Building a Mobile App Security Risk Management Program
Your Presenters

Who Are We?

Chris Salerno, Consultant, Security Risk Advisors
- Lead consultant for mobile, network, web application penetration testing
- Researcher and director of content and knowledge management
- 100’s of penetration tests, web, and mobile applications assessments
- PCI Security Assessments and technical security workshops

Vas Rajan, CISO, ING Direct US
- Over 18 years of IT security, operations, application development and consulting experience
- Responsible for compliance with PCI, FFIEC and oversees eDiscovery and information lifecycle management

Copyright © 2012, Security Risk Advisors, Inc. All Rights Reserved
Mobile Security Risk Management

What are we Talking About?

- Driving the Program
- MEAPs
- Contrasting Application Types
- Example Process Flow
- Developing the Application
- Assessing the Solution
- Defending and Monitoring
- Securing new Technologies
- Drawing Conclusions
Mobile Application Risk Management

Driving the Program

Drivers
1. Customer Driven
2. Competitive Advantage
3. Security and Privacy

1. Vision
   - Drivers and Objectives
   - Sponsorship
   - Requirements
   - Peer Benchmarks

2. Design
   - App dev standards
   - Evaluate MEAPs and dev. partners
   - Design services infrastructure

3. Build
   - Procure / build services infrastructure
   - Publish re-usable service endpoints
   - Develop and publish apps
Mobile Application Risk Management

MEAP

MEAP (Mobile Enterprise Application Platform)

- Mobile Middleware
- Service Endpoints
- Authentication and Authorization services
- Mobile Development
- Mobile Management

When Selecting, Look For:

- Cross Platform and Device Support
- Multiple Application Type Support
- Secure and Scalable Back-End System Connections
- Industry Standard Encryption
## Contrasting Application Types

### Native and HTML5 / CSS

### Native

- Traffic can be encrypted end-to-end with more secure protocols
- Advanced device fingerprinting
- Certificate Validation
- Custom “Look and Feel” options

### HTML5 / CSS

- More data stored on device
- Harder to monitor user activity
- Platform specific code changes required
- Forcing application updates can be difficult
- More “new” code introduced

- On-device sensitive information storage can be limited
- Back-end application logic already exists and vetted
- Cross-platform compatibility
- Application always updated
- No App Store approvals
- No mobile coding expertise required

- Relying on device browser
- No rooted or jailbreak detection
- Easier MITM attacks
- Limited functionality options
## Hybrid Model

### Hybrid

- Look and feel of a native application
- On-device sensitive information storage can be limited
- Back-end application logic already exists and vetted
- Utilize existing internal developer knowledge
- Still able to do rooted and jailbreak detection
- Potential for “tiered” authentication approach

### Limitations

- Still requires some mobile coding expertise
- Existing MEAP platforms are immature
- Forcing application updates can be difficult
Selecting the Components

Example Process Flow

A. User requests access and authenticates to MEAP server
B. MEAP Server calls Token Server to create / retrieve Token from DB
C. Session Token passed to Web Application
D. Web Application verifies Session Token and returns content
Mobile App Development

Mobile Security Standards

Why Standardize?

- 3rd parties may need to be involved in coding
- Secure mobile code repository

Developer Expectations

- **Internal**: Existing code expertise, bridging the gap between mobile and web
- **MEAP**: Provide a platform, lead mobile component coding, work closely with in-house experts, integrate business and security requirements

Secure Coding Standards

- Common set of principles (e.g. authentication, authorization, input validation)
- Security considerations unique to each platform
- Leverage MEAP and open-source secure coding resources (e.g. SANS)
- Key off of good web application practices
- Model threats and address risks specific to your business
Mobile App Development

iOS and Android Security Standards

- Apple Memory Extraction
- Caching of Screenshots
- Custom URL Handlers
- Runtime attacks
- Data Protection API for keychain items and files
- Apple Dynamic Dictionary

- Input Validation
- Client-Side Injection
- Hard-Coded Credentials
- On-Device Data Protection
- Authentication/Authorization
- Strong Transport Encryption
- Error Handling & logging
- Test/Debug Functionality
- Geo-location Services
- Session Mgmt

- Droid Memory Extraction
- Droid Component Abuse & Permissions
- Exportable Components
- Debug Flags
- Code Obfuscation
- Droid File Permissions
Mobile App Security Testing

Creating the Capability

- Leverage existing in-house web application security knowledge
- Work with developers and business units
- Insert the security team into sprints and releases

On-Device
- Memory Analysis
- App Sandbox
- Global Files
- Jailbreak / Root

Static
- Source Code Analysis
- Commercial Analysis Tools
- Reverse Engineering

Dynamic
- MITM (Proxy)
- Business Logic
- Runtime Analysis
- Mobile SDK Tools

Copyright © 2012, Security Risk Advisors, Inc. All Rights Reserved
Mobile App Security Testing

Common Examples: Memory

```
01-19 13:21:09.583  2866 2866 D BankApp :{"ContinuationKey":"-3df34a5a:134ed49ddc2:=-4314|18203894|CU","InteractionId":"18203894","DeviceInfo":{'DeviceToken":"PMV31toKjdZ/8NE00M5sZ9mEdqzjbiwKQnBKWjrZsIVHOkDFTRuL6lUgCZLaloukdvUCVOiBTZ9ENJw+ANwSGo44IQ==","Bound":"false","Current":"false","User ID":"58","PIN":"123321","LastName":"Testman","VerifyNewApplicant":"false"}},info:[]},responseID:660,statusCode:200,errors:[],"isSuccessful":true,"statusReason":"OK","FirstName":"Mark","Question2":{"Text":"What was your favorite sport you played as a child?","Id":"Q8.4"},"AuthenState":"Continue","ActivityGroupId":"11941573","Question1":{"Text":"What was your favorite childhood television show?","Id":"Q8.3"},"warnings":[]},"InfoType":""}
```

Copyright © 2012, Security Risk Advisors, Inc. All Rights Reserved
Mobile App Security Testing

Common Examples: Database
Mobile App Security Testing

Common Examples: Screenshot
Defending and Monitoring Tools and Techniques

Fraud Rules

- Traditional fraud rules apply
- Educating the fraud team how to recognize a mobile device attack
- Early Warning
- Silvertail and others

Screen Scraping

- TeaLeaf and others: Ability to trace activity

IDS/IPS

- Monitor excessive requests and scripting attempts
- Rate throttling the API requests
Mobile App Security Testing

Securing Mobile Payments

Instant P2P Payments (Bump)
- Using unique ID's
- Bump Jacking; Use protection when you Bump
- XSS...Again
- Information stored in client side log files

Mobile Check Deposits
- Curious customers will do the testing for you
- The same check fraud issues apply
  - Verifying check authenticity
  - Confirming account balances (The $200 rule)
- Capacity planning for increased usage
- Making sure that current fraud tools are ready for mobile check processes
- Those check images are stored somewhere (lock down your shares)
Mobile Application Risk Management

Drawing Conclusions

- Pick a model
- Select a MEAP

- Design

- Pick a model
- Select a MEAP

- Deploy
  - Continuous Monitoring
  - App Enhancements

- Develop
  - Identify Platforms
  - Address Skill Gaps
  - Secure Coding Standards

- Monitor
  - Monitor attacks / fraud
  - Remediate Common Mobile Vulnerabilities

- Assess
  - Test the Application
  - Assess end-points
  - Assess infrastructure
Q&A
You Ask, We Answer

Mobile Security
✓ Mobile security strategy
✓ Policy and controls expertise
✓ Development standards
✓ Mobile app security testing

DLP & Data Protection
Data Loss Prevention (DLP)
✓ requirements and selection
✓ DLP implementation
✓ DLP process improvement

Technical Assessment
✓ Penetration testing
✓ Web application security
✓ Cloud applications
✓ SAP risk assessment
✓ Product security architecture

PCI & Compliance
PCI gap analysis
✓ Remediation assistance
✓ Scope reduction advice
✓ ISO, FFIEC, HIPAA/HITECH
✓