SMART BOMBS
Mobile Vulnerability and Exploitation

John Sawyer – InGuardians
Tom Eston – SecureState
Kevin Johnson – Secure Ideas
John Sawyer

- InGuardians, Inc. - Senior Security Analyst
- DarkReading.com - Author/Blogger
- 1@stplace - Retired CTF packet monkey
  - winners DEFCON 14 & 15
- Avid Mountain Biker…in Florida.
Tom Eston

- Manager, SecureState Profiling & Penetration Team
- Blogger – SpyLogic.net
- Infrequent Podcaster – Security Justice/Social Media Security
- Zombie aficionado
- I like to break new technology
Kevin Johnson

- Father of Brenna and Sarah
- Secure Ideas, Senior Security Consultant
- SANS Instructor and Author
  - SEC542/SEC642/SEC571
- Open-Source Bigot
  - SamuraiWTF, Yokoso, Laudanum
- Ninja
What are we talking about today?

- What’s at risk?
- Tools, Testing and Exploitation
- Common vulnerabilities found in popular apps (this is the fun part)
What are Smart Bombs?

- We’ve got powerful technology in the palm of our hands!
- We store and transmit sensitive data
- Mobile devices are being used by:
  - Major Businesses (PII)
  - Energy Companies (The Grid)
  - The Government(s)
  - Hospitals (PHI)
  - Your Mom (Scary)
That’s right...your Mom
Testing Mobile Apps

What are the 3 major areas for testing?

- **File System**
  What are apps writing to the file system? How is data stored?

- **Application Layer**
  How are apps communicating via HTTP and Web Services? SSL?

- **Transport Layer**
  How are apps communicating over the network? TCP and Third-party APIs
OWASP Top 10 Mobile Risks

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
OWASP Top 10 Mobile Risks

6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure
OWASP Mobile Security Project

- You should get involved!
Other Issues

- Privacy of your data!
  - Mobile apps talk to many third party APIs (ads)
  - What’s collected by Google/Apple/Microsoft?
Common Tools

- SSH
- VNC server
- A compiler (gcc / agcc)
- Android SDK (adb!)
- XCode
- Jailbroken iDevice
- Rooted Android Device
Forensics & Incident Response

- Filesystem artifacts
- Timeline analysis
- Log analysis
- Temp files
Forensic Tools

- Mobile Forensic Tools
  - EnCase, FTK, Cellebrite
- Free and/or Open Source
  - file, strings, less, dd, md5sum
  - The Sleuthkit (mactime, mac-robber)
Timelines

- Timelines are awesome
  - Anyone know log2timeline?
- Filesystem
  - mac-robber
  - mactime
- Logs
  - Application- & OS-specific
Filesystem Timelines

- mac-robber
  - C app
  - free & open source
  - must be compiled to run on devices

- mactime
  - Part of The Sleuthkit
  - runs on Mac, Win, Linux
Compiling mac-robber

- Android
  - Install arm gcc toolchain
  - Compile & push via adb
Compiling mac-robber

- iOS (jailbroken)
  - Download & Install libgcc onto device
  - Install iphone-gcc
  - Download & Install C headers/libraries

```
curl http://iphone-gcc-full.googlecode.com/files/libgcc.deb > libgcc.deb
curl http://iphone-gcc-full.googlecode.com/files.headers-libss.deb > headers-libs.deb
dpkg -i libgcc.deb
dpkg -i --force-overwrite headers-libs.deb
gcc -o mac-robber mac-robber.c
```
Running mac-robber

- iOS & Android via SSH

```
ssh root@ipad "~/mac-robber /" > iPad-AttachmentOpen.body
mactime -b iPad-AttachmentOpen.body > iPad-AttachmentOpen.tm
```

- Android via adb

```
./adb shell '/system/bin/mac-robber /' > ~/tmp/DrawFree-post.body
mactime -b ~/tmp/DrawFree-post.body > ~/tmp/DrawFree-post.tm
```

- Then, process each with mactime
## Filesystem Timelines

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Size</th>
<th>Permissions</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Mar 12</td>
<td>18:35:48</td>
<td>mac.</td>
<td>1792</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/IMG_20120229_074128-2.jpg</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:35:51</td>
<td>mac.</td>
<td>2422</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/IMG_20120229_074432-2.jpg</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:35:54</td>
<td>mac.</td>
<td>2377</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-8.png</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:35:57</td>
<td>mac.</td>
<td>2377</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-9.png</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:35:59</td>
<td>mac.</td>
<td>2377</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-10.png</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:36:02</td>
<td>mac.</td>
<td>2377</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-11.png</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:36:05</td>
<td>mac.</td>
<td>1085</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-4.bmp</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:36:08</td>
<td>mac.</td>
<td>1085</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-5.bmp</td>
</tr>
<tr>
<td>Mon Mar 12</td>
<td>18:36:13</td>
<td>mac.</td>
<td>334</td>
<td>-rw---------</td>
<td>/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/-WRD000-2.jpg</td>
</tr>
</tbody>
</table>
Where is the data?
Temp Files
Gallery Lock Lite

“Protects” your images
`202:tmp john$ file carved.jpg

carved.jpg: JPEG image data, EXIF standard`
Viewing & Searching Files

- `cat`, `less`, `vi`, `strings`, `grep`
- SQLite files
  - GUI browser, API (Ruby, Python, etc)
- Android apps
  - `ashell`, `aSQLiteManager`, `aLogViewer`
Application Layer - HTTP

- Tools Used:
  - Burp Suite
  - Burp Suite
  - oh yeah Burp Suite!
Why Look at the App Layer?

- Very common in mobile platforms
- Many errors are found within the application
  - And how it talks to the back end service
- Able to use many existing tools
Launching Burp Suite

- Memory!

```
Tyrea:Downloads kjohnson$ java -jar burpsuite_pro_v1.4.06.jar
^CTyreaj:Downloads kjohnson$ java -Xmx4096M -jar burpsuite_pro_v1.4.06.jar
Deleting temporary files - please wait ... done.
Tyrea:Downloads kjohnson$ java -Xmx4096M -jar burpsuite_pro_v1.4.03.jar
```
Misunderstanding Encryption

```
GET /api/?/gettoken/2GpkmRq2GpkmRkamRq,CFzc3dVcmQ= HTTP/1.1
Host: smestorage.com
User-Agent: iSMEStorage/2.10 CFNetwork/485.12.7 Darwin/10.4.0
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: _utma=170435234.225567397.1308798565.1308798565.1308798565.1; _utmz=170435234.1.10.1308798565; _utmc=170435234; _utmz=170435234.1308798565.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none); PHPSESSID=b03591f6e02169eb9f4d6c84475d659
Connection: keep-alive
Proxy-Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Thu, 23 Jun 2011 03:26:27 GMT
Server: Apache
X-Powered-By: PHP/5.2.14
```
Want Credentials?
Transport Layer - TCP

Tools Used:
- Wireshark
- Tcpdump
- Network Miner
Why look at the transport layer?

- Check to see how network protocols are handled in the app
- Easily look for SSL certificate or other communication issues
NetworkMiner

- Extracts files/images and more
- Can pull out clear txt credentials
- Quickly view parameters
TCP Lab Setup

- Run tcpdump directly on the device

```
tcpdump -w drawfree.pcap -i en0 -nXs 0 host 192.168.1.16
```

- Run Wireshark by sniffing traffic over wireless AP or network hub setup (lots of ways to do this)

- Import PCAPs into NetworkMiner
App Vulnerabilities

- Several examples that we’ve found
- Many from the Top 25 downloaded apps
Evernote

- Notebooks are stored in the cloud
- But…caches some files on the device…
- OWASP M1: Insecure Data Storage
MyFitnessPal

- Android app stores sensitive data on the device (too much data)
sqlite> .dump users
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE `users` (id integer primary key autoincrement, master_id integer unique, username text not null);
INSERT INTO `users` VALUES(1, NULL, "_local", "", NULL);
INSERT INTO `users` VALUES(2, 1, "_local", "", NULL);
COMMIT;
sqlite> .dump user_properties
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE `user_properties` (id integer primary key autoincrement, user_id integer not null, property_name text, value text, create_date text, update_date text);
INSERT INTO `user_properties` VALUES(2, 1, "usemetric", ",yes", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(4, 1, "date_of_birth", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(5, 1, "country_name", ",United States", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(6, 1, "postal_code", ",", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(7, 1, "lifestyle_name", ",", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(8, 1, "current_weight_in_pounds", ",", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(9, 1, "goal_weight_in_pounds", ",", ",2012-01-30 13:10:16");
INSERT INTO `user_properties` VALUES(10, 1, "height_in_inches", ",", ",2012-01-30 13:10:16");
Password Keeper “Lite”

- PIN and passwords stored in clear-text SQLite database
- So much for the security of your passwords...
<table>
<thead>
<tr>
<th>ZGROUP</th>
<th>ZITEMID</th>
<th>ZPOS</th>
<th>ZVISIBLE</th>
<th>ZSITEMS</th>
<th>ZDEFAULTVAL</th>
<th>ZNAME</th>
<th>ZTYPE</th>
<th>ZVALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>No notes</td>
<td>Notes</td>
<td>note</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Username</td>
<td>text</td>
<td>securestate</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Password</td>
<td>password</td>
<td>password</td>
</tr>
</tbody>
</table>

Note: The 'ZITEMID' column contains an error, as it should not contain the value 'password'.
<table>
<thead>
<tr>
<th>Z_PK</th>
<th>Z_ENT</th>
<th>Z_OPT</th>
<th>ZDESTROYTIME</th>
<th>ZPASSWORD</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1234</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Draw Something

- Word list stored on the device
- Modify to mess with your friends
LinkedIn

- SSL only for authentication
- Session tokens and data sent over HTTP
- Lots of apps do this
- M3: Insufficient Transport Layer Protection
Auth over SSL

Data sent over HTTP
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>52.622196</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>CONNECT touch.www.linkedin.com:443 HTTP/1.1</td>
</tr>
<tr>
<td>14</td>
<td>52.683236</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>HTTP</td>
<td>HTTP/1.0 200 Connection established</td>
</tr>
<tr>
<td>16</td>
<td>52.684469</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Client Hello</td>
</tr>
<tr>
<td>18</td>
<td>57.729721</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Server Hello, Certificate, Server Hello Done</td>
</tr>
<tr>
<td>20</td>
<td>57.764075</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Client Key Exchange</td>
</tr>
<tr>
<td>21</td>
<td>57.764373</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Change Cipher Spec</td>
</tr>
<tr>
<td>22</td>
<td>57.764741</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Encrypted Handshake Message</td>
</tr>
<tr>
<td>26</td>
<td>57.790665</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Change Cipher Spec</td>
</tr>
<tr>
<td>28</td>
<td>57.795318</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Encrypted Handshake Message</td>
</tr>
<tr>
<td>30</td>
<td>57.796594</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>32</td>
<td>58.651948</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>33</td>
<td>58.652018</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Encrypted Alert</td>
</tr>
<tr>
<td>32</td>
<td>58.653205</td>
<td>192.168.1.16</td>
<td>192.168.1.16</td>
<td>TLSv1</td>
<td>Encrypted Alert</td>
</tr>
<tr>
<td>54</td>
<td>58.787168</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>GET <a href="http://media.linkedin.com/mpr/mpr/shrink_80_80/p/2/000/089/1lee">http://media.linkedin.com/mpr/mpr/shrink_80_80/p/2/000/089/1lee</a>,</td>
</tr>
<tr>
<td>60</td>
<td>58.984158</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>77</td>
<td>60.088613</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (JPEG JPG image)</td>
</tr>
<tr>
<td>211</td>
<td>60.178427</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>299</td>
<td>60.129778</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
<tr>
<td>308</td>
<td>60.533624</td>
<td>192.168.1.16</td>
<td>192.168.1.20</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (application/json)</td>
</tr>
</tbody>
</table>
Pandora

- Registration over HTTP
- User name/Password and Registration info sent over clear text
- Unfortunately...lots of apps do this
POST /pad/register/6CUD747 HTTP/1.1
Host: www.pandora.com
User-Agent: Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A405
Content-Length: 113
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: http://www.pandora.com
Content-Type: application/x-www-form-urlencoded
Referer: http://www.pandora.com/pad/register/6CUD747
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: v2regbstage=true
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive

email=******%40gmail.com&password=******&password_confirm=******&zip=44112&year=1974&gender=male&terms=on
Hard Coded Passwords/Keys

- Major Grocery Chain “Rewards” Android app
- Simple to view the source, extract private key
- OWASP M9: Broken Cryptography
- Do developers really do this?

```
<string name="user_token" />
<string name="private">3h1ut1ns0v3</string>
```
Why yes, they do!

iOS/Android authentication and security

Here is what I am trying to do and can anyone provide some best practice advice for authentication and security?

Each user will have their own private database on the cloud. He will have his local couchdb on iOS/Android. My iOS/Android app will replicate between mobile and the cloud. Users can also access their data on the cloud from the web. I am using CouchDB authentication and there is no middle tier.

When a user sign up for a new account, I will create a new database in the cloud with his account name. I compared Iris Couch and Cloudant and and chose Iris Couch because Cloudant doesn't give me admin privilege to achieve this.

My questions:

1. Is it a good idea or possible for the iOS/Android/Web client to have admin privilege to create a new database when they sign up for a new user account? I could hard code the admin username and password on the iOS/Android clients but that feels very wrong. For the web client, I won't have the option to hard code the admin password at all. Alternatively, I can setup a new machine in the cloud to monitor _users database changes and create new databases accordingly.

2. Shall I use the user's credential to replicate between mobile and cloud?

3. I am using Iris Couch for hosting. What is the best way to integrate Facebook authentication into my authentication model? I saw this plugin but does it require my own hosting and making changes to the server?

https://github.com/sander/CouchDB-Facebook-Authentication

Out of curiosity, I also look at Cloudant hosting. But it doesn't look like I can create CouchDB users and support my database-per-user model. I don’t have admin access to _user database.
Privacy Issues

- Example: Draw Something App (Top 25)
- UDID and more sent to the following third-party ad providers:
  - appads.com
  - mydas.mobi
  - greystripe.com
  - tapjoyads.com
What is UDID?

- Alpha-numeric string that uniquely identifies an Apple device
Pinterest and Flurry.com
Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs

KIM-MAI CUTLER

Saturday, March 24th, 2012

Amid extra scrutiny from Congress around privacy issues, Apple this week has started rejecting apps that access UDIDs, or identification numbers that are unique to every iPhone and iPad.

Apple had already given developers a heads-up about the change more than six months ago when it said in some iOS documentation that it was going to deprecate UDIDs. But it looks like Apple is moving ahead of schedule with pressure from lawmakers and the media. It can take more than a year to deprecate features because developers need time to adjust and change their apps. A few weeks ago, some of the bigger mobile-social developers told me that Apple had reached out and warned them to move away from UDIDs.
Conclusions

- Mobile devices are critically common
- Most people use them without thinking of security
- Developers seem to be repeating the past
- We need to secure this area
Contact Us

- John Sawyer
- Tom Eston
  - Twitter: @agent0x0
  - teston@securestate.com
- Kevin Johnson
  - Twitter: @secureideas
  - kjohnson@secureideas.net