MDM, COPE, BYOD, MAM, MIM, PIM...

Peter Teufl
peter.teufl@iaik.tugraz.at
Overview

Deployment scenarios
- Managed
- COPE
- BYOD
- Consumer

Platform security
Application security
Best Practice
Managed

- Handing out devices to employees
- Devices/platform selected by company
- Ensuring that the devices comply with the security policy
- Locking down devices via Mobile Device Management (MDM), Mobile Application Management (MAM) etc.
- Enforcing password rules, remote wiping, forbidding installation sources
- Tracking
- High security can be achieved (depending on platforms etc.)
COPE

Corporately-Owned, Personally-Enabled (COPE)

- similar to managed, however, more private use cases for the employee
- still closely related to the managed scenario
- for not highly secure deployment scenarios
- security/legal issues
BYOD

Bring Your Own Device (BYOD)

- Light years away from managed/COPE
- No influence on platform security (no MDM due to legal issues)
- Application security becomes much more important (own encryption etc.)
- Current solutions...
BYOD

MDM

Container App

Smartphone

App Wrappers

Application Wrapper Management

MDM

Security

Config

App

App

App

App

Container App Management

Blackberry Balance

Business Area

MDM

Security

Config

App

App

Private Area

MAM

Security

Config

App

App

App

Smartphone

App

App

App

Smartphone

App

App

App

Smartphone

App

App
Consumer Applications

- Security critical consumer applications (e.g. banking)
  - Similar scenario as BYOD, although even less influence
  - Application security and knowledge about platform security/features
  - Detailed knowledge for security critical applications
Security

Platform security
- Security features
- User/developer influence (BYOD...)

Application security
- Secure implementations?
- Platform-specific functions

Android "Master Key" vulnerability - more malware exploits code verification bypass
Platform Security

---

Platform security

- Basic security: ALSR, DEP etc.
- Access protection (locks, encryption)
- Mobile Device Management
- Applications: sources, APIs, market
- Cloud: Push notifications, storage etc.
- Backups: local, cloud, encrypted vs. unencrypted
Basic Security

Updates?

Fragmentation: Versions, Functionality?

Operating System?

Architecture?

Malware Protection (buffer overflows, sandboxes)
Encryption/Access Protection

Notes on the implementation of encryption in Android 3.0

1. File-system? Files? Credentials?
2. Influence of the developer?
3. Always active? User interaction?
4. Hardware chip in use?
5. Encryption depends on PIN/passcode?
6. Key derivation?
7. Remote Wipe?
Mobile Device Management

Which policies?

Removing policies?

Applications, markets?

Fragmentation?

MDM - agent? OS or app based?
Applications

- Application sources?
- APIs for applications?
  - Access to SMS
  - multi-tasking
  - Permissions (Usability?)
- Developer influence on security related functions (encryption, backup)?
Secure Application Development

- Detailed knowledge about platform security and platform features
- Detailed knowledge for implementing own security functions
  - Encryption
  - Key Derivation
  - Secure Communication
  - External Commands: SMS etc.
  - Root-Checks
  - Inter-process communication

Eurograbber: A Smart Trojan Attack
Hackers’ Methods Reveal Banking Know-How
By Tracy Kitten, December 17, 2012. Follow Tracy @FraudBlogger
Example

Container applications

Key Derivation (Password to key...)
key security function on encryption systems

Key Derivation

   - Salt

   - Long derivation times (e.g., 80ms per passcode)

   - Know-How to get it right...

   - Mistakes: easy brute-force “gentle-force” attacks
## Example

<table>
<thead>
<tr>
<th>Lock-Screen Type</th>
<th>Length</th>
<th>Chars</th>
<th>Number of passcodes</th>
<th>Brute-Force Days</th>
<th>Cost $ GPU</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Numerical</strong></td>
<td>4</td>
<td>10</td>
<td>10000</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>10</td>
<td>1000000</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>10</td>
<td>100000000</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10</td>
<td>100000000000</td>
<td>0.2</td>
<td>0.0</td>
</tr>
<tr>
<td><strong>Alphanum</strong></td>
<td>4</td>
<td>36</td>
<td>1679616</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>10/26 letters</td>
<td>6</td>
<td>36</td>
<td>2176782336</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>36</td>
<td>78364164096</td>
<td>1.3</td>
<td>0.2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>36</td>
<td>2.82111E+12</td>
<td>46.6</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>36</td>
<td>1.0156E+14</td>
<td>1,679.2</td>
<td>299.0</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>36</td>
<td>3.65616E+15</td>
<td>60,452.4</td>
<td>10,763.7</td>
</tr>
<tr>
<td><strong>Alphanum</strong></td>
<td>4</td>
<td>62</td>
<td>14776336</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>10/52 letters</td>
<td>5</td>
<td>62</td>
<td>916132832</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>62</td>
<td>56800235584</td>
<td>0.9</td>
<td>0.2</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>62</td>
<td>3.52161E+12</td>
<td>58.2</td>
<td>10.4</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>62</td>
<td>2.1834E+14</td>
<td>3,610.1</td>
<td>642.8</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>62</td>
<td>1.35371E+16</td>
<td>223,827.5</td>
<td>39,852.9</td>
</tr>
<tr>
<td><strong>Complex</strong></td>
<td>4</td>
<td>107</td>
<td>131079601</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>107</td>
<td>14025517307</td>
<td>0.2</td>
<td>0.0</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>107</td>
<td>1.50073E+12</td>
<td>24.8</td>
<td>4.4</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>107</td>
<td>1.60578E+14</td>
<td>2,655.1</td>
<td>472.7</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>107</td>
<td>1.71819E+16</td>
<td>284,091.6</td>
<td>50,583.1</td>
</tr>
</tbody>
</table>
Platform vs. App Security

Managed Devices (MDM), COPE

- Platform Security
- Application Security

BYOD

- Platform Security
- Application Security

Consumer

- Platform Security
- Application Security