Practical Cellphone Spying

Chris Paget
ivegotta@tombom.co.uk / @ChrisPaget
Defcon 18

Before we start: Privacy

- Cellular calls will be recorded during the talk
- TURN OFF YOUR PHONE if you don't consent
- Data will not be kept after the talk
  - The BTS is booted from USB with no HDD
- A best-effort will be made to connect all calls

What is an IMSI?

- International Mobile Subscriber Identity
- Primary identifier for a subscriber
  - Kind of like a GSM username
- Lives on the SIM card
- Somewhat protected
  - Replaced by a TMSI when you camp to a tower
- ICCID (printed on the SIM) is closely related
  - Less so outside the USA

What's an “IMSI Catcher”?

- A spoofed GSM tower
- The handset camps to the strongest signal
  - The attacker can always win
- In GSM the BTS (tower) picks all the settings
  - Instructs handset on A5 use, Tx power, Rx gain, etc
- Strong signal + negotiate A5/0 = pwned
- Attacker is the tower -> full control of handset
- Technique was patented by R&S in Europe in 1993
  - Not sure about the USA, either way it's public info

IMSI Catcher Crypto

- Attacker creates the BTS
- Cellphone connects to BTS
- BTS tells cellphone to disable crypto (A5/0)
- Attacker wins, no rainbow tables needed.

- The cellphone could warn you, but won't
  - Too confusing for users
  - Warning is explicitly disabled by operators

Spectrum Usage

- Four bands for GSM globally:
  - 850, 900, 1800, 1900
- GSM-850 and GSM-1900 used in the USA
  - 900 and 1800 are primarily European
- GSM-900 downlink: 880-914MHz
- US ISM Band: 902-928MHz
  - Overlap at 902-914MHz
- Quad-band phones can see an ISM-band BTS
  - European phones, too

ISM band

- Industrial, Scientific, Medical
  - Low power, low utilisation, frequency hopping
- ISM is a secondary user
  - It's a ham band!
- Hams don't like it because of ISM
  - Too much clutter
- So, can we operate a BTS on a Ham license?
  - In the ISM band, at least?

Amateur Radio

- Licenses are fairly easy to get
  - http://kb0mga.net/exams/ for parrot-learning
  - Take the time to understand, much better
- 1500W power limit (!)
- Unspecified digital codes are OK
  - As long as the specifications are public
- No crypto allowed (not a problem here :)
- No antenna limits, only RF exposure limits
- Station must identify itself every 10 minutes

Identifying the Station

- Morse out a callsign every 10 minutes
    - Straight CW, no modulation needed
- It's kinda hard to integrate morse into GSM...

- Easy solution - a second transmitter
    - Same frequency, slightly higher power
    - Overwrite the GSM signal (self-DoS for a sec)
- Need an easily-scriptable 900MHz transmitter

ID-ME

- A hacked IM-ME is perfect
  - Travis Goodspeed did most of the work already:
  - http://travisgoodspeed.blogspot.com/2010/03/im-me-goodfet-wiring-tutorial.html
- +10dBm output, wide frequency range
- Easily programmable in C
  - Again, use Travis' GoodFET to flash it
- Match frequency and power level to the USRP
- Combine signals together and amplify

BTS Setup

- USRP1
  - 2x RFX900 daughterboards
  - ClockTamer (http://code.google.com/p/clock-tamer/)
    - Very precise configurable clock (+/- 100Hz at 1.9GHz)
- Laptop computer
  - Debian
  - OpenBTS
  - Asterisk
- Basic BTS, voice only (no data)

Demo 1

Starting the BTS in test mode

Spoofing a Network

- Networks are identified by MCC / MNC
- Mobile Country Code (310 for USA)
  - List on Wikipedia
- Mobile Network Code (2-3 digits)
  - Again, Wikipedia
- Trivial to change
  - Spoof any GSM network, worldwide
- Network Name is sometimes also checked
  - Case-sensitivity isn't much of a defense

Demo 2

Spoofing MNC/MCC
Changing Network Name

That's all, folks!

- We now have a simple IMSI catcher
  - Phones will camp to the tower & send their traffic
- Can filter handsets by IMSI / IMEI
  - IMEI == Equipment Identifier

- It takes time for handsets to migrate across
  - We can make the process faster...
- Outbound calls only
  - More to come on that

Speeding up Handover

- How to make more handsets connect?
  - And do so more rapidly?

- Lots of possibilities:
  - Neighbour lists
  - Changing LAC
  - Band Jamming
  - Receive Gain

GSM Neighbours

- Each BTS knows what other towers are nearby
  - It tells the handset what channels to look on
- Handsets monitor neighbour channels
  - Speedier handoff when you relocate
- Attacker can use this info to:
  - Identify a neighbour that's far from the local cell
  - Set up the IMSI catcher on that frequency
  - Make cellphones attach to his BTS more quickly

Finding Neighbours

- Nokia 3310 (900/1800) / 3390 (1900)
  - Network Monitor mode
    - Effectively sniffs your own GSM connection
- Fbus/Mbus switching cable
- Gammu

- Records traces to XML
  - Open in Wireshark
- Neighbour list is in “System Info type 2” burst

Demo 3

Finding GSM neighbours

Location Area Code

- LAC is broadcast by the BTS
- It groups together a bunch of cells in one area
  - Easier handoffs within that area

- If a handset sees the LAC change...
- ...it assumes it has moved to a new location...
- ...and hands off to the new tower.
- Change the LAC, entice more handsets.

Demo 4

Changing LAC

Handset Powerup

- When first turned on, handset knows nothing
  - No tower frequencies, current LAC, etc
- Performs a long scan to find towers
  - Chooses which by MCC/MNC and signal strength
- Shorter scan once towers are found.

- When signal is lost, a similar process happens
  - Advantageous to an attacker

Loss of Signal

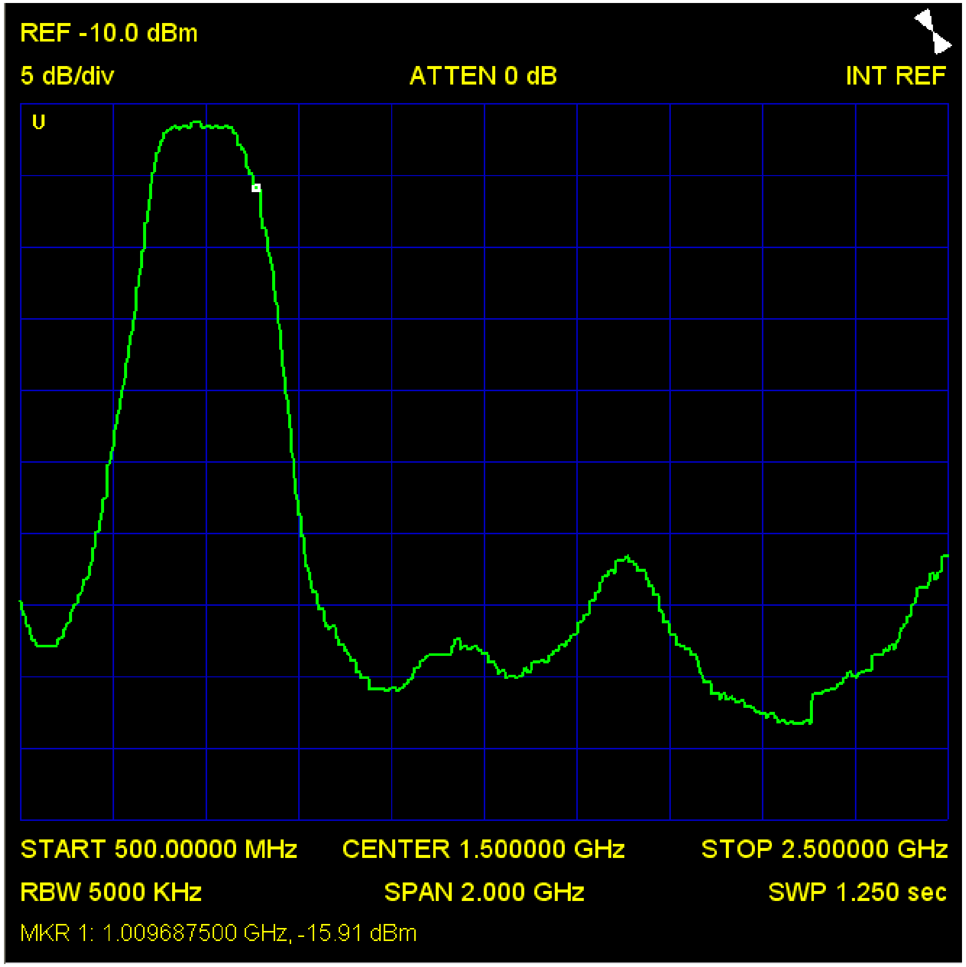
- We're only talking about 2G GSM here
  - 3G is much better
- Jam GSM, handset performs wider search
  - Easier to find the attackers BTS
- Jam 3G, handset drops back to 2G
  - Intercepting 3G is much harder
  - Force the victim down to 2G instead

- Can the attacker jam both bands?

Noise Generation

- Attacker can transmit high-power noise
  - Obscure the signal from the tower
  - Same end result – handset loses signal
- Noise generators aren't too expensive
  - $450 on eBay
- Power amps aren't too expensive
  - $400 for 100W
- 100W of noise == BIG cellphone disruption

Noise Output



REF -10.0 dBm

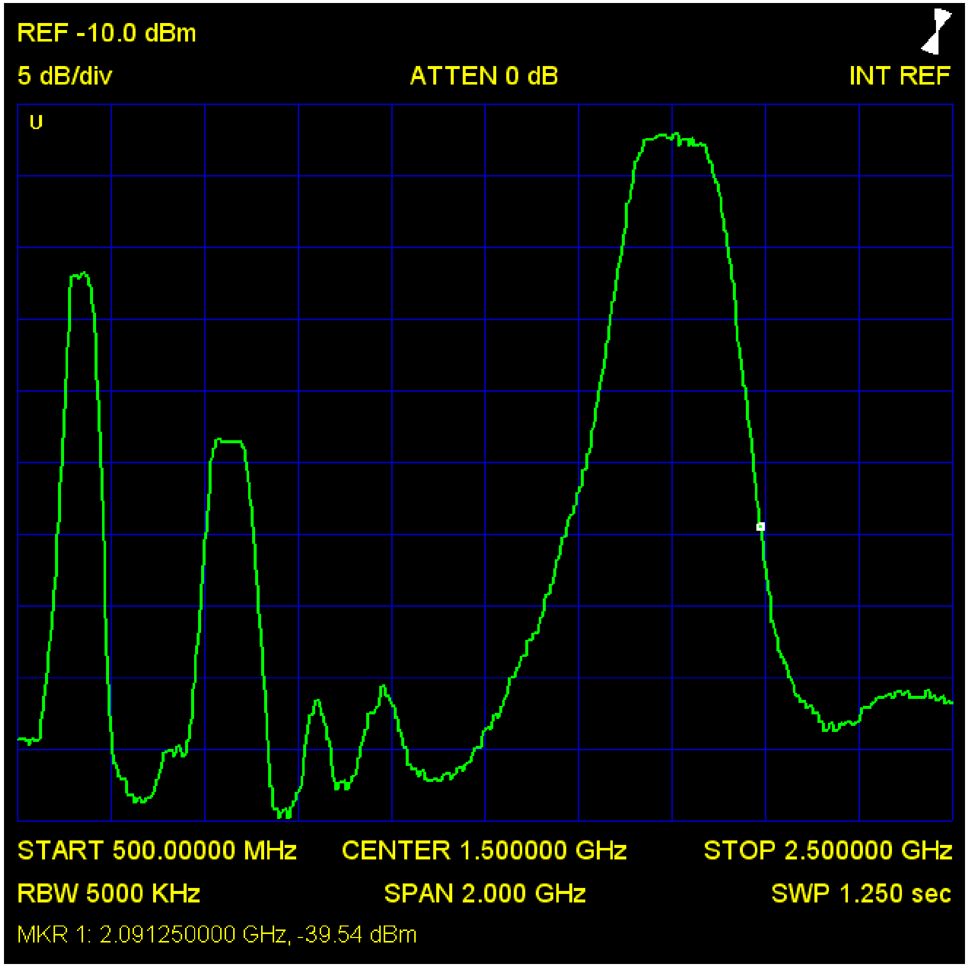
5 dB/div ATTEN 0 dB INT REF

START 500.00000 MHz CENTER 1.500000 GHz STOP 2.500000 GHz

RBW 5000 KHz SPAN 2.000 GHz SWP 1.250 sec

MKR 1: 1.009687500 GHz, -15.91 dBm

892 Mode



REF -10.0 dBm

5 dB/div ATTEN 0 dB INT REF

START 500.00000 MHz CENTER 1.500000 GHz STOP 2.500000 GHz

RBW 5000 KHz SPAN 2.000 GHz SWP 1.250 sec

MKR 1: 2.091250000 GHz, -39.54 dBm

1910 Mode

Demo 5

Jamming cellular bands

Just kidding!!!

- Jamming cellphone bands is evil
    - Knocks out everything: GSM, CDMA, 3G, etc.
- Impossible to defend against
- Only a short burst needed...
    - WAY too offensive for this demo
- How far would the DoS extend?
    - I have a 100W amplifier and good antennas
    - That'll probably DoS most of Las Vegas
    - Obviously not going to happen :)

Receive gain

- BTS can tell handset (effectively):
  - “Treat my signal as if it were X dB stronger”
- The handset will go along with this
  - It's an instruction from the BTS – has to comply
- Attacker can configure this in his BTS settings
  - OpenBTS doesn't support it yet
- This method is the essence of the R&S patents.

Inbound calls

- IMSI catcher is a completely separate network
  - Carrier thinks phone is off or has no signal
- If phone is off, carrier sends calls to voicemail
  - Where else is it going to go?
- Result: Attacker doesn't see inbound calls

- Solution: Spoof the caught IMSI
  - At least as far as the “real” network.

Spoofing to the Carrier

- Already know IMSI/IMEI
  - Don't know Ki (secret key that authenticates IMSI)

- Connect to carrier with victim IMSI
- Pass RAND challenge along to victim
- Break victim's keystream, recover session key
- Re-use session key to talk to carrier

Breaking the session key

- ONLY time when crypto attacks are needed
  - For an IMSI catcher, at least
- Attacker negotiates weakest cipher possible
  - A5/2 ideally, trivial to crack
- Handset may reject A5/2 (some do)
  - Negotiate A5/1 instead, need rainbow tables for Kc
- Either way, outbound calls are plaintext.

Are there solutions?

- Not really - GSM is badly broken.
- Many of these weak configs are needed
  - GSM is global, countries have differing crypto laws
- Primary solution: Use 3G!
  - 3G cipher is showing cracks, not broken yet
- Secondary solution: More crypto
  - Treat GSM like the internet – encrypt before using
- Best solution: Turn off 2G GSM
  - We're at 3.5G(HSPA), 4G on the horizon.

Demo 6

Making and recording calls

Questions?

@ChrisPaget
ivegotta@tombom.co.uk