unavailable through the official Apple App Store. Jailbreaking also removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information. One can use tools such as Pangu, Absinthe, RedSn0w, evasi0n7, and GeekSn0w to jailbreak iOS devices.



Discussed below are the three types of Jailbreaking:

- **Userland Exploit**

  A userland exploit uses a loophole in the system application. You cannot secure iOS devices against this exploit, as nothing can cause a recovery mode loop. Only firmware updates can patch these types of vulnerabilities.

- **iBoot Exploit**

  This type of exploit can be semi-tethered if the device has a new bootrom. This exploit takes advantage of a loophole in iBoot (iDevice's third bootloader) to delink the code-signing appliance. Firmware updates can patch these types of exploits.

- **Bootrom Exploit**

  A bootrom exploit uses a loophole in the SecureROM (iDevice's first bootloader) to disable signature checks, which can be used to load patch NOR firmware. Firmware updates cannot patch these types of exploits. Only a hardware update of bootrom by Apple can patch this exploit.

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**

Jailbreak. Pangu iOS 7.1-7.1.x

http://en.pangu.io

Untethered Jailbreaking of iOS 7.1.1/7.1.2 Using Pangu for Mac

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

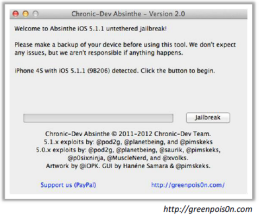
Redsn0w

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

http://redsn0w.info

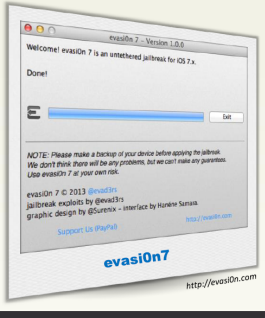
Absinthe

- 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



http://evasi0n.com

http://geeksn0w.it

Discussed below are a few more jailbreaking tools:

Sn0wbreeze

Source: *http://ih8sn0w.com*

Sn0wBreeze is a jailbreaking tool for Windows OS used to create a custom Pre-Jailbroken iOS firmware file to restore your iPhone, iPod Touch, or iPad, if it were to become jailbroken. It allows iPhone unlockers to update to the latest firmware without updating their baseband in the process. This gives you full control over your jailbreak, allowing you to customize advanced options such as your root partition size.

PwnageTool Features:

Source: *http://blog.iphone-dev.org*

- Allows iPhone unlockers to update to the latest firmware without updating their baseband in the process
- Gives full control over the Jailbreak; allowing to customize advance options such as root partition size

Given below are few more jailbreaking tools:

LimeRa1n

Source: *http://www.limera1n.com*

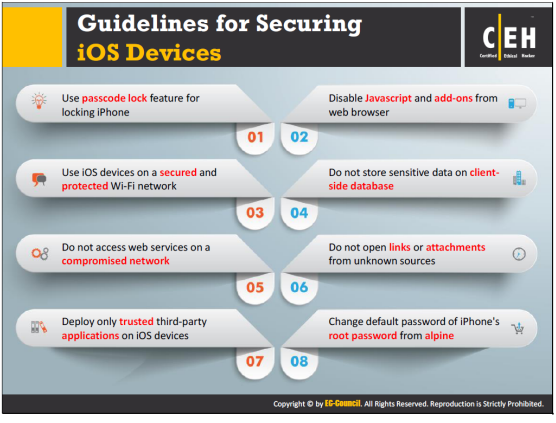
LimeRa1n is a jailbreaking tool invented by GeoHot (professional hacker) to halt Chronic Dev from releasing a bootrom exploit called SHAtter. One of its features includes enabling you to switch between jailbreaking methods; it supports both Windows and Mac OS X operating systems.

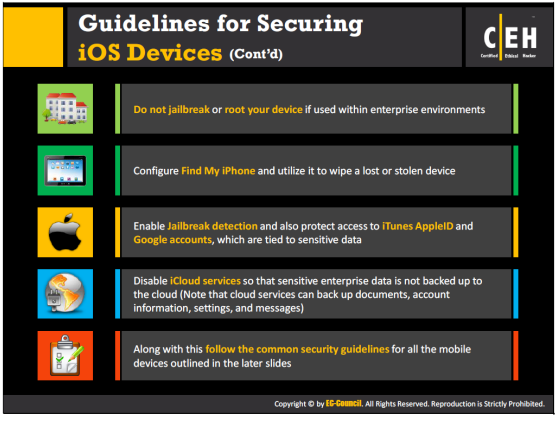
Blackra1n

Source: *http://blackra1n.com*

Blackra1n is a jailbreaking tool developed by GeoHot that allows you to jailbreak devices such as an iPhone, iPod, or iPad on firmware. This can work on all devices without having to make adjustments in the software in advance. It works on both Windows and Mac OS X.

To execute the unsigned code, the program uses a bug in the USB code of the firmware for iDevices. Blackra1n uses this exploit to patch the firmware of the iDevice while in DFU (Device Firmware Upgrade) mode. This mode is useful while upgrading firmware through iTunes, but also can be activated by the user. The program allows users to install the Cydia, Icy (removed in blackra1n RC3), and Rock package managers, which allow the user to access tweaks, and homebrew applications, the root directory, and the file system of the iDevice.





Listed below are some additional guidelines that help you to secure iOS devices and their data from attackers:

- Enable the Passcode Lock feature on your iPhone. Go to **Settings → Touch ID & Passcode Lock**, and then tap **Turn Passcode On.**
- Set **separate passcodes** for the applications containing sensitive data.
- Always download applications from the **Apple App Store.**
- Set the **Auto-Lock Timeout** to enter a passcode after a set time. Go to **Settings → General → Auto-Lock.**
- Enable **Ask to Join Networks** function, this prevents you from randomly connecting to available Wi-Fi networks. Go to **Settings → Wi-Fi → Ask to Join Networks.**
- Regularly **update** your device OS with security patches released by Apple. To receive updates connect to the **iTunes**. For iOS5 and greater, updates can be received using **Settings → General → Software Updates.**
- Enable **Erase Data** feature on iPhone to erase all the data and settings completing 10 attempts. Go to **Settings → Touch ID & Passcode → Erase Data.**
- Disable the **Voice Dial** feature on iPhone to prevent attackers from accessing the phone without entering a passcode. Go to **Settings → Touch ID & Passcode**, and then **Turn Voice Dial to OFF.**

- Delete **Keyboard Cache** on iPhone to remove all your keystrokes recorded. Go to **General → Reset**, tap on **Reset Keyboard Dictionary**, and then **Confirm** on the warning screen.
- Disable **Geotagging** (storage of location-based data in images) on the iPhone. Go to **Settings → Privacy → Location Services**, and then toggle the **Camera to OFF**.
- Enable **Safari's Privacy and Security Settings** on the iPhone. Go to **Settings → Safari**. Here you can Enable Block Pop-ups, Disable Passwords and AutoFill, Enable Fraudulent Website Warning, Block cookies, Clear History and Website data, and others.
- Enable **Do Not Track** feature to keep your web browsing private. Go to **Settings → Safari →** and then enable **Do Not Track** option.
- Disable **Bluetooth** when not in use. Go to **Settings → Bluetooth**, and then **toggle it to OFF**.
- Disable **Wi-Fi** when not in use. Go to **Settings → Wi-Fi,** and then **toggle it to OFF**.
- Set **separate passwords** for the applications containing sensitive data.
- Always download applications from the **Apple App Store**.

Note: The paths given above to enable/disable respective features may change based on the iOS version or device used.

Given below are few iOS device tracking tools:

Find My iPhone

Source: *https://itunes.apple.com*

Find My iPhone iOS Device tracking tool allows you to use another iOS device to track a lost or misplaced mobile, iPhone, iPad, iPod touch, or Mac and protect its data. To use this, you need to install the app on another iOS device, open it, and sign in with your Apple ID. It helps you locate your missing device on a map, remotely lock it, play a sound, display a message, and erase all the data on it.

If the iDevice you want to locate is running iOS 6 or later, Find My iPhone also includes Lost Mode. Lost Mode locks your missing device with a passcode and can display a custom message such as a contact phone number right on the Lock Screen. While in Lost Mode, your device can also keep track of where it has been, so you can view its recent location history from the Find My iPhone app.

iHound

Source: *https://www.ihoundsoftware.com*

iHound is an iOS device tracking tool that allows you to track your device by simply turning it on, minimizing it, and letting it run. It uses a combination of the significant location GPS, real-time GPS, and Wi-Fi signals built into your devices to determine its location.

Using the app and iHound Software's tracking website, you can:

- **Track the location of the device**: The iHound App reports your location to iHound's servers every time the device makes a significant location change.
- **Sound the alarm**: Sends your iPhone or iPod Touch a push notification with a loud alarm.
- **Set up Geofencing Location Alerts**: Receive alerts and check in automatically with Facebook, Foursquare, and/or Twitter when you arrive. It is simple to use and completely "opt in."
- **Manage your account using iHound's Mobile Web Site**: Track multiple devices on multiple platforms, and set up "geofences" while you are on the go.

GadgetTrak iOS Security

Source: http://www.gadgettrak.com

With GadgetTrak, one can increase the chances of recovering his or her lost iPhone, iPad, or iPod touch. This app has the ability to track devices and even snap a photo of the thief.

Features:

- **Advanced hybrid positioning**: Uses a combination of GPS, Wi-Fi positioning, and cell tower triangulation to pinpoint the device location.
- **Push notifications**: Sends a discrete message to user's device enticing the thief to initiate a tracking report.
- **Camera support**: Snaps a photo with built-in cameras to collect crucial evidence that can help in catching the thief.
- **Location Reports**: When tracking occurs, the user receives an email with detailed information about its current location.
- **Tamper proof**: Once tracking is activated, the software settings cannot be modified unless deactivated.
- **Secure Connection**: When tracking data is being transmitted from your device, a secure SSL connection is used.
- **Privacy Safe**:
  - Only the user of the device can access the location reports and camera.
  - All images, network information, and location data are sent directly to the user from his or her device .

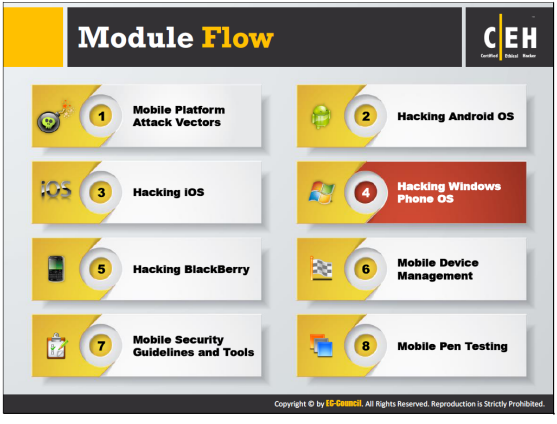
iLocalis

Source: http://ilocalis.com

With iLocalis, you can control your iPhone from your computer connected to the Internet. If you lost your iPhone or it is stolen, you can find it with the track feature, or even make a remote call or SMS to see the new number to check whether the SIM is changed or not.

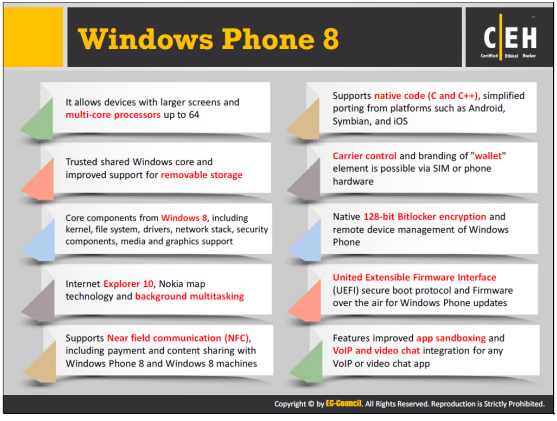
Features:

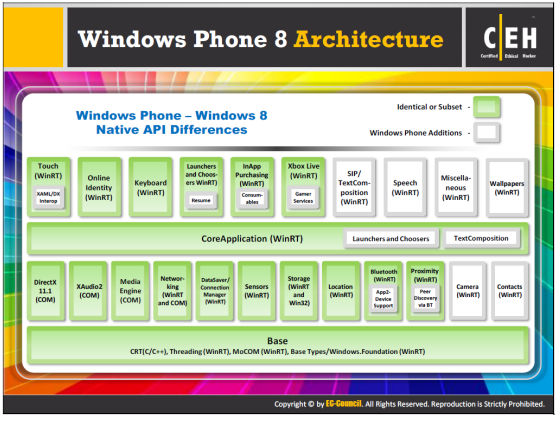
- Location tracking
- Share your location with others
- Notify friends nearby
- Remote iPhone control
- Remote SMS commands
- Remote backup
- Remote wipe
- Alter zones
- Push support
- Remote audio recording
- Remote iPhone lock
- Lock iLocalis uninstallation

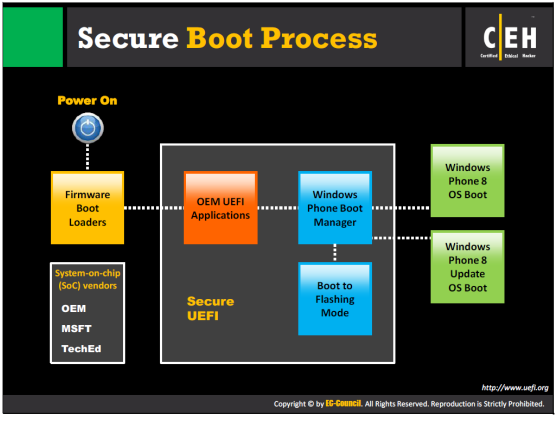


Windows Phone OS is an operating system built by Microsoft for mobile devices. The OS is used across devices such as mobile phones, tablets, and phablets. This operating system also is vulnerable to certain attacks and attackers try to take advantage of unpatched security vulnerabilities in Windows Phone OS to launch attacks in order to steal confidential data stored on the devices running on it.

This section discusses Windows Phone 8 and its architecture, secure boot process, guidelines to secure Windows OS devices, and Windows OS device tracking tool.







Windows Phone 8 platform integrity is maintained by means of secure boot and code-signing features. These features protect the Windows Phone 8 boot process and OS from malware attacks (especially rootkits), allowing only trusted software components to execute.

Secure boot process validates firmware images on Windows phone devices before they load the OS. All boot components have cryptographically validated digital signatures from the pre-UEFI (**Unified Extensible Firmware Interface**) boot loaders to the UEFI environment. Secure boot ensures that it is the authorized code executed, to initialize the device and load the Windows Phone OS.

Windows Phone architecture uses a **System-on-a-Chip** (SoC) design. The SoC vendors and device manufacturers provide the pre-UEFI boot loaders and the UEFI environment. The UEFI environment implements the UEFI secure boot standard that describes a process by which all UEFI drivers and applications are validated against keys provisioned into a UEFI runtime variable before they are executed.

Once the boot processes of pre-UEFI and UEFI components finishes, the Windows Phone boot manager takes over to complete the boot process. The user can then use the smartphone. Microsoft, together with OEM drives and applications, signs all code in the Windows Phone OS. In addition, applications added after device manufacturing or in-store installation, must be properly signed to run in the Windows Phone.

Source: *http://www.uefi.org*

In Windows Phone, many security features are turned-on by default. Below are additional guidelines that enable you to enhance the security of your Windows Phone devices and their data:

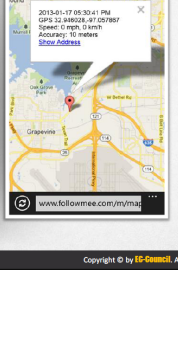
- Setup **passwords** for Windows Phone lock screen. Go to **Settings → lock screen → Password**, and then set a complex password for the device.
- Keep your phone updated with Windows Phone **security updates**. Go to **Settings → phone update**, and then tap **check for updates**.
- Make sure to clear all your browsing history from **Internet Explorer**. Go to **Internet Explorer → Settings**, tap **delete history**, and then **confirm** the deletion.
- Protect your **Windows Phone SIM** (Subscriber Identity Module) with a **PIN** (Personal Identification Number). Tap → **SIM security**, and then enter a **SIM PIN**.
- Disable **Wi-Fi** when not in use. Go to **Settings → Wi-Fi**, and then tap **Wi-Fi networking** to **OFF**.
- Disable **Bluetooth** when not in use. Go to **Settings → Bluetooth**, and then tap **Status** to **OFF**.
- Configure **Find My Phone** to help you locate the phone and to remotely wipe sensitive data from Windows Phone if lost or stolen.

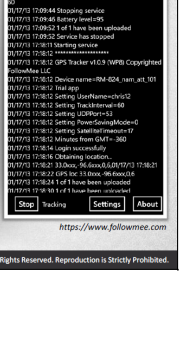
- Enable **apps corner,** which lets you set up a **custom Start screen** on your device, on which you can share only the apps of your choice with the people you allow to use your phone. Go to **Settings → apps corner**, select the apps you wish to share, and then tap **launch**.
- Enable **VPN** to access Internet in an organization over a **secure channel**. Go to **Settings → VPN**, and then tap **Status** to **ON**.

Note: The paths given above to enable/disable the respective features may change according to the Windows Phone OS version or device used.

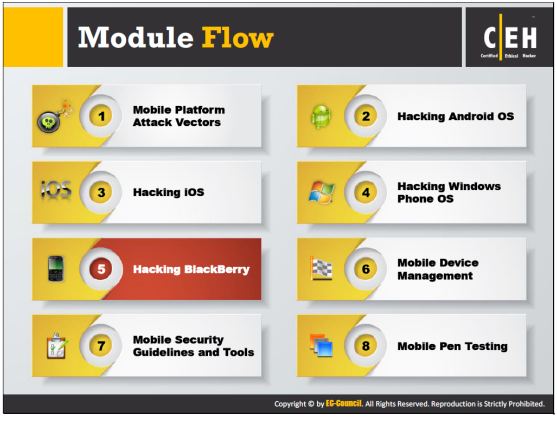
Windows OS Device Tracking Tool: FollowMee GPS Tracker

- 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**



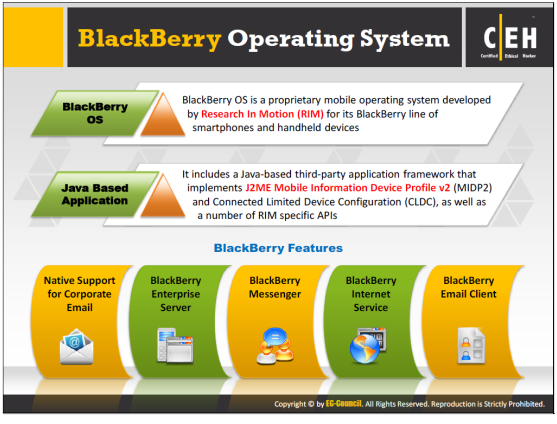


https://www.followmee.com



BlackBerry refers to a line of wireless handheld devices and services designed and marketed by BlackBerry (formerly known as Research In Motion [RIM]) Limited. Built for professional use, Blackberry devices store sensitive work-related information, which attracts attackers. The attackers try to exploit vulnerabilities in the BlackBerry device according to its hardware, OS, or firmware bugs to steal sensitive information.

This section discusses the BlackBerry operating system, enterprise solution architecture, and attack vectors; the guidelines for securing BlackBerry devices; and BlackBerry device tracking tools.



BlackBerry OS is a proprietary mobile operating system developed by Research In Motion (RIM), currently known as BlackBerry Limited. This OS exclusively works for BlackBerry line of smartphones and wireless handheld devices. It provides multitasking and supports specialized input devices such as trackwheel, trackball, trackpad, and touchscreen adopted by BlackBerry for use in its handhelds. Third-party developers can use BlackBerry API classes to create software and apps for BlackBerry devices. 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.

Features:

- **Native Support for Corporate Email**

  BlackBerry platform provides support for corporate email via MIDP, which allows complete wireless activation and synchronization with Microsoft Exchange, Lotus Domino, or Novell GroupWise email, calendar, tasks, notes, and contacts, when used with BlackBerry Enterprise Server. It also supports WAP 1.2.

- **BlackBerry Enterprise Server (BES)**

  BES is a middleware software package and is a part of BlackBerry wireless platform delivered by BlackBerry Ltd. It enables BlackBerry devices to connect to the corporate messaging and collaboration software (MDaemon Messaging Server, Lotus Domino, Microsoft Exchange, and Novell GroupWise) and redirects emails and synchronizes

contacts and calendaring data among mobile devices, desktop workstations, and servers.

- **BlackBerry Messenger**

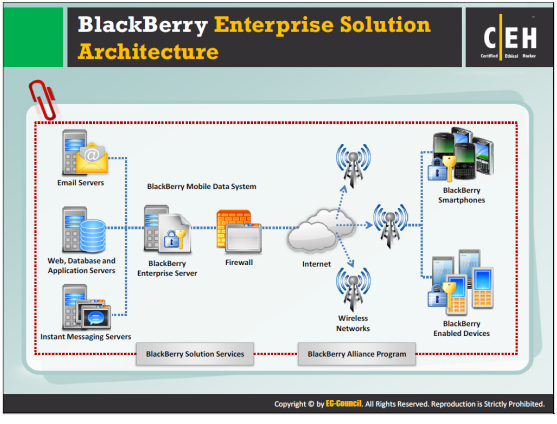
  BlackBerry Messenger (BBM) is a proprietary Internet-based PIN instant messenger and video telephony application that enables messaging and voice calls between BlackBerry, iOS, Windows Phone, and Android users.

- **BlackBerry Internet Service**

  BlackBerry Internet Service is an email and synchronization service that lets users to receive email from multiple POP3, IMAP, and Outlook Web App (OWA) on BlackBerry, and synchronize contacts, deleted items, and so on from some email providers.

- **BlackBerry Email Client**

  LogicMail is a discrete BlackBerry e-mail client that provides support for email protocols such as IMAP, POP, and SMTP over the device's Internet connection. It serves as an alternative to the service-oriented "push" E-mail system that comes along with the device.



The BlackBerry enterprise solution architecture includes various components that lets you to extend organization's comunication methods to BlackBerry devices.

Component	Description
BlackBerry Administration Service	• It connects to the BlackBerry Configuration Database. It manages BlackBerry Enterprise Server components, user accounts, and features for a BlackBerry device
BlackBerry Attachment Service	• It converts supported message attachments into a format that the user can view on a BlackBerry device
BlackBerry Collaboration Service	• It provides a connection between organization's instant messaging server and the collaboration client on a BlackBerry device

BlackBerry Configuration Database	• It is a relational database that contains configuration information that BlackBerry Enterprise Server components use
	• Information it stores include:
	  ○ details about the connection from a BlackBerry Enterprise Server to the wireless network contact list
	  ○ address mappings between PINs and email addresses for BlackBerry MDS Connection Service push features
	  ○ read-only copies of device transport keys, which encrypt the message keys that encrypt data that the BlackBerry Enterprise Server and BlackBerry device send between each other

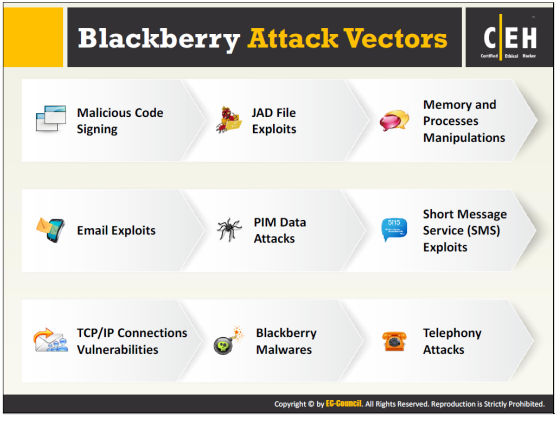
BlackBerry Controller	• It monitors other BlackBerry Enterprise Server components and restarts them if they stop responding
BlackBerry® Desktop Software	• It is an integrated suite of applications that a user installs on the user's computer • It manages the association between a BlackBerry device and the email account, synchronizes organizer data, calendar entries, and inboxes, and permits the user to download applications and BlackBerry® Device Software updates to a BlackBerry device
BlackBerry device	• It provides the user with access to BlackBerry services such as messaging and browsing
BlackBerry Device Software	• It consists of applications on a BlackBerry device that permit the user to send and receive email messages, PIN messages, and text messages; manage calendar entries; etc.
BlackBerry Dispatcher	• It compresses and encrypts all data that a BlackBerry device sends and receives • It sends the data through the BlackBerry Router, to and from the wireless network
BlackBerry Enterprise Server	• It consists of various components that process, route, compress, encrypt, and send data over the wireless network to a BlackBerry device • It opens a two-way connection that is highly secure between the user's email account and the BlackBerry device
BlackBerry® Infrastructure	• It is designed to manage the wireless transport of messages between the wireless network and a BlackBerry device
BlackBerry® Internet Service	• It provides a subscriber with messaging service and access to Internet content on a BlackBerry device
BlackBerry Mail Store Service	• It connects to the messaging servers in the organization environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts on the messaging servers
BlackBerry MDS Connection Service	• It permits the user to access web content, the Internet, or organization's intranet from a BlackBerry device • It also permits applications on a BlackBerry device to connect to the organization's application servers or content servers to retrieve application data and updates
BlackBerry MDS Integration Service	• It provides application-level integration for BlackBerry® MDS Runtime Applications and BlackBerry® Browser Applications on BlackBerry devices • It can also install BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on a BlackBerry device

BlackBerry MDS Integration Service database	It stores application data for the BlackBerry MDS Integration Service
BlackBerry® MDS Studio	It enables organization's developers to create BlackBerry MDS Runtime Applications and to publish the applications to the BlackBerry MDS Application Repository
BlackBerry Messaging Agent	It connects to the organization's messaging server to provide messaging services, calendar management, contact lookups, attachment viewing, and attachment downloading. It also generates device transport keys and acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. It synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.
BlackBerry® Mobile Voice System	It integrates the organization's PBX phone system with the BlackBerry Enterprise Server to extend desk phone features to a BlackBerry device
BlackBerry Monitoring Service	It helps to monitor organization's BlackBerry Domain It can also be used to troubleshoot issues and monitor the health of the organization's BlackBerry Domain proactively
BlackBerry Policy Service	It sends IT policies and IT administration commands and provisions service books It sends service books to configure settings for features and components on a BlackBerry device.
BlackBerry profiles database	It is an IBM Lotus Domino database that the BlackBerry Enterprise Server for IBM Lotus Domino uses to store configuration data for the user account
BlackBerry® Provisioning System	It permits wireless service providers to configure and manage BlackBerry services for their subscribers A wireless service provider can assign, activate, deactivate, suspend, and resume BlackBerry services and check the status of service requests for a BlackBerry device on the wireless network.
BlackBerry Router	It connects to the wireless network to send data to and from a BlackBerry device It also sends data over the organization's network to a BlackBerry device that is connected to a computer that hosts the BlackBerry Device Manager
BlackBerry® Smart Card Reader	It controls access to the organization's sensitive communications using Bluetooth® technology and the latest encryption technologies It also permits an organization to use two-factor authentication.

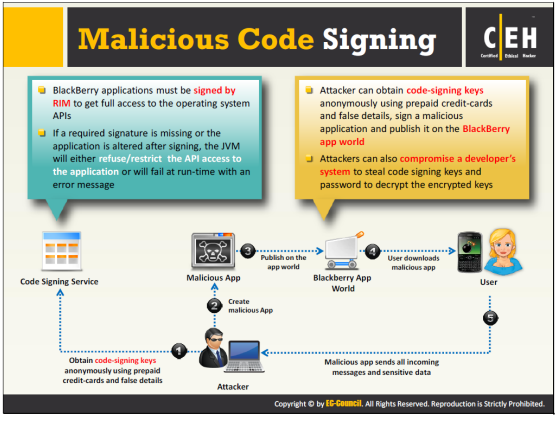
BlackBerry state databases	• They are Lotus Domino databases that the BlackBerry Enterprise Server for IBM Lotus Domino uses to store data that associates email messages that a BlackBerry device sends or receives to corresponding messages in the user's email application • The data in the BlackBerry state databases supports features such as email message reconciliation, email message forwarding, email message filing, and replying with text
BlackBerry Synchronization Service	• It synchronizes organizer data between a BlackBerry device and the organization's messaging server over the wireless network
instant messaging server	• It stores instant messaging accounts
messaging server	• It receives, sends, and stores all email messages
organization's application server or content server	• Your organization's application server or content server provides push applications and intranet content that the BlackBerry MDS Services use to install on a BlackBerry device

TABLE 15.2: Various components of BlackBerry Enterprise Solution

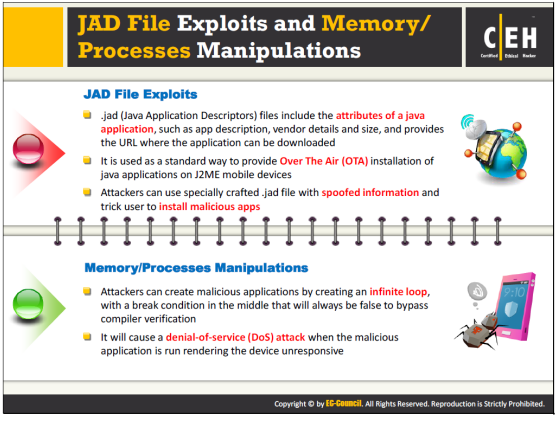
Source: *http://global.blackberry.com*



BlackBerry attack vectors enable an attacker to exploit vulnerabilities present in the OS, device firmware, apps, and so on to gain access to the BlackBerry mobile device to deliver a payload or malicious outcome.

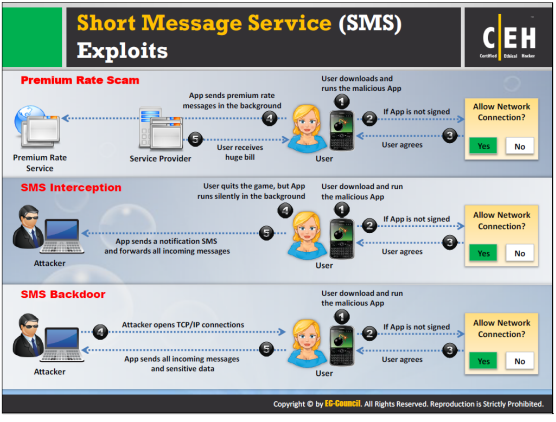


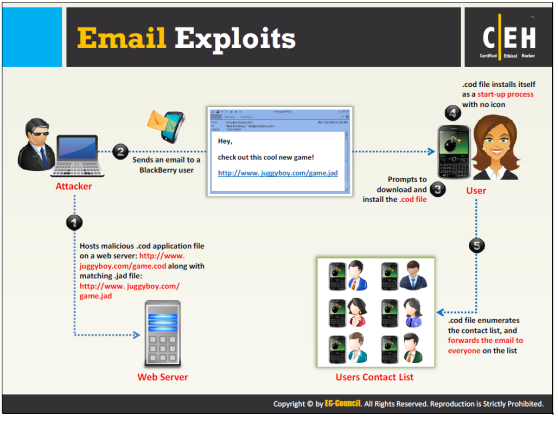
Here, the attacker obtains code-signing keys from the Code Signing Service anonymously by using prepaid credit cards and false details. Then the attacker creates a malicious application and publishes it on the BlackBerry App World. The user connects to the BlackBerry App World and downloads that malicious application (thinking that it is legitimate), thereby allowing the attacker to gain access to his/her device. The malicious application running on the user's device thereafter sends all incoming messages and other sensitive data to the attacker.



JAD File Exploits

When a BlackBerry user opens a .jad file, he/she can go through the application details, and can decide whether to download and install the application or not. However, attackers create a specially crafted .jad file with spoofed information and send it to the user as a hyperlink in the SMS, MMS, or email, tricking him/her to install the malicious app. Measures to mitigate JAD spoofing include employing a firewall, restricting app downloads from untrusted sources, setting application controls and permissions.





Email Exploits

BlackBerry device supports sending, receiving, and reading emails via the **net.rim.blackberry.api.mail** package, only by signed applications. It allows sending any kind of attachment via email but restricts viewing attachments of only supported file types. BlackBerry attachment service enable users to view attachments, and it supports file types that include .doc, .pdf, .txt, .wpd, .xls, and .ppt, but it does not support the executable file types such as .cod.

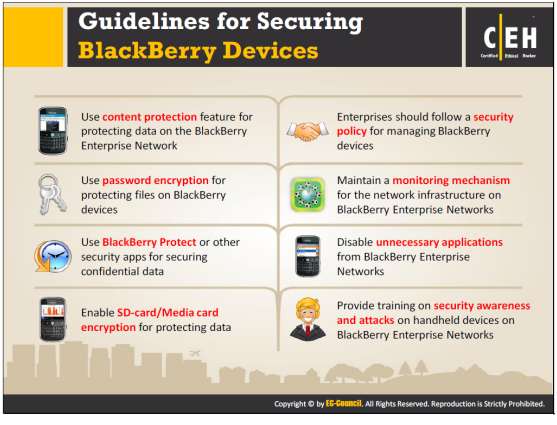
PIM Data Attacks and TCP/IP Connections Vulnerabilities

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**

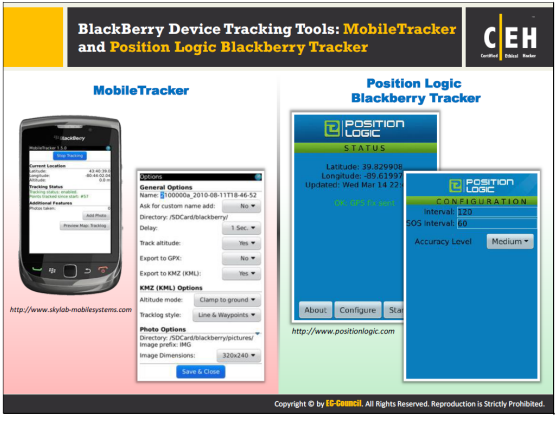
TCP/IP Connections Vulnerabilities

- 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**



Listed below are additional guidelines for securing your BlackBerry devices:

- Enable **Content Protection** feature in BlackBerry by going to **Options → Security Settings** for protecting data on BlackBerry Enterprise Network.
- Enable password protection going to **Options → Password** in the BlackBerry device. You can also set other features such as **timeout duration**, permission for application installation, number of **password attempts**, and logging restrictions.
- Disable **Bluetooth connection** in the BlackBerry device when not in use by selecting **Options** within the Bluetooth section and selecting **No** under the "**Discoverable**" field.
- Use Blackberry's built-in **Password Keeper** utility to save user accounts and passwords.
- Clear the memory of your BlackBerry device to delete sensitive data stored in it by going to **Options → Security Options → Memory Cleaning**.



Discussed below are the BlackBerry device tracking tools:

Mobile Tracker

Source: *http://www.skylab-mobilesystems.com*

MobileTracker records tracklogs using BlackBerry smartphone and allows to view them in Google Earth or publish them with Google Maps. It records data that include latitude, longitude, altitude, timestamp, total time, distance travelled, total number of waypoints, direct distance to start point, and average travelling speed.

Features:

- Records a GPS tracklog
- Elevation and time can be tracked
- Track to SD card or internal memory
- Track to GPX or KML/KMZ file
- View list of tracked tracklogs
- Extensive statistical information and background tracking

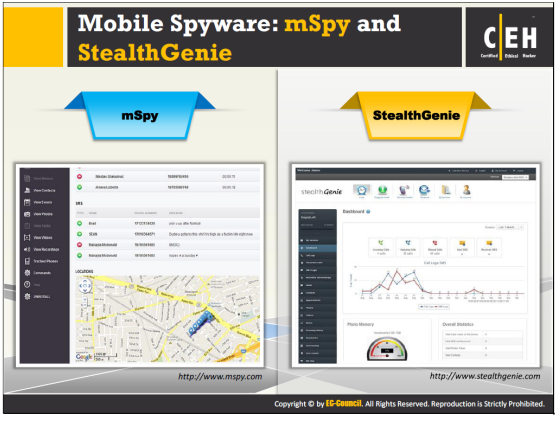
Position Logic Blackberry Tracker

Source: *http://www.positionlogic.com*

Position Logic Blackberry Tracker is a GPS tracking app for Blackberry phones

Features:

- GPS Tracking
- Improved individual supervision
- Reduce theft losses
- Increase employee accountability



Below are a few mobile spywares that obtain information from mobile device without the knowledge or consent of user:

mSpy

Source: *http://www.mspy.com*

mSpy is a mobile monitoring application that can log everything from call history, text messages, WhatsApp chats, to keystrokes and emails. This product is useful for monitoring versatile online/offline actions of employees and underage children.

Features:

- View call history
- Record calls
- Read emails and text messages
- Track location
- View photos and videos
- Lock the device
- Block websites and apps
- Restrict incoming calls
- Get access to calendar and contacts

- Read iMessages and Viber chats
- Track Browsing History
- View Skype chats and WhatsApp chats

StealthGenie

Source: *http://www.stealthgenie.com*

StealthGenie is the cell phone spy and tracking software that lets you monitor all the activities of any iPhone, Blackberry, or Android phone remotely and invisibly.

Features:

- Spy on calls and SMS messages
- View multimedia files
- View GPS location
- View Instant Messengers
- Read emails
- View Internet activities (web browser history, bookmarks, etc.)
- Remotely control the phone (lock phone, view installed apps, etc.)
- Sends alerts and notifications on SIM change

Discussed below are various mobile spyware applications:

Mobile Spy

Source: *http://www.mobile-spy.com*

Mobile Spy helps parents and employers monitor the smartphones and tablets that they own or have proper consent to monitor. They use it to learn about their child or employee's call information, websites visited, text message activities, photos and social media activity, GPS locations, and so on.

Features:

- Monitor WhatsApp and iMessage
- Monitor Facebook and Twitter messages
- View memos, contacts and email
- Block Apps from running on the phone
- View LIVE Screen with LIVE Panel Option

SpyBubble

Source: *http://www.spybubble.com*

SpyBubble is parental control software for mobile phones that allows you to restrict the use of the cell phone while monitoring the phone's activities. It also helps employers to ensure their

employees are working during work hours. It is compatible with smart phones (Android, iPhone, BlackBerry), iPad, and Android tablets.

Features:

- Monitor calls and text messages
- Track GPS location
- Read emails
- Monitor Instant Messengers
- View multimedia files, contacts, and Calendar activities
- Monitor Internet Activities
- Remotely Control Phone

Mobistealth

Source: *http://www.mobistealth.com*

Mobistealth cell phone spyware is comprehensive solution to monitor iPhone, BlackBerry, Android, Nokia and Windows Mobile phones. It tracks all cell phone activities and sends the information back to the Mobistealth user account. It is meant for all parents (worried about child's cell phone activities) and employers (worried about misuse of company owned devices) looking to monitor cell phones of kids and employees.

Features:

- Real-time and historical location tracking
- Videos and pictures logging so parents can see inappropriate ones
- Email and text message logging
- Web history and contact details

FlexiSPY

Source: *http://www.flexispy.com*

FlexiSpy is the mobile monitoring software used to spy on mobile phones and tablets. It supports Android, iPhone, iPad, and BlackBerry.

FlexiSPY features to monitor employees:

- Allows you to keep real-time tabs on whom your employees chats, emails, and SMS messages with
- Ability to judge via GPS positioning the location of your employees
- Monitor and record phone calls for training and quality purposes
- Find out what website your employees are visiting
- Know and block dangerous mobile applications

Highster Mobile

Source: http://www.highstermobile.com

Highster Mobile is a parental and employee monitoring software for mobile phones and tablets.

Features:

- **Remote Access** – Text messages, Calls, GPS, Emails, etc.
- **Tracking** – Calls, SMS, Emails, Chats, Location, Device, etc.
- **Record and view** – Video, Slide Screen, Messages, etc.
- **Get notified** – Data stored in online account for viewing.

SpyPhoneTap

Source: http://www.spyphonetap.com

SpyPhoneTap has a variety of software that lets you convert your mobile phone into a high-tech tracking or surveillance device. It can intercept phone calls and SMS, record conversations, track the location of your target phone, and notify you through SMS.

SpyPhoneTap Features:

- **Spy Phone** – lets you listen to the conversations and sounds surrounding the phone.
- **Cell phone Tracker** – capable of sending the location info of the target phone.
- **SMS Spy** – intercepts all incoming and outgoing SMS of the target phone and creates a duplicate of the SMS which, in turn, is sent to you.
- **Text Alerts** – Sends the incoming caller's number as well as the dialed number to you in real-time via SMS.
- **Call Interceptor** – **Cell Phone Tapping** When the target phone have an ongoing call, whether it's an incoming or outgoing call, an SMS is sent to you and you could call the target phone which then creates a conference call so you could listen to both parties.
- **Control Software Remotely** – Allows you to reboot the software at any given time.
- **SpyPhone SIM Change Alerts** – sends an SMS notification whenever the target phone is turned on or whenever the target phone changes its SIM card.

Spyera

Source: http://spyera.com

Spyera is a cell phone spy app that allows live call listening, live call recording, spy on IM, ambient listening, ambient recording, track SMS messages, track location, track emails, grab passwords, spy on VoIP apps, and so on. It is compatible with Android phone and tablet, iPhone, iPad, BlackBerry, Symbian, etc.

PhoneSheriff

Source: http://www.phonesheriff.com

PhoneSheriff allows you to monitor child or employee's phone or tablet usage.

Features:

- Block phone numbers from calls and text messages.
- Set custom time restrictions and block apps you choose.
- Monitor text messages and get custom activity alerts.
- Real time location tracking and lock commands.

My Mobile Watchdog

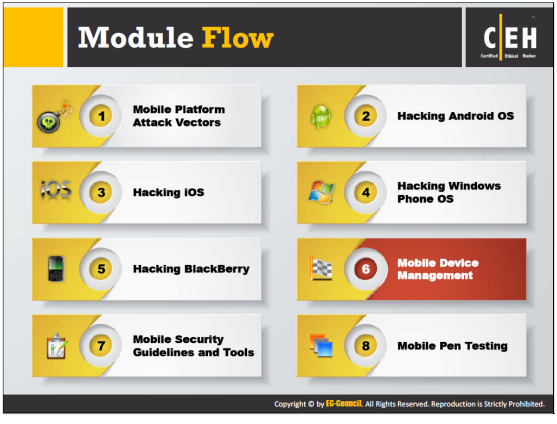
Source: https://www.mymobilewatchdog.com

My Mobile Watchdog is a parental control app that allows you to monitor all of your child's smartphone use from the parent dashboard, setup time limits, app blocking, website blocking, and what alerts you want to receive, and so on.

SpyToMobile

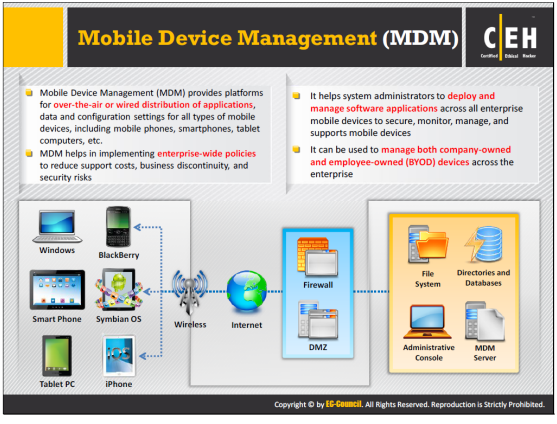
Source: http://spytomobile.com

The SpyToMobile application allows you to intercept incoming and outgoing SMS messages remotely, get contacts list, access call history, and follow the location of the device.



Mobile Device Management (MDM) is gaining much importance with adoption of policies like Bring Your Own Device (BYOD) across the organizations. The increase in types of mobile devices such as smartphones, laptops, tablets, and so on has made it difficult for the enterprises to make policies and manage these devices securely. MDM is a policy that helps to handle the devices carefully, while ensuring that the devices are secure. The companies use a kind of security software for administration of all the mobile devices connected to the enterprise network.

This section deals with Mobile Device Management (MDM) and MDM solutions that help to secure monitor, manage, and support mobile devices.



Basic features of Mobile Device Management (MDM) software include:

- Use of a passcode to the device
- Remotely lock the device if lost
- Remotely wipe data in the lost or stolen device
- Detects if the device is rooted or jailbroken
- Enforce policies and track inventory
- Perform real time monitoring and reporting

MaaS360 Mobile Device Management (MDM) Features:

- **Rapidly enroll mobile devices:** MaaS360 MDM streamlines the platform set-up and device enrollment process
- **Integrate Mobile Devices with Enterprise Systems:** Discovers devices accessing enterprise systems
  - Integrates with Microsoft Exchange, Lotus Notes, and Microsoft Office 365
  - Leverages existing Active Directory/LDAP and Certificate Authorities
- **Centrally Manage Mobile Devices:** MaaS360 provides a unified console for smartphones and tablets with centralized policy and control across multiple platforms
- **Proactively Secure Mobile Devices:** Dynamic security and compliance features continuously monitor devices and take action
- **Streamline Mobile Device Management Support:** MaaS360 helps you diagnose and resolve device, user, or app issues in real time
- **Monitor and Report on Mobile Devices:** MI360™ (Mobility Intelligence) dashboards deliver an interactive, graphical summary of your operations and compliance

Source: *http://www.maas360.com*

In addition to MaaS360 Mobile Device Management (MDM), software technologies that offer integrated mechanisms of all mobile devices in an organization for MDM include:

XenMobile

Source: http://www.citrix.com

XenMobile delivers mobile device management (MDM), mobile application management (MAM), and enterprise-grade productivity apps in one comprehensive solution. It enhances the user experience on BYO or corporate devices without compromising security.

XenMobile enterprise grade mobile device management allows configuring, securing, and supporting mobile devices. It protects company data on any device or corporate asset and selectively wipe any device if lost, stolen, or out of compliance.

Absolute Manage MDM

Source: http://www.absolute.com

Absolute Manage MDM allows organizations to remotely manage and secure iOS, Android, and Windows Phone devices in their deployment. It includes support for employee-owned devices as well as a web-based user interface, so that IT can perform selected administrative and security tasks working remotely or on the go. One can wirelessly (over cellular or Wi-Fi) configure, query, and even wipe or lock managed devices. Absolute Manage MDM is available as an on-premise installation or as a cloud-based solution.

SAP Afaria

Source: http://www.sybase.com

SAP Afaria's software platform delivers centralized control of all mobile devices and tablets including iPhone, iPad, Android, and BlackBerry, as well as the apps that run on them. It offers Enterprises the flexibility to deploy on-premises or partner-hosted.

Device Management Centre

Source: http://www.sicap.com

Sicap's Device Management Centre enables subscribers to easily migrate to smart-phones and cope with the complexities of their advanced devices.

Features:

- Increases usage of data services
- Achieves greater customer retention
- Dramatically reduces customer care costs
- Averts return of full-functioning devices

AirWatch

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

AirWatch® Mobile Device Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. It enables to enroll devices in enterprise environment quickly, configure and update device settings, and secure mobile devices.

With AirWatch, one can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile, Windows PC/RT, and Windows Phone devices from a single management console.

Good Mobile Manager

Source: http://www1.good.com

Good Mobile Manager provides mobile device management (MDM) to support the complete device life cycle. It can control device settings on any managed device and ensure safe access to proprietary business information.

MobileIron

Source: http://www.mobileiron.com

MobileIron's MDM capabilities enable IT to secure and manage mobile devices across multiple operating systems, providing secure corporate email, automatic device configuration, certificate-based security, and selective wipe of enterprise data for both corporate and user-owned devices.

Features:

- Multi-OS support, including iOS, Android, and Windows Mobile

- Establish mobile security policies and compliance rules
- Enterprise infrastructure integration
- On-board certificate authority
- Wi-Fi, email, and VPN Configuration
- Support for bring-your-own-device (BYOD) programs
- Secure access gateway and email attachment protection

Tangoe MDM

Source: *http://www.tangoe.com*

MatrixMobile MDM is a comprehensive monitoring, management, and support software and service suite for mobile devices and applications in the enterprise offering complete control of the device life cycle—from device setup to decommissioning. Mobile device management provides organizations with unmatched visibility and control of any managed device, whether corporate or individual liable, ensuring safe and secure access to invaluable corporate resources.

MDM provides the connected enterprise with the ability to:

- Completely manage mobile device environment within a single console
- Securely access enterprise content from any authorized device
- Enforce security and policy through role-based models
- Allow personal and corporate data to securely coexist on the same device

MatrixMobile MDM includes support for security and policy compliance, application management and deployment, device containerization, content management, anti-virus protection, and MDM-managed services.

MobiControl

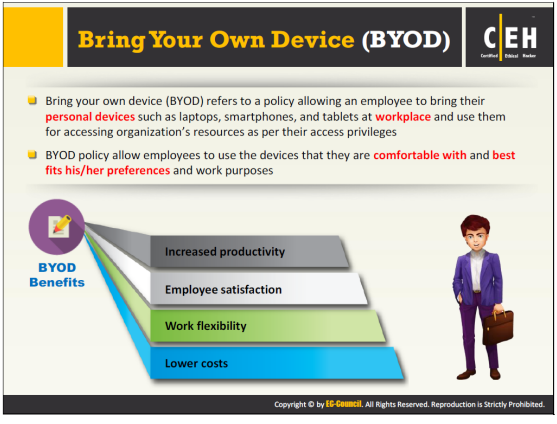
Source: *https://www.soti.net*

MobiControl is the enterprise mobility management (EMM) and bring-your-own-device (BYOD) management solution. MobiControl enables organizations to centrally manage, support, secure, and track corporate-liable and employee-liable mobile devices, regardless of device type, mobile platform, and location.

MediaContact

Source: *http://www.device-management-software.com*

MediaContact is a device-management software program designed for remote computing (mobile and fixed) that combines data synchronization and device management services.



With "**work anywhere**, **anytime**" strategy, the challenge in the BYOD trend is to secure company data and meet compliance requirements.

BYOD Benefits

Adopting BYOD is an advantage to the company as well as the employee. Discussed below are some of the benefits of BYOD:

- **Increased productivity**

  Employees become expert in using their personal devices and this increases productivity from them. In addition, users tend to upgrade their personal devices with cutting-edge technologies. So, the enterprise can benefit from the latest features (both software and hardware) of the device.

- **Employee satisfaction**

  By implementing BYOD, employees use devices of their own choice, for which they invest themselves without the company having selected it. Moreover, employees are more comfortable with their personal devices, as they contain both personal data and corporate data, thus eliminating the usage of multiple devices.

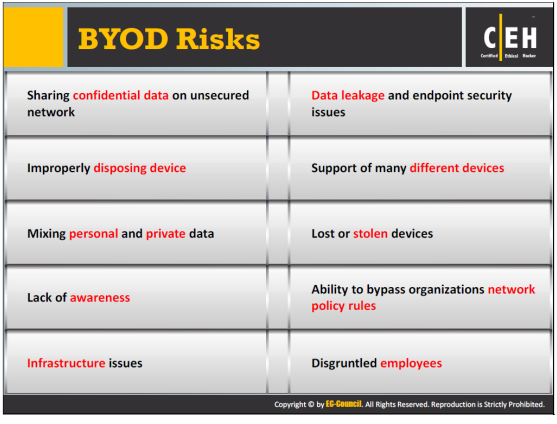
- **Work flexibility**

  By practicing BYOD, employees can carry a single device to satisfy their personal and work needs. The work usually done in the office can be done from anywhere in the world, as employees are provided with access to the corporate data. BYOD users have

more freedom, as their companies do not impose strict rules that they would have to follow in using company property. BYOD replaces the traditional client-server model with a mobile and cloud-centric strategy, which can have far-reaching benefits.

- **Lower costs**

  A business that employs BYOD does not have to spend on devices but saves money, as employee themselves purchase their own devices. In addition, the cost of data services shifts to employees who can take better care of their own property (device).



Employees connecting to the corporate network or accessing corporate data using their own mobile devices pose security risks to an organization. Discussed below are some BYOD security risks:

- **Sharing confidential data on unsecured network**

  Employees might access corporate data via a public network. These connections may not be encrypted; sharing confidential data via an unsecured network may lead to data leakage.

- **Data leakage and endpoint security issues**

  In this cloud-computing era, mobile devices are insecure endpoints with cloud connectivity. By synchronizing with organizational email or other apps, these mobile devices carry confidential information. If the device is lost, it could potentially expose all corporate data.

- **Improperly disposing device**

  A device improperly disposed of could contain a wealth of information, such as financial information, credit-card details, contact numbers, and corporate data. Therefore, it is important to ensure that the mobile device do not contain any data before it is disposed or passed on to others.

- **Support of many different devices**

  Organizations allow employees to access its resources from anywhere in the world, enhancing productivity and driving employee satisfaction. Support of many different devices and processes can increase cost. Employee-owned devices have limited security and come in a variety of different platforms. This deters company's IT department capability to manage and control devices.

- **Mixing personal and private data**

  Mixing personal and corporate data on mobile devices leads to enormous security and privacy implications. Therefore, it is a good practice to keep the corporate data separate from the employee's personal data; this helps an organization to apply specific security measures such as encryption to protect the critical corporate data stored on the mobile device. In addition, it becomes easy for the organization to remotely wipe the corporate data without affecting the employee's personal data when an employee leaves the organization.

- **Lost or stolen devices**

  Due to their small size, mobile devices are often lost or stolen. When an employee loses the mobile device that he/she uses for both personal and official purposes, the organization might face a security risk, as attackers can compromise the corporate data stored in the lost device.

- **Lack of awareness**

  Organizations must educate its employees regarding the BYOD security issues. Failing to do so might result in compromising the corporate data stored in mobile devices.

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

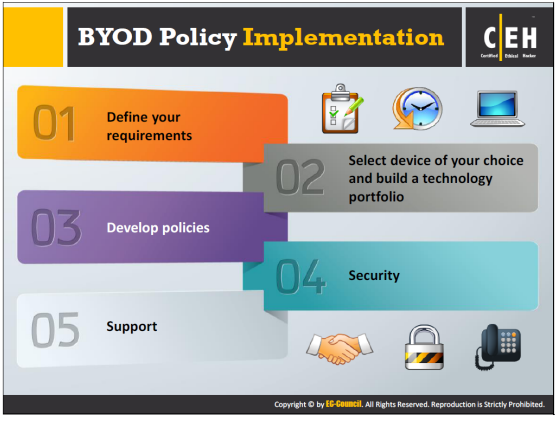
  According to their particular requirements, the policies imposed may differ for wired network and wireless networks. BYOD devices connected to wireless networks have the ability to bypass organization network policy rules enforced only on wired LANs.

- **Infrastructure issues**

  A BYOD program involves dealing with various platforms and technologies. Not all employees carry the same devices. Different devices, each running different OSs and programs, come with their own security loopholes. Thus, it can be problematic for an IT department to set up and maintain infrastructure to support different device needs such as managing data, security, back up, and compatibility among devices.

- **Disgruntled employees**

  Disgruntled employees in an organization can misuse corporate data stored on their mobile devices. They may also leak sensitive organization information to competitors.



It could be argued that BYOD policy implementation could reap significant benefits to an organization, ranging from higher user satisfaction to greater productivity working with advanced devices. However, the nature of new technology and processes could pose risks to an organization if not properly managed. Discussed below are the five principles involved in BYOD policy implementation, using which an organization can minimize risk concerns associated with data security and privacy.

Define your requirements

Not all user requirements are alike. Thus, organize or group employees using mobile devices at work, into segments considering job criticality, time sensitivity, value derived from mobility, data access, and systems access. It is best to define end-user segments by location/type of worker (e.g., employee working from home: full-time remote; day extender: part time remote). Next, align a technology portfolio for each segment, as per user needs.

Carry out a privacy impact assessment (PIA) at the very beginning of each BYOD project, in the presence of all the relevant teams, after assigning responsibilities and collecting the requirements. A PIA provides an organized procedure to document facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project life cycle, and should be a central activity carried out by your mobile governance committee (end-users from each segment/line of business and IT management).

Select the devices of your choice and build a technology portfolio

Decide how you want to manage your users and their data access.

Apart from MDM system that provides a minimum level of control, you may use other options such as virtual desktops or on-device software to improve security and data privacy. Also, ensure that your corporate environment supports WLAN device connectivity and management.

Develop policies

A delegation of company resources should develop the policies, not just the IT. It should include key participants: HR, Legal, Security, and Privacy.

Key components of a general BYOD policy:

- Information security concerns
- Data protection concerns
- Confidentiality and ownership issues
- Information regarding any tracking/monitoring
- Considerations regarding termination of employment
- Guidance regarding how to assess the security of Wi-Fi networks
- Acceptable and unacceptable behavior

Ensure that end users have a clear idea about the acceptable-use policy prior to entering a BYOD program. Finally, organizations must ensure that their BYOD policy is applicable against their employees and any third parties on their behalf, should the need arise, and follow through with its implementation.

Security

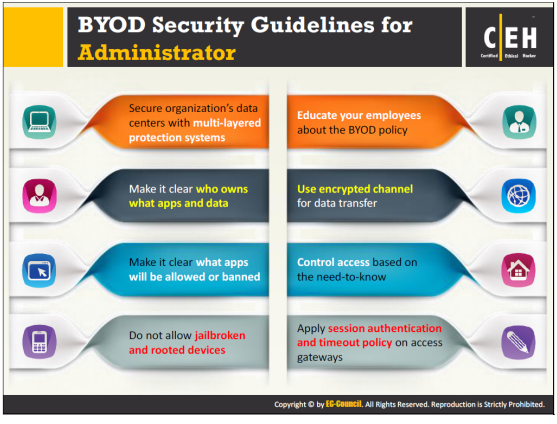
Mobile management technology is effective only when policies are established, implemented, and supported. It is essential that the organizations keep the mobile ecosystem adequately secure to make the BYOD programs work. This requires thorough assessment of the operating environment, and the development of a solution that provides for: asset and identity management, local storage controls, removable media controls, network access levels, network application controls, corporate versus personal app controls, Web and messaging security, device health management, data loss prevention, and so on.

Mainly consider assessing and documenting risks in:

- Information security (for data, application and user segment)
- Operations security (for protecting user information)
- Transmission security (for a secured data transmission)

Support

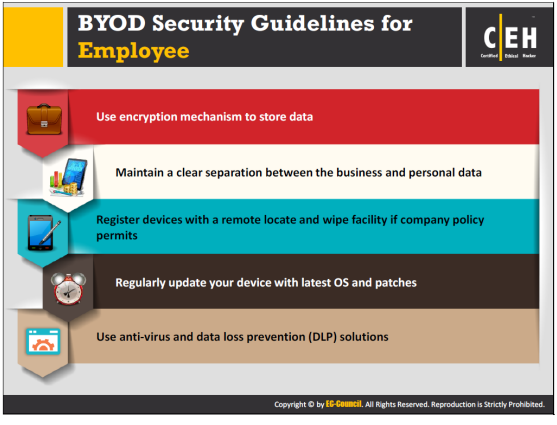
The inconsistent nature of BYOD users will increase the frequency of support calls. The organizations should establish the process and capabilities in early stages to ensure success. Mobile committees should frequently reassess the support levels and ensure productivity of their mobile employees.



With the increase in the use of tablets, smartphones, and other devices at work, mobile security has become a great concern. Listed below are additional security guidelines an administrator should follow to keep the organization's network and data secure:

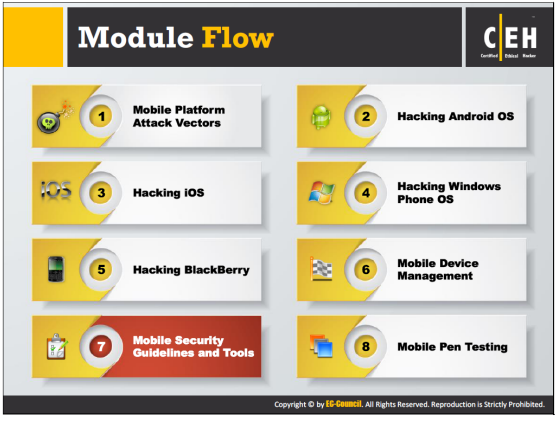
- Impose company WLAN access when on-site.
- Make users to use complex passcodes and change them quite often.
- Ensure that the user's mobile device is registered and authenticated before allowing access to the organization's network.
- Consider multi-factor authentication methods to enhance the security in remotely accessing the organization's information systems.
- Make users to agree and sign the BYOD policy before they can access organization's information system.
- When employee leaves the organization, state whether total device wipe or selective wipe of certain apps and data is required. Also, ensure to maintain organization's data separately from the user's personal data.
- Implement strong algorithms to encrypt all the organization's data stored in the user's mobile, also use an encrypted channel for data transfer.
- In case the user's mobile device lost or stolen, remotely reset or wipe device passwords to prevent unauthorized access to the organization's sensitive data.

- Implement SSL-based VPN, which provides secure remote access.
- Ensure that users' devices are regularly updated with the latest operating systems and other software, which could avoid and sometimes even fix any security vulnerabilities.
- Do not provide offline access to the organization's sensitive information, which should be accessible only via the company's network.



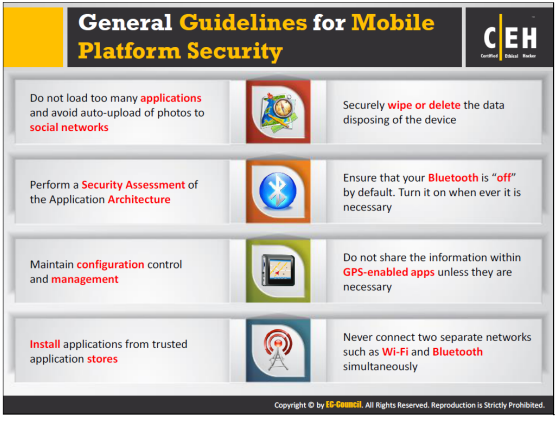
Listed below are the guidelines an employee should follow to secure sensitive personal or corporate information stored on a mobile device:

- Set a strong passcode to the device and change it quite often
- Use strong algorithms to encrypt data
- Set passwords for apps to restrict others from accessing them
- Do not download files from untrusted sources
- Be cautious while browsing websites and opening links or attachments sent via an email



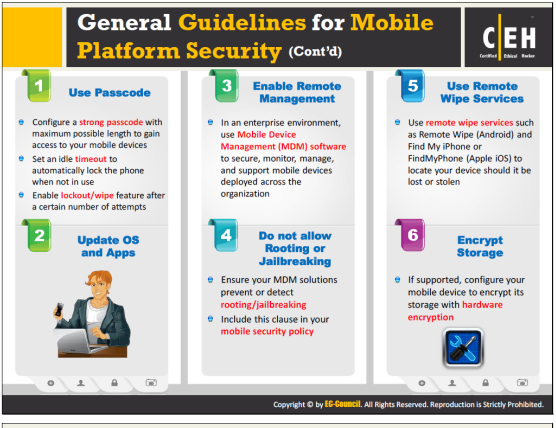
Like personal computers, mobile devices store sensitive data and can be susceptible to various threats. Therefore, it is best to secure them to prevent the compromise or loss of confidential data, to lessen the risk of various threats such as viruses and Trojans, and to mitigate other forms of abuse. To secure these devices, one should take strict measures and use security tools.

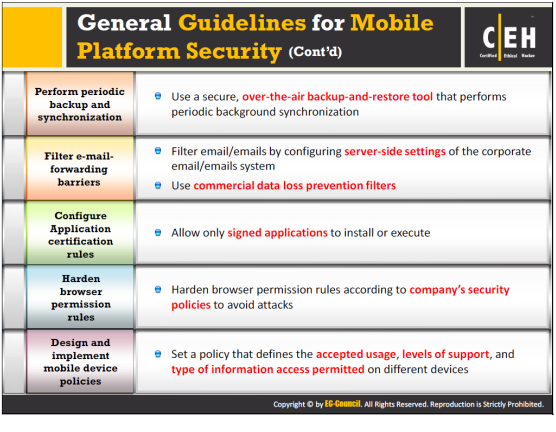
This section deals with various mobile security guidelines and mobile protection tools that help to secure mobile devices.

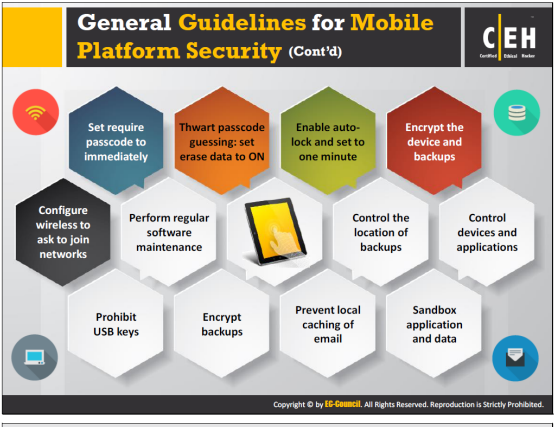


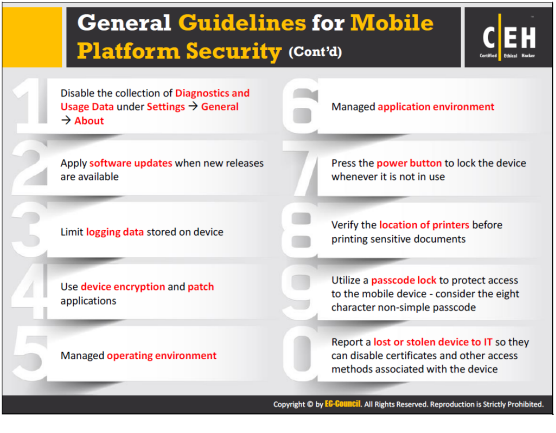
Given below are various guidelines that help one to protect their mobile device:

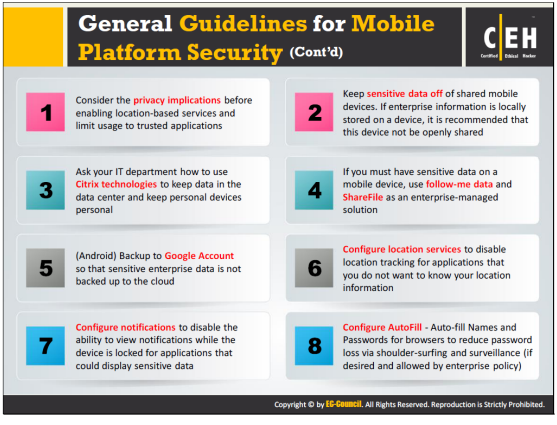
- Disable wireless access such as Wi-Fi and Bluetooth, if not in use, to avoid illegal wireless access to the device
- Use a secure data-transfer utility or encrypt data in transit to or from the device, to ensure confidentiality and data integrity
- Disable sharing/tethering Internet connections over Wi-Fi and Bluetooth when not in use

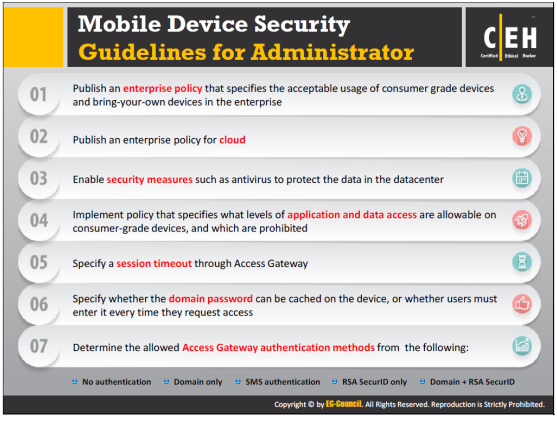






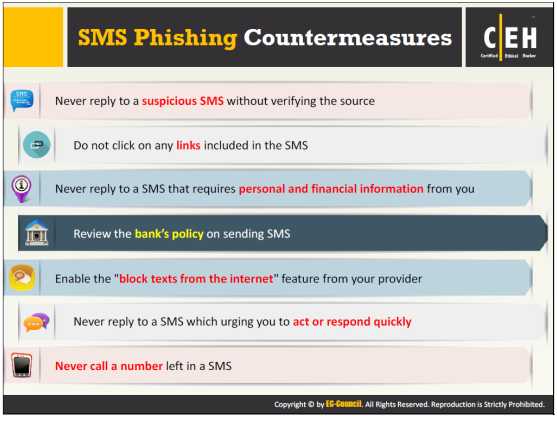






Below are some additional guidelines for an administrator to implement in order to maintain corporate mobile device security:

- Develop and maintain a mobile device security policy that states organizational resources to access via mobiles, types of mobiles allowed, access privileges, and others.
- Develop system threat models for mobile devices and the resources accessed using them, which enables an organization to design security solutions.
- Enable all the required security settings for mobile devices prior to issuing them to users.
- Regularly maintain mobile device security, including keeping OS and apps up to date, ensuring that mobile clocks are synched to a common time source, reconfiguring access privileges, identifying and documenting abnormalities within device infrastructures, and so on.
- Regularly monitor whether users properly follow policies and procedures framed for device security.
- Consider the best services provided by various service providers, determine the services that suit your environment, then design and attain one or more solutions to meet these and any other requirements.
- Test the solutions prior to placing them into production. Evaluate various aspects of solutions such as authentication, app functionality, security, connectivity, and performance.



Below is a list of countermeasures to defend against SMS phishing attacks:

- Do not fall for scams, gifts, and offers that seem to be unexpected.
- Attackers might send text messages through an Internet text relay service to conceal their identity; thus, it is best to avoid messages from non-telephonic numbers.
- Check for spelling mistakes, grammatical errors, or language inconsistency in text messages.

BullGuard Mobile Security is an app for Android devices that provides total protection for mobile devices and personal data.

Features:

- **Antivirus** – stops viruses, spyware, adware, trackware with live updates from the cloud.
- **Antitheft** – lock, locate and wipe device remotely if lost or stolen.
- **SIM protection** – automatically locks device if SIM is removed, includes optional data wipe.
- **Backup** – backup and restore your data.
- **Call Manager** – blocks the scourge of spam calls and SMS messages.
- **Parental controls** – keeps the kiddies safe with discreet monitoring and tracking.
- **Mobile Security Manager** – web-based platform to remotely manage and monitor your devices.

Source: http://www.bullguard.com

Lookout helps to protect your device from security threats, loss, and theft, available for Android and iPhone devices.

Features:

Security and Privacy

- **Advanced Security** – helps to stay safe from viruses, malware, and spyware when downloading apps or files.
- **Safe Dialing** – Scan all click-to-call links to stay safe from dialer-related threats that can wipe your data, photos or factory reset your phone.
- **Safe Browsing** – Surf the mobile web safely and ensure every site you visit and every link you click on from emails, texts, Facebook, and so on is safe.
- **Privacy Protected** – protects your privacy and knows which apps can access your private information.

Missing Device

- **Find My Phone** – maps the location of your phone from any device with an Internet browser and sound a loud alarm—even if the ringer is silent.
- **Lock It Down** – allows to remotely lock the phone to block access to personal data.
- **Wipe It Clean** – allows to remotely wipe the device to prevent illegal access to the personal info in it.

Backup

- Allows backing up contacts, photos, call history, and others
- Allows downloading or transferring back up data to a new device

Management

- Allows you to remotely manage your phone

Source: *https://www.lookout.com*

WiseID protects your data using any combination of:

- Password
- Face recognition
- Dot pattern

Features:

- Secure password management
- Works on multiple devices: iPhone®, iPad®, Android, Mac and Windows PCs, and Kindle
- Offers X.509 digital ID credentials for securing emails
- Protected sign on to websites
- Safe security: 256 bit AES, PBKDF2 encryption keys
- Syncs data between devices

Source: http://www.wiseid.com

Zimperium Mobile IPS (zIPS) is a mobile intrusion prevention system to defend your Android devices from advanced mobile threats. zIPS uses advanced machine-learning techniques to identify and prevent both network-based and host-based threats, such as:

- Man-in-the-Middle attacks that can intercept your passwords and other confidential information when you are using public or private WiFi networks
- SpearPhishing attacks that can compromise high-value targets in your organization and infect them with data-stealing code
- Reconnaissance scans to identify APTs and compromised devices in your network
- Rogue Wi-Fi AP attacks that can hijack secure SSL sessions to steal confidential information

It provides automated alerts to both the security officer and user in the event of an incident. It uses "**non-intrusive packet monitoring**" to detect advanced mobile threats.

Source: *https://www.zimperium.com*

Unlike the mobile devices of the past, today's mobiles come with advanced computing capability and connectivity (smartphones). One can use them to store data, browse the Internet, record videos, send SMS, play games, capture photos, and many other things. Therefore, it has become the major source for intruders to steal data.

Given below are few mobile protection tools one can use to secure their mobile devices:

McAfee Mobile Security

Source: *http://home.mcafee.com*

McAfee Mobile Security allows you to safely and confidently select new apps, shop online, browse social networks, or use the device for banking and payments.

Features:

- Keeps personal device safe
- Preserves privacy
- Finds and protects phone if lost or stolen
- Allows to surf and shop safely by avoiding dangerous websites and links

AVG AntiVirus Pro for Android

Source: http://www.avg.com

AVG AntiVirus Pro for Android not only keeps the phone and private data safe from viruses and malware, but also it assists in recovering a lost or stolen mobile devices and helps the smartphone to run at optimal performance.

Features:

- Finds and protects phone if lost or stolen
- Keeps personal device safe
- Enhance performance
- Preserve privacy
- Backup apps
- Call and text message blocker

avast! Mobile Security

Source: http://www.avast.com

avast! Mobile Security protects against privacy loss and identity theft. It backups personal data and track your phone or sound an alarm if it is lost or stolen. Other features include remote lock and wipe, lock specific apps, filter incoming calls and SMS, antivirus, SIM-Card-Change notification, Web shield, and firewall.

Norton Mobile Security

Source: http://us.norton.com

Norton Mobile Security protects Android smartphones and tablets, as well as iPhones and iPads.

Features:

Anti-Theft

- Sets off a "scream" alarm, so you can quickly find your missing mobile device
- Locks a lost or stolen phone or tablet to prevent strangers from using it
- Allows you erase the information on your missing mobile device, including any data on phone memory cards
- Pinpoints your lost or stolen phone or tablet on a map to find it

Privacy Protection

- Saves contacts from your Android, iPhone, or iPad so you can restore them if they are lost or deleted
- Blocks fraudulent (phishing) websites to protect your sensitive personal information when you use mobile networks

- Blocks annoying and unwanted calls and text messages

Anti-Malware

- Detects and removes mobile threats that hackers could use to steal your data and spam you via text messages
- Checks your apps and app updates for threats and removes them without slowing down device performance

ESET Mobile Security

Source: http://www.eset.com

ESET Mobile Security for Android protects smartphones and tablets against various threats.

Features:

- **Anti-Theft** – recovers lost or stolen device by enabling it to email you notifications, transmit its location, sound an alarm or even erase the contents remotely.
- **Apps Audit** – scans and organizes all installed apps to show permission levels and what information on the phone or tablet they can access.
- **Anti-virus** – Anti-virus technology scans all files, websites and emails. Anti-phishing shields identity and personal data against theft.

Kaspersky Internet Security for Android

Source: http://www.kaspersky.com

Kaspersky Internet Security for Android delivers Kaspersky Lab's latest mobile security technologies, including anti-theft and Android anti-virus protection. It has an advanced mechanism to protect both Android smartphones and Android tablets from Internet security threats with minimal impact on the performance of devices.

Features:

- **Anti-malware Protection** – includes Kaspersky's latest Android antivirus technologies.
- **Web Protection** – against Internet-based attacks and phishing websites.
- **Anti-Theft Protection** – with remote access to special security features on missing device.
- **Privacy Protection** – to control what others can see or access when they pick up your smartphone.
- **Call and Text Filter** – the smartphone receives only wanted calls and texts.

F-Secure Mobile Security

Source: http://www.f-secure.com

F-Secure Mobile Security protects tablet or smartphone, and the personal content on it, against various threats.

Features:

- Locate or erase a missing smartphone or tablet
- Protect children against mobile threats and unsafe apps
- Surf, bank and shop safely on smartphone and tablet
- Block unwanted callers
- Scan and clean smartphone or tablet of harmful applications
- Use banking protection for extra safety when online banking (Google Chrome, Safe Browser and Dolphin)

Trend Micro™ Mobile Security

Source: http://www.trendmicro.com

Trend Micro Mobile Security provides protection and privacy for digital life. It safeguards against lost devices and data, viruses, spyware, dangerous and fraudulent websites, fake apps and identity theft on Facebook. It extends battery life and optimizes device performance and memory.

Comodo Mobile Security

Source: http://www.comodo.com

COMODO Mobile Security (CMS protects Android devices against viruses, unsafe apps, potentially risky settings, and from theft. In addition, it helps to protect your privacy and keeps your system optimized.

Bitdefender Mobile Security

Source: http://www.bitdefender.com

Bitdefender Mobile Security protects the device from electronic threats and saves battery.

Features:

- **App Lock** – protects private information from being seen or stolen by hackers.
- **Privacy Advisor** – gives detailed info as to what your installed apps are doing in the background without your knowledge.
- **Malware Scanner** – ensures applications installed on the device or kept in the phone's storage are legitimate and safe.
- **Web Security** – uses the Bitdefender Cloud services to alert users, when browsing, about webpages that contain malware, phishing or fraudulent content.
- **Anti-Theft** – provides options to remotely locate, lock, wipe or send a message to the Android device.

Given below are few mobile anti-spyware softwares that are designed to detect and remove spyware, adware, and other malware (Trojans, rootkits, keyloggers, etc.) from mobile devices:

SeCore Security

Source: *http://www.securelab.com*

SeCore Security protects against advanced persistent threats.

Features:

- **Antivirus** – detects and removes viruses, trojans, malware, spyware, greyware.
- **Anti-Adware** – protects from aggressive and noisy ads apps.
- **Anti-Spyware** – discovers and removes suspicious spyware that can track your location and monitor you.
- **Burn after read** – deletes particular call log and SMS message immediately after you have read it.
- **Wipe after Lost** – remotely erases any number of latest photos, videos, SMS messages and call logs as you want whenever your phone disappears.
- **Anti-Sim-Cloning** – discovers and protects you from suspicious SIM cloning activities.

AntiSpy Mobile

Source: *http://www.antispymobile.com*

AntiSpy Mobile is a Android application that detects and removes spyware apps on your cell phone. An advanced persistent protection monitors all applications that are installed on your phone and notifies you if there are any new spywares or applications with suspicious spy-able permissions.

Features:

- Protects from mobile spywares
- Automatically perfroms scan in the background
- Advanced spyware detection
- Updates spyware definitions on regular basis
- Helps identify who is tapping your cell by install time and date

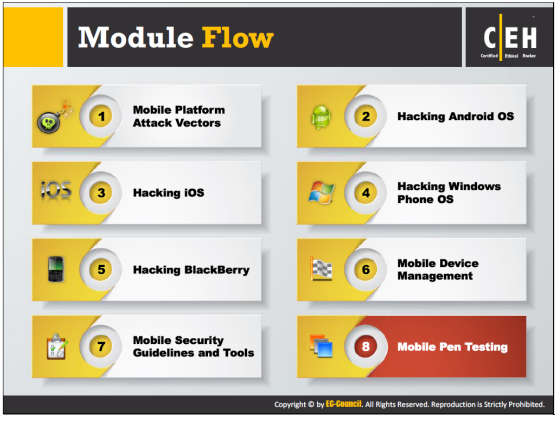
Malwarebytes Anti-Malware Mobile

Source: *https://www.malwarebytes.org*

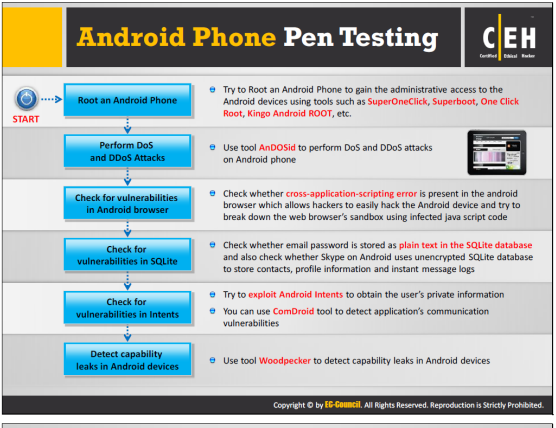
Malwarebytes Anti-Malware Mobile is an app for Android smartphone or tablet, which guards your identity and personal data defending against malware, infected applications, and unauthorized surveillance.

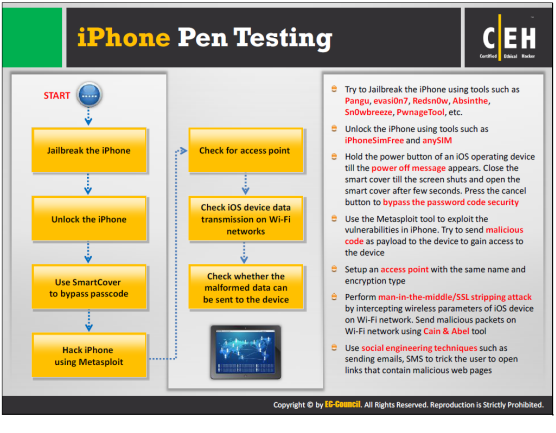
Features:

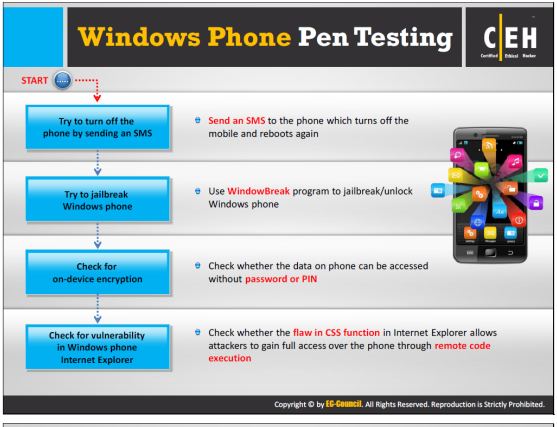
- Detects and eliminates malware, including spyware and Trojans
- Scans your apps for malicious code or Potentially Unwanted Programs (PUPs)
- Scans archived files and files stored on external SD card for complete coverage
- Stops unauthorized access to your personal data
- Scans your Android device for security vulnerabilities
- Identifies applications that are tracking your location

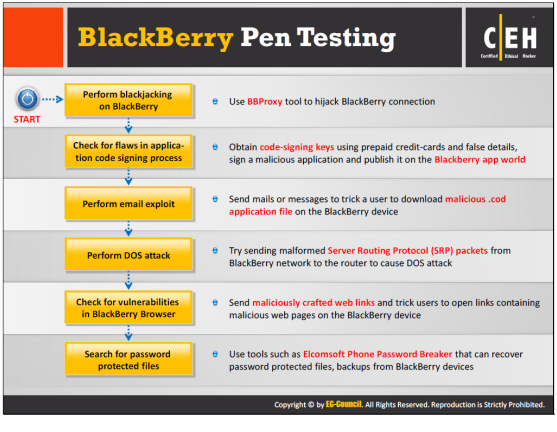


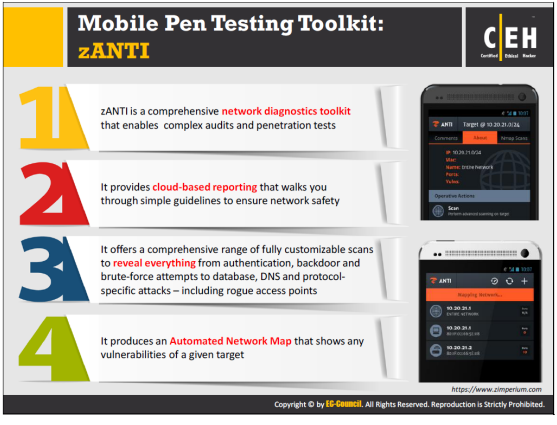
Usage of smartphones is enormously increasing day-to-day for personal and business purposes. Smartphones come with lot more tools and features that support a wide range of functionality. These tools and features not only increase functionality but also introduce new security issues, or increase existing risks. Attackers take advantage of this to launch various kinds of attacks to extract sensitive personal or business information stored on smartphones. Therefore, one should perform mobile security penetration testing to find existing security loopholes. This section deals with systematic process involved in the mobile pen testing.











zANTI is a comprehensive network diagnostics toolkit that enables complex audits and penetration tests. It provides cloud-based reporting that walks you through simple guidelines to ensure network safety.

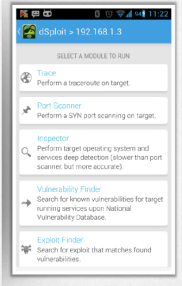
Features:

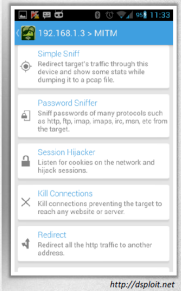
- It offers a host of penetration-testing features, including everything from Man-In-The-Middle and password complexity audits to port monitoring and a sophisticated packet sniffer.
- It employs cloud-based reporting to demonstrate flaws and rationalize budgeting for necessary network upgrades.
- It 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.
- It produces an Automated Network Map that shows any vulnerabilities of a given target.

Source: *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





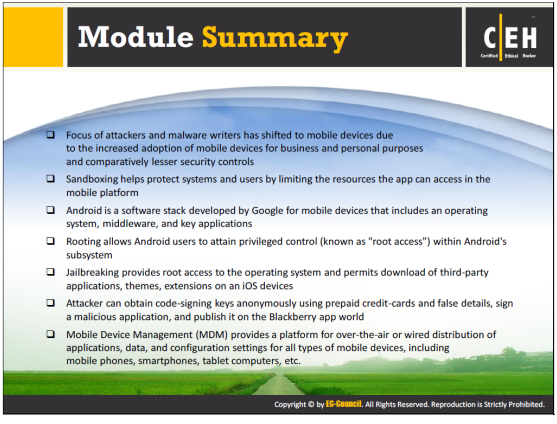
http://dsploit.net

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



This module discussed various mobile operating systems, the types of attacks typically launched on them, the tools used in doing so, and countermeasures for securing them. The next module discusses how attackers evade network security components such as IDS, firewalls, and honeypots, as well as countermeasures for preventing it.