Discovering and Triangulating Rogue Cell Towers

Eric Escobar, PE
Security Engineer
A bit about me:

- Started off in Civil Engineering (MS, PE)
- Always loved computers
- Nerded out on all things wireless
  - Licensed HAM
- I love to automate things
  - Chicken coop
  - Sprinklers
- Caught the DEF CON bug
  - Wireless CTF
A bit about what I do:

- Security Engineer for Barracuda Networks
  - Incident Response
  - Pentesting
  - Red Team, Blue Team
  - Social Engineering
  - Phishing Campaigns
  - Bug bounty
  - Infrastructure scanning
  - Product team relations
  - 2FA, IPAM
Here’s what we are going to cover:

• What is a rogue cell tower?
• Why should you care about rogue cell towers?
• How can you detect a rogue cell tower?
• How do you find a rogue cell tower?
• How do you build a detector at home?
• You’ve detected a rogue tower... now what?
What is a rogue cell tower?

• A device created (or purchased) by companies, 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.
How are cell simulators used today?

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
  • IMSI Catcher Counter-Surveillance Freddy Martinez
• It’s possible to make an IMSI-catcher at home
  • DEFCON 18: Practical Cellphone Spying - Chris Paget
How are cell simulators used today?

Further reading:
• EFF.org – Cell-site simulator FAQ
• ACLU – “Stingray Tracking Devices: Who’s Got Them”
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.
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
What’s the IMSI in “IMSI-catcher”?

**MNC & MCC**

- All country codes (MCC) are available on Wikipedia
- All network codes (MNC) are available on Wikipedia
What’s an IMSI?

IMSI = Unique identifier to your device
Sample IMSI:

<table>
<thead>
<tr>
<th>MCC</th>
<th>MNC</th>
<th>MSIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>310</td>
<td>026</td>
<td>0123456789</td>
</tr>
</tbody>
</table>

- **MCC**: 310 (USA)
- **MNC**: 026 (AT&T)
- **MSIN**: Unique Identifier

Country: USA
Carrier: AT&T

Barracuda
Why you should care? – A short story

• You are a fish about to be caught in one big net
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, and some hardware that is CHEAP.
• Your company could be leaking trade secrets.
• Your privacy is at risk.
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
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
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.
How do you detect a rogue cell tower?

<table>
<thead>
<tr>
<th>ARFCN</th>
<th>Channel</th>
<th>0694</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCC</td>
<td>Country Code</td>
<td>310</td>
</tr>
<tr>
<td>MNC</td>
<td>Network Code</td>
<td>026</td>
</tr>
<tr>
<td>Cell ID</td>
<td>Unique ID</td>
<td>1799</td>
</tr>
<tr>
<td>Power Level</td>
<td></td>
<td>Constant</td>
</tr>
</tbody>
</table>
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
Why locate a tower?

• So you’ve found a tower
• Cell tower or white van?
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
How do you locate a tower?

(There’s probably a tower there)
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
- TDOA – Time distance of arrival
  - I don’t have accurate enough timings
How do you locate a tower?

Trilateration vs Triangulation
(I get it, but some people don’t)
Triangulation
Triangulation
Triangulation

This is the “angle” in triangulation
Triangulation
Triangulation

- Looking forward this is a feature I would like to add
- Conceptually makes sense, I haven’t tried it out
Triangulation
Triangulation
How do you locate a tower?

My detector **technically** uses trilateration
How do you locate a tower?
How do you locate a tower?
How do you locate a tower?

Detector 1

1000ft
How do you locate a tower?

Detector 1

Detector 2
How do you locate a tower?
How do you locate a tower?

Detector 1

Detector 2

Detector 3
How do you locate a tower?
Trilateration
Trilateration

There are scripts that do the math...
How do you locate a tower?

Power is not linear
- More data
- More monitoring nodes
- Back of the envelope math
- Cell towers have different sectors
How do you locate a tower?

Multipoint trilateration

• Drive around collecting lots of data
• Gives you way more accurate results
• Tested on real towers
How do you locate a tower?

(There’s probably a tower there)
What’s the build?

- Raspberry Pi 3, power adapter, SD card (running stock Raspbian)
- SIM900 GSM Module
- Serial GPS module
- Software defined radio (depending where you are)
- *Scrap wood & hot glue*
Brace yourself...
this is quite literally a hack.
What’s does it cost?

- $10 Raspberry Pi Zero
- $5 Wireless adapter
- $5 USB hub
- $5 SD card (running stock Raspbian)
- $27 SIM900 GSM Module
- $16 Serial GPS module (Optional)
- Free? Scrap wood & hot glue

----------------

$52 Total
SIM900

- SIM900
- Seven towers with the highest signal
  - Gives you a ton of information via a serial connection
  - No SIM card is required for engineering mode
  - Does not sniff traffic
SIM900 or Field test mode

- Many phones will let you see this information

- iPhones
  - Pretend to dial a number
  - *3001#12345#*
  - Hit call

- Android
  - Field test mode can vary phone to phone
  - Google for apps that let you see this info
AT
OK
AT+CENG=1,1
OK
AT+CENG?
+CENG: 1,1
+CENG: 0,"0235,63,99,310,410,36,109f,00,69,7935,255"
+CENG: 1,"0181,48,12,10a1,310,410,7935"
+CENG: 2,"0239,36,46,0109,310,410,7930"
+CENG: 3,"0130,36,169,04d5,310,410,7935"
+CENG: 4,"0233,32,180,10a0,310,410,7935"
+CENG: 5,"0238,17,165,04d4,310,410,7935"
+CENG: 6,"65535,255,00,0000,000,00,0"

OK
SIM900

```
+CENG:1,"0181,48,12,10a1,310,410,7935"
```
GPS Serial

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

NMEA Data - National Marine Electronics Association
# GPS Serial

```
$GPGGA,151332.000,3606.7062,N,11510.2864,W,1,06,1.07,720.1,M,-24.4,M,,*5E
```

<table>
<thead>
<tr>
<th>lat</th>
<th>lon</th>
<th>satellite</th>
<th>gps_quality</th>
<th>altitude</th>
<th>altitude_units</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36.84029</td>
<td>-119.770985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
</tbody>
</table>

---

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
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

WARNING!!!
Data collection:

- Everything dumps to a SQLite database for later use

```
SELECT * FROM CellData;
```

<table>
<thead>
<tr>
<th>time</th>
<th>arfcn</th>
<th>rxl</th>
<th>mcc</th>
<th>mnc</th>
<th>bsic</th>
<th>cellid</th>
<th>lac</th>
</tr>
</thead>
<tbody>
<tr>
<td>146724912</td>
<td>0694</td>
<td>14</td>
<td>310</td>
<td>260</td>
<td>35</td>
<td>1799</td>
<td>12c</td>
</tr>
<tr>
<td>146724912</td>
<td>0696</td>
<td>16</td>
<td>310</td>
<td>260</td>
<td>28</td>
<td>1cf3</td>
<td>12c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lat</th>
<th>lon</th>
<th>satellite</th>
<th>gps_quality</th>
<th>altitude</th>
<th>altitude_units</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
<tr>
<td>36 029</td>
<td>-119.985</td>
<td>8</td>
<td>2</td>
<td>105.1</td>
<td>M</td>
</tr>
</tbody>
</table>
Let’s make it pretty:

• QGIS
  • Free and Open Source Geographic Information System
  • IDW – Inverse Distance Weighting
  • OpenLayers Plugin – Maps & GIS data
  • Python command line automation
  • Makes it very easy to visualize
Let’s make it pretty:

- QGIS Python Console
  - Once you’re comfortable making maps manually you can begin automatically generating them

```python
output_file = open('c:/Users/eric/Desktop/wifidata.txt', 'w')
for f in layer.getFeatures():
    geom = f.geometry()
    line = '%s, %f, %f
    % (f['power'],
        geom.asPoint().y(), geom.asPoint().x())
    unicode_line = line.encode('utf-8')
    output_file.write(unicode_line)
output_file.close()
```
Let’s make it pretty:
There’s a disturbance in the force

• How do you get alerts?
  • Email
  • SMS - Twilio
  • Push notifications - PushOver
There’s a disturbance in the force

- Your detector goes off now what?
  - Turn off your phone
  - Start looking at the data
  - Go on a road trip
Want to help?
Questions?

defconjusticebeaver@gmail.com

RagingSecurity.Ninja