How to hack your way out of home detention
About me

- William "@Amm0nRa" Turner
- @Assurance
Disclaimer:

- I own this system (and Own it)
- The following information is for academic purposes only
- Don’t use this for evil
- If you do, you may go to jail
Home Detention Systems

- Used to monitor 'low risk' criminals in their homes. e.g.:

- “Woman gets home detention in ‘green card’ immigration scheme” [October 2014, Los Angeles]

- Private investigator who “hacked” email gets 3 months jail, 6 months home detention [June 2015, New York]
How home detention systems work

- Older systems ran over phone lines, used RF for anklet bracelet proximity
- Newer systems use GPS, cell network as well as short range RF
In America

- “On a normal day some 200,000 people wake up with a black plastic box strapped to their leg” – James Kilgore, 2012
Getting hold of one

• Very hard to even get info

• Social Engineered a 'sample' unit out of a Taiwan manufacturing company for ~$1k - “GWG International Inc”

• Different states/police forces use different trackers, difficult to know if/where this unit is used in the USA.

• Other trackers probably have at least some of the same vulns

• Lacked detailed manuals - found car tracking system running same 'OS' (GS-818 - SAN JOSE TECHNOLOGY, INC)
Operation

• GPS for location, home base unit with short range RF, tamper detection

• Battery life depends on configuration, can be recharged without removing anklet

• Base unit also has battery to deal with power outages

• Communicates over SMS or GPRS (TCP socket) with server

• Accepts commands to change settings – username and password
The System – base unit
The System – base unit

- Power Adjuster
- Paring Button
- PWR
- Tamper detector1
- Tamper detector2
- Tamper detector3
Internals Teardown
Anklet
Anklet:

- reed switch magnetic sensor
- IR LED
- Push pin button
- IR sensor
- JTAG Header(?)
- power
- SIM card
Anklet Internals

- Cinterion MC551
- K9F5608U0D
- vibration motor
Anklet Internals

M430F5418

434.01MHz Module
Operation

• Interesting commands/features which can be set/enabled/triggered:

  - username
  - password
  - network APN
  - SMS-TCP mode
  - SMS numbers
  - status report interval
  - Geo-Fence coords
  - buzzer
  - vibration alert
  - log to file settings
  - clear log
  - fiber optic break detection
  - reed switch detection
GSM Security

- GSM is encrypted using A5/1 (/2/3)
- Ki embedded in SIM card used to authenticate SIM, network not authenticated – well known issue
- Kc is temporary key used to encrypt traffic
- IMEI used as unique ID, phone number only known by network, not SIM
SDR

- SDR – software defined radio
- BladeRF
YateBTS

• Open source GSM stack – based on OpenBTS, allows JS scripts to control network functions

• Can be used to spoof real network. need to find MCC/MNC of local telcos - illegal

• Faraday cage ($2 roll of tin foil) to block real telco signal and encourage connecting to rogue network
MitMing

- If in TCP mode, can simply MitM socket - easy
- If in SMS mode, much harder, but doable
Intercept status messages

- #username,
  $GPRMC,110834.902,V,3750.580,S,14459.1854,E,0.00,0.00,141014,,*07,ST-1-M27-0-3885mV-50.0

- username – used to auth commands sent to anklet, sent in status messages

- $GPRMC...*07 is a NMEA standard “Recommended minimum specific GPS/Transit data”, GPS cords/timestamp

- 07 is hex checksum on GPS data
Understanding message

• Last part of message: e.g. ST-1-M27-0-3885mV-50.0

• Not fully decoded, but not required

• Does include: RF beacon code, charging status

• Possibly includes message type, battery charge, local cell towers
Spoofing SMS

• Many different 'providers'
• costs ~30c per sms
• We will be using smsgang.com
• Must know the number to spoof...
• 3 ways to get it...
Pull SIM card

- Why not just do this normally?
- Replace with another SIM card?
Brute force pin

• Default pin is 0000, start brute force with dictionary attack

• Need to drop status messages and let anklet retransmit on real network

• Once pin is found: have full control of device. To get number, change config to send status to phone you control
Brute force pin

• Pin must be 4 chars long
• Only allows letters and numbers
• Math.pow(36, 4) == 1,679,616
• “SMS transmission speed of about 30 SMS messages per minute”
• Around 39 days to try every possible pin
Kraken rainbow tables

- Karsten Nohl (BlackHat 2010)
- Allow reversing Kc of GSM traffic captured from air using SDR
- Once Kc is known, can decrypt SMS/GPRS/voice
- Can forge messages
- Send forged message to your own phone to get number
Kraken rainbow tables

• Not able to stop real messages
• But if you have a faraday cage and two SDRs...
• Kc changes often
• Probably have to wait a long time to snoop command – get pin
“Alcoholics Anonymous”
Live Demo!

- Assume we have the anklet number from one of the attacks I just described
- Faraday cage, spoof network
- Decode message, replace latlings
- Recalculate checksum, encode
- Script POST to SMS spoof service
- Google map to points, green – delivered to phone, red – captured by spoofed network
RF Base Unit

- Uses 434.01 MHz
- Frequency Shift Keying (FSK)
- Heartbeat beacon every 10 seconds
Attacks?

- Static – doesn’t change until rebooted (unknown: unique to each device?)
- Record base station heartbeat with hackRF/BladeRF/other SDR, replay
BLACK HAT

- DO NOT USE THIS IN THE REAL WORLD
- YOU WON'T MAKE IT TO JAIL
System detection

• War drive scanning for base unit RF beacons

• Slow/expensive – unless you can detect RF from a long range. Better to use court docs/newspapers to get names and dox

• Jam base station, cell, gps – cheap, easy – very illegal

• Spoof real network and brute force pin, take control of anklet, impersonate user/ crack Kc, get number, jam real device, spoof fake coords
BLACKHAT/Monetization

• If people break the rules of their sentence, they normally go to jail.

• Black mail user? How?

• Sell spoofing device/service

• Do 'cyber hit's on people for a fee
Summary

• Home detention systems have issues

• Could be improved – mutual auth, encryption

• Can't be improved/hard – jamming, user locating
Future?

• Try to get code exec from malformed SMS?

• Remove IC, dump ROM and look for bugs/backdoors

• Write software 'emulator' for the anklet – pull SIM and plug into any smartphone

• Use SDR to spoof GPS – see other talk happening right now...

• Questions?

• I probably ran out of time, so talk to me later.