SITCH

Open Source Cellular Counter-surveillance

About You

- Systems, network administration skills

- Interest in cellular network security

About Me

- Background in:
  - Systems/network engineering
  - Security automation/integration
- Currently in Strategic Engineering @ CloudPassage

“Thoughts and opinions expressed are my own, and not my employer’s. If you take anything away from this talk and act on it, I’m not responsible if you go to jail, become a pariah, or your dog stops liking you. Know the laws you’re subject to and operate accordingly.”

–Me

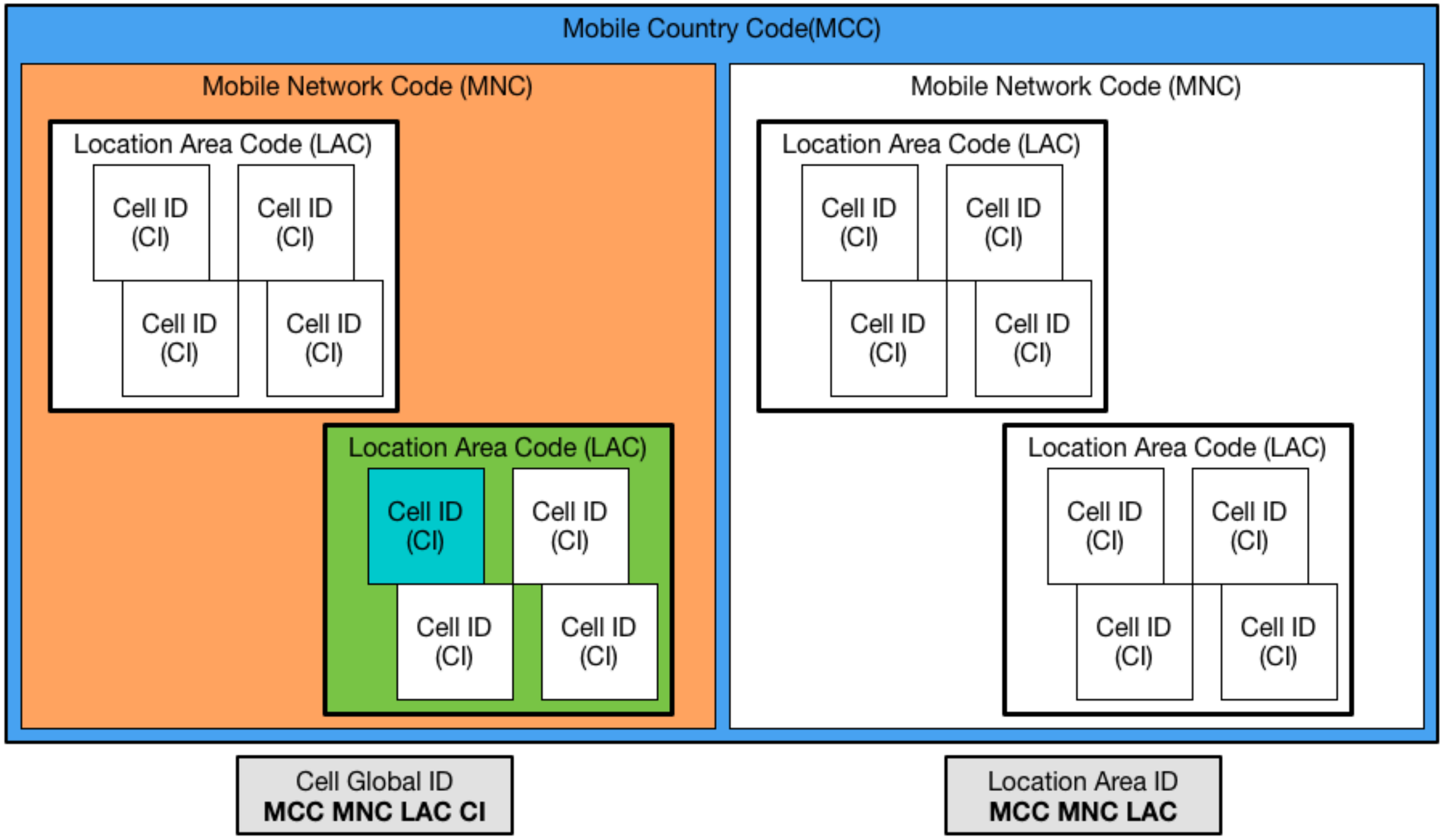
Why Care?

- Surveillance technology has been democratized
- Easy and inexpensive to build surveillance devices
- Homemade units are small and easy to conceal

Terminology

- **IMSI**
  - International Mobile Subscriber Identity
  - Stored in the SIM card, tied to your account
- **ARFCN**
  - Absolute Radio Frequency Channel Number
  - Licensed frequencies, tied to geographic area
- **BTS**
  - Base Transceiver Station
  - The physical device your cell phone connects to

GSM Addressing



Inspiration

- EvilBTS
  - Inexpensive (~$600)
  - Mimics a 2G cellular base station
- Femtocells
  - Free from carrier if you have bad reception
  - Hackable to record traffic (audio and SMS)

Challenges

- Cellular anomaly detection
    - Difficult
    - Expensive
- Attribution
    - Difficulty increases with reaction time

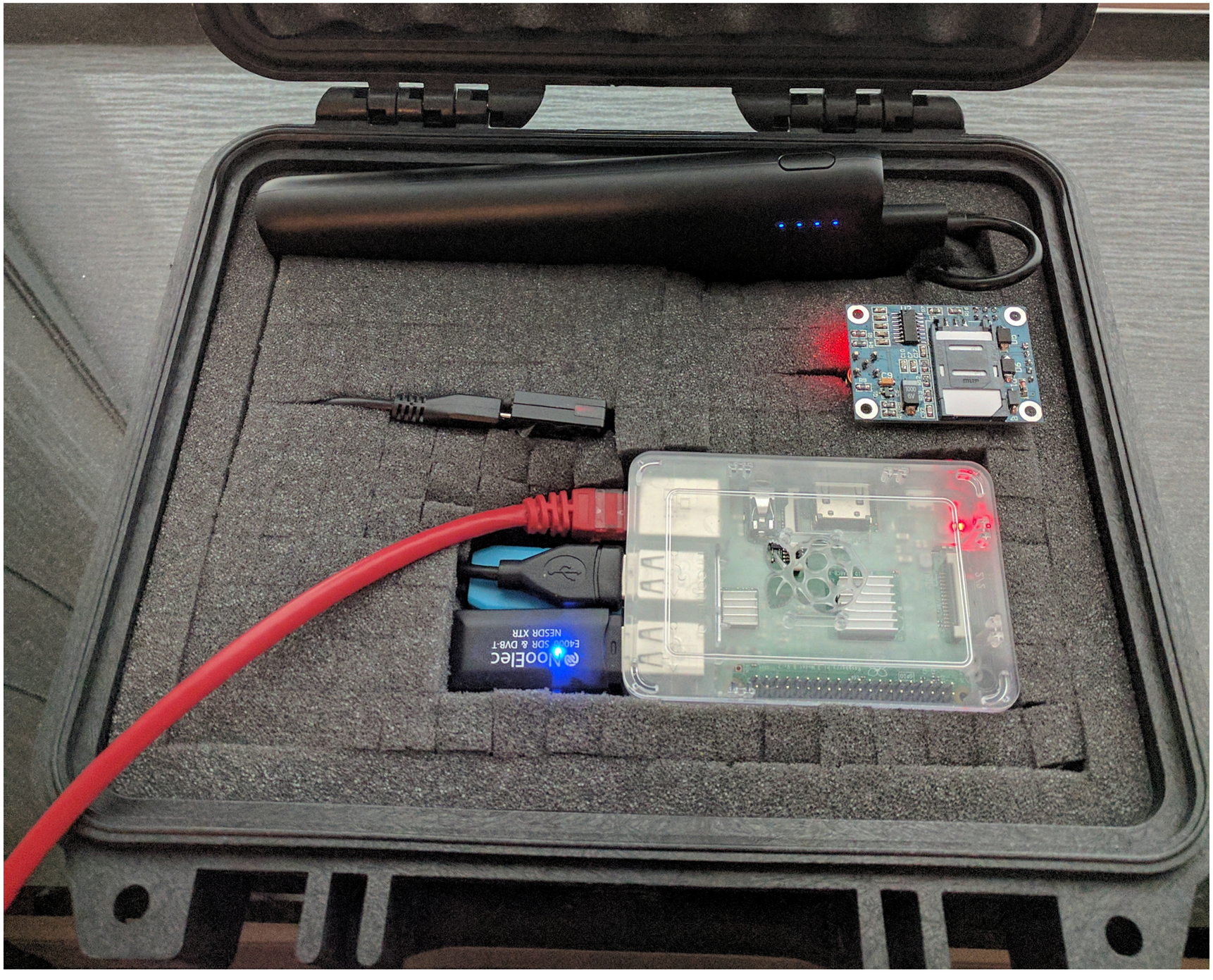
Design Goals

- Distributed sensors
- Easy, centralized administration
- Graceful scaling characteristics
- Enable rapid response

SITCH Components

- **Sensor**
  - Multiple radios
  - Initial detection and correlation
- **Service**
  - Aggregates information from all sensors
  - Secondary correlation
  - Sends alerts

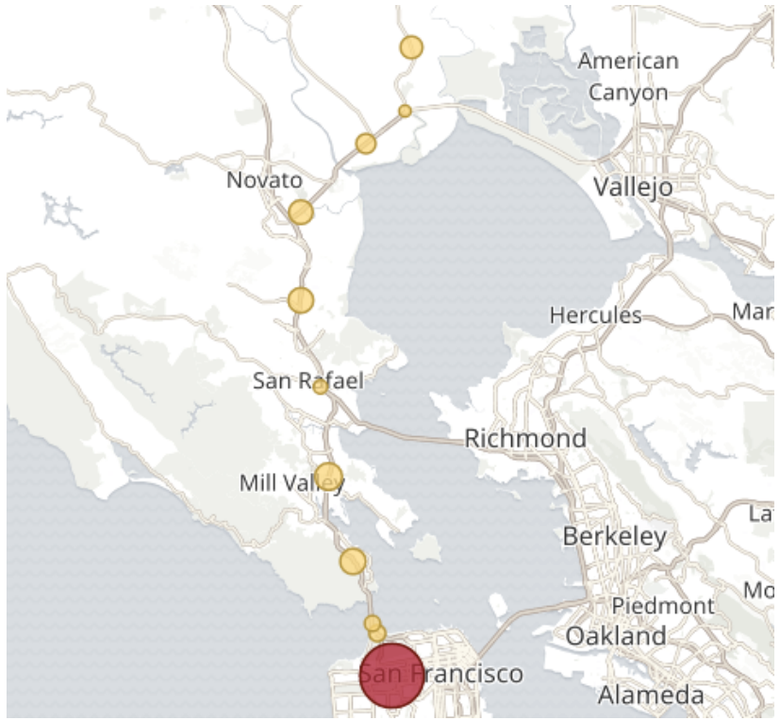
Sensor

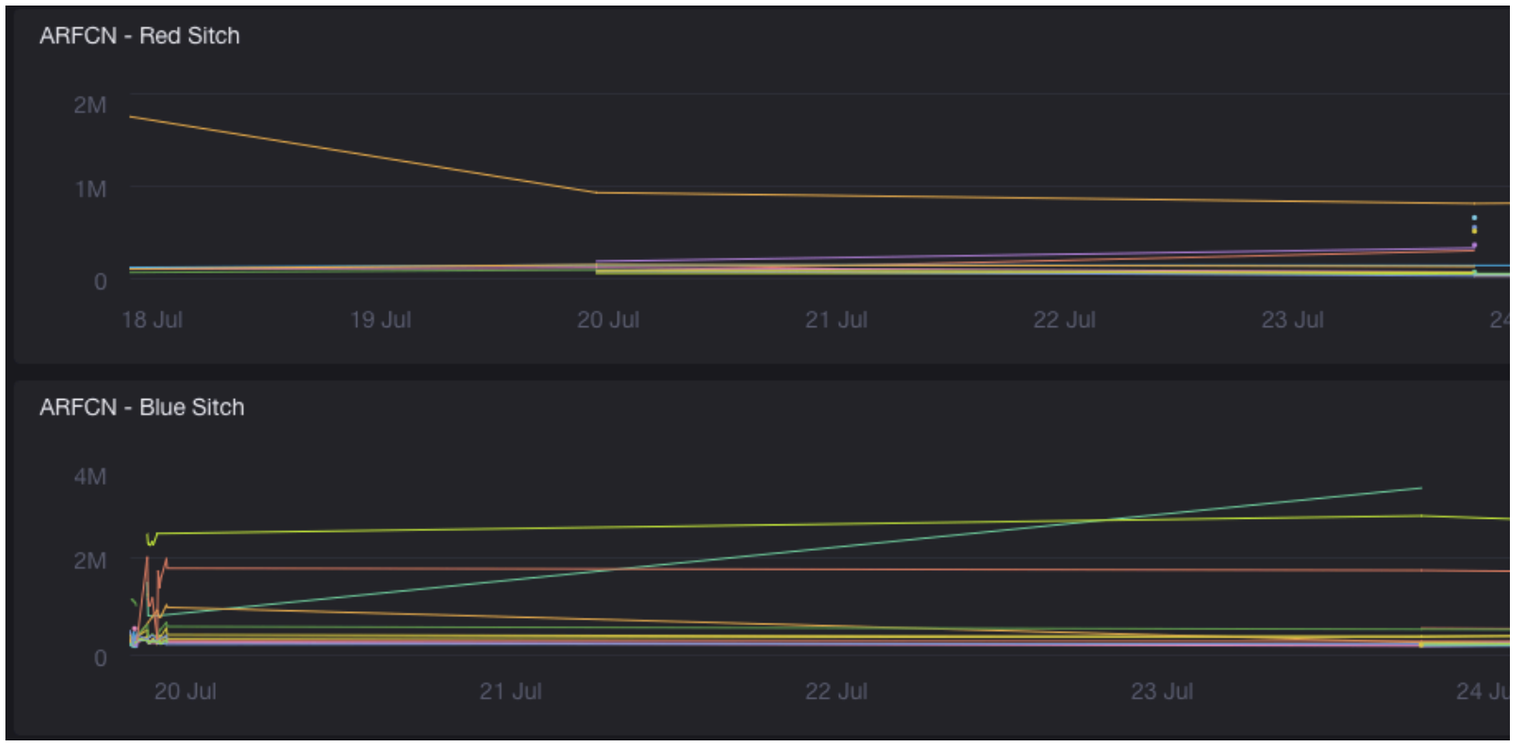


Sensor

- CPU: Raspberry Pi 2/3
- Radios: SDR, GPS, GSM
- Database/Geo correlation
  - FCC License DB
  - OpenCellID DB

Service/Management





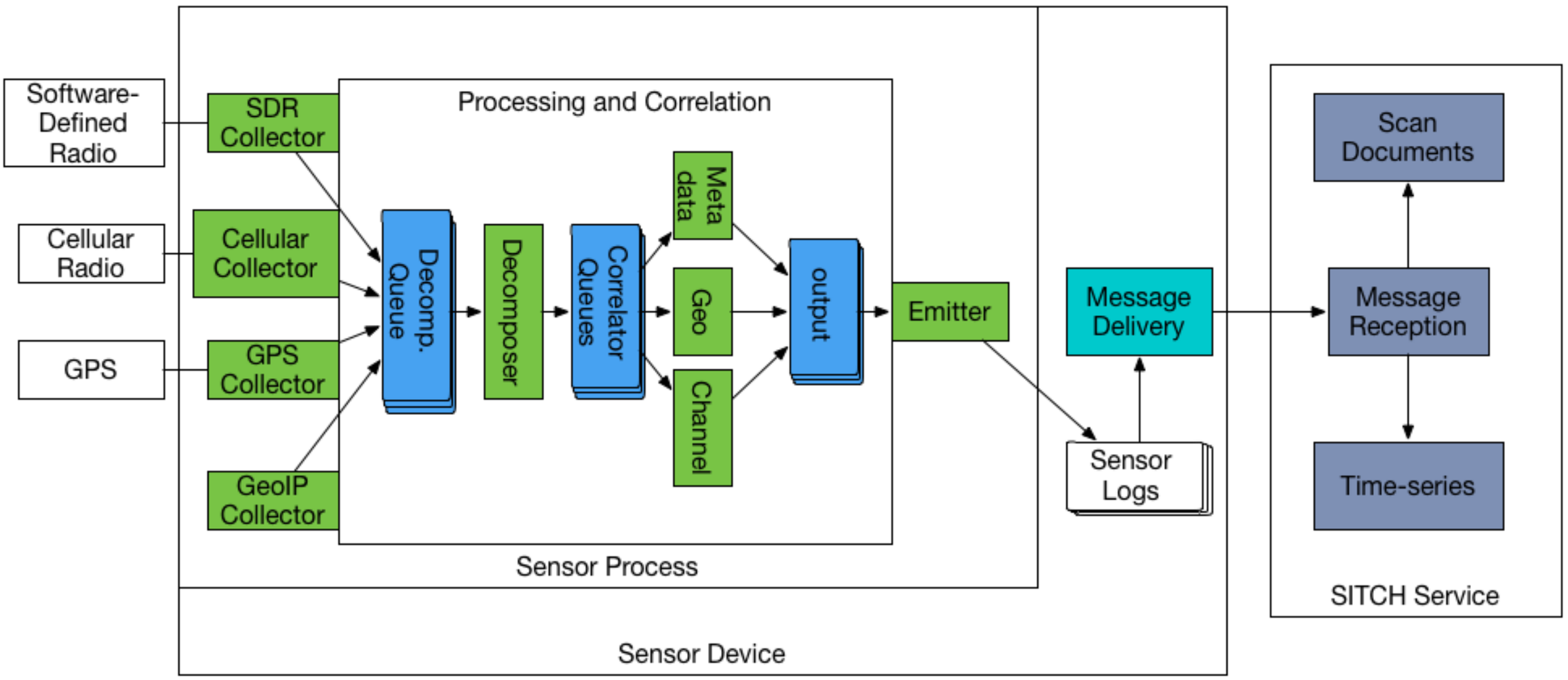
WhateverMan APP 5:50 PM

Message Type: 300 | Original Message: Possible GPS spoofing attack! 251 delta from anchor at SECURITY_SUMMER_CAMP / two-sitch https://www.google.com/maps/search/?api=1&query=36.104396238,-115.171655001 ! https://www.google.com/maps/search/?api=1&query=36.105212227,-115.174261351 | Host ID: ad6ad57

Service/Management

- ELK + InfluxDB: Data aggregation and analysis
- Hashicorp Vault: Secrets Management
- Resin.io: Device firmware management
- Slack: Alerts

Information Flow



Rapid Response

- GSM radio metadata samples every few seconds
- ARFCN power readings every ~4 mins
- ~1-2s in-sensor for correlated alerts
- Service immediately sends alerts to Slack

Sensor Alerts

ID	Description	GSM	SDR	GPS
100	Tower out of range	X		X
110	Primary BTS change	X		
120	Tower not in feed DB	X		
130	Bad Mobile Country Code (MCC) detected	X		
140	Preferred Neighbor Outside LAI	X		
141	Serving Cell Has No Neighbor	X		
200	ARFCN detected power over threshold		X	
300	GPS geo delta over threshold			X
310	GPS time delta over threshold			X
400	Failed to locate a valid ARFCN license in the area		X	X

Development History

- v1: Ugly, never released
- v2: Announced/demo @ DEFCON 24
    - GSM modem + SDR > ELK stack
- v3: November 2016
    - GPS, more supported GSM modems
    - Heartbeat/Health, Performance tracking
    - More Signatures
- v4: July 2017
    - Performance, logging improvements
    - Solo mode
    - More signatures

Demo!

- Power-up sequence
- Kibana
- InfluxDB
- Slack

Data and Observations

- LAI Study
- Trip to Napa
- The Road to Security Summer Camp
- While in Vegas...

LAI Study

- LAI distribution is counter-intuitive

- Code and results: https://github.com/sitch-io

Trip to Napa

- First excursion testing out ‘solo’ mode.

- Found oddities on Park Presidio in SF

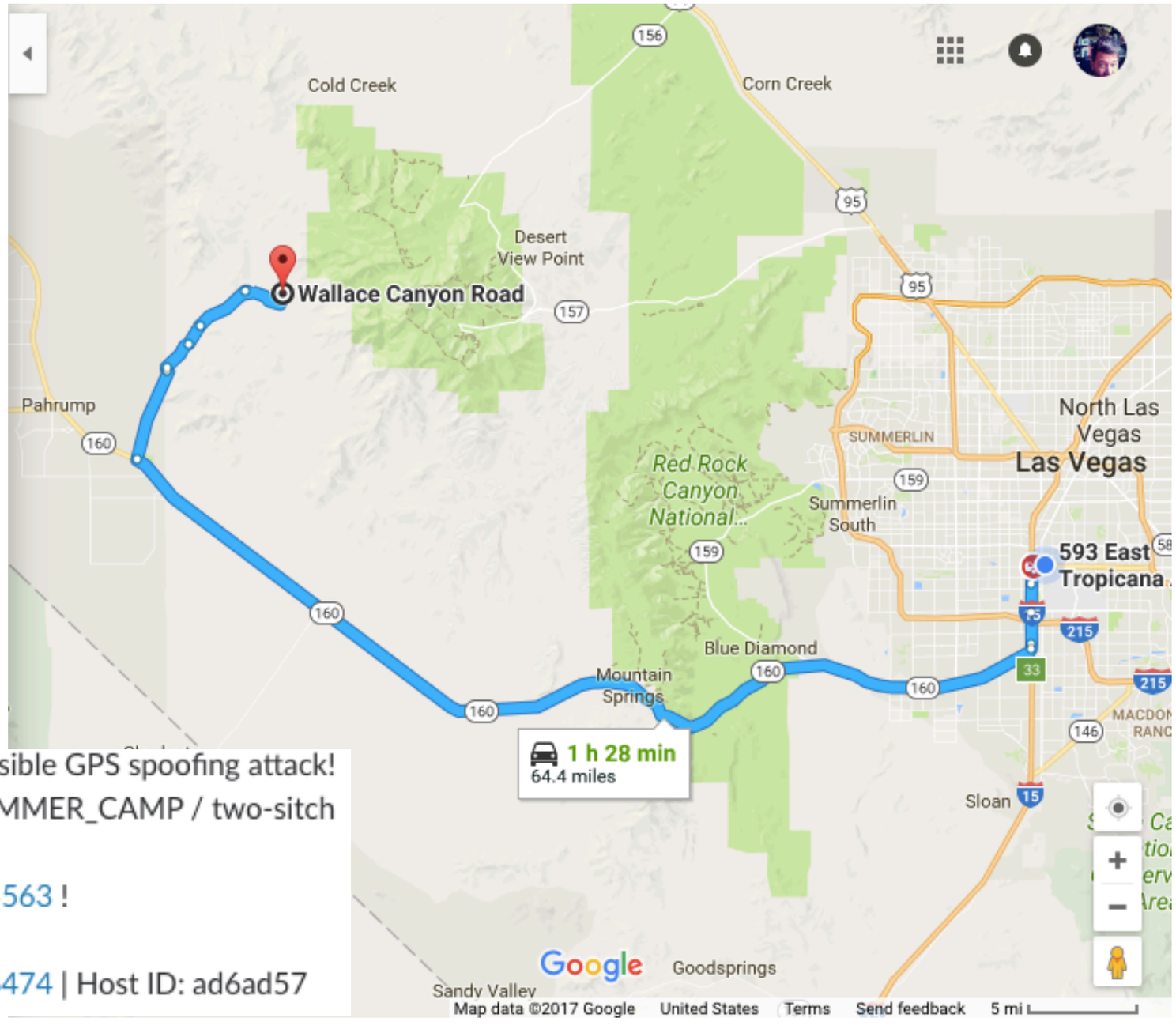
The Road to Vegas

- Sensors in ‘solo’ mode

- Drive from San Francisco to Las Vegas

Go up on a steep hill in Las Vegas and look west...

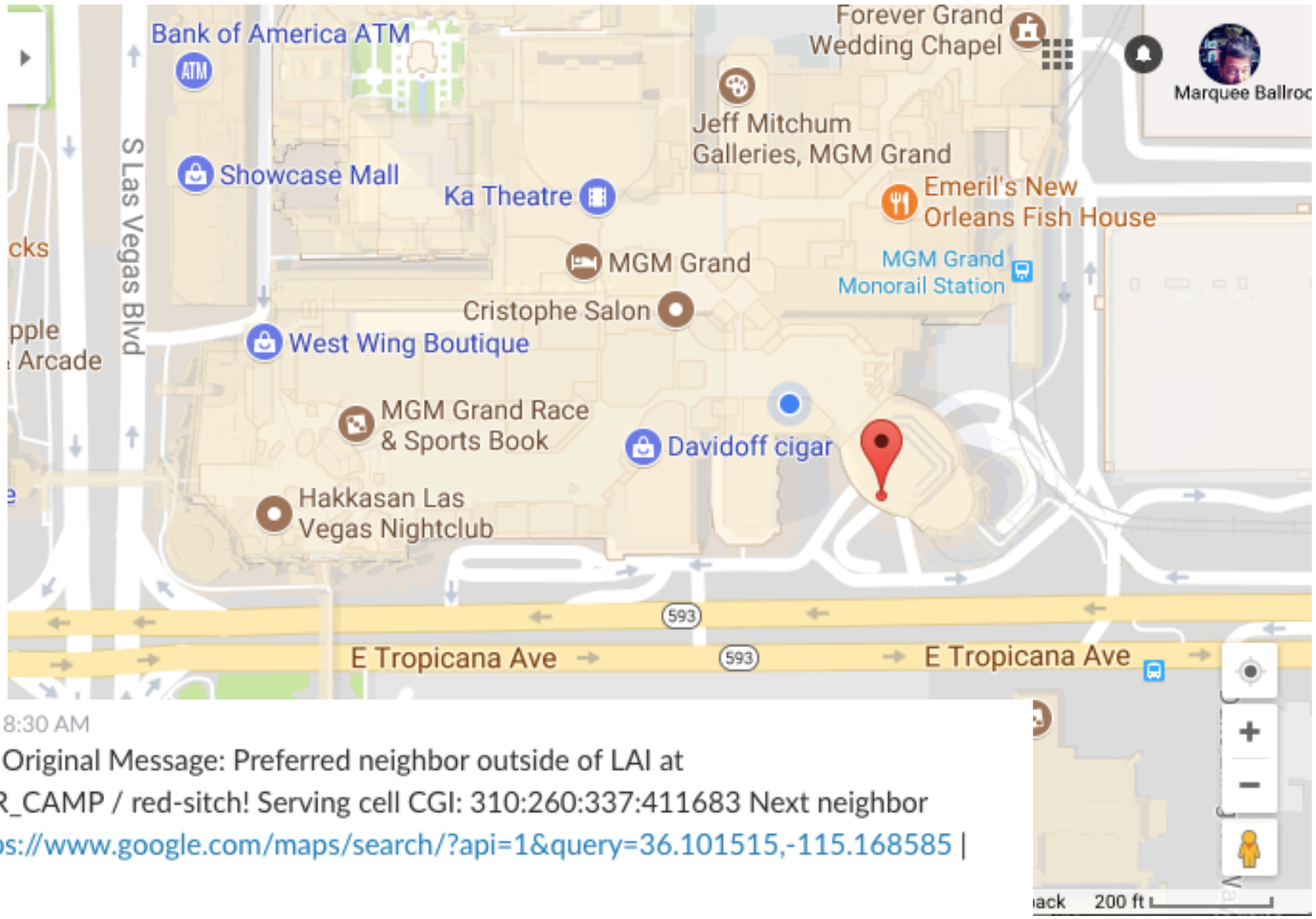
- 2017-07-25 08:56:



Message Type: 300 | Original Message: Possible GPS spoofing attack! 59982 delta from anchor at SECURITY_SUMMER_CAMP / two-sitch https://www.google.com/maps/search/?api=1&query=36.283261696,-115.798525563 ! https://www.google.com/maps/search/?api=1&query=36.101601654,-115.169156474 | Host ID: ad6ad57

With the right kind of eyes...

- 2017-07-25 08:30:



WhateverMan APP 8:30 AM
Message Type: 140 | Original Message: Preferred neighbor outside of LAI at SECURITY_SUMMER_CAMP / red-sitch! Serving cell CGI: 310:260:337:411683 Next neighbor CGI: 000:00:0:0 https://www.google.com/maps/search/?api=1&query=36.101515,-115.168585 | Host ID: a4a12e5

Future

- 3G/4G
- Standard case design
- Service-side web app
- Service-side feed enrichment
- Cross-device correlation (triangulation, etc...)

Gratitude Slide

- EFF
- Buzzfeed
- New America
- Evan Light, York University
- Seamus Tuohy
- Mike Tigas

Got Research?

[redacted]cellular[redacted]
[redacted] counter-
surveillance [redacted]
[redacted]sitch.io


@sitch_io