Security for Mobile Devices

FedCASIC
March 2014
Dennis Pickett
Westat

Introduction

- Who am I?
  - Dennis Pickett, Senior Manager of Information Security at Westat
- What will we be discussing?
  1. Securing mobile devices as a general need
  2. What are the risks you need to be aware of with mobile devices, and how do you mitigate those risks?

What do we mean by “mobile device”?

- Most often when we discuss “mobile devices” it mean just tablets and smart phones, those devices with a mobile operating systems
  - Apple’s iOS
  - Google’s Android OS
  - Microsoft’s Windows Phone and RT OS
  - Blackberry
  - Firefox OS

- “Mobile” can vary, it could mean anything portable
  - Heart rate monitors
  - GPS devices
  - Accelerometers
  - Laptops are included, but generally have traditional tools available for security

What are the benefits of mobility?

- Since the iPhone, and later the iPad, we've seen an explosion in smartphone and tablet adoption for personal and business use
- Users love them because
  - Convenience
  - Portability
- Businesses Love them
  - Cheaper than laptops
  - More user friendly
  - Can leverage user's existing equipment, BYOD
- Mobile devices are here to stay, and the form factors will only become more varied (e.g. Google Glass)

What are the risks with the adoption of mobility devices?

- Two categories, existing and new risks

Existing Risks

- Most of these have proven mitigation strategies for laptops, and options for solving them on mobile OS devices are only now becoming ‘mature’
  - Theft and device loss
  - Malicious software
  - Sharing devices and accounts
  - Controlling access to the network
  - Keeping devices up to date

What are the risks with the adoption of mobility devices? (cont.)

New Risks

- Mobile devices bring new risks that many, including organizations who have devices in use, haven't yet considered. It's a ticking clock, it's a question of when, not if, a security breech will occur if there is no mitigation put in pace.
  - Voice input – Anything you speak goes off device for translation
  - Built in accessories: Camera, Recorder, GPS
  - Employee personal information on company device
  - Finding solutions that work across different OSs, versions, etc.
  - Corporate information on personal devices – Is email ok? What about contact information for other employees or study participants, what about study participant data, network login credentials, contract information?

How do we know what security controls are needed, and how do we know when we've achieved success?

- Appropriate security is achieved through compliance with Federal information assurance laws and requirements
  - Federal Information Systems Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Information Processing Standards (FIPS) 140-2

- As much as we want a "silver bullet", security is a layered process. You must have goals before you can have IT to achieve them.
- Managerial, Operational, Technical
  - Decide on your rules
  - Put practices in place
  - Implement IT to enables those rules and practices

What solutions exist, and how do I go about implementing them?

Managerial – policy, company decisions

- Strategy - Your organization, or at least your project, needs a mobile device security strategy, document it in a policy.
- Once it's on paper you have a boundary drawn, it becomes more manageable.
  - Decide what is and isn't allowed on the corporate network
  - May users use their own devices?
  - Standardize platform for distributed devices
  - What investigative rights does your organization have over a user's personal device if used for work?
  - Users must sign roles and responsibilities before using any mobile device for work

What solutions exist, and how do I go about implementing them? (cont.)

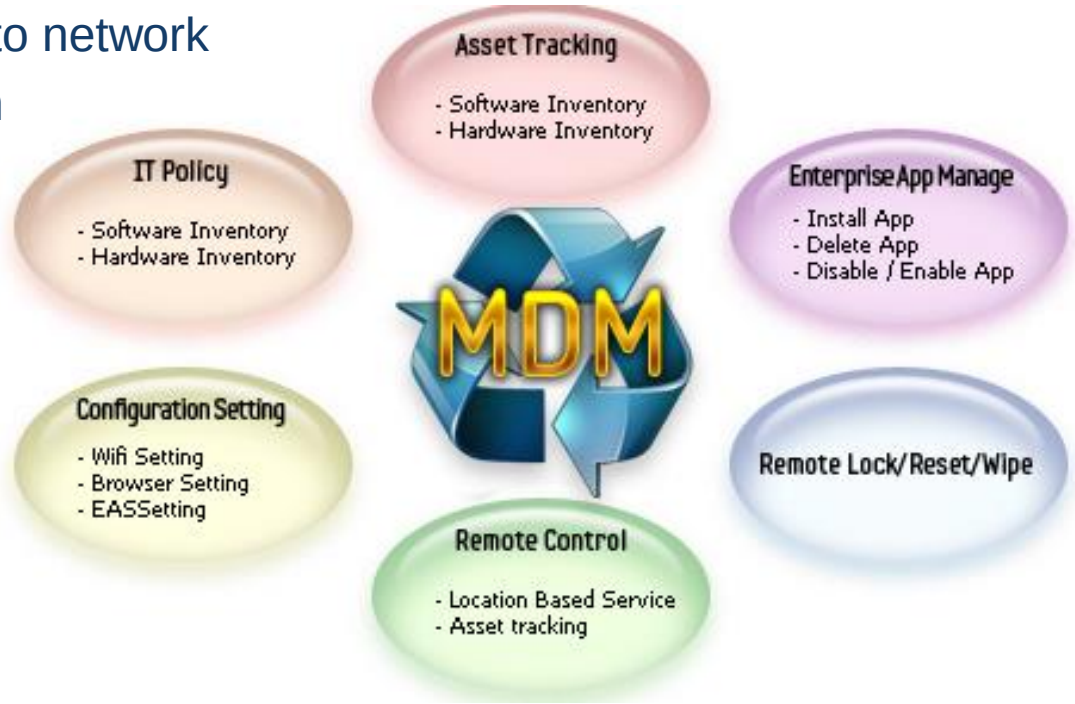
Operational

- Process and Procedures - Implement, test, and train in operational procedures related to mobile devices, and follow best practices where possible. Key items:
  - Software (app) development procedures must include security controls and testing
  - De-Identification of Data
  - Offloading of Data

What solutions exist, and how do I go about implementing them? (cont.)

Technical

- Apply technical controls at the Device Level where possible, and at the Application Level in other cases
- Implementation - Device
  - Mobile Device Management (MDM)
    - Control access to network
    - Containerization
    - Remote wipe



What solutions exist, and how do I go about implementing them? (cont.)

Technical

- Implementation - Device
  - Leverage what the OS provides
    - FIPS 140-2 Cryptographic Modules
    - Apple Configurator, Samsung Android Knox, Blackberry Playbook
    - VPN at application layer
    - Access controls
    - Full disk encryption
  - Antivirus and malware

What solutions exist, and how do I go about implementing them? (cont.)

Technical (cont.)

- Implementation – Apps and Network
- YOU are responsible for building, or buying, apps with appropriate security controls that will enforce:
  - Authentication and authorization of users
  - Access to corporate resources
  - Protection of credentials on the device
  - Protection of data at rest
  - Protection of data in transit
  - Security logging and auditing
- Don’t expect another component to secure your app, understand what you are getting from the device, and what you need to build into your program.

Case study

- Data Collection Project
  - In home interviews
  - 1,200 devices in field
- Security was achieved through a layered approach
  - Security plan with policy, practices, and procedures
  - De-identified information
  - Device level
    - Full disk encryption (FDE) through OS
    - PIN authentication to device
  - App level
    - Complex password to access application
    - Authentication required to transfer to server
    - HTTPS to encrypt data in transit

What does the future hold?

- The Good
  - More security and management tools and options
  - More mature products
  - More products aimed at Federal compliance
- The Bad
  - More sophisticated attacks as more as more valuable information is stored on mobile devices and use becomes more widespread

Questions?

Dennis Pickett, CISSP
Westat
Senior Manager of Information Security
301-251-8203
dennispickett@westat.com