Mobile Application Security Sharing Session
May 2013
Agenda

Introduction of speakers
Mobile Application Security – Trends and Challenges
5 Key Focus Areas for an mobile application assessment
Introduction of speakers

Felix Kan (Senior Consultant, PwC)

- PwC Global Mobile Core Team
- Certified Ethical Hacker (CEH)
Mobile application security

Trends and Challenges
Trends and Challenges

Overall

Applications
- Security design
- Secure coding
- Data protection
- Mobile application protection

Device
- Security features
- Mobile device management
- Use case in business contexts

Network
- Communication security
- Protocols
- Cellular carriers’ offerings

We should stay succinct in this section…
Trends and Challenges
Applications

- Offline access to data
- Anti-virus / malware
- Device compromise detections
- Social media apps
- Hidden (premium) features
**Trends and Challenges**

**Applications**

**Offline storage – Why?**
- Presentations
- Edit offline

**The Challenges**
- Remote wipe?
- Data leakage
- Identity thefts

**Trends**
- Business applications enable business intelligence reports – store corporate data **and** credentials
# Trends and Challenges

## Applications

<table>
<thead>
<tr>
<th>Why anti-malware?</th>
<th>Is it working?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compensation</td>
<td><strong>Bouncer</strong>, an in-house malware discovery tool of Google, could be bypassed by malwares that “play dead” for 5 min.</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Why malware?</td>
<td></td>
</tr>
<tr>
<td>Approval process</td>
<td></td>
</tr>
<tr>
<td>Sandbox design</td>
<td></td>
</tr>
<tr>
<td>Code signature</td>
<td></td>
</tr>
</tbody>
</table>

- **Device**
  - Security features
  - Mobile device management
  - Use case in business contexts

- **Network**
  - Man-in-the-middle attacks
  - Denial-of-service
  - Cellular carriers’ offerings
Trends and Challenges
Applications

JB detection - Why?

Reduce attack surface

The Challenges

Application integrity

Trends

Hacking tools can be downloaded to go around the JB detection and other validation logic (e.g., in-app purchase)

Device
- Security features
- Mobile device management
- Use case in business contexts

Network
- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings
**Trends and Challenges**

**Applications**

**Self destructed media**

- For fun
- Private communications
- Traceability
- Data leakage

**The Challenges**

- More sophisticated options are available for self destructed communications (e.g., encryptions)

**Trends**

- Security features
- Mobile device management
- Use case in business contexts

**Network**

- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings
Hidden features – Why?

Trends

Back doors are not uncommon in mobile;
Premium features are locked unless users have paid.
Challenges

A Chicago-based digital forensics company performed a 2010-2011 assessment and discovered the following mobile statistics:

- 76% of Android and iOS apps store Usernames in clear text on mobile devices

- 10% of Android and iOS apps store Passwords in clear text on mobile devices


PwC
“SQL injection attacks, cross-site scripting, authentication bypass, and exploitation of session variables contributed to nearly half of breaches attributed to hacking or network intrusion. It is no secret that attackers are moving up the stack and targeting the application layer.

Why don’t our defences follow suit?”
**Trends and Challenges**

**Device**

- Enhanced security features on device
- QR reader
- Device tracking
- Data forensics

**Applications**
- Security design
- Secure coding
- Data protection
- Mobile application protection

**Network**
- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings
**Trends and Challenges**

**Device**

**Applications**
- Security design
- Secure coding
- Data protection
- Mobile application protection

**Network**
- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings

**Jailbreak: Why?**
- Free Apps
- Awesome utilities

**Jailbreak: So?**
- Data leakage
- Identity thefts

**And the Demand:**

**JB tool** was installed for **4M** devices – by US and China users.
Similarly...

- Free Apps
- Awesome utilities

Additionally...

- Security features
- Bloatware
- Performance

Fundamentally...

- Full disk encryption is not available
- Data on SD card can be stolen
- 580% increase of malware in 2012.

Applications
- Security design
- Secure coding
- Data protection
- Mobile application protection

Network
- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings
Trends and Challenges

Device

Applications
- Security design
- Secure coding
- Data protection
- Mobile application protection

QRishing”: Phishing with QR code

Scan code with your smartphone to access our mobile website

Network
- Man-in-the-middle attacks
- Denial-of-service
- Cellular carriers’ offerings
Trends and Challenges

Device

Apps gathering your PII

iOS 6
- more granular privacy controls
- From UDID to IDFA (Identifier for Advertising)

Mobile device management
- GPS tracking
**Trends and Challenges**

**Device**

**Forensic on smart phones**

**Android**

- Multiple tools available: XTC clip
- File extractions in recovery mode (yes, bypassing the device passcode)
- Boot into “HBOOT” mode and run “fastboot” command

**iOS**

- Data recovery for deleted files (passcode required)
Mobile application security

5 Key Focus Areas for an mobile application assessment
5 Key Focus Areas

- Security strategy
- Defined mobile security platform architecture
- Application security assessment
- Application provisioning
- Software development life cycle
Security across mobility requires an examination of the various layers across the mobile ecosystem

Security strategy and governance

Policies, standards, and procedures

Mobile security platform architecture

* Mobile Devices include Smartphones, tablets and supporting devices
Pain points of secure application development process

In order to satisfy market demand and reap the benefits of mobile technology, organizations are often pushing these applications to production without considering security imperatives. The questions to the right are often present in client environments as they implement mobile solutions.

While many traditional web application vulnerabilities remain present in the mobile environment, mobile-specific challenges must also be addressed.

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>• What is the sensitivity of the data that will be accessed by the mobile applications?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient Risk Assessments</td>
<td>• What are the potential consequences that an application data breach may have on the organization?</td>
</tr>
</tbody>
</table>
| Aligning Security Controls with Risk Appetite | • What regulatory requirements exist for relevant sensitive data?  
• What security controls should be implemented in accordance with regulations and risk appetite? |
| Insecure Data Storage | • Does the business case require storage of data on the device?  
• Can the application function locally and without server connectivity?  
• Is all stored data sufficiently encrypted? |
| Application Reverse Engineering | • Can attackers access the application flow and create duplicates?  
• Can attackers reverse engineer the application to circumnavigate security controls? |
Mobile Application Security Considerations:

- Mobile security controls should be considered throughout every step of the SDLC to enhance secure development.

- Mobile application developers along with Infrastructure and Information Security personnel should consider implementing controls of the following domains as deemed appropriate by risk.
Considerations—Developers

- Storage
- Authentication
- Authorization
- Session Management
- Audit / Logging
- Memory
- Miscellaneous

Mobile Application SDLC Components
- Security Management
- Infrastructure

Developers

Architecture
Considerations–Architecture

Security  Maintainability
Scalability  Availability

Developers  Architecture
Mobile Application SDLC Components
Security Management  Infrastructure

PwC
Considerations—Infrastructure

Access to Network Resources  Application Behavior

Firewalls

Developers  Architecture
Mobile Application SDLC Components
Security Management  Infrastructure
Considerations–Security Management

Privacy Policies

Risk Assessments

Application Behavior

Developers

Architecture

Mobile Application SDLC Components

Security Management

Infrastructure
Application provisioning

Apps Classification

Access Control

Mobile Device Management
**Application security assessment**

**Model Threats**
- Gather prerequisite information about the application and systems supporting the application to develop appropriate testing scenarios
  - Identify relevant threats
  - Determine applicable testing scenarios and attack vectors

**Targeted Automated Scanning**
- Perform targeted automated scanning against the mobile application’s web services and input fields for known vulnerabilities.

**Advanced Manual Attacks**
- Attempt to circumvent mobile application controls
  - OWASP top 10 mobile risks
  - Native application and web-based attacks
  - Network-based attacks
  - Privilege escalation
  - Identify sensitive data remaining on the device

**Remediation Validation**
- Conduct retesting of high and medium risk vulnerabilities to ensure defects have been adequately addressed

May 2013
# Mobile Top Ten security risks

Common mobile application flaws published by industry groups, including the Open Web Application Security Project (OWASP) Mobile Top Ten security risks

<table>
<thead>
<tr>
<th></th>
<th>Insecure or unnecessary client-side data storage</th>
<th></th>
<th>Client-side injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Lack of data protection in transit</td>
<td></td>
<td>Client-side DOS</td>
</tr>
<tr>
<td>3</td>
<td>Personal data leakage</td>
<td></td>
<td>Malicious third-party code</td>
</tr>
<tr>
<td>4</td>
<td>Failure to protect resources with strong authentication</td>
<td></td>
<td>Client-side buffer overflow</td>
</tr>
<tr>
<td>5</td>
<td>Failure to implement least privilege authorization policy</td>
<td></td>
<td>Failure to apply server-side controls</td>
</tr>
</tbody>
</table>

May 2013