Strong Authentication for Physical Access using Mobile Devices

DoD Identity Protection and Management Conference

May 15-17, 2012

Dr. Sarbari Gupta, CISSP, CISA
sarbari@electrosoft-inc.com
703-437-9451 ext 12
Agenda

- Establishing Context
- Need for Strong Authentication for Physical Access
- Mobile Device Capabilities
- Authentication using Mobile Devices
- Strengths and Weaknesses
- Applicability
- Wrap-Up
Establishing Context (I)

- **Strong Authentication**
  - Identifying an individual through 2 or more factors of authentication:
    - Something you Know
    - Something you Have
    - Something you Are
Physical Access

- Entry into a controlled physical space such as a Government Facility or Lab
Establishing Context (III)

- Mobile Devices
  - Cell Phones, Smart Phones, PDAs, etc.
Determining the Need for Strong Authentication

- **Guidance/Policy on Protection of Physical Facilities**
  - **MCO 5530.14A** – Marine Corps Physical Security Program Manual
  - **DoD 5100.76-M** – Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
  - **ISC Facility Security Level (FSL)** Determinations for Physical Facilities
  - **NIST 800-116** – A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
**ISC Facility Security Level (FSL) Determination**

- Interagency Security Committee (ISC)
- Standard for determining “Facility Security Level (FSL)” of a Federal facility based on:
  - Mission Criticality; Symbolism; Facility Population; Facility Size; Threat to Tenant Agencies
- FSL determines security protections needed
- However, *no guidance on authentication mechanisms* to be used at each FSL
- A Recommendation for Use of PIV Credentials in Physical Access Control Systems (PACS)
- **Assigns Authentication Factors required for each type of Security Area**

<table>
<thead>
<tr>
<th>Security Areas</th>
<th>Basis for Authentication</th>
<th># Authentication Factors Req'd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled</td>
<td>Proof of Affiliation</td>
<td>1</td>
</tr>
<tr>
<td>Limited</td>
<td>Functional Roles</td>
<td>2</td>
</tr>
<tr>
<td>Exclusion</td>
<td>Individual Authorization</td>
<td>3</td>
</tr>
</tbody>
</table>
Government Position on Personal Mobile Devices

- Obama Executive Order (Nov 2011)
  - “limit the number of information technology devices (e.g. cell phones, smartphones, tablets, laptops) that can be issued to individual employees”
  - **IMPLICATION** → Employee personal mobile devices to be utilized when possible

- “BYOD” Phenomenon
  - Most Agencies crafting “bring your own device” policy

- DoD developing “no nonsense policy” on use of mobile devices
Mobile Device Capabilities

- Telephone
- SMS (Short Message Service)
- Email
- Web Access
- Secure Storage
  - User Identifier, Crypto Keys, PKI certs, Other …
- One Time Passwords (OTP)
- Cryptographic Functions
  - Symmetric, Asymmetric
- NFC (Near Field Communications)
One Time Password (OTP)

- Random Authentication Code
  - Valid for only one logon session / transaction
  - Has a short time to live
  - Resistant to “Replay Attacks”
  - Frequently more complex than passwords humans can memorize

- Both Server and Client may need to be synchronized
  - Time synchronization
  - Counter Synchronization
  - Chaining of previous passwords
  - Challenge-Response
OTP on Mobile Devices

- Delivered (from Server) to mobile device
  - Voice call
  - SMS
  - Email

- Generated locally on mobile device
  - Mobile device application (App)
    - App initialized to synchronize with Server
  - May require user to enter a PIN
    - Second Factor of Authentication
Near Field Communications (NFC)

- Wireless communication protocol built into late model mobile devices
  - Range typically 2 - 4 cm
  - Data stored locally in Secured Element (SE)
    - Embedded secure element, secure micro SD cards

- Communication Modes
  - Passive – Initiator device provides power to target device
  - Active – Both Initiator and Target devices need own power

- Used for:
  - Contactless payments
  - Ticketing
  - Holder Authentication
  - Sharing data between mobile devices
  - Other …
NFC for Mobile Device Authentication

- **Data in SE can be accessed by:**
  - Software Applet on the phone
  - Single Wire Protocol (SWP)
    - Enables communication with partnered device (Card reader, other phone …)
    - Allows access without power to the host phone
  - Device can be configured to grant or restrict access to individual SE applets from the SWP
- **NFC allows mobile device to act as a contactless smart card**
Possible Schemes:

- Delivered-OTP + User Password
- Generated-OTP using User PIN
- User Data Read + Visible Match
- Cryptographic Challenge Response
- One Time Password (OTP) delivered to mobile device
  - On User request to Server
  - Delivered via Phone, SMS, or Email

- At Physical Entry Point, User enters:
  - OTP received
  - User’s static password

- Notes:
  - Requires device to be charged
  - Requires cellular or data connection
  - Easy to use; Inexpensive
  - Delays due to OTP request and delivery time
Generated-OTP using User PIN

- **OTP generated on mobile device**
  - Using App on device
  - Requires User to enter PIN on device

- **At Physical Entry Point:**
  - User enters OTP generated, OR
  - OTP communicated to reader via NFC

- **Notes:**
  - Requires device to be charged
  - Does not require cellular or data connection
  - Easy to use; Inexpensive
  - Very fast
User Data Read + Visible Match

- Assumes presence of Guard
- At physical entry point, device presented to Guard
  - Guard device reads User Data from device using NFC
  - Guard’s Device displays User Data (e.g. Facial Image)
  - Guard matches device holder face to displayed image

- Notes:
  - Does not require device to be charged
  - Does not require cellular or data connection
  - Easy to use; Inexpensive
  - Delays due to integrity check of User data read
Cryptographic Challenge Response with User PIN

- Assumes presence of contactless card reader

- At physical entry point:
  - User holds device close to card reader
  - User required to enter PIN on device
  - Card reader conducts cryptographic challenge-response with mobile device via NFC
  - Symmetric or Asymmetric (PKI) based schemes possible

- Notes:
  - Does not require device to be charged
  - Does not require cellular or data connection
  - Easy to use; Inexpensive
  - Delays due to cryptographic operations
Mobile Devices as Authentication
“Tokens” – Pros and Cons

- **Strengths**
  - Lower cost “token” since widely deployed
  - Fewer “tokens” for User to track and manage
  - Higher security through fewer cases of “forgotten card”
  - Device may be “wiped clean” remotely if lost

- **Weaknesses**
  - Risk of hacking through “Trojan Horse” Apps
  - User authentication data represents high value target for theft
  - NFC interface (if present) poses significant risk from “skimming” attacks
- Individuals with PIV, CAC or other smart cards
  - Credentials transferred to mobile device
- Visitors or Short-Term Workers
  - Visitor mobile phones registered during “enrollment” process
Dr. Sarbari Gupta – Electrosoft

- Email: sarbari@electrosoft-inc.com
- Phone: 703-437-9451 ext 12
- LinkedIn: http://www.linkedin.com/profile/view?id=8759633