Towards a Unified Framework for Mobile Device Security

Wayne A. Jansen, NIST
Mobile Device Background

• Inexpensive, ubiquitous, wireless, networked, expandable
• Increasingly hold sensitive information or the means to access sensitive information
• At the fringe of corporate influence and control
• Physical security exposure to theft or loss
• Limited computing power, display size, battery life
• Intermittent connectivity
• Many devices per user
• Many operating systems – Palm OS, Pocket PC, Linux
• Users unaware of security implications
• Lack of adequate security mechanisms

*Commercial products and trade names are identified in this presentation to illustrate technical concepts; it does not imply recommendation or endorsement by NIST.
Piecemeal add-on security solutions often present problems in software integration, usability, and administration.

As an alternative, we have developed a unified framework that incorporates the following core security components:

- **User Authentication** – Strong user authentication is the first line of defense for an unattended, lost, or stolen device. Multiple modes of authentication increase the work factor for an attacker; however, very few devices support more than one mode, usually password-based authentication.

- **Content Encryption** – With sufficient time and effort an authentication mechanism can be compromised. Content encryption is the second line of defense for protecting sensitive information.

- **Policy Controls** – When a device is active, various attacks can occur. Policy rules, enforced for all programs regardless of associated privileges, protect critical components from modification and limit access to security-related information.
<table>
<thead>
<tr>
<th>Multi-mode Authentication</th>
<th>Policy Controls</th>
<th>Content Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required Authentication</td>
<td>Effective Policy</td>
</tr>
<tr>
<td>Level 3</td>
<td>Zero or More</td>
<td>Policy C</td>
</tr>
<tr>
<td>Level 2</td>
<td>Zero or More</td>
<td>Policy B</td>
</tr>
<tr>
<td>Level 1</td>
<td>Zero or More</td>
<td>Policy A</td>
</tr>
<tr>
<td>Level 0</td>
<td>None – default at power on and boot up</td>
<td>Most Restrictive</td>
</tr>
</tbody>
</table>

Mobile Security Project
## Example Configuration

<table>
<thead>
<tr>
<th>Level</th>
<th>Required Authentication</th>
<th>Effective Policy</th>
<th>Cryptographic Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0 - Locked</td>
<td>None – default at power on and boot up</td>
<td>Most Restrictive</td>
<td>Unavailable</td>
</tr>
<tr>
<td>L1 - Low</td>
<td>Password</td>
<td>All PIMS, but no communications</td>
<td>Unavailable</td>
</tr>
<tr>
<td>L2 - Medium</td>
<td>Token</td>
<td>All PIMS &amp; wireless with socket restrictions</td>
<td>Available</td>
</tr>
<tr>
<td>Level</td>
<td>Required Authentication</td>
<td>Effective Policy</td>
<td>Cryptographic Repository</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------</td>
<td>-------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>L3 - High</td>
<td>Token</td>
<td>All PIMS with no wireless socket restrictions</td>
<td>Unavailable</td>
</tr>
<tr>
<td>L2 - Medium</td>
<td>None – user choice</td>
<td>All PIMS &amp; wireless with socket restrictions</td>
<td>Available</td>
</tr>
<tr>
<td>L1 - Low</td>
<td>Password, Biometric</td>
<td>A few basic PIMS, IrDA, Bluetooth</td>
<td>Available</td>
</tr>
<tr>
<td>L0 - Locked</td>
<td>None – default at power on and boot up</td>
<td>Most Restrictive</td>
<td>Unavailable</td>
</tr>
</tbody>
</table>
Conventions:
# -- echelon level #
##p -- pre-handler for level #
#_p -- post-handler for level #
#α -- authentication mechanism α at level #
An echelon selector GUI is used to navigate among echelon levels as needed.

The buttons at the center are used to change levels.

A change in level may trigger the execution of one or more authentication modules.

The button for the current echelon level is highlighted.

A slider at the left sets the maximum level to which the device can transition automatically.

An icon is used to display the current echelon level and launch the Level Selector.
• We are developing authentication modules for the framework that include visual authentication and novel forms of smart cards
• The traditional means for user authentication is an alphanumeric password, but a number of drawbacks exist for handheld devices, such as the lack of a full keyboard
• Moreover, translating existing desktop solutions to handheld devices can be problematic:
  – Obstacles include computational speed, network connectivity, battery capacity, and supported hardware interfaces
  – Any inconvenience due to a cumbersome peripheral attachment, lengthy authentication process, or error-prone interaction discourages use
  – Handheld devices have features (e.g., power-on/off behavior) that need addressing
Picture Password

- During enrollment, the user selects a sequence of images, which must be entered for any subsequent login attempt.
- The software supports several different themes and user-defined images/themes.
- Two selection methods are provided: single (single tap) and paired (tap-and-hold, tap).
- The password generated from the image sequence is used to authenticate the user.
- Reenrolling the same image sequence results in a different password value.
- Shuffling images between authentications is an option.
The mechanism relies on a smart card chip packaged in a multimedia card format.

The authentication mechanism adjusts the echelon level on insertion or removal of a valid card and entry of its PIN.

In addition to its smart card capabilities, the card functions as a memory device.

This technology eliminates the need for an expansion sleeve, smart card reader, and full sized smart card that would otherwise be needed.
• Instead of bringing a token into physical contact with a PDA, use a short distance wireless interface
• A challenge-response protocol periodically verifies the presence of the device
• If verification or communications between the token and the device fail, the PDA shuts down
• The proximity token has its own battery and been prototyped using both Bluetooth and near-field magnetic communications
• Rather than bringing a smart card into physical contact with a PDA, use a wireless interface instead
• Bluetooth is present on most handheld devices – no specialized smart card reader is needed by the PDA or another computer
• Unlike wireless smart cards, which draw power directly from the PDA, the Bluetooth smart card token has its own battery
• The device also houses a smart card and Bluetooth radio – it could be a cell phone
• Policy is represented by a set of policy entries
• The policy language follows a grant-style specification by which all actions are denied unless enabled by a policy entry
• Policy entries are a triple of action, source, and target values
  – Action refers to operations performed at the PDA, such as enabling an interface or accessing a file
  – Source refers to objects (resources or services) on the PDA, such as interfaces for PC cards, the serial port, or connections via Bluetooth, 802.11, etc.
  – Target refers to external points of interface or reference needed to complete the semantics of the operation
  – Web access example: action="socket" source="out:inet:*:129.6.0.0/16:80" target="*"
• **X.509-formatted certificate:**

<table>
<thead>
<tr>
<th>Certificate Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the certificate</td>
</tr>
<tr>
<td>Owner</td>
<td>Owner of the certificate</td>
</tr>
<tr>
<td>Issuer</td>
<td>Issuer of the certificate</td>
</tr>
<tr>
<td>Signature Algorithm ID</td>
<td>Algorithm used for signature</td>
</tr>
<tr>
<td>Certificate Serial Number</td>
<td>Serial number of the certificate</td>
</tr>
<tr>
<td>Validity Period</td>
<td>Duration for which the certificate is valid</td>
</tr>
<tr>
<td>Attributes</td>
<td>Additional attributes related to the certificate</td>
</tr>
<tr>
<td>Issuer Unique ID</td>
<td>Unique identifier for the issuer</td>
</tr>
<tr>
<td>Extensions</td>
<td>Additional extensions related to the certificate</td>
</tr>
</tbody>
</table>

Represented in XML:

```xml
<policyEntry action="socket" source="out:inet:*:129.6.0.0/16:80" target="*" />
```

*Mobile Security Project*
Framework Recap

• Generic multi-policy level framework for centrally assigning and administering security policies on handheld devices
  – Externally represented security policy, with an extensible policy language and format
  – Multi-mode authentication and content encryption at any policy level
  – Policies can be conveyed within certificates and handled as part of a policy management infrastructure
  – Simple policy perspective for users
  – Easy to navigate among echelon levels
  – Several suitable authentication mechanisms including visual login and novel forms of smart cards
Further Information

- Wayne Jansen – Wayne.Jansen@NIST.Gov
- Project Website – http://csrc.nist.gov/mobilesecurity/publications.html