Booz | Allen | Hamilton

Compliance Management for Mobile Devices

MOBILE SOLUTIONS

Agenda

- Mobile Device Use – Today
- Mobile Device Use – Tomorrow
- Mobile Device Configuration
- Challenges in the Mobile Device Environment
- Policy and Configuration Guidance
- Device Deployment Models
- Devices
- SCAP Issues Today
- Potential SCAP Use
- Questions

Mobile Device Use - Today

- **Early usage of mobile devices in Government focused almost exclusively on Blackberry devices.**
  - **Primarily for E-mail access**
  - **Some web-browsing**
  - **Phone**
- **Government owned and issued devices strictly controlled via Blackberry Enterprise Server (BES).**

PHOTO: DANA LIPNICKAS, DAVID GOLDMAN/CNNMONEY

Mobile Device Use – Tomorrow

- **Proliferation of smartphone devices has greatly expanded the use and interest in using non-Blackberry devices. Rich feature sets provide a number of new uses for these devices within the government. In addition to functions used in the Blackberry devices, Apps and other resources now provide tools such as:**
  - **GPS used for Blue Force Tracking and Navigation**
  - **Apps for command and control of Unmanned Aerial Vehicles**
  - **Camera used for Intel gathering**
  - **Aviation use to eliminate bulky maps and charts**

Mobile Device Configuration

Like the traditional computing environment, mobile devices can be configured on the device itself or through a tool known as a Mobile Device Manager (MDM). Each solution has benefits and costs:

- **Per Device Configuration**
  - **Benefits: easy for anyone to do, doesn't require access to a network to configure the device**
  - **Cost: easily overridden by the user, no consistency, not scalable**
- **MDM Configuration**
  - **Benefits: consistent configuration, can serve as a policy enforcement point**
  - **Cost: additional cost, requires technical expertise**

Challenges in the Mobile Device Environment

Mobile devices bring tremendous capabilities to the government workforce but along with these capabilities and flexibility come some new challenges and paradigms that must be considered. These include:

- **Policy and Configuration Guidance**
  - **Unclear policy**
  - **Narrow configuration guidance**
  - **Undefined usage model**
- **Deployment Models**
  - **Government issued and controlled**
  - **Bring your own device (BYOD)**
- **Devices**
  - **Device capabilities vary significantly on the Android platform**
  - **COTS products that are updated regularly**
  - **Limited support for traditional Information Assurance tools**

Policy and Configuration Guidance

Policy and Guidance for traditional devices is well established and defined. However, there have been some challenges in developing this level of maturity with respect to mobile devices.

- **No "universal" policy**
  - **Many capabilities are left to the site to determine what is appropriate**
    - **Example – Should cameras be enabled or disabled?**
- **Narrow configuration guidance**
  - **STIGs for Android, iOS and Windows Mobile 6.5 are currently based on Good Technology's Mobile Device Manager (MDM) only**
- **Undefined usage model**
  - **Who will "own" the device physically and from a Certification and Accreditation (C&A) perspective**
    - **Example - Will the Army issue each solider one at Boot Camp for the duration of their service or will they issue/return per duty assignment?**

Device Deployment Models

The features offered by mobile devices are attractive to government and there is a desire to use them now. The challenges include a limited budget to purchase these new devices so should employees be allowed to bring their own device (BYOD)?

- **Government issued and controlled**
  - **Government authorizes usage and pays for service. Clear lines of ownership permit total device control and clear usage guidelines.**
- **Bring your own device (BYOD)**
  - **What government resources can the user access?**
  - **Does the government have the right to wipe the phone?**
  - **Can the government limit usage of a personally owned device?**
  - **Is government data stored and sandboxed within an encrypted security container?**
  - **Do the benefits outweigh the risks?????**

Devices

As COTS products, the mobile device market is highly competitive. New devices and features are put out at a rapid pace. The business model of these companies is different from traditional PC vendors as is the buying/lifecycle from the customer perspective.

- **Business Models**
  - **Wide variety of operating systems and devices as well as MDM tools. Stiffer competition leading to challenges in cross-platform support**
    - **Apple and RIM have own devices, OSs, and MDMs**
      - **Support by 3rd party MDMs often limited or restricted by RIM, Apple**
    - **Android OS is only supported 3rd party devices and MDMs**
      - **Very few security features out-of-the-box (must be supplemented)**
  - **Devices can also vary based on cellular service provider**
- **Consumer Lifecycle**
  - **Relatively inexpensive so more frequently replaced that PCs/laptops**
    - **Apple pre-sold 1 Million iPhone 4S models in the 1st 24hrs!**
- **Limited support for traditional Information Assurance tools**
  - **Antivirus, Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS)**

SCAP Issues Today

Issues with leveraging SCAP today in a mobile environment include:

- **Lack of Vendor Adoption**
  - **Unlike the desktop environment where SCAP is being adopted, this same effort has not yet migrated to the mobility world**
- **Lack of Content**
  - **As with existing SCAP implementations, coding resources are limited**
  - **SCAP specifications were not designed to work with resources sitting on another carrier's network**
- **Limited Configuration Guidance**
  - **As mentioned before, unclear configuration guidance makes it difficult to build tools to support checking of the configuration**

Potential SCAP Use

Communication between the various MDMs and devices will likely remain proprietary. However, SCAP could possibly be leveraged to gather reporting information. Our task is looking into:

- **Information gathered in the MDM database**
  - **Identifying configuration management related items and how they are captured such as unique identifiers**
- **Development of a prototype capability to extract the information from the MDM database and act as an SCAP translator**
- **Leveraging this SCAP data in existing tools for visualization purposes.**

Questions?