

White-Stingray

Evaluating IMSI Catchers Detection Applications



Shinjo Park ¹

Altaf Shaik ¹

Ravishankar Borgaonkar ²

Andrew Martin ²

Jean-Pierre Seifert ¹

¹TU Berlin & Telekom Innovation Labs

²Department of Computer Science
University of Oxford

WOOT '17, 2017. 8. 15.

- Introduction to IMSI catchers and its detection
- Parameters used by IMSI catcher detection apps
- Introduction to White-Stingray framework
- Evaluation of IMSI catcher detection apps
- Countermeasures for apps
- Conclusion and future work

IMSI Catchers: Who Are They?

- Mobile phones are identified by two permanent identifiers:
 - IMEI (International Mobile Equipment Identity) for device
 - IMSI (International Mobile Subscriber Identity) for subscriber
 - Often they are linked to the physical person
- IMSI catchers (ICs) collect the identities of nearby mobile phones
- Law enforcement agencies often use ICs to track the person

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

Police frequently uses Silent SMS to locate suspects

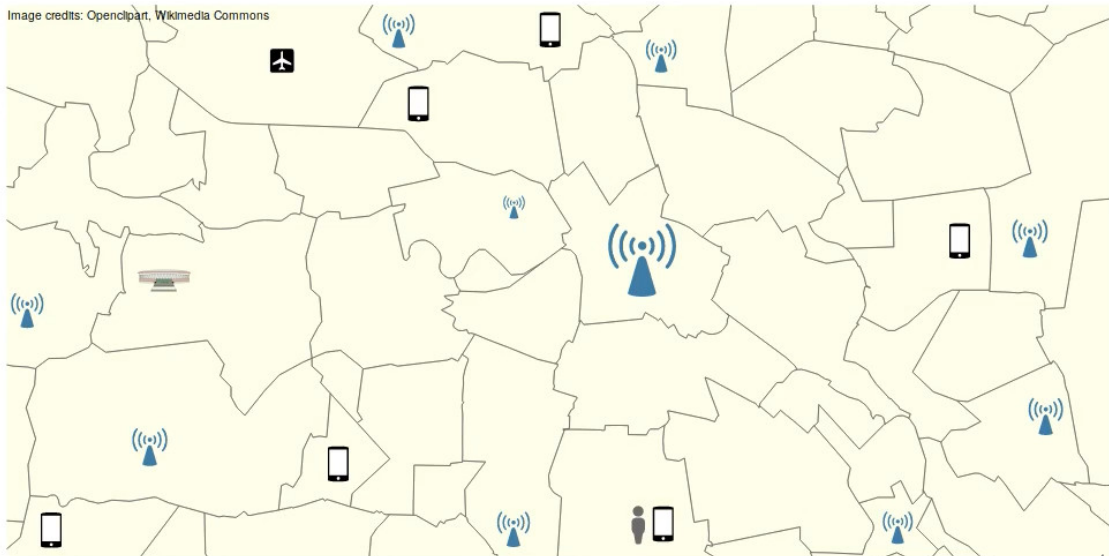
By EDRI

Someone could be secretly spying on mobile communications at White House and Pentagon – but who?

■ A defence contractor has noticed highly-suspicious activity coming from mobile base stations in Washington DC.

Simplified Operation of IMSI Catchers

Image credits: Openciptart, Wikimedia Commons



Whoa, Sounds Scary. How Can We Detect It?

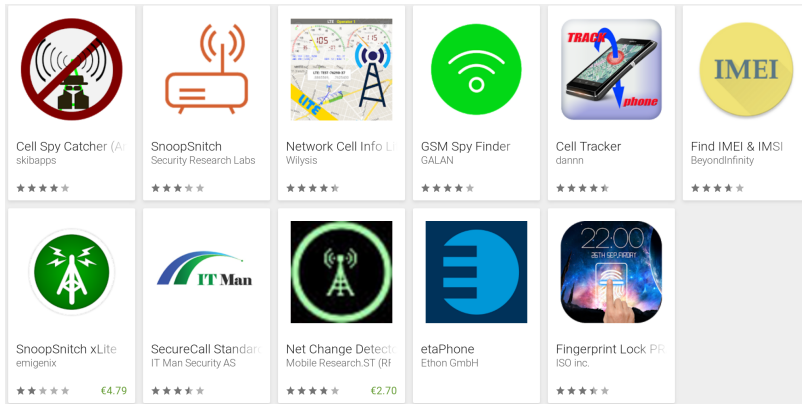
Wikipedia, Duck Typing

“If it walks like a duck and it quacks like a duck, then it must be a duck.”

- Both real base stations (BSs) and ICs speak the same protocol to the phone
- Phones have no idea whether the BS is legit or not
- However, ICs can not perfectly mimick the behavior of the real BS because of technical limitations
- Several IMSI catcher detection apps (ICD apps) on smartphones exist

Motivation of the Study

- How can we rely on these apps for detection of ICs?
- No previous study existed for evaluating the capability of these apps
- Build a framework to systematically evaluate them



- Searched Google Play store for “IMSI Catcher” and selected highest number of downloads (100-500k)
- SnoopSnitch, Cell Spy Catcher, GSM Spy Finder, Darshak, AIMSICD
 - AIMSICD is not on Google Play but has the ICD functionality
 - SnoopSnitch, Darshak, AIMSICD are open source software, others are not

Selecting and Implementing Parameters

- Capabilities and limitations of the apps based on the source code and documentation
- Publicly available documentation of ICs for their patterns
- Since ICs are not available for the general public, even the leaflet for basic capability is unavailable in most cases
- We categorized parameters of ICs into three categories:
 - Layer 1: Rx power
 - Broadcasted signaling
 - Dedicated signaling
- Details about the parameters will be covered in the following slides

Layer 1: Rx Power

- The phone is connecting to the BS with the strongest signal by standards
- ICs operate in higher 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
- Only small number of apps are monitoring Rx power
- Rx power only is not a reliable parameter, as it can be changed by other factors

Broadcasted Signaling

- BS is broadcasting System Information Block (SIB) messages to identify itself
- 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
 - Parameters used for network connection
- BS also pages mobile phone when there is an incoming service request (call, SMS or data)
- All broadcasted signaling messages are not encrypted
- Phones acquire information from the broadcasted signals and connects to the network

Broadcasted Signaling of ICs

- ICs exploit broadcasted signaling in various ways:
- Configuration parameters are highly deviating from the nearby real BS
- Cell identities (LAC and CID) are stolen from the nearby cells, making them appear in unexpected place
- Neighboring cell list is absent, to prevent handover from it
- Paging in IMSI, which happens rarely
- ICD apps typically use this as a parameter, specific usage varies among apps

Dedicated Signaling of ICs

- Phones initiate connection procedure to ICs just same as real BS
- ICs and real BS differ in dedicated signaling:
 - Identity requests, always ask for permanent identities
 - Authentication can be never successful due to the lack of master key (ciphering is also not possible)
 - Unintended signaling messages including silent SMS, location request, NITZ, etc.

ICD Apps and Dedicated Signaling

- Android public API exposes only limited information for apps
- ICD apps needs to use **root permission** and private API for more information
- Opening up root permission may expose another security risk
- Only 2 out of 5 tested apps required root permission to operate
- Each apps have different degree of analyzing dedicated signaling

White-Stingray Framework

- A framework for evaluating ICD apps by emulating the ICs patterns
- Based on open-source software and low cost hardware
- Although 4G support is possible, we exclude 4G as only one of the tested app explicitly mentioned it

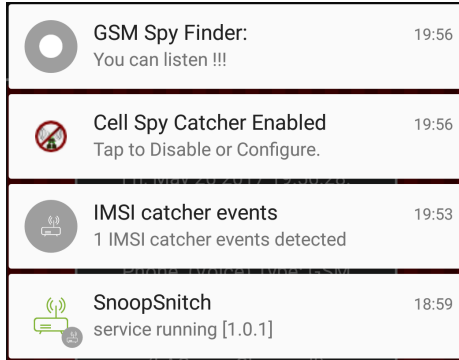
White-Stingray Framework: Setup



- Hardware: USRP B210 (RF frontend) + UDOO x86 (host PC)
- Software: OpenBTS (2G), OpenBTS-UMTS (3G), ICD apps
- Softwares are modified to simulate IC patterns

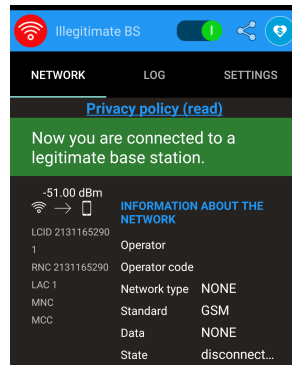
App Evaluation: Overview

- Certain ICs patterns can trigger false positive or false negative alarms
- Patterns to evade ICD app's detection algorithm were implemented



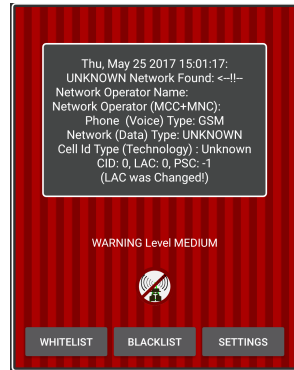
App Evaluation: Broadcasted Signaling

- Rx power: some of the apps detect it, but not using as a primary parameter
- Some apps give warning when the current LAC/CID is suspicious
- Android API only provides above data reliably
 - While neighboring cell API exist, they are not reliable on every devices
 - Some app mention this fact in its help message
- Root permission is required for more parameters




App Evaluation: Broadcasted Signaling

- Rx power: some of the apps detect it, but not using as a primary parameter
- Some apps give warning when the current LAC/CID is suspicious
- Android API only provides above data reliably
 - While neighboring cell API exist, they are not reliable on every devices
 - Some app mention this fact in its help message
- Root permission is required for more parameters



App Evaluation: Dedicated Signaling

- Only SnoopSnitch, Darshak and AIMSICD can detect these patterns
- Requesting IMSI, IMEI and rejecting connection
 - Typical identity collection performed by IMSI catchers
 - SnoopSnitch gives an alarm upon the reject message
- SnoopSnitch and Darshak evaluates authentication parameters, only visible in app and no alarm is triggered
- All apps detect null ciphering, only SnoopSnitch and Darshak generates alarm based on this
- Silent calls and SMS, downgrading



Time: May 21, 2017 4:13:28 PM
Location: 52.5106346 | 13.3247712
Cell ID: 1000/10
Score: 4.00, a2=0.5, a5=1.0, t1=1.5,
t3=1.0

Bypassing the ICD app's detection

- Broadcasted signaling
 - Mimicking the real BS as much as possible
- Dedicated signaling
 - Connection rejection by timeout is not covered
 - Certain corner cases of signaling messages are not detected
 - App makes incorrect assumptions on 3G ICs
 - Unimplemented but noteworthy parameters: location request, difference of presence of clock information

Limitation of ICs Detection

- Endless hide and seek game between ICs and detectors
- Android API alone provides only basic information
 - Accessing baseband data requires usage of manufacturer specific private APIs
 - Tied to certain processor, baseband, OS version and any combination of these
- Mostly focusing on the 2G ICs pattern, little is available for 3G ICs
- Protocol exploits: are they used by ICs to avoid detection?
- Differentiation of small cells and ICs

Countermeasures

- Know the limitations of Android API
- Evaluate corner cases
- Provide clear and reasonable alarm
- Make baseband access feasible, risk of new attack vectors exist
- IC detection on baseband level, implemented by some Chinese vendors

Conclusion and Future Work

- Current ICD apps have limitation on its detection strategies
- Building ICs avoiding detection is possible by systematical analysis of patterns
- Possible protocol exploits should be reflected in ICD apps
- IMSI catchers are endless game between attacker and defender – persistent measurement will give more clear view on detection
- Locating IMSI catchers based on device measurements
- Preemptive warning for IMSI catcher, will it be possible?

Thanks!

- Questions and discussions



This research was partly performed within the 5G-ENSURE project of the EU Horizon 2020.