LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

OWASP NZ Day 2011

Testing Mobile Applications

Presenter: Nick von Dadelszen

Date: 7th July 2011

Company: Lateral Security (IT) Services Limited

LATERAL | SECURITY

Company overview

- Company
  - Lateral Security (IT) Services Limited
  - Founded in April 2008, offices in Wellington and Auckland
  - Directors Ratu Mason and Nick von Dadelszen
- Services
  - Information security testing (design, architecture, penetration testing, security controls, policy and compliance)
  - Lifecycle auditing (design, pre prod, post prod)
  - Regular ongoing testing programmes
- Differentiators
  - True vendor independence
  - Security testing is our unique specialty
  - Very highly skilled staff

LATERAL | SECURITY

Agenda

- Why mobile apps
- How to test
  - Attacking the communication
  - Attacking the server
  - Attacking the client
    - iPhone
    - Android
- What to test for
- Roundup
  - What we talked about
  - What we didn’t talk about

LATERAL | SECURITY

Why Mobile Apps

- Everyone is developing Mobile apps these days
  - Banks
  - Travel industry
  - Trademe
  - Subway
- Not Web Apps
- Similar to my Kiwicon 2007 Fat Client talk BUT
  - Mobile apps generally customer facing

LATERAL | SECURITY

How To Test

- Two different approaches to testing:
  - Whitebox testing
    - Full information and source code provided
  - Blackbox testing
    - No code or information provided
    - Working only with downloadable app
- Three areas to focus on:
  - Attack the network communication
  - Attack the server component
  - Attack the client component

LATERAL | SECURITY

Attacking The Communication

- Need to check how information is passed between the client and server
  - Is it encrypted?
  - Can it be MITMed?
  - What authentication is performed for network traffic?
- If HTTP protocol is used several methods to intercept traffic
  - Configure HTTP proxy on phone/emulator
  - Use tool such as Burp in reverse proxy mode

LATERAL | SECURITY

Attacking the Communication

- If URL is hard coded and app doesn't use system proxy:
  - If FQDN use hosts file on devices (need root)
  - If fixed IP use wifi gateway to redirect to fake server
- Or use Mallory
  - Works as a gateway
  - Pipes all traffic through the tool
  - Able to analyse non-standard traffic
  - Able to identify apps that send personal data

LATERAL | SECURITY

Attacking the Server

- In most cases this is:
  - Standard HTML over HTTP
  - XML/SOAP over HTTP
- Follow standard web application or web service attack methodology
- Sometimes proprietary
  - Have not had to review one of these in mobile space
- Have to reverse protocol etc

LATERAL | SECURITY

Attacking the Client - iPhone

- Whitebox approach:
  - Load source into Xcode
  - Can run in simulator for ease of testing
  - Can review source directly
- Blackbox approach:
  - Cannot load app into simulator
  - Can get app from phone and reverse

LATERAL | SECURITY

iPhone Simulator

LATERAL | SECURITY

Sharing iPhone Simulator App

- **Trick: You can share a iPhone simulator app without having to share the source code:**
  - Run code in simulator on local machine
  - Copy the following folder to other testers:
    - Library/Application Support/iPhone Simulator/<version>/Applications/<unique id>

LATERAL | SECURITY

Reversing An iPhone App

- Obtain app from phone or download
  - From phone
    - Use a tool called iPhone Explorer
    - Doesn’t need to be jailbroken
    - Get .app file
- .app is simply archive file so can view package contents
- **Trick: iPhone only checks signatures during install so you can modify files and reload them onto the phone.**
- iPhone applications can be reversed using otool provided with Xcode

LATERAL | SECURITY

Demo – Modifying An iPhone App

Attacking the Client - Android

- Whitebox approach:
  - Load source into Eclipse
  - Can run in emulator for ease of testing
  - Can review source directly
- Blackbox approach:
  - Can get .apk file from phone and reverse
  - Can load .apk file directly into emulator

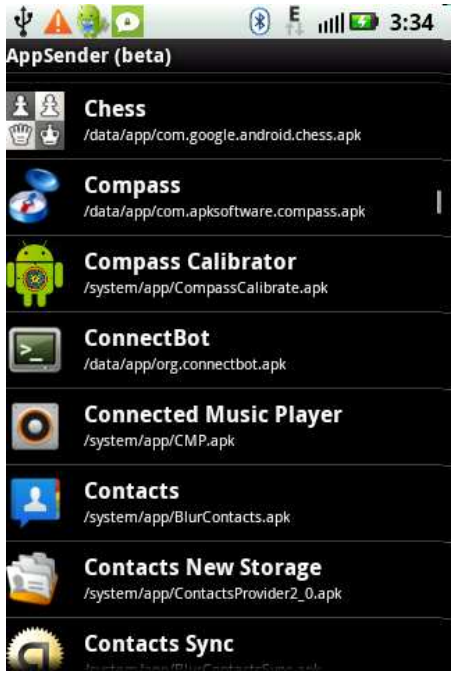
LATERAL | SECURITY

Android Emulator

LATERAL | SECURITY

Obtaining .APK Files

- **TRICK: If you need to get an .apk file off an Android phone but don't want to root it:**
  - Get the AppSender app
  - Use the app to get the full path to .apk file



  - Use ADB to get file
    - Adb pull /data/app/<.apk filename>

LATERAL | SECURITY

Installing .APK Files In Simulator

- List devices with ADB
  - # adb devices
- Devices will be emulator or physical device
- Install .apk file into specific device
  - # adb –s <device serial> install <path_to_apk>
- ABD can also be used to run shell commends on the device
  - # adb –s <device serial> shell

LATERAL | SECURITY

Decompiling Android Apps

- .apk files are just .zips
- Pull out the .dex files
- Use baksmali to decompile to smali assembly

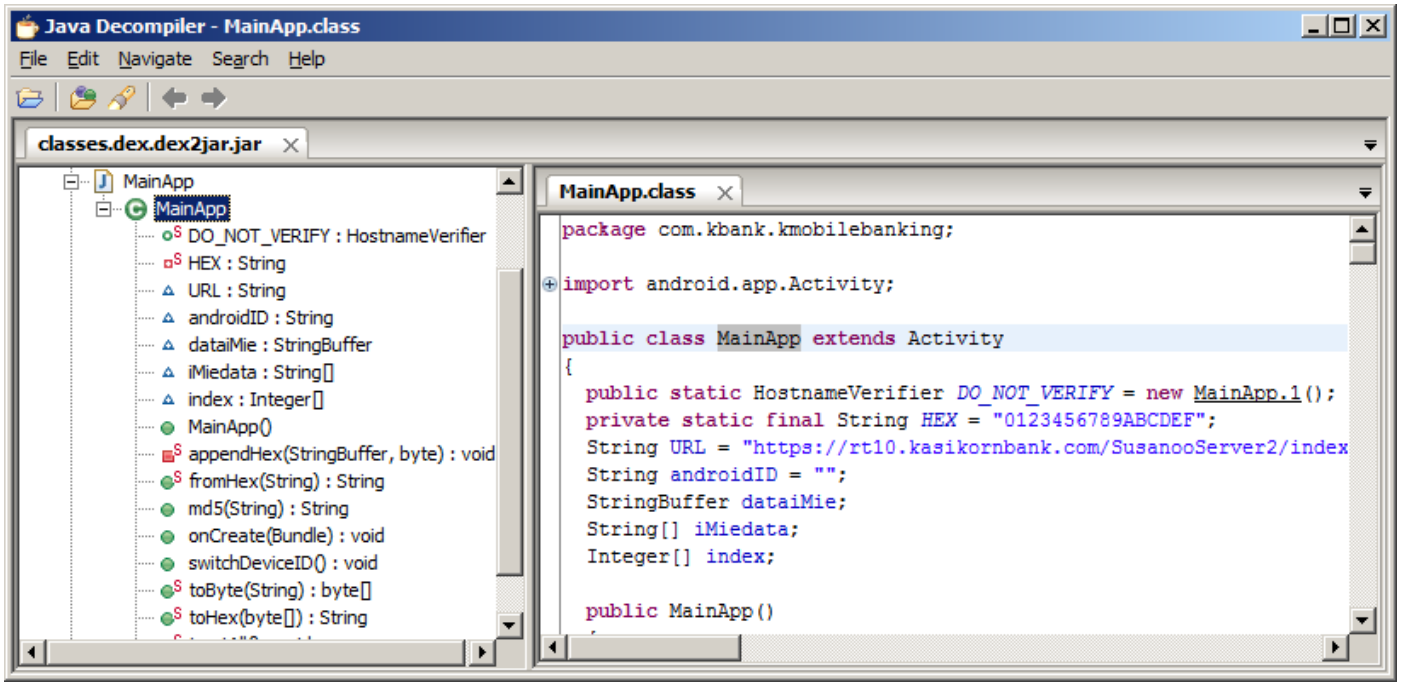
MainApp.smali

```
.class public Lcom/kbank/kmobilebanking/MainApp;
.super Landroid/app/Activity;
.source "MainApp.java"


# static fields
.field public static DO_NOT_VERIFY:Ljavax/net/ssl/HostnameVerifier; = null

.field private static final HEX:Ljava/lang/String; = "0123456789ABCDEF"


# instance fields
.field URL:Ljava/lang/String;

.field androidID:Ljava/lang/String;

.field dataiMie:Ljava/lang/StringBuffer;

.field iMiedata:[Ljava/lang/String;

.field index:[Ljava/lang/Integer;

```

LATERAL SECURITY

Decompiling Android Apps

- Use dex2jar to get Java classes
- Use Java decompiler such as JD to get Java source



LATERAL SECURITY

Modifying And Recompiling Apps

- Android-APKtool can decompile and recompile .apk files
- Provides AndroidManifest.xml in readable format
- Can modify and rebuild the app
- Must manually sign app after rebuild

LATERAL | SECURITY

Demo – Recompiling An Android App

What To Test For

- Number 1 rule:

NEVER TRUST DATA FROM THE CLIENT!

LATERAL | SECURITY

OWASP Mobile Top Ten *

1. Insecure or unnecessary client-side data storage
2. Lack of data protection in transit
3. Personal data leakage
4. Failure to protect resources with strong authentication
5. Failure to implement least privilege authorization policy
6. Client-side injection
7. Client-side DOS
8. Malicious third-party code
9. Client-side buffer overflow
10. Failure to apply server-side controls

* Still draft

LATERAL | SECURITY

Client-Side Storage

- iPhone:
  - Citi mobile app issue
  - SQLite databases
  - Snapshots
  - Copy and Paste
  - Keyboard cache
  - Cached files
  - Logs
- Android
  - SQLite databases
  - Logs

LATERAL | SECURITY

Demo – iPhone Storage

Application Permissions

- Android
  - AndroidManifest.xml permissions
    - SMS trojans in the wild
    - Wallpaper apps
- File permissions
  - Android
    - Skype for Android vuln

LATERAL | SECURITY

Examples Of Issues Found

- Use of UUID for authentication
- Logging of sensitive information
- CSRF in mobile app
- Lots of issues with server trusting client
- Hardcoded credentials

LATERAL | SECURITY

Roundup

- What we talked about
  - How to test
  - What to test for
- What we didn’t talk about
  - Blackberries
  - Platform security
  - Mobile access to corporate data

LATERAL | SECURITY

Resources - Information

- OWASP Mobile Security Project
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- Foundstone papers
  - http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pen-testing-iphone-ipad-apps.pdf
  - http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pen-testing-android-apps.pdf

LATERAL | SECURITY

Resources - Tools

- Mallory
  - http://intrepidusgroup.com/insight/mallory/
- Baksmali
  - http://code.google.com/p/smali/
- Android-apktool
  - http://code.google.com/p/android-apktool/
- iPhone Explorer
  - http://www.macroplant.com/iphoneexplorer/

LATERAL | SECURITY

Questions

- Anything else you want to know?

LATERAL | SECURITY

Contact Details

Wellington	38-42 Waring Taylor Street
	Petherick Tower, level 7
	PO Box 8093
	The Terrace, Wellington 6143
Phone:	+64 4 4999 756
Auckland	187 Queen Street
	Landmark House, level 8
	PO Box 7706
	Wellesley Street, Auckland
Phone:	+64 9 377 0700
Presenter	nick@lateralsecurity.com
Web	www.lateralsecurity.com

LATERAL | SECURITY