Mobile Device Management

1. Introduction

This document introduces security risks with mobile devices, guidelines for managing the security of mobile devices in the Enterprise, strategies for mitigating threats of mobile devices in the Enterprise, challenges of Bring Your Own Device (BYOD) program, and policies to address the security risks and challenges of BYOD.

2. Security Risks with Mobile Devices

The security risks associated with using mobile devices include the following:

1) Device hardware and OS vulnerabilities

Mobile device and Operating systems can have vulnerabilities susceptible to security breaches by hackers as well as malware attacks. Such attacks can cause unauthorized data access by hackers, degrade or shut down system performance. According to Marble’s Mobile Security Lab, the Apple iOS and Android mobile operating systems are comparably risky though they expose users to different threats [1]. A team of researchers recently discovered three serious vulnerabilities in cross-app resource sharing protocols on Apple's desktop and mobile platforms which were used to steal data such as passwords and secret authentication keys [2].

The risk of jailbreaking iOS and the risk of rooting Android devices are similar[1]. Jailbreaking iOS is a hacking process that removes hardware restrictions on iOS, permitting root access to the iOS file system and manager, and allowing the download of applications unavailable through office Apple App Store [3, 4]. Rooting an android device gives the hacker access to the root, i.e., administrative permissions [5].

2) Mobile malware

According to CYREN’s security report for 2013, Android operating system had on average 5,768 malware attacks daily over a 6-month period. [6] There are a variety of mobile malware. Examples of mobile malware include: (1) Trojans that send short message service (SMS) messages to premium rate number; (2) background calling applications that make long distance calls; (3) key logging applications; (4) worms that infect the devices and spread to other devices listed in the address book; (5)spyware that monitors device communication. Spyware could be remotely controlled by cyber criminals [7]. When hacker compromises a mobile device, the hacker can illegally watch and impersonate the user, participate in dangerous botnet activities, capture the user’s personal data, and steal money[8].

3) Mobile application security risks

Due to poor implementation, various security vulnerabilities exist in legitimate mobile apps. Common vulnerabilities in mobile apps include sensitive data leakage, unsafe sensitive data storage, unsafe sensitive data transmission, hardcoded passwords/keys, etc. [9]. Zhou, Y. and Jing, X. found that two types of vulnerabilities – passive content leak and content pollution exist in large number of apps on various android markets [10]. The passive content leak vulnerability refers to leaking private in-app information to any other apps without any
dangerous permission. The content pollution vulnerability refers to manipulating security-sensitive in-app settings or configurations that may cause undesirable side effects such as blocking all incoming phone calls or SMS messages. Recently, Jin X., et. al at Syracuse University discovered that HTML5-based mobile apps are at the risk of malicious code injection – Cross Device Scripting Attacks [11, 12].

4) Using unsecure connection
Mobile devices connected to insecure network such as free Wi-Fi network at an airport or a hotel are susceptible to eavesdropping and man-in-the-middle (MITM) attacks [7].

5) Device lost or stolen
The portability of mobile device leads to the very common incidence of loss or theft of mobile devices. The loss or theft of mobile devices jeopardize the device users’ person data, such as pre-connected email accounts, calendar events, personal photos, social media accounts, contacts, etc. The loss of a mobile device used for work related functions can also expose intellectual property, sensitive employee and customer information, and other corporate assets [7].

3. Guidelines for managing the security of mobile devices in the Enterprise

National Institute of Standards and Technology (NIST) published “Guidelines for Managing the Security of Mobile Devices in the Enterprise” [13]. The guidelines are described below:

1) Organizations should have a mobile device security policy that defines
   • the types of resources in the organization that may be accessed via mobile devices.
   • the types of mobile devices that are permitted to access organization’s resources.
   • the degree of access of different classes of mobile devices, such as organization issued devices and personally owned devices.
   • the requirements for mobile device management technologies such as the administration of the organization’s centralized mobile device management servers, the updating of policies in the servers, etc.

2) System threat models for mobile devices and resources accessed through the mobile devices should be developed. This involves identifying resources, feasible threats, vulnerabilities, analyzing attack likelihood and impacts, and determining where security controls need to be improved or added.

3) Organizations should consider the services provided by mobile device solutions, and select those needed for their environment. Mobile device solutions provide the following categories of services:
   • General policy. Services that enforce enterprise security policies on the mobile device, such as restricting access to hardware and software, managing wireless network interfaces, detecting and reporting policy violation.
   • Data communication and storage. Services that support strongly encrypted data communication and storage, device wiping, and wiping device remotely.
   • User and device authentication. Services that include device/user authentication, resetting forgotten passwords remotely, automatically locking idle devices, and remotely locking devices.
• Applications. Services that restrict the app store that may be used, the applications that may be installed, permissions assigned to the applications, installing and updating applications, the use of synchronization services, etc. This category of services also include verifying digital signature on applications, and distributing the organization’s applications from a dedicated mobile application store.

4) A pilot mobile device solution needs to be implemented and tested before putting the solution to production.

5) Organization issued mobile device should be fully secured before being used

6) Mobile device security should be regularly maintained. Maintenance processes include the following:
  • checking for and deploying upgrades and patches,
  • ensuring that the clocks of mobile device infrastructure components are synced to a common time source,
  • reconfiguring access control features as needed,
  • detecting and documenting anomalies,
  • keeping an active inventory of mobile devices and their users and applications,
  • revoking access to or deleting an application,
  • wiping devices before reissuing them to other users
  • periodically perform assessments to confirm what mobile device policies, processes, and procedures are being followed properly

4. Threats of Mobile Devices and Mitigation Strategies

Threats and vulnerabilities in the Enterprise and mitigation strategies are listed in Table 1 [13].

<table>
<thead>
<tr>
<th>Threats and Vulnerabilities</th>
<th>Mitigation Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of physical security control</td>
<td>• Require authentication before gaining access to the device or organization’s resources accessible through the device</td>
</tr>
<tr>
<td>• lost or stolen devices</td>
<td>• Encrypt the device’s storage or not store sensitive data on mobile devices</td>
</tr>
<tr>
<td>• Malicious parties attempt to recover sensitive data from the</td>
<td>• User training and awareness to reduce insecure physical security practices</td>
</tr>
<tr>
<td>acquired mobile device, or access organization’s remote</td>
<td>• Restrict or prohibit BYOD devices</td>
</tr>
<tr>
<td>resources using the device</td>
<td>• Fully secure organization-issued devices, monitor and address deviations from secure state</td>
</tr>
<tr>
<td></td>
<td>• For BYOD devices, run organization’s software in a secure, isolated sandbox on the mobile device, or use device integrity scanning applications</td>
</tr>
<tr>
<td>Use of untrusted mobile devices</td>
<td>• Use VPN</td>
</tr>
<tr>
<td>• Restriction on security, OS, etc. could be bypassed through</td>
<td>• Use mutual authentication mechanism to verify the identities of both endpoints before transmitting data</td>
</tr>
<tr>
<td>jailbreaking and rooting</td>
<td>• Prohibit use of insecure Wi-Fi networks</td>
</tr>
<tr>
<td>Use of untrusted network</td>
<td>• Use VPN</td>
</tr>
<tr>
<td>• Eavesdropping</td>
<td>• Use mutual authentication mechanism to verify the identities of both endpoints before transmitting data</td>
</tr>
<tr>
<td>• Man-in-the-Middle attacks</td>
<td>• Prohibit use of insecure Wi-Fi networks</td>
</tr>
<tr>
<td>Use of untrusted applications</td>
<td>Disable network interfaces that are not needed</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>• User can download untrusted third party mobile device application</td>
<td>• Prohibit all installation of third-party applications</td>
</tr>
<tr>
<td>• User can access untrusted web-based applications through the device’s built-in browsers</td>
<td>• allow installation of approved applications only</td>
</tr>
<tr>
<td></td>
<td>• verify that applications only receive the necessary permissions</td>
</tr>
<tr>
<td></td>
<td>• implement a secure sandbox that isolates the organization’s data and applications from all other data and applications on the mobile device</td>
</tr>
<tr>
<td></td>
<td>• perform a risk assessment on each third-party application before permitting its use on organization’s mobile device</td>
</tr>
<tr>
<td></td>
<td>• prohibit or restrict browser access</td>
</tr>
<tr>
<td></td>
<td>• force mobile device traffic through secure web gateways, HTTP proxy servers, or other intermediate devices to assess URLs before allowing access</td>
</tr>
<tr>
<td></td>
<td>• Use a separate browser within a secure sandbox for browser-based access related to organization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interact with other systems</th>
<th>Implement security controls on organization-issued mobile device restricting what devices it can synchronize with</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Connect a personally-owned mobile device to an organization-issued laptop</td>
<td>• Implement security controls on organization-issued computer restricting the connection of mobile devices</td>
</tr>
<tr>
<td>• Connect an organization-issued mobile device to personally-owned laptop</td>
<td>• block use of remote backup services or configure the mobile devices not to use such services</td>
</tr>
<tr>
<td>• Connect an organization-issued mobile device to a remote backup service</td>
<td>• Do not connect mobile devices to unknown charging devices</td>
</tr>
<tr>
<td>• Connect any mobile device to an untrusted charging station</td>
<td>• Prevent mobile devices to exchange data with each other through logical or physical means</td>
</tr>
<tr>
<td>• Risk of storing organization’s data to unsecured location, and malware transmission</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use of untrusted content</th>
<th>Educate users not to access untrusted content with any mobile devices used for work</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Malicious QR codes could direct mobile devices to malicious websites</td>
<td>• Have applications (e.g., QR readers) display the unobfuscated content (e.g., the URL) and allow users to accept or reject it before proceeding</td>
</tr>
<tr>
<td></td>
<td>• Use secure web gateways, HTTP proxy servers, etc. to validate URLs before allowing access</td>
</tr>
<tr>
<td>Use of location services</td>
<td>• Restrict peripheral use on mobile devices (e.g., disabling camera use) to prevent QR code reading</td>
</tr>
<tr>
<td></td>
<td>• Disable location service</td>
</tr>
<tr>
<td>• Attackers could correlate location information with other sources about who the user associates with and the kinds of activities they perform in particular locations</td>
<td>• Prohibit use of location services for particular applications such as social networking or photo applications</td>
</tr>
<tr>
<td></td>
<td>• Turn off location services when in sensitive areas</td>
</tr>
<tr>
<td></td>
<td>• Opt out of Internet connection location services whenever possible</td>
</tr>
</tbody>
</table>

### 4. Bring Your Own Device (BYOD)

BYOD refers to the strategy that allows people to use their own devices for work [14]. The benefits of BYOD include [15]:

- **Cost savings.** The cost of organization-issued devices could be reduced.
- **Productivity gains.** Employees can work more effectively outside of the office, are more likely to spend more time on work related activities.
- **Operational flexibility.** Employees can carry out their work function away from their desk.
- **Employee satisfaction.** Allowing employees to use devices that they enjoy using increases the satisfaction they derive from job.

In addition to the security risks discussed in the above sections, BYOD has the following challenges:

- **Privacy issues.** Mobile Device Management (MDM) system used to manage and monitor BYODs may require accessing and/or processing of personal data. This may raise concerns on employees’ data privacy rights. Employee consent should be obtained before MDM is deployed to manage employee owned devices [15]. Employee’s personal data may be lost if device data needs to be wiped.
- **Cost issues.** Organizations need to decide whether there is any reimbursement for the employee owned devices and data/voice usage. Additional cost for implementing MDM and for handling the support of BYOD users may incur. Organizations also need to assess tax implications for reimbursement [16].

There are three technological approaches to implementing BYOD program [16]:

- **Virtualization:** provide remote access to computing resources. No data is stored on the personal devices, and no organization’s application is processed on personal devices.
- **Walled garden:** Organization’s data or application processing are contained in a secure application that is segregated from personal data;
- **Limited separation:** Organization’s data and/or application processing are comingleed with personal data and/or application processing, but policies are enacted to ensure minimum security controls.
Enabling completely device-independent computing through desktop virtualization, accessed through a SSL VPN and supplemented by a secure file sync and sharing service is recommended as the ideal approach to BYOD [14].

5. Policies for Addressing BYOD Security and Privacy Risks
Organizations need to have policies that address BYOD security and privacy risks. Policies could include [38] the following:

- Acceptable use policy for email, Internet, mobile device, etc.
- Security policies such as mobile, encryption, password, anti-virus, etc.
- Wireless access policy
- Remote access policy
- Remote working policies
- Privacy policies
- Employee code of conduct
- Incident response policies

Typically, policies for BYOD should address the following [14]:

- Eligibility. Specify who in the organization is allowed to use personal devices
- Allowed devices. Determine and mandate minimum specifications for OS and application support, performance and other device-specific criteria. Desktop virtualization eliminates these considerations.
- Service availability. The specific services the organization wants to make available on BYO devices
- Rollout. Provide guidance to employees when rolling out BYOD. Teach employees about responsibilities like how data is allowed to be accessed, used, and stored, etc.
- Cost sharing. Defines whether the organization will provide full or partial stipends towards the personal devices. Also define who will pay for network access outside the organization firewall.
- Security and compliance. Use desktop virtualization instead of installing apps directly on the device. Disable printing or access to client-side storage. Ensure antivirus/antimalware is installed and updated. Use network access control (NAC) to authenticate people connecting to the network and check for updated antivirus and security patches, or allow access to virtualized desktop using VPN, encryption, mechanism to terminate access to data and apps from BYO device if device is lost or stolen, or employee leaves the organization.
- Device support and maintenance. Specify how various support and maintenance tasks will be addressed and paid for.

The BYOD Working Group has assembled 5 sample policies which could help IT leaders to develop policies for a BYOD program [16]. These sample policies are:

- Policy and guidelines for government-provided mobile device usage
- Bring your own device – policy and rules of behavior
- Mobile information technology device policy
- Wireless communication reimbursement program
- Portable wireless network access device policy
The BYOD Working Group has also developed three case studies to highlight the successful efforts of BYOD programs at several government agencies [16].

References:


