SITCH

Inexpensive, coordinated GSM anomaly detection

About Me

- 2000: Technology career started (I can get paid for this??)
- 2003: Started building with Linux
- Came to infosec through systems and network engineering, integration
- Security tools and integration (SIEM, HIDS, etc...)
- Current: R&D

“Thoughts and opinions expressed are my own. 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.”

–Ashmastaflash

What We're Covering Today

- Why Care?
- Current Threat and Detection Landscape
- Project Goals
- SITCH: MkI
- SITCH: MkII
- Service Architecture
- Future Plans
- Prior Art
- Q&A

Why Care?

- Invasions of privacy are bad, even when they're unnoticed.
- Industrial espionage costs money and jobs.

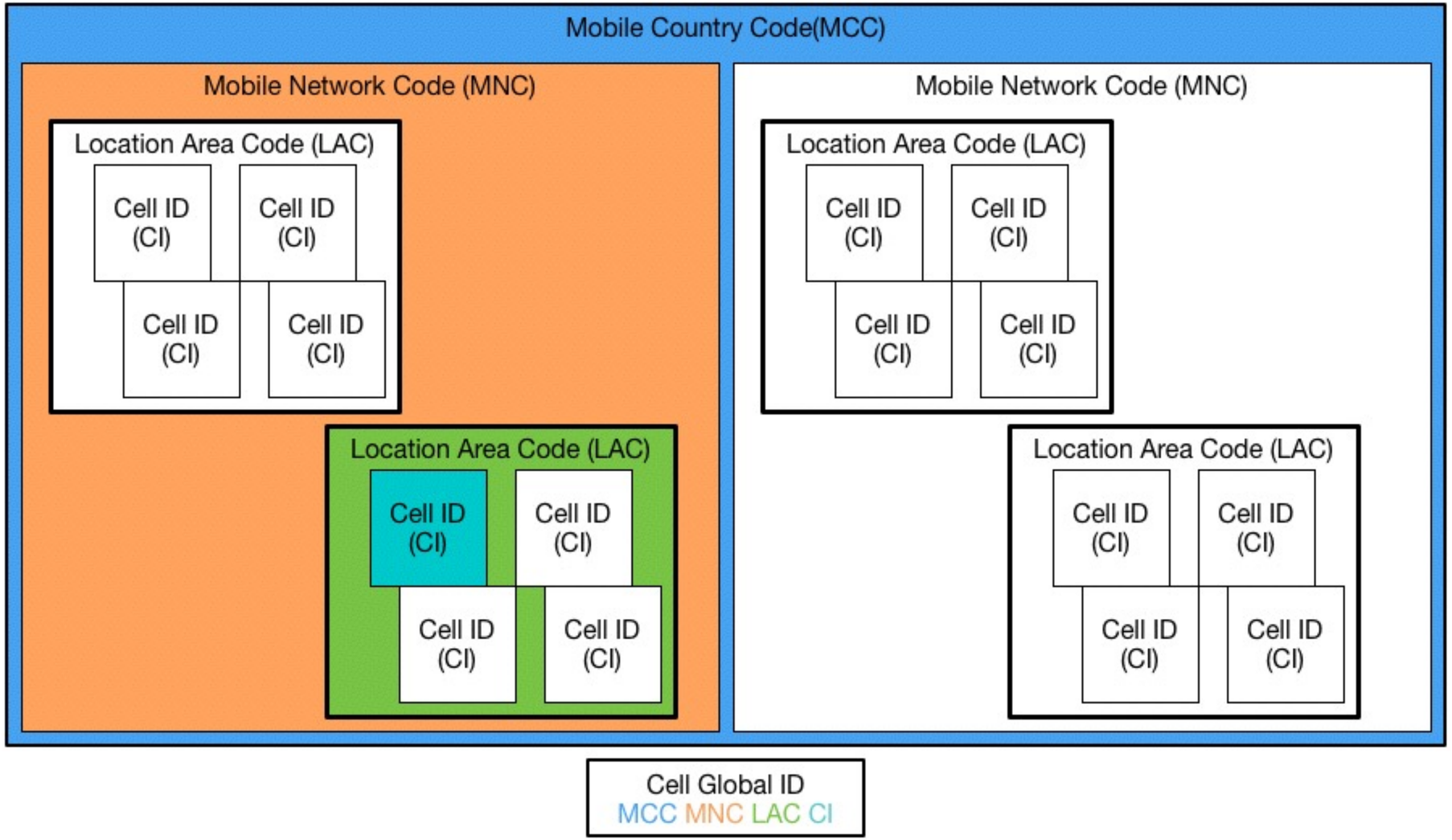
WTF Is Under All That??

Is Anybody Home?

Terminology

- Software Defined Radio (SDR): Using software to perform signal processing in concert with an adjustable-frequency RF receiver
- FCCH: Frequency Correction Channel
- ARFCN: Absolute Radio Frequency Channel Number
- CGI: Cell Global ID (MCC + MNC + LAC + CI)
- IMSI: International Mobile Subscriber Identity

GSM Addressing

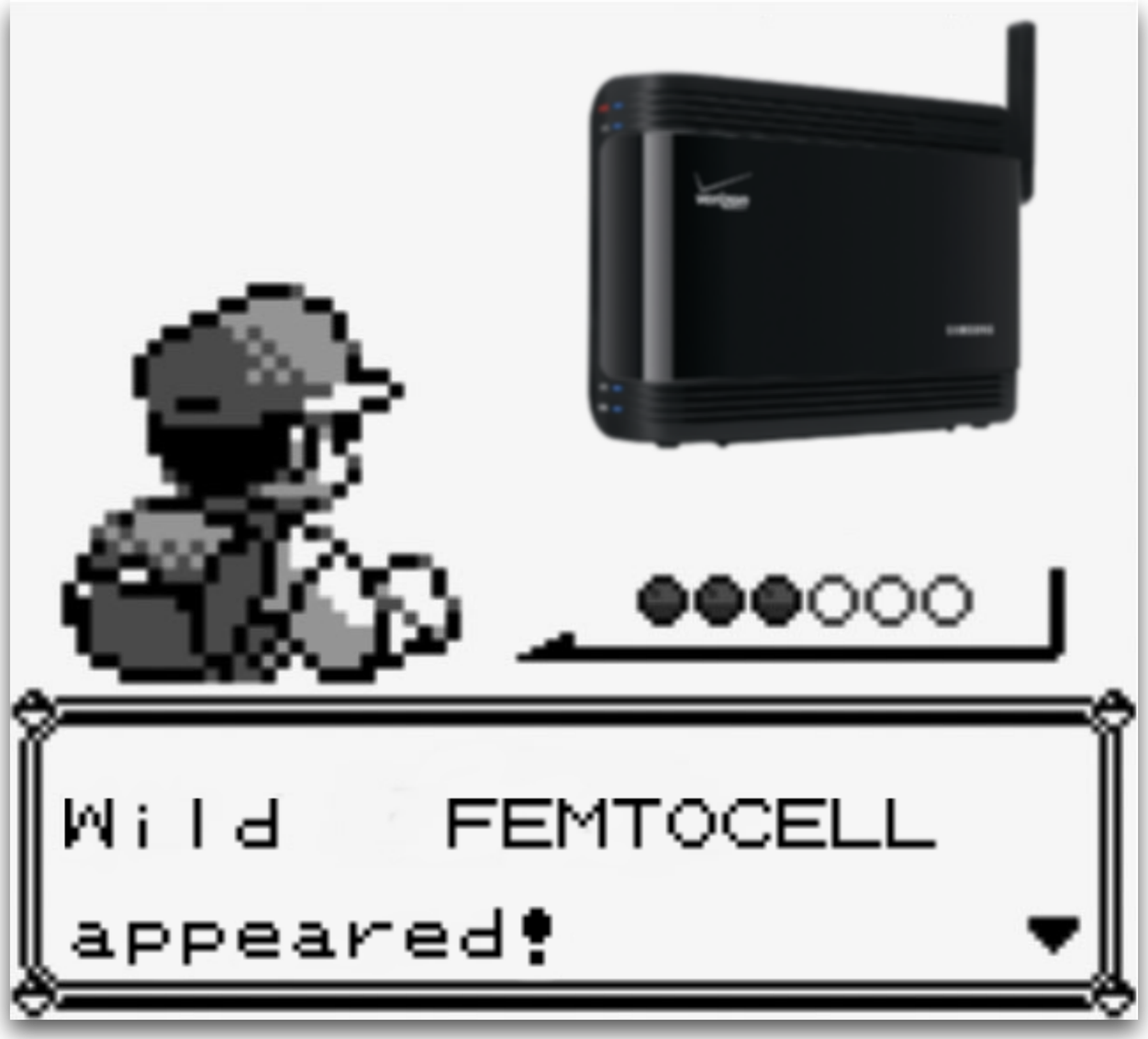


Threat and Detection Landscape

- Malicious Devices
- Indicators of Attack
- Existing Detection Methods

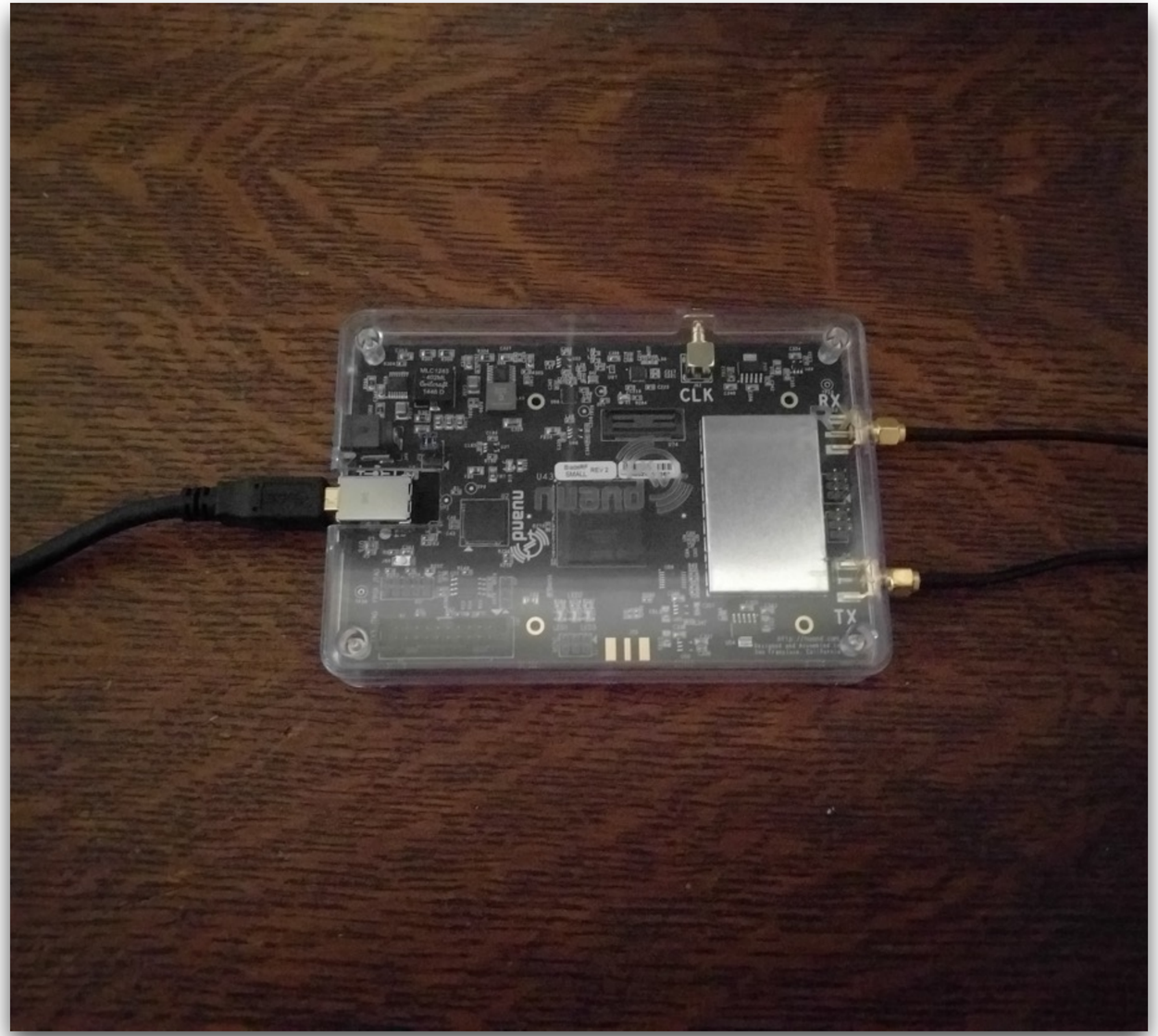
Hacked Femtocell

Trusted part of provider's network
Your phone doesn't know it's evil



Evil BTS

Handset will automatically associate, unable to assert trustworthiness



Indicators of Attack

- ARFCN over threshold
- ARFCN outside forecast
- Unrecognized CGI
- Gratuitous BTS re-association
- BTS detected outside of range

Existing Detection Methods

- Commercial Options:
  - Pwnie Express
  - Bastille Networks
- Open Source:
  - Fake BTS
  - AIMSICD
  - Femto Catcher

Project Goals

- Inexpensive (what can I get for $100?)
- Small footprint, low power requirements preferred
- Functional Targets: Indicators of Attack (IOA) Coverage

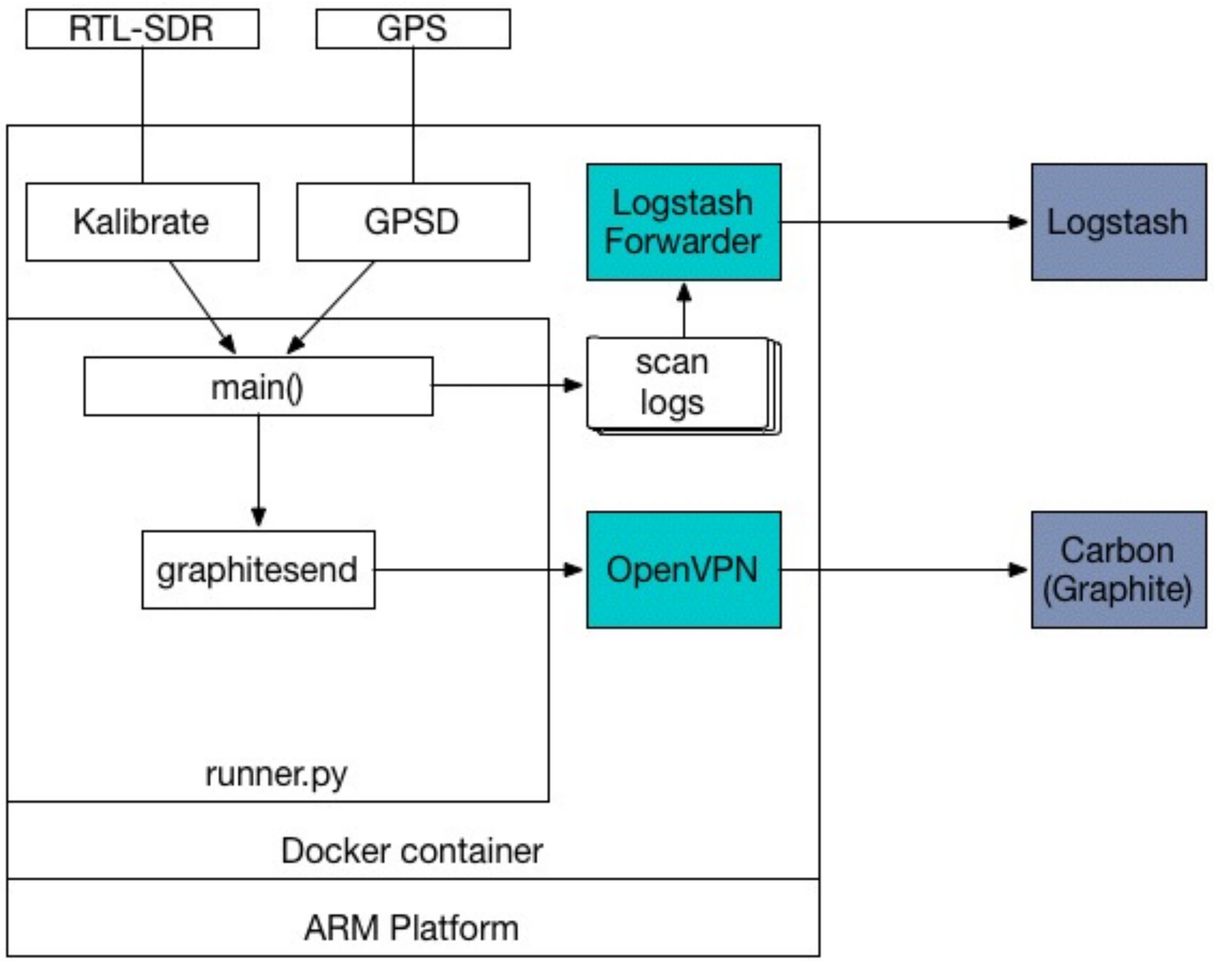
Tested Hardware

(some of it, anyway)

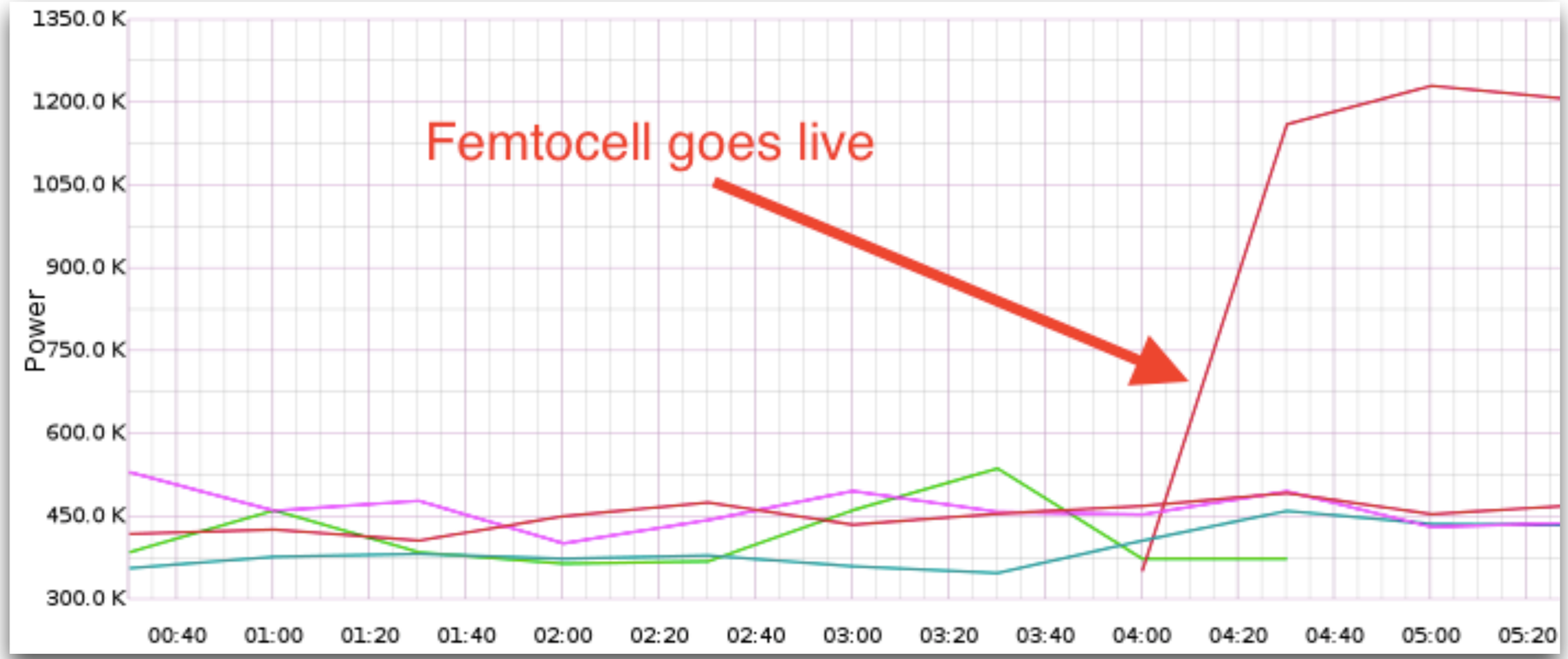
Functional Targets

- ARFCN over threshold
- ARFCN outside of forecast
- Unrecognized CGI
- Gratuitous BTS re-association
- BTS detected out of range

SITCH Sensor MkI



SITCH Sensor MkI



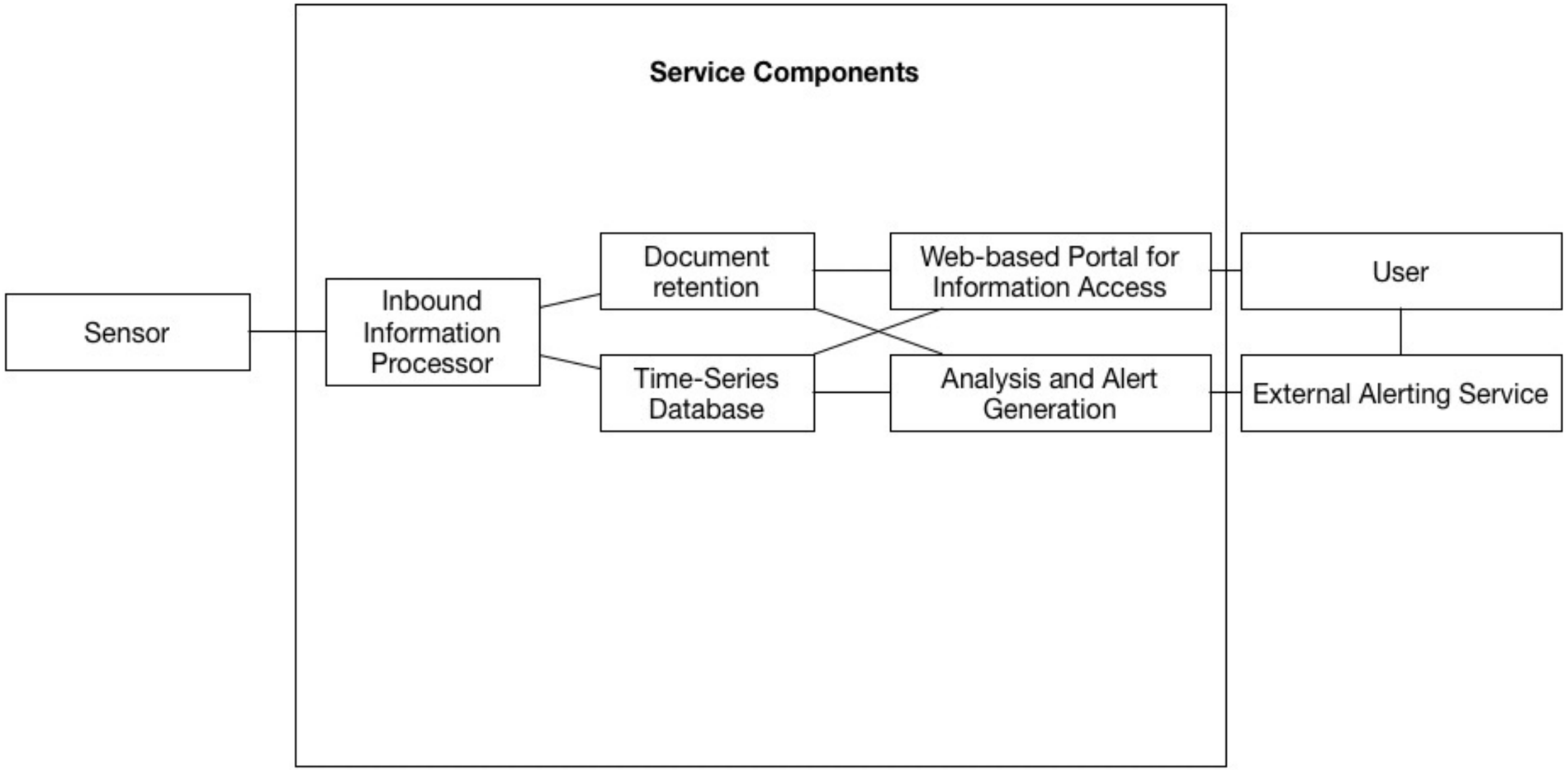
MkI Results

Targets	MkI Coverage
ARFCN over threshold	YES
ARFCN outside of forecast	YES
Unrecognized CGI	NO
Gratuitous BTS re-association	NO
BTS detected outside of range	NO
Price	~$100

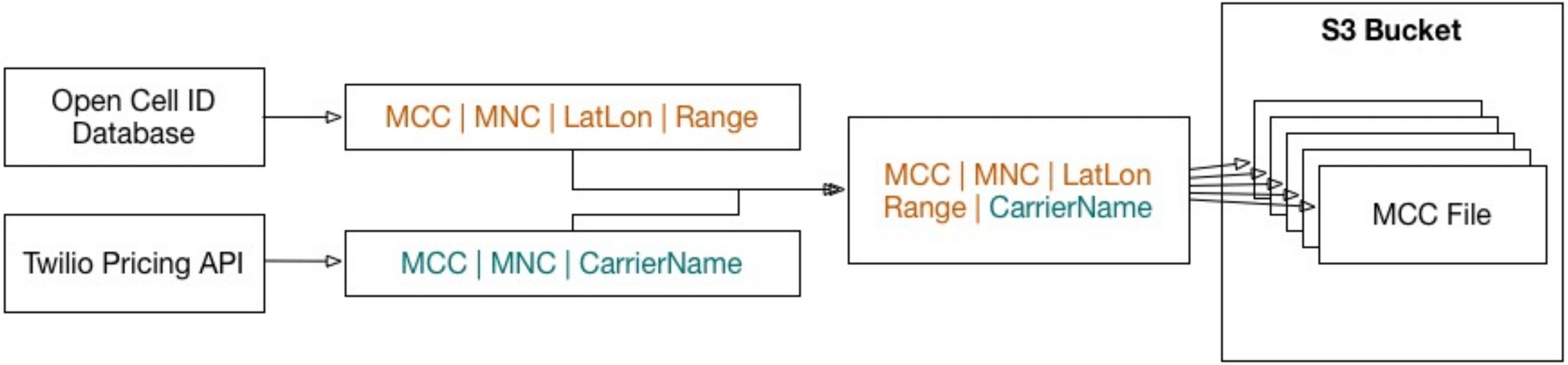
Start Demo Here!

- Install SD Card
- Confirm registration
- Set device-specific environment variables
- Move from staging to production application

SITCH Service Architecture

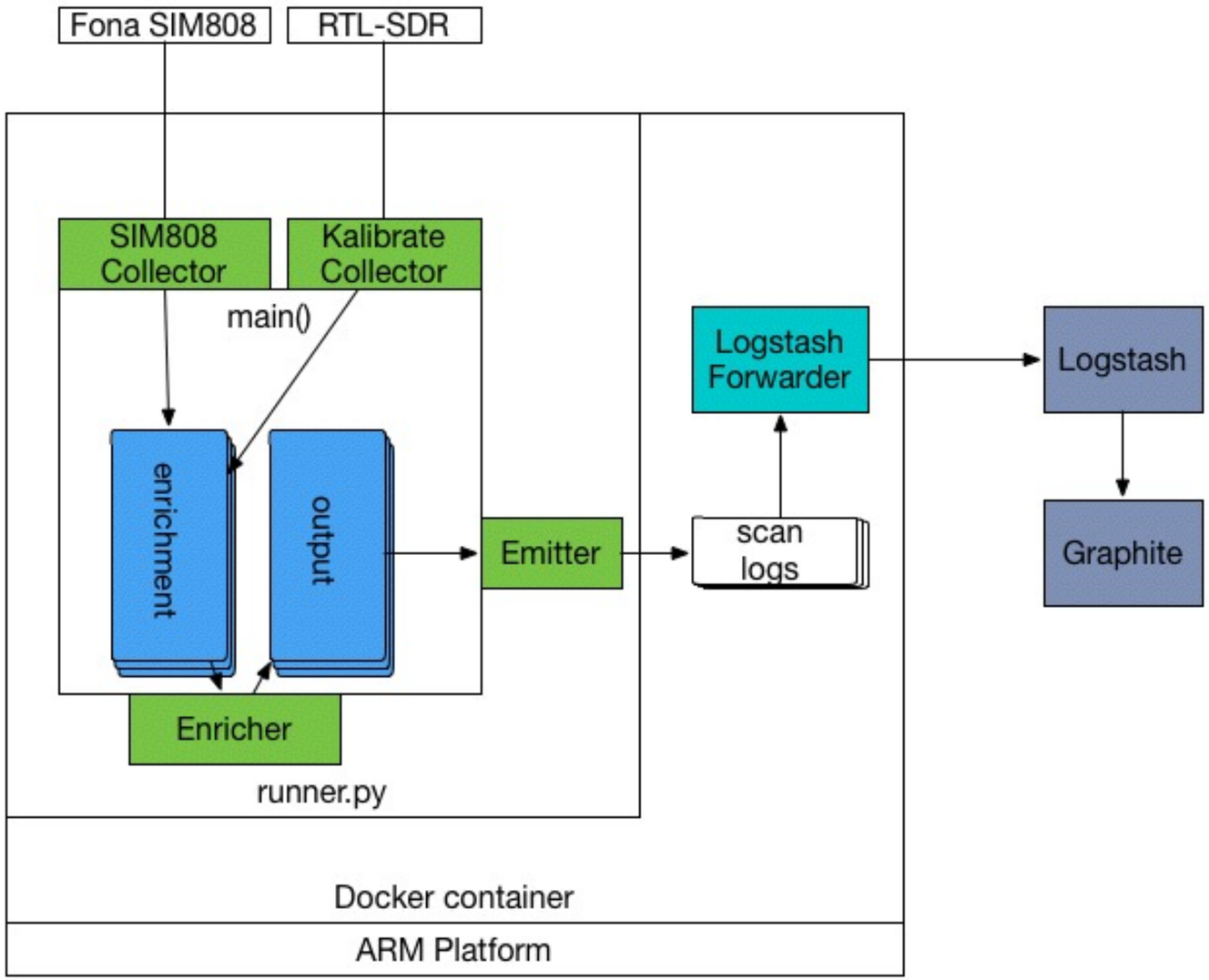


SITCH Intelligence Feed

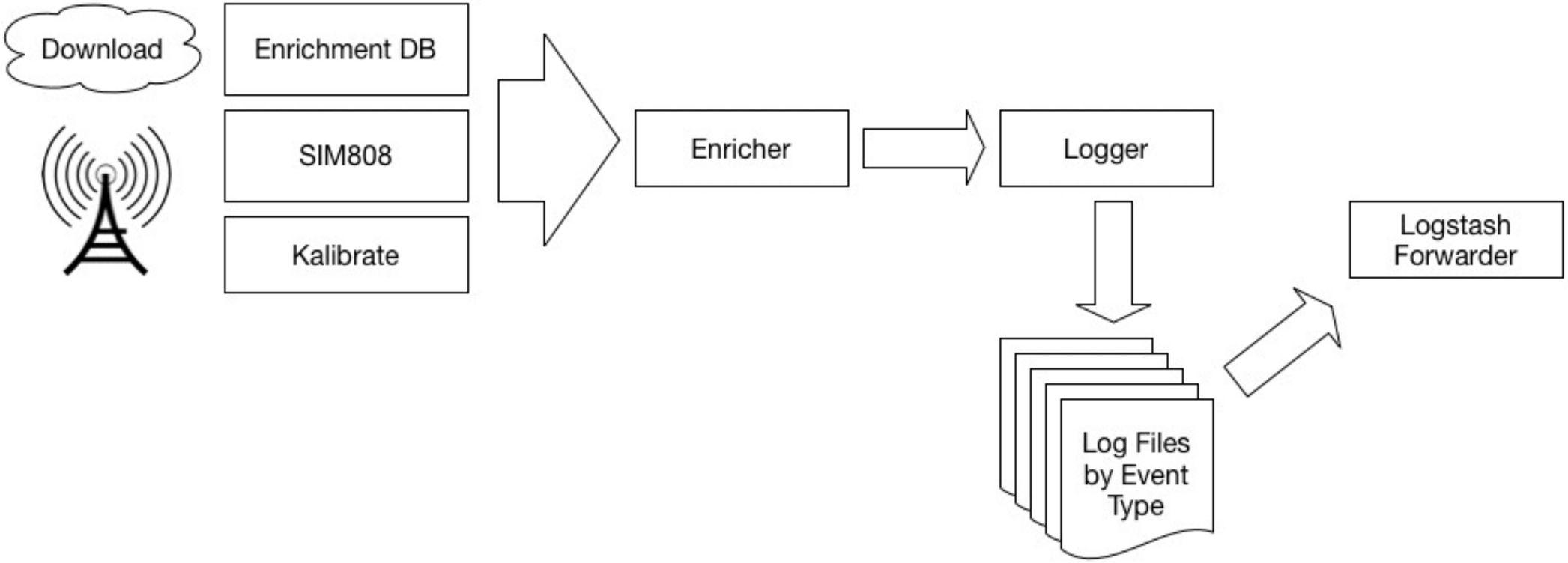


- OpenCellID Database:
  - MCC, MNC, Lat, Lon, Range
- Twilio:
  - MCC, MNC, CarrierName

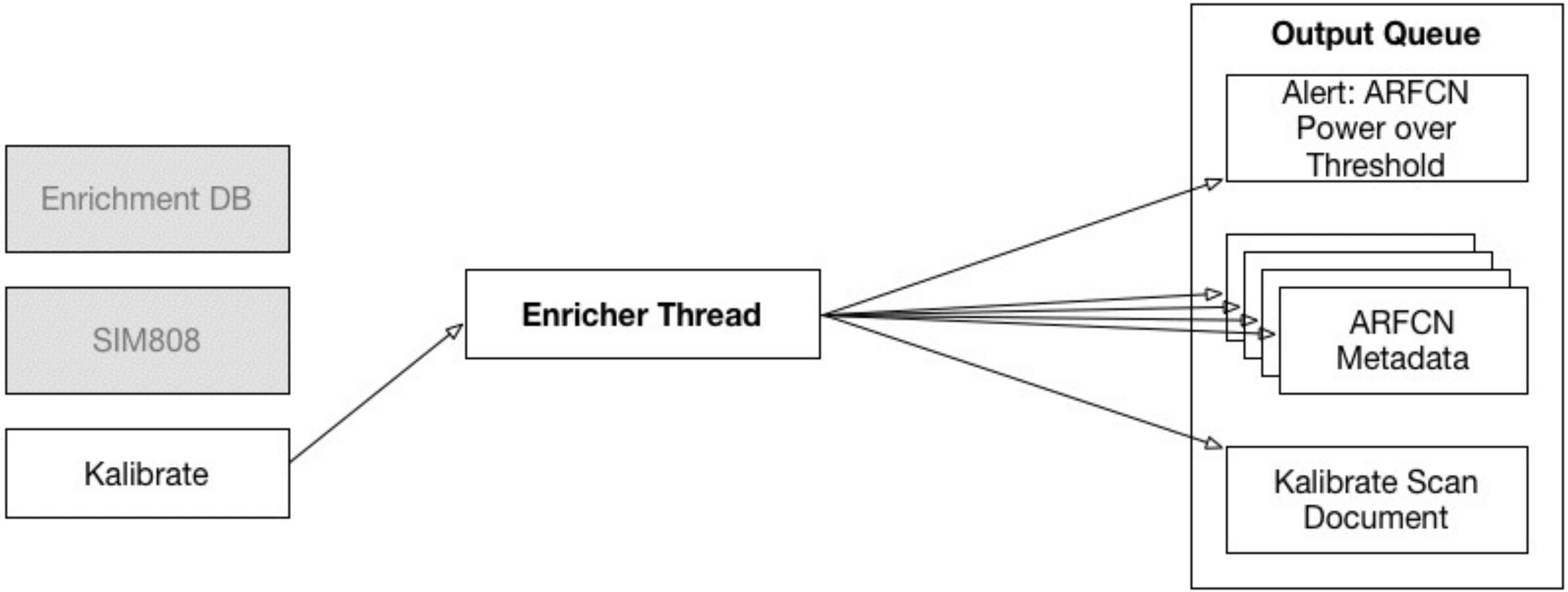
SITCH Sensor MkII



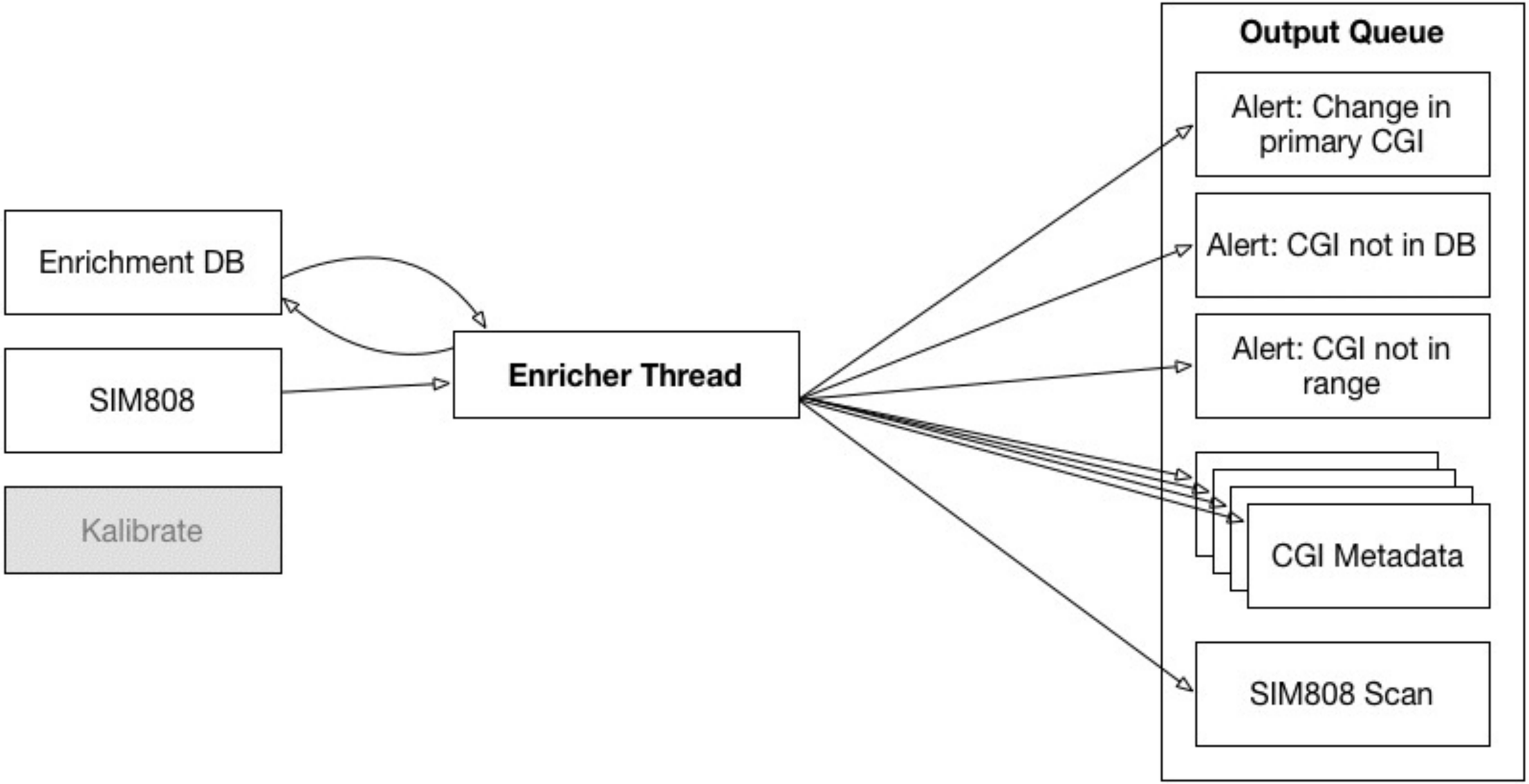
SITCH Sensor MkII



SITCH Sensor MkII



SITCH Sensor MkII



SITCH Sensor MkII

#sitchalerts
2 members | *Add a topic*

primary bts

WhateverMan BOT 10:26 AM
Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 0666 mcc: 310 mnc: 266 lac: 275 cellid: 20082 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 1696 mcc: 310 mnc: 266 lac: 275 cellid: 42302 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 1702 mcc: 310 mnc: 266 lac: 275 cellid: 42301 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 1698 mcc: 310 mnc: 266 lac: 275 cellid: 20271 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 1692 mcc: 310 mnc: 266 lac: 275 cellid: 20081 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

WhateverMan BOT 11:03 AM
Message Type: 200 | Original Message: ARFCN 666 is over threshold at cabronum_test! | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

WhateverMan BOT 12:07 PM
Message Type: 120 | Original Message: BTS not in feed database! Info: ARFCN: 1702 mcc: 310 mnc: 266 lac: 275 cellid: 20084 Site: cabronum_test | Host ID: c10357c2224e2aedcdf13310938391cd97a5b1afbca40a59477a6c407e7dab

WhateverMan BOT 12:27 PM

#sitchalerts
2 members | *Add a topic*

Search

WhateverMan BOT 11:21 PM
[BEACON] CRITICAL <Holt-Winters Aberration: ARFCN power (Kalibrate)>
`holtWintersAberration(channels.cabronum_test.abe1f70e7a813d599bdffd36cf31504ff048cdda9cd4656df09aee2ddab48d.GSM-850.232.kal_power)` failed. Current value: 475.2K
View Graph

[BEACON] NORMAL <Holt-Winters Aberration: ARFCN power (Kalibrate)>
`holtWintersAberration(channels.cabronum_test.abe1f70e7a813d599bdffd36cf31504ff048cdda9cd4656df09aee2ddab48d.GSM-850.232.kal_power)` is back to normal.

WhateverMan BOT 11:51 PM
[BEACON] CRITICAL <Holt-Winters Aberration: ARFCN power (Kalibrate)>
`holtWintersAberration(channels.cabronum_test.abe1f70e7a813d599bdffd36cf31504ff048cdda9cd4656df09aee2ddab48d.GSM-850.232.kal_power)` failed. Current value: 200.1K
View Graph

[BEACON] CRITICAL <Holt-Winters Aberration: ARFCN power (Kalibrate)>
`holtWintersAberration(channels.cabronum_test.abe1f70e7a813d599bdffd36cf31504ff048cdda9cd4656df09aee2ddab48d.GSM-850.231.kal_power)` failed. Current value: 217.8K
View Graph

[BEACON] CRITICAL <Holt-Winters Aberration: ARFCN power (Kalibrate)>

MkI, MkII Results

Targets	MkI Coverage	MkII Coverage
ARFCN over threshold	YES	YES
ARFCN outside of forecast	YES	YES
Unrecognized CGI	NO	YES
Gratuitous BTS re-association	NO	YES
BTS detected outside of range	NO	YES
Price	~$100	~$150

Return to Demo!

- Slack alerts
- Tessera graphs
- Kibana scan search
- Resin logs

Going Forward

- Automatic device detection
- Device and service heartbeats
- Gnuradio = pure SDR:
  - GR-GSM
  - ADS-B
  - FPV drone
- Dedicated radios:
  - Ubertooth One
  - YARD Stick One

Prior Art

- DIY Cellular IDS (Davidoff, Fretheim, Harrison, & Price, Defcon 21)
- Traffic Interception and Remote Mobile Phone Cloning with a Compromised Femtocell (DePerry, Ritter, & Rahimi, Defcon 21)
- Introduction to SDR and the Wireless Village (DaKahuna & Satanklawz, Defcon 23)
- http://fakebts.com - Fake BTS Project (Cabrera, 2014)
- How to Build Your Own Rogue GSM BTS for Fun and Profit (Simone Margaritelli)
- Gnuradio (many)
- Gr-gsm (Krysik, et al.)
- Kalibrate (thre.at)

THANKS!

- John Menerick
- Gillis
- Pedro Cabera
- Piotr Krysik
- Thre.at
- Gnuradio
- Silent Contributors...

Q&A