IMSI-Catch Me If You Can: IMSI-Catcher-Catchers

Adrian Dabrowski, Nicola Pianta, Thomas Klepp
Martin Mulazzani, Edgar Weippl

CS 598 AB Fall 2016
November 10
Presented by: Simon Kim

IMSI Catcher

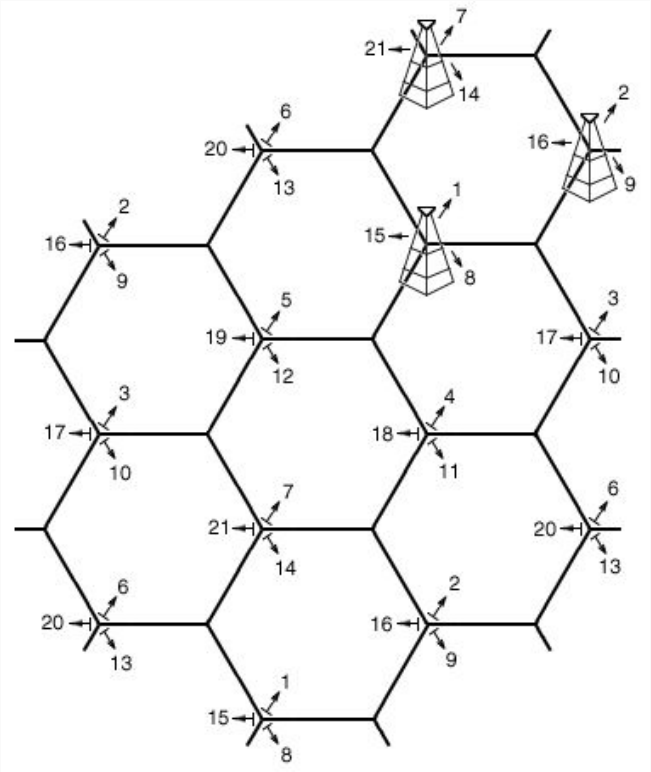
IMSI Catcher

- MITM fake base station
- Exploits GSM(2G)’s lack of mutual authentication
- Obtains device-network information from nearby phones
- Two modes:
  - Identification mode - retrieves information and sends the phone back to genuine network
  - Camping mode - captures data and forwards them to genuine network

https://www.hacking-lab.com/export/sites/www.hacking-lab.com/cases/4052-imsi-catcher/imsi.jpg

Cell Towers

- GSM cell identified by
  - MCC - country
  - MNC - network
  - LAC - location area
  - CI - cell id
- Neighbor list includes frequency and channel quality metrics



https://upload.wikimedia.org/wikipedia/en/5/57/CellTowersAtCorners.gif

Artifacts

- Unusual frequency
  - Unallocated channel (guard channel or reserved)
  - Advertised channel not in use
- Unusual cell ID
  - Cell ID from another region
- Changes in cell capabilities (e.g. GPRS or EDGE)
- Inconsistent network parameters (threshold, timeout values)

Artifacts (cont.)

- Channel noise resulting from RF jamming
  - To force location update/register
  - To force downgrading to GSM
- Absence of cipher
- Empty or inconsistent neighbor cell list
- Missing caller ID
- Short living cells

IMSI Catcher Catcher (ICC)

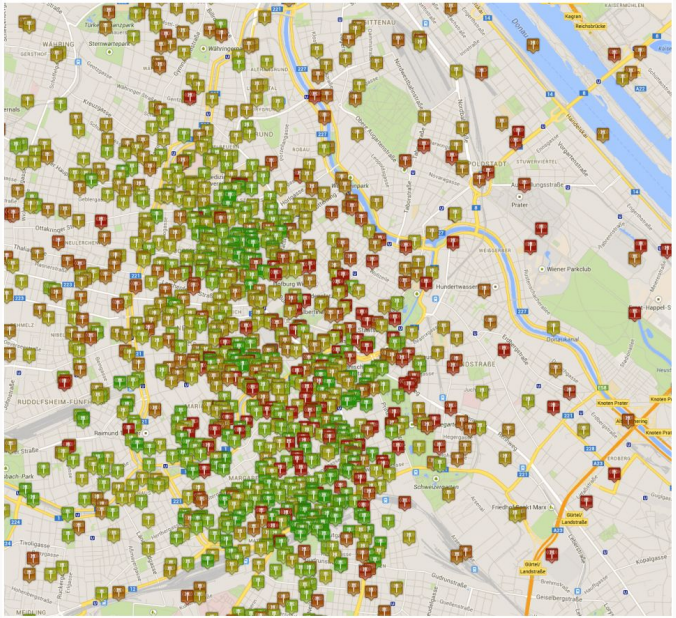
Features

- Simple, cheap, and easily deployable
- Collect and maintain its own cell ID database
- Detection based on the artifacts

IMSI Catcher Artifact	Detection Method
Unusual Cell ID	Cell database
Unusual cell location	
Unusual frequency usage	
Short living cells	
Unusual cell capabilities	
Guard channel usage	Band plan
Network parameters	Network fingerprinting
RF jamming	Watching noise levels
Disabled cipher	Read cipher indicator
Neighbor list manipulation	Cell DB & sanity check
Receive gain	sanity check
Missing caller ID, SMS	Periodic test calls

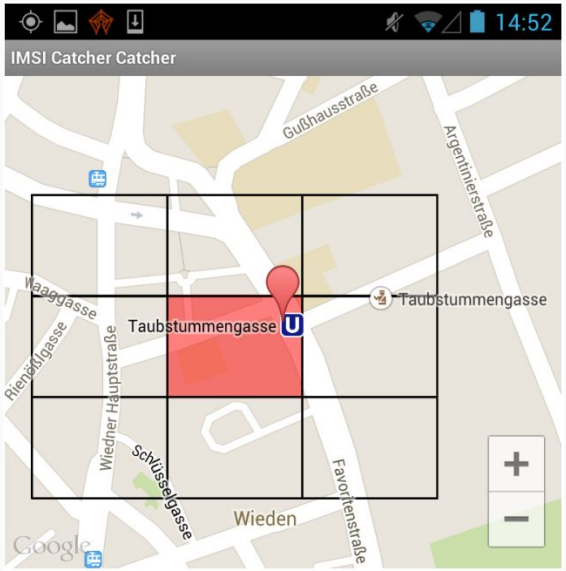
Approaches

- Based on geo-network topology correlation
- Stationary (sICC)
  - Constantly scans all frequency bands
  - Larger coverage (can form a network)
  - Good for detecting transient events
  - Features
    - Cell ID mapping
    - Frequency usage
    - Cell lifetime, capabilities, network parameters
    - Jamming



Approaches (cont.)

- Mobile (mICC)
  - Smartphone application that uses standard Android API
    - No rooting or jailbreak required
  - Uses built-in GPS receiver
    - Geographical correlation
    - Cell ID



Difficulties

- Limited access to cell network information (e.g. neighbor list)
- Support varies by manufacturers
- Short neighbor list (very limited view)
  - Each station could focus on a specific band to extend the view
  - Foreign SIM may be able to use multiple networks

Difficulties (cont.)

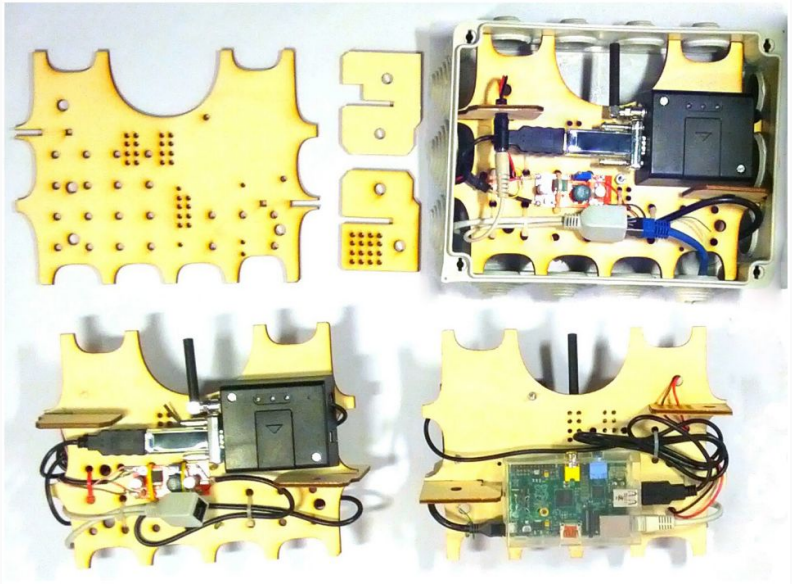
IMSI Catcher Artifact	Android API	iOS API‡
Unusual Cell ID	serving cell & neighbors†	serving cell only
Unusual cell location	yes	yes
Unusual frequency usage	no	no
Short living cells	yes	limited
Unusual cell capabilities	serving cell & neighbors†	indirect
Guard channel usage	no	no
Network parameters	no	no
RF jamming	limited	no
Disabled cipher	expected in future API [4]	no
Neighbor list manipulation	limited†	no
Receive gain	no	no
Missing caller ID, SMS	yes	yes

† Neighbor cells available via standard API, but not implemented in all phones.

‡ Only via iOS private API. See Section 6.2 on reasons why iOS is not considered in this paper.

Implementation - Stationary

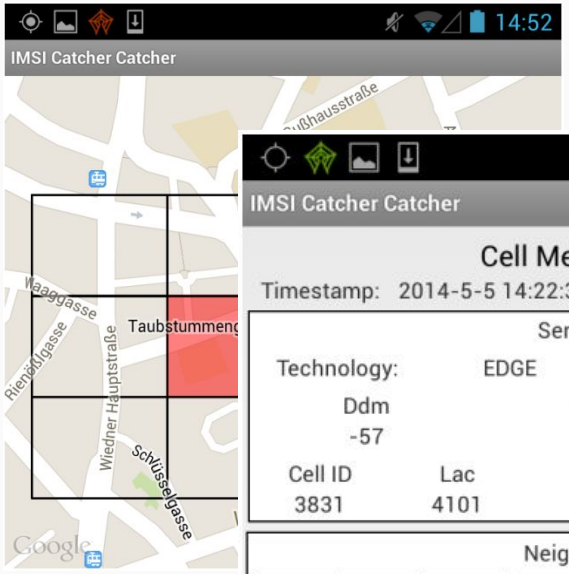
- Telit GT864, Raspberry Pi, Internet connection
- Data collected locally in sqlite3 database
  - Periodically uploaded to central server
- Total cost = € 200

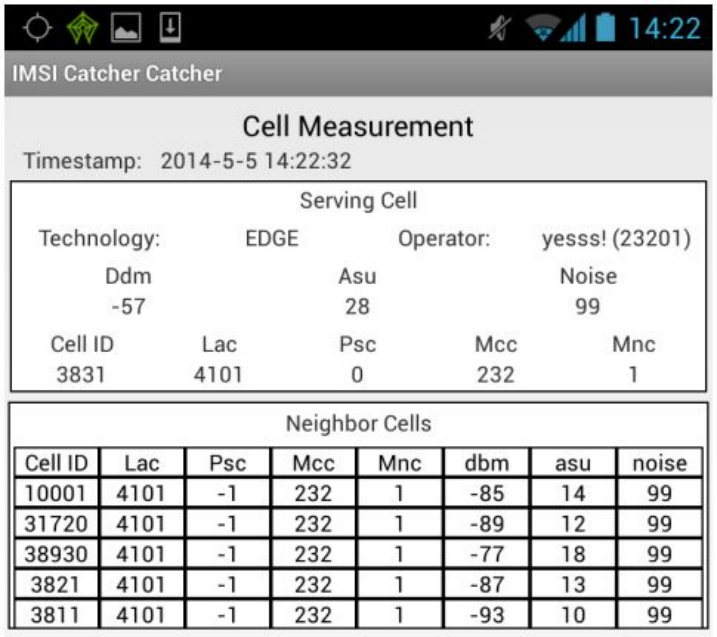


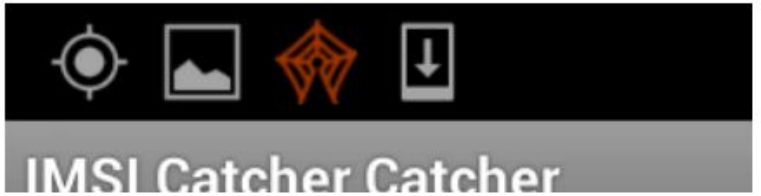
Implementation - Mobile

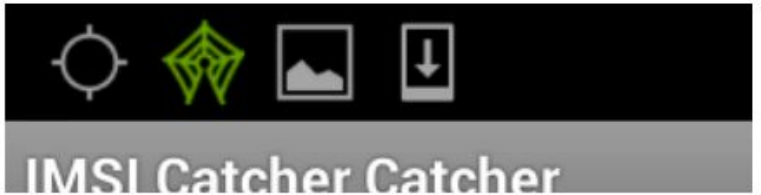
- Measurements triggered by PhoneStateListener.onCellInfoChanged() or 10 second timer
  - Detects redirection from/to another cell (IMSI catcher in identification mode)
- Measured by 150x100 rectangular geographical tiles
- Data stored in local sqlite3 database
- Tile ready for evaluation, only if all 9 tiles have valid information
- Tile obtains information if detected as serving or included in one of the neighbor lists

Implementation - Mobile (cont.)









Evaluation

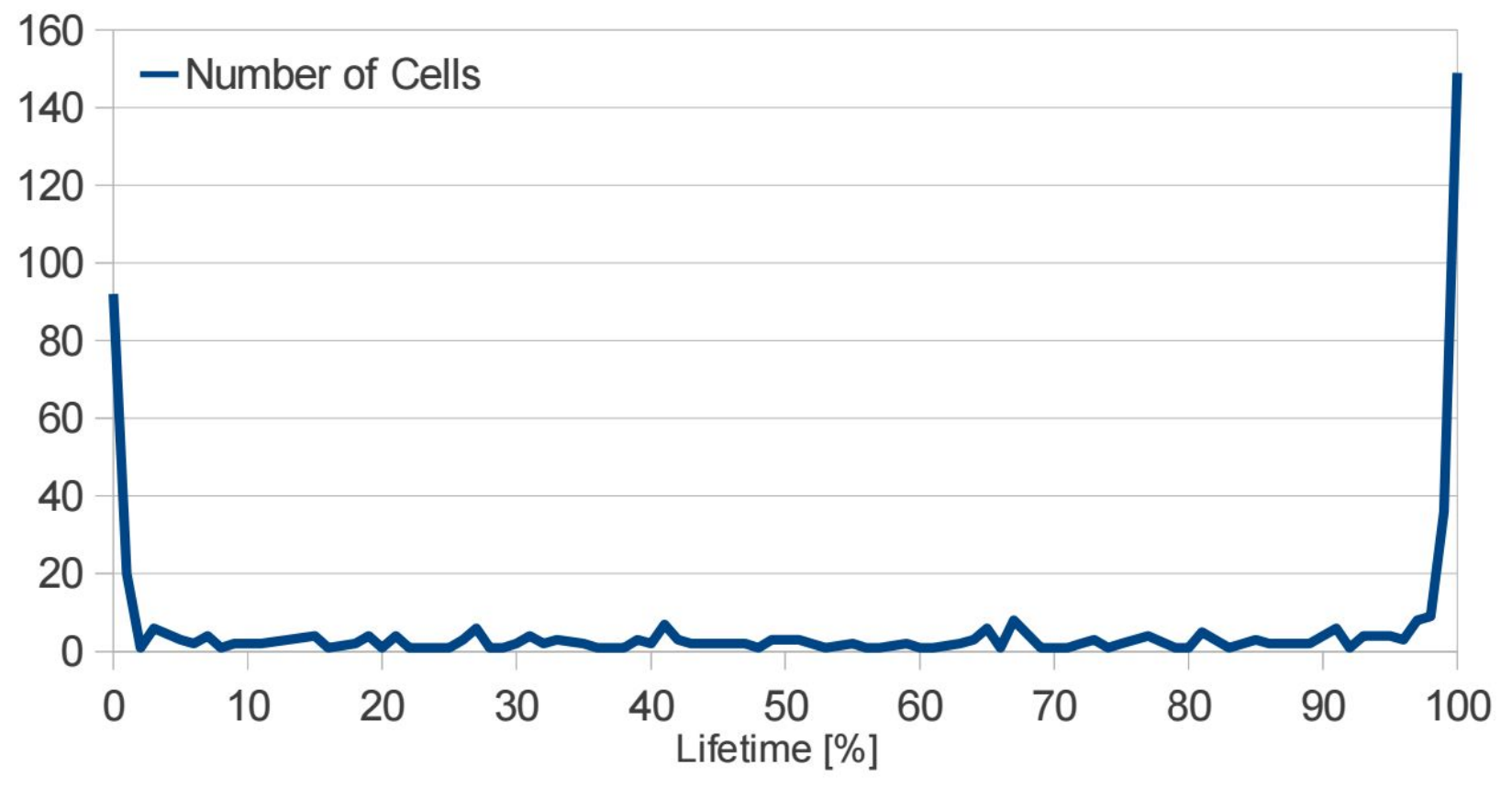
- Lab test - detecting an IMSI catcher in identification mode within a controlled environment
- Field test
  - Stationary - long-term data collection in Viennese city center
  - Mobile - data collection during an event in Vienna

Figure 5: Field test for all three GSM networks

Evaluation - Stationary

- Can sweep whole 900 and 1800 Mhz GSM and EGSM within 5-7 min
- Network parameters
  - Cells within the same network have same values for most information.
  - Values differ by each network operator
- Notable anomalies
  - Some cells operating outside of official range
  - Cells with valid MNC, LAC, CI but invalid NCC (network country code)

Cell ID lifetime throughout the experiment

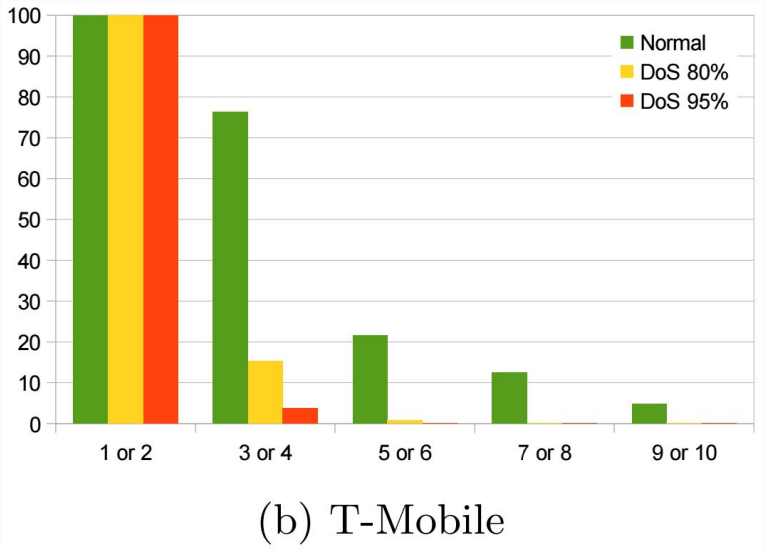


Future Work

- New stationary ICC prototype
  - Directly decoding the broadcast and control channels to gain more information for fingerprinting
  - Could allow detecting some DoS attacks
- Further studies on occasional excessive range caused by weather

Future Work (cont.)

- Detecting DoS attacks
  - Simulation shows that each network has different individual paging retry policy
  - The presence of DoS attack clearly affects the distribution.



(b) T-Mobile

Summary

- Survey of network level artifacts caused by IMSI catchers
- Concept of usable, customer-grade warning system
  - Available and implementable Detection methods by hardware
  - Intentionally excluded expensive protocol analyzers or complex self-built solution

Discussion

- Is 4G LTE doing any better at defending against IMSI catcher? Is ICC still useful for 4G LTE?
- Is it necessary to restrict access to cell network information? Is there any incentive for manufacturers to make them more accessible through API?
    - For example, serving cell or neighbor list became popular because companies found use cases for those information (coarse locating devices in combination with a geolocation cell ID databases)
- How can we make the proposed mICC app better?
    - For example, it doesn't provide large coverage like sICC