Enterprise Mobility - Mobile Device Security

Story Context: TechnoLabs has been focusing and offers Enterprise Mobility as one of its solution offering. No can deny the fact that mobile computing can bring difference to the business visa-vie employees and customers. But the concern remains the data security!! How one can achieve clear demarcation on what constitutes official and how we can protect it even if the Mobile is lost. TechnoLabs is evaluating the mobile original equipment manufacturers (OEMs) so that we can recommend right mobile platform to our enterprise customers.

PS: Please validate if your Enterprise Security provides the Solution points mentioned under each section.

8-2-293/82/A-120, Road No.70, Jubilee Hills, Hyderabad – 500033

Mobile – Enterprise Mobility Security Considerations

a. Client Side Data storage and Protection

Client Side data stored is the data at rest (or in motion) and is always susceptible to attacks. Mobile applications can use plethora of mechanisms to store and retrieve data from the mobile and tablet devices. Especially the applications which are downloaded from public sources (including unknown) and run on Client side resides on user's device. The data stored might be prone to get exposed to various security threats for both users and enterprises. Common way to fall prey to get data exposed if the device is lost. Sensitive data might get accessed by notorious applications through application logs, debug information, cached application messages and transaction histories. Enterprises might not be in control of the users using personal devices under BYOD policy from downloading the unwanted applications from the public stores. The challenge for IT management is to deploy BYOD without compromising security at the same time. So highest priority is to deploy tight client-side storage solution to protect the data.

Solutions:

- To remotely lock a device and enforce lockout duration.
- To method of triggering remote wipe native to device or proprietary.
- Verify wipe completion process.
- Ability to detect block SIM cards and block a stolen device when a new SIM card is detected.
- Provide SD card encryption.
- Ability to control speech recognition function-enable/disable access to functionality on the device.
- Provide pin/pattern/password/biometric access to mobile device–reset either remotely or in a self-service portal.
- Provide auto-alerts.
- Enable/disable device location either by GPS and/or cellular triangulation.
- Malware and virus protection – device level firewall or intrusion detection system.
- Control mobile device camera–enable/disable front and rear cameras, and detect and prevent manual override by user.
- Control speech recognition function-enable/disable access to functionality on the device.

b. Protection for data in transit

The authorized users are allowed to access and transmit key corporate assets such as emails, enterprise applications or some critical documents. This data transmitted between the mobile devices and other networks (servers) done commonly through client-server system. The data transmitted through the carrier network and internet can be transpired through compromised wireless networks, network devices or any malware pre-existing on the devices. How to protect the data in transit to avoid exposing the sensitive data to the notorious attackers?

Solution:

- Prevention, detection, and restriction of jail-broken devices – tethered and over-the-air jailbreak methods.
- Control Bluetooth communication–blacklist/whitelist by vendor or peripheral type.
- Provide Wi-Fi control–blacklist/whitelist selective Wi-Fi networks, and detect and prevent manual override by user.
- Enable/disable device location either by GPS and/or cellular triangulation.
- Control to enable/disable device location either by GPS and/or cellular triangulation.

c. User Authentication features available

User authentication advents from PIN, to Pattern, to Bio Metrics for the right user to have it

d. Device level protection in case of lost mobile

On an average 3 users out of 10 loses the mobile devices. The lost mobile device both iOS and Android can easily be cracked and the enterprise data can be retrieved if it is not encrypted. Not having a phone lock will ease the attackers to impersonate the victim to access critical information.

- Jailbreak/root detection mechanism.
- Enable/disable device location either by GPS and/or cellular triangulation.
- Enable/disable location-based services.
- Enable remotely lock a device and enforce lockout duration.
- Run a tool of triggering remote wipe native to device or proprietary.
- Verify wipe completion process.
- Detect block SIM cards and block a stolen device when a new SIM card is detected.
- Provide malware and virus protection – device level firewall or intrusion detection system.

- Prevent, detect, and restrict jail-broken devices – tethered and over-the-air jailbreak methods.
- Provide SD card encryption.
- Control mobile device camera–enable/disable front and rear cameras, and detect and prevent manual override by user.
- Control Bluetooth communication–blacklist/whitelist by vendor or peripheral type.
- Control speech recognition function-enable/disable access to functionality on the device.
- Secure pin/pattern/password/biometric access to mobile device–reset either remotely or in a self-service portal.
- Trigger auto-alerts.

e. Data backup and restore

Data backup is critical for the enterprises and the users.

- Schedule over-the-air backup to a central archive and restoration by authorized users and administrators. Available on either a Wi-Fi or cellular network.
- In the event a user loses their device, MDM solution back up application information so that it can be restored on the user's next device.
- Ability to perform selective backup (i.e. business files, apps, device settings, etc.)
- Install the softwares and configure by sending configuration file via message.
- Feature to restore the device by using the device backup stored at the server.

f. Suspicious alerts to your mail ID or other mobile

Must be Intelligent enough to read unusual behavioral pattern and report to the Business Administrator. Also on reading unusual behavior, the device should ask for authentication.

g. Malicious software

It is very likely the mobile user downloads Android applications from unknown sources. The potential malicious software applications may be downloaded from the internet or copied from Secure Digital (SD) cards which might expose the enterprise data which can intelligently attack the system. The malicious software can attack both the device and also enterprise system in the backend. No policy to control users from downloading applications on personal device under

Bring Your Own Device (BYOD) in current corporate scenario would lead to exposing Enterprise applications and data to malware applications. The user innocently would be victimized to the criminal activity of the malicious software also ricking the Enterprise data. Peer to Peer sharing is the biggest and weakest form of networking (Bluetooth) to transmit the data and notable mobile malware infections are spread in this environment by spying sensitive data and loss of financial data.

h. Default device management software

Solution:

- Separate personal and private user data from business data.
- Supports virtualized OS and apps.
- Conduct auto audits, remote assessment, remediation, and compliance reporting.
- Ability to enter user information or phone information not listed elsewhere.
- Integrates mobile device data with Microsoft SCCM.
- Integrates with existing enterprise systems, such as WLAN and other consumer management solutions.
- Manages multi-user devices with user profiles, device check-in/check-out, and app store account management.
- Multi-factor authentication.
- Self-help library with answers to simple technical questions online.
- Provides terms of use for access to State resources.
- Registers devices by either system administrator or end-user.
- Supports business intelligence features, such as automated report generation and distribution, and custom reporting capabilities.
- Reports on data usage and trends.
- Reports on inventory classification - unknown, authorized, provisioned, decommissioned, etc.
- Reports on last-connected status, updates, and push status.
- Automatically configures the exchange connection and configuration upon device activation.

i. **Encryption and login implementation to specific file or folder**

Enterprise Applications communicates with the backend system without strong mutual authentication and encryption of the communication channel can expose the data and might fuel attacks in future.

j. **Enterprise – Mobile Document Management**

As TechnoLabs developed mobile document management product, **MobiDocs**, we would like to have special protection for documents and collaboration.

Solution:

- Digital signature for mails.
- Push documents out to MDM devices.
- Provide an integrated document container.
- Integrate with third party document containers (i.e. DropBox, SkyDrive, etc.).
- Provide document editing and or integrations with third party document editing tools.
- Host a document library for publishing iBooks or shared containers.
- Newsstand implementation similar to iPhone.

8-2-293/82/A-120, Road No.70, Jubilee Hills, Hyderabad – 500033