

Module 17

Hacking Mobile Platforms

This page is intentionally left blank.

The screenshot shows a slide titled 'Module Objectives' under the 'Hacking Mobile Platforms' module. The slide lists the following objectives:

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

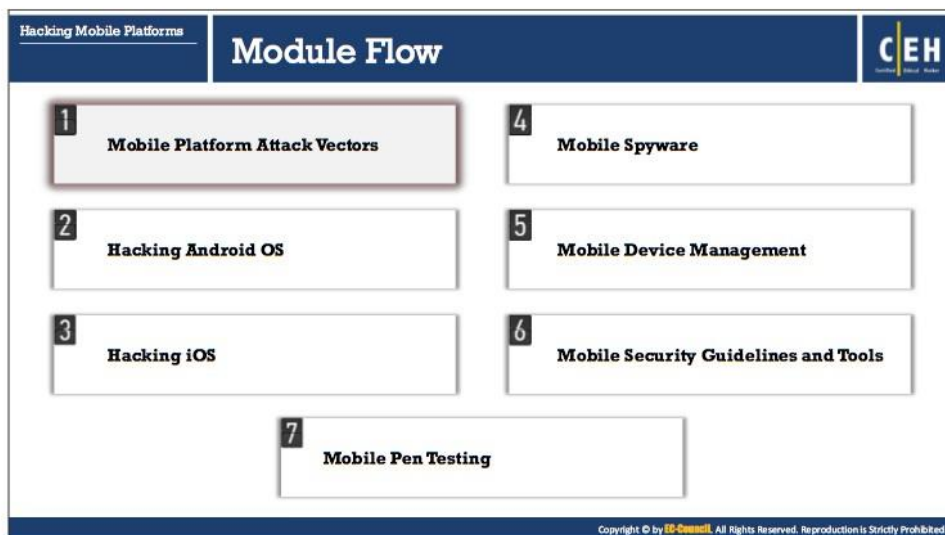
Module Objectives

With the advancement of mobile technology, mobility has become the key parameter for internet usage. People's lifestyle is becoming increasingly reliant on smartphones and tablets. 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. In addition, 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 for attackers. This module explains the potential threats to mobile platforms and provides guidelines for using mobile devices securely.

At the end of this module, you will be able to perform the following:

- Understand mobile platform attack vectors
- Understand various Android threats and attacks
- Understand various iOS threats and attacks
- Use various mobile spyware
- Describe Mobile Device Management (MDM)
- Apply various mobile security countermeasures
- Use various mobile security tools
- Perform mobile penetration testing



Mobile Platform Attack Vectors

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 vulnerable areas in mobile business environment, OWASP top 10 mobile risks, 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.

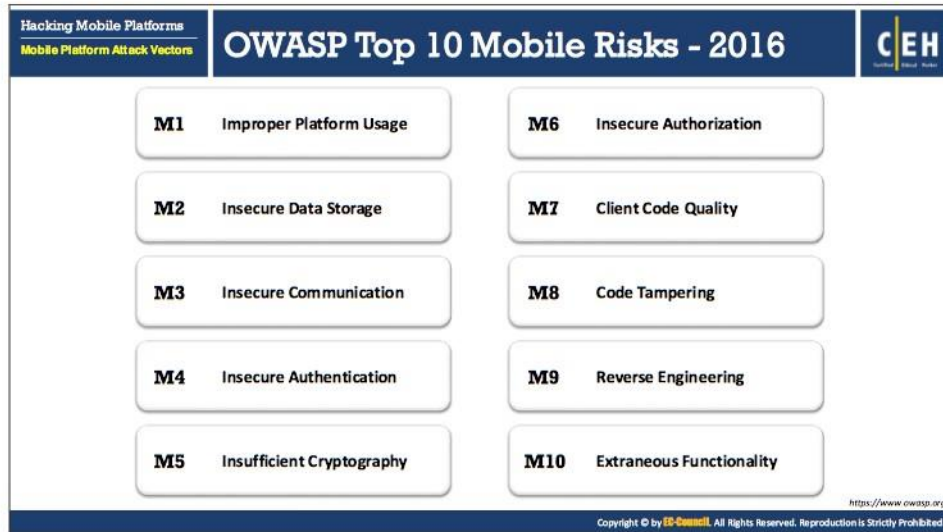


Vulnerable Areas in Mobile Business Environment

Source: <https://www-935.ibm.com>

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 increased because of Internet connectivity, use of business and other applications, different methods of communication available, and so on. Apart from the security threats that are specific to mobile devices, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers.

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



OWASP Top 10 Mobile Risks—2016

Source: <https://www.owasp.org>

According to OWASP, following are the top 10 mobile risks:

- **M1—Improper Platform Usage**

This category covers misuse of a platform feature or failure to use platform security controls. It includes Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile's OS. There are several ways that mobile apps can experience this risk.

- **M2—Insecure Data Storage**

This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.

Insecure data storage 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 application programming interfaces (APIs) and calling them appropriately.

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 normally caused due to vulnerabilities in 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.

▪ **M3—Insecure Communication**

This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, and so on. This flaw exposes an individual user's data and can lead to account theft. If the adversary intercepts an admin account, the entire site could be exposed. Poor Secure Socket Layer (SSL) setup can also facilitate phishing and man-in-the-middle (MITM) attacks.

▪ **M4—Insecure Authentication**

This category captures notions of authenticating the end user or bad session management such as the following:

- Failing to identify the user when that should be required.
- Failure to maintain the user's identity when it is required.
- Weaknesses in session management.

▪ **M5—Insufficient Cryptography**

The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. This category is for issues where cryptography was attempted, but it was not done correctly. This vulnerability will result in the unauthorized retrieval of sensitive information from the mobile device. In order to exploit this weakness, an adversary must successfully return encrypted code or sensitive data to its original unencrypted form due to the weak encryption algorithms or flaws within the process of encryption.

▪ **M6—Insecure Authorization**

This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, and forced browsing). It is distinct from authentication issues (e.g., device enrolment and user identification).

If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.

▪ **M7—Client Code Quality**

This is the "Security Decisions Via Untrusted Inputs," one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client, which is distinct from server-side coding mistakes. This would capture things such as buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that is running on the mobile device. Most exploitations that fall into this category result in foreign code execution or denial-of-service (DoS) on remote server endpoints (and not the mobile device itself).

- **M8—Code Tampering**

This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.

- **M9—Reverse Engineering**

This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Softwares such as IDA, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back-end servers, cryptographic constants and ciphers, and intellectual property.

- **M10—Extraneous Functionality**

Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of two-factor authentication during testing.

Typically, an attacker seeks to understand extraneous functionality within a mobile app in order to discover hidden functionality in the backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by the end users.



Anatomy of a Mobile Attack

Source: <https://www.nowsecure.com>

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

Following are the device-based attacks:

- **Browser-Based Attacks**

Following are the browser-based points of attack:

- **Phishing:** Phishing emails or pop-ups redirect users to fake web pages 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 web page integrated into another web page using iFrame elements of HTML. An attacker exploits iFrame functionality used in

target website, embeds his/her malicious web page, 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. Consequently, attackers obtain sensitive information or take control of the device.
 - **Man-in-the-Mobile:** Attacker implants malicious code into the victim's mobile device to bypass password verification systems that send one-time passwords (OTPs) via Short Message Service (SMS) or voice calls. Thereafter, the malware relays the gathered information to the attacker.
 - **Buffer Overflow:** 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 to interact 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**
- Following are the phone/SMS-based points of attack:
- **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 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 (SSNs), credit card numbers, and online banking username and password.
- **Application-based Attacks**
- Following are the application-based points of attack:
- **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 in 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 SSL validation process may allow attackers to circumvent the data security.
- **Configuration 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.

Other application-based points of attack include UI overlay/pin stealing, third-party code, intent hijacking, Zip directory traversal, clipboard data, URL schemes, GPS spoofing, weak/no local authentication, integrity/tempering/repackaging, side channel attack, App signing key unprotected, App transport security, XML specialization, and so on.

○ **The System**

Following are the OS-based points of attack:

- **No Passcode/Weak 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 OS and removes sandbox restrictions. Thus jailbreaking, such as 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.
- **OS Data Caching:** An OS cache stores used data/information in memory on temporary basis in the hard disk. An attacker can dump this memory by rebooting the victim's computer to a malicious OS and can extract sensitive data from the dumped memory.

- **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.
- **User-initiated Code:** User-initiated code is an activity that tricks the victim to install malicious applications or clicking links where an attacker can install malicious code to exploit a user's browser, cookies, and security permissions.

Other OS-based points of attack include no/weak encryption, confused deputy attack, TEE/secure enclave processor, side channel leak, multimedia/file format parsers, kernel driver vulnerabilities, resource DoS, GPS spoofing, device lockout, and so on.

- **The Network**

Following are the network-based points of attack:

- **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.
- **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.
- **SSLStrip:** SSLStrip is a type of MITM attack in which attackers exploit vulnerabilities in the SSL/TLS implementation on websites. 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.

- **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/CLOUD**

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

- **Web server-based attacks**

Following are the web server-based vulnerabilities and attacks:

- **Platform Vulnerabilities:** Attackers exploit vulnerabilities in the OS, 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):** 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):** 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'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, and so on 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 that allow any number of input attempts are generally prone to brute-force attack.

Other web server-based vulnerabilities and attacks include cross origin resource sharing, side channel attack, hypervisor attack, VPN, and so on.

○ **Database Attacks**

Following are the database-based vulnerabilities and attacks:

- **SQL injection:** SQL injection is a technique used to take advantage of nonvalidated 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.
- **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.
- **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.

Hacking Mobile Platforms
Mobile Platform Attack Vectors

How a Hacker can Profit from Mobile when Successfully Compromised

CEH
Certified Ethical Hacker

- Surveillance**
 - Audio
 - Camera
 - Call logs
 - Location
 - SMS messages
- Financial**
 - Sending premium rate SMS messages
 - Stealing Transaction Authentication Numbers (TANs)
 - Extortion via ransomware
 - Fake antivirus
 - Making expensive calls
- Data Theft**
 - Account details
 - Contacts
 - Call logs
 - Phone number
 - Stealing data via app vulnerabilities
 - Stealing International Mobile Equipment Identity Number (IMEI)
- Botnet Activity**
 - Launching DDOS attacks
 - Click fraud
 - Sending premium rate SMS messages
- Impersonation**
 - SMS redirection
 - Sending email messages
 - Posting to social media

1,598,196 Malicious installation packages

108,073 Mobile ransomware Trojans

19,748 Mobile banking Trojans

<https://www.sophos.com>

<https://securelist.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How a Hacker Can Profit from Mobile when Successfully Compromised?

Source: <https://www.sophos.com>, <https://securelist.com>

Nowadays, pictures, contact lists, banking apps, social media, email accounts, financial information, business information, and so on reside on our smartphone 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 most 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).

After successfully compromising, hackers can exploit the following:

Surveillance	Financial	Data Theft	Botnet Activity	Impersonation
Audio	Sending premium rate SMS messages	Account details	Launching DDoS attacks	SMS redirection
Camera	Fake antivirus	Contacts	Click fraud	Sending emails
Call logs	Making expensive calls	Call logs and phone number	Sending premium rate SMS messages	Posting to social media
Location	Extortion via ransomware	Stealing data via app vulnerabilities		
SMS messages	Stealing Transaction Authentication Numbers (TANs)	Stealing International Mobile Equipment Identity Number (IMEI)		

TABLE 17.1: List of information that hackers can exploit

The infographic is divided into two main sections: 'Mobile Attack Vectors' and 'Mobile Platform Vulnerabilities and Risks'. The 'Mobile Attack Vectors' section lists four categories: Malware (Virus and rootkit, Application modification, OS modification), Data Exfiltration (Extracted from data streams and email, Print screen and screen scraping, Copy to USB key and loss of backup), Data Tampering (Modification by another application, Undetected tamper attempts, Jail-broken device), and Data Loss (Application vulnerabilities, Unapproved physical access, Loss of device). The 'Mobile Platform Vulnerabilities and Risks' section lists 12 numbered items: 01 Malicious Apps in Stores, 02 Mobile Malware, 03 App Sandboxing Vulnerabilities, 04 Weak Device and App Encryption, 05 OS and App Updates Issues, 06 Jailbreaking and Rooting, 07 Mobile Application Vulnerabilities, 08 Privacy Issues (Geolocation), 09 Weak Data Security, 10 Excessive Permissions, 11 Weak Communication Security, and 12 Physical Attacks.

Mobile Attack Vectors and Mobile Platform Vulnerabilities

- **Mobile Attack Vectors**

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 below are some of the attack vectors that allow an attacker to exploit vulnerabilities present in mobile’s OS, device firmware, or mobile apps.

Malware	Data Exfiltration	Data Tampering	Data Loss
Virus and rootkit	Extracted from data streams and email	Modification by another application	Application vulnerabilities
Application modification	Print screen and screen scraping	Undetected tamper attempts	Unapproved physical access
OS modification	Copy to USB key and loss of backup	Jail-broken device	Loss of device

TABLE 17.2: List of attack vectors

- **Mobile Platform Vulnerabilities and Risks**

Increased usage of smartphones with ever-evolving technological features has made mobile device security a primary security concerns 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 toward research and implement possible attack schemes against mobile platforms to compromise users' security and privacy, or even gain complete control over the victim's devices.

Following are some of the mobile platform vulnerabilities and risks:

- Malicious apps in stores
- Mobile malware
- App sandboxing vulnerabilities
- Weak device and app encryption
- OS and app updates' issues
- Jailbreaking and rooting
- Mobile application vulnerabilities
- Privacy issues (Geolocation)
- Weak data security
- Excessive permissions
- Weak communication security
- Physical attacks

Hacking Mobile Platforms
Mobile Platform Attack Vectors

Security Issues Arising from App Stores

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

```
graph LR; Attacker[Attacker] --> App[Mobile App]; App --> NoVetting[No Vetting]; NoVetting --> TPA[Third-Party App Store]; Official[Official App Store] -.-> TPA; TPA --> User[Mobile User]; User --> App; App --> Attacker; subgraph DataFlow; App --> Attacker; end; DataFlowText[Malicious app sends sensitive data to attacker  
Call logs/photo/videos/sensitive docs];
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Issues Arising from App Stores

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, games, and many others. In general, apps are made available via application distribution platforms, which could be official app stores operated by the owner of mobile's 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. Attackers may use the information gathered to exploit the devices and launch many more attacks. Attackers can also perform social engineering which force the 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. Malicious apps can damage other applications and data and send your sensitive data to attackers.

Hacking Mobile Platforms
Mobile Platform Attack Vectors

App Sandboxing Issues

CEH

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

The diagram illustrates two scenarios of app sandboxing. On the left, a 'Secure Sandbox Environment' shows an app with 'Unrestricted Access' to 'System Resources' and 'User Data', but with 'No Access' to 'Other User Data' and 'Other System Resources'. On the right, a 'Vulnerable Sandbox Environment' shows the same app with 'Unrestricted Access' to 'System Resources' and 'User Data', but with 'Access' to 'Other User Data' and 'Other System Resources' through a 'Bypass the Sandbox' mechanism. The word 'SANDBOX' is written vertically in the center of each environment.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

App Sandboxing Issues

Smartphones are increasingly gaining the focus of cyber criminals. Mobile app developers must understand the threat to security and privacy to mobile devices by running a nonsandboxed 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, malwares 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; however, malicious applications may exploit vulnerabilities and bypass the sandbox.

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.

Hacking Mobile Platforms
Mobile Platform Attack Vectors

Mobile Spam

CEH

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

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

Significant amount of **bandwidth is wasted** by Spam messages

Spam attacks are done for **financial gain**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Spam

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, Multimedia Message Service (MMS), Instant Messaging (IM), and email IDs 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 to known/unknown phone numbers/email IDs that targets a mobile phone.

Following are the typical messages delivered via spam to mobile phones:

- Spam messages contain advertisements or malicious links that can trick users to reveal confidential information
- 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, and so on, which an attacker can use later 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.

Hacking Mobile Platforms
Mobile Platform Attack Vectors

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

CEH

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

Why SMS Phishing is Effective?

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

Text messaging is the most prevalent nonvoice communication on a mobile phone. Users send and receive some billions of text messages around the world within a day. With that amount of huge data, 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 systems to send bogus text messages. It is the act of trying to acquire personal and financial information by sending SMS (or IM) containing deceptive link. 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 SSNs, 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. Then, they send SMS bait to a user. The SMS may 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 the 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, SNNS, and 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.
- Easy to set up a mobile phishing campaign.
- Difficult to detect and stop before they cause harm.

Module 17 Page 1892

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Mobile users are not conditioned to receiving spam text messages on their mobile.
- No mainstream mechanism for weeding out spam SMS.
- Most of the mobile anti-virus does not check the SMS.

SMS Phishing Attack Examples

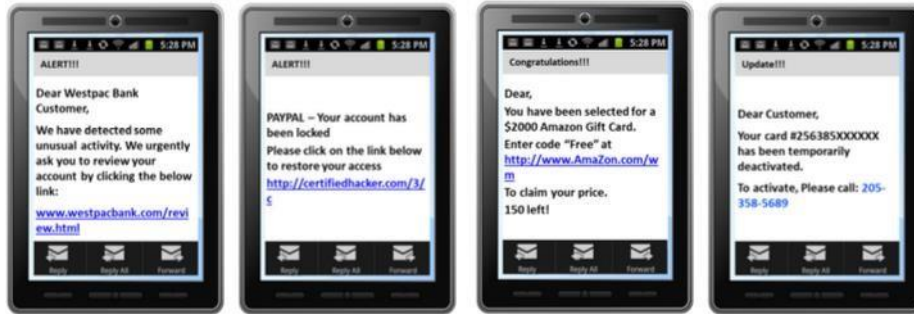



FIGURE 17.1: Examples of SMS Phishing


Hacking Mobile Platforms
Mobile Platform Attack Vectors

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections



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

Bluebugging Attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

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 a 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 or unencrypted Wi-Fi routers).

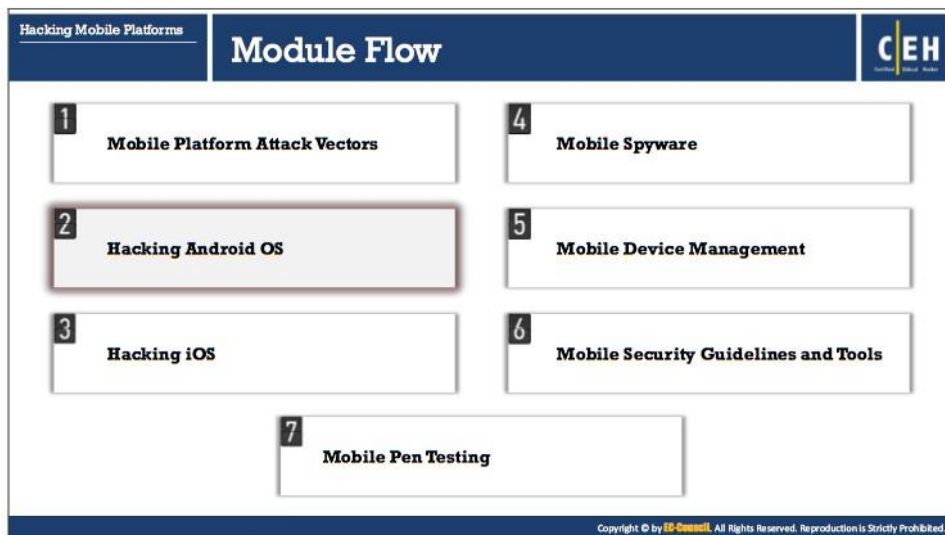
- **Bluesnarfing** (Stealing Information via Bluetooth)

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)

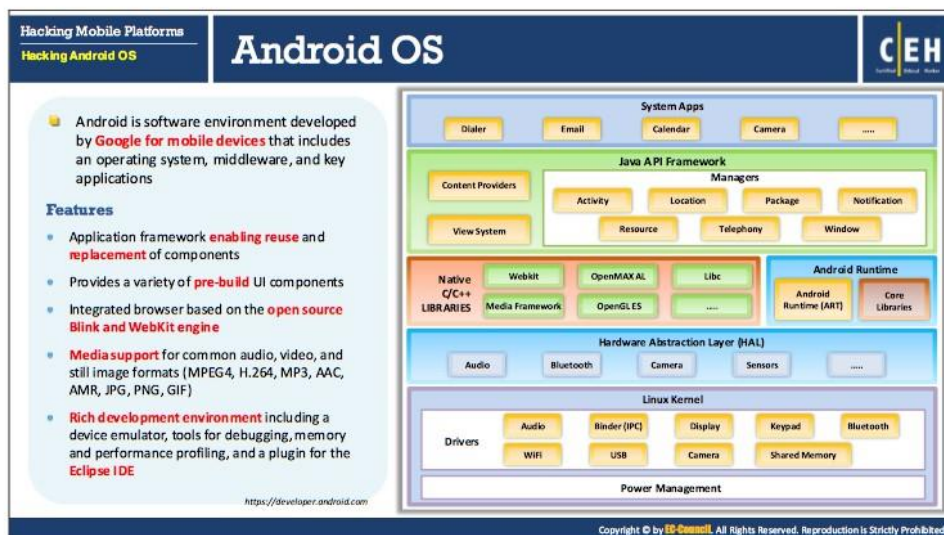
Bluebugging involves gaining remote access to a target Bluetooth-enabled device and use its features without a victim's knowledge or consent. Attackers compromise the target device's security to create a backdoor attack prior to returning control of it to its owner. Bluebugging allows attackers to sniff 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.



Hacking Android OS

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 OSs, 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 the victims' devices.

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.



Android OS

Source: <https://developer.android.com>

Android is software environment developed by Google for mobile devices that includes an OS, middleware, and key applications. The Android OS relies on the Linux kernel and is an open-source platform.

Features:

- Provides a variety of prebuilt 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, near-field communication (NFC), Wi-Fi P2P, USB, and session initiation protocol (SIP), in addition to standard network connections.

- Application framework enabling reuse and replacement of components.
- Android runtime (ART) optimized for mobile devices.
- Integrated browser based on the open-source Blink and WebKit engine.
- SQLite for structured data storage.
- Media support for common audio, video, and still image formats (e.g., MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, and GIF).
- Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE.

Android OS Architecture

Source: <https://developer.android.com>

Android is a Linux-based OS designed especially for portable devices such as smartphones and tablets. It is a stack of software components categorized into six sections (system applications, Java application framework, Native C/C++ libraries, Android runtime, Hardware Abstraction Layer (HAL), and Linux kernel) and five layers.

- **System Applications**

All Android system 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 dialer, email, calendar, camera, SMS messaging, web browsers, contact managers, and so on. Most Android apps are “written” in Java programming language.

- **Java API Framework**

Android platform functions are made available to developers through APIs written in Java programming language. The application framework offers many higher-level services to applications, which developers incorporate in their development.

Following are some of the application framework blocks:

- **Content Providers**—Manages data sharing between applications.
- **View System**—For developing lists, grids, text boxes, buttons, and so on.
- **Activity Manager**—Controls the activity life cycle of applications.
- **Location Manager**—Manages location, using GPS or cell towers.
- **Package Manager**—Keeps track of the applications installed on the device.
- **Notification Manager**—Helps applications display custom messages in a status bar.
- **Resource Manager**—Manages various types of resources used.
- **Telephony Manager**—Manages all voice calls.
- **Window Manager**—Manages application windows.

- **Native C/C++ 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.

Following are the native libraries:

- **WebKit and Blink**—web browser engine to display HTML content
- **Open Max AL**—it is a companion API to OpenGL ES but is used for multimedia (video and audio) rather than audio only
- **Libc**—Comprises System C libraries
- **Media Framework**—provides media codecs that allows recording and playback of different media formats
- **Open GL | ES**—is a 3D graphics library
- **Surface Manager**—meant for display management
- **SQLite**—a database engine used for data storage purposes
- **FreeType**—meant for rendering fonts
- **SGL**—is a 2D graphics library
- **SSL**—meant for Internet security

- **Android Runtime**

It includes core libraries and the ART virtual machine.

- **Android Runtime (ART)**

For the Android versions above 5.0, apps have its own runtime process and with its own instance. Android runtime has features such as ahead-of-time (AOT) compilation, just-in-time (JIT) compilation, and optimized garbage collection (GC).

- **Core Libraries**

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

- **Hardware Abstraction Layer**

Hardware abstraction layer is used to expose the device’s hardware capabilities to the Java API framework that is sitting at higher-level. It acts as an abstraction layer between the hardware and the software stack. HAL comprises of various modules that are required for the hardware equipments in the device such as audio, camera, Bluetooth, sensors, and so on.

- **Linux Kernel**

The Android OS relies on the Linux kernel. This layer comprises low-level device drivers such as audio driver, binder (IPC) driver, display driver, keypad driver, Bluetooth driver, camera driver, shared memory driver, USB driver, Wi-Fi driver, Flash memory driver, and

power management for its various hardware components. Functions of this layer include memory management, power management, security management, and networking.

Hacking Mobile Platforms
Hacking Android OS

Android Device Administration API

CEH

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

Policies Supported by the Device Administration API

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

Activate device administrator?

Sample Device Admin

https://developer.android.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Administration API

Source: <https://developer.android.com>

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

Following are some examples of the types of applications that might use the device administration API:

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

Below table lists 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 password to have a combination of letters and numbers and may include symbolic characters.
Complex password required	Requires that password 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 nonletter characters required in password	The minimum number of nonletter 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 <i>n</i> unique passwords. Typically, you can use this policy in conjunction with <code>setPasswordExpirationTimeout()</code> , 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 17.3: List of policies supported by the Android Device Administration API

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

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

Hacking Mobile Platforms
Hacking Android OS

Android Rooting

CEH

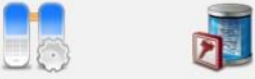
- Rooting allows Android users to **attain privileged control** (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the **device firmware**, and copying the su binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the **chmod command**

Rooting enables all the user-installed applications to **run privileged commands** such as:

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

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

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting

The goal behind rooting Android 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. Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. Rooting process involves exploiting security vulnerabilities in the device's firmware, and copying the su binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the chmod command.

Rooting enables all the user-installed applications to run privileged commands such as

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

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

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

One can use tools such as KingoROOT, TunesGo Root Android Tool, and so on to root Android devices.

Rooting Android Using KingoRoot

Android Rooting With PC

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

Android Rooting Without PC

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Rooting Android Using KingoRoot

Source: <https://www.kingoapp.com>

KingoRoot is the tool used to root android devices. This tool can be used with or without PC. KingoRoot helps users root their Android devices to the following:

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

Following are the steps involved in rooting android device with this tool:

Android Rooting with PC:

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

Android Rooting Without PC:

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

The screenshot shows a website titled "Android Rooting Tools" with a navigation bar for "Hacking Mobile Platforms" and "Hacking Android OS". The main content area features two large tool descriptions: "TunesGo" and "One Click Root". To the right, there is a vertical list of other tools: "Unrevoked", "MTK Droid", "Superboot", "Superuser X [Root]", and "Root Uninstaller". Each tool entry includes a small icon and a URL. At the bottom of the screenshot, there is a copyright notice for "ED-Council".

Android Rooting Tools

- **TunesGo Root Android Tool**

Source: <https://tunesgo.wondershare.com>

TunesGo—This tool has an advanced android root module that recognizes and analyzes your Android device and chooses the appropriate Android-root-plan for it automatically.

Following are the steps to root android device using TunesGo Root Android tool:

- Download **TunesGo Root Android tool**
- Connect your device to your computer
- Find “**One-click Android Root**” in Toolbox and click it to root your device
- Android device is successfully rooted!

- **One Click Root**

Source: <https://www.oneclickroot.com>

One Click Root is Android rooting software that supports the most devices and comes with extra fail-safes (like instant unrooting) feature and offers full technical support. It 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.

Following are some of the additional android rooting tools:

- Unrevoked (<http://www.unrevoked.com>)
- MTK Droid (<https://androidmtk.com>)
- Superboot (<http://www.galaxynexusforum.com>)
- Superuser X [Root] (<http://www.ksharkapps.com>)
- Root Uninstaller (<https://play.google.com>)
- Root Browser File Manager (<http://jrummyapps.com>)
- Titanium Backup Root (<http://www.matrixrewriter.com>)

Blocking Wi-Fi Access using NetCut

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

Steps to Block Wi-Fi Access

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

Note: This tool works only on rooted devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Blocking Wi-Fi Access using NetCut

Source: <http://www.arcai.com>

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

Note: This application works effectively only on rooted devices.

Follow the steps given below to block Wi-Fi access:

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

The screenshot displays the zANTI application interface. On the left, a text box lists the following attacks: Spoof MAC Address, Create malicious Wi-Fi hotspot, Scan for open ports, Exploit router vulnerabilities, Password complexity audits, Man-in-Middle attack, and DoS Attack. Below the list is the Android robot icon. The main area shows three panels of the app's settings. The top panel, 'Replace Images', has a toggle for 'Replace Images' set to 'ON' and a 'Select Image' button. The middle panel, 'Tether Control', has a toggle for 'Tether Control' set to 'OFF'. The bottom panel shows various other settings like 'Logged Requests', 'Logged Images', 'Packet Editor', 'SSL Strip', 'Redirect HTTP', 'Replace Images', 'Capture Download', and 'Intercept Download', with their respective toggles.

Hacking with zANTI

Source: <https://www.zimperium.com>

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

- Spoof MAC Address
- Create malicious Wi-Fi hotspot to capture victims in order to control and hijack victims device traffic
- Scan for open ports
- Exploit router vulnerabilities
- Password complexity audits
- MITM and DoS attack
- View, modify, and redirect all HTTP requests and responses
- Redirect HTTPS to HTTP, redirect HTTP request to particular IP or web page
- Insert html code into the web pages
- Hijack sessions
- View and replace all images that are transmitted over network
- Capture and intercept downloads

Hacking Mobile Platforms
Hacking Android OS

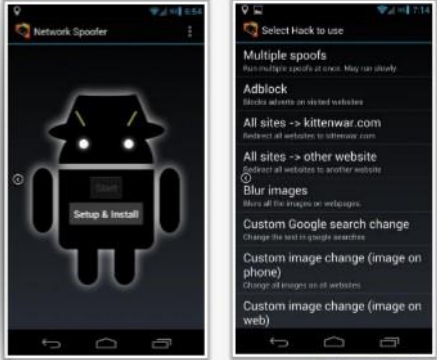
Hacking Networks Using Network Spoofer

CEH

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

Features:

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



<https://www.digitalsquid.co.uk>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Networks Using Network Spoofer

Source: <https://www.digitalsquid.co.uk>


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

Features

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

Hacking Mobile Platforms
Hacking Android OS


Launching DoS Attack using Low Orbit Ion Cannon (LOIC)



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

Steps to Launch DoS Attack

- Step 1:** Download and install LOIC android application from Android Play Store
- Step 2:** Launch the LOIC application
- Step 3:** Enter the target IP address or the URL in **GET Target IP** field and click **GET IP** button
- Step 4:** Select the DoS attack method by selecting any of **UDP, HTTP, TCP** radio buttons under **Send Method** option
- Step 5:** Enter the port and number of threads. Numbers must be a positive whole number
- Step 6:** Click on **START** button at the bottom of the interface to launch the DoS attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch DoS attack using Low Orbit Ion Cannon (LOIC)

Source: <https://play.google.com>

LOIC is a mobile application that allows the attackers to perform DoS/DDoS attacks on the target IP address. This application can perform UDP, HTTP, or TCP flood attacks.

Features:

- Full control over traffic flow
- Send data packet to any IP address
- Various methods to send data packets (HTTP, UDP, or TCP)
- Retrieve IP address from any real web-address
- Send data packets to any port

Follow the steps given below to launch DoS attack:

- **Step 1:** Download and install LOIC android application from Android Play Store.
- **Step 2:** Launch the LOIC application.
- **Step 3:** Enter the target IP address or the URL in **GET Target IP** field.
- **Step 4:** Select the DoS attack method by selecting any of **UDP, HTTP, or TCP** radio buttons under **Send Method** option.
- **Step 5:** Enter the port and number of threads. Numbers must be a positive whole number
- **Step 6:** Click on **START** button at the bottom of the interface to launch the DoS attack.

Hacking Mobile Platforms
Hacking Android OS

Performing Session Hijacking Using DroidSheep

CEH

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

The diagram illustrates the session hijacking process. A User is connected to an Access Point/Switch, which is connected to the Internet. An Attacker is also connected to the Access Point/Switch. The Attacker intercepts the User's request for a web page (ARP Spoofing). The Attacker then modifies the session IDs and relays them to the web server. The User is unaware of the interception.

The screenshot shows the DroidSheep interface on an Android device. It displays the following information:

- Connected to SAMSUNG
- Spoofing IP: 192.168.4.1
- Running and Spoofing mode
- Buttons for ARP-Spoofing and Generic mode
- Buttons for RUNNING AND SPOOFING and Stop
- URLs and session IDs being captured:

URL	IP	Session ID
http://www.tldev.com	192.168.4.11	539000154
http://www.4shared.com	192.168.4.11	1849008921
http://counter.yadro.ru	192.168.4.11	116591582
http://pixel.quantserve.com	192.168.4.11	1193088721
http://www.adshost1.com	192.168.4.11	872682735
http://l.simplifi	192.168.4.11	2000327422
http://dwww.objectify.ca.d.chango...	192.168.4.11	1165334141

http://droidsheep.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Performing Session Hijacking Using DroidSheep

Source: <http://droidsheep.org>

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

Hacking Mobile Platforms
Hacking Android OS

Hacking with Orbot Proxy

CEH

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



https://guardianproject.info
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking with Orbot Proxy

Source: <https://guardianproject.info>

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

Hacking Mobile Platforms
Hacking Android OS

Android-based Sniffers

FaceNiff

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

Packet Sniffer
<https://play.google.com>

tPacketCapture
<http://www.taosoftware.co.jp>

Android PCAP
<https://www.kismetwireless.net>

Wicap. Sniffer Demo [ROOT]
<https://play.google.com>

Testeldroid
<https://play.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android-based Sniffers

- **FaceNiff**

Source: <http://faceniff.ponury.net>

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

Following are some of the additional android-based sniffers:

- Packet Sniffer (<https://play.google.com>)
- tPacketCapture (<http://www.taosoftware.co.jp>)
- Android PCAP (<https://www.kismetwireless.net>)
- Wicap. Sniffer Demo [ROOT] (<https://play.google.com>)
- Testeldroid (<https://play.google.com>)
- Postern (<https://github.com>)
- WiFinspect [Root] (<https://play.google.com>)
- SniffDroid (<https://play.google.com>)

Hacking Mobile Platforms
Hacking Android OS

Android Trojans

BankBot (Android/Spy.Banker.LA)

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms
Hacking Android OS

Android Trojans (Cont'd)

SpyDealer

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

```

String pkgName = this.m_service.m_cont.getPackageName();
String cmd = "settings put secure enabled_accessibility_services " + (String.valueOf(pkgName) + "/"
+ pkgName + ".MobileService") + "&" + "ls" + "settings put secure accessibility_enabled 1";
while(!this.isRooting_SSP_INF == "18") {
if(!this.isAccessibilitySettingsOn(this.m_service.m_cont) && ((this.CheckAccessibility(this
.m_service.m_wf()) || (this.CheckAccessibility(this.m_service.m_3g)) && (this
.m_service.CheckSo())) {
this.m_service.RootCmd(cmd);
}
}
                
```

- Android/Trojan.AsiaHitGroup
- Ghost Ctrl malware
- Triada
- AndroRAT
- ZkMo (Zeus-in-the-Mobile)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Trojans

- **BankBot (Android/Spy.Banker.LA)**

BankBot is a banking Trojan that has been evolving and affecting large number of targets. It is available both off the Google play store and on the play store as well. It comprises sophisticated techniques in code obfuscation, payload dropping, and infection mechanism affecting android accessibility service.

BankBot spreads by Jewels Star Classic android game application from Google play store developed by the developer GameDevTony. When a victim downloads and installs the game, the payload sets off in 20 minutes from the first execution of the app. Then an alert prompt will be generated asking the user to enable the service "Google Service" which is a malicious one.

On enabling this service from Android accessibility page, the user will be redirected to a credit card details entry page where the details of the credit card are to be entered. If the user falls in this trap, then all the credit card details will be transmitted to the attacker causing a serious damage.

- **SpyDealer**

SpyDealer is a spying Trojan that ex-filtrates the private and sensitive data from 40 Android applications including WeChat, Facebook, WhatsApp, Skype, Line, Viber, QQ, Tango, Telegram, Sina Weibo, Tencent Weibo, Android Native Browser, Firefox Browser, Oupeng Brower, QQ Mail, NetEase Mail, Taobao, and Baidu Net Disk, and so on. It employs exploits from a commercial rooting app "Baidu Easy Root" to gain root privilege; abuses the Android Accessibility Service feature; extracts information such as phone number, IMEI, IMSI, SMS, MMS, contacts, accounts, phone call history, location, and connected Wi-Fi information; and so on; performs remote control of the device via UDP, TCP, and SMS channels; and records phone calls and the surrounding audio and video information.

Following are some of the additional Android Trojans:

- Android/Trojan.AsiaHitGroup
- GhostCtrl malware
- Triada
- AndroRAT
- ZitMo (Zeus-in-the-Mobile)
- FakeToken
- TRAMP.A
- Fakedefender
- Obad
- FakeInst
- OpFake
- Dendroid

The infographic is titled "Securing Android Devices" and is part of the "Hacking Mobile Platforms" series. It features a grid of 8 tips, each with an icon and a status indicator (green checkmark for good, red X for bad). The tips are: 1. Enable screen locks (good). 2. Do not directly download Android package files (APK) (bad). 3. Never root your Android device (bad). 4. Update the operating system regularly (good). 5. Download apps only from official Android market (good). 6. Use free protector Android app like Android Protector (good). 7. Keep your device updated with Google Android antivirus software (good). 8. Customize your locked home screen with the user's information (good). The infographic also includes a copyright notice for EC-Council at the bottom.

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

Securing Android Devices

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

- Enable screen locks for your Android phone for it to be more secure
- Never root your Android device
- Download apps only from official Android market
- Keep your device updated with Google Android antivirus software
- Do not directly download Android package files (APK)
- Update the OS regularly
- Use free protector Android app such as Android Protector where you can assign passwords to text messages, mail accounts, and so on
- Customize your locked home screen with the user information
- 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 do not inadvertently connect to a wireless network when you do not wish to connect

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

Hacking Mobile Platforms
Hacking Android OS

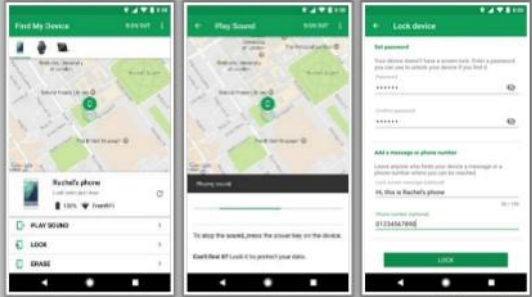
Android Security Tool: Find My Device

CEH

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

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

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



<https://www.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Security Tools: Find My Device

Source: <https://www.google.com>

Find My Device helps you to easily locate your lost Android device and keeps your information safe and sound while you look. It allows you to 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 find, lock, or erase a lost Android device.

One can select this service 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.

To use Find My Device, your lost device must

- Be turned on
- Be signed in to a Google Account
- Be connected to mobile data or Wi-Fi
- Be visible on Google Play
- Have Location turned on
- Have Find My Device turned on

To find, lock, or erase a lost or stolen device follow the steps given below:

- Go to <https://www.google.com/android/find> and sign in to your **Google Account**.
- If you have more than one device, click the lost device at the top of the screen.

- The device gets a notification.
- On the map, see about where the device is.
 - The location is approximate and might not be accurate.
 - If your device cannot be found, then you will see its last known location, if available.
- Pick what you want to do. If needed, first click **Enable lock & erase**.
 - **Play sound:** Rings your device at full volume for 5 minutes, even if it is set to silent or vibrate.
 - **Lock:** Locks your device with your PIN, pattern, or password. If you do not have a lock, you can set one. To help someone return your device to you, you can add a message or phone number to the lock screen.
 - **Erase:** Permanently deletes all data on your device (but might not delete SD cards). After you erase, Find My Device will not work on the device.

The screenshot shows a webpage titled "Android Security Tools" with a dark blue header. On the left, there's a section for "Kaspersky Mobile Antivirus: AppLock & Web Security" with a list of features. In the center is a large image of the Kaspersky app interface on a smartphone. On the right, there are five boxes, each representing a different security app with its logo and website URL: Avira Antivirus Security, Avast Antivirus & Security, McAfee Mobile Security & Lock, Lookout Security & Antivirus, and Sophos Mobile Security. A copyright notice for EC-Council is at the bottom of the page.

Android Security Tools

- **Kaspersky Mobile Antivirus**

Source: <https://my.kaspersky.com>

Kaspersky mobile antivirus 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 case if it is lost or stolen. It also protects the device against virus or malware attacks.

Features:

- **Antivirus protection**—Acts as a virus cleaner and automatically blocks malware from phones and tablets.
- **Background check**—Scans for viruses, spyware, and Trojans.
- **App Lock**—Lets you add a secret code to access your private messages, photos, and more.
- **Find my phone**—Tracks and finds your Android phone or tablet if it is lost or stolen.
- **Anti-Theft**—Protects vulnerable personal information from prying eyes.
- **Anti-Phishing**—Keeps your financial information secure while shopping and banking online.
- **Call blocker**—Blacklists unwanted phone calls and text/spam messages.
- **Web filter**—Filters out dangerous links and sites while surfing the Web.
- **Android 8 Support**—So that you can get the most from the new OS being protected.

- **Antivirus Database Expansion**—To improve protection against sophisticated threats.

Following are some of the additional android security tools:

- Avira Antivirus Security (<https://www.avira.com>)
- Avast Antivirus & Security (<https://www.avast.com>)
- McAfee Mobile Security & Lock (<https://www.mcafeemobilesecurity.com>)
- Lookout Security & Antivirus (<https://www.mylookout.com>)
- Sophos Mobile Security (<https://www.sophos.com>)
- Malwarebytes for Android (<https://www.malwarebytes.com>)
- AVG AntiVirus FREE for Android Security 2017 (<https://www.avg.com>)
- TrustGo Mobile Security (<https://www.trustgo.com>)
- 360 Security -Free Antivirus,Booster,Space Cleaner (<http://www.360safe.com>)
- Trend Micro Mobile Security & Antivirus (<https://www.trendmicro.co.in>)
- DroidSheep Guard (<http://droidsheep.org>)
- Bull Guard Mobile Security (<https://www.bullguard.com>)
- AVL Pro (<http://www.antiy.net>)

Android Vulnerability Scanner

- **X-Ray**

Source: <https://labs.duo.com>

X-Ray allows you to scan your Android device for security vulnerabilities that put your device at risk. It scans to determine whether there are vulnerabilities that remain unpatched by your carrier. It presents you with a list of vulnerabilities that it is able to identify and allows you to check for the presence of each vulnerability on your device. X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered and disclosed.

Following are some of the additional android vulnerability scanners:

- Threat Scan (<http://free.kaspersky.com>)
- Norton Halt exploit defender (<https://community.norton.com>)
- Shellshock Scanner – Zimperium (<https://www.zimperium.com>)
- Hackode (<http://www.ravikumarpurebey.com>)
- BlueBorne Vulnerability Scanner by Armis (<https://www.armis.com>)
- EternalBlue Vulnerability Scanner (<https://ebvscanner.firebaseio.com>)



Android Device Tracking Tools

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

- **Where's My Droid**

Source: <http://wheresmydroid.com>

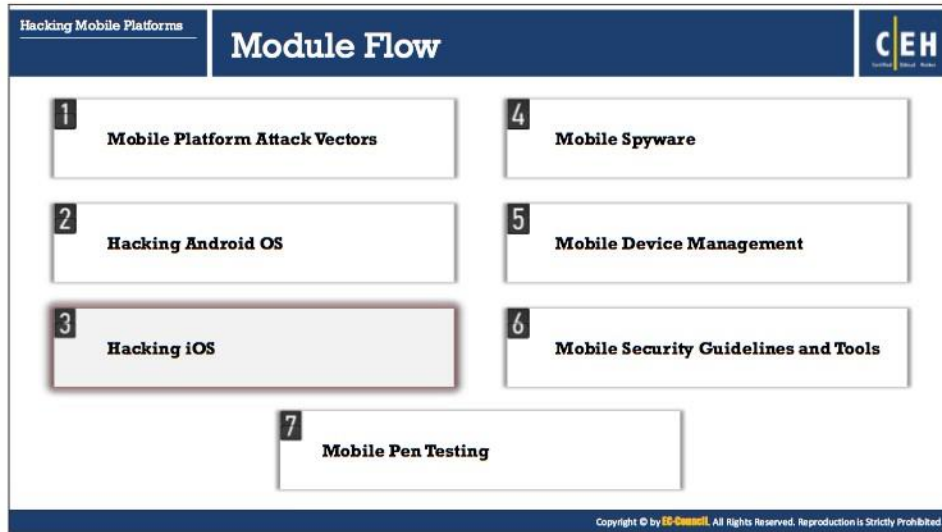
Where's My Droid is an Android device tracking tool that allows you to track your phone from anywhere, either with a text messaged attention word or through the online control center known as Commander.

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

Following are some of the additional android device tracking tools:

- Prey Anti-Theft: Find My Android and Mobile Security (<https://preyproject.com>)
- iHound (<http://ihoundgps.com>)
- Mobile Tracker for Android (<https://play.google.com>)
- Tech Expert (<https://protection.sprint.com>)
- GadgetTrak Mobile Security (<http://www.gadgettrak.com>)
- My Device (<https://play.google.com>)
- Lost Android (<http://www.androidlost.com>)



Hacking iOS

iOS is a mobile OS 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, 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, MITM attacks, etc. Attackers hack the iOS to gain root-level access to these devices.

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

The screenshot shows a presentation slide titled "Apple iOS" with a dark blue header. On the left, it says "Hacking Mobile Platforms" and "Hacking iOS". On the right, there is a logo for "CEH". The main content area has a white background with a list of bullet points and a diagram of the iOS architecture. The diagram consists of five horizontal bars representing layers: Applications (orange), Cocoa Touch (green), Media (blue), Core Services (red), and Core OS (purple). Within the Cocoa Touch layer, there is a box for "UIKit". Within the Core Services layer, there is a box for "Foundation". A red label "Core Framework" points to the UIKit and Foundation boxes. To the right of the diagram is an image of an iPhone displaying the iOS logo. At the bottom right of the slide, there is a small copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

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

Apple iOS

iOS is Apple's mobile OS, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV. 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 UI is based on the concept of direct manipulation, using multi-touch gestures. The iOS architecture comprises four layers (Cocoa Touch, Media, Core Services, and Core OS) under the application layer. 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 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.

Hacking Mobile Platforms
Hacking iOS

Jailbreaking iOS

CEH

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

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

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

Types of Jailbreaking

- Userland Exploit**
A userland jailbreak **allows user-level access** but does not allow iBoot-level access
- iBoot Exploit**
An iBoot jailbreak allows **user-level access** and **iBoot-level access**
- Bootrom Exploit**
A bootrom jailbreak allows **user-level access** and **iBoot-level access**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS

Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor. It 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 OS 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 Cydia, Pangu8 Anzhuang, Yalu, TaiG, Velonzy, Keen Jailbreak, and so on to jailbreak iOS devices.

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

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

Types of Jailbreaking

Discussed below are the three types of Jailbreaking:

- **Userland Exploit**

Userland Exploit uses a loophole in the system application. It allows user-level access but does not allow iBoot-level access. 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. An iBoot jailbreak allows user-level access and iBoot-level access. 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**


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. A bootrom jailbreak allows user-level access and iBoot-level access. Only a hardware update of bootrom by Apple can patch this exploit.

Hacking Mobile Platforms
Hacking iOS

Jailbreaking Techniques

CEH


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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 jailbreak 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 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.

Hacking Mobile Platforms
Hacking iOS


Jailbreaking iOS 11.2.1 Using Cydia

CEH

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

Steps to Jailbreak iOS 11.2.1 using Cydia

- 01 On your iPhone or iPad, open the **Safari browser**
- 02 From the address bar, go to **cydiaios7.com**
- 03 Locate the **UP arrow** on the web page, top right on the iPad and bottom center on the iPhone screen, and tap on it
- 04 When the new page loads, tap **Add to Home Screen**
- 05 Now type **Cydia** into the box for naming the app icon. Tap the **Add** button and close Safari browser
- 06 Look on your home screen for the **Cydia** icon



<https://www.cydiaios7.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS 11.2.1 Using Cydia

Source: <https://www.cydiaios7.com>

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.

Following are the steps to jailbreak iOS 11.2.1 using cydia:

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



FIGURE 17.2: Launch Safari App

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



FIGURE 17.3: Enter URL

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



FIGURE 17.4: Locate Up Arrow

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



FIGURE 17.5: Add to Home screen

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



FIGURE 17.6: Name the App

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



FIGURE 17.7: Cydia icon on homescreen

Hacking Mobile Platforms

Hacking iOS

Jailbreaking of iOS 11.2.1 Using Pangu Anzhuang

CEH
Certified Ethical Hacker

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

Steps to Install Pangu Anzhuang

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

<http://pangu8.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms

Hacking iOS

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

CEH
Certified Ethical Hacker

Steps to Install Cydia Jailbreak Apps

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS 11.2.1 Using Pangu Anzhuang

Source: <http://pangu8.com>

Pangu Anzhuang is a simple application that allows you to install jailbreak apps for iOS 11.2.1 - iOS 10.2 versions. It is a No PC required jailbreak method. It is an online jailbreaking app installer for latest iOS versions. Anzhuang helps you to install jailbreak apps using the dev code extraction method. The specialty of Pangu Anzhuang is that it perfectly works with all 64-bit and 32-bit devices.

It allows you to install Cydia and popular Jailbreak apps to your latest iOS versions from developer code extraction method. You must install third-party app manager such as zJailbreak to install Pangu Anzhuang.

Anzhuang Compatible devices:

- **iPhone:** iPhone X, iPhone 8, iPhone 8 Plus, iPhone 7 & 7 Plus, iPhone 6S & 6S Plus, iPhone 6 & 6 Plus/iPhone SE / iPhone 5s, iPhone 4s, iPhone 5, and iPhone 5c
- **iPad:** iPad Mini 2 / iPad Mini 3 / iPad Mini 4/iPad Air /iPad Air 2 /iPad Pro, iPad mini, iPad 2, iPad 3rd gen, and iPad 4th gen
- **iPod:** iPod Touch 6G and iPod Touch 5G

Steps to Install Pangu Anzhuang

- **Step 1**—Download zJailbreak app
- **Step 2**—Open the zJailbreak app. Go to **Pangu8 Anzhuang** app available under jailbreak clicking on it
- **Step 3**—Click on **“Install”** and then click **“Allow”** to popup message
- **Step 4**—Again click on **“Install”** from the popup screen and enter your regular **passcode**

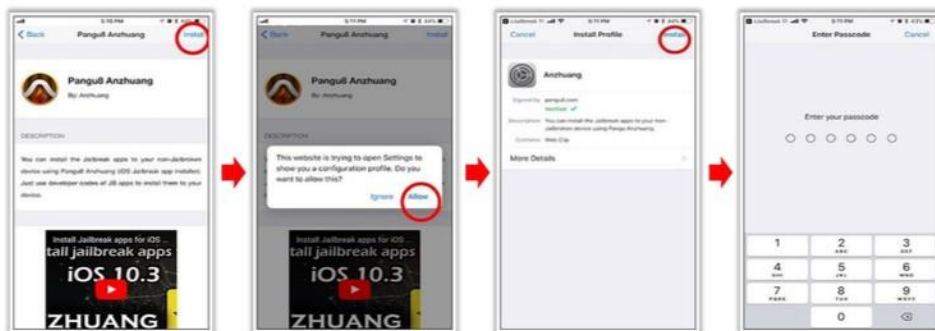


FIGURE 17.8: Pangu8 Anzhuang installation

- **Step 5**—Now Tap on **“Install”** → **“Done”**. It will begin to install Anzhuang app to your device
- **Step 6**—Once you complete the installation process, Anzhuang icon will be appeared on your home screen

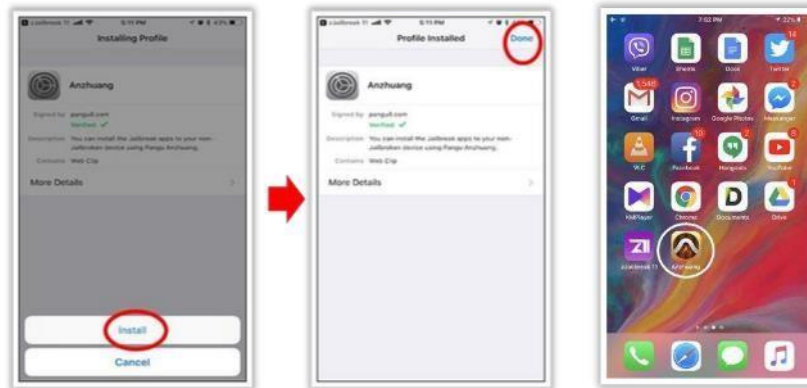


FIGURE 17.9: Pangu8 Anzhuang icon on home screen

Steps to Install Cydia Jailbreak Apps

- **Step 01**—Open the **Pangu8 Anzhuang** app. Tap on **“Browse the Jailbreak App list”** to copy the app code
- **Step 02**—Click on the **“App managers”** Then you need to click on **“Generate Code”** in Cydia lite icon
- **Step 03**—Go back to Anzhuang App and Paste the Code and Tap on **“Install”**

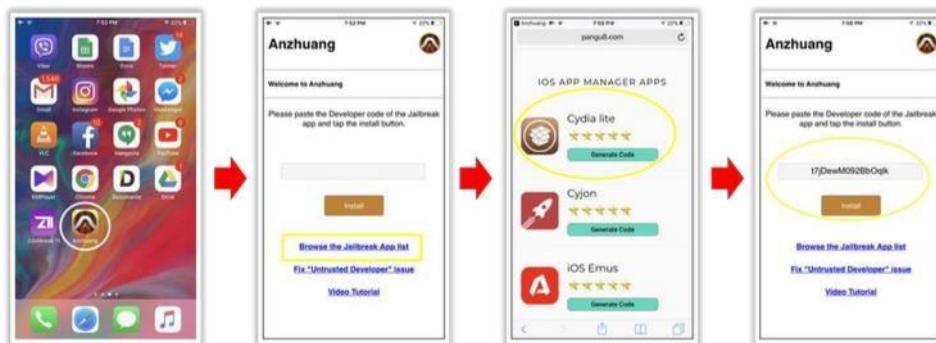


FIGURE 17.10: Cydia Jailbreak application installation

- **Step 04**—Click **“Allow”** to popup message and tap on **“Install”**
- **Step 05**—It will ask your **passcode**. Enter it and then tap on **“Install”** → **“Done”**
- **Step 06**—Finally you can see the Cydia app icon on your home screen

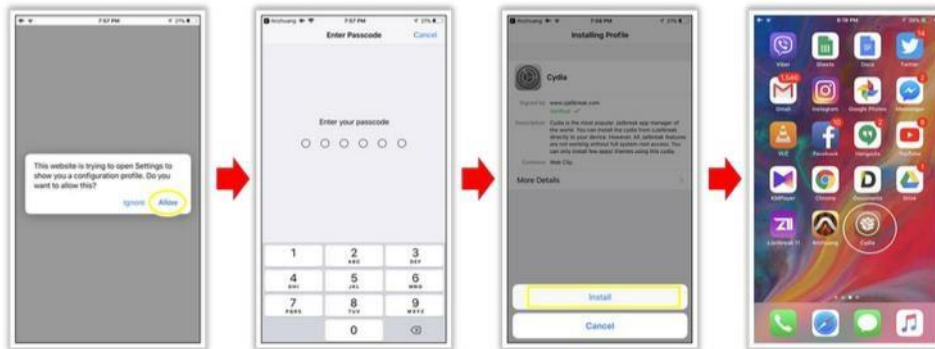


FIGURE 17.11: Cydia Jailbreak application icon on home screen

The screenshot shows a webpage titled "Jailbreaking Tools" with a "Keen Jailbreak" section. The section text reads: "Keen Jailbreak is an unofficial Semi-tethered tool that was released for iOS 11 beta versions. It is compatible to jailbreak following devices: Phone 7 & 7 Plus, iPhone 6S & 6S Plus, iPhone 6 & 6 Plus, iPhone SE / iPhone 5s, iPod Touch 6G, iPad Mini 2 / iPad Mini 3 / iPad Mini 4, iPad Air / iPad Air 2 / iPad Pro". To the right, there are links to other tools: Yalu (http://pangu8.com), Velonzy (http://pangu8.com), Pangu9 Jailbreak (https://pangu9.net), TaiG (https://www.taigjailbreak.org), and Pangu (http://en.pangu.io). The page also features a "CEH" logo and a copyright notice for EC-Council.

Jailbreaking Tools

- **Keen Jailbreak**

Source: <http://pangu8.com>

Keen Jailbreak is an unofficial semi-tethered tool that was released for iOS 11 beta versions.

It is compatible to jailbreak the following devices:

- Phone 7 & 7 Plus, iPhone 6S & 6S Plus, iPhone 6 & 6 Plus
- iPhone SE/iPhone 5s, iPod Touch 6G
- iPad Mini 2/iPad Mini 3/iPad Mini 4
- iPad Air/iPad Air 2/iPad Pro

Following are some of the additional iOS Jailbreaking tools:

- Yalu (<http://pangu8.com>)
- Velonzy (<http://pangu8.com>)
- Pangu9 Jailbreak (<https://pangu9.net>)
- TaiG (<https://www.taigjailbreak.org>)
- Pangu (<http://en.pangu.io>)
- JAILBREAK (<http://www.evad3rs.net>)
- Redsn0w (<http://www.redsn0w.us>)
- evasi0n7 (<http://evasi0n7.us>)

- GeeksN0w (<http://geeksn0w.net>)
- Sn0wbreeze (<https://ih8sn0w.com>)
- LimeRa1n (<http://www.limera1n.com>)
- Blackra1n (<http://blackra1n.com>)

Hacking Mobile Platforms
Hacking iOS

iOS Trojans

AceDeceiver

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

Spy/MobileSpy:iPhoneOS

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

Aliases

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Trojans

▪ AceDeceiver Trojan

AceDeceiver Trojan is capable of conducting MITM attacks on any iPhone and is not limited to jailbroken devices. This Trojan exploits design flaws in Apple's Digital Rights Management (DRM) mechanism and does not require an enterprise certificate. It uses the Fair Play MITM technique to spread pirated iOS apps via fake iTunes software on iOS devices.

Following figure depicts the AceDeceiver Trojan's FairPlay MITM attack scenario:

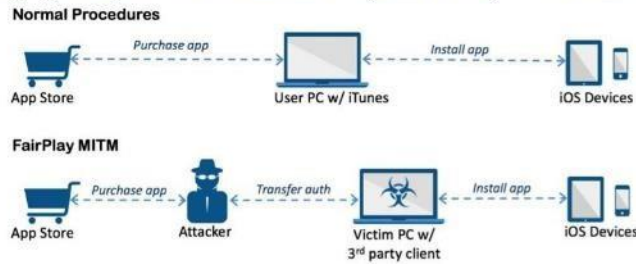


FIGURE 17.12: AceDeceiver Trojan's FairPlay MITM attack scenario

▪ Spy/MobileSpy:iPhoneOS

This malware allows an attacker to eavesdrop all incoming and outgoing calls, SMSs, URLs, and GPS position to a remote server on the infected iOS device. Jailbroken applications are usually installed using an application named Cydia. Installation of this spyware requires a jailbroken iPhone.

Aliases:

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

The spyware installs or creates the following files on the iPhone:

- **System/Library/LaunchDaemons/com.ms.msd.plist**: this file ensures the msd daemon is run after reboot, and then run permanently.
- **System/Library/LaunchDaemons/com.ms.mslocd.plist**: same but for the mslocd daemon.
- **User/Library/SMS/sms.db**: this is a SQLite 3 database. It stores victim's messages, the spyware's version, and various internal counters.
- **User/Library/CallHistory/call_history.db**: same as sms.db but for call logs.
- **usr/libexec/msd**: the main spyware daemon
- **usr/libexec/mdlocd**: location manager daemon
- **var/mobile/.ll.dat**

Following are some of the additional iOS Trojans:

- | | |
|------------------|---------------|
| ▪ DualToy Trojan | ▪ iKeyGuard |
| ▪ KeyRaider | ▪ PawnStorm.B |
| ▪ XcodeGhost | ▪ WireLurker |
| ▪ AdThief/Spad | ▪ Ikee/Eeki |
| ▪ Trapsms | |

The infographic is titled "Guidelines for Securing iOS Devices" and is part of the "Hacking Mobile Platforms" series. It lists 12 guidelines:

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Guidelines for Securing iOS Devices

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
- Disable Javascript and add-ons from web browser
- 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**
- Use iOS devices on a secured and protected Wi-Fi network
- Do not store sensitive data on client-side database
- Do not access web services on a compromised network
- Do not open links or attachments from unknown sources
- Deploy only trusted third-party applications on iOS devices
- Change default password of iPhone's root password from alpine
- Do not jailbreak or root your device if used within enterprise environments
- Configure Find My iPhone and utilize it to wipe a lost or stolen device

- Enable Jailbreak detection and also protect access to iTunes AppleID and Google accounts, which are tied to sensitive data
- Disable iCloud services so that sensitive enterprise data is not backed up to the cloud (Note that cloud services can back up documents, account information, settings, and messages)
- 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**

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

The screenshot shows a webpage titled "iOS Device Tracking Tools" with a navigation bar for "Hacking Mobile Platforms" and "Hacking iOS". The main content is titled "Find My iPhone" and includes the following text:

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

Below this is a section titled "How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods" with the following steps:

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

In the center is a screenshot of an iPhone's "iCloud" settings page, with "Find My iPhone" highlighted. To the right is a list of tracking services:

- Phonty (<https://phonty.com>)
- SpyBubble (<https://thespybubble.com>)
- GadgetTrak (<http://www.gadgettrak.com>)
- iLocals (<http://locals.com>)
- GPS Tracker by FollowMee (<https://itunes.apple.com>)

At the bottom of the screenshot, there is a URL <https://support.apple.com> and a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

iOS Device Tracking Tools

Given below are few iOS device tracking tools:

- **Find My iPhone**

Source: <https://support.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 protects 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 version, then 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 also keeps track of where it has been so that you can view its recent location history from the Find My iPhone app.

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

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

Following are some of the additional iOS device tracking tools:

- Phonty (<https://phonty.com>)
- SpyBubble (<https://thespybubble.com>)
- GadgetTrak (<http://www.gadgettrak.com>)
- iLocalis (<http://ilocalis.com>)
- GPS Tracker by FollowMee (<https://itunes.apple.com>)
- iHound (<http://ihoundgps.com>)

Hacking Mobile Platforms
Hacking iOS

iOS Device Security Tools

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

<https://www.avira.com>

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Device Security Tools

- **Avira Mobile Security**

Source: <https://www.avira.com>

This Avira Mobile Security tool provides features such as web protection, identity safeguarding, identifies Phishing websites that target you personally, securing emails, tracking your device, identifying activities, organizing device memory, and backing up all your contacts, and so on for all iOS devices.

Following are some of the additional iOS device security tools:

- Norton Mobile Security (<https://us.norton.com>)
- LastPass Password Manager (<https://www.lastpass.com>)
- Lookout for iOS (<https://www.mylookout.com>)
- SplashID Safe Password Manager (<https://www.splashid.com>)
- Webroot SecureWeb Browser (<https://www.webroot.com>)
- Wickr Me - Private Messenger (<https://www.wickr.com>)
- 1Password (<https://1password.com>)
- GadgetTrak (<http://www.gadgettrak.com>)
- iLocalis (<http://ilocalis.com>)

Hacking Mobile Platforms

Module Flow

CEH

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms

Mobile Spyware

Mobile Spyware

CEH

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Spyware

People's lifestyles are becoming increasingly reliant on smartphones and tablets. In addition, recent developments in mobile commerce have enabled users to perform transactions such as purchasing goods, booking tickets, banking, and so on from their smartphones. However, weak mobile's moderately lax security has made them attractive and valuable targets of attackers. Attackers use mobile spyware to trace information from their target person's or organization's telephones/cell phones.

This section discusses the various mobile spyware that attackers use to collect the information.

Mobile spyware is a software tool that gives you full access to monitor a victim's phone or cell. It will completely hide itself from the user of the phone. It will record and log all activity on the phone such as Internet use, text messages, and phone calls. Then you can access the logged information via the software's main website, or you can also get this tracking information through SMS or email. Usually, this spyware helps to monitor and track phone usage of employees. However, attackers are using this spyware to trace information from their target person's or organization's telephones/cell phones. Using this spyware does not require any authorized privileges.

Following are the most common telephone/cellphone spyware features:

- **Call History:** Allows you to see the entire call history of the phone (both incoming and outgoing calls).
- **View Text Messages:** Enables you to view all incoming and outgoing text messages. It even shows deleted messages in the log report.
- **Web Site History:** Records the entire history of all websites visited through the phone in the log report file.
- **GPS Tracking:** Shows you where the phone is in real time. There is also a log of the cell phone's location so you can see where the phone has been.

Hacking Mobile Platforms
Mobile Spyware

Mobile Spyware: mSpy

CEH
Certified Ethical Hacker

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



<https://www2.mspy.com>
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms
Mobile Spyware

Mobile Spywares

CEH
Certified Ethical Hacker

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



- Spyera**
<http://spyera.com>
- Highster Mobile**
<http://www.highstermobi.com>
- TeenSafe**
<http://www.teenSAFE.com>
- MobiStealth**
<http://www.mobistealth.com>
- TheTruthSpy**
<http://thetruthspy.com>

<https://www.flexispy.com>
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Spywares

Following are some of the mobile spywares that obtain information from mobile device without the knowledge or consent of the user:

- **mSpy**

Source: <https://www2.mspy.com>

mSpy is a mobile monitoring and spying application which runs on the target device to log all activities including call log history, GPS location, calendar updates, text messages,

emails, web history, instant messenger chats, keystrokes, and so on and also can control applications. This product is useful to monitor versatile online/offline actions of employees and underage children.

Features:

- Manage Calls (Call Logs, Incoming Calls Restriction)
- Track text messages (Sent/Received text messages)
- Read emails (Incoming/Outgoing Emails)
- Track GPS Location (Current GPS Location, Geo-Fencing)
- Monitor Internet Use (Browsing History, Website Bookmarks, Blocking Websites, Wi-Fi Networks, Keyword alerts)
- Access Calendar and Address Book (Calendar Activities, Contacts)
- Read Instant Messages (Skype, WhatsApp, iMessage, Social Network, Viber, Snapchat, LINE, Telegram, Tinder)
- Control Apps and Programs (Installed Applications, Application blocking, Keylogger)
- View Multimedia Files (Photos, Videos)
- Remote Control (Device Wipeout, Locked Device, Additional Device Info, Control Panel)

▪ **FlexiSPY**

Source: <https://www.flexispy.com>

FlexiSpy is the mobile monitoring software used to spy on mobile phones and tablets. It supports Android, iPhone, iPad, PC and Mac and it can silently monitor all communications, locations, and user behavior of a smartphone from any web browser.

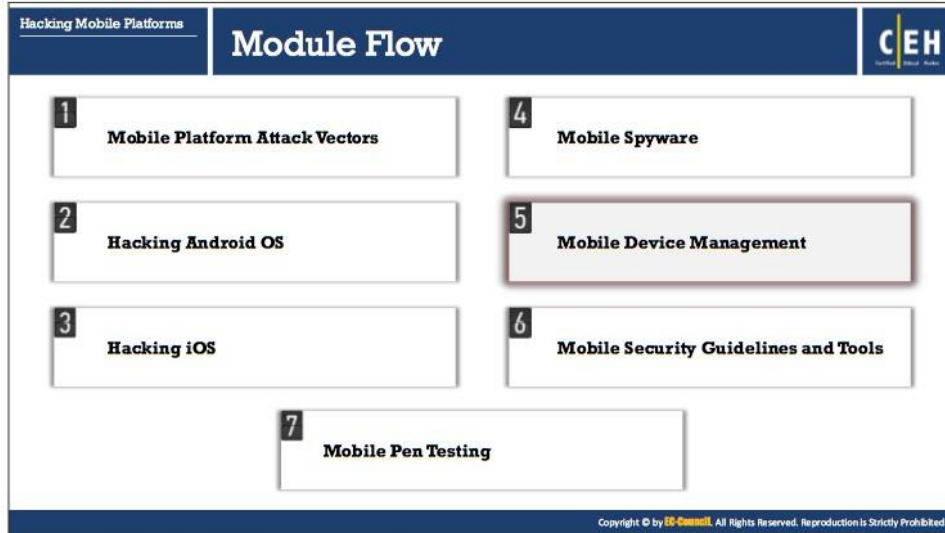
Features:

- | | |
|------------------------------|------------------------|
| ○ Spying On Instant Messages | ○ Cell Phone Tracker |
| ○ Call Interception | ○ Spy On Mobile Phones |
| ○ SMS Tracker | ○ VoIP Call Recording |
| ○ Tap Into the Room | ○ Spy Remotely |

Following are the some of the additional mobile spyware applications:

- Spyera (<https://spyera.com>)
- Highster Mobile (<http://www.highstermobi.com>)
- TeenSafe (<https://www.teensafe.com>)
- MobiStealth (<http://www.mobistealth.com>)
- TheTruthSpy (<http://thetruthspy.com>)
- OneSpy (<https://www.onespy.in>)
- Mobile Spy (<http://www.mobile-spy.com>)

- iKeyMonitor (<https://ikeymonitor.com>)
- XNSPY (<https://xnspy.com>)
- SpyBubble (<https://thespybubble.com>)
- SpyPhoneTap (<http://www.spyphonetap.com>)
- PhoneSheriff (<http://www.phonesheriff.com>)
- My Mobile Watchdog (<https://www.mymobilewatchdog.com>)
- SpyToMobile (<https://spytomobile.com>)
- Hoverwatch (<http://www.hoverspyapp.com>)
- Spyzie (<https://www.spyzie.com>)
- Phone Spy (<http://www.phonespysoftware.com>)
- MobileSpyAgent (<http://www.mobilespyagent.com>)
- VRS Recording System (<http://www.nch.com.au>)




Mobile Device Management

MDM is gaining much importance with adoption of policies such as BYOD across 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. Companies use a kind of security software for administration of all the mobile devices connected to the enterprise network.

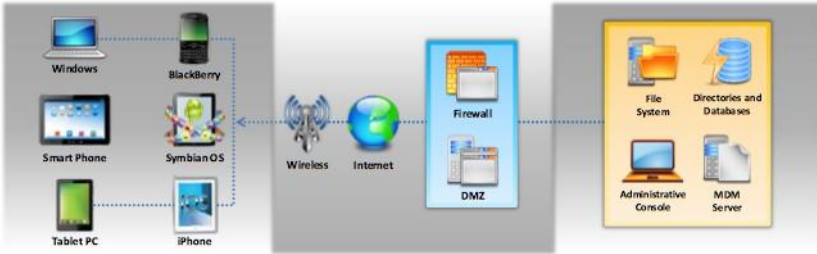
This section deals with MDM and its solutions that help to secure monitor, manage, and support mobile devices.

Hacking Mobile Platforms
Mobile Device Management

Mobile Device Management (MDM)



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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM)

MDM provides platforms for over-the-air or wired distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on. It helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and supports mobile devices. It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise.

Following are basic features of MDM software:

- 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

Mobile Device Management Solutions

- **IBM MaaS360**

Source: <https://www.ibm.com>

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

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:** It 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 MDM 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.

The screenshot shows a webpage titled "Mobile Device Management Solutions" with a sub-header "Mobile Device Management". The main content area features a large section for "XenMobile" with a description: "Citrix XenMobile contains mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), secure network gateway, and enterprise-grade mobile productivity apps in one comprehensive enterprise mobility management solution". Below this is a screenshot of the XenMobile dashboard, which displays various metrics and charts. To the right of the XenMobile section, there is a list of other MDM solutions, each with a logo and a URL: VMware AirWatch (https://www.air-watch.com), Sicap Device Management Centre (https://www.sicap.com), SOTI MobiControl (https://www.soti.net), MobiLock Pro (https://mobilock.in), and ManageEngine Mobile Device Manager Plus (https://www.manageengine.com). At the bottom of the screenshot, there is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

- **XenMobile**

Source: <https://www.citrix.com>

Citrix XenMobile contains MDM, mobile application management (MAM), mobile content management (MCM), secure network gateway, and enterprise-grade mobile productivity apps in one comprehensive enterprise mobility management solution. XenMobile lets you configure and manage mobile devices that can be shared by multiple users. With XenMobile, shared devices and apps are kept secure. IT can apply security policies specific to each user's role in the organization, and can also geo-fence devices by locking each device to a specific network ID. This approach can reduce the appeal for device thieves. Geo-fenced devices also improve productivity in many work scenarios. XenMobile enhances the user experience on BYO or corporate devices, without compromising security.

Following are the some of the additional MDM solutions:

- VMware AirWatch (<https://www.air-watch.com>)
- Sicap Device Management Centre (<https://www.sicap.com>)
- SOTI MobiControl (<https://www.soti.net>)
- MobiLock Pro (<https://mobilock.in>)
- ManageEngine Mobile Device Manager Plus (<https://www.manageengine.com>)
- MobileIron's Mobile device management (<https://www.mobileiron.com>)
- Tangoe MDM (<https://www.tangoe.com>)
- Microsoft Intune (<https://www.microsoft.com>)

- MediaContact (<https://en.telelogos-mediacontact.com>)
- Amtelnet EMM (<http://www.amtelnet.com>)
- Beachhead's SimplySecure Management System (<https://www.beachheadsolutions.com>)
- Absolute Manage (<https://www.absolute.com>)
- BlackBerry® Unified Endpoint Manager (<https://global.blackberry.com>)
- Good Mobile Manager (<http://help.blackberry.com>)

Hacking Mobile Platforms
Mobile Device Management

Bring Your Own Device (BYOD)

CEH

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

BYOD Benefits

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bring Your Own Device (BYOD)

BYOD refers to a policy allowing an employee to bring their personal devices such as laptops, smartphones, and tablets at workplace and use them for accessing organization's resources as per their access privileges.

The policy of BYOD allows employees to use the devices that they are comfortable with and best fits his/her preferences and work purposes. With "work anywhere, anytime" strategy, the challenge in the BYOD trend is to secure company's 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 that 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, 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 professional 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. It 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).



The infographic is titled "BYOD Risks" and is part of a "Hacking Mobile Platforms" series. It lists ten risks in a two-column grid. Each risk is numbered in a black circle and includes a key term in red. The risks are: 01. Sharing confidential data on unsecured network; 02. Data leakage and endpoint security issues; 03. Improperly disposing device; 04. Support of many different devices; 05. Mixing personal and private data; 06. Lost or stolen devices; 07. Lack of awareness; 08. Ability to bypass organizations network policy rules; 09. Infrastructure issues; 10. Disgruntled employees. A copyright notice for EC-Council is at the bottom.

Number	Risk Description
01	Sharing confidential data on unsecured network
02	Data leakage and endpoint security issues
03	Improperly disposing device
04	Support of many different devices
05	Mixing personal and private data
06	Lost or stolen devices
07	Lack of awareness
08	Ability to bypass organizations network policy rules
09	Infrastructure issues
10	Disgruntled employees

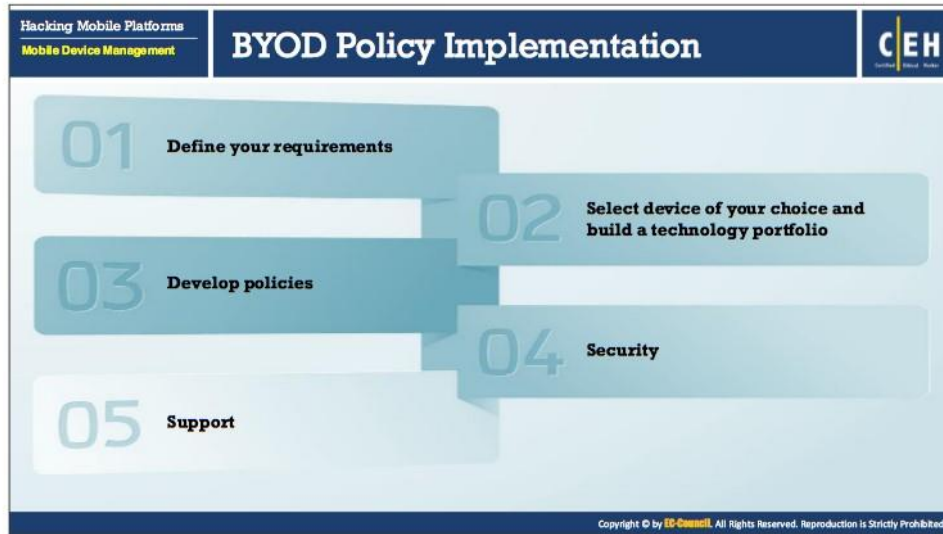
BYOD Risks

Employees connecting to the corporate network or accessing corporate data using their own mobile devices pose security risks to an organization. Following 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:** An improperly disposed of device 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 device does 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 for different devices and processes can increase cost. Employee-owned devices have limited security and come in a variety of different platforms. This deters IT department's capability to manage and control devices in a company.
- **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 his/her mobile device that is used for both personal and official purposes, the organization might face a security risk, as the 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's 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 devices' 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 information to competitors.



BYOD Policy Implementation

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.

Perform 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. It provides an organized procedure to document facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project life cycle. It should be a central activity performed 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. In addition, 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 such as HR, Legal, Security, and Privacy.

Following are the 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 a thorough assessment of the operating environment and the development of a solution that provides for the following: 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 the following aspects:

- 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.

The infographic is titled "BYOD Security Guidelines" and is divided into two columns: "For Administrator" and "For Employee". The "For Administrator" column lists eight guidelines, including securing data centers, educating employees, clarifying app ownership, using encrypted channels, controlling app access, and applying session authentication. The "For Employee" column lists seven guidelines, including using encryption, separating business and personal data, registering devices, updating OS and patches, using anti-virus and DLP, setting strong passcodes, and setting app passwords. The infographic includes a header with "Hacking Mobile Platforms" and "Mobile Device Management" on the left, and "CEH" on the right. A copyright notice is at the bottom.

For Administrator

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

For Employee

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

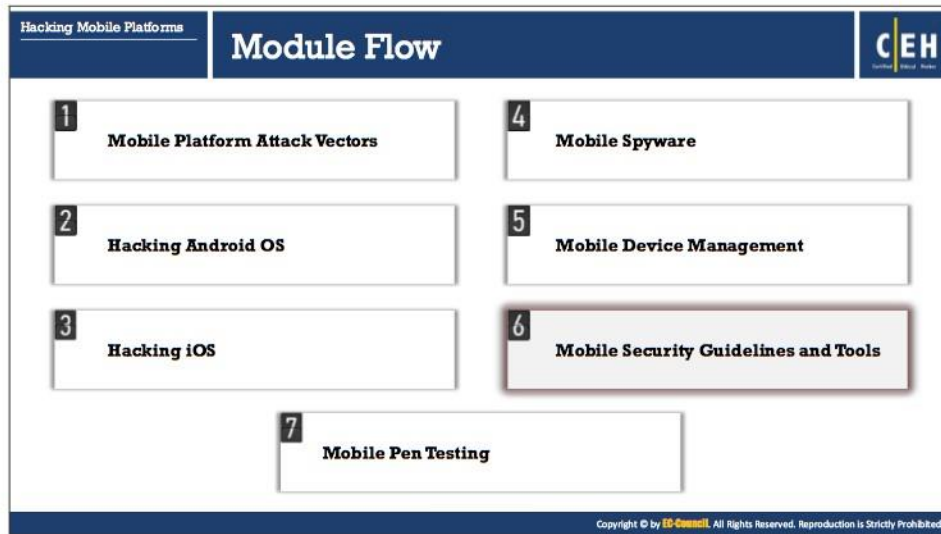
BYOD Security Guidelines

▪ For Administrator

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

- Secure organization's data centers with multi-layered protection systems
- Educate your employees about the BYOD policy
- Make it clear who owns what apps and data
- Use encrypted channel for data transfer
- Make it clear what apps will be allowed or banned
- Control access based on the need-to-know
- Do not allow jailbroken and rooted devices
- Apply session authentication and timeout policy on access gateways
- 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. In addition, 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 is 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 OSs 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.
- **For Employee**
- Listed below are the guidelines an employee should follow to secure sensitive personal or corporate information stored on a mobile device:
- Use encryption mechanism to store data
 - Maintain a clear separation between the business and personal data
 - Register devices with a remote locate and wipe facility if company policy permits
 - Regularly update your device with latest OS and patches
 - Use anti-virus and data loss prevention (DLP) solutions
 - 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



Mobile Security Guidelines and Tools

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.

Hacking Mobile Platforms
Mobile Security Guidelines and Tools

General Guidelines for Mobile Platform Security

CEH





















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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms
Mobile Security Guidelines and Tools

General Guidelines for Mobile Platform Security (Cont'd)

CEH

  Use passcode	 Perform periodic backup and synchronization 
  Update OS and Apps	 Filter e-mail-forwarding barriers 
  Enable remote management and use remote wipe services	 Configure Application certification rules 
  Do not allow Rooting or Jailbreaking	 Harden browser permission rules 
  Encrypt storage	 Design and implement mobile device policies 

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for Mobile Platform Security

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

- Do not load too many applications and avoid auto-upload of photos to social networks
- Perform a Security Assessment of the Application Architecture
- Maintain configuration control and management

- Install applications from trusted application stores
- Securely wipe or delete the data disposing of the device
- Do not share the information within GPS-enabled apps unless they are necessary
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Disable wireless access such as Wi-Fi and Bluetooth, if not in use
 - Ensure that your Bluetooth is “off” by default. Turn it on whenever it is necessary
 - Disable wireless access such as Wi-Fi and Bluetooth, if not in use, to avoid illegal wireless access to the device
 - Disable sharing/tethering Internet connections over Wi-Fi and Bluetooth when not in use
- **Use Passcode**
 - Configure a strong passcode with maximum possible length to gain access to your mobile devices
 - Set an idle timeout to automatically lock the phone when not in use
 - Enable lockout/wipe feature after a certain number of attempts
 - Consider the eight character nonsimple passcode
 - Thwart passcode guessing: set erase data to ON
- **Update OS and Apps**
 - Update OS and apps to keep them secure
 - Apply software updates when new releases are available
 - Perform regular software maintenance
- **Enable Remote Management**
 - In an enterprise environment, use MDM software to secure, monitor, manage, and support mobile devices deployed across the organization
- **Do not allow Rooting or Jailbreaking**
 - Ensure your MDM solutions prevent or detect rooting/jailbreaking
 - Include this clause in your mobile security policy
- **Use Remote Wipe Services**
 - Use remote wipe services such as Find My Device (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen
 - Report a lost or stolen device to IT so that they can disable certificates and other access methods associated with the device

- **Encrypt Storage**
 - If supported, configure your mobile device to encrypt its storage with hardware encryption
 - Use device encryption and patch applications
 - Encrypt the device and backups
- **Perform periodic backup and synchronization**
 - Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization
 - (Android) Backup to Google Account so that sensitive enterprise data is not backed up to the cloud
 - Control the location of backups
 - Encrypt backups
 - Keep sensitive data off of shared mobile devices. If enterprise information is locally stored on a device, then it is recommended that this device not be openly shared.
 - Limit logging data stored on device
 - Use a secure data-transfer utility or encrypt data in transit to or from the device, to ensure confidentiality and data integrity
- **Filter email-forwarding barriers**
 - Filter email/emails by configuring server-side settings of the corporate email/email system
 - Use commercial data loss prevention filters
 - Prevent local caching of email
- **Configure Application certification rules**
 - Allow only signed applications to install or execute
 - Configure wireless to ask to join networks
 - Sandbox application and data
 - Enable auto-lock and set to one minute
 - Consider the privacy implications before enabling location-based services and limit usage to trusted applications
 - Configure location services to disable location tracking for applications that you do not want to know your location information
 - Configure notifications to disable the ability to view notifications while the device is locked for applications that could display sensitive data

- Configure AutoFill—Auto-fill names and passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by enterprise policy)
- Disable the collection of Diagnostics and Usage Data under **Settings → General → About**
- **Harden browser permission rules**
 - Harden browser permission rules according to company's security policies to avoid attacks
- **Design and implement mobile device policies**
 - Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices
- Control devices and applications
- Prohibit USB keys
- Manage operating and application environment
- Press the power button to lock the device whenever it is not in use
- Verify the location of printers before printing sensitive documents
- Ask your IT department how to use Citrix technologies to keep data in the data center and keep personal devices personal
- If you must have sensitive data on a mobile device, use follow-me data and ShareFile as an enterprise-managed solution

The screenshot shows a document titled "Mobile Device Security Guidelines for Administrator" from the "Hacking Mobile Platforms" section. It lists seven guidelines (01-07) and a set of authentication options. The guidelines are:

- 01 Publish an **enterprise policy** that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise
- 02 Publish an enterprise policy for **cloud**
- 03 Enable **security measures** such as antivirus to protect the data in the datacenter
- 04 Implement policy that specifies what levels of **application and data access** are allowable on consumer-grade devices, and which are prohibited
- 05 Specify a **session timeout** through **Access Gateway**
- 06 Specify whether the **domain password** can be cached on the device, or whether users must enter it every time they request access
- 07 Determine the allowed **Access Gateway authentication methods** from the following:

Authentication methods listed:

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Guidelines for Administrator

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








- Publish an enterprise policy that specifies the acceptable usage of consumer-grade devices and BYOD in the enterprise
- Publish an enterprise policy for cloud
- Enable security measures such as antivirus to protect the data in the data center
- Implement policy that specifies what levels of application and data access are allowable on consumer-grade devices and which ones are prohibited
- Specify a session timeout through Access Gateway
- Specify whether the domain password can be cached on the device or whether users must enter it every time they request access
- Determine the allowed Access Gateway authentication methods from the following:
 - No authentication
 - Domain only
 - SMS authentication
 - RSA SecurID only
 - Domain + RSA SecurID
- 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, etc.
- 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

Hacking Mobile Platforms
Mobile Security Guidelines
and Tools

SMS Phishing Countermeasures

CEH
Certified Ethical Hacker

- 01 Never reply to a **suspicious SMS** without verifying the source 
- 02 Do not click on any **links** included in the SMS 
- 03 Never reply to a SMS that requires **personal and financial information** from you 
- 04 Review the **bank's policy** on sending SMS 
- 05 Enable the "**block texts from the internet**" feature from your provider 
- 06 Never reply to a SMS which urging you to **act or respond quickly** 
- 07 **Never call a number** left in a SMS 

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Countermeasures

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

- Never reply to a suspicious SMS without verifying the source
- Do not click on any links included in the SMS
- Never reply to a SMS that requires personal and financial information from you
- Review the bank's policy on sending SMS
- Enable the "block texts from the internet" feature from your provider
- Never reply to a SMS that urges you to act or respond quickly
- Never call a number left in a SMS
- 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 nontelephonic numbers
- Check for spelling mistakes, grammatical errors, or language inconsistency in text messages

Hacking Mobile Platforms
Mobile Security Guidelines and Tools

Mobile Protection Tools

Lookout Personal

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

Features

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



<https://www.lookout.com>

Zimperium's zIPS

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



<https://www.zimperium.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms
Mobile Security Guidelines and Tools

Mobile Protection Tools (Cont'd)

BullGuard Mobile Security

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



<https://www.bullguard.com>

McAfee Mobile Security
<https://www.mcafee.com>

Kaspersky Internet Security for Android
<https://my.kaspersky.com>

AVG AntiVirus Pro for Android
<https://www.avg.com>

F-Secure Mobile Security
<https://www.f-secure.com>

Avast Mobile Security
<https://www.avast.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Protection Tools

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.

- **Lookout Personal**

Source: <https://www.lookout.com>

Lookout Personal helps to protect your device from security threats, loss, and theft, available for Android and iPhone devices. It provides mobile security, identity protection, and theft prevention in a single app.

Features:

- **All-in-one Protection:** Lookout combines the most advanced mobile security with all-in-one identity protection and intelligent theft prevention.
- **Mobile Threat Security:** Secure your smartphone against mobile threats such as malware, adware, and phishing, before they harm with the world's most advanced mobile security.
- **Identity Theft Protection:** Lookout gives you 24/7 access to ID Restoration Experts and \$1M Identity Theft Insurance to help recover and restore your identity.
- **Breach Report:** Get timely alerts on corporate breaches that may affect you and advice on simple steps to protect your personal information.
- **Theft Protection:** Lookout gives you the easiest tools to find your lost or stolen phone, including email alerts with a photo and map if a thief tries to steal it.
- **Data Backup:** Quickly access photos and data from your smartphone or tablet using any internet connected device.

- **Zimperium's zIPS**

Source: <https://www.zimperium.com>

Zimperium's zIPS is the mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device and application cyber attacks. It uses advanced machine-learning techniques to identify and prevent both network-based and host-based threats such as

- MITM attacks that can intercept your passwords and other confidential information when you are using public or private Wi-Fi 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

zIPS is equipped with a behavioral analysis engine to automatically detect and block malicious threats by monitoring how they change the characteristics of the mobile device. It scans all mobile applications and browsers to enhance the security of user device and keeps your whole organization safe from MITM, IPv4, and even IPv6 attacks.

It provides automated alerts to both the security officer and the user in the event of an incident. It uses “nonintrusive packet monitoring” to detect advanced mobile threats.

- **BullGuard Mobile Security**

Source: <https://www.bullguard.com>

BullGuard Mobile Security is an app for Android devices that provides total protection for mobile devices and personal data. It delivers complete mobile phone antivirus against all mobile phone viruses. It locks, locates, and wipes data remotely if the device gets lost or stolen. It blocks unwanted calls and SMSs.

Features:

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

Following are some of the additional mobile protection tools:

- McAfee Mobile Security (<https://www.mcafee.com>)
- Kaspersky Internet Security for Android (<https://my.kaspersky.com>)
- AVG AntiVirus Pro for Android (<https://www.avg.com>)
- F-Secure Mobile Security (<https://www.f-secure.com>)
- Avast Mobile Security (<https://www.avast.com>)
- Trend Micro Mobile Security for Android (<https://www.trendmicro.com>)
- Norton Mobile Security (<https://my.norton.com>)
- Comodo Mobile Security (<https://www.comodo.com>)
- ESET Mobile Security (<https://www.eset.com>)
- Bitdefender Mobile Security (<https://www.bitdefender.com>)
- Sophos Mobile Security for Android (<https://www.sophos.com>)
- WISEID (<https://www.wiseid.com>)

The screenshot shows a webpage titled "Mobile Anti-Spyware" with a dark blue header. On the left, there is a section for "Malwarebytes for Android" with a list of features. In the center, two smartphone screens are shown: one displaying the Malwarebytes interface and another showing a "Ransomware Detected" warning. On the right, four boxes list other mobile security tools: "AntiSpy Mobile", "FREE Spyware & Malware Remover", "D-Vasive Anti-Spy", and "SpyWare Removal (Anti Spy)". A footer at the bottom of the screenshot reads "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Mobile Anti-Spyware

- **Malwarebytes for Android**

Source: <https://www.malwarebytes.org>

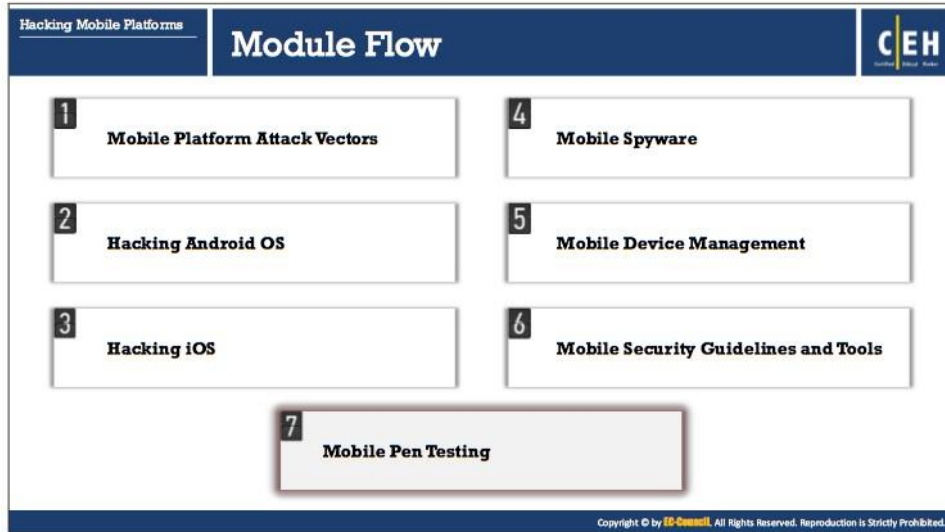
Malwarebytes anti-malware mobile tool is a protection against malware, ransomware, and other growing threats to Android devices.

Features:

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

Following are some of the additional mobile anti-spyware tools:

- AntiSpy Mobile (<http://www.antispy-mobile.com>)
- FREE Spyware & Malware Remover (<https://play.google.com>)
- D-Vasive Anti-Spy (<http://www.dvasive.com>)
- SpyWare Removal (Anti Spy) (<https://play.google.com>)



Mobile Pen Testing

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 the device's 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.

Hacking Mobile Platforms
Mobile Pen Testing

Android Phone Pen Testing

```

graph TD
    START((START)) --> A[Root an Android Phone]
    A --> B[Perform DoS and DDoS Attacks]
    B --> C[Check for vulnerabilities in Android browser]
    C --> D[Check for vulnerabilities in SQLite]
    D --> E[Check for vulnerabilities in Intents]
    E --> F[Detect capability leaks in Android devices]
            
```

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

Copyright © by **ED-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms
Mobile Pen Testing

iPhone Pen Testing

```

graph TD
    START((START)) --> A[Jailbreak the iPhone]
    A --> B[Unlock the iPhone]
    B --> C[Use SmartCover to bypass passcode]
    C --> D[Hack iPhone using Metasploit]
    D --> E[Check for access point]
    E --> F[Check IOS device data transmission on Wi-Fi networks]
    F --> G[Check whether the malformed data can be sent to the device]
            
```

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

Copyright © by **ED-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Pen Testing Toolkit

- **Hackode**

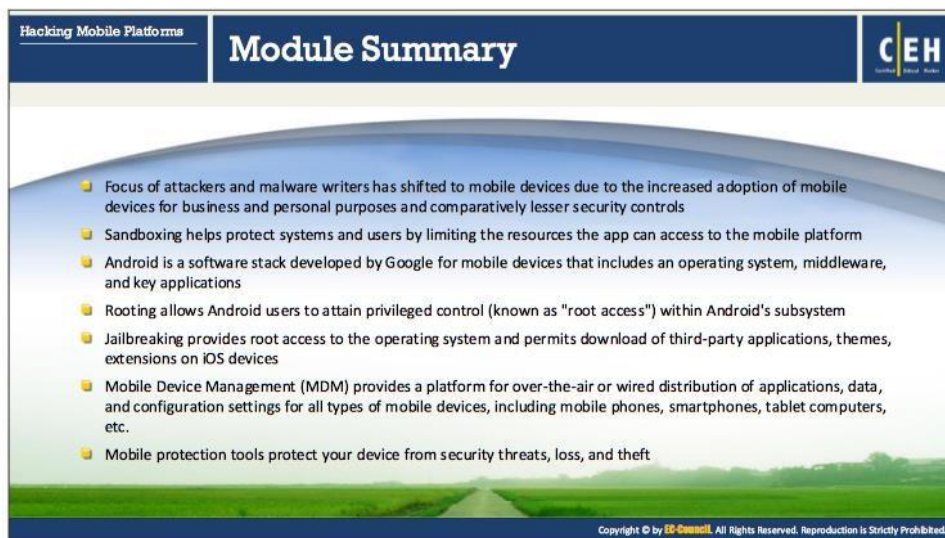
Source: <https://play.google.com>

Hackode is the hacker's toolbox. It is an application for penetration testers, ethical hackers, IT administrators, and cyber security professionals to perform different tasks such as reconnaissance, scanning for exploits, and so on. It contains modules including reconnaissance, scanning, exploits, and security feed.

Reconnaissance module contains Google Hacking that can identify websites for PHPMYADMIN, PHP CONFIG, SQL INJECTION, MYSQLSERVER, LOGINPORTALS, PASSWORDS, and Whois Lookup, which can identify domain name, email, and DNS Lookup.

Scanning module allows you to perform PING, TRACEROUTE, MX RECORD, and DNS DIG functions.

Google Hacking and Google Dorks, Whois, Ping, Traceroute, DNS lookup, MX Records, DNS Dig, Exploits and Security Rss Feed, and so on are some of the important features of this toolkit.



The slide features a dark blue header with the text 'Hacking Mobile Platforms' on the left and 'Module Summary' in the center. On the right side of the header is the CEH logo. The main content area has a light blue background with a curved top and a green landscape at the bottom. It contains a bulleted list of seven items. At the bottom right of the slide, there is a small copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

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

Module Summary

This module discussed various mobile OSs, the types of attacks typically launched on them, the tools used in doing so, and countermeasures for securing them. The next module will explain how attackers hack IoT devices and countermeasures to protect them.