Security for Mobile Technology

Solicitation Number: HSHQDC-14-R-B0005

Industry Day

6/24/2014

Luke Berndt
Program Manager
Cyber Security Division

Homeland Security

Commercial Marketplace

- Enterprise requirements originally drove the commercial smart phone marketplace
  - Made management and security a market priority and Blackberry a market leader
- Consumers now drive the market and have different priorities
  - Gov has demanding requirements but makes up a small percentage of sales
  - Devices not designed for centralized management & policy
- Consumer Mobile Devices (e.g., Android & iOS tablets and phones) would improve the effectiveness of Government but do not meet security requirements
- Government needs security solutions that allow for these devices to meet its requirements
  - These advances would benefit private sector as well

Mobility Drivers

- Federal Gov productivity gains from mobile devices = $28B / year
  - Surveyed Feds believe mobile devices provide 9h per week productivity gains[1]
- Fed spends $1.3 billion annually for wireless services and mobile devices and has about 1.5 million active accounts[2]
  - Fed purchased +400k Blackberries last year
- Mobility is a priority in the White House's "Digital Government Strategy"
  - Both for gov use and citizen facing
- Ability to effectively work remotely
  - Telework, continuity of operations, less office space
  - Can work during non-work hours
- Provide new ways to collaborate and communicate
  - Custom apps for verticals – GIS, Remote Data Entry
- Employee demand, workforce retention

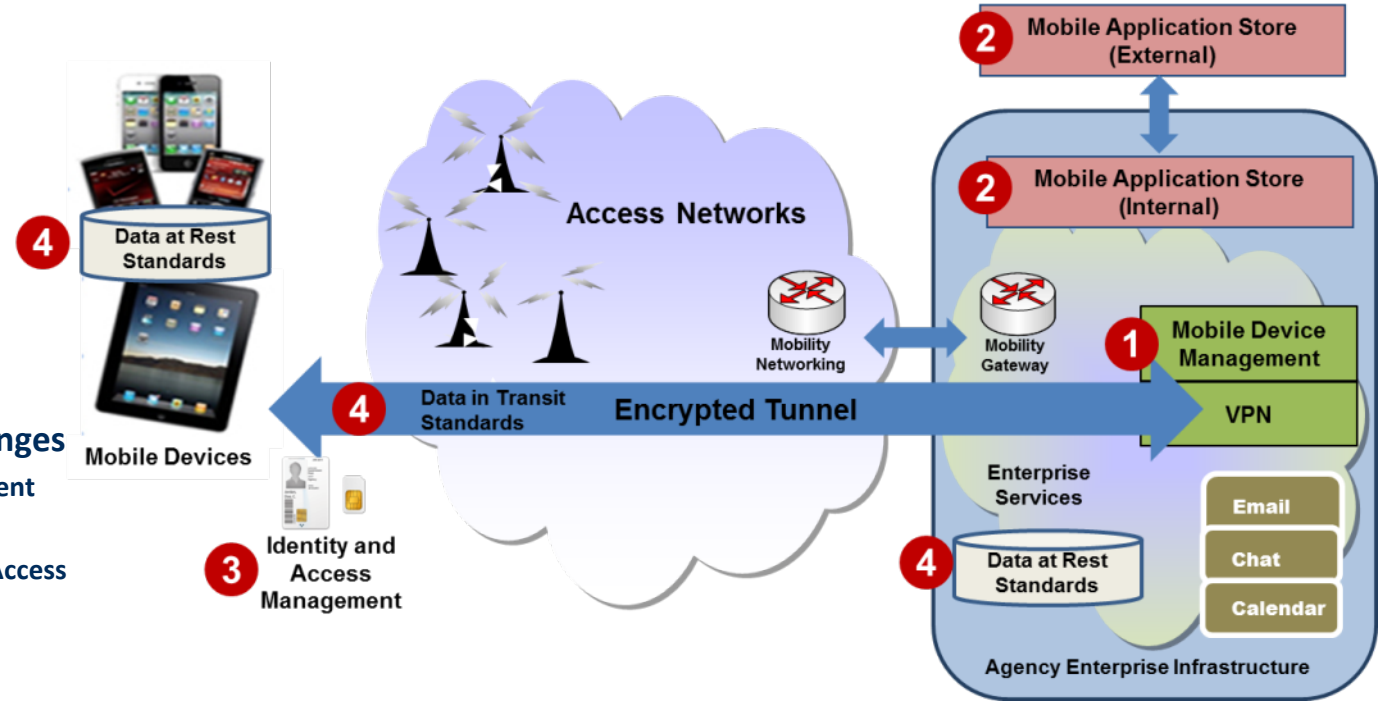
1: The 2013 Digital Dilemma Report – Mobile Work Exchange

2: GSA Wireless blanket purchase agreement

DHS Use Case Pilots

DHS Component	User Test Case	Mobile Platform	Application	Business Case
CBP	20 Executives and IT Personnel	Android	Cargo Processing	Allows CBP inspectors to screen and release cargo in near real-time.
ICE	500 Law Enforcement, Executives, and Management Personnel	Apple iOS Android	Alien Criminal Response Information Management System (ACRIMe)	Provide immigration status, identity information, and real-time assistance to law enforcement agencies requesting assistance with identifying illegal immigrants suspected, arrested, or convicted of criminal activity.
USCG	Employees and Pilots	Apple iOS	Electronic Flight Bag	Aviation operations to reduce paper waste and costs by replacing flight bags and loads of paperwork they hold with the electronic tablets.

Threats to Mobility



Top Mobile Challenges

1. Mobile Device Management
2. Mobile Application Store
3. Identity, Credential and Access Management (ICAM)
4. Data Standards (FIPS)

Mobility threats target all elements of mobile architecture

- Applications – malware, vulnerable code
- Devices – insecure configuration, password protection
- Infrastructure – lack of encryption of data in transit, behavior/location tracking
- Users – acceptable use, loss of device

Threat is real; attacks not widespread yet, but increasing – Chance to get ahead

Program Overview

Mobile Security Program

- S&T Center of Excellence (CoE)
- Small Business Innovative Research (SBIR)
- Cyber BAA
- Pilots

Challenge Space

- Device Management
- App Screening
- Identity Management
- Data Management

Key areas that require improvements in tools and processes to "accelerate the secure adoption of mobile technologies into the Federal environment"

– **Government Use of Mobile Technology Federal CIO Council**

Program Activities

Mobile Challenge	Vehicle	Effort	Description	Benefits
Mobile Application Management (MAM)	S&T CoE	Research dataset	UCSB: Collecting, analyzing and classifying mobile malware and based on this insight, developing techniques for attack prevention, detection and recovery	• Builds a research dataset for mobile malware to inform future research/ mobile app development
Mobile Application Management (MAM)	S&T CoE	Mobile App Communications analysis	GMU: Track mobile app data emissions/system calls and develop analysis tool.	• Develop the ability to ID malware based on app behavior
Mobile Device Management (MDM) Device Trust	SBIR	Software Based Roots of Trust (SRoT)	SBIR projects underway exploring a range of SW solutions to provide secure root of trust	• Identifies promising techniques (e.g. PUFs, firmware, etc) for Phase II follow on work
Mobile Device Management (MDM)	Pilot	9.1 Baseline mobility Proof of Concept with DHS OCIO	Working with DHS OCIO to provide technology to support a centralized pilot across DHS (Devices, PIV card readers, etc.)	• Implement a solution focused on meeting 9.1 Security Baseline
Identity and Access Management (IAM)	Pilot	Initial: PIV Integration	Working with OCIO to examine derived credentials	• Enables capability to handle more sensitive data on mobile devices (e.g. PII)

Responsive Web Design

A site for every device category

A responsive design that responds to screen size and device

The number of devices, platforms and browsers that your site needs to work on is growing

Instead of having to manage multiple sites, a business with a responsive site can take a unified approach to content management

http://johnpolacek.github.io/scrolldeck.js/decks/responsive/

Responsive Security

- Access patterns change
- Device usage changes
- Walking differently
- Crypto certs

User

- New OS loaded
- Firmware changes
- Unusual location
- Suspicious Wi-Fi

Device

Inputs

- Accessing other App data
- New behavior
- Unusual network traffic
- Suspicious author or libraries

Apps

- Sensitivity based upon how data is used and interacted with
- Enterprise Data to inform security

Data

Security that responds to Context

Context & Risk
Allows for security decision to be continually and responsively made

Security policy that is unified and adaptive

Program Objective

Static

PC Centric approach

- Enterprise PCs
- Corporate Network
- Guards control physical access

Access to data is all or nothing - rarely reviewed

Goal: A wide range of consumer devices can be augmented to meet government security requirements, using a responsive approach to security

Responsive

Mobile Native approach

Risk continuously evaluated

- Device location & integrity
- App configuration & behavior
- User actions

Access to data is adjusted based upon risk

TTA #1: Mobile Device Instrumentation

Goal: Use the full capabilities of device to better determine who is using it and the environment it is being used in.

- Continuously:
  - authenticate the user
  - perform a risk based assessment of device context
- Devices are loaded with sensors
- Users physically interact with devices differently than desktops

TTA #2: Transactional Security Methods

Goal: Security is evaluated with every request instead of only at sign-on. A range of responses is possible instead of all or nothing.

- Methods to provide a continuum of risk-based responses for data requests
  - Within a device: between Apps and also between OS & Apps
  - Over a network: include methods that are not reliant on the end device, but benefit from it

TTA #3: Mobile Security Management Tools

Goal: Tools that provide insight across all of the devices an employee may use. Alert trigger will be multifactor and complex, and need to be explained clearly.

- Security management tools that tie together a User's actions across platforms
- Operate across a range of time instead of instantaneous decisions based upon discrete events
- Present information in an actionable way that provides context around why an event was triggered

TTA #4: Protecting Mobile Device Layers

Goal: Advanced methods for protecting core elements of a mobile device from infection.

- Novel approaches for protecting the layers and components from infection by malicious applications
  - E.g., firmware, baseband, and OS
- Allow for the device to be returned to a known good state:
  - Either prevention or detection and remediation

Topic Specifics

- Types:
  - No Type I
  - Type II – 2 year & $2m + transition option
  - Type III – 1 year & $500k + transition option
- Transition Task Option – 6mo, with Fed partner
- Metrics & Go/No Go
- Targeted Mobile Platform(s)
- Targeted TTA, explanation if more than 1
- Current threat model and known vulnerabilities

Homeland Security

Science and Technology