Detecting Fake 4G Base Stations in Real Time

Cooper Quintin - Senior Security Researcher - EFF Threat Lab
Defcon Safe Mode With Networking 2020
Intro

• Cooper Quintin
  – Senior security researcher
  – Has a toddler (dad jokes)
  – Former teenage phone phreak

• EFF
  – Member supported non profit
  – Defending civil liberties
  – 30 years

• Threat lab
None of this research would have been possible without her hard work. This is as much her project as mine.

Twitter: @rival_elf
Technology that Targets At Risk People

- Activists, human rights defenders, journalists, domestic abuse victims, immigrants, sex workers, minority groups, political dissidents, etc...

- Goals of this technology
  - Gather intelligence on opposition
  - Spy extraterritorially or illegally
  - Locate and capture
  - Extortion
  - Harass and intimidate
  - Stifle freedom of expression
Jeff Bezos Can Afford a Security Team

Cybersecurity and AV companies care about the types of malware that affects their customers (usually enterprise.) We get to care about the types of technology the infringe on civil liberties and human rights of at risk people.

This guy is not at risk.
Our Goals

- Protect people
- Broaden our communities’ understanding of threats and defenses
- Expose bad actors
- Make better laws
Previous Project

Stalkerware

Dark Caracal
What We are Going to Talk About Today

- Cell-site simulators AKA Stingrays or IMSI Catchers
- How they work
- Previous efforts to detect them
- A new method to detect them
- How to fix the problem
Cell Technology Overview

- **UE** - The phone - User Equipment
- **IMSI** - International Mobile Subscriber ID - ID for the SIM card
- **IMEI** - International Mobile Equipment ID - ID for the hardware
- **eNodeB** - Base station, what the UE is actually communicating with.
- **EARFCN** - The frequency a UE/EnodeB is transmitting on
- **Sector** - A specific antenna on the base station
Cell Technology Overview

- MIB - Master Information block, broadcast by the enodeb and tells where to find the SIB
- SIB - System information block, contains details about the enodeb
- PLMN = MCC + MNC, Public Land Mobile Network
Cell Technology Overview

IMSI catcher, Stingray, Hailstorm, fake base station == cell-site simulator (CSS)

This is acronym hell and I’m sorry.
Cell Technology Overview

![Diagram of cell technology overview](image-url)
Stingray
What Changed Between 2G and 4G

- eNodeB and UE mutually authenticate
- Better encryption between eNodeB and UE
- No longer naively connect to the strongest tower
How do 4G CSS Work

- What are the vulns next gen CSS are taking advantage of?
- Pre authentication handshake attacks
- Downgrade attacks

Gotta catch em all whitepaper by Yomna
Pre-Authentication Vulnerabilities

• 4G has a glass jaw
• Even though the UE authenticates the tower there are still several messages that it sends, receives, and trusts before authentication happens or w/o authentication
• This is the weak spot in which the vast majority of 4G attacks happen
Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil - Hussein et al. 2019
Here there be dragons
How Often are CSS Being Used

- ICE/DHS - hundreds of times per year
- Local law enforcement
  - Oakland - 1-3 times per year
    - https://oaklandprivacy.org/oakland-privacy-sues-vallejo/
  - Santa Barbara PD - 231 times in 2017
    - https://www.eff.org/deeplinks/2019/05/eff-asks-san-bernardino-court-review-device-search-and-cell-site-simulator
How Often are CSS Being Used

- **Foreign Spies**
  - IMSI Catchers in DC

- **Cyber Mercenaries**
  - NSO Group

- **Criminals**
  - [https://venturebeat.com/2014/09/18/the-cell-tower-mystery-gripping-america-has-now-been-solved-or-has-it/](https://venturebeat.com/2014/09/18/the-cell-tower-mystery-gripping-america-has-now-been-solved-or-has-it/)
Previous Efforts to Detect CSS

App Based
- AIMSICD
- Snoop Snitch
- Darshark

Strengths
- Cheap
- Easy to use

Weaknesses
- Limited data
- Lots of false positives
- False negatives?
Previous Efforts to Detect CSS

Radio Based
• Seaglass
• SITCH
• Overwatch

Strengths
• Better data
• Lower level information

Weaknesses
• Harder to set up, use, interpret
• Cost of hardware
• Can’t transmit
Previous Efforts to Detect CSS
I HAVE NO IDEA WHAT I'M DOING
Can we detect 4G IMSI Catchers?

- How can we improve on previous attempts
  - Lower level data
  - See all towers not just what we are connecting to
  - Compare that data over time
  - Look at 4G antennas!
  - Verify results!
Introducing Crocodile Hunter
Crocodile Hunter Software Stack

- Backend based on SRSLTE
  - Open source LTE software stack
  - Written in C++
  - Communicates with frontend over a local socket
- Python for heuristics, database and frontend
  - Get data from socket
  - Add it to database
  - Run heuristics
  - Display tower locations
- API for sharing data
Crocodile Hunter Hardware Stack

- Laptop / Raspberry Pi
- USB GPS Dongle
- SDR compatible with SRSLTE: BladeRF, Ettus B200
- LTE Antennas
- (Battery for Pi)
Crocodile Hunter Hardware Stack
Workflow

1. Decode MIB and SIB1 for all the cells that we can see and record them.
2. Map the probable location of cells
3. Look for anomalies in the readings
4. Locate suspicious cells and confirm results
Decode MIB and SIB1

- SRSLTE scans a list of EARFCNS
- If we find a mib we decode mib and sib and send over socket
# Database

```sql
MariaDB [dreamforce]> describe tower_data;
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>mcc</td>
<td>int(11)</td>
</tr>
<tr>
<td>mnc</td>
<td>int(11)</td>
</tr>
<tr>
<td>tac</td>
<td>int(11)</td>
</tr>
<tr>
<td>cid</td>
<td>int(11)</td>
</tr>
<tr>
<td>phyid</td>
<td>int(11)</td>
</tr>
<tr>
<td>earfcn</td>
<td>int(11)</td>
</tr>
<tr>
<td>lat</td>
<td>float</td>
</tr>
<tr>
<td>lon</td>
<td>float</td>
</tr>
<tr>
<td>timestamp</td>
<td>datetime</td>
</tr>
<tr>
<td>rssi</td>
<td>float</td>
</tr>
<tr>
<td>suspiciousness</td>
<td>int(11)</td>
</tr>
<tr>
<td>frequency</td>
<td>float</td>
</tr>
<tr>
<td>enodeb_id</td>
<td>int(11)</td>
</tr>
<tr>
<td>sector_id</td>
<td>int(11)</td>
</tr>
<tr>
<td>cfo</td>
<td>float</td>
</tr>
<tr>
<td>rsrq</td>
<td>float</td>
</tr>
<tr>
<td>snr</td>
<td>float</td>
</tr>
<tr>
<td>rsrp</td>
<td>float</td>
</tr>
<tr>
<td>tx_pwr</td>
<td>float</td>
</tr>
<tr>
<td>est_dist</td>
<td>float</td>
</tr>
<tr>
<td>raw_sib1</td>
<td>varchar(255)</td>
</tr>
<tr>
<td>classification</td>
<td>enum('unknown','legitimate','small_cell','suspicous','CSS')</td>
</tr>
<tr>
<td>external_db</td>
<td>enum('not_present','unknown','wigele','opencellid')</td>
</tr>
</tbody>
</table>
Mapping out antennas in real time

- Using trilateration and distance estimates we can figure out where all the towers are
- Compare this to a ground truth such as wigle or opencellid
Trilateration vs Triangulation

**Trilateration**

\[ L = R_1 \cap R_2 \cap R_3 \]

**Triangulation (Bearing)**

\[ L = B_1 \cap B_2 \cap B_3 \]
Looking for Anomalies

• Cells moving
• Cells that change signal strength
• Cells that aren’t where they should be
• Cells changing parameters
• Cells missing parameters
• New cells
• Anomaly != CSS, that's why we have to verify
Why Don’t we Transmit?

EFF Lawyers

Wait. That’s illegal.
What we Found so Far

Cell on wheels at Dreamforce

CELL SITE SIMULATORS AREN'T ALWAYS THIS OBVIOUS

THAT'S WHY WE HAVE CROCODILE HUNTER
What we Found so Far

Suspicious eNodeBs in Washington DC

<table>
<thead>
<tr>
<th>ID</th>
<th>Frequency</th>
<th>Country Code</th>
<th>Count</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>653671</td>
<td>350-490</td>
<td>None</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>653671</td>
<td>310-410</td>
<td>None</td>
<td>4</td>
<td>1995</td>
</tr>
<tr>
<td>654486</td>
<td>310-410</td>
<td>None</td>
<td>3</td>
<td>1187</td>
</tr>
<tr>
<td>654538</td>
<td>310-410</td>
<td>None</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>654794</td>
<td>308-451</td>
<td>None</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>654794</td>
<td>310-410</td>
<td>None</td>
<td>3</td>
<td>221</td>
</tr>
</tbody>
</table>
## Washington DC

<table>
<thead>
<tr>
<th>earfcn</th>
<th>est_dist</th>
<th>external_db</th>
<th>Mhz</th>
<th>mcc</th>
<th>mnc</th>
<th>phyld</th>
<th>rsrp</th>
<th>rsrq</th>
<th>rssi</th>
<th>sid</th>
<th>snr</th>
<th>sus</th>
<th>tac</th>
</tr>
</thead>
<tbody>
<tr>
<td>5110</td>
<td>58.4614</td>
<td>Unknown</td>
<td>739.0</td>
<td>350</td>
<td>490</td>
<td>193</td>
<td>7.31153</td>
<td>-14.3092</td>
<td>-21.4078</td>
<td>167</td>
<td>-2.52688</td>
<td>59</td>
<td>4694</td>
</tr>
<tr>
<td>850</td>
<td>0.507082</td>
<td>Not_Present</td>
<td>1955.0</td>
<td>310</td>
<td>410</td>
<td>193</td>
<td>-4.16847</td>
<td>-12.1525</td>
<td>-32.1733</td>
<td>125</td>
<td>2.92086</td>
<td>30</td>
<td>4630</td>
</tr>
<tr>
<td>5110</td>
<td>38.2501</td>
<td>Not_Present</td>
<td>739.0</td>
<td>310</td>
<td>410</td>
<td>193</td>
<td>8.35644</td>
<td>-12.9575</td>
<td>-23.3778</td>
<td>133</td>
<td>3.90337</td>
<td>30</td>
<td>4630</td>
</tr>
<tr>
<td>850</td>
<td>0.662138</td>
<td>Wigle</td>
<td>1955.0</td>
<td>308</td>
<td>451</td>
<td>419</td>
<td>3.12503</td>
<td>-16.4038</td>
<td>-27.0273</td>
<td>10</td>
<td>-0.58374</td>
<td>50</td>
<td>4661</td>
</tr>
<tr>
<td>850</td>
<td>2.69926</td>
<td>Wigle</td>
<td>1955.0</td>
<td>310</td>
<td>410</td>
<td>419</td>
<td>4.28062</td>
<td>-13.3471</td>
<td>-27.7592</td>
<td>10</td>
<td>-0.356425</td>
<td>0</td>
<td>4661</td>
</tr>
<tr>
<td>850</td>
<td>1.55341</td>
<td>Wigle</td>
<td>1955.0</td>
<td>310</td>
<td>410</td>
<td>419</td>
<td>3.49412</td>
<td>-15.6305</td>
<td>-26.3221</td>
<td>10</td>
<td>-1.20262</td>
<td>0</td>
<td>4661</td>
</tr>
</tbody>
</table>
Ongoing Tests

- Latin America (FADe Project)
- DC
- NYC
- Your hometown (coming soon...)

Defcon Safe Mode // Aug 2020
Future Work

• Better heuristics
• Better location finding
• Machine learning for detection of anomalies
• Port to cheaper hardware
What’s With the Name?

Press F to pay respects to Steve
How Can we Stop Cell-Site Simulators

• End 2G support on iOS and Android now!
  – [https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be](https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be)

• Eliminate pre-authentication messages
  – TLS for the handshake with towers

• More incentives for standards orgs (3GPP), carriers, manufacturers, and OEMs to care about user privacy

• Nothing is foolproof but we aren’t even doing the bare minimum yet.
Key Takeaways

• We have a pretty good understanding the vulns in 4G which commercial cell-site simulators might exploit
• None of the previous IMSI catcher detector apps really do the job any more.
• We have come up with a method similar to established methods but targeting 4G.
• The worst problems of CSS abuse can be solved!
Thanks to the following people

- Yomna!
- The whole EFF crew
- Andy and Bob at Wigle
- Roger Piqueras-Jover
- Nima Fatemi with Kandoo, Surya Mattu, Simon
- Carlos and the FADE Project
- Karl Kosher, Peter Ney, and others at UW (SEAGLASS)
- Ash wilson (SITCH) and Eric Escobar (Defcon Justice Beaver)
- Kristin Paget
Thank you!

Cooper Quintin
Senior Security Researcher
EFF Threat Lab
cooperq@eff.org - twitter: @cooperq
https://github.com/efforg/crocodilehunter
References

2. https://github.com/srsLTE/srsLTE