ASEI MICHIGAN CHAPTER

Security of Smart Devices

Sajay Rai CPA, CISSP, CISM
Securely Yours LLC
sajayrai@securelyyoursllc.com

June 27, 2013

Securely Mobile

Topics

- Native Security in Devices
- Typical use of Devices
- MDM and Security

iOS Security Features

Data protection

Hardware Encryption: Every iPad device has a dedicated AES 256-bit crypto engine built in that is used to encrypt data on the device.

File Data Protection: Apple uses a technology called "Data Protection" to further protect data stored in flash memory on the device.

Encrypted Backups: When an iPad device is backed up to iTunes, it can be encrypted to prevent access to information stored in the backup.

Effaceable Storage: The "Erase all content and settings" option in the Settings menu destroys all the keys in Effaceable Storage, making all user data on the device cryptographically inaccessible.

iOS Security Features

Network protection

Wi-Fi protection: iOS devices supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses AES encryption.

Internet protection: Native internet Applications such as Safari, Calendar, Mail, etc. automatically use SSL/TLS to enable an encrypted communication between the device and networks.

Built-In VPN: iOS features a built-in VPN client to securely connect to Cisco IPSec, L2TP, and PPTP VPN servers right out of the box

iOS Security Features

Application protection

Mandatory Code Signing: iOS requires that all executable code be signed. Built-in apps like Mail, are signed by Apple. Third-party apps must be signed using a certificate from the iOS Developer Program.

Application Sandbox: All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device.

System Software Personalization: All iOS devices prevents the installation of unauthorized operating system and prevents iOS from being downgraded to a less secure version.

Typical Use of The Devices

- Exchange ActiveSync is a Microsoft Exchange synchronization protocol. Exchange ActiveSync lets you synchronize a mobile phone, tablet or other supported smart device with your Exchange mailbox.

- Exchange ActiveSync enables mobile phone users to access their e-mail, calendar, contacts, and tasks and to continue to be able to access this information while they're working offline.

- Mobile phones that are compatible with Microsoft Exchange include the following: Apple IOS, Android, Symbian, Motorola, Nokia, Palm

ActiveSync Security Features

- Set policies such as minimum password length, device locking, and maximum failed password attempts
- Initiate a remote wipe to clear all data from a lost or stolen mobile phone
- Require encryption on device
- Force Secure Sockets Layer (SSL) encryption for communications between the Exchange server

But what if we want to manage…

- Blacklisting of applications
- Whitelisting of applications
- Camera
- Bluetooth
- Wi-Fi
- Separation of business data from personal data
- Etc. etc. etc.

Mobile Device Management

- Enforcement of security policies
- Inventory of devices
- Central Management of devices
- Compliance needs