SOCIAL ZOMBIES

RISE OF THE MOBILE DEAD
STARRING...
TOM ESTON

• Profiling & Penetration Team Manager, SecureState
• Social Media Security Podcast Co-Host
• SANS Mentor
• OWASP Mobile Threat Model Project Lead
• Survivor of the Zombie Apocalypse
KEVIN JOHNSON

- CEO, Secure Ideas
- Instructor and Author
  - SEC542/642/571
- IANS Faculty
- Open-Source Fanatic
- Ninja
PREVIOUSLY ON

SOCIAL ZOMBIES...
IN 2009 YOUR FRIENDS REALLY WANTED TO EAT YOUR BRAINS
BOT or NOT

The FASTEST way to FIND BOTS on Facebook!

Official Score

9.3

294 votes
SOCIAL NETWORK BOTNETS AND MALWARE DELIVERY

Kreios C2

Thanks to Robin Wood (@digininja)!
YOU GAVE THIS GUY YOUR PERSONAL DATA

LOLZ!
THANKS!
$$$
TOM IS NOT MY FRIEND
GUESS WHAT?
NOTHING HAS CHANGED

- Your friends are still bots
- Ed Skoudis will STILL not accept my friend request..why??
- Malware is delivered via social networks
- Your private data is harvested more than ever
- Zuckerburg is a now a billionaire
- Your mom is still on Facebook
- MySpace still sucks...
  - Except in some comments lately?!?!
ALSO

- Charlie Miller works at Twitter now!

“I’m not clicking on any tweets from this guy...”
AIR FRESHENERS ARE POSTING STATUS UPDATES?

WTF
WHY HAS IT GOTTEN WORSE?

• Rapid adoption of mobile applications and platforms
  – We use mobile devices for everything
• Advancements in mobile technology
• Mobile application developers lack awareness
  – It’s 2008 all over again!
  – Or 1999?
ARE WE ON BATH SALTS??

My credit card!! yey
pic.twitter.com/yyZg7PTz

Tamar El Dahri
@tamareldahr

Debit Card
@NeedADebitCard
Please quit posting pictures of your debit cards, people.
APPARENTLY, YES
PROOF: THE DUCK FACE
Am I sexy, baby?

OFMG SO HOT
IS PRIVACY DEAD?

• Let’s hope not
• But...do we still care?

WHAT’S THE POINT OF BEING AFRAID OF THE ZOMBIE APOCALYPSE

WHEN YOU’RE ALREADY A ZOMBIE?
• We love mobile devices!
  – They provide us with data
  – They give us new attack vectors
• We discuss new ways to leverage mobile devices, applications and new technology for pentesting
NEW SECURITY CONCERNS
ANDROID JELLY BEAN

• Face Unlock
• Google Now
  – “Cards” that are modified based on what you do
“It’s like having unprotected sex with another device!”
NFC

• **Near Field Communication**
• Two-way short range communication
• Designed for ease of use
• “tap” your device with another device to transfer data
• More research recently released
  – Charlie Miller (Black Hat 2012)
NFC PROOF OF CONCEPT ATTACK

- Using NFC to launch BeEF hook
- Great for physical and/or social engineering attacks
DEMO
Google wants NFC to be open and have little authorization

“When an Android-powered device discovers an NFC tag, the desired behavior is to have the most appropriate activity handle the intent without asking the user what application to use.”

MOO BUSINESS CARDS

• Now with NFC! Imagine all the FUN!

INTEGRATIONS
iOS 6

• iOS keeps adding integrations
  – Cause it wants to just be friends!
• Facebook now integrated into the OS
  – Twitter since iOS 5
• Provides simple access to share
  – Providing more chance for problems
PASSBOOK

• Centralized integration point
  – Designed to provide access!
• Tickets, coupons, geofencing and your data
• Two methods to use
  – Apps now contact you based on your location
  – You can access application data
Target
INSTALLED

Automatic Updates
ON

Show On Lock Screen
ON

Show based on time or location.

Barcode Number
9856 0401 2700 0000 1311
9836 4894 32

Mobile Coupon
Expires 09/28/2012
Anyone See This?

Apple Updates Find My Friends with Friend Location Notifications

Wednesday September 19, 2012 11:48 am PDT by Arnold Kim

Apple has updated its and Find My Friends with iOS 6 support and a few new features, including push notifications for locations.

ArsTechnica digs deeper into the new features of the app, which includes a revamped interface and the ability to send texts to friends from within the app. They also note one particularly notable new feature: push notifications for friend locations:

"But the most significant new feature—and the one that will undoubtedly cause at least a bit of controversy—is the ability to set notifications for when your iOS-using friends arrive or leave a certain location. You can set this notification by viewing a specific friend’s location and then tapping the "Notify Me" button on the top right. This brings you to a screen that allows you to decide whether you want to be notified when that person is coming or going, and with which address to associate the notification.

ArsTechnica notes that you can disable permissions from friends but it disables the Find My Friends functionality completely for that individual, not just automated notifications."
OSX MOUNTAIN LION

• OSX is becoming iOS ;)
  – Or so it seems

• 10.8.2 adds integration with FB and Twitter
  – Partially on by default
  – Share via

• Accounts add it to Contacts and the others
MOBILE APP SECURITY
OAuth and API Keys

- OAuth Tokens Stored in PLIST file (Apple iOS)
- Simply copy the PLIST file to another device, you’re logged in as them!
- We are finding OAuth tokens in lots of PLIST files...Dropbox and apps that use Dropbox like *password managers*...
- Found in LinkedIn (Fixed), Facebook (Fixed) and others
<key>FBSessionAccessToken</key>
<string>66285683791fe9df3de7ff7006e5ea69218.0-12099544371mhHkVps[REDACTED]</string>
<key>FBSessionKey</key>
<string>fe9df3de7ff7006e5ea69[REDACTED]</string>
<key>FBSessionSecret</key>
<string>114f298d17f752ab[REDACTED]</string>
<key>FBShareNearbyCityEnabled</key>
POOR AUTHORIZATION AND AUTHENTICATION

• CNN Mobile App (iOS) – Disqus Comment System API Key Vulnerability
  - Potentially allows you to delete, update and modify user comments
  - Passed in the GET request

GET /api/get_thread?user_api_key=m3aFIDJiIt thread_id=8228846290
Host: disqus.com
User-Agent: CnnApp4iPad/2802 CFNetwork/548.0.4 Darwin/11.0.0
Accept: */*
Accept-Encoding: gzip
Accept-Language: en-us
Connection: keep-alive
Proxy-Connection: keep-alive
NEW PRIVACY CONCERNS
MORE SOCIAL
MORE PROBLEMS

• Facebook, Twitter and LinkedIn have grown exponentially
• 900 Million!
• Privacy issues have increased as well

EVOLUTION: FACEBOOK DESIGN TRICKS

Image: TechCrunch http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/
FACEBOOK DESIGN TRICKS

Image: TechCrunch http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/
FACEBOOK DESIGN TRICKS

Image: TechCrunch http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/
FACEBOOK DESIGN TRICKS

Image: TechCrunch http://techcrunch.com/2012/08/25/5-design-tricks-facebook-uses-to-affect-your-privacy-decisions/
MOBILE DATA EXPOSURE
YOUR UDID IS SHOWING

• UDID = Unique Device Identifier
• Privacy concern since this uniquely identifies your mobile device
• Research has shown that it can be used to correlate the person using the device!
Device

Name: securestate's iPad
Capacity: 13.86 GB
Software Version: 5.0.1 (9A405)
Serial Number: 5Z0EF0F3B1735
Identifier: fb730186d420c7c72 (redacted)
IMEI: Unknown
MEID: Unknown
WiFi MAC Address: e0:b9:ba:da:52:6f
Bluetooth MAC Address: e0:b9:ba:da:52:70
Last Connected: March 29, 2012 12:35 PM

Contact

Phone Number:
Name: 
Email Address: 

Certificate
Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs

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.
1 MILLION UDIDS EXPOSED

• Anonymous said it’s from the FBI, FBI denies
• Really from a third-party company...
SIDE CHANNEL DATA LEAKAGE

• Many apps are still using UDID...(for example)
  – Draw Something
  – Words with Friends
  – Redbox
  – United Airlines
  – Pinterest
  – Flipboard
  – Calculator (really?)

• Some of these apps use UDID with third-party services like flurry.com!
**PINTEREST USING FLURRY.COM**

<table>
<thead>
<tr>
<th>request</th>
<th>response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>raw</strong></td>
<td><strong>params</strong></td>
</tr>
<tr>
<td>POST /aas.do HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>Host: data.flurry.com</td>
<td></td>
</tr>
<tr>
<td>User-Agent: Pinterest/1.4.3 CFNetwork/548.0.4 Darwin/11.0.0</td>
<td></td>
</tr>
<tr>
<td>Content-Length: 453</td>
<td></td>
</tr>
<tr>
<td>Accept: <em>/</em></td>
<td></td>
</tr>
<tr>
<td>Content-Type: application/octet-stream</td>
<td></td>
</tr>
<tr>
<td>Accept-Language: en-us</td>
<td></td>
</tr>
<tr>
<td>Accept-Encoding: gzip, deflate</td>
<td></td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td></td>
</tr>
<tr>
<td>Connection: keep-alive</td>
<td></td>
</tr>
<tr>
<td>Proxy-Connection: keep-alive</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>raw</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REDBOX
CNN IOS MOBILE APP

• Sometimes the server response tells you interesting details
• What if you wanted to post comments on a news site anonymously?
• Sure you can see the user id but...
CNN MOBILE APP

• Disqus comment system leaks emails...
CNN MOBILE APP

• ...and IP Addresses
OH WELL!
MOBILE APP PRIVACY POLICIES

• Bottom Line
  – Painful to read, no idea what is captured, I just want to play Angry Birds...

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>POLICY SPECIFICS</th>
<th>COLLECTION</th>
<th>SHARING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WORD COUNT</td>
<td>GRADE LEVEL</td>
<td>WEB = MOBILE?</td>
</tr>
<tr>
<td>Apple</td>
<td>2413</td>
<td>14.6</td>
<td>Yes</td>
</tr>
<tr>
<td>Brewster</td>
<td>1607</td>
<td>12.2</td>
<td>Yes</td>
</tr>
<tr>
<td>Facebook</td>
<td>8780</td>
<td>11.5</td>
<td>Unknown</td>
</tr>
<tr>
<td>Google</td>
<td>2240</td>
<td>13</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Wallet</td>
<td>1156</td>
<td>14.5</td>
<td>Yes</td>
</tr>
<tr>
<td>Indeed</td>
<td>1895</td>
<td>14.3</td>
<td>Unknown</td>
</tr>
<tr>
<td>Instagram</td>
<td>2696</td>
<td>14.2</td>
<td>Yes</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>6342</td>
<td>15.2</td>
<td>Unknown</td>
</tr>
<tr>
<td>MyFitnessPal</td>
<td>2323</td>
<td>15.4</td>
<td>Yes</td>
</tr>
<tr>
<td>YELP</td>
<td>2353</td>
<td>12.9</td>
<td>Yes</td>
</tr>
</tbody>
</table>
INSECURE DATA STORAGE
## CLEAR TEXT FTW

![SQLite Database Browser](image)

**Table: ZDBITEM**

<table>
<thead>
<tr>
<th>ZGROUP</th>
<th>ZITEMID</th>
<th>ZPOS</th>
<th>ZVISIBLE</th>
<th>ZITEMS</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>No notes</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>
BREWSTER

- Hardcoded “production” user name and password used for data access
CONTACT LIST HARVESTING
ALL UR DATA R BELONG TO THEM

• More apps are doing this
• “See if your friends are using this app”
• Apple iOS apps can access contact data without permission (fixed in iOS 6)
• Install prompt on Android
• Developers can notify you on their own...
Find Friends
To find friends, we'll need to upload your contacts to Yelp. Don't worry, we're not storing them.

No Thanks  OK
BREWSTER

• Takes your:
  – Address book
  – LinkedIn contacts
  – Facebook Friends List
  – Who you follow on Twitter
  – Gmail address book
  – FourSquare Locations
  – And more...

Image: Brewster.com
FIND AND CALL MALWARE

• First “Trojan” for Apple iOS?
• It was a spammy app that sent your contact list to a third-party server
• Your friends get SMS spammed from the server
• App removed from the App Store and Google Play
NEW TWISTS WITH GEOLOCATION
FACEBOOK TIMELINE

• Easier than ever to view where someone has been
• Pulls location data from photos, status updates and more...
• Facebook Graph Search!
“...you can now much more easily access photos you and others took months or even years ago.”

– Kevin Systrom, co-founder and CEO of Instagram
THE FUTURE
MORE APPS LIKE VINE

See & share beautiful looping videos

Capture your world in a fun & simple way
SOCIAL FACIAL RECOGNITION

- “Facedeals”
- Camera matches your photo to photos on Facebook to give you deals
MINORITY REPORT: IRL?

How’d those assorted tank tops work out for you?
DO NOT WANT!!!!!!!!
CONCLUSIONS

• Not much has changed over the years
• Technology has advanced, privacy has not
  – It's only going to get worse!
  – What about privacy policies?
• You’re responsible for your data and the services you use!
• Don’t complain if you click Kevin’s links...
QUESTIONS?

You thought duck face was bad. This is called “bagel face” and it’s a popular saline injection in Japan. Awesome. You’ve been warned.