WILLIAM STALLINGS

EFFECTIVE CYBERSECURITY

A Guide to Using Best Practices and Standards

Effective Cybersecurity

Use of Untrusted Networks

If a mobile device is used on premises, it can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from the Internet to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks. Thus, a security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy.

Use of Applications Created by Unknown Parties

By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software. An organization has several options for dealing with this threat, as described later in this chapter.

Interaction with Other Systems

A common feature on smartphones and tablets is the ability to automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage. Unless an organization has control of all the devices involved in synchronization, there is a considerable risk that the organization's data will be stored in an unsecured location, and there is also a risk of malware introduction.

Use of Untrusted Content

Mobile devices may access and use content that other computing devices do not encounter. An example is the quick response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. A QR code translates to a URL, and a malicious QR code could direct mobile devices to malicious websites.

Use of Location Services

The GPS capability on mobile devices can be used to maintain knowledge of the physical location of the device. While this feature might be useful to an organization as part of a presence service, it creates security risks. An attacker can use the location information to determine where the device and user are located, which may be helpful to the attacker.

Mobile Device Security Strategy

The recent DHS report *Study on Mobile Device Security* [DNS17] groups security threats and defenses into five primary components of the mobile ecosystem and their associated attack surface: the mobile device technology stack, mobile applications, mobile network protocols and services, physical access to the device, and enterprise mobile infrastructure (see Table 7.5). This is a useful way of organizing the security strategy for mobile devices. The following sections examine these five primary components in more detail.

rooting

The act of removing a restricted mode of operation. For example, rooting may enable content with digital rights to be used on any computer, or it may allow enhanced third-party operating systems or applications to be used on a mobile device. While rooting is the term used for Android devices, **jailbreaking** is the equivalent term used for Apple's devices.

sideloading

The act of downloading an app to a device without going through the official app store, via links or websites. While enterprises often use sideloading as a method for distributing homegrown apps, malicious actors also use sideloading (via enterprise certificates in many cases bought on the black market) to distribute their malware.

TABLE 7.5 Common Mobile Device Threats

Mobile Ecosystem Element	Threats
Mobile device technology stack	Delays in security updates Zero-day exploits against software and firmware, particularly the baseband Bootloader exploitation **Jailbreaking/rooting** **Sideloading** Supply chain compromise Trusted Execution Environment (Android) or Secure Enclave (iOS) exploitation Compromised cloud system credentials
Mobile applications	Malware (including backdoors, ransomware, and privilege escalation) Vulnerable third-party libraries Exploitation of vulnerable apps Insecure app development practices Exploitation of a public mobile app store
Mobile networks	Rogue cellular base stations and Wi-Fi access points Man-in-the-middle attacks on communications Data/voice eavesdropping Data/voice manipulation Device and identity tracking DoS/jamming

Mobile Ecosystem Element	Threats
Device physical systems	Loss or theft of a mobile device Physical tampering Malicious charging station
Mobile enterprise	Compromised EMM/MDM system or admin credentials Compromised enterprise mobile app store or developer credentials Bypassed app vetting

Mobile Device Technology Stack

A number of organizations supply mobile devices for employee use and preconfigure those devices to conform to the enterprise security policy. However, many organizations find it convenient or even necessary to adopt a bring your own device (BYOD) policy that allows the personal mobile devices of employees to have access to corporate resources. IT managers should be able to inspect each device before allowing network access. IT should establish configuration guidelines for operating systems and applications. For example, rooted or jailbroken devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage. Whether a device is owned by the organization or an employee, the organization should configure the device with security controls, including taking the following measures:

- Enable auto-lock, which causes the device to lock if it has not been used for a given amount of time, requiring the user to reenter a PIN or a password to reactivate the device.
- Enable password or PIN protection. The PIN or password is needed to unlock the device. In addition, it can be configured so that email and other data on the device are encrypted and can be retrieved only with the PIN or password.
- Avoid using auto-complete features that remember usernames or passwords.
- Enable remote wipe.
- Ensure that Transport Layer Security/Secure Sockets Layer (TLS/SSL) protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either prohibit users from storing sensitive data on mobile devices or require users to encrypt sensitive data.

- Ensure that IT staff have the ability to remotely access devices, wipe devices of all data, and disable devices in the event of loss or theft.
- Possibly prohibit installation of third-party applications, implement whitelisting to prohibit installation of all unapproved applications, or implement a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device. Any application that is on an approved list should be accompanied by a digital signature and a public-key certificate from an approved authority.
- Implement and enforce restrictions on what devices can synchronize and on the use of cloud-based storage.
- To deal with the threat of untrusted content, disable camera use on corporate mobile devices and train personnel on the risks inherent in untrusted content.
- To counter the threat of malicious use of location services, ensure that such services are disabled on all mobile devices.

Mobile Applications

Millions of apps are available from the two major stores, the Apple App Store and Google Play, and millions more can be obtained from other public app stores. The reliability and security of apps may vary widely, and the vetting process may be opaque or insufficiently robust, particularly for apps from outside the two major stores.

Regardless of the source of an app, an enterprise should perform its own evaluation of the security of the app to determine if it conforms to the organization's security requirements. The requirements should specify how data used by the app should be secured, the environment in which the app will be deployed, and the acceptable level of risk for the app.

Figure 7.6 illustrates *app vetting*, the process of evaluating and either approving or rejecting apps within an organization, which is described in NIST SP 800-163, *Vetting the Security of Mobile Applications*. The vetting process begins when an app is acquired from a public or enterprise store or submitted by an in-house or third-party developer. An administrator is a member of the organization who is responsible for deploying, maintaining, and securing the organization's mobile devices as well as ensuring that deployed devices and their installed apps conform to the organization's security requirements. The administrator submits the app to an app testing facility in the organization that employs automated and/or human analyzers to evaluate the security characteristics of apps, including searching for malware, identifying vulnerabilities, and assessing risks. The resulting security report and risk assessment are conveyed to an auditor or auditors.

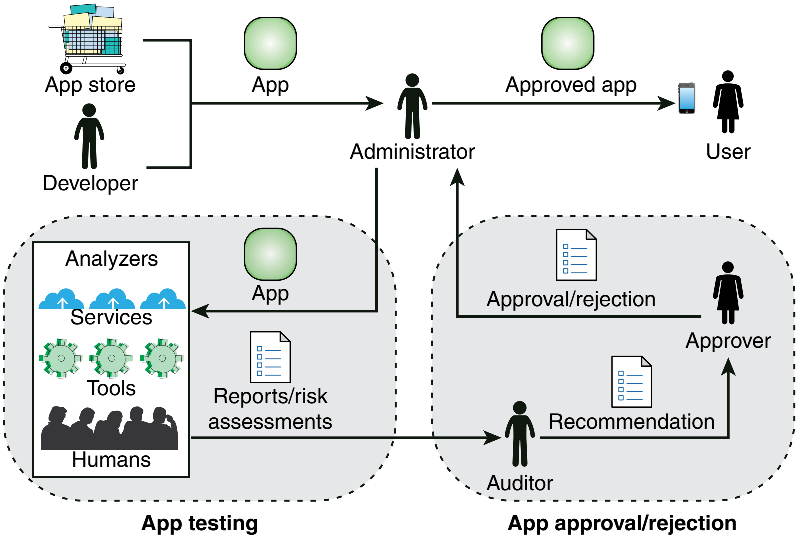

FIGURE 7.6 App Vetting Process

AppVet
http://appvet.github.io/appvet/

The role of the auditor is to inspect reports and risk assessments from one or more analyzers to ensure that an app meets the security requirements of the organization. The auditor also evaluates additional criteria to determine if the app violates any organization-specific security requirements that could not be ascertained by the analyzers. The auditor then makes a recommendation to someone in the organization who has the authority to approve or reject an app for deployment on mobile devices. If the approver approves an app, the administrator can then deploy the app on the organization's mobile devices.

NIST has developed a tool, AppVet, that provides automated management support for app testing and app approval/rejection activities

Mobile Network Protocols and Services

Traffic security is based on the usual mechanisms for encryption and authentication. All traffic should be encrypted and travel by secure means, such as SSL or IP Security (IPsec). **Virtual private networks (VPNs)** can be configured so that all traffic between a mobile device and the organization's network is via a VPN.

virtual private network (VPN)

A restricted-use, logical (that is, artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (that is, real) network (for example, the Internet), often using encryption (located at hosts or gateways) and authentication. The endpoints of the virtual network are said to be tunneled through the larger network.

A strong authentication protocol should be used to limit access from the device to the resources of the organization. Often, a mobile device has a single device-specific authenticator because it is assumed that the device has only one user. A preferable strategy is to have a two-layer authentication mechanism, which involves authenticating the device and also authenticating the user of the device.

The organization should have security mechanisms to protect the network from unauthorized access. The security strategy can also include firewall policies specific to mobile device traffic. Firewall policies can limit the scope of data and application access for all mobile devices. Similarly, intrusion detection and intrusion prevention systems can be configured with tighter rules for mobile device traffic.

Physical Access to the Device

The small, portable nature of mobile devices increases their susceptibility to physical-based threats. The DHS's *Study on Mobile Device Security* [DHS17] lists the following as common threats resulting from gaining physical access to a device:

- Substitution of a compromised Bluetooth headset to facilitate eavesdropping
- Replacement of a SIM card to facilitate illegal activity such as identity fraud or theft of services
- Brute-force attacks on a stolen device
- **Side-channel attacks** to obtain cryptographic private keys
- Installation of malicious apps via USB, an infected computer, or a charging station without the user's knowledge

side-channel attack

An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.

The DHS report recommends the following defenses [DHS17]:

- Ensure that devices are enterprise managed so that the organization can enforce security policies, monitor device state, and remotely track or wipe lost or stolen devices.
- Ensure that the device's **screen lock** is enabled. The lock should be enabled with an appropriately strong password.

screen lock

A security feature for computers and mobile devices that helps prevent unauthorized access to the device. A screen lock requires the user to perform a specific action, such as entering a PIN code or presenting a fingerprint, to gain access to the device.

Enterprise Mobile Infrastructure

Attacks on mobile devices with enterprise access can spread to other enterprise systems. As shown in Figure 7.5, these enterprise threats are in two broad areas: attacks related to an enterprise app store and attacks on the EMM system.