Mobile Device as a Platform for Assured Identity for the Federal Workforce

Dr. Sarbari Gupta

President and CEO, Electrosoft

U.S. Army Information Technology Agency (ITA) Security Forum
Fort Belvoir

October 20, 2014

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- Strong Push to Enable Federal Mobile Workforce
- Security Concerns and Mitigations for Mobile Computing
- Use of “Derived PIV Credentials” for Identity Assurance
- Wrap-Up

Mobile Workforce – Drivers (I)

- **Telework Enhancement Act of 2010**
  - ***A framework for agencies to better leverage technology and to maximize the use of flexible work arrangements***
- **Key Objectives of Telework**
  - ***Improve Continuity of Operations (COOP)***
  - ***Promote Management Effectiveness***
  - ***Enhance Work-life Balance for Workers***
- **Benefits of Telework**
  - ***Recruit new Federal workers***
  - ***Retain valuable talent***
  - ***Maintain productivity***

Mobile Workforce - Drivers (II)

- **Digital Government Strategy of 2012**
  - ***To seize the digital opportunity and fundamentally change how Federal Government serves its internal and external customers***
- **Strategy Objectives**
  - ***Information and services anywhere, anytime and on any device***
  - ***Procure and manage devices/applications/data in smart, secure and affordable ways***
  - ***Unlock the power of Government data to spur innovation***

Mobile Workforce – Drivers (III)

- **Presidential Memo – Enhancing Workplace Flexibilities and Work-Life Program of 2014**
- **Key Objectives:**
  - ***Right to Request Work Schedule Flexibilities***
  - ***Expanding Access to Workplace Flexibilities***
  - ***Expanding Availability and Encouraging Use of Work-Life Programs***

Mobile Computing - Wave of the future…

- **Gartner: Smart Machines To Be Most Disruptive Trend (Oct 2014)**
  - ***"The smart machine is upon us, and it will be the most disruptive in the history of IT …"***
- **Federal CIOs recognize the need to embrace and facilitate mobile computing for their workforce**
- **However, key challenges exist in the security and privacy arena**

Security Challenges with Mobile Devices

- **Small form factor makes it easy to lose, misplace**
- **Device passwords seldom enabled**
- **Multiple channels of attack and access**
  - ***Poorly secured communication channels (e.g. WiFi)***
- **Complexity and proprietary nature of Mobile OS**
  - ***Multiplicity of Mobile OS versions in the field***
  - ***Patches and updates implemented sporadically***
- **Plethora of mobile apps**
  - ***Ease of quick download and use of malware***
  - ***Difficulty of source verification and integrity checks***
- **Ease of unauthorized OS modification (e.g. "jailbreak")**

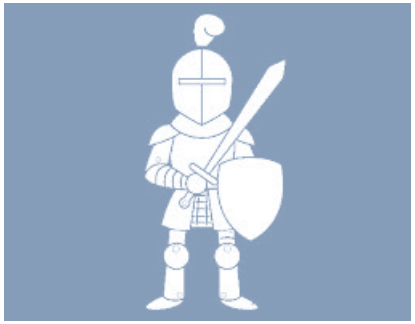
*** Reference: 2012 GAO Report "Better Implementation of Controls for Mobile Devices Should Be Encouraged"**

Mobile Device Attack Paths

- Attacker gains physical control of device
- User visits malicious website
- User download Apps from web (other than from reputable source)
- Attacker eavesdrops on unencrypted communications from device

Mobile Device Security Controls - User

- Maintain physical control of device
- Enable user authentication to device
- Use 2-factor to protect sensitive transactions
- Limit use of insecure communication channels
- Download Apps from reputable sources only
- Install security software – firewall, anti-malware
- Install security updates promptly
- Enable remote wipe of data



* Reference: 2012 GAO Report "Better Implementation of Controls for Mobile Devices Should Be Encouraged"

Mobile Device Security Controls - Agency

- **Establish / Implement Mobile Device Security Program**
  - ***Security Policy***
  - ***User Training***
  - ***Deployment Plan***
- **Implement layered security for mobile device**
  - ***Authentication to device***
  - ***Cryptographic protection of data and transactions***
  - ***User training and awareness of security risks***
- **Implement Mobile Device Management (MDM) solution – Server and Client App(s)**
  - ***Run in the background***
  - ***Run in "sandboxed" environment***
  - ***Manage the security configuration of device***
  - ***Implement 2-factor techniques***
  - ***Encrypt stored data***

Federal Mobile Security References

- **National Institute of Standards and Technology**
  - ***SP 800-164 DRAFT: Hardware Rooted Security in Mobile Devices***
  - ***SP 800-124 Rev 1: Managing the Security of Mobile Devices***
  - ***SP 800-121 Rev 1: Bluetooth Security***
  - ***SP 800-163 DRAFT: Vetting 3rd Party Mobile Applications***
  - ***SP 800-101 Rev 1: Mobile Device Forensics***
- **Office of Management and Budget**
  - ***M-06-16: Protection of Sensitive Agency Information***
  - ***M-15-01: Guidance on Improving Federal Information Security and Privacy Management Practices***
- **Federal CIO Council (May 2013)**
  - ***Federal Mobile Security Baseline***
  - ***Mobile Computing Decision Framework***
  - ***Mobile Security Reference Architecture***

What are Derived PIV Credentials?

- **Specified in NIST Special Publication 800-157 DRAFT**
- **A security token, implemented and deployed directly on a mobile device (such as smart phone or tablet)**
- **Issued to holder of a valid PIV Card**
- **Set of PKI credentials similar to those on PIV Card**
  - ***PIV Authentication (for identity authentication)***
  - ***PIV Signature (for digital signature)***
  - ***PIV Key Management (for encryption)***
- **To be used with secure Apps on mobile device**

Derived PIV Credentials - Life Cycle

- **Initial Issuance**
  - ***Subscriber proves possession/control of valid PIV card***
  - ***Issuer checks that PIV Card is not revoked***
  - ***Derived PIV credentials issued to mobile device***
- **Maintenance**
  - ***Updates to Derived PIV credentials done remotely or in-person***
  - ***Derived PIV credentials usable even if PIV Card is lost / revoked***
- **Termination**
  - ***When Derived PIV credentials no longer needed***
  - ***When PIV Card is terminated***

- **Linkage with PIV Card**
  - ***Maintenance of Derived PIV credentials linked to PIV Card***
  - ***Linkage updated when Subscriber gets new PIV Card***

Derived PIV Credential Implementation

- **Form Factors**
  - ***Removable (non-embedded) Hardware Crypto Token***
    - **Secure Digital (SD) Card**
    - **Universal Integrated Circuit Card (UICC)**
    - **Universal Serial Bus (USB) Token**
  - ***Embedded Crypto Token***
    - **Hardware implementation**
    - **Software Implementation**
- **Who can issue**
  - ***Agency that issues PIV Card***
  - ***Other Agency***

How do Derived PIV Credentials Facilitate Federal Mobile Workforce?

- **Enables initialization of mobile devices for secure use by Federal mobile worker**
  - ***Agency-issued device***
  - ***Personal device (BYOD)***
- **Facilitates the use of Derived PIV Credentials for**
  - ***Standalone Secure Apps***
  - ***MDM Client Apps***
- **Possible Uses Cases**
  - ***Secure Browsing with 2-factor authentication***
  - ***Secure email send and receive***
  - ***IPSEC-based VPN tunnels to agency network***
  - ***Strong encryption of sensitive data on device***
  - ***Sign and verify signature on digital document***

Wrap-Up and Contact Information

- **Summary**
  - ***Mobile computing a core part of future Federal IT***
  - ***Security challenges need to be addressed***
  - ***Derived PIV Credentials offer strong foundation for security***
  - ***Multiple use cases to leverage Derived PIV Credentials for secure mobile computing for Federal workforce***
- **Questions / Comments ?**

- **Contact Info:**
  - ***Dr. Sarbari Gupta – Electrosoft***
    - **Email: sarbari@electrosoft-inc.com**
    - **Phone: 703-437-9451 ext 12**
    - **LinkedIn: http://www.linkedin.com/profile/view?id=8759633**

Mobile Device Security Controls - User

- Maintain physical control of Device
- Enable user authentication to device
- Use 2-factor to protect sensitive transactions
  - *Use 2-factor Authentication for access to websites*
  - *Encrypt data stored on device*
  - *Use VPN to connect to Organizational network*
  - *Encrypt and/or sign email communications*
- Restrict download of mobile Apps
  - *Allow download only from "whitelisted" sources*
  - *Verify authenticity of downloaded Apps*
- Install security software – firewall, anti-malware
- Install security updates promptly
- Enable remote wipe of data
  - *For device loss, too many authentication attempts, etc.*
- Limit use of other communication channels
  - *Limit use of public/shared WiFi networks*
  - *Configure Bluetooth default to "non-discoverable"*

*** Reference: 2012 GAO Report "Better Implementation of Controls for Mobile Devices Should Be Encouraged"**