Discovering and Triangulating Rogue Cell Towers

Eric Escobar, PE

Security Engineer

Barracuda

What is a rogue cell tower?

- A device created by governments or hackers that has the ability to trick your phone into thinking it's a real cell phone tower.
- Also known as IMSI catchers, interceptors, cell-site simulators, Stingrays, and probably a few more.
- Rogue cell towers have the ability to collect information about you indirectly through metadata (call length, dialed numbers)
- In some conditions can collect content of messages, calls, and data.

Barracuda

How are cell simulators used today?

At Home (In the United States):

- IMSI-catchers are used by US law enforcement agencies to help locate, track, and collect data on suspects.
- ACLU has identified 66 agencies and 24 states that own stingrays.
- Used to monitor demonstrations in the US
  - Used in Chicago political protests
- It's possible to make an IMSI-catcher at home
  - DEFCON 18: Practical Cellphone Spying - Chris Paget

Barracuda

How are cell simulators used today?

Abroad:

- Reported use in Ireland, UK, China, Germany, Norway, South Africa
- Chinese spammers were caught sending spam and phishing messages.
- Used by governments and corporations alike.

Barracuda

What's the IMSI in "IMSI-catcher"?

- IMSI stands for International Mobile Subscriber Identity.
- Is used as a means of identifying a device on the cell network.
- Typically 15 digits long
- Contains general information about you device (Country & Carrier)
  - Mobile Country Code – MCC
  - Mobile Network Code – MNC
  - Mobile Subscription Identification Number – MSIN

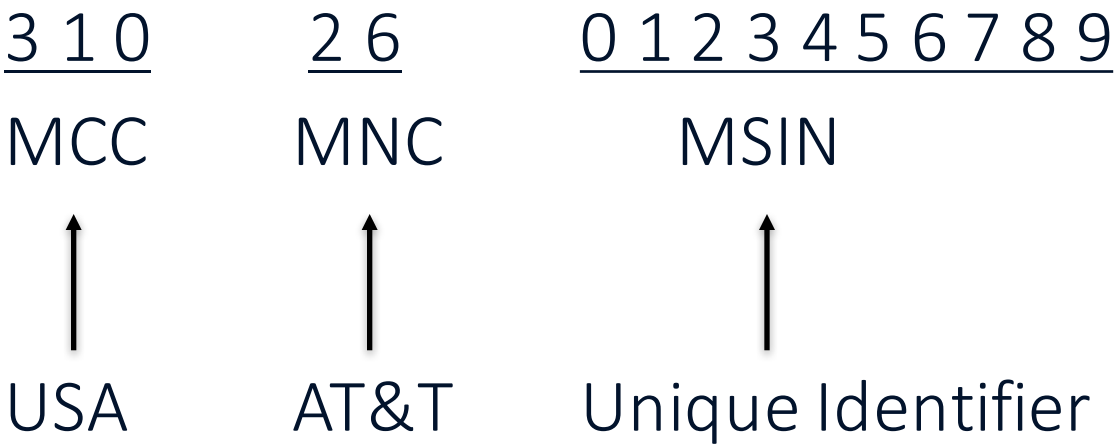
Barracuda

What’s an IMSI?

IMSI = Unique identifier to your device

Barracuda

Sample IMSI:



Barracuda

Why you should care?

- Your phone will connect automatically to cell site simulators.
- Thieves can steal your personal information.
- Hacker's can track where you go, who you're talking to, and grab all sorts of other data about you.
- Your digital life can be sniffed out of the air by anyone with some technical chops, and a laptop.
- Your company could be leaking trade secrets.
- Your privacy is at risk.

Barracuda

Why build a detector?

- There are some great apps for Android phones and that have the ability to detect cell tower anomalies.
  - You need specific phone models & root for this to work
- I wanted a device that met the following conditions:
  - Cheap ~$50/device
  - I wanted to set it and forget it.
  - I wanted to be alerted to any anomalies.
  - I wanted the ability to network multiple devices together.

How do you detect a rogue cell tower?

- Every cell tower (Base Transceiver Station, BTS) beacons out information about itself
  - ARFCN – Absolute radio frequency channel number
  - MCC – Mobile Country Code
  - MNC – Mobile Network Code
  - Cell ID – Unique identifier (within a large area)
  - LAC – Location area code
  - Txp – Transmit power maximum
  - Neighboring cells

Barracuda

How do you detect a rogue cell tower?

- Typically these values remain constant:
  - ARFCN – Absolute radio frequency channel number
  - MCC – Mobile Country Code
  - MNC – Mobile Network Code
  - Cell ID – Unique identifier (within a large area)
  - LAC – Location area code
  - Txp – Transmit power maximum
  - Neighboring cells
  - Power level

Barracuda

How do you detect a rogue cell tower?

- If values deviate from what's expected it can mean that there is maintenance taking place.
- It can mean changes are being made to the network.
- It could also mean that there is a rogue cell tower is nearby!
- The idea is to get a baseline of your cellular neighborhood over a period of time.
- It would be like keeping an eye on the cars that come in and out of your neighborhood, after a while you begin to know which doesn't belong.

Barracuda

How do you detect a rogue cell tower?

- Examples:
  - A new tower (Unknown Cell ID), high transmission power
  - Mobile country code mismatch
  - Mobile network code mismatch
  - Frequency change
  - Location Area Code mismatch

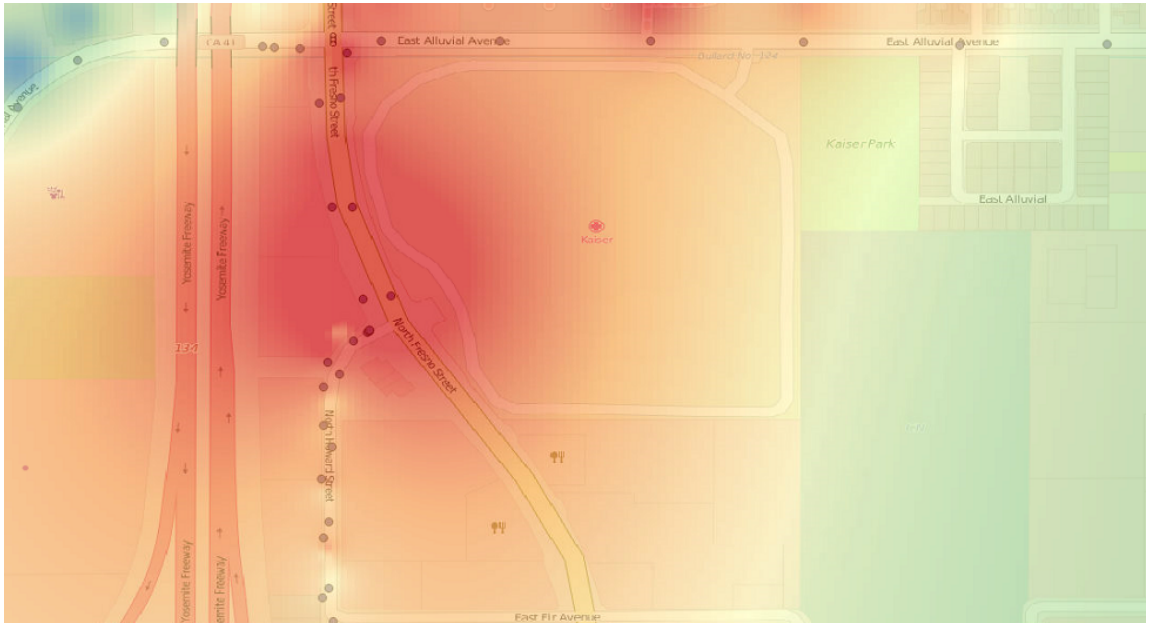
Barracuda

How do you locate a tower?

- Combine unique cell tower data, receive power, and location.
- One detector can be moved around with an onboard GPS
  - Readings of unique tower identifiers, power level and GPS coordinates allow for a single detector to create a map.
  - Some math, open source GIS software, and pretty colors can approximate locations of towers or possible rogue towers

Barracuda

How do you locate a tower?



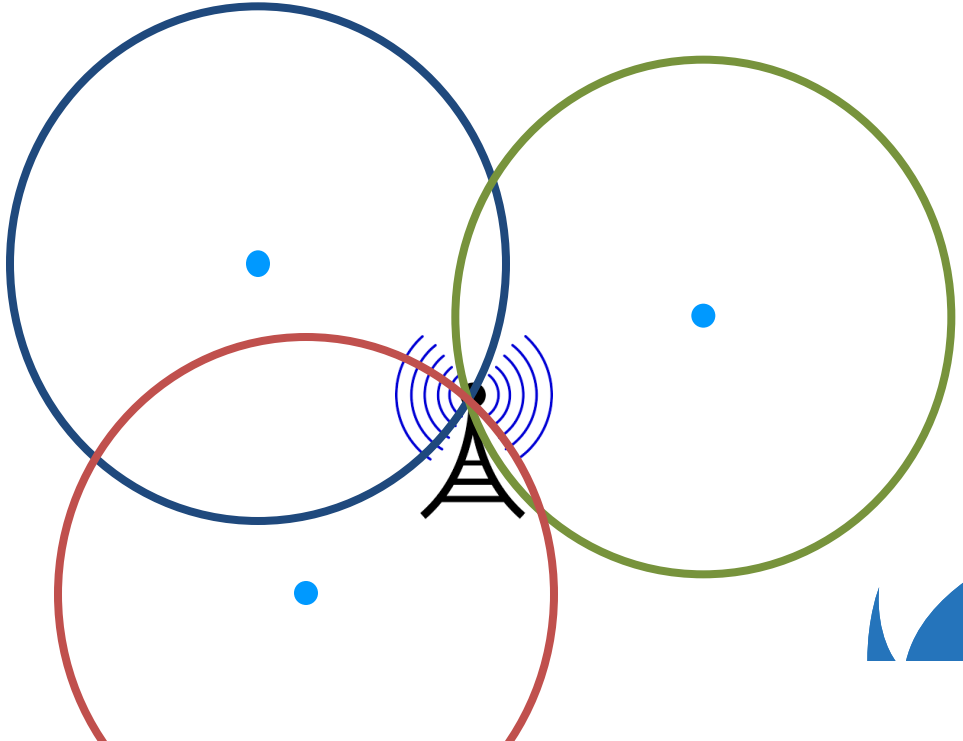
Barracuda

How do you locate a tower?

- Multiple detectors with known locations allow for trilateration of the suspected rogue tower.
- Receive power and distance are not inversely proportional
  - Regression formulas were required to be calculated in order to fine tune the results.
  - Less accurate but still pretty good

Barracuda

How do you locate a tower?



Barracuda

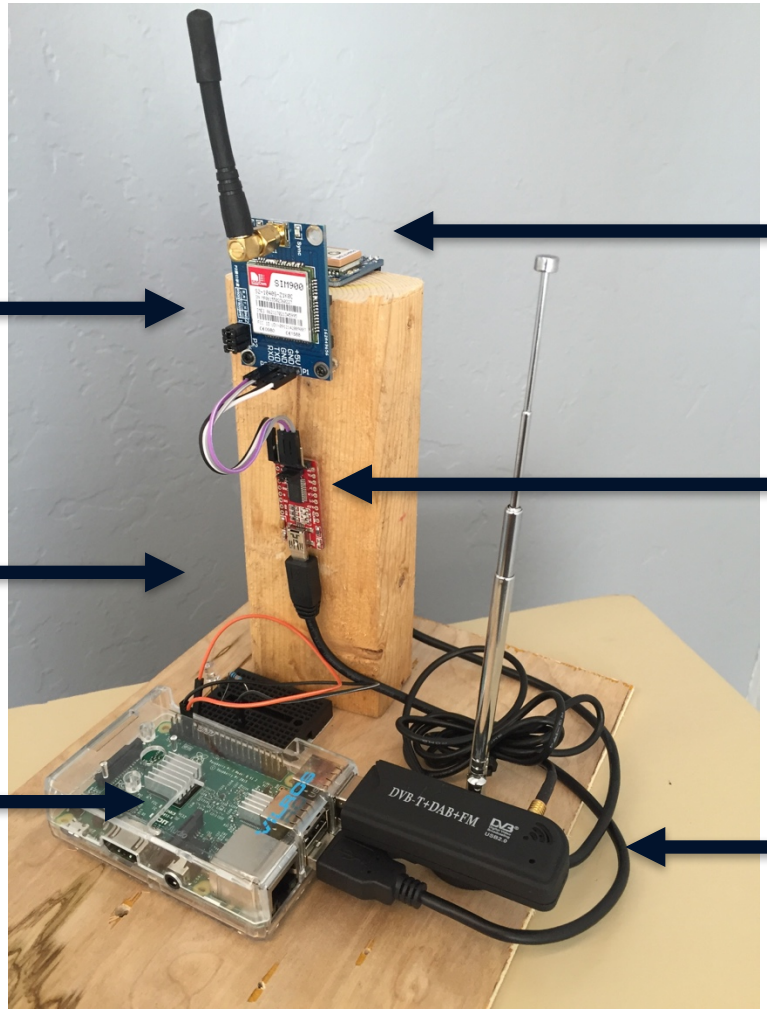
What’s the build?

- Raspberry Pi 3, power adapter, SD card (running stock Raspbian)
- SIM900 GSM Module
- Serial GPS module
- TV tuner software defined radio
- *Scrap wood & hot glue*

Barracuda

Brace yourself…
this is quite literally a hack.

Barracuda



SIM 900 Cell Module

GPS Module

Serial to USB

Scrap wood & hot glue

Raspberry Pi

Software defined radio (USB TV Tuner)

Barracuda

SIM900

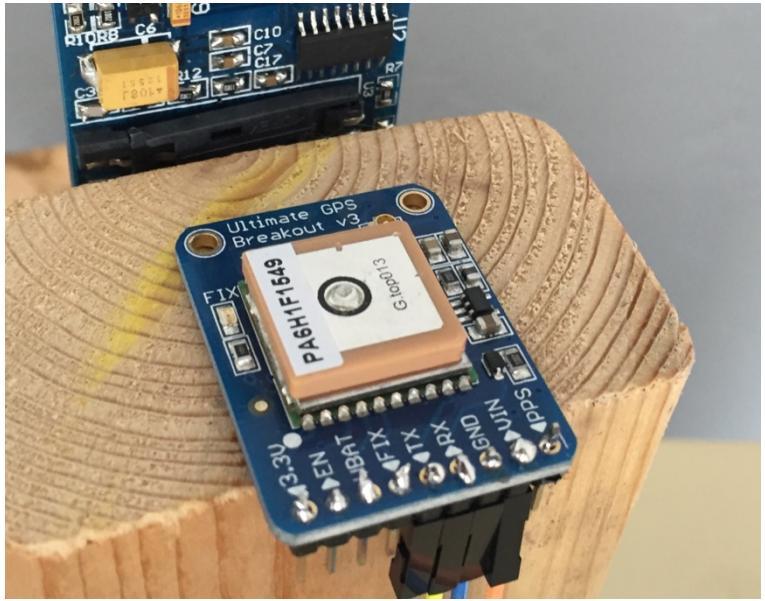
- SIM900 Engineering mode
  - Seven towers with the highest signal
  - Gives you a ton of information via a serial connection
  - No SIM card is required for engineering mode

Read Command **AT+CENG?**	Response Engineering Mode is designed to allow a field engi network information received by a handset, when th idle mode or dedicated mode (that is: with a call act engineer is able to view network interaction for the the handset is currently registered with) or for the n TA returns the current engineering mode. The netw including serving cell and neighboring cells are retu <mode>=1 or <mode>=2. <cell> carry with them c interaction. **+CENG: <mode>,<Ncell>** **[+CENG:** **<cell>,"<arfcn>,<rxl>,<rxq>,<mcc>,<mnc>,<bsic>,<cellid>,<rla>,** **<txp>,<lac>,<TA>"** **<CR><LF>+CENG:** **<cell>,"<arfcn>,<rxl>,<bsic>[,<cellid>],<mcc>,<mnc>,<lac>"…]** **OK**

Barracuda

GPS Serial

- Adafruit Ultimate GPS module
  - Fixes position quickly.
  - Good indoor reception
  - Works exactly how you would expect



Barracuda

Raspberry Pi 3

- Stock Raspbian OS (debian for pi)
- Pi 3 has enough power to run a SDR
- Has four USB ports for serial adapters
- Easily powered by a USB battery pack

Barracuda

TV Tuner

- $20 Software defined radio
- Wide range of frequencies
- Github: Gr-Gsm
  - Can listen to raw GSM traffic
  - See all the raw frames
  - Not necessary for locating cell towers
  - Provides deeper insights

Barracuda

Data collection:

- Everything dumps to a SQLite database for later use

```
lect * from CellData;
  time        arfcn       rxl         mcc         mnc         bsic        cellid      lac         l
  ----------  ----------  ----------  ----------  ----------  ----------  ----------  ----------  -
  1467249192  0694        14          310         260         35          1799        12c         3
  1467249192  0696        16          310         260         28          1cf3        12c         3
  146                                                                                 12c         3
  146 lat         lon          satellite   gps_quality  altitude    altitude_units     12c         3
  146 ----------  -----------  ----------  -----------  ----------  --------------     0           3
  146 36.84029    -119.770985  8           2            105.1       M                  0           3
  146 36.84029    -119.770985  8           2            105.1       M                  0           3
  146 36.84029    -119.770985  8           2            105.1       M                  12c         3
  146 36.84029    -119.770985  8           2            105.1       M                  12c         3
  146 36.84029    -119.770985  8           2            105.1       M                  12c         3
  146 36.84029    -119.770985  8           2            105.1       M                  12c         3
  146 36.84029    -119.770985  8           2            105.1       M                  0           3
  146 36.84029    -119.770986  8           2            105.1       M                  0           3
  146 36.84029    -119.770986  8           2            105.1       M                  0           3
  146 36.84029    -119.770986  8           2            105.1       M                  12c         3
  146 36.84029    -119.770986  8           2            105.1       M                  12c         3
      36.84029    -119.770986  8           2            105.1       M
      36.84029    -119.770986  8           2            105.1       M
      36.84029    -119.770986  8           2            105.1       M
      36.84029    -119.770986  8           2            105.1       M
      36.84029    -119.770986  8           2            105.1       M
      36.84029    -119.770986  8           2            105.1       M
```

Barracuda

Questions?