White-stingray

bypassing stingray detectors

Altaf Shaik[1,2], Ravishankar Borgaonkar[2] , Shinjo Park[1], Jean-Pierre Seifert[1]

[1]Technische Universität Berlin & Telekom Innovation Labs
[2]Kaitiaki Labs

What’s the talk about

- IMSI catcher detector applications claim to detect stingrays and offer protection
- Study Strengths and Weaknesses – Hands ON testing

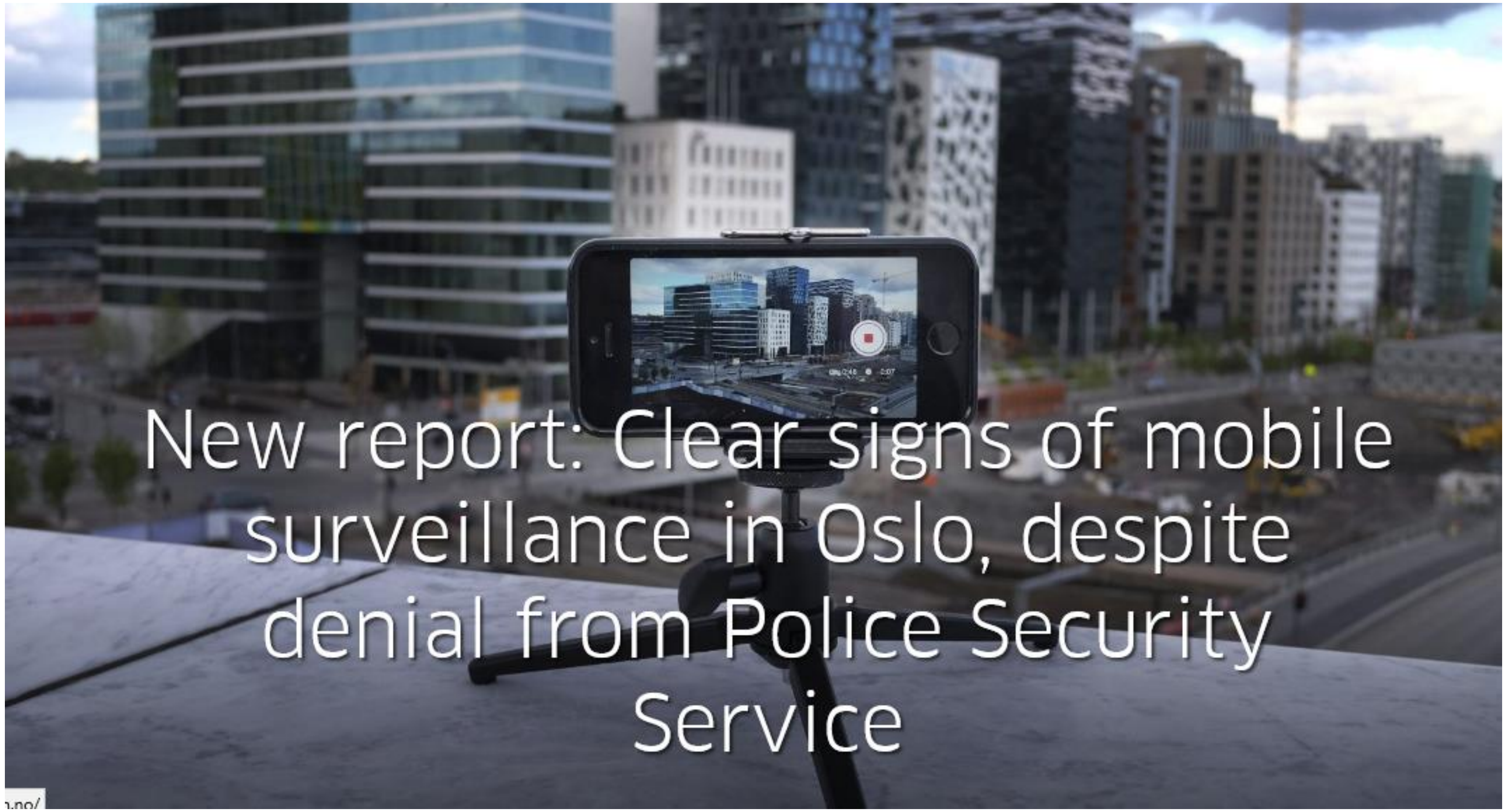
What to expect

- Stingray striking on mobiles – security breach
- Any tools for protection.
- How do they work. Can we trust them?
- Lets test..! Need a stingray..!
- What’s the story? Bypassed or caught.?
- Key learnings

Stingray

- AKA **IMSI Catcher – fake base station**
- Used by law enforcement agencies, police, criminals
- Call/SMS interception, identity theft, Denial of Service, spoofing, MITM
- Exploiting weaknesses in 2G and 3G mobile networks
  - Lack of mutual authentication
  - Phone loves high power base stations
  - Identity requests 24/7 with zero security
  - Full authority of the base station – security regulation (ON/OFF)

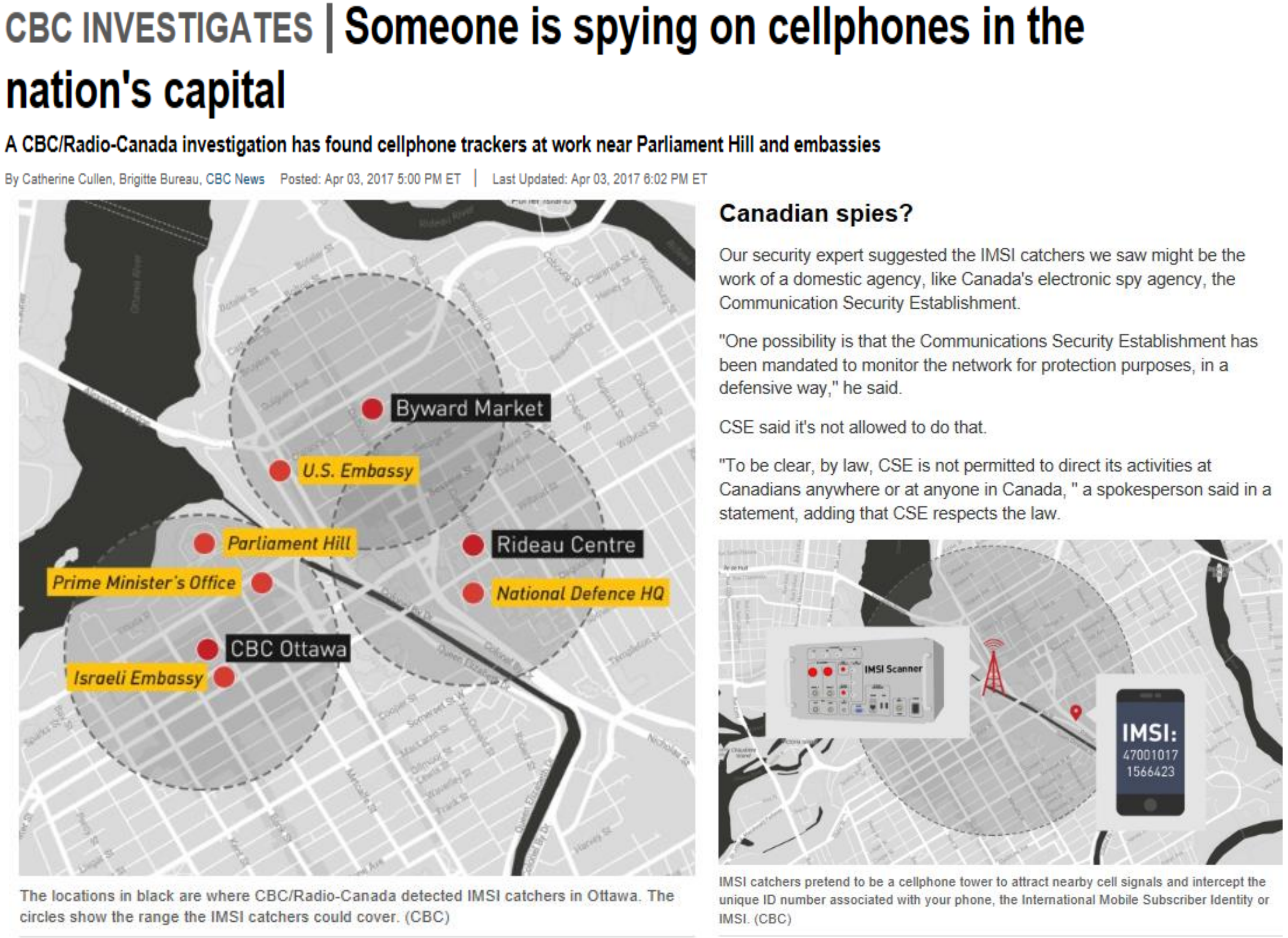
Stingray Spotted



New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service

https://www.aftenposten.no/norge/i/kamWB/New-report-Clear-signs-of-mobile-surveillance-in-Oslo_-despite-denial-from-Police-Security-Service

Stingray Spotted



CBC INVESTIGATES | Someone is spying on cellphones in the nation's capital

A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies

By Catherine Cullen, Brigitte Bureau, CBC News Posted: Apr 03, 2017 5:00 PM ET | Last Updated: Apr 03, 2017 6:02 PM ET

The locations in black are where CBC/Radio-Canada detected IMSI catchers in Ottawa. The circles show the range the IMSI catchers could cover. (CBC)

Canadian spies?

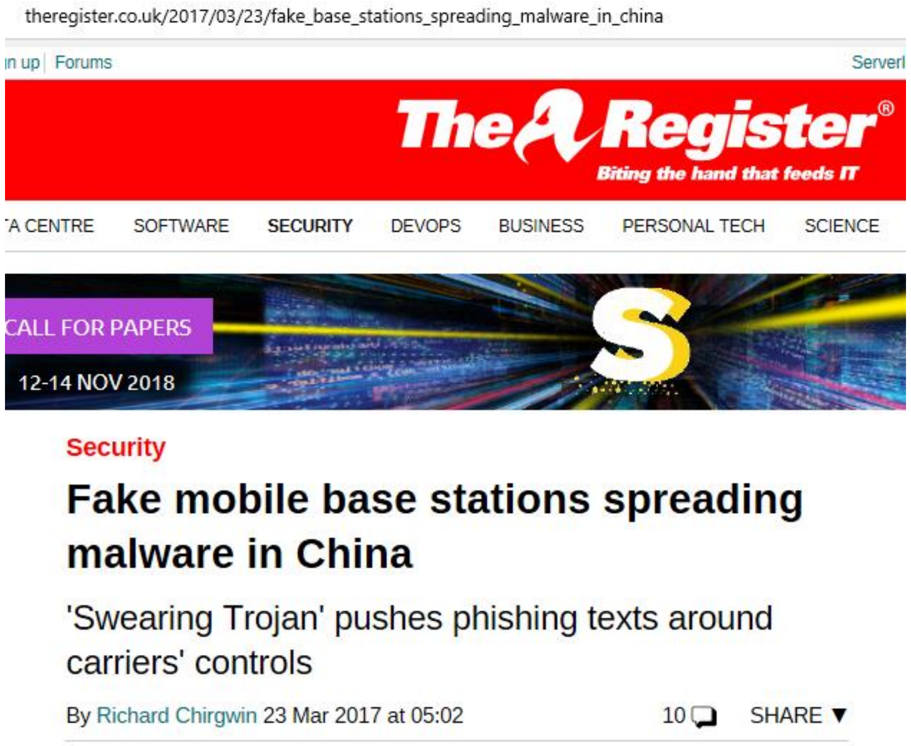
Our security expert suggested the IMSI catchers we saw might be the work of a domestic agency, like Canada's electronic spy agency, the Communication Security Establishment.

"One possibility is that the Communications Security Establishment has been mandated to monitor the network for protection purposes, in a defensive way," he said.

CSE said it's not allowed to do that.

"To be clear, by law, CSE is not permitted to direct its activities at Canadians anywhere or at anyone in Canada, " a spokesperson said in a statement, adding that CSE respects the law.

IMSI catchers pretend to be a cellphone tower to attract nearby cell signals and intercept the unique ID number associated with your phone, the International Mobile Subscriber Identity or IMSI. (CBC)



theregister.co.uk/2017/03/23/fake_base_stations_spreading_malware_in_china

n up | Forums
Serverl
The Register®
Biting the hand that feeds IT
A CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE
CALL FOR PAPERS
12-14 NOV 2018

Security

Fake mobile base stations spreading malware in China

'Swearing Trojan' pushes phishing texts around carriers' controls

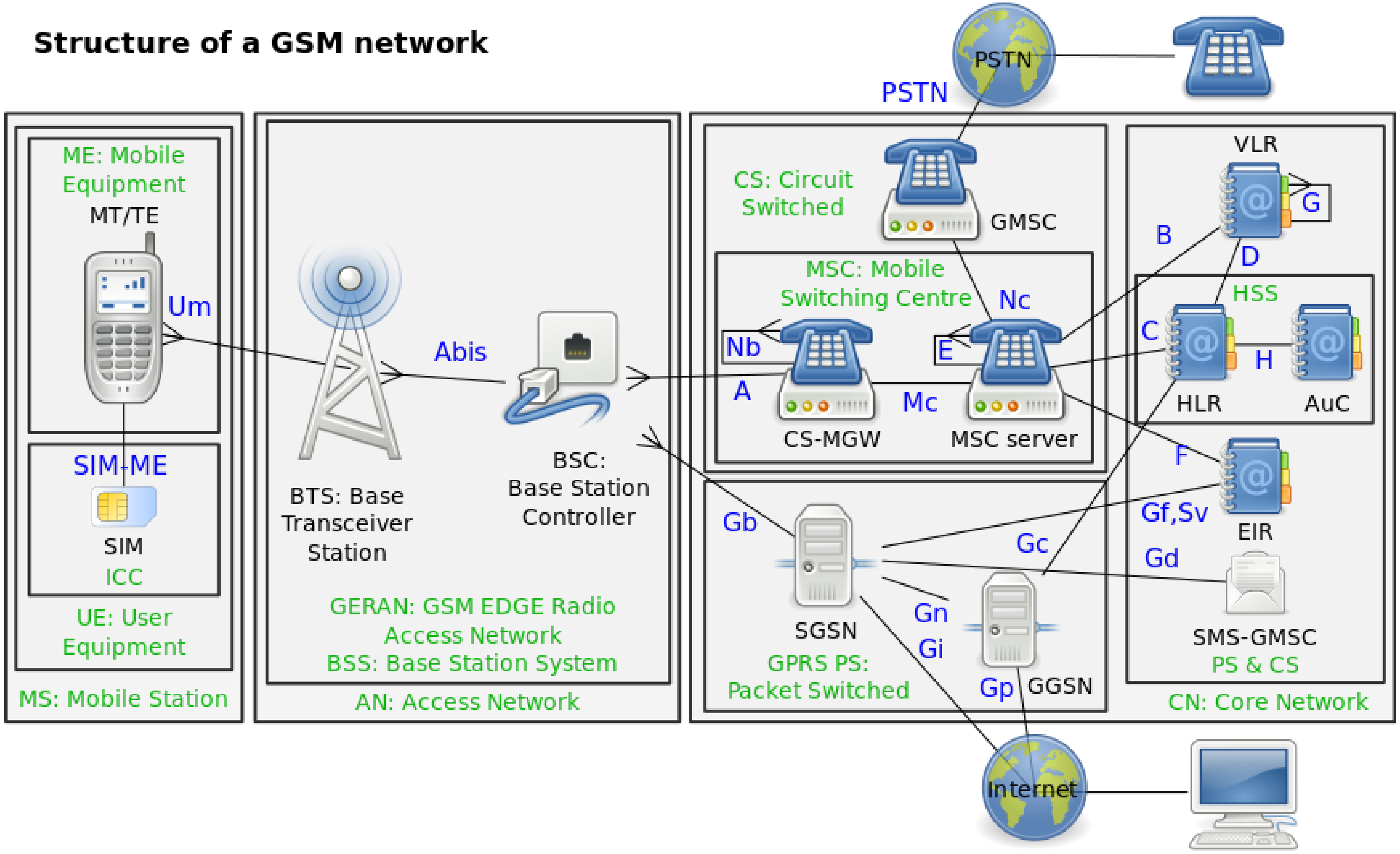
By Richard Chirgwin 23 Mar 2017 at 05:02 10 SHARE ▼

Police frequently uses Silent SMS to locate suspects

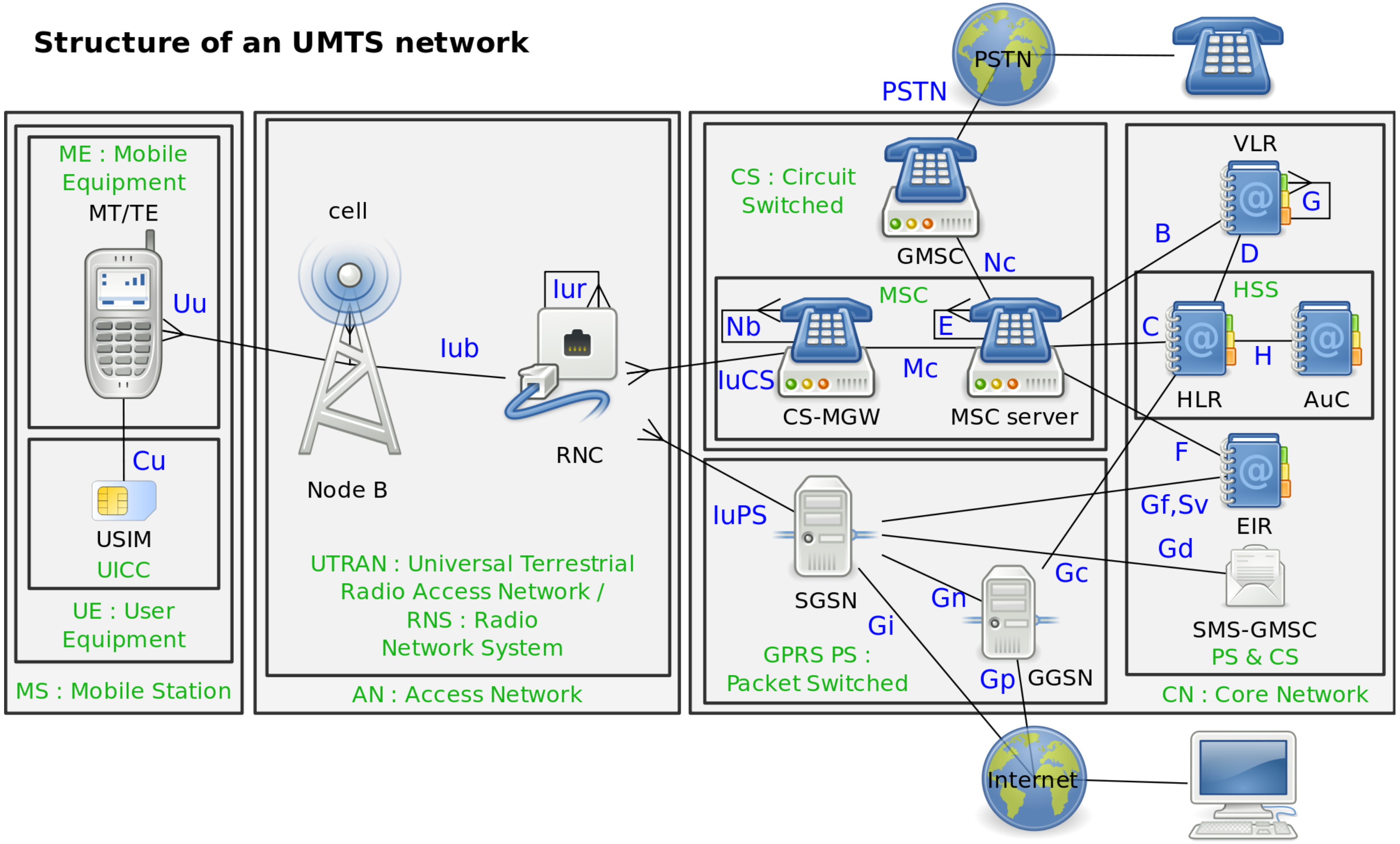
By EDRi

https://www.theregister.co.uk/2017/03/23/fake_base_stations_spreading_malware_in_china/
http://www.cbc.ca/news/politics/imsi-cellphones-spying-ottawa-1.4050049

Recalling 2G network



Recalling 3G network



Need protection.. But How.? Any tools.?

- IMSI Catcher detector (ICD)
  - App based
    - Open source, mostly android based, available for common users (need root)
    - Can detect, but cannot prevent from connecting
  - Commercial
    - *GSMK cryptophone, Overwatch* Expensive, not-open for research
    - Detect and avoid connecting back
  - Network based
    - Installed on operators network, require operator support

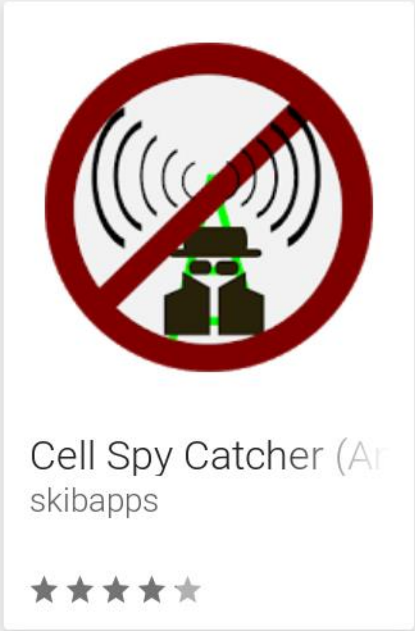
Basic operation of ICD

- **Analysis** of cellular network **traces**
- Traces = communication between phone and base station
- Traces directly from the modem **diagnostics port** – interfaces provided by smartphone OS (only android; no apple and windows)
- Abnormal message pattern, unauthorized requests for data/identities, security-OFF indicators

Target - Which ICD apps

- *AIMSICD, Snoopsnitch, Darshak* – open source, require root, access to traces

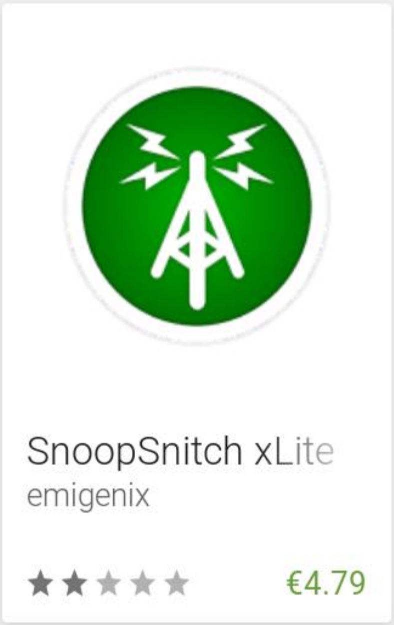
- *GSM Spy Finder, Cell Spy Catcher* – only apk, non-root, minimal info to detect



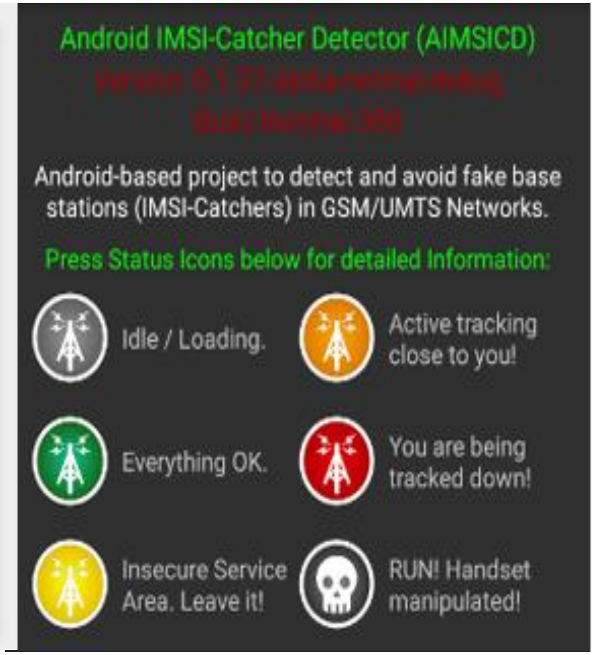
Cell Spy Catcher (Ar
skibapps
★★★★☆

SnoopSnitch
Security Research Labs
★★★☆☆

GSM Spy Finder
GALAN
★★★★☆



SnoopSnitch xLite
emigenix
★★☆☆☆ €4.79



Android IMSI-Catcher Detector (AIMSICD)
Version: 0.1.37-alpha-[illegible]
[illegible]

Android-based project to detect and avoid fake base stations (IMSI-Catchers) in GSM/UMTS Networks.

Press Status Icons below for detailed Information:

Idle / Loading.	Active tracking close to you!
Everything OK.	You are being tracked down!
Insecure Service Area. Leave it!	RUN! Handset manipulated!

Target – Why these apps

- Type “IMSI Catcher” in google play store -> apps with max downloads
- These applications safe and reliable? Developers claim so..!
- Zero (0) studies – testing these apps, no clear idea about their operation
- Very little data is online about their success and effective operation

How did we study ICD apps

- Learn their capabilities and limitations through source code and documentation
- Typically there is a detection engine monitoring and analyzing several "**Parameters**" – can fit into three categories
  - Layer 1 information
  - Broadcasted signaling
  - Dedicated signaling

Layer 1 Information – Rx Power

- By design phone always connects to a BS with the strongest signal
- ICs operate in higher and power than real BS to attract nearby mobile phones (higher Rx values on the phone side)
- ICs also have different operating schedule than real BS
- Rx power – not a reliable parameter, affected due to surroundings

Broadcast Signaling

- BS broadcasts System Information Block (SIB) messages for identification
- SIB messages contain network information, including:
  - Identity of the network, mobile country code and mobile network code
  - Identity of the BS, location area code (LAC) and cell ID (CID)
  - Neighboring cell list
- BS pages mobiles for incoming service request (call, SMS or data)
- All broadcasted signaling messages are not encrypted
- Phones trusts broadcasted signals sent by any network

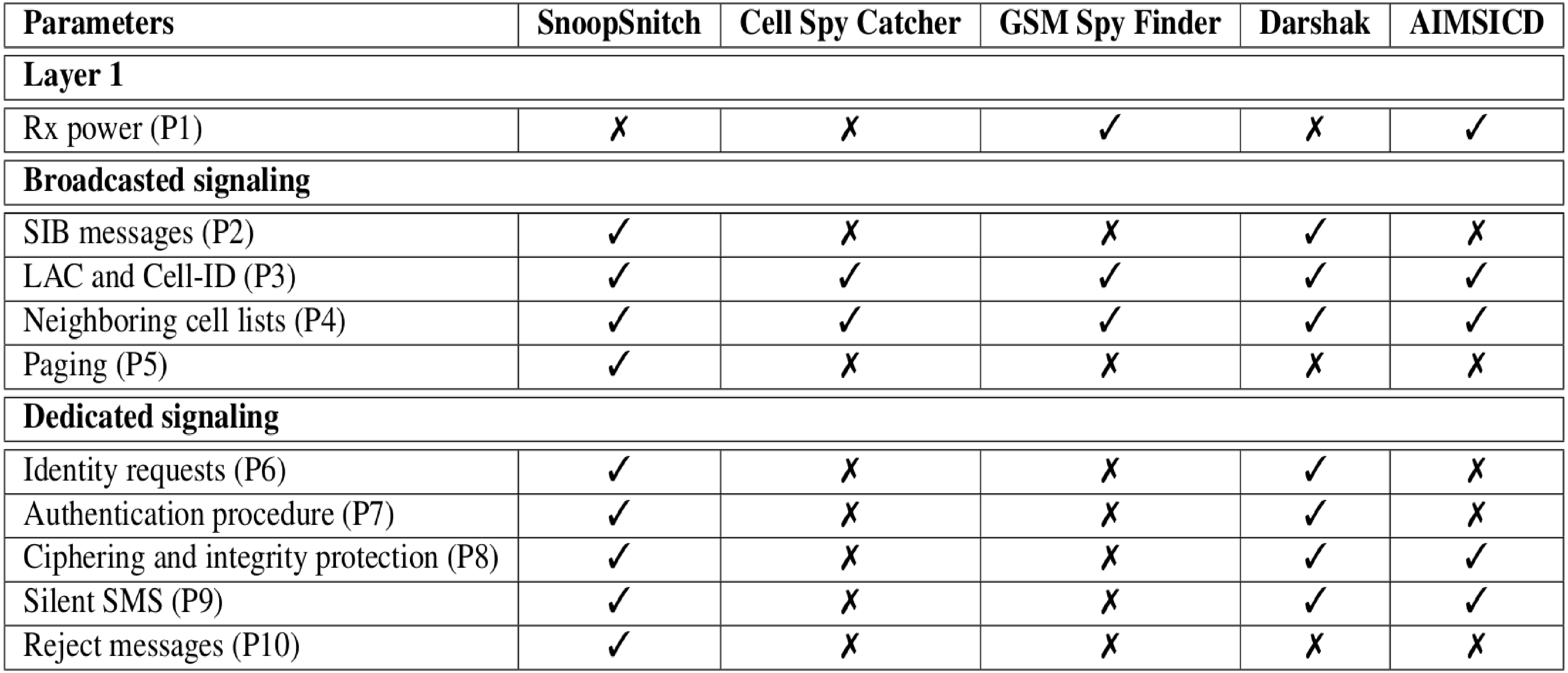
Dedicated Signalling

- By default phone **cannot distinguish** b/w real and fake base stations
- Phones exchanges messages with fake base station same as a real one
- ICs have quest for information, hence exhibit a **different signaling pattern**
    - Identity requests, always ask for permanent identities (IMEI)
    - Authentication can be never successful in 3G due to the lack of master key (ciphering is also not possible). But in 2G skip it with no hassle
    - Unintended signaling messages including silent SMS, location request, NITZ, etc.

Unexplored parameters

- ICD apps did not implement certain important parameters that stingray could use
  - RAND and AUTN (Authentication parameters, tracking attacks)
  - Location requests (for emergency calling or location based services, geolocation)
  - NITZ (Network information and Time Zone, DoS and time spoofing)

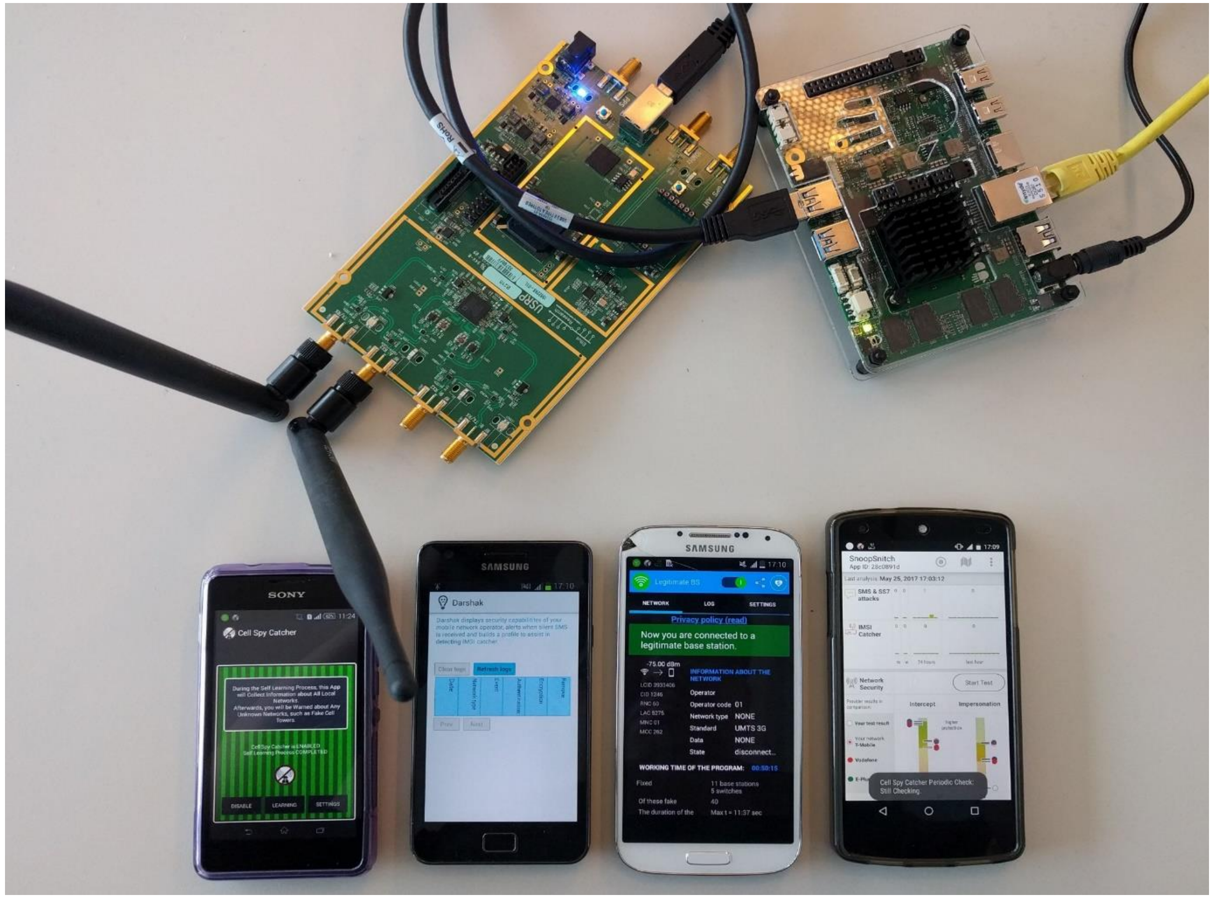
Apps and parameters



Parameters	**SnoopSnitch**	**Cell Spy Catcher**	**GSM Spy Finder**	**Darshak**	**AIMSICD**
Layer 1					
Rx power (P1)	✗	✗	✓	✗	✓
Broadcasted signaling					
SIB messages (P2)	✓	✗	✗	✓	✗
LAC and Cell-ID (P3)	✓	✓	✓	✓	✓
Neighboring cell lists (P4)	✓	✓	✓	✓	✓
Paging (P5)	✓	✗	✗	✗	✗
Dedicated signaling					
Identity requests (P6)	✓	✗	✗	✓	✗
Authentication procedure (P7)	✓	✗	✗	✓	✗
Ciphering and integrity protection (P8)	✓	✗	✗	✓	✓
Silent SMS (P9)	✓	✗	✗	✓	✓
Reject messages (P10)	✓	✗	✗	✗	✗

The White-Stingray

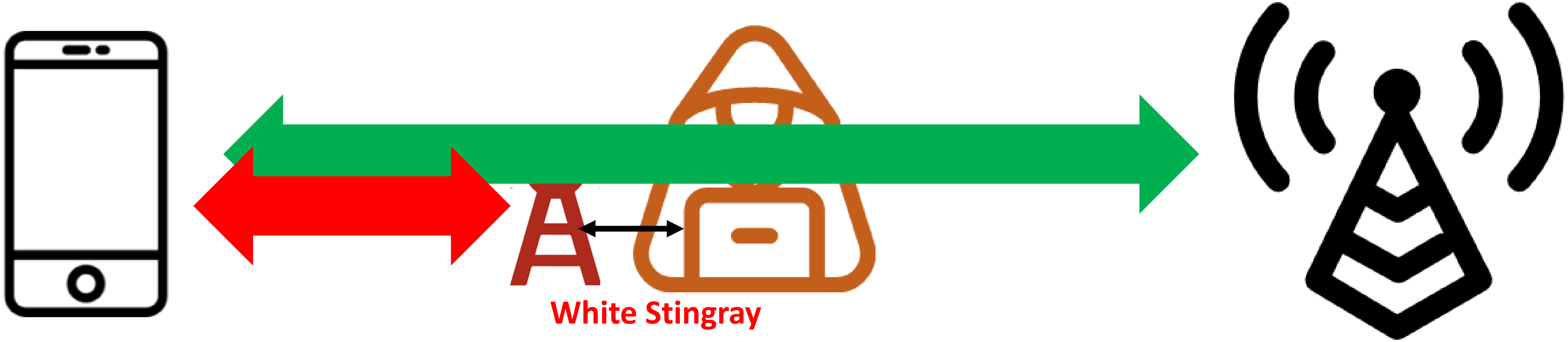
- Hardware: ***USRP*** B210 (RF frontend) + *UDOO* x86 (embedded PC)
- Software: ***OpenBTS*** (2G), ***OpenBTS-UMTS*** (3G), ICD apps
- Software modified to operate IC patterns
- 4G IC patterns also available, but apps support only 2G and 3G
- Faraday cage for testing



White-Stingray features

- Generates IC patterns
- normal and abnormal network configurations
- Unexpected protocol sequences.. smart fuzzing
- Unauthenticated message operation
- Bypass security mechanisms - plain-text communications
- Denial of Service, Jamming
- Silent call, Spam SMS

Game time



White-stingray vs ICD apps

- Rogue Base station with normal and abnormal identities
- IMSI catching – Asking for IMSI
- IMEI catching – Asking for IMEI, traditional and abnormal
- Location requests - RRLP
- Authentication bypass – Skip authentication
- NULL encryption – Skip encryption or use A5/0

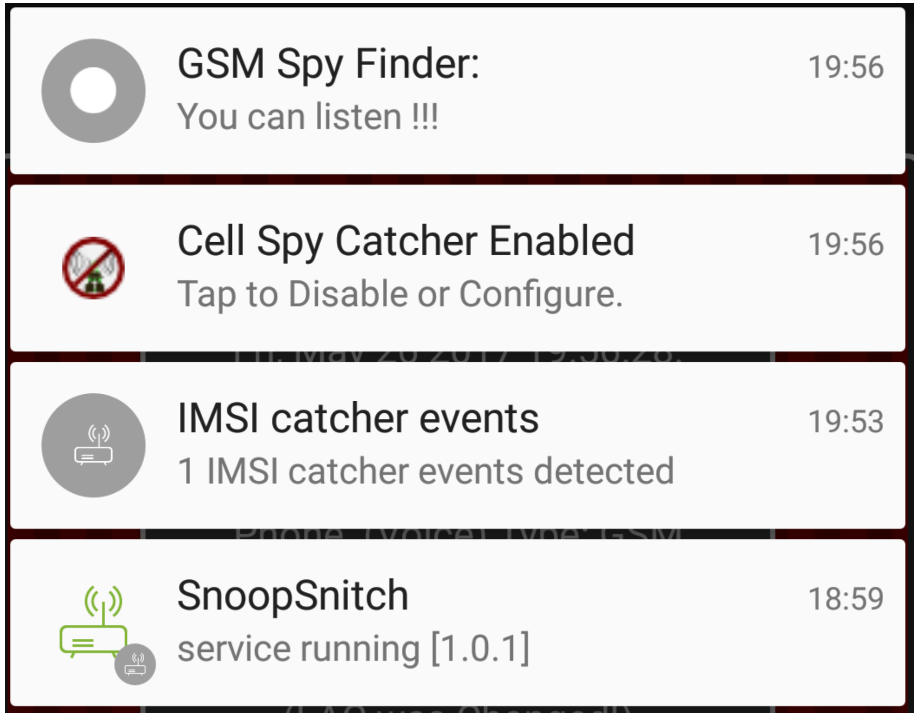
White-stingray vs ICD apps

- Paging with IMSI, TMSI, IMEI
- Bogus neighbor cell lists – Empty or fake cells
- High Power transmissions – Detect short and long lived high power
- Silent calls and silent SMS
- Spoofing false time and location information
- Downgrade from 3G to 2G

Bypassed or Caught. What happened?

Findings

- Apps exhibit false positive and false negative alarms



GSM Spy Finder: 19:56
You can listen !!!

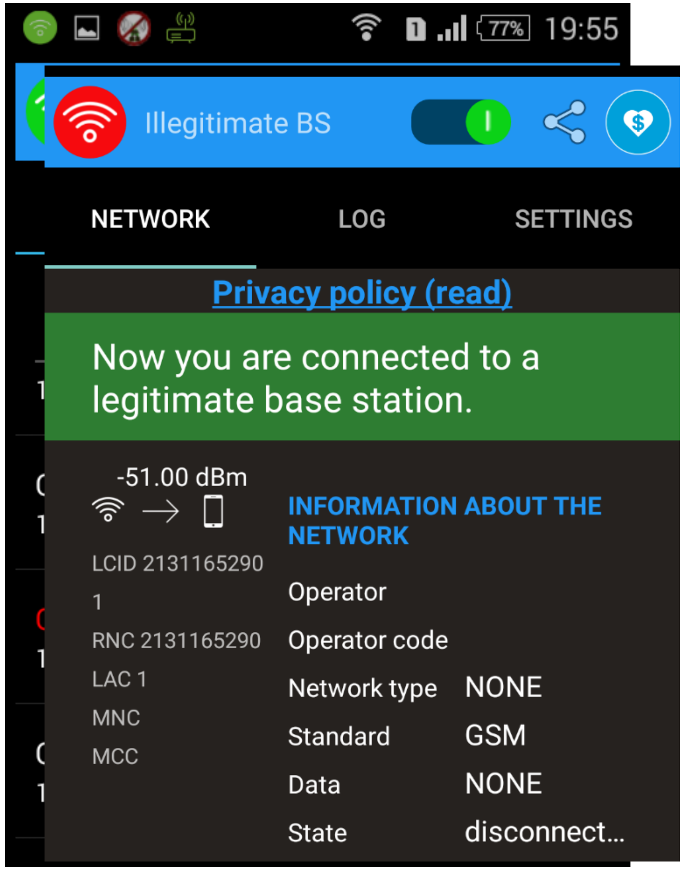
Cell Spy Catcher Enabled 19:56
Tap to Disable or Configure.

IMSI catcher events 19:53
1 IMSI catcher events detected

SnoopSnitch 18:59
service running [1.0.1]

Findings

- Rx power is stored by all apps, but none use it detect
- SpyFinder warn for abnormal network codes
  - Location Area Code: 1 to 9 , rest is normal
- Some apps warn for every new location code
  - False positives
- AIMSICD stores every cell for each Location and warns during mismatch



Privacy policy (read)

Now you are connected to a legitimate base station.

-51.00 dBm

INFORMATION ABOUT THE NETWORK

LCID 2131165290

1

RNC 2131165290

LAC 1

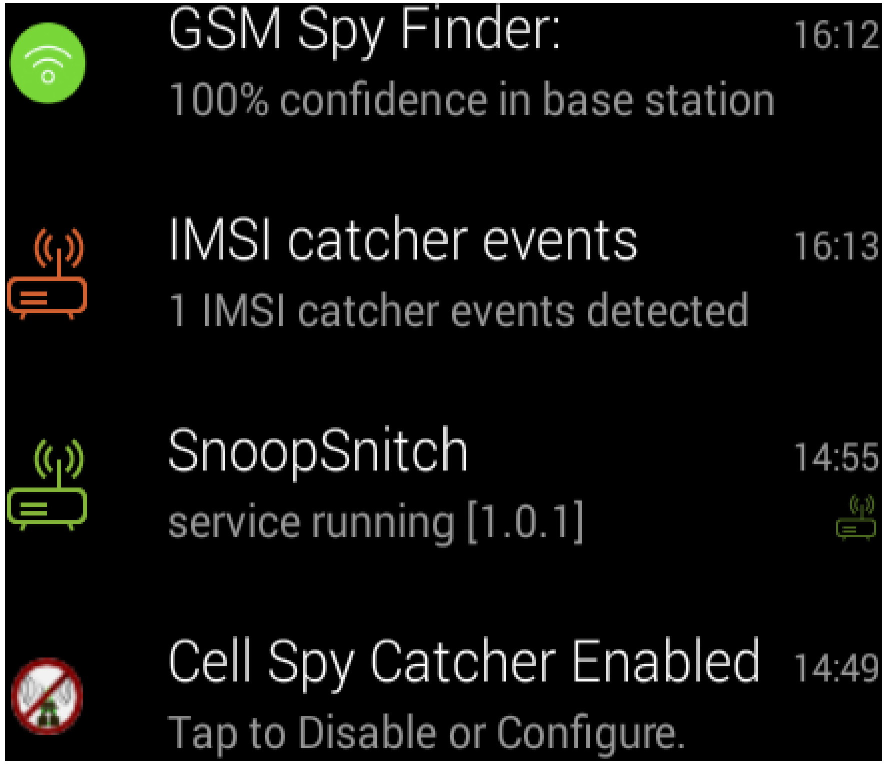
MNC

MCC

Operator	
Operator code	
Network type	NONE
Standard	GSM
Data	NONE
State	disconnect...

Findings

- Paging by IMSI – only *snoopsnitch* detects
- SpyFinder shows 100% confidence in rogue base station
- No response from CellSpyCatcher



GSM Spy Finder: 16:12
100% confidence in base station

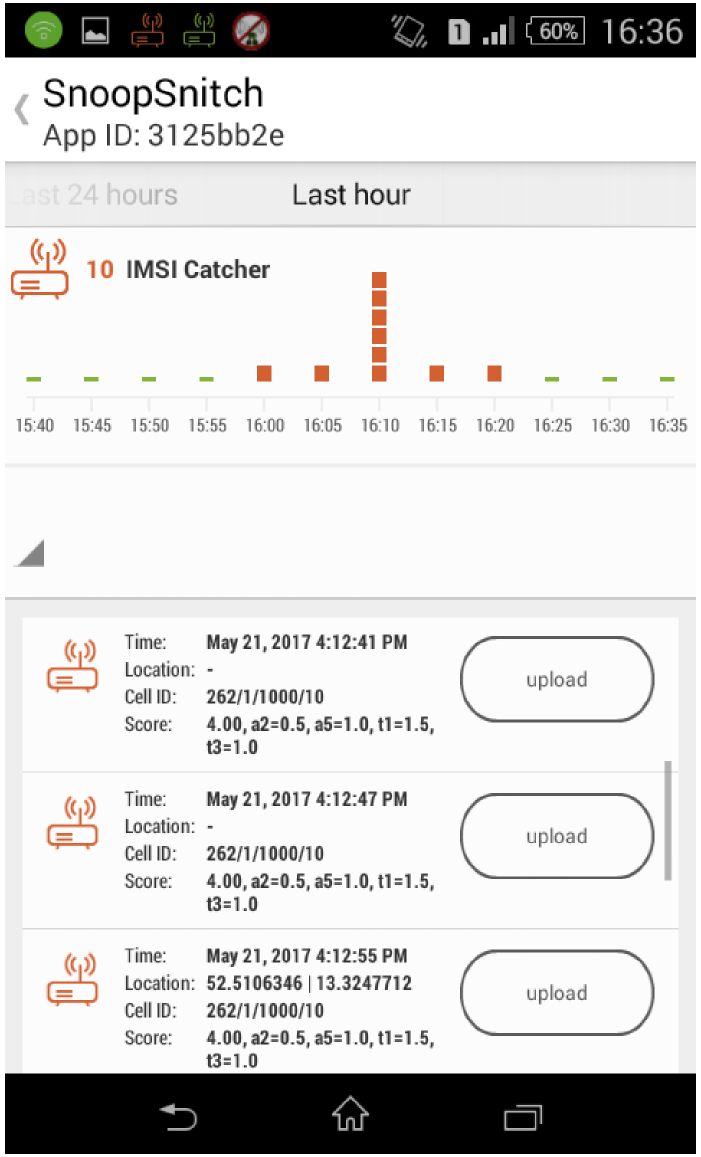
IMSI catcher events 16:13
1 IMSI catcher events detected

SnoopSnitch 14:55
service running [1.0.1]

Cell Spy Catcher Enabled 14:49
Tap to Disable or Configure.

Findings

- Collecting IMSI, IMEI and closing connection
- Only SnoopSnitch, Darshak and AIMSICD detect
- Sometime alarms from snoopsnitch are delayed – internal analysis takes time
- SnoopSnitch and Darshak evaluates **authentication** parameters, but no alarm is triggered



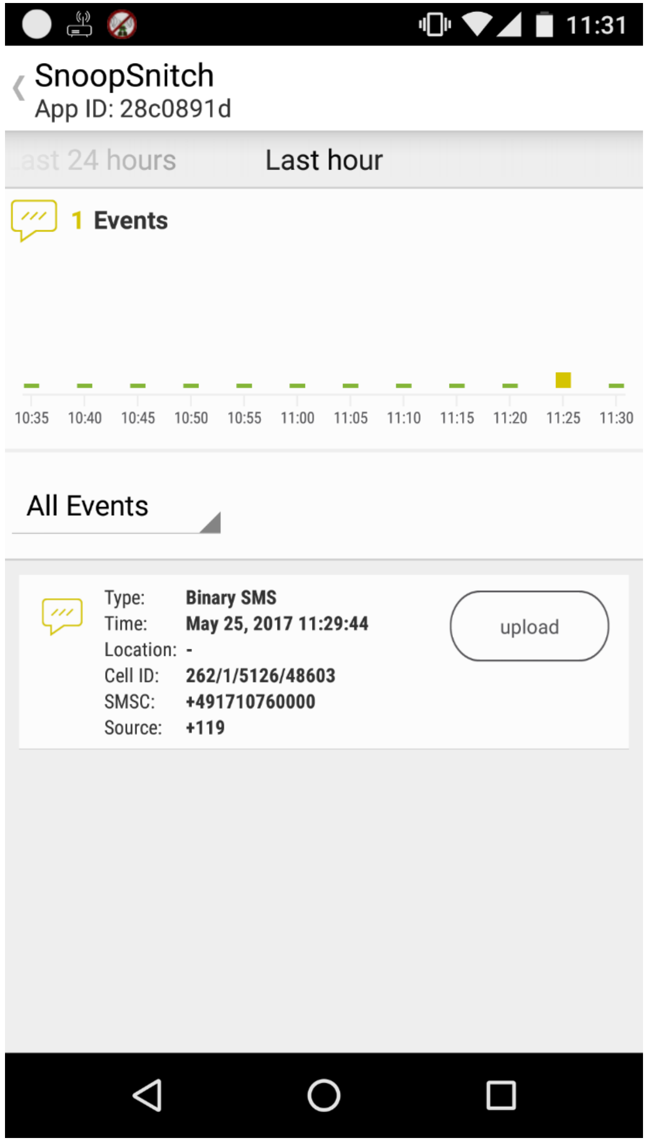
Time: May 21, 2017 4:12:41 PM
Location: -
Cell ID: 262/1/1000/10
Score: 4.00, a2=0.5, a5=1.0, t1=1.5, t3=1.0

Time: May 21, 2017 4:12:47 PM
Location: -
Cell ID: 262/1/1000/10
Score: 4.00, a2=0.5, a5=1.0, t1=1.5, t3=1.0

Time: May 21, 2017 4:12:55 PM
Location: 52.5106346 | 13.3247712
Cell ID: 262/1/1000/10
Score: 4.00, a2=0.5, a5=1.0, t1=1.5, t3=1.0

Findings

- Apps **detect null ciphering**, only SnoopSnitch and Darshak generates alarm
- Silent SMS detected by Snoopsnitch and Darshak
- Silent calls, Fake NITZ and downgrading can bypass detection

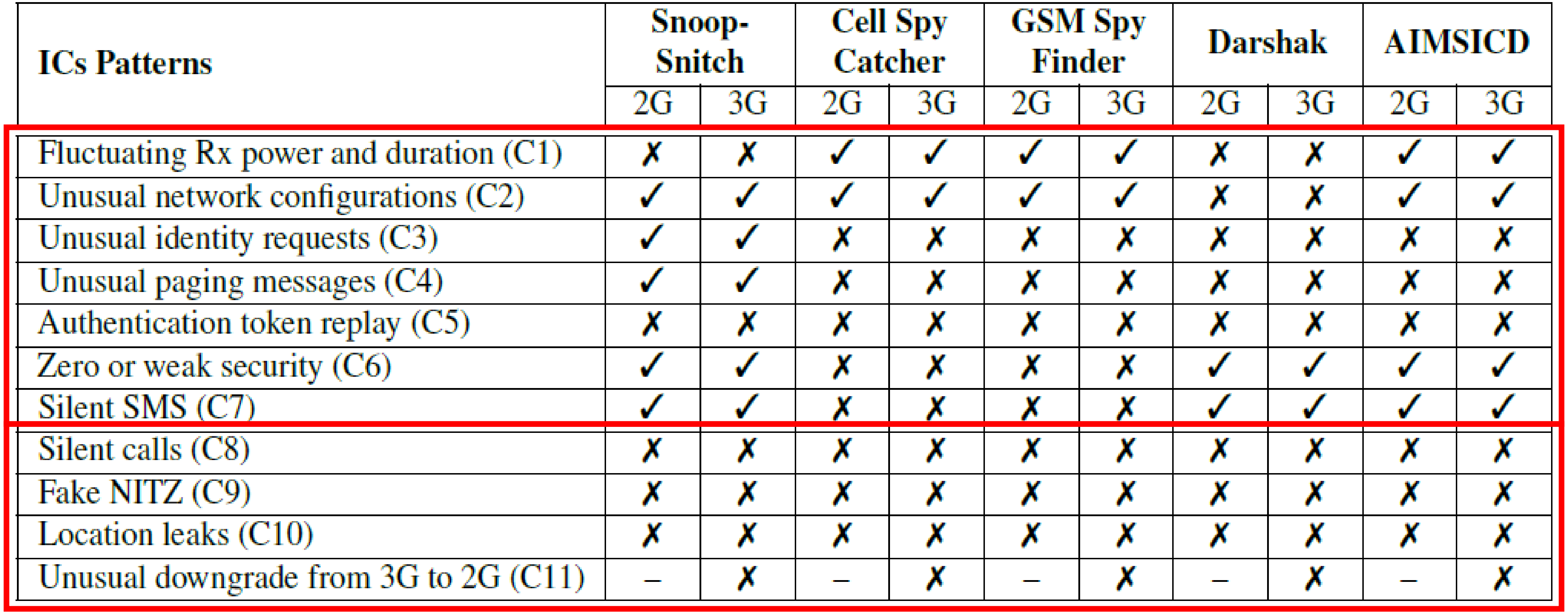


Type: Binary SMS
Time: May 25, 2017 11:29:44
Location: -
Cell ID: 262/1/5126/48603
SMSC: +491710760000
Source: +119

New bypassing techniques

- Using identical parameters like real base station
  - Reply the same System Information messages
- Operating incomplete protocol sequence
  - Ask for IMSI, IMEI and stay silent – do not issue reject
- Certain corner cases of signaling messages are not detected
- App makes incorrect assumptions on 3G ICs –lack of maturity
- Unimplemented parameters bypassed

Detection map



ICs Patterns	Snoop-Snitch		Cell Spy Catcher		GSM Spy Finder		Darshak		AIMSICD	
	2G	3G	2G	3G	2G	3G	2G	3G	2G	3G
Fluctuating Rx power and duration (C1)	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓
Unusual network configurations (C2)	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓
Unusual identity requests (C3)	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Unusual paging messages (C4)	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Authentication token replay (C5)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Zero or weak security (C6)	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓
Silent SMS (C7)	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓
Silent calls (C8)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Fake NITZ (C9)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Location leaks (C10)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Unusual downgrade from 3G to 2G (C11)	–	✗	–	✗	–	✗	–	✗	–	✗

Strengths

- Identity requests are detected
- Simple and common threats are detected
  - Binary SMS, abnormal cell IDs
- Notification to users by certain apps

Weaknesses

- Weak detection strategies
  - Improper parameter selection
  - Not ready for unexpected protocol sequences
- Insufficient features
  - Design issues for developers
  - Missing parameters

Fixes

Developers

- Bad idea to rely only on broadcast parameters – false positives and negatives
- Protocol sequence handling – all possible types
- Radio messages with privacy sensitive info – need more inspection
- Right notifications and alerts at right time – real time
- Don’t annoy the user with false alarms and too often

Fixes

OS and baseband Makers

- Full open access to baseband via the OS – very risky
- But, baseband makers should consider offering a secure and controlled access b/w smartphone OS and baseband OS
- Access network traces without root access
- Xiaomi announces smartphone processor with integrated baseband chip – with ICD features. Bingo..!

Commercial ICD

GSMK cryptophone, Overwatch

- Reliably detects many patterns of white-stingray
  - 70% detection, good score
- Although some new circumventing techniques bypassed
- Real-time alerts and phone reboots with strong signs of IMSI catcher

Learnings

- Phones are vulnerable
- We can still fight IMSI catchers – easier compared to life on Mars
- Potentially weak detectors – fail to catch
- Require more robust and smart detection algorithms
- Vendors and manufacturers should provide more controlled access to baseband

The End