Protecting Mobile Apps and security in the context of Bring Your Own Device

Shane Williams
THE BASICS AND BACKGROUND
Basics – Security is the same

Confidentiality

LOSS = unauthorized disclosure of information.
Basics – Security is the same

Availability

LOSS = disruption of access to or use of information or an information system.
Basics – Security is the same

Integrity

LOSS = unauthorized modification or destruction of information
Basics – Security is the same

Confidentiality
LOSS = unauthorized disclosure of information.

Integrity
LOSS = unauthorized modification or destruction of information

Availability
LOSS = disruption of access to or use of information or an information system.
Threat paths

Threat Agents

Attack Vectors

Security Weaknesses (Vulnerabilities)

Weakness

Security Controls

Control

Technical Impacts

Business Impacts
Threat paths

- Threat Agents
- Attack Vectors
- Security Weaknesses (Vulnerabilities)
- Security Controls
- Technical Impacts
- Business Impacts
Threat paths

Threat Agents

Attack Vectors

Security Weaknesses (Vulnerabilities)

Security Controls

Technical Impacts

Business Impacts

Attack

Weakness

Control

Attack

Weakness

Control

Attack

Weakness

Control
Threat paths

Threat Agents

Attack Vectors

Security Weaknesses (Vulnerabilities)

Security Controls

Technical Impacts

Business Impacts

Threat-Source

Attack

Weakness

Control

Asset

Impact

Attack

Weakness

Control

Function

Impact

Attack

Weakness

Control

Asset

Impact

Weakness

Control

Asset

Impact
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

ISO 13335 – Information Technology Security Techniques
Top 10 Mobile Risks

1. Insecure Data Storage  
   - Data at rest control
2. Weak Server Side Controls  
   - Bypass client to attack
3. Insufficient Transport Layer Protection  
   - Over-the-wire
4. Client Side Injection  
   - XSS, etc.
5. Poor Authorization and Authentication  
   - Low factors
6. Improper Session Handling  
   - Allow Hijacking
7. Security Decisions Via Untrusted Inputs  
   - Keyboards
8. Side Channel Data Leakage  
   - Listening, in-Sophisticated
9. Broken Cryptography  
   - Easily breakable, WEP
10. Sensitive Information Disclosure  
    - Data leakage, Social
Attacks
Attacks
Attacks 2013
Attacks

**Attack Confidentiality**
- Eavesdrop/Copy

**Attack Integrity**
- Stop/Delay/Modify
- Masquerade/Assume identity/Authenticity

**Attack Availability**
- Destroy channel, corrupt, overwhelm
- Eavesdropping
- No Physical Boundaries
- Tracing/Tracking
- Device Capture
- SSL Stripping
- Reputation
- Fraud (Monetary/Identity)
- Browser icons common

Attacks Integrity
- Distributed Denial of Service
- Bandwidth Constraints
- Interference and Jamming
Recent Real World Examples

• Feb 2013 – Watering Hole attack

• Notable and news worthy
SECURITY CONTROLS
Security controls

Platform Controls

Custom Controls
Custom controls

BYOD
- Personal Data
- Company Data

LOA2+
- Client Data
- Employee Data
## NIST Levels of Assurance (LOA)

<table>
<thead>
<tr>
<th>Level of Assurance</th>
<th>Data Classification</th>
<th>Data Examples</th>
<th>Cumulative Authentication Requirements</th>
<th>Authentication Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0 – No knowledge of identity.</td>
<td>Public Anonymous</td>
<td>Public Website</td>
<td>None</td>
<td>Public website</td>
</tr>
<tr>
<td>L1 - Little or no confidence in the asserted identity’s validity.</td>
<td>Public</td>
<td>Public discussion forum</td>
<td>One of any factor</td>
<td>Username + password i.e. something you know</td>
</tr>
<tr>
<td>L2 - Some confidence in the asserted identity’s validity.</td>
<td>Internal</td>
<td>Team process documents in SharePoint</td>
<td>One of any factor Verified identity</td>
<td>Username + password i.e. something you know, checked against company HR controlled LDAP directory.</td>
</tr>
<tr>
<td>L3 - High confidence in the asserted identity’s validity.</td>
<td>Confidential</td>
<td>Company strategy presentation</td>
<td>Two or more of any factor</td>
<td>Password protected X509 soft certificate, is both something you have and something you know.</td>
</tr>
<tr>
<td>L4 – Very high confidence in the asserted identity’s validity.</td>
<td>Strictly Confidential</td>
<td>Client or employee identifying documents</td>
<td>Two or more factors One hard FIPS 140-2 token Independent reader</td>
<td>Password protected smartcard over reader with button</td>
</tr>
</tbody>
</table>

**Factors:** something you know (username, password), you have (smartcard), you are (fingerprints)
Control categories

- Secure Boot
- Code Protection
- Data Protection
- Mobile Management
- Server Protection
Secure Boot – Apple Example

- Protecting low level to create start of a chain of trust
- Processor boots from read-only boot ROM – trusted – Protects Integrity
- Contains the Apple Root CA
  - Verifies Low-Level boot loader is signed by Apple
  - Secure boot chain ensures lowest levels of software are tamper free
  - Boot process ensures only Apple signed code can run on the device
- Jailbreaks have exploited boot loader vulnerabilities
Code Protection

Platform

- Signed application
- Vetted applications
- ASLR
- Application sandboxing
Code Protection

Custom

- Static code analysis
- Code obfuscation
- Jailbreak Detection
- Trusted Execution Environment
- Anti-malware
Code Protection

**Platform**
- Signed application
- Vetted applications
- ASLR
- Application sandboxing

**Custom**
- Static code analysis
- Code obfuscation
- Jailbreak Detection
- Trusted Execution Environment
- Anti-malware
DATA Protection

Platform

- User Authentication
- Hardware Encryption
- Device VPN
Data Protection - Encryption

Hybrid
- Symmetric
- Asymmetric

Homomorphic
Data protection

Custom

- Container FIPS 140-2 Encryption
- Container Tunnels
- Digital Rights Management
- Secure Tokens & OS
Data Protection - Encryption

App Code

PKCS#11 over PS/SC

HW Crypto API

Effaceable Memory

Keys
### Data Protection - Authentication

#### Top 20 used pins...do you have one?

<table>
<thead>
<tr>
<th>PIN</th>
<th>Freq</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>1234</td>
</tr>
<tr>
<td>#2</td>
<td>1111</td>
</tr>
<tr>
<td>#3</td>
<td>0000</td>
</tr>
<tr>
<td>#4</td>
<td>1212</td>
</tr>
<tr>
<td>#5</td>
<td>7777</td>
</tr>
<tr>
<td>#6</td>
<td>1004</td>
</tr>
<tr>
<td>#7</td>
<td>2000</td>
</tr>
<tr>
<td>#8</td>
<td>4444</td>
</tr>
<tr>
<td>#9</td>
<td>2222</td>
</tr>
<tr>
<td>#10</td>
<td>6969</td>
</tr>
<tr>
<td>#11</td>
<td>9999</td>
</tr>
<tr>
<td>#12</td>
<td>3333</td>
</tr>
<tr>
<td>#13</td>
<td>5555</td>
</tr>
<tr>
<td>#14</td>
<td>6666</td>
</tr>
<tr>
<td>#15</td>
<td>1122</td>
</tr>
<tr>
<td>#16</td>
<td>1313</td>
</tr>
<tr>
<td>#17</td>
<td>8888</td>
</tr>
<tr>
<td>#18</td>
<td>4321</td>
</tr>
<tr>
<td>#19</td>
<td>2001</td>
</tr>
<tr>
<td>#20</td>
<td>1010</td>
</tr>
</tbody>
</table>

![PIN frequencies](image)

**No Password**

**Long Password**

**Ease of use**

**Protection**
Data Protection - Authentication

- Mutual
- Negotiated
- SSO
- Federated
- Delegated
Data protection

Platform
- User Authentication
- Hardware Encryption
- Device VPN

Custom
- Container FIPS 140-2 Encryption
- Container Tunnels
- Digital Rights Management
- Secure Tokens & OS
Mobile Management

Platform

Mobile Device Management
Mobile Management

Custom

Mobile Application Management

Mobile Hypervisor Management
Mobile Management

Platform
- Mobile Device Management

Custom
- Mobile Application Management
- Mobile Hypervisor Management
Securing Access to Services

Diagram:
- Internet
- Reverse Proxy
- Application Server

Steps:
1. Internet
2. Reverse Proxy
3. Application Server
Securing Access to Services

- Risk Assessment
Securing Access to Services

- Black Hats and White Hats
Securing Access to Services

- Penetration Test
Closing Thoughts

- You get a lot without trying on mobile platform
- You have to spend the effort on the controls (Client / Server)
- Technology is improving to support security
Thank You!
And Stay Safe

Shane Williams