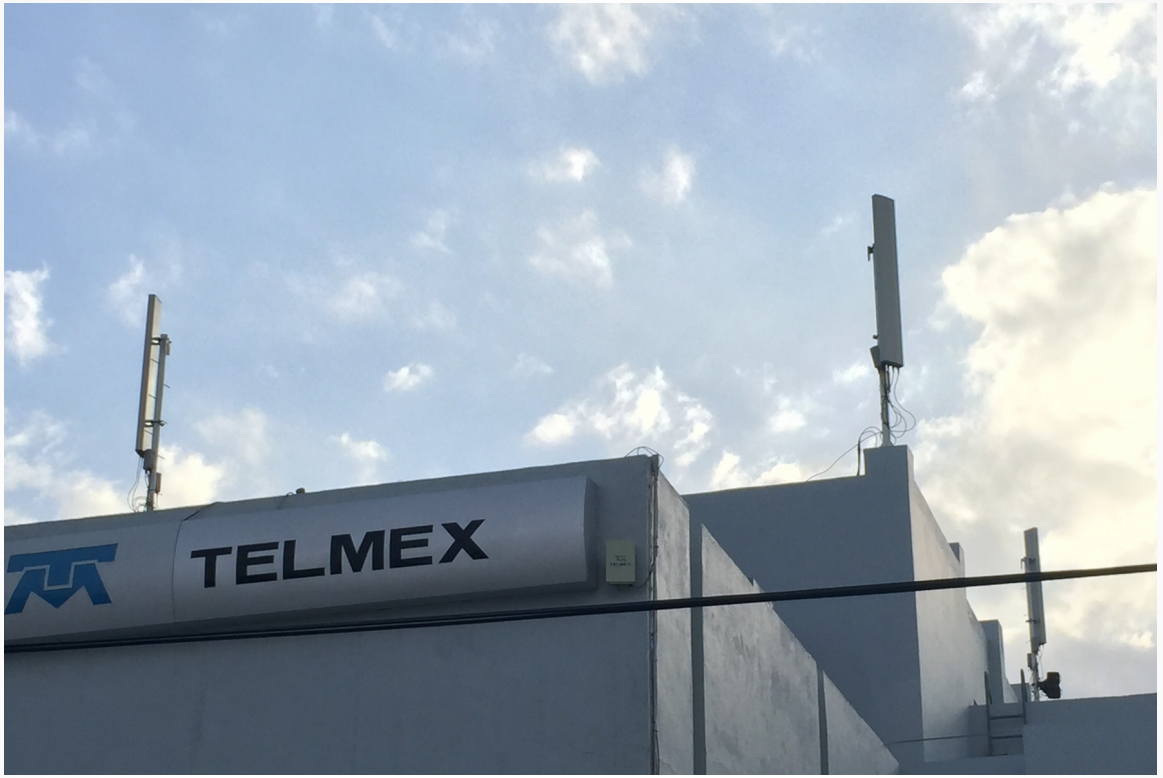
Active Cellphone Site Simulators



Freddy Martinez
4554 DB89 B856 F6E7 487D 59BF F319 5C29
2A82 2EF5
@B_meson

HARRIS

Harris Proprietary

Quote	QTE6779-05095
Date	10/6/2014
Page:	1

HARRIS CORPORATION
P.O. BOX 9800, M/S R5-11A
MELBOURNE, FL 32902-9800
PH: 800-358-5297, FAX: 321-309-7437

Quotation

Bill To:

Chicago Police Department
Jack Costa
jack.costa@chicagopolice.org
3340 W. Filmore
Room 2180
Chicago IL 60624

Ship To:

Chicago Police Department
Jack Costa
jack.costa@chicagopolice.org
3340 W. Filmore
Room 2180
Chicago IL 60624

Overview

Our FOIA work

Stingrays / IMSI Catchers

Physical Stack

Electronic Signature of GSM

Detecting GSM disruptions

- Software
- Hardware

Biography

Physicist

Linux System Admin by night

“A skinny fidgety twenty-seven year old” – VICE

IMSI: Who *you* are

Uniquely identify *your phone*

Example IMSI: 310410XXXXXXXXXX

- MCC 310 USA
- MNC 410 AT&T GSM 850 / GSM 1900 / UMTS 850 / UMTS 1900
- MSIN (phone number) XXX XXX XXXX

Chicago FOIA Work

After previous denials, lawsuit uncovered at least 2-3 Stingrays

- Funding came from asset forfeiture

Hailstorm upgrade purchased in Oct 2014

CPD obtains PR/TT **see IL SB2828**

exempt from disclosure under FOIA. The potentially responsive court orders and related applications gathered by Sergeant Costa were issued pursuant to Title 18, United States Code, Sections 3122 and 3123, and were ordered to remain under seal until further order of the court. *Id.* Indeed, 18 U.S.C. § 3123(d)(1) specifically provides that "[a]n order authorizing or

FOIA Work (Cont)

Contract btw CPD and Harris state they can't disclose to courts they own HailStorm

CPD claims no records of anyone checking IMSI catchers in / out.

International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130. The ITAR requires anyone, prior to making an export of technical information, to obtain a license from the Department of State. Technical information need not leave the borders of the United States to be deemed an export. Providing technical information without a license to anyone intending to publicize the information, as is your stated intention, could constitute a violation of the Arms Export Control Act.

Pen Register/Trap and Trace

Lower legal standard than search warrants. Requires only that information be “relevant and material to an ongoing investigation”

After 2001, PR/TT began being used for cell tracking

See also: No “reasonable expectation of privacy” after handing off data to 3rd party (*Smith v. Maryland*)

GSM Simplified

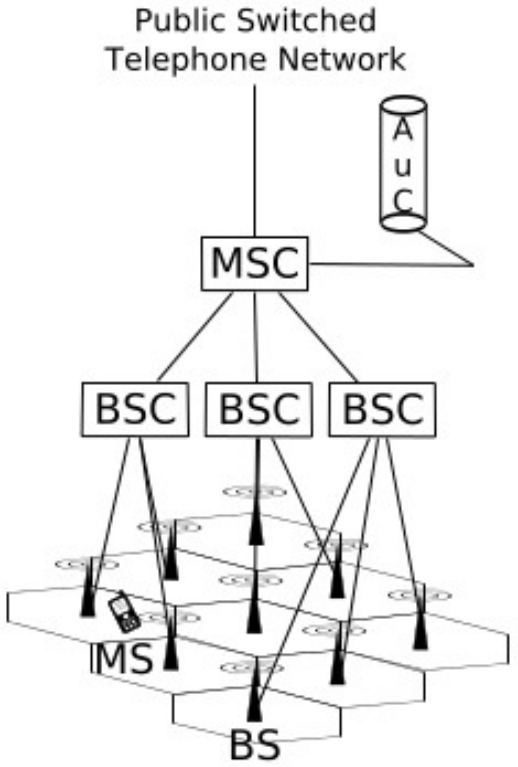


Figure 2.1: Simplified architecture of a GSM network

[6]

GSM Simplified

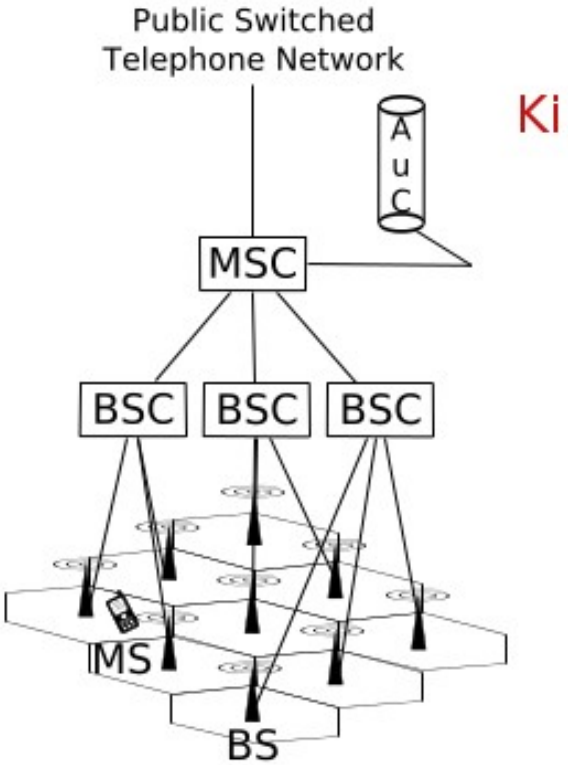


Figure 2.1: Simplified architecture of a GSM network

[6]

GSM Simplified

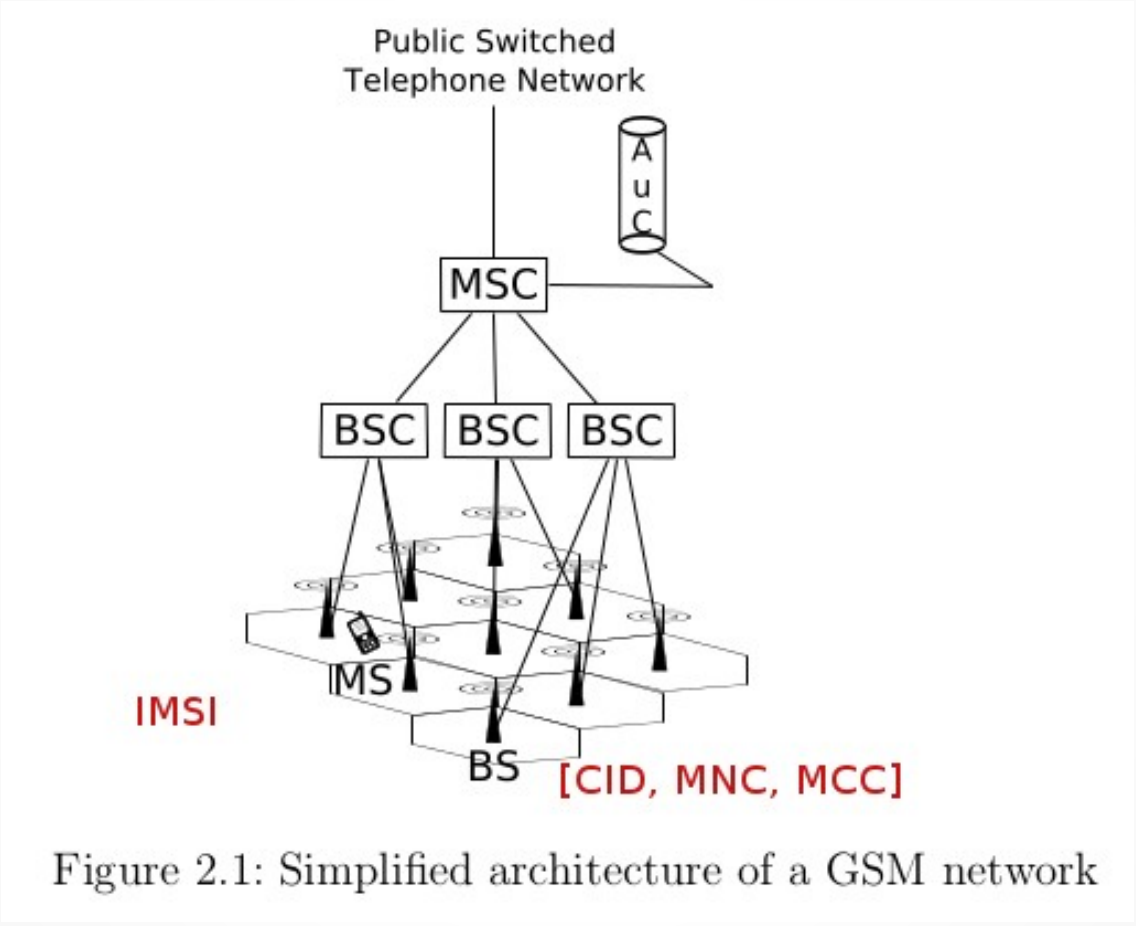


Figure 2.1: Simplified architecture of a GSM network

[6]

GSM Simplified

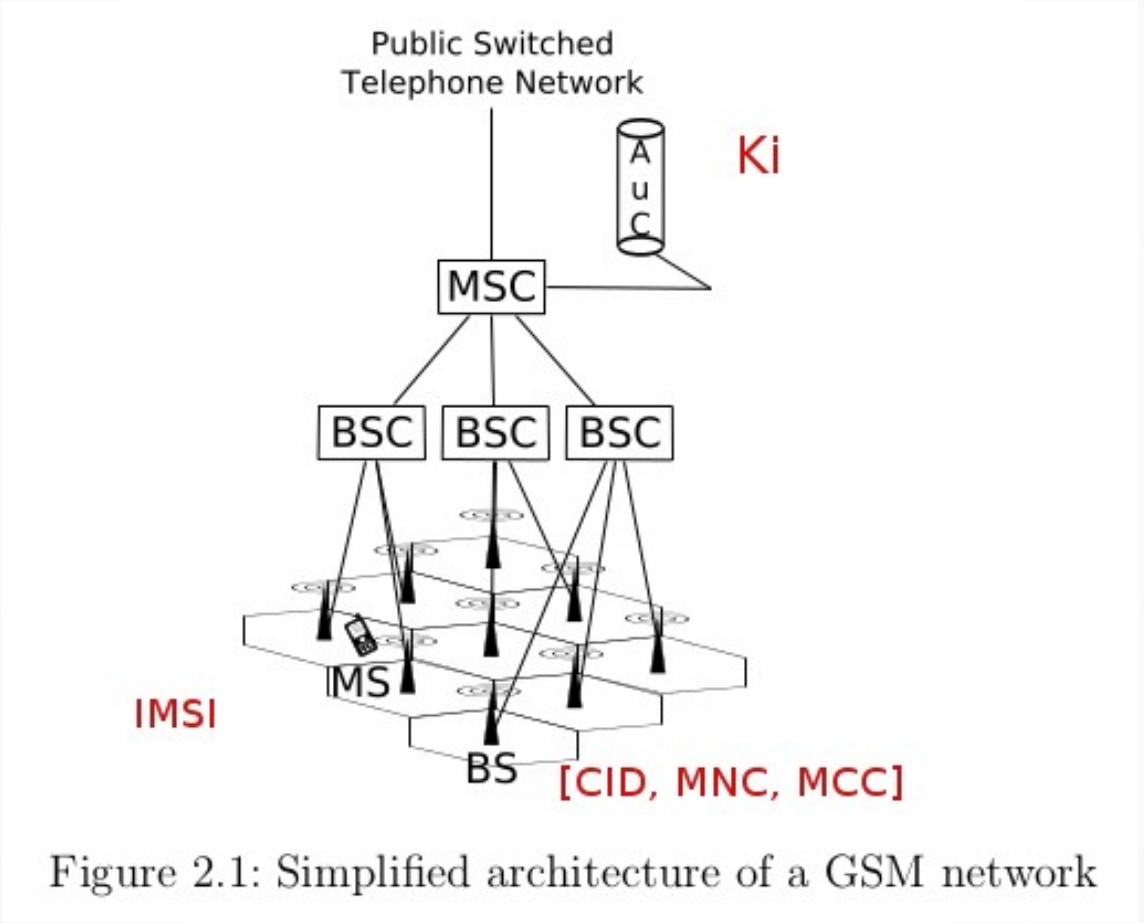


Figure 2.1: Simplified architecture of a GSM network

[6]

GSM Simplified

BTS (identified by Cell ID)

LAC (wider area multiple BTS operate on)

ARFCN: Absolute Radio-Frequency Channel Number

Authenticate to network via IMSI

- IMSI (International Mobile Subscriber Identity)
  - TMSI (Temporary Mobile Subscriber Identity)
- K_c (Short-Term Encryption Key)

Problems with GSM

Downgrade attacks (i.e. 3G jammers)

Many known weaknesses in encryption

Lack of Forward Secrecy

BTS *decides* encryption

BTS can say your TMSI is invalid

- So you had over your IMSI

Authentication

1. MS transmit IMSI
2. AuC generates RAND (128 random)

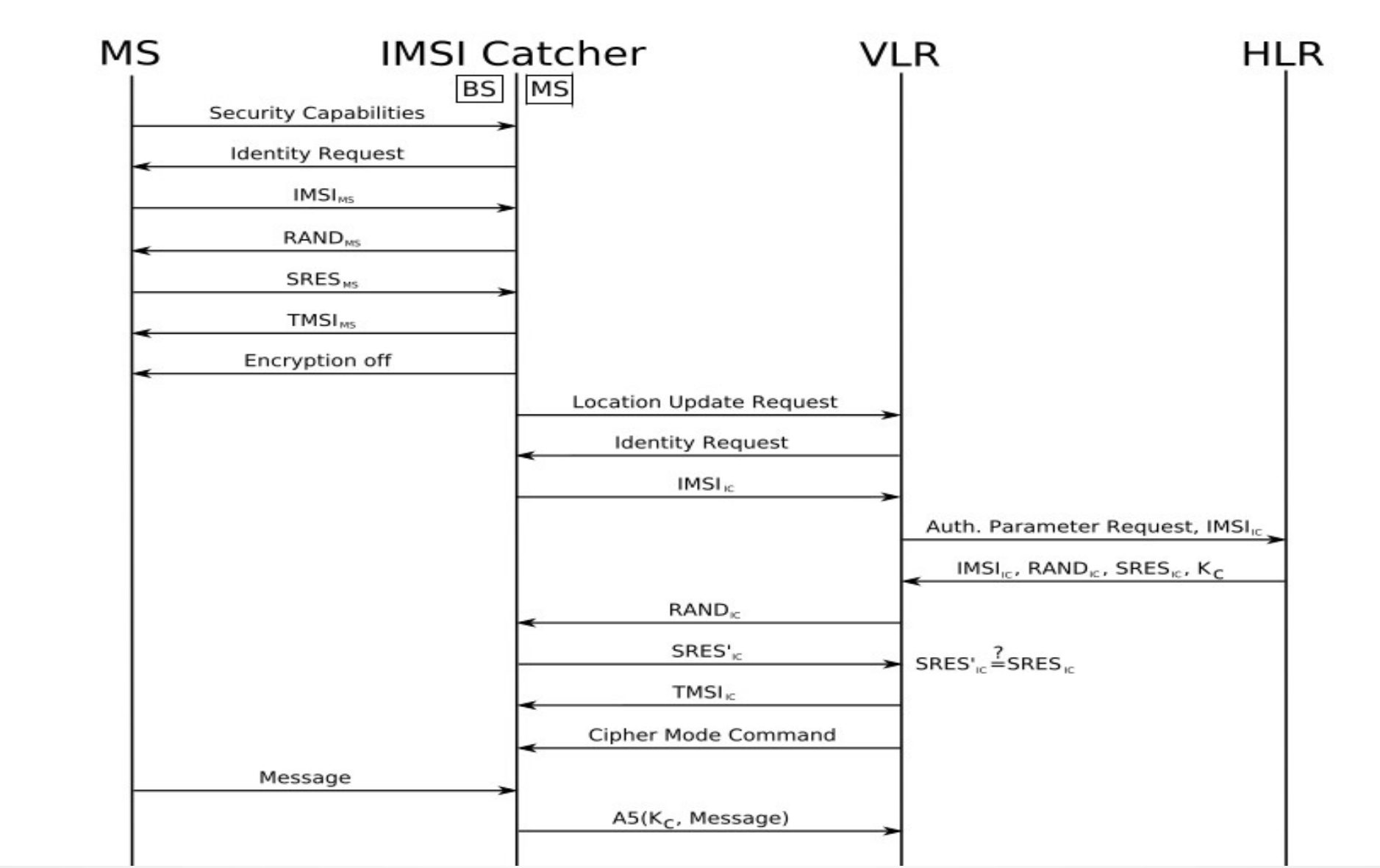
   A3(RAND,Ki) → SRES → BSC(RAND) → MS

   A8(RAND,Ki) → Kc → BSC
3. MS gets RAND

   A3(RAND,Ki) → SRES → BSC

   A8(RAND,Ki) → Kc → BSC

MiTM Attack


MS
IMSI Catcher
BS
MS
VLR
HLR
Security Capabilities
Identity Request
IMSI_MS
RAND_MS
SRES_MS
TMSI_MS
Encryption off
Location Update Request
Identity Request
IMSI_IC
Auth. Parameter Request, IMSI_IC
IMSI_IC, RAND_IC, SRES_IC, K_C
RAND_IC
SRES'_IC
SRES'_IC ?= SRES_IC
TMSI_IC
Cipher Mode Command
Message
A5(K_C, Message)

Motivations for Hostile BTS

Send Spam SMS messages

Pull IMSI without warrant

Gather routing metadata and/or *content*

- Stingrays can but no evidence police have the "upgrade")

IMSI Catchers used by CIA / JSOC for SIGINT

Stingray / Hailstorm

Capabilities

Catch dialed numbers, IMSI, etc *after* a call is placed (passive)

Force registration on phones (active)

- CELL_RESELECT_HYSTERESIS dB of fake BTS exceeds value defined in BCCH

Force phones to transmit at full output

- C2 = C1 + CELL_RESELECT_OFFSET - TEMPORARY OFFSET * H(PENALTY_TIME - T) for PENALTY_TIME <> 11111
- TEMPORARY_OFFSET applies a negative value for PENALTY_TIME

Other capabilities

Capture / modify content in real-time

Initiate calls from target without consent

Force phone to ring (?)

Malware (?)

Detecting a Disruption

New LAC appears

New CID or CID = (empty)

Broadcast on new ARFCN

GetNeighboringCell changes

- [<MCC>,<MNC>,<LAC>,<CI>,<BSIC>,<BCCH Freq>,<RxLev>...]

Weighed averages to various events

Software Countersurveillance

SnoopSnitch: Reverse engineering of low-level baseband.

- Bonus: Detects SS7 events

AIMSICD: Like SnoopSnitch an “IMSI catcher” catcher application for Android

Hardware Countersurveillance

Adafruit 2G microcontroller wired to a Beagle Bone

Bunyan

- Logger of AT commands

Github → freddymartinez9

Pseudo Code

```
PySerial.open(/dev/ttyS0,115200)
#Read Neighboring Cell
Pyserial.open(AT+CCED=1 \n)
        time.sleep(waitTime)
        # Signal Stregth shouldn't fluctuate drastically
        if(RSSI_current-5 < RSSI_previous || RSSI_current+15 > RSSU_previous)
                f.write('UNUSUAL RSSI FLUCTUATION \n')
                f.write(localtime = time.asctime( time.localtime(time.time()) ))
                RSSI_current=RSSI_previous
        else
                time.sleep(waitTime)
```

Miscellaneous / Future Work

Finding attacks "in the wild" remains elusive

- We are looking now

Dialing 911 forces de-registration

Need micro-controllers in 3G/LTE bands

References

[0] *Snoop Snitch*.

https:// opensource. srlabs .de/projects/ snoopsnitch

[1] *AIMSICD* https://github.com/SecUpwN/Android-IMSI-Catcher-Detector

[2] “*Mobile Self-Defense*”. #31c3 Karsten Nohl

[3] “*SS7: Locate. Track. Manipulate*”. #31c3 Tobias Engel

References

[4] "*Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About*" ACLU. https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about

[5] "*IMSI Catcher*" Daehyun Strobel. Jul 2007 Ruhr-Universität Bochum

[6] *"Introduction to GSM"*

[7] *"IMSI-Catcher and Man-in-the-Middle attacks"* Dammann. 2011

References

[8] *OsmocomBB* http:// bb.oscom.org/trac

[9] *“Stingray Talk”* AACJ Winter Seminar. Daniel Rigmaiden

[10] *“Your Secret StingRay’s No Secret Anymore”.* 2014 Stephanie K. Pell & Christopher Soghoian

References

[11] *“Cellular Dragnet: Active Cell Site Simulators and the Fourth Amendment”*, Jan 2015. Aimee Thomson

[12] *“Fake BTS Attacks of GSM System on Software Radio Platform”*. Journal of Networks, Feb 2012 Song, Zhou, Chen

Thanks

THOTCON organizers

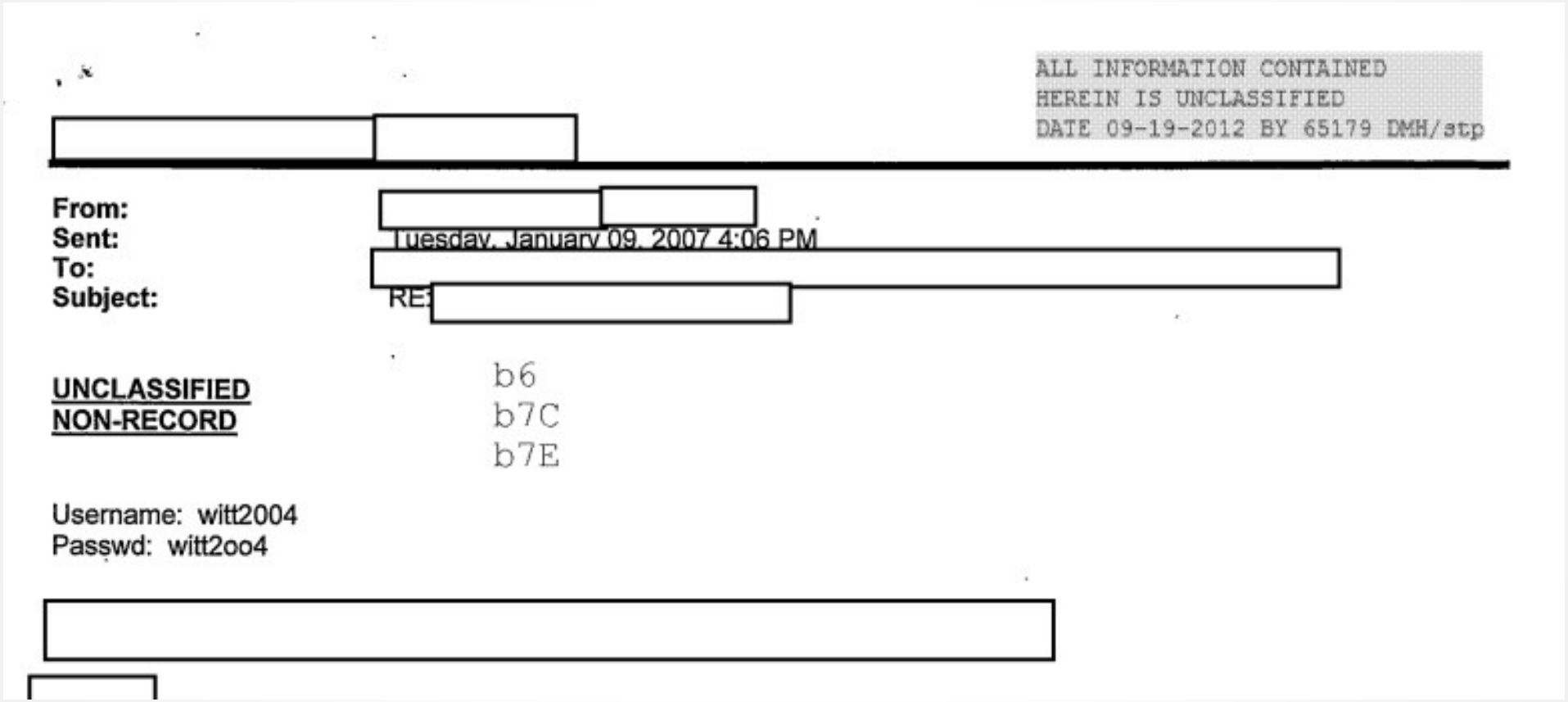
Drew Fustini

SSHc: Southside Hacker Space Chicago

Wally Valters & Matasano

Matt Topic (attorney Loevy & Loevy)

Questions?



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY 65179 DMH/stp

[redacted]

From: [redacted]
Sent: Tuesday, January 09, 2007 4:06 PM
To: [redacted]
Subject: RE: [redacted]

b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Username: witt2004
Passwd: witt2oo4

[redacted]

[redacted]