Cellular Privacy

A Forensic Analysis of Android Network Traffic

Hi There

Eric Fulton
Lake Missoula Group
Missoula, MT

ForensicsContest.com
(Also doing a Defcon Contest!)
Triskt.com
@Trisk3t

Thank You:
Sherri Davidoff
Jonathan Ham

Preview

- Definitions
- Testing methodology and setup
- Analyzing the captured packets
- Fun Findings
- Conclusion

What is Network Forensics?

"Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection." - Wikipedia

Or, listening to the wire for fun, ???, profit, and lulz.

How Network Forensics Affects Us

- (Almost) Everything we do is network based // uses a network
- We send: usernames, passwords, hashs, url's, personal information, credit card information, chats, lolcats, reddit comments, etc. over the Internet.
- Our applications send: licensing and registration data, update information, demographic information, UUID information, etc.
- All network data can be filtered, logged, and analyzed by a third party.

How Our Phones Could F**ck Us

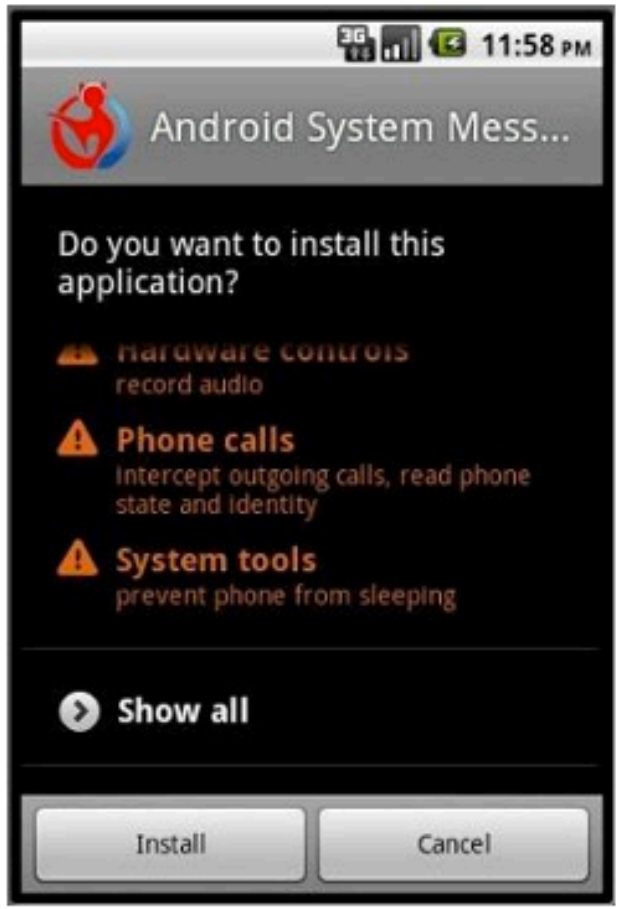
- Conversation recording
- Call history
- Private Keys
- Emails
- Usernames // Passwords
- Usage Data
- GPS Location
- Movement data (accelerometer)
- Data ex-filtration (Pics, Txt's, etc.)
- AND MORE!

Anyone can build a freaky evil app

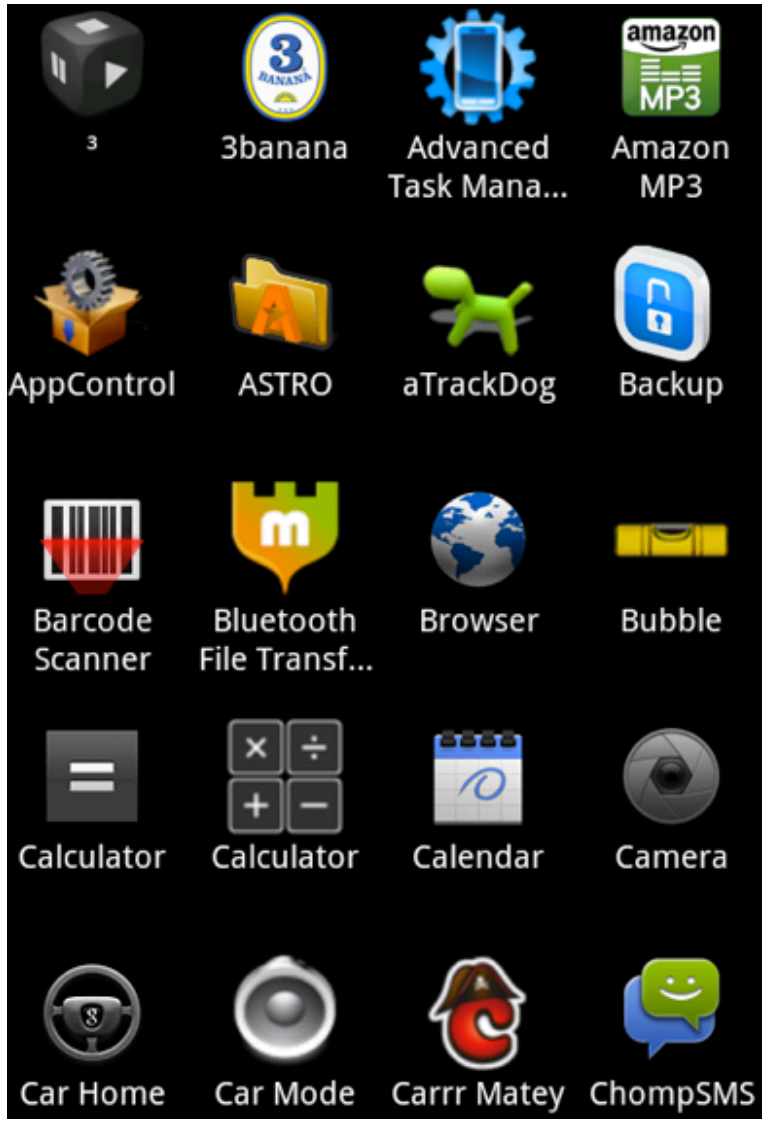
New Android trojan can record phone calls, expose your embarrassing fantasy baseball talk

By Terrence O'Brien posted Aug 2nd 2011 at 11:41AM

Mobile malware is nothing new, especially for Android users who have trained themselves to navigate the sometimes shady back alleys of the Market. The fine folks at CA Technologies came across an interesting new trojan though, that does something slightly more unnerving than max out your credit cards -- it records your conversations. There's no evidence that this has actually found its way into the wild yet, but it's entirely possible that some nefarious developer could capture your calls and upload them to a remote server. Obviously, this wouldn't hold much interest for your traditional cyber crook, but suspicious significant others and corporate spies could have a field day with such capabilities. All we can do is suggest you remain vigilant and maintain a healthy dose of paranoia about any apps on your phone.



...but what are current apps doing?



Previous Research

- Wall Street Journal
  - Privacy Articles
  - Android Articles
- Aldo Cortesi:
  - A coder and security consultant living in Dunedin, New Zealand.
  - http://corte.si/index.html

Scientific Method!

1. Question
2. Hypothesis
3. Experiment
4. Testing Methodology
5. Applications Tested
6. Results
7. Conclusion

Question

To what extent do participants in the cellular ecosystem (OS creators, app creators, carriers, etc) respect user privacy?

Hypothesis

Software applications and operating systems transmit private user information to the author or third parties, without the user's knowledge or consent:

- Personal data/identifying data
- User names
- Passwords
- Contact lists
- Location data
- Usage statistics
- Timing of activities
- Other Content

Experiment

- Build a lab
- Install and use apps on Android Phone
- Capture Packets
- Analyze Packets
- ???
- Profit!

Experiment

Building a lab!

- 1x Verizon Femtocell
- 1x Original A855 Motorola Droid
- 1x WRT54GL Wireless Router
  - DD WRT
- 1x Sniffing Laptop
  - SSL Strip
  - TCP Dump
- 1x Internet Connection

Original Testing Methodology

Tests are broken into 4 parts

Application Tests
-Purchase/Install of the application
-Initial usage and setup of the application
-Regular Usage of Application
-Uninstalling the application

OS Tests
-First usage
-Light usage
-IDLE Time
-Re-setting the phone

Actual Testing Methodology

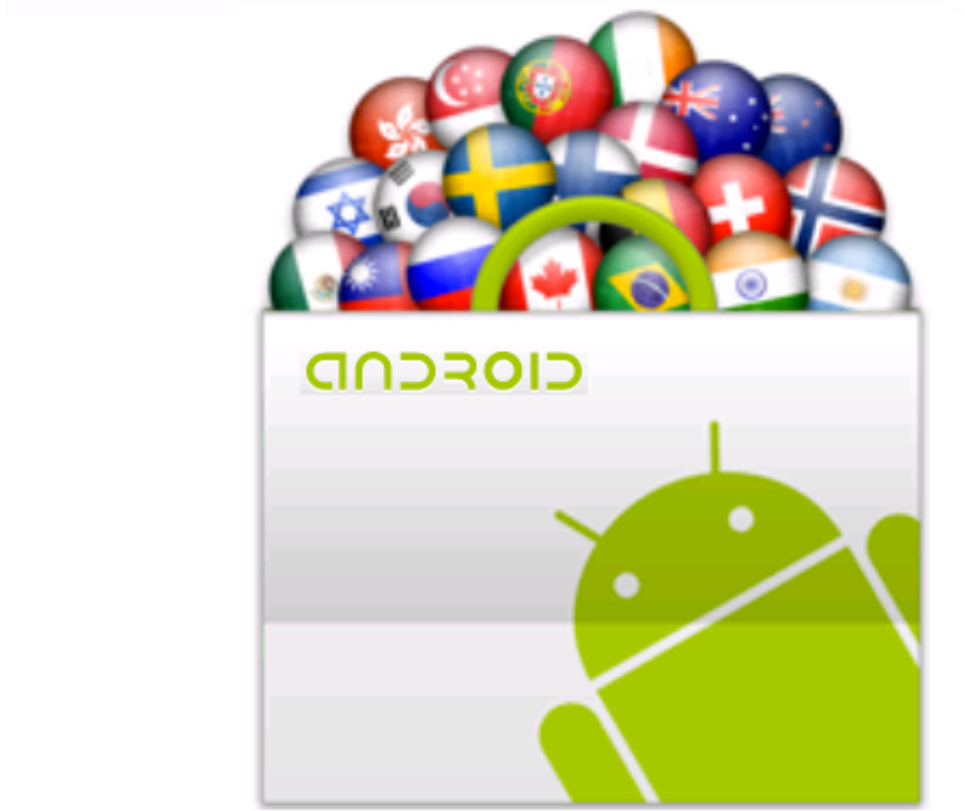
-Install Apps
-SSLStrip + TCPDump each app/OS

...makes for a fun drinking game.

Apps Being Tested

- Angry Birds
- Chinese App
- enel-solar
- Facebook
- Google.com (via browser)
- Intelli Pilot
- Mousetrap
- Pandora
- Red Phone
- Words With Friends
- Zynga Poker

It's A Work In Progress



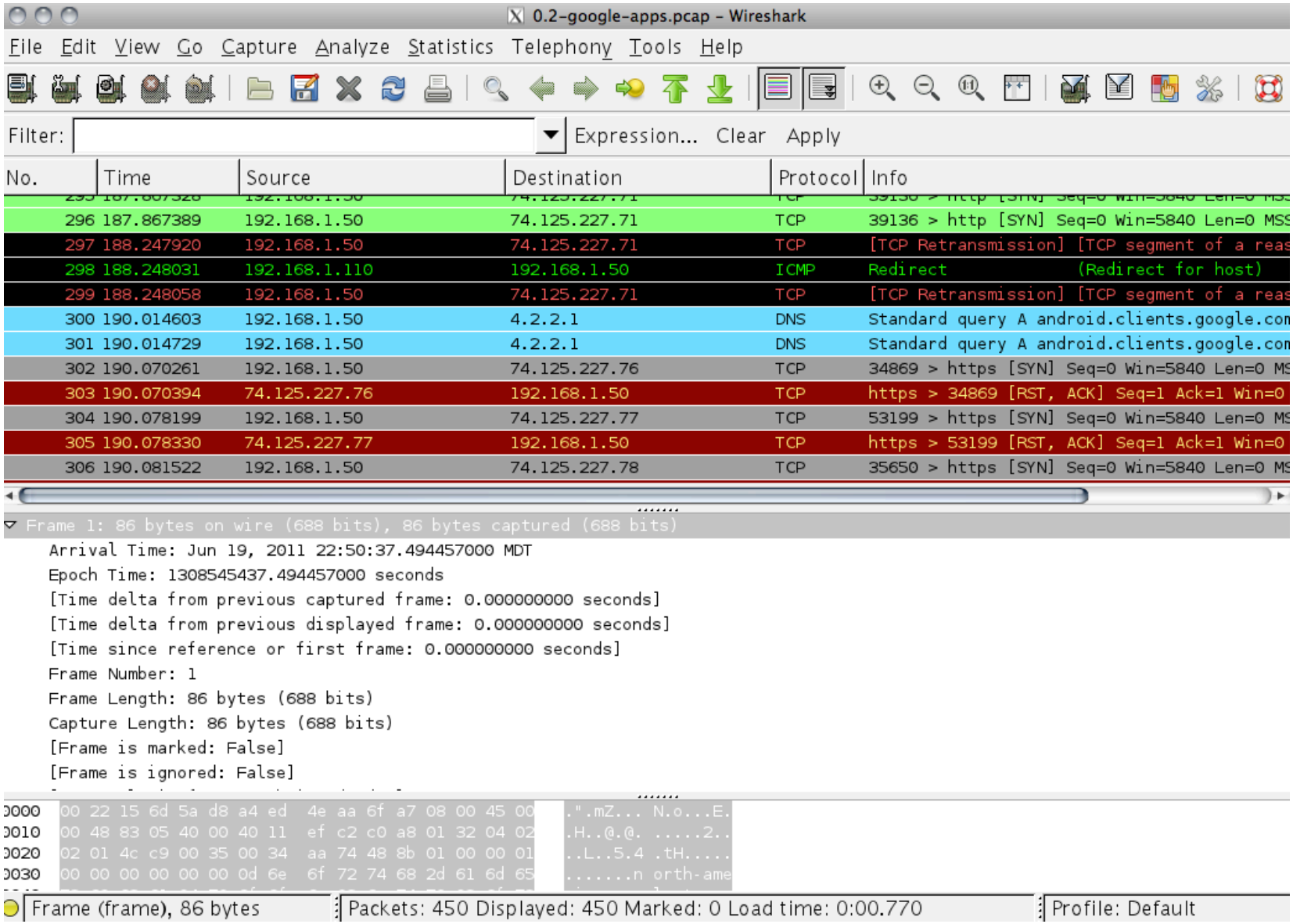
What We Have to Work With

```
$ls
analysis                facebook.pcap           pumphouse
angry-birds             fbook2                  pumphouse.pcap
angry-birds.pcap        frozenbubble            redphone
argus                   frozenbubble.pcap       redphone.pcap
carhome                 gibberbot               russian
carhome.pcap            gibberbot.pcap          russian.pcap
chinese                 google-calendar         wordswf
chinese.pcap            google-calendar.pcap    wordswf.pcap
dropbox                 intelli-pilot           zyngapoker
dropbox-a               intellipilot.pcap       zyngapoker.pcap
dropbox.pcap            mousetrap               zyngapoker1
enel-solar              mousetrap.pcap          zyngapoker2
enel-solar.pcap         pANDORA.pcap            zznotest.txt
facebook                pandora
$
```

Let's Start Analyzing!

- Let us start poking around with all the captured files
  - Peering around in Wireshark
  - Analyzing Conversations
  - Strings + Grep
  - DNS Play
  - ARGUS Flows

WireShark


0.2-google-apps.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
296 187.867389 192.168.1.50 74.125.227.71 TCP 39136 > http [SYN] Seq=0 Win=5840 Len=0 MSS
297 188.247920 192.168.1.50 74.125.227.71 TCP [TCP Retransmission] [TCP segment of a reas
298 188.248031 192.168.1.110 192.168.1.50 ICMP Redirect (Redirect for host)
299 188.248058 192.168.1.50 74.125.227.71 TCP [TCP Retransmission] [TCP segment of a reas
300 190.014603 192.168.1.50 4.2.2.1 DNS Standard query A android.clients.google.com
301 190.014729 192.168.1.50 4.2.2.1 DNS Standard query A android.clients.google.com
302 190.070261 192.168.1.50 74.125.227.76 TCP 34869 > https [SYN] Seq=0 Win=5840 Len=0 MS
303 190.070394 74.125.227.76 192.168.1.50 TCP https > 34869 [RST, ACK] Seq=1 Ack=1 Win=0
304 190.078199 192.168.1.50 74.125.227.77 TCP 53199 > https [SYN] Seq=0 Win=5840 Len=0 MS
305 190.078330 74.125.227.77 192.168.1.50 TCP https > 53199 [RST, ACK] Seq=1 Ack=1 Win=0
306 190.081522 192.168.1.50 74.125.227.78 TCP 35650 > https [SYN] Seq=0 Win=5840 Len=0 MS
Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Arrival Time: Jun 19, 2011 22:50:37.494457000 MDT
Epoch Time: 1308545437.494457000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 86 bytes (688 bits)
Capture Length: 86 bytes (688 bits)
[Frame is marked: False]
[Frame is ignored: False]
0000 00 22 15 6d 5a d8 a4 ed 4e aa 6f a7 08 00 45 00 ."·mZ··· N·o···E·
0010 00 48 83 05 40 00 40 11 ef c2 c0 a8 01 32 04 02 ·H··@·@· ·····2··
0020 02 01 4c c9 00 35 00 34 aa 74 48 8b 01 00 00 01 ··L··5·4 ·tH·····
0030 00 00 00 00 00 00 0d 6e 6f 72 74 68 2d 61 6d 65 ·······n orth-ame
Frame (frame), 86 bytes
Packets: 450 Displayed: 450 Marked: 0 Load time: 0:00.770
Profile: Default

Conversation Analysis

Basic reading of the captures
$ tshark -r *.pcap

List conversations.
$ tshark -qn -z conv,tcp,ip -r $FILE.pcap

...Whois like a mofo

What servers are we talking to (Zynga)?

ws.tapjoyads.com
ma.mkhoj.com
cvt.mydas.mobi
mobile.poker.zynga.com
cvt.mydas.mobi
ws.tapjoyads.com
mobile.poker.zynga.com
m.facebook.com
static.ak.fbcdn.net
www.facebook.com
m.facebook.com
static.ak.fbcdn.net
www.facebook.com
static.ak.fbcdn.net
profile.ak.fbcdn.net

What servers are we talking to (Zynga)?

static.ak.fbcdn.net
www.facebook.com
mobile.poker.zynga.com
www.macromedia.com
mobile.poker.zynga.com
www.adobe.com
stats.iphone.zynga.com
mobile.poker.zynga.com
profile.ak.fbcdn.net
mobile.poker.zynga.com
facebook.poker.zynga.com
mobile.poker.zynga.com
playerstatics1.poker.static.zynga.com
statics.poker.static.zynga.com
playerstatics1.poker.static.zynga.com

What is being sent without you knowing?

Strings

Strings is quick and dirty
$strings *.pcap | grep "[http://, password, w00tdefcon, etc.]"

Strings | General Output

$strings *.pcap | grep "w00tdefcon"
Apps exposing password (remember, we are SSL Stripping):

- Facebook

$strings *.pcap | grep "droid.net.foren@gmail.com"
Apps exposing email:

- Facebook
- Words With Friends
- Zynga Poker

Strings | Words With Friends

$strings wordswf.pcap | less

{"data":{"Id":"254912c0","acceptLanguage":"","adPool":0,"adSizes":
["320x48","320x24","300x50","250x50","320x480"],"bundleId":"com.zynga.words","ccs":"31000;**Verizon Wireless;CDMA**","cct":2,"cctDetailed":"","clientDateTime":"4,842","cookie":
[{"domain":"appadserver.com","expires":"Thu, 23 Jun 2011 14:42:31 GMT","maxage":
86400,"name":"iuq1S7ZzRhvUejl0-cTBRERA","path":"/","value":"x"},
{"domain":"appadserver.com","expires":"Wed, 22 Jun 2011 15:02:31 GMT","maxage":
1200,"name":"loc","path":"/","value":"hPfbpX1WMnIDQ9sEsNMeag4tK2k/Q6zry+BisZm8nx4AKRl3WMU//
uVudIRG+5YVPgzSpa7mKiNMKPkHL+3hLCnR62ytEKWDu04a1L+Kj6o="},
{"domain":"appadserver.com","**expires":"Mon, 12 Dec 2016** 14:42:31 GMT","maxage":
172800000,"name":"u","path":"/","value":"KG1GgnC5vEe0xdwq3SKpCw"}],"crParms
":"","debugFlags":0,"deviceId":"9aace5ebb3b2a1d3e31bbad914813153d2b4cefd","ipAddress":"",
"noTrack":0,"placement":"","pubTargeting":"**Millennial=1**","publisher":"q1S7ZzRhvUejl0-
cTBRERA","rvCR":"","type":"iq","userAgentInfo":
{"Build":"1.7.2.116","Density":"High","Device":"**Droid**","DeviceFamily":"**verizon**","Platform":"Android"
,"PlatformVersion":"**2.2.2**","ScreenResolution":"480x854","v":"1"},"zone":"09551518791392046 89"}}

Strings | Words With Friends

path":"/","value":"hPfbpX1WMnIDQ9sEsNMeag4tK2k/Q6zry+BisZm8nx4AKRl3WMU//uVudIRG
+5YVPgzSpa7mKiNMKPkHL+3hLCnR62ytEKWDu04a1L+Kj6o="},
{"domain":"appadserver.com","expires":"Mon, 12 Dec 2016 14:42:31 GMT","maxage":
172800000,"name":"u","path":"/","value":"KG1GgnC5vEe0xdwq3SKpCw"}]
,"crParms":"timestamp=1308754393784,appversion=3.51,email='**droid.net.foren**
%40gmail.com'
,gwf_id=31443183,last_move_was_a_word=1,last_move_word='about',last_move_score=18,
words='about',pass_and_play=1","debugFlags":
0,"**deviceId":"9aace5ebb3b2a1d3e31bbad914813153d2b4cefd"**
,"ipAddress":"","noTrack":0,"placement":"","pubTargeting":"timestamp=1308754393784,appversion=3.51,
Millennial=2,last_move_was_a_word=1**,last_move_word='about',last_move_score=18**,words='ab
out',
pass_and_play=1","publisher":"q1S7ZzRhvUejl0-cTBRERA","rvCR":"","type":"iq",

Strings | Google.com

BAILEY-PC_Network
94:44:52:5e:78:xx
Belkin.58F8
30:46:9a:3d:ce:xx
OWNER-PC_Network
00:22:75:58:0d:xx
Slampig
00:24:b2:50:f9:xx
seriesoftubes
94:44:52:3d:8a:xx
kill
00:1c:df:f6:5a:xx
yaquis
00:17:3f:e8:ce:xx
pieceofshit
68:7f:74:c5:e4:xx
[...]

Strings | Google.com

fg3EnA:ZHMt2zkSDMwGTvXx:QhSA90NM6_DIyA0S:CzGLQuIQYZuHNKTy:zmMAuhLgJ
1maRYuY:ZkilgzONHDfiNlXy:mGNpSWTLDyMV-39w:AMR_DQgqXyUOf7Da;
devloc=468xxxxx:-1140xxxxx:21; HSID=A5likOthDuKnGqHMM;
MPRF=H4sIAAAAAAAAAKs4u-
b08261LiaGSUwKqQYmlpaphkmGZmbGlonGKWamyQbJFkIJhsnGhgYWBoYTmBkAziEK
gDAAAAA; NID=48=Jveim4GhoNx6ViXf_6b7Lh-gLKzL2wgJuFoANQ8xh-5a-
Ry1r2HA75353ATRtF5D6amyxyPOhVoe-
kWIGyRBZYKTPVug9LH3xxnASulqOs7YiWN9Cx9zBKniO-jfHJ3H;
PREF=ID=9ae930e9b2149d59:U=785173e78f0434c7:TM=1308545456:LM=1308545456:
S=1JH-bPtba8ixWdkX; SID=DQAAAKYAAACMhbFUDFZ27g-54PL-
apylTPEqkaPEmzcplS9hEgUARK-
ZBp4OVmOhg6QZv6qUlOuBBC16QxlDJ3rbKSUZcQyImv7Wj52TtKJi03IxfCf-
R85FtE5z6mhs3yAhrQf1uoAGFTUcZfqaW2523Ox2rTb7QzIC1ANLDIILeKZIKQXcBijqfZz
bY0Eb-e1oBfeRpK6lyligXkF8mem8IrJY2JV1ODueljecWYJRrFqwVwYKvg;
SSID=AV0Q0t23EIGKoco2I

Strings | Google.com

{lan_mac::00:1C:10:B3:CC:EE
{wan_mac::00:1C:10:B3:CC:EF
{wl_mac::00:1C:10:B3:CC:F0
{lan_ip::192.168.1.1
...
{wl_mode_short::ap
{lan_proto::dhcp
{mem_info::,
...
{active_wireless::'xx:xx:xx:xx:6F:A7','eth1','N/A','N/A','-54','-92','38'
{active_wds::}
{dhcp_leases::}
{uptime:: 17:03:50 up 3 min, load average: 0.17, 0.20, 0.08
{ipinfo:: IP: 72.174.68.xxx
{gps_text::
{gps_lat::
{gps_lon::}
{gps_alt::
{gps_sat::

Why do they need this data?

Why Data is Collected:

(I'm hypothesizing here)

- Advertising
- Statistics...
- Advertising
- Legitimate Business Purposes
- Advertising
- Increasing value of service
- Advertising
- ...

What about MiTM?

- Traffic can be intercepted
- SSL Strip
- Exploits
- Etc.

Question (Refresher)

To what extent do participants in the cellular ecosystem (OS creators, app creators, carriers, etc) respect user privacy?

Not Very Much.

Hypothesis (Refresher)

Software applications and operating systems transmit private user information to the author or third parties, without the user's knowledge or consent:

- Personal data/identifying data
- User names
- Passwords
- Contact lists
- Location data
- Usage statistics
- Timing of activities
- Other Content

Were We Right?

Hypothesis (Refresher)

Software applications and operating systems transmit private user information to the author or third parties, without the user's knowledge or consent:

- Personal data/identifying data **YES**
- User names **YES**
- Passwords **YES**
- Contact lists **YES**
- Location data **YES**
- Usage statistics **YES**
- Timing of activities **YES**
- Other Content **YES**

Conclusion

- Your smartphone erodes your privacy
- You agreed to it
- Why does it matter?

Conclusion | Future Research

- Mapping out advertising networks
- Fully cataloging information an app is sending / receiving
- Automating the above process
- ...

Cheers!

Have a safe trip home.