IMSI Catcher Detection Method for Cellular Networks

Hamad Alrashede, Riaz Ahmed Shaikh
Computer Science Department,
Faculty of Computing and Information Technology,
King Abdulaziz University
Jeddah, KSA
halrashede0001@stu.kau.edu.sa, rashaikh@kau.edu.sa

Abstract— **Mobile communications are not trustful as many people think about it. The IMSI catcher device is one of the most effective threats that can compromise the security of mobile communications. It is a radio device that acts as a fake cellular base station allowing near mobiles to join it instead of legitimate base stations. It uses a type of attack called man in the middle (MITM). The IMSI catcher can do almost everything after being connected to its victims, such as eavesdropping calls, intercepting SMS messages, locating phone's location and so many. It is widely used by government agencies legally to track criminals and terrorists, but nowadays it could be used by unauthorized individuals and criminal organizations for different purposes. Several of countermeasures against this threat are proposed by many researchers but most of them are reliant on real base station features to expose fake base stations. Those features are limited and could be easily imitated by IMSI catcher device. This paper presents a new IMSI catcher detection method, which relies on location area features for detection that makes it unique as compared to most of the existing schemes.**

Keywords- Fake base station; IMSI catcher; Mobile privacy; Mobile network security; Cell site simulator

I. INTRODUCTION

International Mobile Subscriber Identity (IMSI) is a unique number for the SIM (Subscriber Identity Module) card, it is given to the Client by the network operator. It contains 15 digit number used to identify the user device when it connects to any base station (mobile tower). The IMSI number includes three parts [1]:

a) 3-digit Mobile Country Code (MCC)
b) 2/3-digit Mobile Network Code (MNC)
c) 9/10-digit Mobile Subscriber Identity (MSI)

The IMSI catcher is a radio device designed with special features to catch the IMSI number and intercept mobile phone communications [1][2]. It can show itself as a fake cellular base station to exploit vulnerabilities in GSM networks and 4G/LTE networks. The IMSI catcher uses a famous technique called man-in-the-middle (MITM) attack.

It acts simultaneously as a fake mobile phone to the real base station and a fake base station to the real mobile phone [2].

When IMSI catcher device complete connection between mobile phone and base station it can do almost everything with its victims [3]. For example, it can eavesdrop on calls and record them, intercept SMS messages and redirect them, locate phone user's location, retrieve files from the target phone including photos, texts, turn on the microphone, the camera, other tools from the target phone and so many. There are different names for IMSI catcher such as StingRay, cell site simulator and cell site emulator [4]. Also, there are many types differ in size, price, and functionality. In the beginning, those devices were exclusively used by governments and law enforcing agencies to track criminals and terrorists. Nowadays, these devices are commercially available which means they can be used by unauthorized people such as terrorists, criminal gangs, drug dealers and even individuals for different purposes. The IMSI catcher devices are sold online by some web sites [20] and can be easily built and programmed by using available hardware and software with clear manuals [5][6]. Several countermeasures against this threat have been presented in various articles such as [3]4][9][10][11][12][15]. Most of the existing solutions depend on mobile tower features to distinguish real base stations from fake ones. The mobile tower features are limited and can be simply simulated by IMSI catcher devices. This research focuses on a new method that relies on entire location area features to detect and address IMSI catcher presence in a particular location area.

The contributions of this research include the following:

1. Focusing on location area features instead of the base station features to mitigate IMSI catcher threats.
2. Presenting a new concept of cell fingerprint (cellprint) for each location area in the cellular network and use that for detecting and preventing IMSI catcher threat.
3. Improving the AKA authentication algorithm by integrating it with the new proposed cellprint algorithms to authenticate base stations before sending the IMSI number.

978-1-7281-0108-8/19/$31.00 ©2019 IEEE

4. Conducting a qualitative comparison between the proposed scheme with some other related schemes.

The rest of this paper is organized as follows: the next section covers a literature review to show the main concepts of GSM networks and its architecture, IMSI catcher devices and their features. The third section describes the proposed scheme in detail. The fourth section includes theoretical analysis. Conclusion and future work are presented in section five.

II. Literature Review

GSM stands for Global System for Mobile Communication. It is the widest telecommunication network technology used across all the world. Billions of subscribers are using the GSM networks as well used by most mobile network operators. GSM network has some security procedures to protect communications between the user side and network, but it is also having some vulnerabilities that have been exploited and demonstrated by different security teams and researchers.

The GSM network architecture is divided into the following four main components:

1. Mobile Station (MS): It is a mobile phone or a device with a removable SIM card, this card has a unique IMSI number. The mobile device itself also has a unique number called IMEI (International Mobile Equipment Identity), this number helps the network operator to block network services from stolen phones and devices. The SIM card also contains 3 security-related things, (A3) the authentication algorithm, (A8) the key generation algorithm and (Ki) the long-term secret key [2][3].
2. Base station (BS): It is also called cell towers and mobile towers. Those towers communicate directly with mobile phones (Mobile Stations) and each one of them manages a particular cell in the cellular network [2][3].
3. Base Station Controller (BSC): Each one of those controllers manages some of the cell towers. When mobile phones move among cells, the location update is required. This operation is managed by the Base Station Controller and (MSC) mobile switching center [2][3].
4. Mobile Switching Center (MSC): It is the main core of GSM networks and has four database servers to control the different operations inside the network.
   a. Home Location Register (HLR): It stores all information about subscribers and their IMSI numbers.
   b. Visitor Location Register (VLR): It stores some information about subscribers and their authorities.
   c. Authentication Center (AuC): It stores the long-term secret key (Ki)for each SIM card in the network and has same algorithms that used inside SIM card (A3) algorithm and (A8) algorithm.
   d. Equipment Identity Register (EIR): It stores IMEI numbers for all stolen phones or devices to block them from accessing the network services [2][3].

When a mobile station (MS) try to connect to a base station (BS), it must authenticate itself to the base station but the vice versa is not required. This is the vulnerability of GSM networks used by IMSI catcher devices to exploit network communications [7][9].

IMSI Catcher Device is a radio device that can show itself as a cellular base station (BS) to exploit and hack vulnerabilities in GSM networks and intercept mobile phone calls and traffic in its vicinity. It is also called cell site emulator, Stingray or cell site simulator. There are various types of IMSI catcher devices, and they are different in their sizes and features [7].

The GSM networks are vulnerable to different types of attacks including cracking encryption, passive interception attack, and active interception attack [8]. The IMSI catcher attack is classified as an active attack [1]. It uses a famous technique called Man-In-The-Middle (MITM) attack, it acts simultaneously as a fake mobile phone to the real base station and as a fake base station to the real mobile phone as shown in Fig. 1.

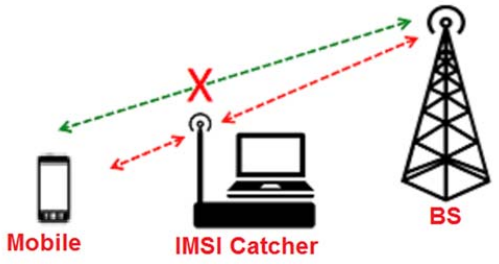


Figure 1. IMSI Catcher Attack (MITM)

IMSI catcher device can catch the IMSI numbers sent by mobile phones in its area and intercept the data traffic, that is why it is called IMSI catcher [13]. The IMSI number is used to identify any mobile phone on the network, StingRay is one of the most famous IMSI catcher devices [14]. It is sold by a private company called (Harris Corporation) to several governmental agencies around the world [16][17].

III. Proposed Idea

A. Cellular Location Area

The cellular network is divided into several location areas, each location area has some base stations (mobile towers) (radio cells) to serve a particular area. Figure 2 shows an example of a location area and its cells.

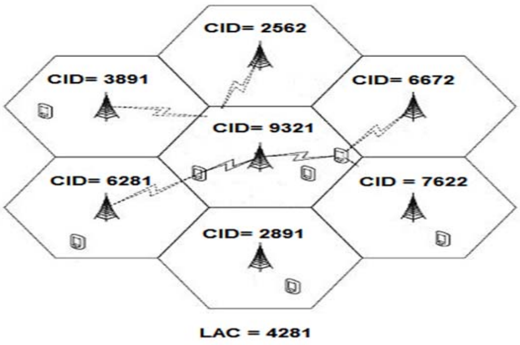
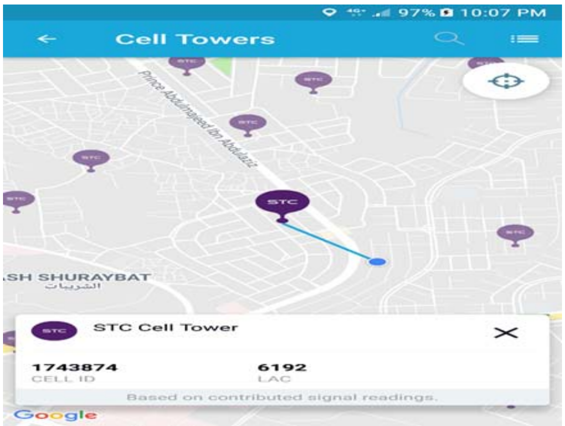


Figure 2. Cellular Network Location Area and its Cells

This location area is one of many location areas that connected to represent the cellular network. Each location area has its own location area code LAC different from other LACs in the network. Each base station (mobile tower) inside this location area has also a unique ID number (cell id) CID.

B. *Representing LAC and CID*

The LAC and the CID are publicly available and could be represented by different ways such as using some network monitor apps e.g. OpenSignal app, Cellidfinder app [18][19]etc., or using the service mode (test mode) of the mobile by calling *#0011# which shows some interesting information about the current network the mobile connected with. The next Fig. 3 is a screenshot that has been taken by a smartphone using OpenSignal app, it shows the LAC where the smartphone was and the CID for the connected base station.



STC Cell Tower

1743874 CELL ID

6192 LAC

Based on contributed signal readings.

Figure 3. LAC and Cell ID as Shown on OpenSignal App

C. *Assumptions and System Model*

The proposed solution depends on finding a fingerprint (cellprint) for each location area in the cellular network and use that to identify the location area and detect any intruder inside it before establishing any connection with any mobile tower in that area. Many of the previous articles proposed to use features of the base station as parameters to differentiate between real mobile stations and fake ones. However, those parameters could be simply imitated by IMSI catcher device, therefore it is not a practical way to use only the features of the mobile tower for detection. The proposed solution assumes that using the features of the whole location area which contains numerous base stations to build a unique cellprint for each location area. It will make the mission so difficult for IMSI catcher device to avoid detection. There is more than one way to build such as cellprint, the next section explains that in details.

D. *CellPrint Generation Algorithms*

This section describes the two proposed cellprint generation algorithms:

1. CID-based cellprint generation algorithm
2. The location-based cellprint generation algorithm

1) *CID-based cellprint generation algorithm*

The cellrprint could be generated by using the summation of all CIDs numbers for each location area. The result of this summation could be hashed and saved. So, when IMSI catcher device includes itself to a particular area the cellprint for that area will change from the original one. This allows the mobile user and the network operator to detect and address the presence of IMSI catcher devices in that area by cross check the cellprint. For example, the cellprint of the previous location area in figure 1 which has the LAC 4281 is the summation of the CIDs numbers in that area.

Equation 1. Calculating Cell IDs for Current LAC

$$= \sum \text{Cell IDs (CIDs)}$$

$$= 2562 + 6672 + 7622 + 2891 + 6281 + 3891 + 9321 = \mathbf{39240}$$

This calculation could be done in different ways, from the user side such as a special app on the platform. Or by the network operator side who monitors the cellprint for each location area and inform the mobile users about any malicious presence in that area. The formal description of CID-based cellprint generation algorithm is defined in Algorithm 1.

Algorithm 1: CID-based cellprint generation algorithm

```
Start
Read the current LAC
 For each BS belongs to current LAC (has same LAC)
   R = ∑ CIDs
cellprint = R  # the value could be hashed
End
```

Detecting and Addressing IMSI Catcher Presence

If the calculation result for any location area is higher than the cellprint this means there is an intruder inside the area, and the ID number for this intruder is the result of the new summation minus the cellprint for that area. For example, when IMSI catcher device includes itself to the previous location area it has to use a CID to imitate real base stations inside that area Fig. 4.

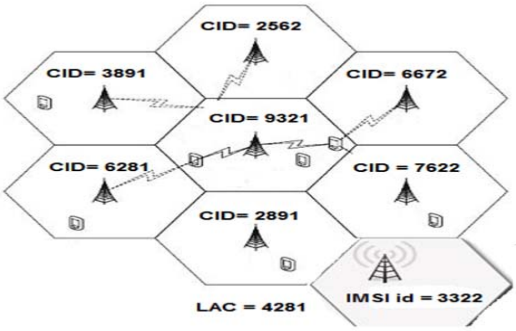


Figure 4. Cellular Network Location Area (LAC) with IMSI Catcher

The cellprint of this location (LAC 4281) is already known which is 39240 when a mobile user initiates a connection or updates its location to connect to another location area it has to make a new calculation for this area and compares it with the original cellprint for that area. The cellprint for the location area LAC 4281 with IMSI catcher included is

$= \sum$ Cell IDs (CIDs)

= 2562 + 6672 + 7622 + 2891 + 6281 + 3891 + 9321 + 3322 = **42562**

42562 (new summation) $\neq$ 39240 cellprint which means there is an intruder inside the location area (LAC 4281). The intruder ID number can be addressed and exposed by subtraction.

New summation – cellprint = 42562 – 39240 = 3322 (the intruder ID)

The tower which has the ID number 3322 is a fake base station, therefore, it will be blocked and added to the blacklist to avoid connection with it.

2) *Location-based cellprint generation algorithm*

Another way to represent the cellprint is by using the distance value between the base stations for each location area to form a unique shape that identifies and extinguish the location area from others. So, when IMSI catcher device includes itself to the location area the shape of the original location area will be different from the shape with IMSI catcher device included, Fig. 5 and Fig. 6.

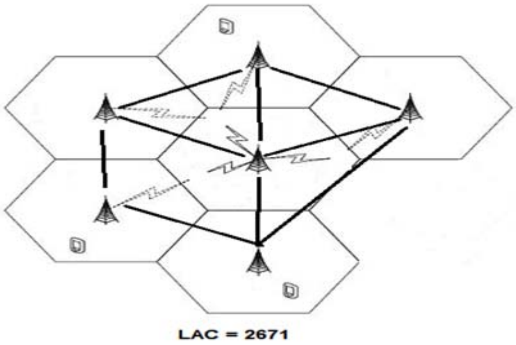


Figure 5. Original Shape of Location Area

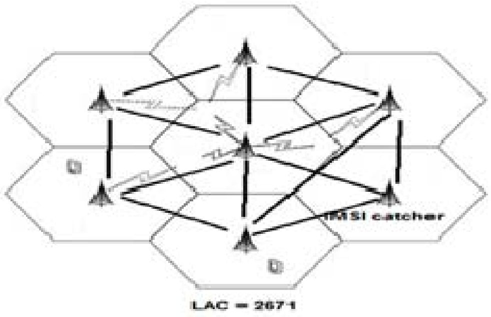


Figure 6. Location Area Shape with IMSI Catcher

When a mobile user initiates a new connection or updates its location area, it must compare the shape of the new location area with the cellprint for that location area. The distance between mobile towers inside location areas is well known by the network operator and could be used for this purpose. Well known graph algorithms such as minimum spanning tree (MST) can help to build the cellprint for each LAC. The formal description of location-based cellprint generation algorithm is defined in Algorithm 2.

Algorithm 2: Location-based cellprint generation algorithm

```
Start
Read the current LAC
For each BS belongs to current LAC (has same LAC)
    Find the minimum spanning tree (MST)
    R = The length of MST
cellprint = R  # the value could be hashed
End
```

E. *Proposed Solution Integrated With AKA*

AKA authentication is the current method used by GSM networks to authenticate the mobile station to the base station but not the vice versa [2]. Integrating the proposed solution with AKA algorithm [7] gives the ability to apply the vice versa, the mobile station authenticates the base station before sending it's IMSI and before establishing any connection with it. Additionally, the proposed method can also identify the intruder ID in the location area. The formal description of the proposed CID-based cellprint generation algorithm with AKA Authentication mechanism is given in Algorithm 3.

Algorithm 3: Proposed Algorithm with AKA

```
Start MS (switch on) or update the location area
MS read LAC and cellprint for the current location area (publicly available)
MS calculates the cell id for all BSs in this area and the result saved in R
        R = $\sum$ CIDs
IF R = = cellprint THEN    # (MS compares between R and cellprint)
        MS sends its IMSI to BS
        BS sends the IMSI to authentication center AuC
        AuC generates the authentication vectors (AV) by using RAND and Ki
        SRES = A3(RAND, Ki)
        Kc = A8(RAND, Ki)
        AV (SRES, Kc, RAND) sends back to the BS
        BS sends the RAND to MS
        MS calculates the challenge response by using the RAND received from BS
        RES = A3(RAND, Ki)
        MS sends RES back to BS
        IF RES = = SRES THEN    # RES received from MS and SRES received from AuC
        connection successful
        ELSE
        connection failure
        ENDIF
ELSE
        Intruder id (IID) = R – cellprint
        ALERT "there is an intruder (Intruder id= IID) in this LAC"
        Reject Connection Request
ENDIF
```

IV. THEORETICAL ANALYSIS

A. *Delay Analysis*

To analyze the complexity of the proposed solution, we have focused on time complexity as the space complexity will not be impacted when applying the proposed scheme. The time complexity of the AKA authentication algorithm is linked to the number of messages between MS, BS, and AuC. In the normal case to accomplish authentication operation, the messages between those parts are five. Analyzation will be on authentication delay, which is the time between MS to requests connection with the cellular network until the completion of registration. When assume that the delay time between MS and BS is ($DT_{\text{MS to BS}}$), the delay time from BS to MS is ($DT_{\text{BS to MS}}$), the delay time from BS to AuC is ($DT_{\text{BS to AuC}}$) and the delay time from AuC to BS is ($DT_{\text{AuC to BS}}$). Then the delay time of authentication operation will be represented as the next.

Equation 2.

$$DA = 3 * DT_{\text{MS to BS}} + 2 * DT_{\text{BS to AuC}}$$

This is the delay time to complete the connection for one mobile station MS during the AKA authentication steps.

If there are n MS, the delay time to complete the connection for all of them is

$$DA = (3 * DT_{\text{MS to BS}} + 2 * DT_{\text{BS to AuC}}) * (n)$$

So, the worst case to accomplish authentication for n MS is **O(*n*)**.

The next Fig. 7 are showing a graph that generated in Matlab to show the behavior of authentication delay equation in milliseconds when applying the proposed method.

$$DA = 3 * DT_{\text{MS to BS}} + 2 * DT_{\text{BS to AuC}},$$

in which the values of ($DT_{\text{MS to BS}}$) and ($DT_{\text{BS to AuC}}$) are selected randomly between 1 and 100, the size of the dataset is 100.

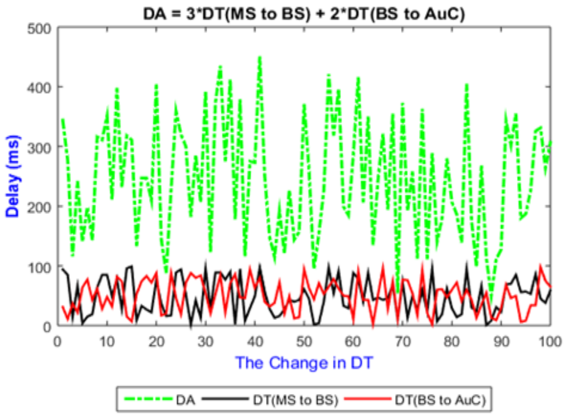


Figure 7. Authentication Delay Equation Graph 2D

B. Complexity Analysis

In addition to the previous, the proposed solution needs to calculate CID for BSs and compares the result R with cellprint and expose the intruder id (IID) if exist (Algorithm 3, steps 21-24), before continuing AKA authentication steps.

Equation 1. Calculating Cell ID for Current LAC

$$R = \Sigma \text{ CIDs}$$

Equation 2. Comparing R with Original cellprint for Current LAC

$$R == \text{cellprint?}$$

Equation 3. Locating IMSI Catcher in Current LAC

$$IID = R – \text{cellprint}$$

The complexity of the equations above is always constant, the constant values are always ignored in term of studying algorithm complexity, which means the complexity of our proposed solution integrated with AKA authentication will stay as is O(n), that means we could improve the security aspects without affecting the performance side.

C. Discussion

From the previous illustrations, we can notice that when using information and features of whole cell towers inside the cellular location area, a unique cellprint can be built. Using this cellprint for authentication will make the mission very difficult for IMSI catcher to evade detection when it becomes a part of a specific location area (LAC). To build such as cellprint, two convenient methods were mentioned. The first one is CID-based cellprint, depends on the calculation of cell IDs inside the location area, the result of this calculation represents the cellprint for that area. This value could be saved and retrieved from base station controller (BSC) anytime as the BSC has the control of all base stations BSs (cell towers) included in its location area, and in case of installing new base station or remove it from the location area this value will be updated. The second method is Location-based cellprint, depends on the distance between the towers inside the location area. The distance between towers is well known by the network operator, therefore it can be used for this purpose. There are different common graph algorithms can help to build the cellprint such as minimum spanning tree algorithm (MST). This method might need more computation than the first one, but it is still easy to be applied. Using other parameters of the location area to build other cellprints is also possible, the idea is to depend on some location area parameters instead of depending on cell tower parameters as proposed by many previous articles. It is easy for IMSI catcher device to imitate one or some parameters of a cell tower but very difficult to do so with location area level. This concept could be very helpful as we are heading towards 5G technology and new infrastructures will be made and updated.

The limitation of the proposed solution is that, it does not protect against passive attack, as well the current AKA authentication algorithm which is widely used all around the world needs to be updated.

D. Qualitative Comparison

In order to make a comparison between the proposed scheme and other related schemes, some security aspects will be considered, such as mutual authentication (S1), protection of IMSI privacy (S2), detection of IMSI catcher presence (S3), exposing IMSI catcher ID (S4), protection against passive attack (S5), protection against MITM attack (S6) and the last aspect will be efficiency (E) which depends on how many changes in the network architecture are needed and what is the corresponding security improvements for these changes, when change is low with high-security benefit, the efficiency will be high, when change is high or medium with low-security benefit, the efficiency will be low and the other probabilities will be considered as medium efficiency. The following table is showing the result of this comparison.

Table 1. A comparison between the proposed scheme and other schemes

REF	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**E**
Engelstad, *et al.* [3]	NO	NO	YES	NO	NO	NO	LOW
Steig, *et al.* [4]	NO	NO	YES	NO	NO	YES	MID
T. Van Do, *et al.* [11]	NO	NO	YES	NO	NO	NO	LOW
Dabrowski, *et al.* [15]	NO	NO	YES	NO	NO	YES	MID
Ginzboorg, *et al.* [16]	NO	YES	YES	NO	YES	YES	HIGH
Ramadan, *et al.* [21]	YES	YES	YES	NO	NO	YES	HIGH
Proposed Scheme	YES	YES	YES	YES	NO	YES	HIGH

V. Conclusion and Future Work

In this research a new method is proposed that can help to detect and prevent IMSI catcher threat. The proposed solution is different from previous works as it depends on location area features instead of base station features. A new concept of cellprint was introduced to distinguish each location area from others, new algorithms were mentioned to generate such as cellprints. IMSI catcher device can easily imitate one or more features of the base station but the mission is very difficult if not impossible when dealing with features and parameters of whole location area. The proposed solution can help in more than one security aspects such as mutual authentication between the network and mobile user before sending IMSI number, allocating and exposing the intruder ID, preventing and isolating the malicious intruders.

In future work, simulations and experiments will be conducted on this theoretical study. The proposed scheme will be extensively simulated and tested either by having some support of local cellular network operators or purchasing some related open source hardware and software to practically accomplish more results and assessments.

VI. References

[1] Cattaneo, G., De Maio, G., Faruolo, P. and Petrillo, U.F., 2013, March. A review of security attacks on the GSM standard. In Information and Communication Technology-EurAsia Conference (pp. 507-512). Springer, Berlin, Heidelberg.

[2] Park, S., Shaik, A., Borgaonkar, R., Martin, A. and Seifert, J.P., 2017, August. Whitestingray: Evaluating IMSI catchers detection applications. In USENIX Workshop on Offensive Technologies (WOOT). USENIX Association.

[3] Engelstad, P., Feng, B. and van Do, T., 2016, August. Strengthening mobile network security using machine learning. In International Conference on Mobile Web and Information Systems (pp. 173-183). Springer International Publishing.

[4] Steig, S., Aarnes, A., Van Do, T. and Nguyen, H.T., 2016, September. A Network Based IMSI Catcher Detection. In IT Convergence and Security (ICITCS), 2016 6th International Conference on (pp. 1-6). IEEE.

[5] Mjølsnes, S.F. and Olimid, R.F., 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. arXiv preprint arXiv:1702.04434.

[6] Suraev, M., 2014, September. Implementing an Affordable and Effective GSM IMSI Catcher with 3G Authentication. In International Conference on Security and Privacy in Communication Systems (pp. 239-256). Springer, Cham.

[7] Arapinis, M., Mancini, L.I., Ritter, E. and Ryan, M.D., 2017. Analysis of privacy in mobile telephony systems. International Journal of Information Security, 16(5), pp.491-523.

[8] Ney, P., Smith, I., Cadamuro, G. and Kohno, T., 2017. SeaGlass: enabling city-wide IMSI-catcher detection. Proceedings on Privacy Enhancing Technologies, 2017(3), pp.39-56.

[9] Li, Z., Wang, W., Wilson, C., Chen, J., Qian, C., Jung, T., Zhang, L., Liu, K., Li, X. and Liu, Y., 2017, March. Fbs-radar: Uncovering fake base stations at scale in the wild. NDSS.

[10] Gunyel, M., Bayraktar, I., Koyuncu, O. and Gorkemli, B., ArgelaYazilimveBilisimTeknolojileri San. ve Tic. AS, 2017. Statistical system and method for catching a man-in-the-middle attack in 3G networks. U.S. Patent 9,628,994.

[11] van Do, T., Nguyen, H.T. and Momchil, N., 2015, September. Detecting IMSI-catcher using soft computing. In International Conference on Soft Computing in Data Science (pp. 129-140). Springer, Singapore.

[12] Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M. and Weippl, E., 2014, December. IMSI-catch me if you can: IMSI-catcher-catchers. In Proceedings of the 30th annual computer security applications Conference (pp. 246-255). ACM.

[13] Song, Y., Hu, X. and Lan, Z., 2011, November. The GSM/UMTS phone number catcher. In Multimedia Information Networking and Security (MINES), 2011 Third International Conference on (pp. 520-523). IEEE.

[14] Hadžialić, M., Škrbić, M., Huseinović, K., Kočan, I., Mušović, J., Hebibović, A. and Kasumagić, L., 2014, November. An approach to analyze security of GSM network. In Telecommunications Forum Telfor (TELFOR), 2014 22nd (pp. 99-102). IEEE.

[15] Dabrowski, A., Petzl, G. and Weippl, E.R., 2016, September. The messenger shoots back: Network operator based IMSI catcher detection. In International Symposium on Research in Attacks, Intrusions, and Defenses (pp. 279-302). Springer International Publishing.

[16] Ginzboorg, P. and Niemi, V., 2016, June. Privacy of the long-term identities in cellular networks. In Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications (pp. 167-175). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[17] Norrman, K., Näslund, M. and Dubrova, E., 2016, June. Protecting IMSI and User Privacy in 5G Networks. In Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications (pp. 159-166). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[18] OpenSignal App. [Online]. Available: https://opensignal.com/apps

[19] CellID Finder. [Online]. Available: https://cellidfinder.com/

[20] IMSI Catcher device. [online]. Available: https://www.alibaba.com/product-detail/Imsi-catcher-96-port-gsm-cdma_60552886820.html

[21] Ramadan, M., Li, F., Xu, C., Mohamed, A., Abdalla, H. and Ali, A.A., 2016. User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System. IJ Network Security, 18(4), pp.769-781.