Chapter 17: Hacking Mobile Platforms

Technology Brief

We all know the rapid increase of mobile phone users and flexibility of function and advancement to perform every task has brought a dramatic shift. Smartphones available in the market are running on different popular Operating systems such as iOS, Blackberry OS, Android, Symbian, and Windows, etc. They also offer application store for the users to download compatible and trusted application to run on their respective operating systems such as Apple's App Store, Android's Play Store, etc. As these mobile phones are the source of joy and helpful to perform personal and business work, they are also vulnerable. Smartphone with the malicious application or an infected phone can cause trouble for a secure network. As mobile phones are popularly used for online transactions, banking application, and other financial applications, mobile phone devices must have strong security to keep the transactions secure and confidential. Similarly, mobiles have important data such as contacts, messages, emails, login credentials, and files which can be stolen easily once a phone is compromised.

Mobile Platform Attack Vectors

OWASP Top 10 Mobile Threats

OWASP stands for Open Web Application Security Project. OWASP provides unbiased and practical, information about computer and Internet applications. According to OWASP, top 10 Mobile threats are: -

OWASP Top 10 Mobile Risks (2016)	OWASP Top 10 Mobile Risks (2014)
Improper Platform Usage	Weak Server Side Controls
Insecure Data Storage	Insecure Data Storage
Insecure Communication	Insufficient Transport Layer Protection
Insecure Authentication	Unintended Data Leakage
Insufficient Cryptography	Poor Authorization and Authentication
Insecure Authorization	Broken Cryptography
Client Code Quality	Client Side Injection

Code Tampering	Security Decisions Via Untrusted Inputs
Reverse Engineering	Improper Session Handling
Extraneous Functionality	Lack of Binary Protections

Table 17-01 OWASP Top 10 Mobile Risks

Mobile Attack Vector

There are several types of threats and attacks on a mobile device. Some of most basic threats are malware, data loss, and attack on integrity. An attacker may attempt to launch attacks through victim's browser by a malicious website or a compromised legitimate website. Social engineering attacks, data loss, data theft, data exfiltration are the common attacks on mobile technology. Mobile attack vector includes: -

- Malware
- Data Loss
- Data Tampering
- Data Exfiltration

Vulnerabilities and Risk on Mobile Platform

Apart from Attacks on a mobile platform, there are also several vulnerabilities and risk in a mobile platform. The most common risks are: -

- Malicious third-party applications
- Malicious application on Store
- Malware and rootkits
- Application vulnerability
- Data security
- Excessive Permissions
- Weak Encryptions
- Operating system Updates issues
- Application update issues
- Jailbreaking and Rooting
- Physical Attack

Application Sandboxing Issue

Sandboxing is one of the most important key components of security. It supports security as an integrated component in a security solution. Sandboxing feature is much different from other traditional anti-virus and antimalware mechanisms. Sandboxing technology offers enhanced protection by analysis of emerging threats, malware, malicious applications, etc. in a sophisticated environment with in-depth visibility and more

granular control. However, the advanced malicious application may be designed to bypass the sandboxing technology. Fragmented codes and script with sleep timer are the common techniques that are adopted by the attacker to bypass the inspection process.

Mobile Spam and Phishing

Mobile Spamming is a spamming technique for the mobile platform in which unsolicited messages or emails are sent to the targets. These spams contain malicious links to reveal sensitive information. Similarly, phishing attacks are also performed because of ease to setup and difficult to stop. Messages and email with prize-winning notifications and cash winning stories are the most commonly known spams. An attacker may either ask for credentials on a phone call, message or redirect the user to malicious website, or compromised legitimate website through a link in a spam message or email.

Open Wi-Fi and Bluetooth Networks

Public Wi-Fi, Unencrypted Wi-Fi and Bluetooth networks are another easy way for an attacker to intercept the communication and reveal information. Users connected to public Wi-Fi intentionally or unintentionally may be a victim. BlueBugging, BlueSnarfing and Packet Sniffing are the common attacks on open wireless connections.

Hacking Android OS

Introduction to Android Operating System

Android is an operating system for Smartphones developed by Google. Android is not only for Smartphones but also gaming consoles, PCs, and other IoT devices. Android OS brings flexible features, with an open source platform. Wide support application and integration with different hardware and services are the major features of this operating systems. The Android operating system has since gone through multiple major releases, with the current version being 8.1 "Oreo," released in December 2017.

A popular feature of Android is its flexibility of third-party applications. Users can download and install and remove these applications (APK) file from application stores or from the internet. however, this might be a security risk because of open source nature; this third-party application may include a number of applications that are violating the policy of a trusted application. A lot of Android hacking tools, mentioned in this workbook are also not available at the play store.

Device Administration API

Device Administration API is introduced in Android 2.2. Device Administration API ensures device administration at the system level, offering control over Android devices within a corporate network. Using these security-aware applications, the administrator can perform several actions including wiping the device remotely. Here are examples of the types of applications that might use the Device Administration API:

- Email clients.
- Security applications can do a remote wipe.
- Device management services and applications.

Root Access / Android Rooting

Rooting is basically a process of gaining privileged control over a device, commonly known as Root access. In the Android operating system, rooting is the same process of gaining privileged access to an Android device such as a smartphone, tablet, etc., over subsystems. As mentioned earlier, Android is modified version of Linux kernel; root access gives "Superuser" permissions. Root access is basically required to modify the settings and configurations that require administrator privileges however it can be used to alter the system applications and settings to overcome limitations and restrictions. Once you have root access, you have full control over kernel and applications. This rooting can be used for malicious intentions such as the installation of malicious applications, assigning excessive permissions, installation of custom firmware.
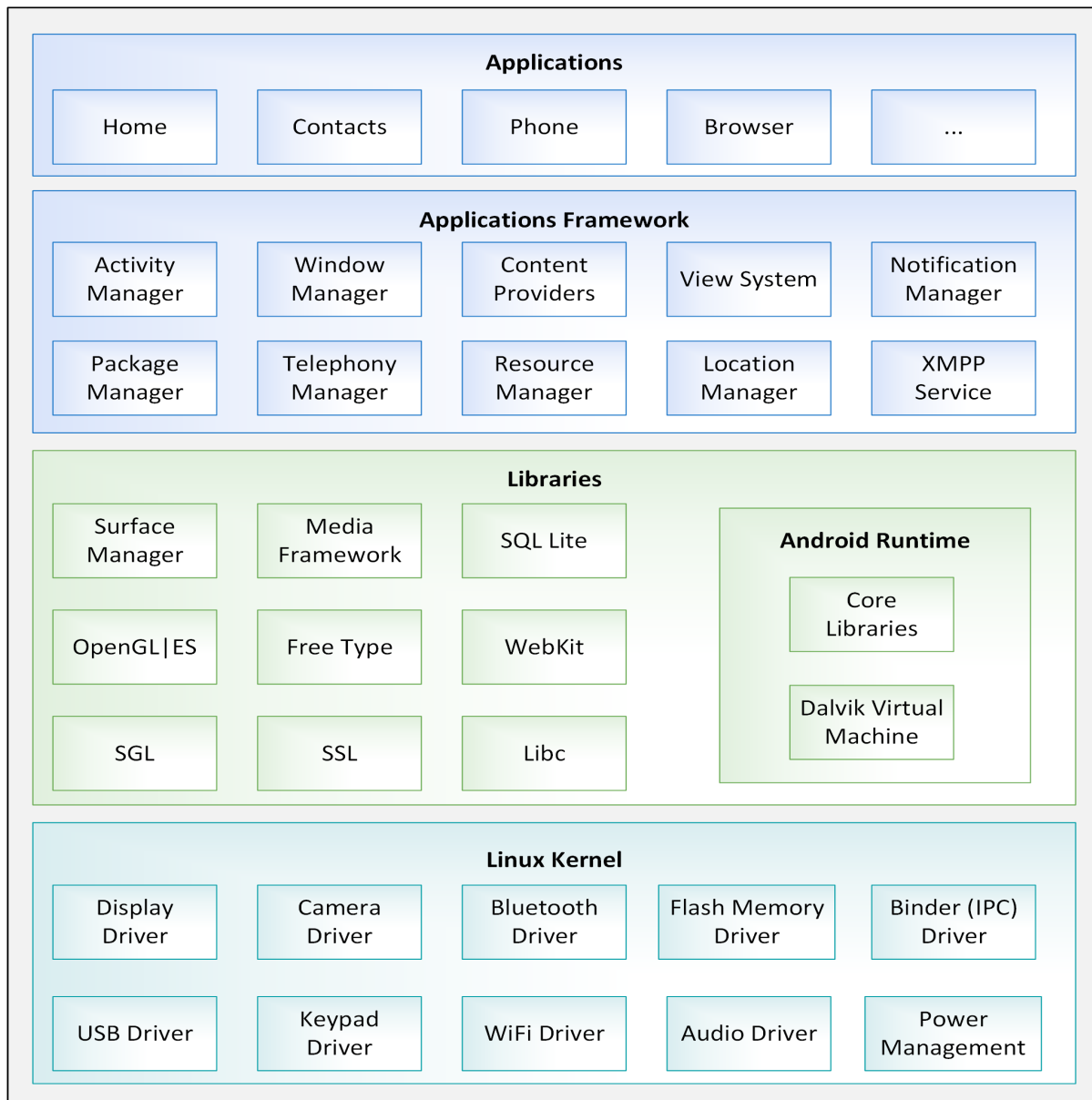
Figure 17-01. Android Framework

Android Phones Security Tools

There are several Anti-virus's applications, protection tools, vulnerability scanning tools, Anti-theft, find my phone applications available on the Play Store. These tools include: -

- DroidSheep Guard
- TrustGo Mobile Security
- Sophos Mobile Security
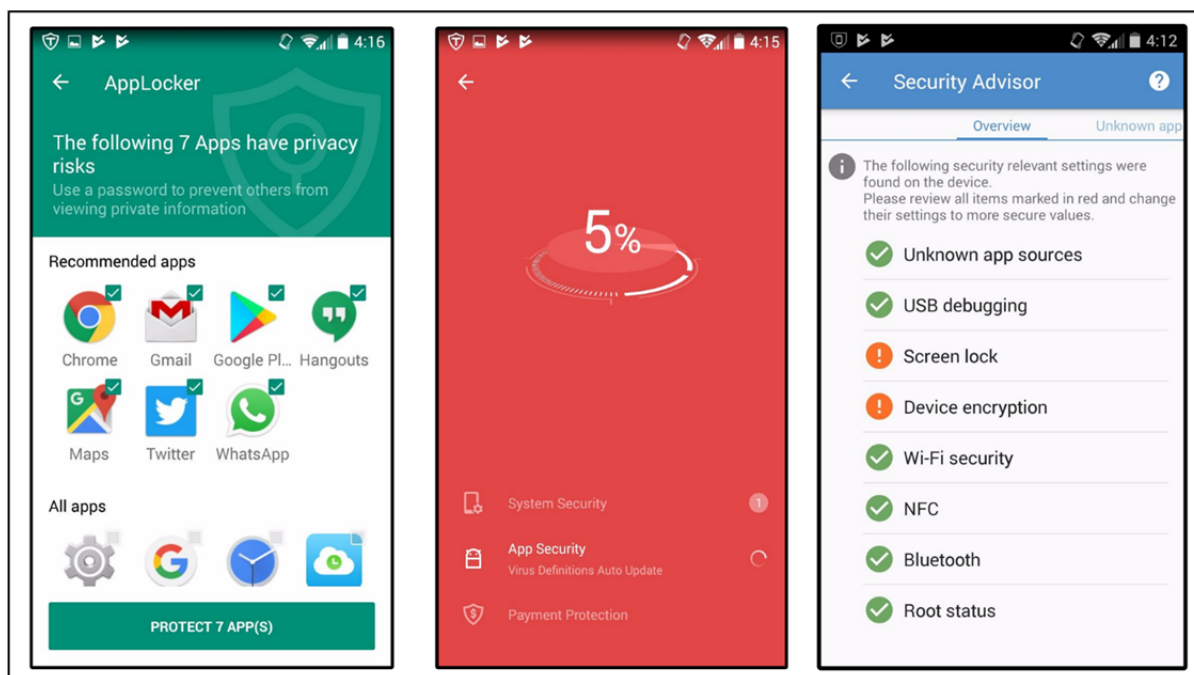- 360 Security
- Avira Antivirus Security
- AVL
- X-ray

Figure 17-02. TrustGo and Sophos Application

Hacking iOS

iPhone Operating System

The operating system developed for the iPhones by Apple.Inc is known as iOS. The is the another most popular operating system for mobile devices including iPhones, iPads, and iPods. The user interface in an iOS is based upon direct manipulation using multi-touch gestures. Major iOS versions are released annually. The current version, iOS 11, was released on September 19, 2017. iOS uses hardware-accelerated AES-256 encryption and other additional encryption to encrypt data. iOS also isolates the application from other applications. Applications are not allowed to access the other apps data.

Jailbreaking iOS

Jailbreaking is the concept of breaking the restriction "Jail." Jailbreaking is a form of rooting resulting in privilege escalation. iOS jailbreaking is the process of escalating the privileges on iOS devices intended to either remove or bypass the factory default restrictions on software by using kernel patches or device customization. Jailbreaking allows the root access to an iOS device which allows downloading unofficial applications. jailbreaking is popular for removing restrictions, installation of additional software, malware injection, and software piracy.

Types of Jailbreaking

Basically, iOS Jailbreaking is categorized into three types depending upon privilege levels, exploiting system vulnerability, a vulnerability in first and third bootloader, etc. Userland exploits and iBoot exploit can be patched by Apple.

1. *Userland Exploit*

A Userland exploit is a type of iOS jailbreaking which allow User-level access without escalating to about-level access.

2. *iBoot Exploit*

An iBoot exploit is a type of iOS jailbreaking which allow User-level access and boot-level access.

3. *Bootrom Exploit*

A bootrom exploit is a type of iOS jailbreaking which allow User-level access and boot-level access.

Jailbreaking Techniques

1. *Tethered Jailbreaking*

In Tethered Jailbreaking, when the iOS device is rebooted, it will no longer have a patched kernel. It may have stuck in a partially started state. With Tethered Jailbreaking, a computer is required to boot the device each time; i.e., the device is re-jailbroken each time. Using Jailbreaking tool, the device is started with the patched kernel.

2. *Semi-tethered Jailbreaking*

Semi-tethered Jailbreaking technique is another solution in between Tethered and Untethered Jailbreaking. Using this technique, when the device is a boot, it does not have patched kernel but able to complete the startup process and entertain normal functions. Any modification will require startup with patched kernel by jailbreaking tools.

3. *Untethered Jailbreaking*

In Untethered jailbreaking, Device is booted completely. While booting, Kernel will be patched without any requirement of the computer thus enabling the user to boot without a computer. This technique is harder to attempt.

Jailbreaking Tools

The following are some of the iOS jailbreaking tools:
- Pangu
- Redsnow
- Absinthe
- evasinon7
- GeekSnow
- Snowbreeze
- PwnageTool
- LimeRaln
- Blackraln

Hacking Windows Phone OS

Windows Phone (WP) is another operating system in the OS family, developed by Microsoft. Windows phone was the first to launch with Windows Phone 7. Windows 7 issue was fixed by later release 7.5 Mango which has very low hardware requirement of 800MHz CPU and 256 MB Ram. Windows 7 devices are not capable of upgrading to Windows 8 due to hardware limitations. Windows 8, 8.1 release in 2014 is eliminated by Windows 10 released in 2017.

Windows Phone

Windows Phone 8 is the second- generation Windows phone from Microsoft. Windows Phone 8 replaces the Windows CE based architecture that was used in Windows 7. Windows Phone 8 devices are manufactured not only by Microsoft but Nokia, HTC, Samsung, and Huawei as well. Windows Phone 8 is the first mobile OS launched by Microsoft using the Windows NT kernel. Improvement of the file system, drivers, security, media, and graphics is featured in windows phone 8. Windows Phone 8 is capable of supporting multi-core CPUs up to 64 cores. It is also capable of supporting 1280×720 and 1280×768 resolutions. Windows Phone 8 also supports native 128-bit Bit locker encryption and Secure Boot. Windows Phone 8 also supports NTFS due to this switch. Internet Explorer 10 is the default browser in windows 8 phones. Windows Phone 8 uses true multitasking, allowing developers to create apps that can run in the background and resume instantly.

Some other measure features of Windows Phone 8 include: -

- Native code support (C++)
- NFC
- Remote Device Management
- VoIP and Video Chat integration
- UEFI and Firmware over the air for Windows Phone updates
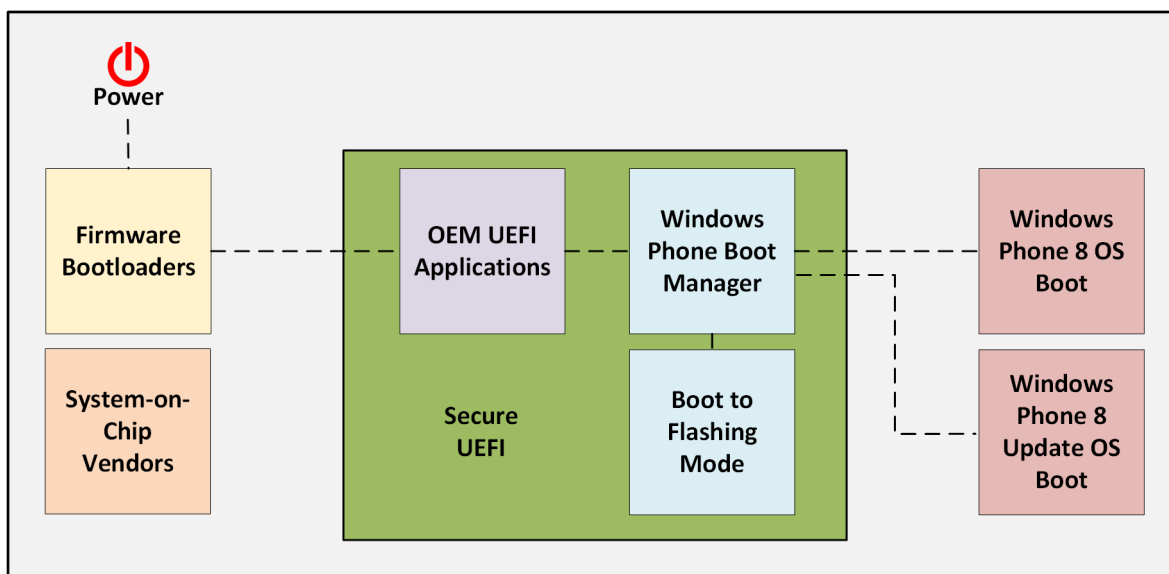- App Sandboxing

Figure 17-03. Windows 8 Secure Boot Process

Hacking BlackBerry

Blackberry is another smartphone company that is formerly known as Research-In-Motion (RIM) limited. Blackberry was considered as a most prominent and secure mobile phone. The operating system of Blackberry phone is known as Blackberry OS.

BlackBerry Operating System

Blackberry OS is the operating system of Blackberry phones. It provides multitasking with special input supports such as trackwheel, trackball, and most recently, the trackpad and touchscreen. Blackberry OS is best known for its features such as its native support for corporate emails, Java Based application framework, i.e., Java Micro Edition MIDP 1.0 and MIDP 2.0. Updates to the operating system may be automatically available from wireless carriers that support the BlackBerry over the air software loading (OTASL) service.

BlackBerry Attack Vectors

Malicious Code Signing

Malicious Code Signing is the process of obtaining a code-signing key from the code signing service. An attacker may create a malicious application with the help of code signing keys obtained by manipulating the information such as using anonymously using prepaid credit-cards and fake details and publish the malicious application on Blackberry App world. Blackberry App world is official application distribution service. User downloads this malicious application which directs the traffic to the attacker.

JAD File Exploit

Java Application Description (.jad) files contain attributes if Java application. These attributes include information and details about the application including URL to download the application. An attacker can trick to installed malicious .jad file on victim

device. This crafted .jad file with spoofed information can be installed by the user. A malicious application can also be crafted for a Denial-of-Service attack.

Mobile Device Management (MDM)

Mobile Device Management Concept

The basic purpose of implementing mobile device management (MDM) is deployment, maintenance, and monitoring of mobile devices that make up BYOD solution. Devices may include the laptops, smartphones, tablets, notebooks or any other electronic device that can be moved outside the corporate office to home or some public place and then gets connected to corporate office by some means. The following are some of the functions provided by MDM:

- Enforcing a device to be locked after certain login failures.
- Enforcement of strong password policy for all BYOD devices.
- MDM can detect any attempt of hacking BYOD devices and then limit the network access of these affected devices.
- Enforcing confidentiality by using encryption as per organization's policy.
- Administration and implementation of *Data Loss Prevention (DLP)* for BYOD devices. It helps to prevent any kind of data loss due to end user's carelessness.

MDM Deployment Methods

Generally, there are two types of MDM deployment, namely:

On-site MDM deployment: On-site/premises MDM deployment involves installation of MDM application on local servers inside the corporate data center or offices and its management is done by local staff available on the site.

The major advantage of On-site MDM is granular control over the management of the BYOD devices, which increases the security to some extent.
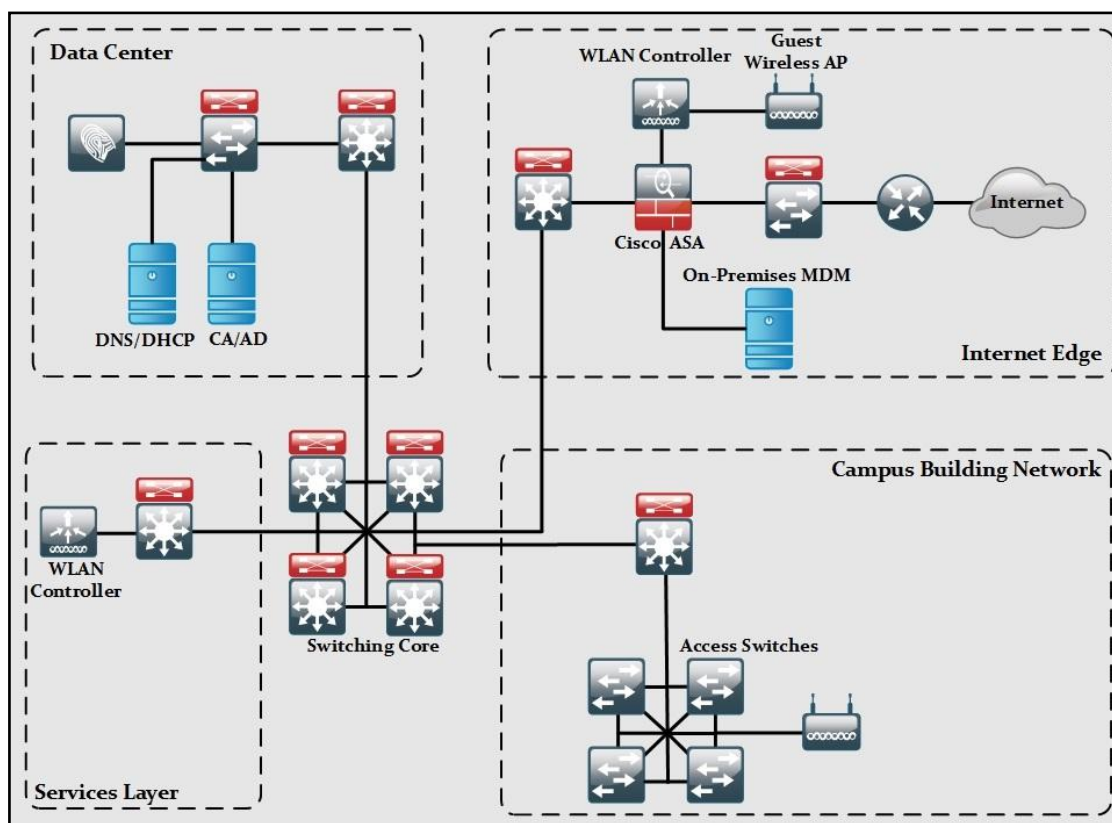
Figure 17-04. On-Premises MDM High-Level Deployment Architecture

The on-site/premises MDM solution is consists of the following architecture:

☐ **Data Center:** may include ISE, DHCP, and DNS servers to support certain services apart from distribution and core switches. ISE is used to provide the enforcement of organization's security policies. DNS/DHCP servers are used to provide the network connectivity. Similarly, CA and AD servers can also be used to provide access only to users with valid authentication credentials.

☐ **Internet Edge:** The basic purpose of this architecture is to provide connectivity to the public internet. This layer includes Cisco ASA firewall to filter and monitor all the traffic ingress and egress towards the public internet. Wireless LAN Controller (WLC) along with Access Points (APs) are also present in internet edge to support guest users. One of the key components at internet edge is On-premises MDM solution, which maintains policies and configuration settings of all BYOD devices, connected to the corporate network.

☐ **Services Layer:** This layer contains WLC for all the APs used by users within a corporate environment. Any other service required by corporate users like NTP and its supporting servers can be found in this section.

☐ **Core Layer:** Just like every other design, the core is the focal point of the whole network regarding routing of traffic in a corporate network environment.

☐ **Campus Building:** A distribution layer switch acts as ingress/egress point for all traffic in a campus building. Users can connect to campus building by connecting to access switches or wireless access points (APs).

Cloud-based MDM deployment: In this type of deployment, MDM application software is installed and maintained by some outsourced managed services provider.

One of the main advantages of this kind of setup is the less administrative load on customer's end as deployment and maintenance is totally the responsibility of service provider.

The cloud-based MDM deployment is consists of the following components, as depicted in the figure:

☐ **Data Center:** may include ISE, DHCP, and DNS servers to support certain services apart from distribution and core switches. ISE is used to provide the enforcement of organization's security policies. DNS/DHCP servers are used to provide the network connectivity. Similarly, CA and AD servers can also be used to provide access only to users with valid authentication credentials.

☐ **Internet edge: the** Basic purpose of this section is to provide connectivity to the public internet. This layer includes Cisco ASA firewall to filter and monitor all the traffic ingress and egress towards the public internet. Wireless LAN Controller (WLC) along with Access Points (APs) are also present in internet edge to support guest users.

☐ **WAN:** The WAN module in cloud-based MDM deployment provides MPLS VPN connectivity from branch office to corporate office, internet access from branch offices and connectivity to cloud-based MDM application software. Cloud-based MDM solution maintains policies and configuration settings of all BYOD devices connected to the corporate network.

☐ **WAN edge:** This component act as a focal point of all ingress/egress MPLS WAN traffic entering from and going to branch offices.
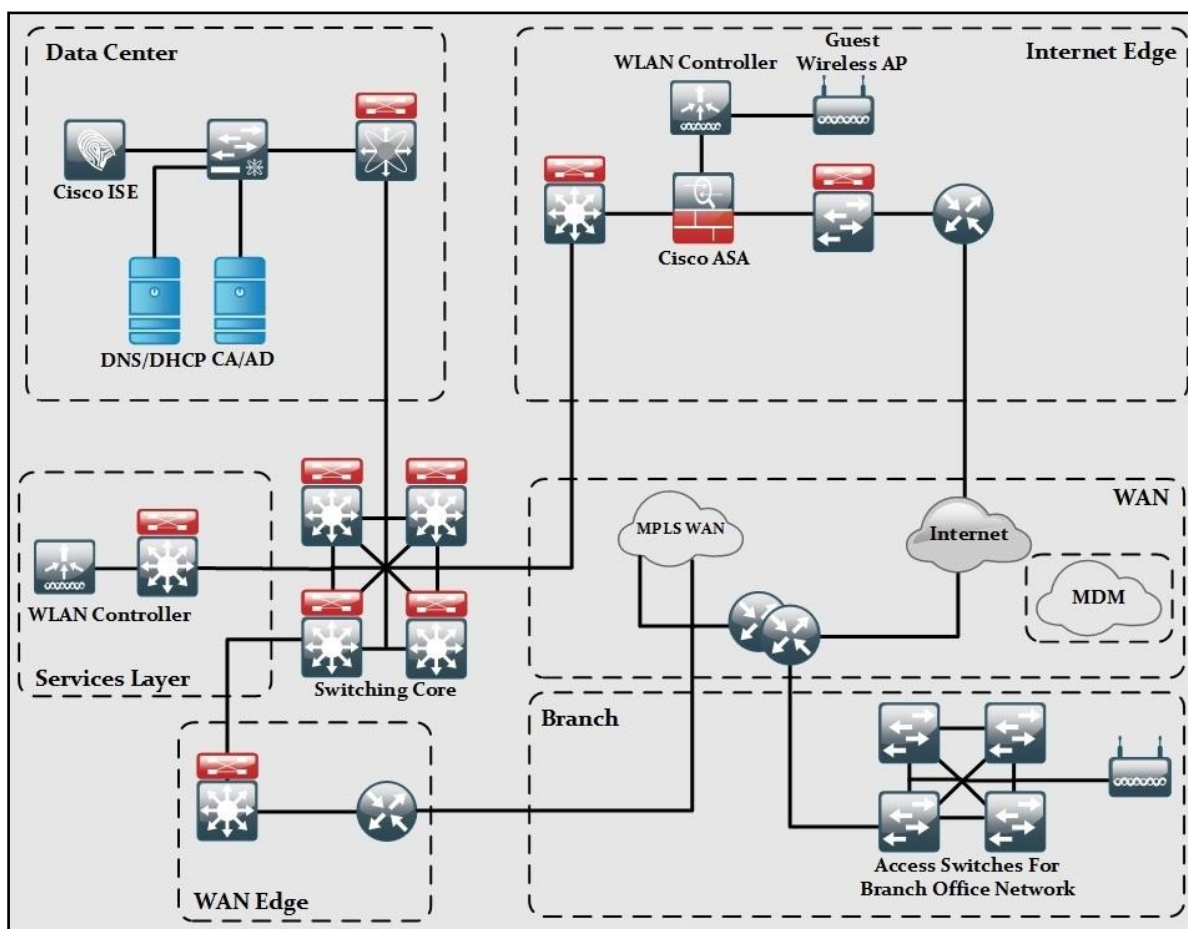
Figure 17-05. Cloud-Based MDM Deployment High-Level Architecture

☐ **Services:** This layer contains WLC for all the APs used by users within a corporate environment. Any other service required by corporate users like NTP and its supporting servers can also be found in this section.

☐ **Core Layer:** Just like every other design, the core is the focal point of the whole network regarding routing of traffic in a corporate network environment.

☐ **Branch offices:** This component is comprised of few routers acting as focal point of ingress and egress traffic out of branch offices. Users can connect to branch office network by connecting to access switches or wireless access points (APs).

Bring Your Own Device (BYOD)

In this section, the importance of *Bring Your Own Device (BYOD)* and its high-level architecture will be discussed. Apart from BYOD, one of its management approach known as *Mobile Device Management (MDM)* will also be discussed.

Although the concept of BYOD facilitates the end users in some way, it also brings new challenges for network engineers and designers. The constant challenge that is faced by today's network designers to provide seamless connectivity while maintaining a good

security posture of an organization. Organizations security policies must constantly be reviewed to make sure that bringing any outside device over the corporate network will not result in theft and comprise of organization's digital assets.

Some of the reasons that demand BYOD solutions to be implemented in an organization are:

- **A wide variety of consumer devices:** In the past, we were used to having only PCs constantly sitting on the table, and wired connection was the only preferred way of communication. In the 21st century, not only higher data rates have resulted in countless opportunities, but the variants of devices on the internet are also increased. If we look around, we see mobile devices like smartphones, tablets and even laptops which are constantly communicating with each other over some wired or wireless network. Employees may connect their smartphones to corporate networks during working hours and to the internet when they move to a home or some café. Such situations demand BYOD solution to be implemented in the corporate environment to stay safe from any kind of theft.

- **No, fix a time for Work:** In the past, we were used to following a strict 8-hour working environment. Now, we work during lunch, and even our working rosters get updated on weekly bases. Sometimes, we even work during the night to meet the deadlines.

- **Connecting to corporate from anywhere:** Employees also demand to connect to the corporate network anytime either they are at home or in some café. The emergence of wireless networks and mobile networks like 3G/4G also enables them to connect even from the most remote location on earth.

BYOD Architecture Framework

There are rules in implementing BYOD in an organization. It depends on the company's policy about how flexible they are in accepting and enabling their employees to bring along different types of devices. Introducing BYOD in an organization may also result in implementing or deploying new software and hardware features to cater the security aspects of BYOD.

The Cisco BYOD framework is based on *Cisco Borderless Network Architecture,* and it tries to implement *best common practices (BCP)* in designing branch office, home office, and campus area networks.

This figure shows the Cisco BYOD architecture with a short explanation of each component in the coming section.
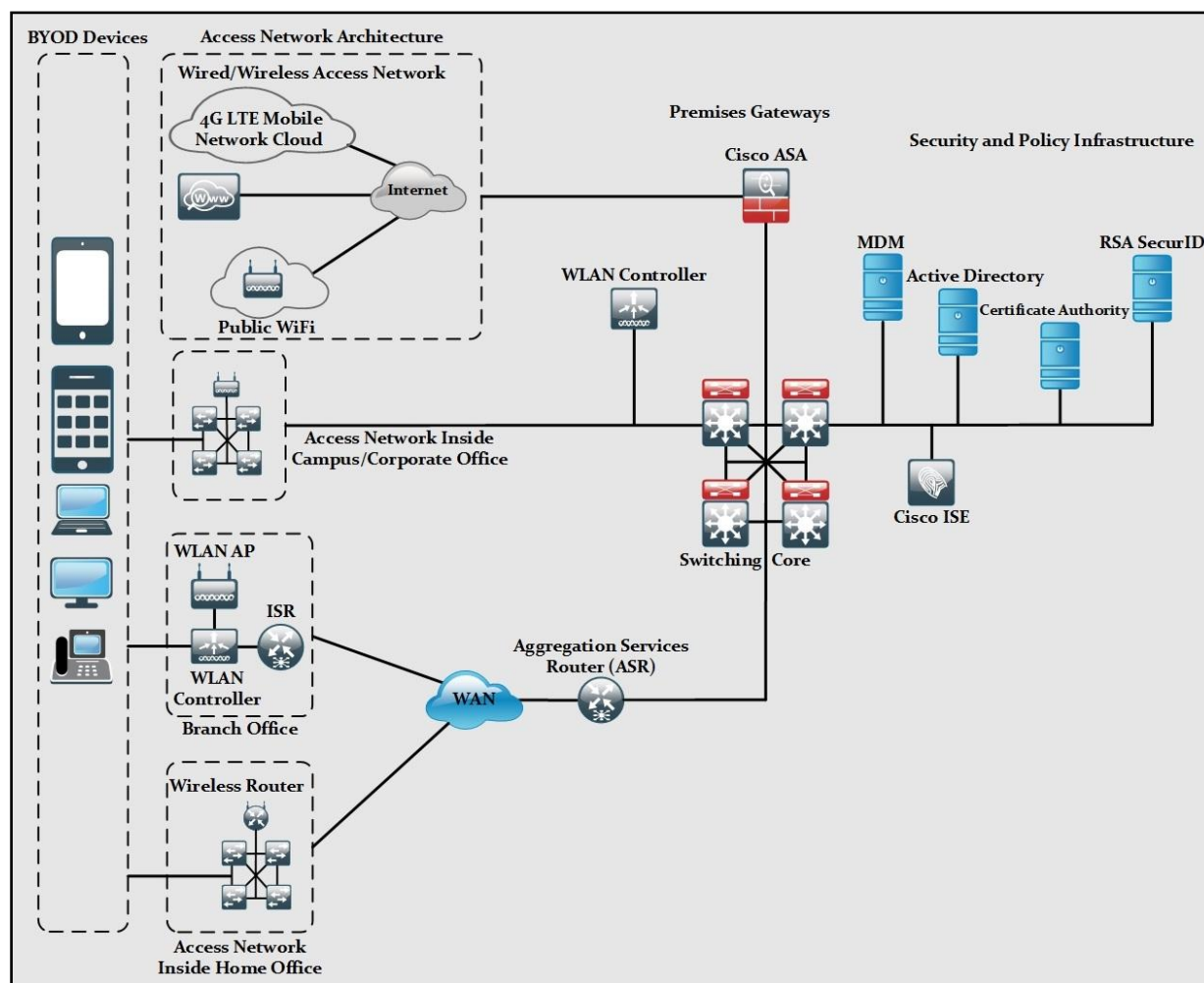
Figure 17-06. BYOD high-level architecture

BYOD Devices: These endpoint devices are required to access the corporate network for daily business need. BYOD devices may include both corporate and personally owned devices, regardless of their physical location. At day, they may be at the corporate office and at night, they may be some café or food restraint. Common BYOD devices include smartphones, laptops, etc.

Wireless Access Points (AP): Cisco wireless access points (APs) provide wireless connectivity to the corporate network for above defined BYOD devices. Access points are installed physically at the campus, branch office, or even at home office to facilitate the employees.

Wireless LAN Controllers: WLAN controllers provides centralized management and monitoring of Cisco WLAN solution. WLAN is integrated with *Cisco Identity Service Engine* to enforce the authorization and authentication of BYOD end-point devices.

Identity Service Engine (ISE): ISE is one of the most critical elements in Cisco BYOD architecture as it implements Authentication, Authorization, and Accounting on BYOD end-point devices.

Cisco AnyConnect Secure Mobility Client: Cisco AnyConnect Client software provides connectivity to the corporate network for end users. Its uses 802.1x features to provide access to campus, office or home office network. When end users need to connect to the public internet, AnyConnect uses VPN connection to make sure the confidentiality of corporate data.

Integrated Services Router (ISR): Cisco ISR routers are preferred in BYOD architecture for proving WAN and internet access for branch and home office networks. They are also used to provide VPN connectivity for mobile BYOD devices within an organization.

Aggregation Services Router (ASR): Cisco ASR routers provide WAN and internet access for corporate and campus networks. They also act as aggregation points for connections coming from the branch and home office to the corporate networks of Cisco BYOD solution.

Cloud Web Security (CWS): Cisco Cloud Web Security provides enhanced security for all BYOD devices which access the internet using public hotspots and 3G/4G networks.

Adaptive Security Appliance (ASA): Cisco ASA provides the standard security solutions at the internet edge of campus, branch and home office networks within BYOD architecture. Apart from integrating IPS/IDS module within itself, ASA also acts as the termination point of VPN connections made by *Cisco AnyConnect Client* software over the public internet to facilitate the BYOD devices.

RSA SecurID: RSA SecurID generates a one-time password (OTP) for BYOD devices that need to access the network applications that require OTP.

Active Directory: Active Directory provides centralized command and control of domain users, computers, and network printers. It restricts the access to network resources only to the defined users and computers.

Certificate Authority: Certificate authority can be used to allow access to corporate network to only those BYOD devices which have a valid corporate certificate installed on them. All those devices without certificate may be given no access to the corporate network but limited internet connectivity as per defined in the corporate policy.

Mind Map
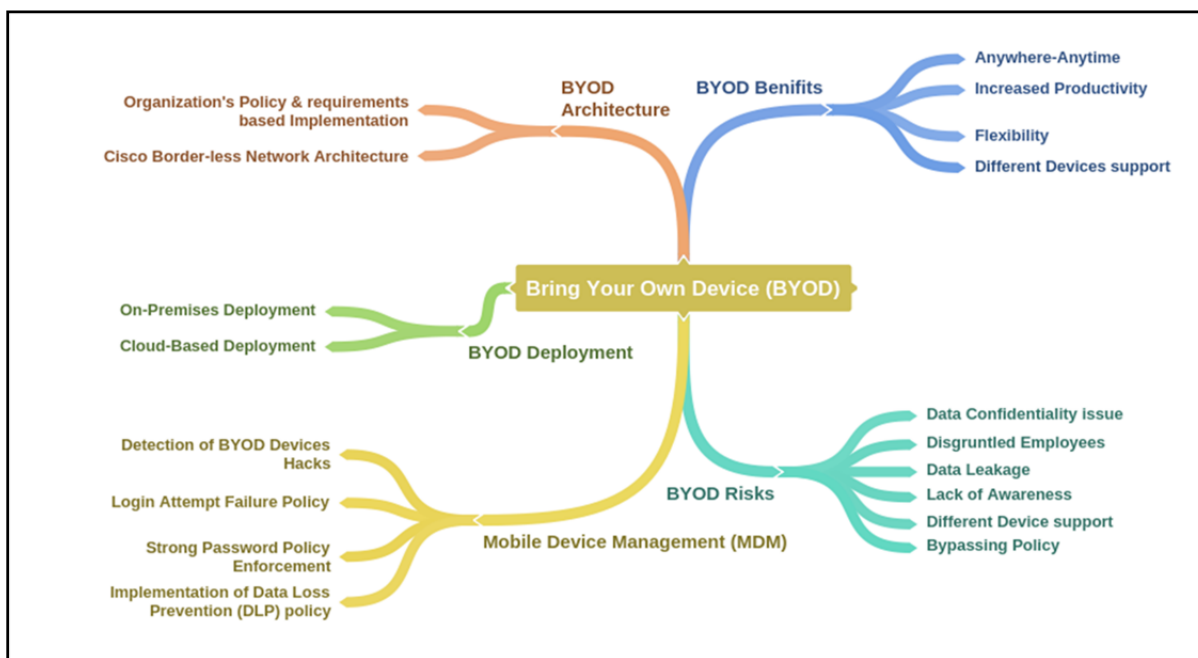
Mobile Security Guidelines

There are a lot of features in a smartphone, a number of techniques and methods which can be followed in order to avoid any trouble while using mobile phones. Apart from this built-in feature and precautions, several tools are also available on every official application stores to provide user better security of their devices. Some of the beneficial guidelines to secure your mobile phone are as follows: -

- Avoid auto-upload of files and photos
- Perform security assessment of applications
- Turn Bluetooth off
- Allow only necessary GPS-enabled applications
- Do not connect to open networks or public networks unless it is necessary
- Install applications from trusted or official stores
- Configure string passwords
- Use Mobile Device Management MDM softwares
- Use Remote Wipe Services
- Update Operating Systems
- Do not allow rooting / jailbreaking
- Encrypt your phone
- Periodic backup
- Filter emails
- Configure application certification rules
- Configure mobile device policies

- Configure auto-Lock