



Understanding IMSI Privacy

Ravishankar Borgaonkar
TU Berlin

Swapnil Udar
Aalto University

Email: darshak@sec.t-labs.tu-berlin.de

Blackhat USA 2014, Las Vegas, 7th August 2014

Overview

- ◆ Unresolved Privacy Issues
(IMSI catchers and Silent SMS)
- ◆ Darshak- Privacy framework
- ◆ Use-cases and demos
- ◆ Future work

Unresolved Privacy Issues

Mobile Security Status

- ◆ Efforts from OS providers, Manufacturers, network operators
- ◆ Efforts from researchers, startup companies
- ◆ Devices are good but cellular network secure???
- ◆ Still all fail when **Targeted Attacks**
- ◆ What is Targeted Attacks and who does it?
 - ★ IMSI catchers
 - ★ Illegal entities?
 - ★ Methods of doing?

Targeted Attacks

IMSI catcher or compromising phone

- ◆ IMSI catchers
 - ★ Often used
 - ★ Exploits cellular weaknesses
 - ★ Location and interception
- ◆ Pegasus
 - ★ Compromising with OTA update
 - ★ SIM toolkit? Like ANT

3G-GSM TACTICAL
INTERCEPTION &
TARGET LOCATION

Small cellular base-sta
homeland security app



The system introduces a powerful and unique monitoring tool, called Pegasus, Which allows remote and stealth

monitoring and full data extraction from remote targets devices via untraceable commands.

Sources: product manuals

Unsolved Security Questions

- ◆ Your last call was encrypted/authenticated?
- ◆ Is someone tracking you?? No app for that
- ◆ Can someone listen to your calls/SMS?
 - ★ Besides legal entities
 - ★ Last call/SMS was encrypted?
- ◆ Are you a victim of IMSI catcher attack?
- ◆ Is your mobile handset and operator using **up-to-date** encryption standards?

More ecosystem problems

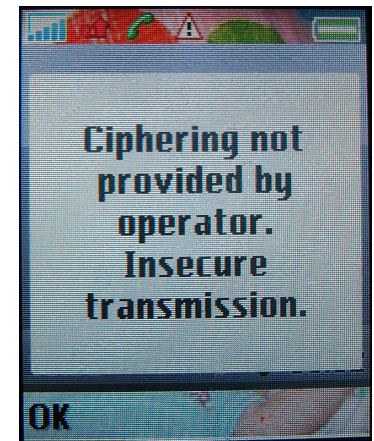
- ◆ 3GPP standard for mobile handset features

ETS 300 505 (GSM 02.07 version 4.8.2): January 1998

Table 1: Basic MS features

Name	Mandatory (M) Optional (O)
1.22 Cipherring Indicator	M*

- ◆ No API for Android, iOS, Windows, BB
 - See issue* 5353: Cipherring Indicator (Android)
- ◆ Flatrate calling/data/sms rates –
 - you getting free calls?



Source:wikipedia

* <https://code.google.com/p/android/issues/detail?id=5353>

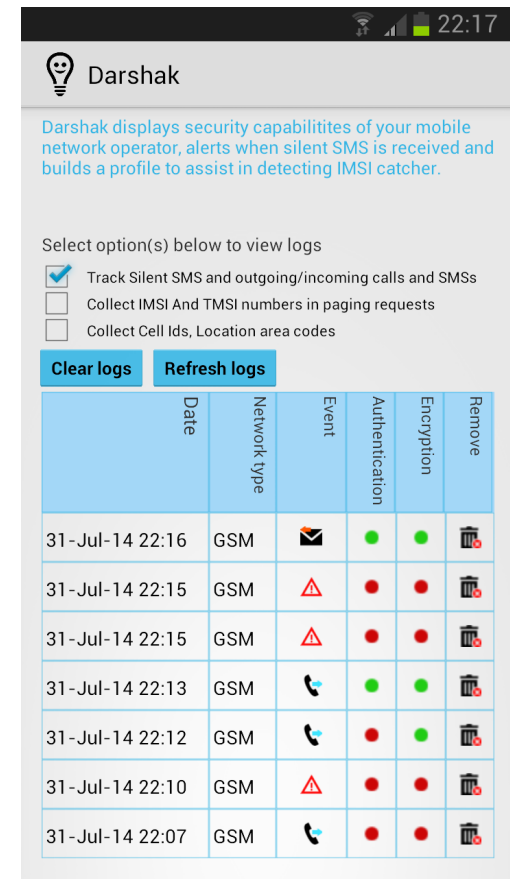
Darshak Framework

Motivation

- ◆ Research platform to collect GSM & 3G security relevant data
- ◆ Easy to use cellular network security indicator

Darshak* Framework

- ◆ Display (in) security capabilities of your cellular network operator
- ◆ Android based framework
 - ★ Detection
 - ★ Notification
 - ★ Intelligence
 - ★ Collection
- ◆ Security features
 - ★ GSM and 3G networks
 - ★ Captures 'silent sms' and notifies user
 - ★ Alerts when operator not doing encryption?
 - ★ Displays suspicious activities

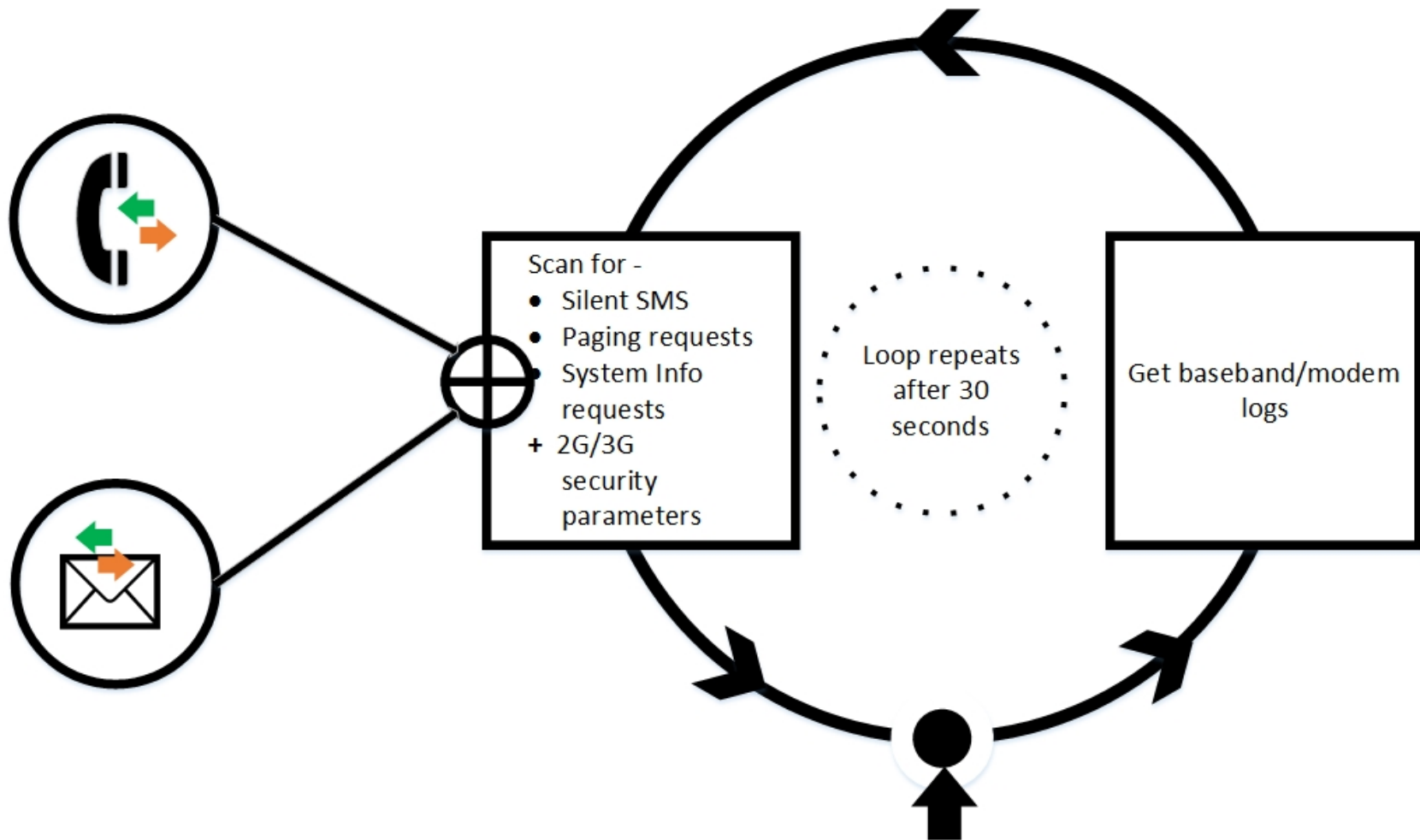


* In ancient Indian language, Darshak means indicator

Technical Details

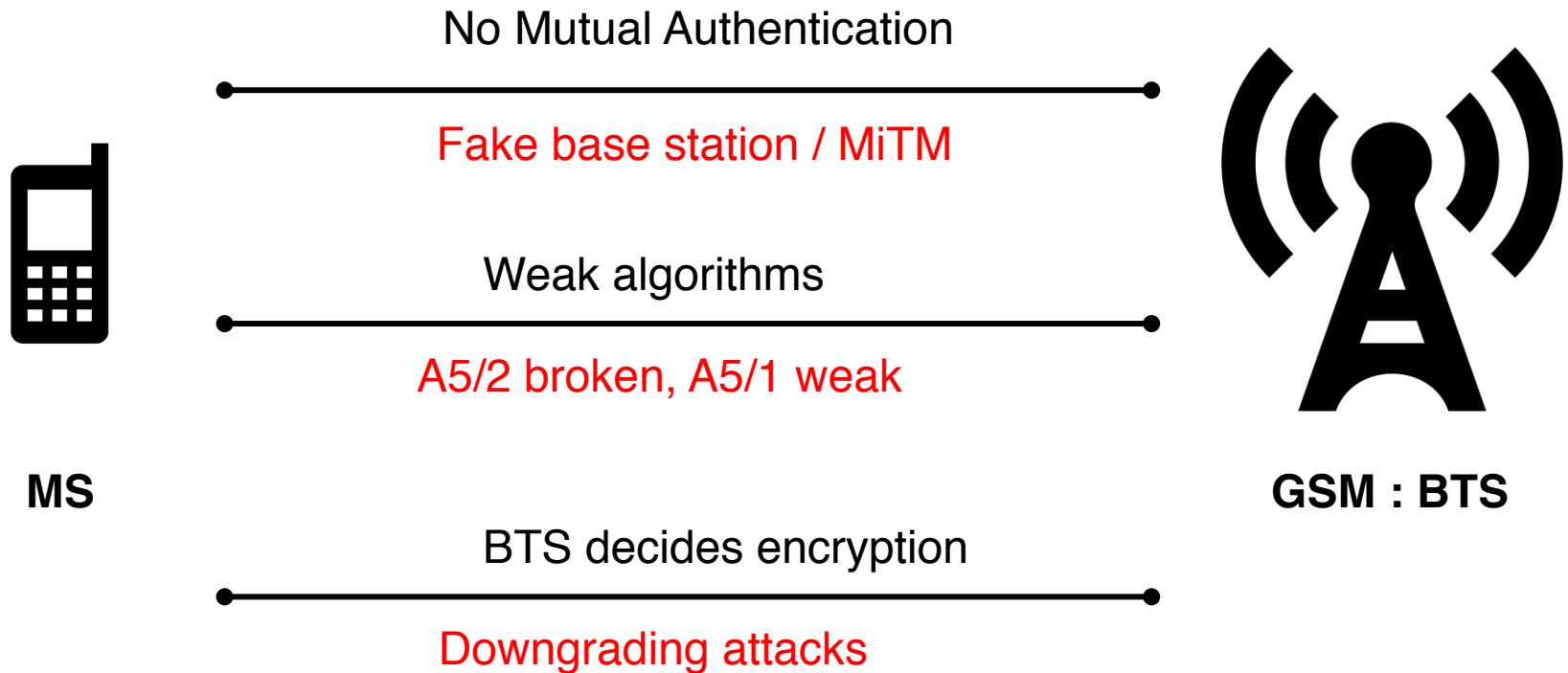
- ◆ Running on Intel baseband devices Samsung S3, S2
- ◆ Primarily based on Xgoldmon idea
- ◆ Thanks to GSMMAP
- ◆ Device needs to be rooted
- ◆ Notifies sender's number - Silent SMS
- ◆ Classify security capabilities of 2G/3G networks A5/0, A5/1, A5/3, (useful while roaming)
- ◆ Current TMSI after every event
- ◆ Displays authentication tokens (RAND, AUTN)

Methodology

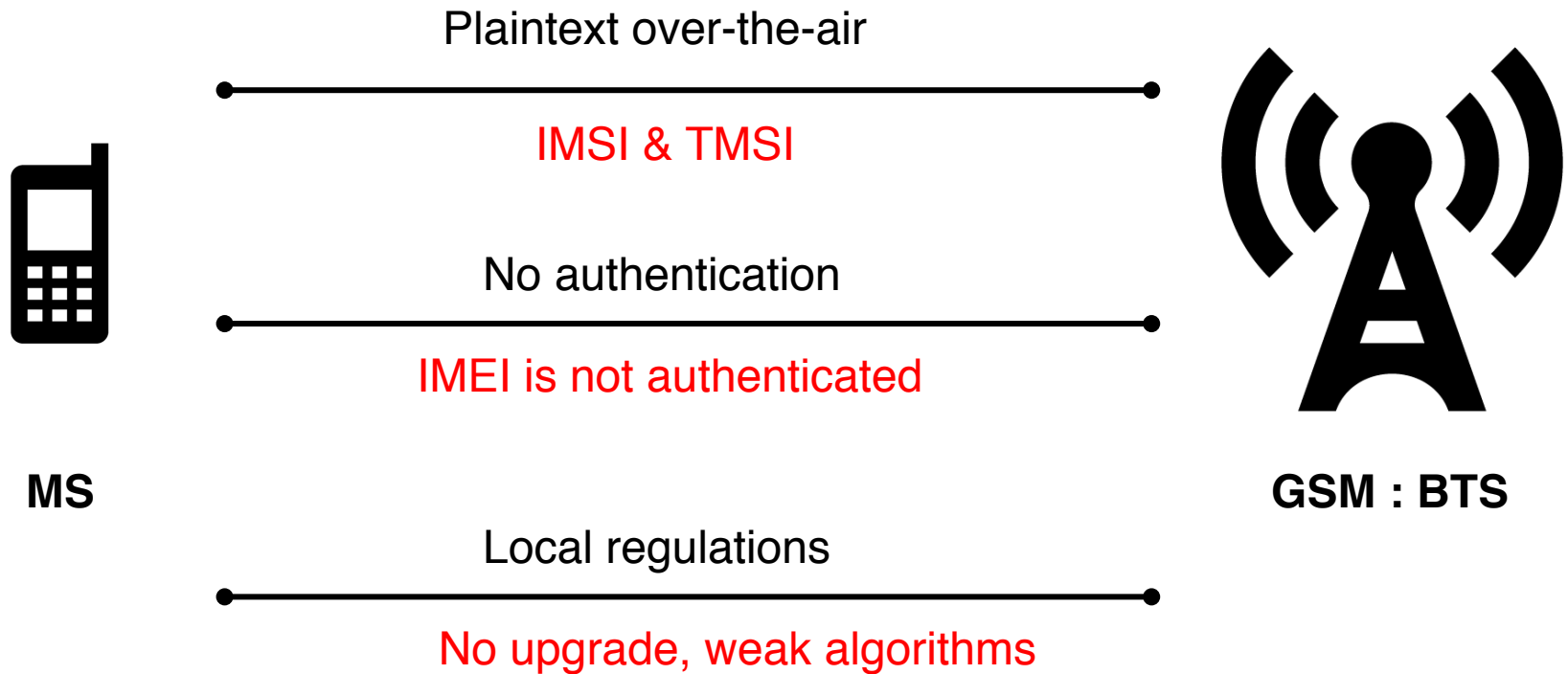


GSM background

GSM Security Issues



GSM Security Issues



GSM badly broken

- ◆ Proven experimentally by various researchers
- ◆ Has it fixed and upgraded by your operator as per GSMA guidelines?
- ◆ Authentication
 - ★ Mobile originated – mostly performed
 - ★ Mobile terminated – not often
- ◆ Encryption - A5/1 vs A5/3 vs A5/0
- ◆ Threat model is not your government (lawful interception) but other illegal entities

Use-cases and Demos

GSM and 3G security indicators









- ◆ Invokes at every incoming and outgoing **radio** event

Darshak					
Date	Network type	Event	Authentication	Encryption	Remove
28-Jul-14 17:03	GSM				
28-Jul-14 15:57	GSM				
28-Jul-14 11:53	GSM				
28-Jul-14 10:38	GSM				
28-Jul-14 01:01	GSM				
27-Jul-14 23:41	GSM				
27-Jul-14 22:36	GSM				
27-Jul-14 22:00	GSM				
27-Jul-14 21:59	GSM				
27-Jul-14 21:56	GSM				
27-Jul-14 20:13	GSM				
27-Jul-14 20:08	GSM				
27-Jul-14 20:03	GSM				

interception attack



3G security indicators

Clear logs		Refresh logs				
Date	Network type	Event	Authentication	Encryption	Remove	
07-Aug-14 19:26	3G					
07-Aug-14 19:16	3G					
Prev		Next				



Detail log

Date:07-Aug-14 19:16

Network type:3G

Network operator:FI elisa

Event:OUTGOING_CALL

_3G_INIT_SERV_REQ

Network operator uses uea1 algorithm for encryption.:

_3G_INIT_SERV_REQ

Network operator uses uea1 algorithm for encryption.:

_3G_INIT_AUTH_REQ

RANDOM Number: 7B 18 B3 3D D0 51 22 E6 E6 3E
CE 6E 8D 56 F8 8A

AUTN Number: 2B 80 D1 EE 06 09 00 00 E3 75 A7
76 90 56 8E 6F


Detecting silent SMS









- ◆ Type 0 messages
- ◆ Standard says mobiles must acknowledge receipt but may discard contents
- ◆ Mobiles do not display any notification to end users
- ◆ Useful for police or other illegal agencies
- ◆ HushSMS tool from @c0rnholio


Detecting silent SMS - Demo

- ◆ HushSMS allows
 - ★ Ping 3 (0-byte WAP Push)
 - ★ Ping 4 (Empty MMSN)
- ◆ Detects, alerts with a notification
- ◆ Option to turn on airplane mode
(not useful until you control the baseband)

Notifications Clear

 **Silent SMS Notification** 19:37
Alert- Silent SMS has been received. It seems suspicious activity based on type of SMS.

Date	Network type	Event	Authentication	Encryption	Remove
05-Aug-14 16:14	GSM				
05-Aug-14 16:10	GSM				

 Detail log

Date:05-Aug-14 19:37
Network type:GSM
Network operator:T-Mobile
Event:INCOMING_SILENT_SMS
SILENT_SMS
Silent SMS Sender number: 49 [REDACTED]
Time at which silent SMS received: 05-Aug-14 12:36:30

IMSI Catcher Detection

- ◆ Finding parameters to detect
- ◆ Need lots of data from different operators
- ◆ LAC or Cell id not enough

scanning first

jamming

downgrading

The basic features of NS-17-2 3G catcher are:

- Operation in 850, 900, 1700, 1900, 2100 3G bands;
- Automatically scanning and detecting parameters of all 3G networks;
- Detecting 3G phones and collecting their IMSI/IMEI identities in real time;
- Displaying phone model and name of network Provider;
- Measuring distance to all 3G phones with accuracy of less than 30 m;
- Jamming 3G selected networks in the working area;
- Forcing handsets to migrate to GSM mode. It makes possible interception of such phones by GSM semi/active and passive interception systems.

All software operations described in this document must be performed by organizations and companies only in accordance with national and international Laws.

Finding parameters

- ◆ System Information Type 3 messages
 - Layer 3 messages about GSM system configuration

```
123 7.284276000 127.0.0.1 127.0.0.1 GSMTAP 71 (CCCH) (RR) System Information Type 3
124 7.309716000 127.0.0.1 127.0.0.1 GSMTAP 71 (CCCH) (SS)
Mobile Country Code (MCC): India (Republic of) (404)
Mobile Network Code (MNC): Bharti Airtel Ltd., Maharashtra (90)
Location Area Code (LAC): 0x1011 (4113)
▽ Control Channel Description
1... .... = MSCR: MSC is Release '99 onwards (1)
.1.. .... = ATT: MSs in the cell shall apply IMSI attach and detach procedure (1)
..00 1... = BS_AG_BLKs_RES: 1
.... .000 = CCCH-CONF: 1 basic physical channel used for CCCH, not combined with SDCCHs (0)
.00. .... = CBQ3: Iu mode not supported (0)
.... .100 = BS-PA-MFRMS: 4
T3212: 40
▽ Cell Options (BCCH)
.1.. .... = PWRC: True
..01 .... = DTX (BCCH): The MSs shall use uplink discontinuous transmission (1)
.... 0100 = Radio Link Timeout: 20 (4)
▽ Cell Selection Parameters
011. .... = Cell Reselection Hysteresis: 3
...0 0000 = MS TXPWR MAX CCH: 0
```

Finding parameters

- ◆ Control Channel Description
 - ★ MSCR: shows current GSM network version
 - ★ 0 – MSCR release version 98 or older
 - ★ 1- MSC release version 99 or newer

	Telekom	O2	Vodafone	Play Network	BSNL	Idea	OpenBTS
MSCR	'99 onwards	'99 onwards	'99 onwards	'98 or older	'99 onwards	'99 onwards	'98 or older

Finding parameters

◆ Radio Link Timeout

- ★ Counter value to judge downlink failure
- ★ Counter decrease when there is error
- ★ When 0 radio link failure

	Telekom	O2	Vodafone	Play Network	BSNL	Idea	OpenBTS
MSCR	64	24	64	64	20	40	64

Finding parameters

- ◆ PWRC - power control indicator
- ◆ Data from various operators and openBTS

	Telekom	O2	Vodafone	Play Network	BSNL	Idea	OpenBTS
MSCR	Flase	True	False	Flase	True	False	False

Building a profile

- ◆ Tool collects such parameters
- ◆ Very seldom change (no change in a week)
- ◆ Build a profile per location : office-work-city
- ◆ Work in progress

SYS_INFO_3

Cell Identity: 01 41

Mobile Country Code: 42 F4

Mobile Network Code: 50

Location Area Code: 23 2D

MSCR: MSCR: MSC is Release '99 onwards

PWRC: True

Cell selection parameters: RXLEV-ACCESS-MIN: 05

Future work

- ◆ Source code will be released (without IMSI catcher)
- ◆ Support to other **possible** devices
- ◆ Data upload functionality (anonymous data)
- ◆ Building more profiles for IMSI catcher detection
- ◆ Collecting and sharing data



Thank you!