Anatomy of Commercial IMSI Catchers and Detectors

Shinjo Park
Technische Universität Berlin
pshinjo@sect.tu-berlin.de

Altaf Shaik
Technische Universität Berlin
altaf329@sect.tu-berlin.de

Ravishankar Borgaonkar
SINTEF Digital
ravi.borgaonkar@sintef.no

Jean-Pierre Seifert
Technische Universität Berlin
jpseifert@sect.tu-berlin.de

ABSTRACT

IMSI catchers threaten the privacy of mobile phone users by identifying and tracking them. Commercial IMSI catcher products exploit vulnerabilities in cellular network security standards to lure nearby mobile devices. Commercial IMSI catcher's technical capabilities and operational details are still kept as a secret and unclearly presented due to the lack of access to these products from the research perspective.

On the other hand, there are several solutions to detect such IMSI catchers to protect the privacy of mobile subscribers. However, detecting IMSI catchers effectively on commercial smartphones is still a challenge.

In this paper, we present a systematic study of IMSI catchers, especially commercially available ones. Starting from publicly available product brochures, we analyze information from the international patent databases, attacking techniques used by them and vulnerabilities exploited in cellular networks (2G, 3G, and 4G). To this end, we survey IMSI catcher detection techniques and their limitations. Finally, we provide insights that we believe help guide the development of more effective and efficient IMSI catcher detection techniques.

CCS CONCEPTS

• **General and reference → Surveys and overviews**; • **Security and privacy → Mobile and wireless security**; *Mobile platform security*; • **Networks → Mobile networks**.

KEYWORDS

IMSI Catcher, base station, detection, StingRay, cellular network

ACM Reference Format:
Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. 2019. Anatomy of Commercial IMSI Catchers and Detectors. In *18th Workshop on Privacy in the Electronic Society (WPES '19), November 11, 2019, London, UK*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3338498.3358649

1 INTRODUCTION

IMSI catcher is a device to identify and track cellular phone subscribers, traced back to the 1990s with devices such as StingRay from Harris Corporation [53] and GA 900 from Rohde & Schwarz [41]. This is achieved by locating the presence of permanent cellular identities such as International Mobile Subscriber Identity (IMSI) tied to the subscriber's SIM card [94], and International Mobile Equipment Identity (IMEI) tied to the mobile device. While it was considered as an expensive device particularly used by the intelligence agencies and cybercriminals, the wider availability of software defined radio (SDR) and free open source software tools [48, 74] have reduced the cost to build such a device [64, 98], therefore potentially increasing the availability of the IMSI catcher for malicious adversaries. The 5G networks provide protection against such IMSI catcher devices [11], however, downgrading attacks (to force subscriber in using 4G, 3G or 2G networks) are still possible in 5G as demonstrated by Shaik et al. [88] Therefore, IMSI catcher devices may be a potential threat in 5G era as well due to support to the legacy cellular networks.

On the other hand, to combat against IMSI catchers, several types of IMSI catcher detection methods have been proposed, including smartphone app-based [49, 85, 91, 95], dedicated sensor networks [51, 69, 99], network operator assisted [29, 92] and correlation with other information sources [34, 35, 60]. These IMSI catcher detectors (ICDs hereafter) mainly operate by gathering cellular information, analyzing them for anomalies and warning the user/operator about the presence of an IMSI catcher.

However, commercial IMSI catcher's technical capabilities and attacking techniques are still considered as a confidential information to the research community due to the lack of access to such devices. Hence, vulnerabilities exploited by commercial IMSI catchers are unclear and consequently, and the effectiveness of IMSI catcher detection solutions may not be reliable in practice.

In this paper, we systematize the technical capabilities and innerworkings of commercial IMSI catchers by analyzing their product brochures and related patent databases. In particular, we analyze configurations and exploitation techniques used in the commercial IMSI catcher products. Further, we perform a survey on IMSI catcher detection methodologies proposed by various research studies and commercial products. The mapping of inner workings of commercial IMSI catchers and a survey of IMSI catcher detection methods enable us to uncover open research questions and challenges for the development of effective strategies.

WPES '19, November 11, 2019, London, United Kingdom
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6830-8/19/11...$15.00
https://doi.org/10.1145/3338498.3358649

Contribution of this paper is summarized as follows:

- We analyze 20 commercial IMSI catchers' product catalogs and 5 related patents to understand their specifications, attacking methods, and type of vulnerabilities in the cellular network standards. The information is correlated with academic publications which discusses about IMSI catcher's operating principles.
- We survey and evaluate multiple ICD's methods including app, sensor, and network-based, comparing their advantages and disadvantages. Evaluation is not only limited to free smartphone apps, but also extended to commercial solutions like dedicated smartphones and sensors.
- Mapping knowledge gained from inner workings on commercial IMSI catchers and their detection methods, we identify the limitations of the state-of-the-art IMSI catcher detection and discuss novel strategies, methods and techniques to improve the detection.

Organization. In section 2, we start from background knowledge for understanding the cellular network and the IMSI catcher's operation. We introduce our analysis on IMSI catcher's capabilities based on the analysis of the materials, w.r.t. 3GPP cellular standards in section 3, followed by evaluation of current ICD solutions in section 4. Based on our analysis, we propose a new set of requirements for future generation ICD system in section 5. Our findings are concluded in section 6.

2 BACKGROUND

To understand the operation of IMSI catchers and their possible detection methods, we begin by an introduction of a generalized cellular network architecture covering 2G, 3G, and 4G network. In particular, we focus on the essentials required to understand IMSI catcher operations and how they could be detected. We then discuss the existing works related to our research.

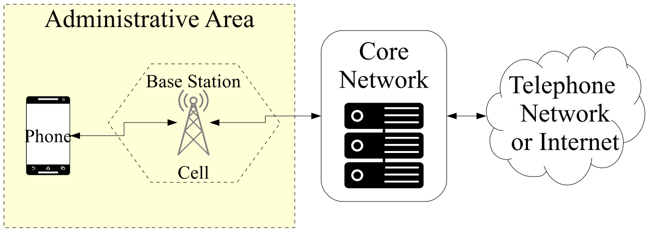


Figure 1: Simplified structure of the cellular network.

2.1 Initial Registration Procedure

Figure 1 presents a generalized cellular network architecture. The main entities in this architecture are core network, base station, and a phone. A cellular network divides a geographical location into several *administrative areas* which are further divided into cells. A base station manages a cell or a group of cells, and offers call/data services to the phones.

A base station periodically advertises the network information which the base station belongs to in the form of *System Information Block* (SIB) messages. SIBs mainly comprises of cell and administrative area identifiers, Mobile Country Code (MCC), and Mobile Network Code (MNC). It also contains the radio channel information required for the phones to connect to the network. A phone with a SIM card registers with the network and receives access to call/SMS/data services. A phone is identified with an IMEI and a SIM with an IMSI. When a phone (with a valid SIM card) is powered on, it performs a radio scan of the cellular frequencies and decodes the SIB messages from the surrounding base stations. This enables the phone to identify its home network (MCC and MNC) and initiate a registration procedure. By the protocol design, the phone always prefers to connect with the base station that offers the highest received power.

A core network controls a set of base stations located in multiple administrative areas and is responsible for the mobility management of the phones. In particular, registration, authentication, and security of the phones are supervised by the core network. It is also responsible for interconnecting the cellular network with the Internet and the public telephone network.

Upon receiving a registration request – technically referred as *Attach Request* in 4G, *Location Updating Request* and *Routing Area Update Request* for 2G and 3G's CS and PS domain respectively, the core network requests the phone for its IMSI. After validating the IMSI, the core network launches an authentication procedure. While authentication is optional in a 2G network, it is mandatory in 3G and later. The authentication is based on a shared secret key between the SIM card and the operator. In 2G only the network authenticates the phone (one-way), while in 3G and 4G both the network and the phone authenticate each other (mutual).

After successful authentication, the core network activates security protection for the signaling message and data exchange. In 2G, encryption is optional, and there is no integrity protection of the signaling messages. In 3G and 4G, while mandatory integrity protection is introduced, encryption still remains optional. After a successful security setup (both encryption and integrity protection), the core network accepts the registration and sends a confirmation to the phone. Additionally, the network assigns a periodically changing temporary identity called TMSI to the phone. The TMSI will be used by the phone to identify itself to the network for the subsequent transactions, and most importantly, it prevents the usage of an IMSI over-the-air thereby concealing the subscriber's permanent identity. A TMSI will only be updated after security protection had been enabled, although the exact update period depends on the operator configuration.

2.2 Mobility Management

Phones continuously monitor the signal strength and SIBs from surrounding base stations and tunes to the base station that offers the highest signal strength. When a phone is traversing across the cells and crosses the boundary of a currently registered administrative area, it has to perform a registration update with the core network. This enables the core network to maintain a track on the phone's location and accordingly route incoming call and data services to the right area. The phone notices the change in the area by monitoring the identifiers in SIBs. This update is performed using the similar *Location Update* message in 2G and 3G whereas in 4G a *Tracking Area Update* message is used. Depending on the configuration of the operator, the update procedure involves similar transactions like the registration procedure. If the core network cannot identify a phone based on its TMSI, it can request the permanent identity and perform authentication and activate security protection again. After this is successful, the phone can continue to use mobile service.

2.3 Paging

When a subscriber has an incoming call/data/SMS, the core network commands the base station to broadcast paging messages in order to notify the phone about this incoming event. Paging messages are directed to the area where the phone was last connected (or registered) to the network. When there is no response from the phone, they are propagated to other adjacent areas. Normally, a paging message contains the TMSI of a subscriber to page. However, in special cases such as no response from the phone or a network error, paging messages are broadcast with an IMSI. When the phone detects a paging message containing its identity, it will send a paging response and confirm its preparedness for the incoming event.

2.4 IMSI Catcher

IMSI catcher is a special kind of cellular equipment, whose main goal is tracking and identifying the cellular phones mainly by collecting permanent identities (IMSI, IMEI) from the phones. They impersonate legitimate networks and mimic the characteristics of real base stations. As a thumb rule, they transmit with a higher power than surrounding base station to attract the phones. They operate using distinct administrative area identification deviating from any nearby cells to trigger the update procedure from the phone and steal their identities. Sophisticated and highly capable IMSI catchers can also perform a Man-in-the-Middle attack to intercept the cellular traffic.

In the next section, we start from the operating principles of IMSI catchers and how they are detected in the existing ICDs.

2.5 Related Work

Previous works on defense against IMSI catcher is spanned into multiple methods. One of the most accessible ICD methods is utilizing a smartphone app. Brenninkmeijer [24] and Park et al. [75] performed an analysis on free ICD apps. We use the evaluation results from these works as a baseline of what ICD should provide, and further extend the detection to cover the newer type of IMSI catchers. Sensor based IMSI catchers have been proposed by Dabrowski et al. [30], Wilson [99], and Ney et al. [69]. Dabrowski et al. [29], Li et al. [60], Steig et al. [92], and Do et al. [34, 35] proposed ICD using network internal data. Rupprecht et al. [83] presented an overview of the exploits discovered in the cellular network, while we are correlating the cellular exploits with the activities of real world IMSI catchers.

In the network side, updates on the cellular network standard to make IMSI catcher ineffective and new ICD methods utilizing network data had been proposed. One of the weak points is the authentication protocol used in 3G and 4G. Zhang [100] and Huang et al. [56] proposed methods to improve the security of AKA authentication method which is used in 3G and 4G. Arapinis et al. [20] proposed a linkability attack on AKA where it is possible to track the user based on the authentication data. Because IMSI catchers are exploiting the initial registration procedure, van den Broek et al. [97], Norrman et al. [71] and Khan et al. [58] proposed pseudo IMSI to hide the real IMSI during these procedures. Although this concept is incorporated into 5G [11], retrofitting this scheme into a currently used network requires modification into all related entities and still can not defend against older devices.

Peeters et al. [76] presented a sensor-based measurement to detect the SS7 redirection attack. This attack is employed by some IMSI catchers and only detectable by artifacts as phones receive the results of SS7 protocol messages processed by the core network, which is detected by some ICD apps on smartphones.

In addition, Raza et al. [82], Hussain et al. [57], Fang et al. [39] and Kim et al. [59] proposed methods to systematically test cellular exploits on smartphones, whose results can be used by an IMSI catcher to exploit the phones.

3 OPERATION OF IMSI CATCHERS

We analyzed public documents on IMSI catchers, namely leaked catalogs and manuals, related patents to better understand their operation. As the target audience of IMSI catchers is rather limited, manufacturers are reluctant to disclose the details to the general public. They are usually available in trade shows and may land on some public websites like Privacy International's Surveillance Industry Index [79] and WikiLeaks [1], with varying degree of details on implementation and operating principles. In contrast to the catalogs, patents are providing detailed technical information about the IMSI catcher's operation. Since patents are intended to be available to the general public, not every company are filing patents. We gathered notable documents such as commercial IMSI catcher catalogs and manuals from various sources and summarized the findings in Table 1.

Unfortunately, those open materials may not be adequate to easily understand the operational strategies of IMSI catchers: catalogs usually mention features with high level keywords, but how those features are implemented is not present. Patents describe features in a fine-grained manner, containing more than enough information to understand the IMSI catcher's operation. Moreover, not every IMSI catcher designs are patented. We start from the configuration details of IMSI catchers when available, like hardware (software defined radio, reuse of the off-the-shelf platform, custom cellular platform) and software configurations. We then use 3GPP cellular specifications as a baseline of IMSI catcher operations and interpreted the capability claimed in catalogs w.r.t specifications to understand what they can do.

Most IMSI catchers advertise the following capabilities: user identification, user locating and (optionally) user data eavesdropping. The major difference between IMSI catcher makers was integration with other data analysis products from the same company, and lower layer radio features. Because the cellular lower layer is more analog rather than digital, differences are mainly coming from each company's optimization know-how which is rather qualitative than quantitative. As we could not obtain the actual product itself, features which are not present in the public materials are not evaluated. The exact technical details of each operational stage are covered in the later sections.

3.1 Configuration

IMSI catcher could be divided into roughly two functional blocks: a radio frontend sending and receiving radiowave, and a network backend simulating a fake cellular core network and implementing the operational logic of an IMSI catcher. Depending on the form factor and hardware design, these two parts could be implemented in two separate boxes or integrated into a single system. An example of a discrete unit based IMSI catcher is Cellxion Optima [27], which uses modular design consists of discrete control, power, and cellular network unit.

Cellular network standards integrated multiple form factor of cells (macrocell, microcell, femtocell) to cope with different size of user demand and deploy requirements. This enabled IMSI catchers to also have multiple form factors, enabling operation in multiple situations: rackmount devices (e.g. Harris [52]), car-installable devices (e.g. Gamma Group [43]), and hand carry devices (e.g. Cambridge Consultants [26]). To facilitate car-based operation, some IMSI catchers can take not only AC mains power but also DC 12V or 24V power which is provided by commercial vehicles.

Some IMSI catchers [26, 42] are advertising that they are based on the commercial off-the-shelf (COTS) femtocell platform, which implements a complete cellular network stack in a single device. The possibility of using a femtocell as an IMSI catcher is already proposed on the previous work on attacks on commercial femtocells [31, 44]. By sharing the implementation with the COTS platform, IMSI catcher developers can save the development resources on the cellular network stack, especially for the lower layer. This makes the detection of IMSI catcher based on radio fingerprinting nearly impossible, as the same stack is also used by the real femtocell.

IMSI catchers can self-configure itself adapting to the nearby cellular environment. Broadcast information of IMSI catchers is adjusted to increase the chance of cell reselection to the IMSI catcher to facilitate the attack. According to Dabrowski et al. [30], IMSI catchers are using either different *Location Area Code*[1] with nearby cells or the same code but different T3212 timer value to trigger a periodic *Location Area Update* on 2G. In the case of 4G, IMSI catchers may set *q-rxLevMin* and *q-rxLevMinOffset* parameter of SIB message different from the neighboring cells to trigger handover in a different received signal level [25]. This kind of self-configuration based on the data from neighboring cells is implemented by listening to the broadcast messages of the nearby cellular network and extracting identities from the visible cells in the area. It is often mentioned as a passive monitoring feature on commercial IMSI catchers. Details of the passive monitoring are further mentioned in the later sections.

3.2 Identification

Operation of IMSI catchers starts with the identification of nearby users, either by a passive method where attacker relies only on the broadcast and unencrypted dedicated signal, or an active method where attacker operates a fake base station and sends messages to the nearby phones.

Passive Tracking. IMSI catchers can passively listen to the nearby radio signals. Because of the nature of passive listening without any radio transmission, neither the phone nor the cellular network can easily detect the presence of the passive tracking IMSI catchers. IMSI catchers can acquire not only the neighboring cell's configuration parameters, but also paging messages using passive tracking, since they are unencrypted and contain identities of nearby subscribers. Then they analyze the identities within paging messages to track the subscriber's presence. For paging with TMSI, IMSI catcher correlates the changes in TMSI across multiple paging messages to track a subscriber. This is possible since some operators allocate a "new" TMSI using a predictable pattern, such as changing only minimal digits or monotonically increasing [55, 87]. For paging with IMSI, some operators page subscribers using IMSI more frequently, which enables IMSI catchers to acquire IMSI easily.

Additionally, some IMSI catchers can listen to the unencrypted portion of dedicated signaling messages. As they are using a different transport channel from paging and broadcast signaling messages, not every passive IMSI catchers are capable of decoding this type of message. How dedicated signaling messages are exploited by IMSI catchers is discussed in the later section.

Active Tracking. IMSI catcher is visible to the phones as another lookalike base station with different administrative area identification, therefore a mobility management procedure is started upon handover. Figure 2 shows an example of signaling message exchange of a real network and an IMSI catcher. IMSI catchers ask for not only the phone (IMEI) and subscriber identity (IMSI) (*Identity Request/Response* of the figure) but also other information for fingerprinting and identifying the target such as the phone's network capabilities (*UECapabilityInquiry* and *UECapabilityInformation* of the figure). Asking these identities without encryption via dedicated signaling messages is allowed according to the cellular network standard, as an identification is needed to authenticate the cellular user accordingly. IMSI catchers can also send signaling messages in abnormal sequence or utilize baseband exploits to further acquire information which is not allowed to be sent to the network without encryption by the specification. This mode of operation is frequently mentioned in IMSI catcher's patent documents [61, 78].

If the target's IMSI or TMSI is already known, mobility management procedure is not required to check its presence within the area. By sending paging messages containing the target's IMSI or TMSI, the presence of the target is identified upon reception of a *Paging Response* message. Upon reception, the IMSI catcher may not respond to any further messages from the target to cloak itself (the end of IMSI catcher's signaling message flow in Figure 2). This is implemented in an IMSI catcher patent [45].

As IMSI catchers lack the secret to perform the mutual authentication in 3G [2] and 4G [3], "native" 3G and 4G IMSI catchers cannot perform the authentication and its capabilities are limited to what is available before authentication was performed.

Downgrading and Denial of Service. After identifying and tracking the subscriber, IMSI catchers may either send the victim

[1] A type of administrative area identification code

Product Name	2G	3G	4G	Passive Tracking (§ 3.2)	Active Tracking (§ 3.2)	Downgrade via Protocol (§ 3.2)	DoS (§ 3.2)	Location Tracking (§ 3.3)	Eavesdropping (§ 3.4)	Injection (§ 3.4)
Ability [18]	✓	✓		✓	✓	✓	✓	✓	✓^{2}	✓^{2}
Altron [19]	✓	✓			✓	✓	✓	✓	✓^{2}	✓^{2}
Cambridge Consultants [26]	✓	✓		No direct mention of capabilities as an IMSI catcher Only claims to be a reference design						
Cell Catcher CC1900 [54]	✓	✓			✓		✓	✓		
Cellxion [27]	✓	✓			✓	✓	✓	✓	✓^{2}	✓^{2}
Digital RF [33]	✓			✓	✓		✓	✓		
Elkat 1700 [37]	✓			✓				✓	✓^{2}	✓^{2}
Elaman [36]	✓	✓		✓	✓	✓	✓	✓	✓^{2}	
Gamma Group [43]	✓	✓			✓	✓	✓	✓	✓^{2}	
Harris Gemini [52]	✓	✓	✓	✓	✓	✓	✓	✓		
Helios [42]			✓		✓					
KingTone [81]			✓		✓					
LongHope PoliEye [22]	✓			✓	✓		✓	✓	✓^{2}	
MaxxGSM [32]	✓	✓	✓	✓	✓		✓	✓	✓^{2}	
Meganet VME [63]	✓			✓	✓		✓	✓	✓^{2}	✓^{2}
Neosoft [68]	✓	✓		✓	✓	✓	✓	✓	✓^{2}	✓^{2}
PKI Electronic [77]	✓	✓	✓	✓	✓	✓	✓	✓	✓^{2}	✓^{2}
Septier [86]	✓	✓	✓		✓	✓	✓	✓	✓^{2}	✓^{2}
Shogi Comms [89]	✓			✓	✓		✓	✓	✓^{2}	
Stratign [93]	✓			✓	✓	✓	✓	✓	✓^{2}	✓^{2}

Table 1: Comparison of surveyed IMSI catcher's capabilities based on available documents. ✓indicates that the IMSI catcher supports particular feature. Number 2 indicates that the feature is 2G only.

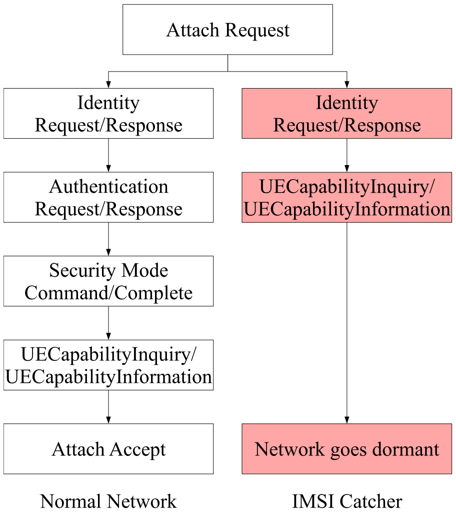

Attach Request
Identity Request/Response
Authentication Request/Response
Security Mode Command/Complete
UECapabilityInquiry/ UECapabilityInformation
Attach Accept
Identity Request/Response
UECapabilityInquiry/ UECapabilityInformation
Network goes dormant
Normal Network
IMSI Catcher

Figure 2: Example of signaling message flow of a normal network and an IMSI catcher before authentication.

phone back to the normal network or downgrade the phone into the older generation network (mostly to 2G) to further exploit the victim, where security measures are less strict than newer generation networks.

Downgrading could be done for everyone connecting to the IMSI catcher, or selectively based on the IMSI. There are several ways to downgrade. Radio jamming is one of the easiest methods to block the 3G and 4G network based on their frequency, forcing phones to use 2G. Mobility management messages could be also used for downgrading. There is a dedicated field for indicating the failure cause (*MM, GMM, EMM Cause*) in the mobility management failure message [7, 9]. Depending on the cause indicated by the network, the phone will not connect to any network, or utilize only lower generation networks. If the phone is instructed not to connect to any kind of network, it effectively results in a denial of service. The exact cause of downgrade or network unavailability is often not displayed to the mobile OS' user interface.

In addition, one of the IMSI catcher patents exploits signaling message for switching from 3G to other generation network (*Handover From UTRAN*) [10] to send the phone back to 2G [62]. As this message is accepted without security activation by standard [2], it could be used for downgrading to 2G. However, the 4G equivalent of this message (*Mobility From EUTRA*) needs to be integrity protected [5], 4G IMSI catchers cannot utilize this downgrade method as they have no authentication material for integrity protection.

Unlike other IMSI catcher operations, downgrading users to 2G or 3G is relatively easily noticed since currently connected network is displayed in the phone's status bar. Therefore, some IMSI catchers are advertising "release back" where the operation is done entirely in 3G or 4G and the phone is not downgraded [68, 77].

3.3 Location Tracking

Depending on the configuration, an IMSI catcher can track the cellular users within the radius ranging from several hundred meters to some kilometers. Once a cellular user is found within the range of an IMSI catcher, it can perform fine-grained location tracking to further locate the user in higher precision. There are two main methods to identify the location of the user in a cellular network: determine the location indirectly based on the RF fingerprint such as measurement data using triangulation, directly query the location via control or data plane messages.

Location tracking using triangulation is based on the signal strength measurements of cellular network standards. A core network can instruct a phone to measure nearby cell's signal strength which is reported by *Measurement Report* messages in 2G [8], 3G [10], and 4G [5]. This procedure is possible without security activation in 2G, 3G, and earlier revision of 4G. IMSI catchers ask for the measurement of at least three cells whose location is already known and performs triangulation to locate the user. The location of base stations is available from online databases such as OpenCellID [96], or some regulating bodies (e.g. ARCEP of France [21]) who mandates the operators to disclose the location of their base stations. In addition, location tracking based on the directional antenna and continuous transmission is mentioned in one of the IMSI catcher's operating manual [52].

Location tracking using cellular control plane messages are possible in two major methods: RRLP (Radio Resource Location services Protocol) [6] for 2G and 3G and LPP (LTE Positioning Protocol) [4] for 4G. They provide a precise location based on GPS. Since RRLP do not mandate any security setup for any location request, IMSI catchers can also send the RRLP position request to query the current precise location. LPP, on the other hand, mandates security before requesting position unless in an emergency call, preventing the usage by IMSI catchers. Users won't be notified that the network asked current GPS location in both cases.

There are other data plane based location service protocols such as OMA SUPL (Secure User Plane Location) [73], but we are not covering these type of technologies as establishing a data connection via an IMSI catcher is not always possible.

3.4 Eavesdropping and Injection

IMSI catchers can eavesdrop the dedicated signaling messages, only in some 2G networks due to the insecurity of used ciphering algorithm. At the beginning of the 2G network, there were two ciphering algorithms available for 2G: A5/1 and A5/2. A5/1 was found vulnerable [23, 47, 70], A5/2 is even more insecure as it is a weaker export version of A5/1. As a result, A5/2 was considered deprecated and a new ciphering algorithm A5/3 was introduced. IMSI catchers often advertise the deciphering functionality for A5/1, allowing live eavesdropping of a 2G network. Unlike 2G, 3G and 4G ciphering algorithms are not known to be broken, so they are immune to the eavesdropping (when the network enabled security).

Injection and Man-in-the-Middle attack on control plane by an IMSI catcher is only possible in 2G, as 2G has no integrity protection and obtaining the ciphering key is only possible in 2G. Because only ciphering is applied to the data plane of 3G [14] and 4G [16], it is possible to modify encrypted data on 4G user traffic [84]. This is not easily detectable as the data is successfully decrypted on the phone, and 3GPP addressed this problem by introducing integrity protection of data plane in 5G [17].

In contrast to the IMSI catchers advertising stealthiness, some IMSI catchers can utilize SMS-based exploits such as [38, 65] to attack the connected phones. Some fake base stations found in China are sending spam SMS messages to connected users, whose content is spoofed as coming from a trusted source [60].

4 IMSI CATCHER DETECTION METHODS

We dedicate this section to discuss the current state of IMSI Catcher Detectors (ICDs) and their detection techniques. Further, we also evaluate their strengths and weaknesses based on their detection capabilities. ICDs can be classified into three categories: app-based, sensor-based and network-based, whose characteristics are illustrated in Figure 3. Earlier studies [75] and [29, 60, 67] have conducted a practical evaluation of app-based ICDs and network-based ICDs respectively. In a similar manner, we have evaluated an app-based ICD and a sensor-based ICD which was not covered in the previous studies.

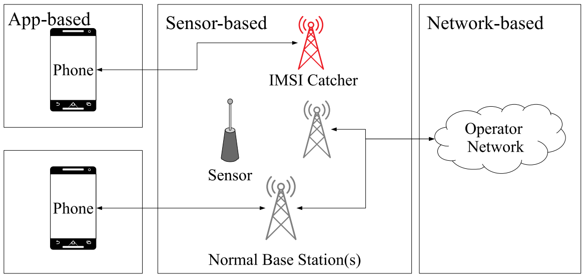


Figure 3: Overview of IMSI catcher detection methods.

4.1 App-Based ICDs

App-based ICDs are available as a free or paid mobile Android app, either as a separate installable application or an integrated part of the smartphone OS. Because of the limitation of the mobile OS API regarding cellular network information [75], these apps require access to the cellular network messages available from the diagnostic interface of the smartphone baseband. These messages are analyzed to detect the presence of an IMSI catcher. The detection results are then displayed to the user as real-time notifications shortly after the IMSI catcher event. As presented in the left hand side of Figure 3, the detection capabilities are based on what a single smartphone can see the cellular network. They optionally utilize openly available base station location databases such as OpenCellID [96] for enhanced detection, e.g. whether the cell is located in a place where it is supposed to be. Examples of such free app include SnoopSnitch [91], AIMSICD [85]. There is also a commercial solution like the CryptoPhone [49], which is Android-based and has a baseband firewall built-in to it.

Previous work [75] analyzed the evaluation criteria of free ICD apps and used a custom IMSI catcher setup to evaluate the detection results of the apps. According to that, ICD apps are acquiring the broadcast and dedicated signaling messages from the baseband and check their content for traces of IMSI catchers. Common examples of analyzed parameters are configuration parameters of the cell, the existence of neighboring cells, unexpected identity requests (IMSI, IMEI, location, etc.), paging with IMSI and insecure downgrading. Commercial ICD apps are also evaluating these set of parameters, along with other parameters that are not directly mentioned in the product description.

Although IMSI catchers configure themselves as close as possible to the nearby real base station, certain parameters are not exactly the same in order to induce handover and facilitate identity acquisition procedure. ICD apps store configuration parameters of each visible base stations and warn the user if certain values do not match or have too many differences with the nearby cells. Since IMSI catchers cannot pass the mutual authentication, IMSI catchers are asking as many identities as possible without authentication through unencrypted dedicated signaling messages allowed by the cellular network standards. ICD apps are monitoring whether there was a successful authentication after asking identities and will warn the user if the authentication was not successful. Similarly, if there was no successful authentication during the downgrade procedure, or the downgrade messages were not integrity protected, ICD apps will warn the user for an insecure downgrade.

While privacy-sensitive users may want to install the ICD apps, the detection results of app-based ICDs have been previously challenged. Although the major blocker of evaluation with a real IMSI catcher is obtaining one, it is possible to simulate the IMSI catcher's operating principles with a custom base station setup with COTS hardware and modified software. The evaluation as conducted by [75] utilizes this concept to implement a simulated 2G and 3G IMSI catcher. Motivated by this setup, we acquired a commercial device with ICD app integrated as a system application, the CryptoPhone CP500i [49] and evaluated its detection capabilities with a similar setup as described in [75]. According to the product description of CryptoPhone, it provides secure voice calls and messaging in addition to the ICD functionality, but we are only focusing on its IMSI catcher detection capability.

Our evaluation of CryptoPhone using the simulated IMSI catcher setup showed that it provides more or equivalent detection capabilities compared to free ICD apps. The technical description of Baseband Firewall on CryptoPhone [50] lists that IMSI catcher detection is done as anomaly detection on both baseband and network behavior. According to the document, CryptoPhone provides additional parameters not existing in SnoopSnitch and AIMSICD. An example of this is inconsistencies between the mobile OS and baseband activity and warns if the network information from the baseband and mobile OS do not match, or the baseband is processing call/SMS/data connection without the knowledge of the mobile OS. In addition, it can optionally share the suspicious detection results to the GSMK Overwatch system [51], where further analysis is performed.

However, inspired by the circumvention techniques mentioned in [75], it is partially possible to circumvent the detection of CryptoPhone. As an example, we tried using the invalid or reserved ciphering algorithm on 2G (such as A5/5) and instead of sending any response for *Location Updating Request* after requesting identities, the IMSI catcher sends nothing and the event is not detected correctly. We consider this behavior as minor implementation issues and believe that this is not difficult to fix.

From the usability point of view, CryptoPhone do not require rooting or device modification as the ICD app is integrated as an out-of-the-box system app. As such, it is immune from the side effects of Android rooting such as malicious usage of root permission by malware. It also provides baseband shutdown feature, which turns off the any cellular communication of the smartphone when an IMSI catcher had been detected. Because the only practical way to avoid IMSI catcher is not using the cellular device near the area of IMSI catcher, this feature provides an extra protection. Similar functionality does not exist in free ICD apps currently. In case of an IMSI catcher event, the log viewer presents more details than free ICD apps. While free ICD app SnoopSnitch also provides event log, it represents the log event data as an internal scoring, whose detail is only mentioned inside the help documentation. CryptoPhone provides a text description of the IMSI catcher event, providing more details directly from the app.

Further, while not yet implemented as a product, Apple's patent [25] defines an additional set of parameters. The patent lists a mixture of adaptation of well-known parameters to the new generation and parameters which were not evaluated before. Examples of new parameters are about the detection of a software-based base station: measurement of frequency error, timing drift, and relatively longer latency. While not all software-based base stations are IMSI catchers, it is relatively easily used as such.

Advantages. Since smartphones are directly facing the user, it can give the user a direct real-time notification shortly upon IMSI catcher activity without further communication with external detection services. Because of the different logical channel for dedicated and broadcast signaling messages, the phone (therefore the ICD app) can easily access both dedicated and broadcast signaling messages. This provides more detection capability as dedicated signaling carries critical information like mobile identities.

Disadvantages. Due to design constraints and inadequate implementations, some apps present false notifications to the user which is sometimes annoying. For example, a smartphone itself does not know the network deployment status, and whether the current cell is located within the expected place without external information. Smartphones have high mobility, persistent measurement of a single place requires a smartphone to be permanently installed which is not feasible. Further, there is a potential burden on a smartphone due to increased battery consumption and side effects such as some security features disabled caused by rooting the smartphone. The latter could be mitigated by providing the ICD engine integrated within the mobile OS. Differently, IMSI catcher might use legitimate network identities and completely remain naive to the app which is a false negative.

4.2 Sensor-Based ICDs

Sensor-based ICDs are either a passive cellular device or an integrated sensor within the base station that continuously monitor broadcast signals of the surrounding base stations, as presented in the center of the Figure 3. Sensor hardware is usually built using an embedded system, with a cellular modem attached to listen to the broadcast messages and an Internet connection to collect and analyze the sensor data in the central network. Either cellular network operator themselves or independent provider can provide the IMSI catcher detection network. Unlike smartphones, they are installed in a fixed place and more than one devices are simultaneously monitoring the networks from multiple places. This provides a persistent and wide-area measurement which is not easily possible in app-based ICDs.

Broadcast signals monitored by an ICD sensor include changes in SIBs, appearances of new base stations, the lifetime of base stations and anomalies in configuration and paging procedures. The appearance of a new base station could be either a legitimate base station or an IMSI catcher. A legitimate base station may use different test configuration initially, but adapt to the configuration used by nearby base stations to harmonize the requirements, and more persistently visible. In contrast, IMSI catchers have a relatively short lifetime and may reuse the identity of another cell which is not supposed to be present on the site. Also, higher prevalence of an IMSI paging can indicate that either the base station is misconfigured or maliciously using IMSI paging to track the user. By continuously monitoring the neighboring cells, an ICD sensor can detect whether the cell is differently configured from its neighbor and flag it as an IMSI catcher.

Some sensors also have active detection capability, such as Overwatch [51]. In the active mode, the sensor is acting analogous to a honeypot [28]. It establishes a connection with the base station and analyzes the dedicated signaling messages exchanged with it, in a similar method with the app-based ICDs. This enables sensors to also see the parameters which are only present in the dedicated signaling messages, such as availability of telephony and data services or whether identity inquiry methods are followed by any security setup procedure. As a result, ICD sensors can get a more accurate result of whether the particular cell is an IMSI catcher or not.

After collecting the data to the sensor operator's database, additional analysis is performed and the detection results are further propagated to the sensor network subscribers or the network operator themselves. The network of sensor-based ICDs is stable than the network of app-based ICDs, as sensors have fixed position and their Internet connection is not affected by any IMSI catcher, unlike phones. As an example of networked detection, by combining the visible cell identities from geographically separate areas, sensor-based ICDs can easily identify the reuse of cell identifiers.

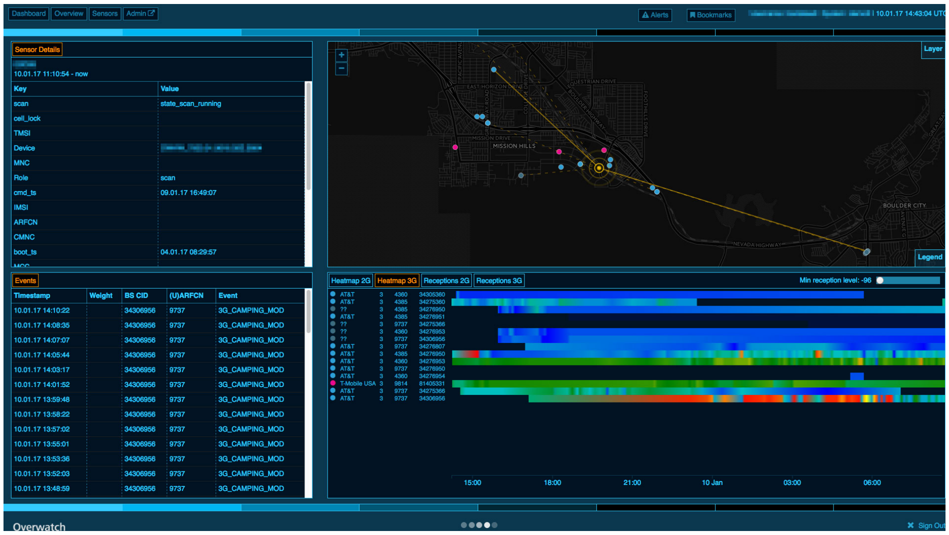
Examples of such sensors include sICC [30], SITCH [99], SeaGlass [69]. The authors opened the sensor node application to the public, and there is an independent report of operating SeaGlass sensor node [72]. However, according to their device description and sensor node application, all of them are limited to 2G because the cellular modem used is only capable of 2G. In addition, FB-Sleuth [101] applied RF fingerprinting on 2G fake base stations to detect and localize them. While IMSI catchers have a tendency of downgrading to 2G and exploit the phone within the 2G network, the downgrading is done in 3G and 4G so monitoring all the generation is important for effective IMSI catcher detection. The sensor software needs to be also updated to parse the parameters in new generations.

We evaluate the Overwatch system, consisting of multiple sensor nodes and an analysis cloud. In particular, we acquired a Overwatch sensor and access to the detection cloud system. Overwatch sensor is based on embedded Linux with cellular and GPS capabilities. GPS is used to locate the sensor and calculate the relative distance from the base station. The sensor could be configured to be either passive or active mode, the latter requiring a SIM card to connect to the network. An example Overwatch web user interface is presented in Figure 4. It is divided into four quadrants: map of the known base station and sensors are displayed in the upper right, sensor events are displayed in the lower left with a heatmap indicating the received signal strength in the lower right, list of sensors is displayed in the upper left. Within the web interface, it is possible to see the data collected from the sensor and the timeline of cellular and IMSI catcher activity.

In the passive mode, we were able to get an IMSI catcher warning based on base station lifetime, configuration changes, suspicious activities like paging with IMSI. In the active mode, the sensor node connects to the specific base station by frequency and cell ID and evaluates the behavior during connection to check whether the cell is an IMSI catcher. However, current Overwatch sensor nodes are limited up to 3G by hardware design and GSMK claimed that the 4G support is in development. Further, an article was released by the developer which claims the system was able to fingerprint IMSI catchers in various locations around the world [46].

Advantages. Thanks to the physically stable installation and bigger antenna size than smartphones, ICD sensors can monitor a larger area compared to smartphones for an extended amount of time. This allows a detailed and focused analysis of a group of base stations. Fixed installation in multiple locations with long-term observation enables the sensor node to understand the dynamically changing configurations, while app-based ICDs are bound to the mobility of the phone. Moreover, since sensors are powered from a mains power and unlike smartphones they do not run any additional background process that may hinder the analysis of incoming signaling messages, they provide more computing power for IMSI catcher detection. Detection is independent of nearby smartphone's activity because it is physically independent.

Disadvantages. Passive only sensors are limited to broadcast channels and cannot analyze the base stations' behavior on the dedicated channels. A smartly configured IMSI catcher can easily bypass the passive sensor detection by closely copying the broadcast parameters of nearby base stations, therefore adding false positives in the detection. In addition, sensors need long observation times and require some time to detect the IMSI catcher event and deliver a warning to the phone. As a result, an IMSI catcher might already succeed in an attack well before it is detected by a sensor. While individual sensors could be easily built with minimal cost, maintaining backend infrastructure for sensor management and analysis requires recurring cost (power, Internet, place rental, management), which will also increase when service coverage is expanding. Especially, when the environment is hostile (e.g. political issues) sensor



[redacted] | 10.01.17 14:43:04 UTC

Sensor Details

[redacted]
10.01.17 11:10:54 - now

Key	Value
scan	state_scan_running
cell_lock	
TMSI	
Device	[redacted]
MNC	
Role	scan
cmd_ts	09.01.17 16:49:07
IMSI	
ARFCN	
CMNC	
boot_ts	04.01.17 08:29:57
MCC	

Events

Timestamp	Weight	BS CID	(U)ARFCN	Event
10.01.17 14:10:22		34306956	9737	3G_CAMPING_MOD
10.01.17 14:08:35		34306956	9737	3G_CAMPING_MOD
10.01.17 14:07:07		34306956	9737	3G_CAMPING_MOD
10.01.17 14:05:44		34306956	9737	3G_CAMPING_MOD
10.01.17 14:03:17		34306956	9737	3G_CAMPING_MOD
10.01.17 14:01:52		34306956	9737	3G_CAMPING_MOD
10.01.17 13:59:48		34306956	9737	3G_CAMPING_MOD
10.01.17 13:58:22		34306956	9737	3G_CAMPING_MOD
10.01.17 13:57:02		34306956	9737	3G_CAMPING_MOD
10.01.17 13:55:01		34306956	9737	3G_CAMPING_MOD
10.01.17 13:53:36		34306956	9737	3G_CAMPING_MOD
10.01.17 13:52:03		34306956	9737	3G_CAMPING_MOD
10.01.17 13:48:59		34306956	9737	3G_CAMPING_MOD

●	AT&T	3	4360	34305360
●	AT&T	3	4385	34275360
●	??	3	4385	34276950
●	AT&T	3	4385	34276951
●	??	3	9737	34275366
●	??	3	4360	34276953
●	??	3	9737	34306956
●	AT&T	3	9737	34276807
●	AT&T	3	4385	34276950
●	AT&T	3	4360	34276953
●	AT&T	3	9737	34276950
●	AT&T	3	4360	34276954
●	T-Mobile USA	3	9814	81405331
●	AT&T	3	9737	34275366
●	AT&T	3	9737	34306956

Figure 4: Example user interface of GSMK Overwatch [90].

deployment is not possible at all so detection using sensor is not also possible.

4.3 Network-Based ICDs

Network-based ICDs mainly utilize the information collected by the network itself, and optionally correlate information from other sources such as Wi-Fi (right of the Figure 3). Unlike app and sensor-based ICDs, network-based ICDs do not rely on the dedicated measurement for IMSI catchers but utilize already existing data and procedures to perform the IMSI catcher detection. The primary data source is precise and up-to-date base station locations and internal operator logs. Examples of such system include FBS-Radar [60] and [29, 67, 92].

Since cellular network operators are utilizing licensed frequency bands, they can perform actions against IMSI catchers as a licensee when it is detected by network-based ICDs. For example, they can utilize signal strength measurements obtained from the phones and correlate with the up-to-date cell deployment information to identify the presence of the IMSI catcher and further track its physical location. In addition, network operators can blacklist IMSI catchers by using dedicated SIBs and prevent the phones connecting to them. Legal enforcement could be done to physically locate and suppress the IMSI catcher.

ICD proposed in [29] monitors previously visited location information, capabilities reported by phone and round-trip time for authentication to identify IMSI catchers. Differently, [67, 92] acquires cell IDs and corresponding power measurements of the cells surrounding the phone. These measurements are cross-checked with the internal database to detect whether the cell is located in the correct location. FBS-Radar [60] adopts Wi-Fi-based localization in addition to cellular power measurements, to help to localize the fake base station. In addition, it supports the analysis of manipulated SMS messages sent from a fake base station to further identify the owner of it. [34, 35] proposed machine learning on the network-acquired data, such as handover patterns, location update, and IMSI-IMEI relations. However, information utilized by these ICD methods is only available inside the operator's network and hence we could not evaluate the detection capabilities by ourselves.

Advantages. Operators retain up-to-date information of the cellular network deployment, hence, detection of unknown cells and base station identities are a clear sign of an IMSI catcher. Further, this reduces false-positives and increases accuracy. Deployment cost is low as it only requires software upgrades within the network.

Disadvantages. Implementation requires cooperation with network operators, which is not always possible. Similar to sensor-based detectors, the detection is performed after the phone was released from the IMSI catcher. The current standard only allows transmitting limited information regarding the interaction with an IMSI catcher. Therefore the network cannot realize to what extent the phone was compromised. For instance, the network cannot detect if the previous voice call made by the phone (with IMSI catcher) was encrypted or not.

5 DISCUSSION ON DETECTION STRATEGIES

We discuss the limitations on current ICD methods and what will be the future requirements of ICDs in this section. In particular, we start from how each individual detection methods could be improved, propose a combination of multiple ICD methods to fill the gap of each method, and efforts of standardization bodies to address the IMSI catcher issue. From the evaluation of currently available ICD solutions, we found that five major problems that should be addressed to achieve efficient and reliable detection. Leaving behind the cost and deployment options, the major problems are due to the lack of:

- Logical and behavioral analysis of IMSI catcher patterns
- Sufficient and reliable data to make decisions
- Efficient and complete implementation of ICD apps
- Real-time attack detection and prevention
- Relative lack of interest by standardization bodies

With the above drawbacks, we understand that a stand-alone ICD cannot always offer reliable detection. Each of the problems could be addressed by extending the implementation of existing solutions and combining multiple detection methods to fill the gap of each other. Using a single method can not solve the IMSI catcher problem completely due to the complex cellular network architecture which is based on a tradeoff between performance and security. Hence, we discuss the detailed requirements of future generation ICDs and what kind of effort had been done to incorporate into the cellular standards.

Better detection methods for app-based ICDs. Smartphone app-based ICDs could be enhanced using additional detection parameters and more integration to the external data sources. As currently available free ICD apps are only providing 2G and 3G support, adaptation of currently available parameters to 4G equivalent and a set of new parameters for all generations will increase the detection accuracy. As an example of 4G LTE specific parameter, 4G LTE changed the radio access network to allow both narrow and high bandwidth network for flexibility and adaption to different regulatory requirements. According to a survey [80], bandwidths of multiples of 5 MHz are preferred over 1.4 and 3 MHz. Because operators tend to configure geographically neighboring cells to use the same bandwidth, so if a cell's bandwidth is different from surrounding cells, the chance of the cell being a fake base station is high. Similarly, parameters indicating the DoS and identity theft attack, such as insecure identity requests, could be enhanced to cover corner cases of current ICD apps. Example of parameters not well evaluated by current solution includes deliberate connection termination, usage of incomplete or invalid values for protocol messages.

Combination of multiple types of ICDs. By integrating the information from a sensor-based ICD with an app-based ICD, it is possible to resolve the ambiguity on the inconclusive detection on an app-based ICD. As an example, downgrading from 4G to 2G could be done in legitimate cases, such as the operator's lack of coverage in a certain area or a user is not subscribed to the higher generation services. This is reflected as a service-related cause carried over the service rejection message. Both an IMSI catcher and the legitimate network can ask identities before rejecting the service and downgrading the user, which is represented as the same set and sequence of signaling messages. In this case, the app-based ICD cannot reliably distinguish whether downgrade was performed by the real cell or not.

Sensor-based ICD can supply additional information to the app-based ICD to clarify about the downgrading. A passive sensor can detect whether the 4G network is available in that place. An active sensor can detect whether the cell is downgrading 4G users. Assuming that the user can use the 4G service normally if the sensor result indicates that the 4G network is available in the place and the cell is also downgrading the active sensor from 4G to 2G, it will be clear that the cell in question is an IMSI catcher. This information could be queried by the app-based ICD as soon as a normal Internet connection is established. In addition, by using information from the network-based ICD, the validity of the rejection cause related to the network status (e.g. congestion) could be cross-checked.

Efficient attack protection. Because app-based ICDs can warn only the currently present IMSI catcher, the result of sensor and network-based ICDs needs to be delivered in a timely manner to protect from the eventual connection to the IMSI catcher. Since IMSI catcher has a short lifetime and chances of handover to an IMSI catcher could be prevented when the target cell is known as an IMSI catcher, having a short propagation delay of IMSI catcher information is needed for efficient attack protection.

Current sensor-based ICDs are primarily relying on the Internet to deliver the IMSI catcher information. However, information delivery via the Internet is not possible when an IMSI catcher is operational, as IMSI catchers can block access to the Internet or actively intercept the Internet traffic. In addition, there are network control plane messages to prevent handover from certain cells, which is only usable by network-based ICDs. The LTE SIB 4 [5] contains a field *intraFreqBlackCellList* to block the handover to the cell listed in it. Listing the IMSI catcher inside the SIB 4 of the operator's base station will prevent handover to it. However, the SIBs are not cryptographically signed so integrity is not guaranteed. Therefore, a secure method of propagating IMSI catcher information using the cellular control plane message with integrity and replay protection is also needed.

Standards regarding ICDs. As long as cellular network standards allow loopholes for the operation of IMSI catchers, the threat will persist. This will not become to the end unless the loopholes of the standards are addressed. Despite the long history of IMSI catcher and ICDs, 3GPP – specifically its SA3 working group for security and privacy – started a work item to address the problems caused by fake base station relatively recently. Henceforth, currently available documents are technical reports [12, 15] addressing the fake base station problem and possible candidate solutions. This problem is covered within the scope of *Radio Access Network (RAN) Security*.

Another example of collaboration between the research community and 3GPP is a minimization of unencrypted IMSI exposure to the radio network. Proposals have been published for minimizing the exposure of IMSI over the air [71, 97] and amendment on authentication protocols to prevent privacy information leakage [40, 56, 100]. Some proposals have been incorporated into the new 5G standard [11, 13], although using the privacy enhancements of 5G in a commercial network is not always mandatory.

Among the addressed problems within [15], we believe that security of unprotected unicast messages and system information can defend against IMSI catcher operation. By protecting unicast messages, downgrading and DoS will not be possible without valid integrity protection. By securing system information, detection of IMSI catcher will become much easier as IMSI catchers cannot sign the system information with the same key used by the real operator. Solutions proposed in [12] includes PKI-based and ID-based digital signature on signaling messages, system query method for a possible fake base station. Although they are still being evaluated, careful implementation in the next-generation network and retrofitting into the current generation network to prevent bidding down attack will require another effort.

We are summarizing the requirements as following: app-based ICDs need to cover more IMSI catcher's behavior for efficient detection, network, and sensor-based ICDs requires better integration to app-based ICDs, and an efficient and secure method to deliver the IMSI catcher information is required.

6 CONCLUSION

We made a systematic analysis of IMSI catcher's product catalogs and patents to understand its capability and how it exploits the cellular network specification to identify and track the cellular users. Aside from proprietary optimizations and analysis solutions, these products are relying on similar methods to achieve the IMSI catcher's goal.

To defend against IMSI catchers, we analyzed currently available ICD solutions, namely app-based, sensor-based, network-based ICDs. Each of the solutions has its own advantages and disadvantages on IMSI catcher's detection, reporting the detection result, and preventing users from targetted by further IMSI catcher operations.

Among the limitations of the current ICD ecosystem, insufficient evaluation of parameters by ICD apps and limited cooperation between entities are one of the main problems. We address this by possible solutions on improving the IMSI catcher detection. Specifically, app-based ICDs require a new set of ICD parameters and more collaboration with network and sensor-based ICDs upon ambiguities in detection. Cellular network standard needs to accommodate the efficient and secure delivery of IMSI catcher information, to cope with the relatively short lifetime of an IMSI catcher.

Future work. Although 5G further enhances security compared to 4G, current generation networks will remain in use for foreseeable amount of time, and security improvements on 5G [66] might not be implemented in a best manner in the commercial network deployment. Not only the extensive real-world testing of our current implementation, but also extending to the next generation network will defend cellular networks against IMSI catchers.

Acknowledgements. This research was partly performed within the SerIOT project (seriot-project.eu) the EU Framework Programme for Research and Innovation Horizon 2020 under grant agreement no. 780139. We would like to thank anonymous reviewers for their valuable inputs and suggestions.

REFERENCES

[1] [n.d.]. WikiLeaks. https://wikileaks.org

[2] 3GPP. [n.d.]. *3G security; Security architecture.* TS 33.102. http://www.3gpp.org/DynaReport/33102.htm

[3] 3GPP. [n.d.]. *3GPP System Architecture Evolution (SAE); Security architecture.* TS 33.401. http://www.3gpp.org/DynaReport/33401.htm

[4] 3GPP. [n.d.]. *Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP).* TS 36.355. http://www.3gpp.org/DynaReport/36335.htm

[5] 3GPP. [n.d.]. *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification.* TS 36.331. http://www.3gpp.org/DynaReport/36331.htm

[6] 3GPP. [n.d.]. *Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP).* TS 44.031. http://www.3gpp.org/DynaReport/44031.htm

[7] 3GPP. [n.d.]. *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3.* TS 24.008. http://www.3gpp.org/DynaReport/24008.htm

[8] 3GPP. [n.d.]. *Mobile radio interface layer 3 specification; GSM/EDGE Radio Resource Control (RRC) protocol.* TS 44.018. http://www.3gpp.org/DynaReport/44018.htm

[9] 3GPP. [n.d.]. *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3.* TS 24.301. http://www.3gpp.org/DynaReport/24301.htm

[10] 3GPP. [n.d.]. *Radio Resource Control (RRC); Protocol specification.* TS 25.331. http://www.3gpp.org/DynaReport/25331.htm

[11] 3GPP. [n.d.]. *Security architecture and procedures for 5G System.* TS 33.501. http://www.3gpp.org/DynaReport/33501.htm

[12] 3GPP. 2017. *Study on the security aspects of the next generation system.* Technical Report (TR) 33.899. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33899.htm Version 1.3.0.

[13] 3GPP. 2017. *System Architecture for the 5G System.* Technical Specification (TS) 23.501. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/23501.htm

[14] 3GPP. 2018. *Radio Link Control (RLC) protocol specification.* Technical Specification (TS) 25.322. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/25322.htm

[15] 3GPP. 2018. *Study on 5G security enhancements against false base stations.* Technical Report (TR) 33.809. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33809.htm Version 0.1.0.

[16] 3GPP. 2019. *Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification.* Technical Specification (TS). 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/36323.htm

[17] 3GPP. 2019. *NR; Packet Data Convergence Protocol (PDCP) specification.* Technical Specification (TS) 38.323. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/38323.htm

[18] Ability Computers & Software Industries Ltd. [n.d.]. Ability GSM & 3G Interception. https://wikileaks.org/spyfiles/files/0/80$_A$BILITY-GSM$_3$G$_I$ntercept.pdf

[19] Altron Development and Production. [n.d.]. Altron GSM/UMTS Grabber. https://assets.documentcloud.org/documents/409196/87-altron-grabber.pdf

[20] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New Privacy Issues in Mobile Telephony: Fix and Verification. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12).* ACM, 205–216. https://doi.org/10.1145/2382196.2382221

[21] Arcep. [n.d.]. La couverture mobile. https://www.arcep.fr/nos-sujets/la-couverture-mobile.html [in French, Online, accessed 15-07-2019].

[22] Beijing LongHope Police Equipment Co., Ltd. [n.d.]. Product List Poli-Eye. https://assets.documentcloud.org/documents/810590/930-longhope-police-equipment-product-list-polieye.pdf

[23] Alex Biryukov, Adi Shamir, and David Wagner. 2001. Real Time Cryptanalysis of A5/1 on a PC. In *Fast Software Encryption: 7th International Workshop, FSE 2000,* Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, and Bruce Schneier (Eds.). Springer Berlin Heidelberg, 1–18. https://doi.org/10.1007/3-540-44706-7$_1$

[24] Bauke Brenninkmeijer. 2016. Catching IMSI-catcher-catchers: An effectiveness review of IMSI-catcher-catcher applications. Bachelor Thesis, Radboud University (Nijmegen, The Netherlands).

[25] Elliot S. Briggs and Zhu Ji. 2018. Detection of a rogue base station. US Patent 10,129,283.

[26] Cambridge Consultants. [n.d.]. Small cellular base-stations for homeland security applications. https://wikileaks.org/spyfiles/docs/CAMBRIDGECONSULTANTS-2011-SmalCellBase-en.pdf

[27] Cellxion Ltd. [n.d.]. Cellular Intelligence Solutions. https://www.documentcloud.org/documents/810703-202-cellxion-product-list-ugx-optima-platform.html

[28] Eric Cole and Stephen Northcutt. [n.d.]. Honeypots: A Security Manager's Guide to Honeypots. https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide

[29] Adrian Dabrowski, Georg Petzl, and Edgar R. Weippl. 2016. The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection. *Research in Attacks, Intrusions and Defenses* (2016). https://doi.org/10.1007/978-3-319-11379-1 arXiv:9780201398298

[30] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-catch Me if You Can: IMSI-catcher-catchers. *Proceedings of the 30th Annual Computer Security Applications Conference* (2014), 246–255. https://doi.org/10.1145/2664243.2664272

[31] Doug DePerry, Tom Ritter, and Andrew Rahimi. 2013. Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell. *BlackHat 2013* (2013).

[32] Detective Store Ltd. [n.d.]. GSM 2G/3G/4G interception system - MaxxGSM. https://www.detective-store.com/gsm-2g3g4g-interception-system-maxxgsm--448.html

[33] Digital RF Ltd. [n.d.]. Digital RF Company Profile. https://assets.documentcloud.org/documents/810461/289-digitalrf-company-information-product-list.pdf

[34] Thanh Van Do, Hai Thanh Nguyen, Nikolov Momchil, and Van Thuan Do. 2015. *Detecting IMSI-Catcher Using Soft Computing.* Communications in Computer and Information Science, Vol. 545. Springer Singapore. 129–140 pages. https://doi.org/10.1007/978-981-287-936-3

[35] Van Thuan Do, Paal Engelstad, Boning Feng, and Thanh van Do. 2016. Strengthening Mobile Network Security Using Machine Learning. In *12th International Conference, MobiWis 2016,* Vol. 4. 173–183. https://doi.org/10.1007/978-3-319-

44215-0

[36] Elaman GmbH. [n.d.]. Governmental Security Solutions - Communications Monitoring Solutions. https://wikileaks.org/spyfiles/files/0/188$_2$01106-ISS-ELAMAN3.pdf

[37] Elkat Security Engineering Ltd. [n.d.]. EKMS 1700 - ELKAT GSM. https://assets.documentcloud.org/documents/810722/595-elkat-brochure-ekms-1700.pdf

[38] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. 2005. Exploiting open functionality in SMS-capable cellular networks. In *Proceedings of the 12th ACM conference on Computer and communications security - CCS '05*. ACM Press, 393. https://doi.org/10.1145/1102120.1102171

[39] Kaiming Fang and Guanhua Yan. 2018. *Emulation-Instrumented Fuzz Testing of 4G/LTE Android Mobile Devices Guided by Reinforcement Learning*. Lecture Notes in Computer Science, Vol. 11099. Springer International Publishing. 1–372 pages. https://doi.org/10.1007/978-3-319-98989-1$_2$

[40] Pierre-alain Fouque, Cristina Onete, and Benjamin Richard. 2016. Achieving Better Privacy for the 3GPP AKA Protocol. In *Privacy Enhancing Technologies Symposium*, Vol. 2016. 255–275. https://doi.org/10.1515/popets-2016-0039

[41] Dirk Fox. 2002. Der IMSI-catcher. *Datenschutz und Datensicherheit* 26, 4 (2002), 212–215.

[42] Fujian Helios Technologies. [n.d.]. About HELIOS. http://www.heliostelecom.com/about/show.php?id=188

[43] Gamma Group. [n.d.]. 3G-GSM Tactical Interception & Target Location. https://info.publicintelligence.net/Gamma-GSM.pdf

[44] Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In *19th Annual Network and Distributed System Security Symposium, NDSS.*

[45] Eithan Goldfarb. 2013. Systems and methods for identifying rogue base stations. European Patent App. EP20,130,165,913.

[46] Les Goldsmith. 2018. Real World Detection and Mitigation of IMSI Catchers. https://www.linkedin.com/pulse/real-world-detection-mitigation-imsi-catchers-les-goldsmith

[47] Jovan Dj. Golić. 1997. Cryptanalysis of Alleged A5 Stream Cipher. In *Advances in Cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques*, Walter Fumy (Ed.). Springer Berlin Heidelberg, 239–255. https://doi.org/10.1007/3-540-69053-0$_1$7

[48] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Douglas J. Leith. 2016. srsLTE: An Open-Source Platform for LTE Evolution and Experimentation. *CoRR* abs/1602.04629 (2016). http://arxiv.org/abs/1602.04629

[49] GSMK. [n.d.]. GSMK Cryptophone 500i. https://www.cryptophone.de/en/products/mobile/cp500i/.

[50] GSMK. [n.d.]. GSMK Cryptophone Baseband Firewall Technical Briefing. http://telephone-museum.org/wp-content/uploads/2014/12/GSMK-Baseband-Firewall-Technical-Briefing.pdf.

[51] GSMK. [n.d.]. GSMK Overwatch: IMSI Catcher Detection. https://www.gsmk.de/products/network-security/#overwatch.

[52] Harris Communications. [n.d.]. Gemini Quick Start Guide. https://assets.documentcloud.org/documents/3105793/Gemini-3-3-Quick-Start-Guide.pdf

[53] Harris Corporation. [n.d.]. Trademark registration for STINGRAY. http://tsdr.uspto.gov/documentviewer?caseId=sn76303503.

[54] Homeland Security Strategies Ltd. [n.d.]. Cell Catcher CC1900 3G. http://www.cellularintercept.com/media/pdf/cc1900$_3$g$_0$03.pdf

[55] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. 2018. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In *25th Annual Network and Distributed System Security Symposium, NDSS.*

[56] Yu Lun Huang, Chih Ya Shen, and Shiuhpyng Winston Shieh. 2011. S-AKA: A provable and secure authentication key agreement protocol for UMTS networks. *IEEE Transactions on Vehicular Technology* 60, 9 (2011), 4509–4519. https://doi.org/10.1109/TVT.2011.2168247

[57] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Proceedings of 2018 Network and Distributed System Security Symposium.* Internet Society. https://doi.org/10.14722/ndss.2018.23313

[58] Mohammed Shafiul Alam Khan and Chris J Mitchell. 2017. Trashing IMSI Catchers in Mobile Networks. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '17).* ACM, New York, NY, USA, 207–218. https://doi.org/10.1145/3098243.3098248

[59] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy (SP).*

[60] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. 2017. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (2017).

[61] Paul Maxwell Martin and Riki Benjamin Dolby. 2009. Acquiring identity parameter. US Patent App. 12/162,548.

[62] Paul Maxwell Martin and Riki Benjamin Dolby. 2010. Method and apparatus for forcing inter-RAT handover. US Patent App. 12/594,387.

[63] Meganet Corporation. [n.d.]. VME Undetectable Cell Phone Interceptors. http://www.meganet.com/meganet-products-cellphoneinterceptors.html

[64] Stig F Mjølsnes and Ruxandra F Olimid. 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. 235–246. https://doi.org/10.1007/978-3-319-65127-9$_1$9 arXiv:1702.04434

[65] Collin Mulliner, Nico Golde, and Jean-Pierre Seifert. 2011. SMS of Death: from analyzing to attacking mobile phones on a large scale. In *USENIX Security*. http://static.usenix.org/events/sec11/tech/full{˝papers/Mulliner.pdf

[66] Prajwol Kumar Nakarmi, Noamen Ben Henda, and Vlasios Tsiatsis. 2019. 3GPP Release 15: An end to the battle against false base stations? (2019). https://www.ericsson.com/en/blog/2019/1/3gpp-release15

[67] Prajwol Kumar Nakarmi and Karl Norrman. 2016. Detecting false base stations in mobile networks. https://www.ericsson.com/research-blog/detecting-false-base-stations-mobile-networks/

[68] Neosoft AG. [n.d.]. Catalogue. https://assets.documentcloud.org/documents/810502/945-neosoft-catalogue.pdf

[69] Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno. 2017. SeaGlass: Enabling City-Wide IMSI-Catcher Detection. *Proceedings on Privacy Enhancing Technologies* 2017, 3 (2017), 39–56.

[70] Karsten Nohl and Chris Paget. 2009. GSM - SRSLY? *CCC* (2009).

[71] Karl Norrman, Mats Näslund, and Elena Dubrova. 2016. Protecting IMSI and User Privacy in 5G Networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications (MobiMedia '16).* ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 159–166. http://dl.acm.org/citation.cfm?id=3021385.3021415

[72] Linus Nyman and Mikael Laakso. 2018. *Assembling your SeaGlass IMSI-catcher detector – a beginner's guide.* https://doi.org/10.5281/zenodo.1309994

[73] OMA. 2014. *Enabler Release Definition for Secure User Plane Location (SUPL).* Technical Report. Open Mobile Alliance.

[74] Osmocom Project. [n.d.]. Cellular Network Infrastructure. https://osmocom.org/projects/cellular-infrastructure/wiki

[75] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, Andrew Martin, and Jean-Pierre Seifert. 2017. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *11th USENIX Workshop on Offensive Technologies (WOOT 17).* USENIX Association.

[76] Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. 2018. Sonar: Detecting SS7 Redirection Attacks with Audio-Based Distance Bounding. In *2018 IEEE Symposium on Security and Privacy (SP).* IEEE, 567–582. https://doi.org/10.1109/SP.2018.00006

[77] PKI Electronic Intelligence GmbH. [n.d.]. Interception and Monitoring Systems. http://www.pki-electronic.com/wp-content/uploads/2012/08/3$_\mathrm{P}$KI$_\mathrm{I}$nterception$_\mathrm{a}$nd$_\mathrm{M}$onitoring$_\mathrm{S}$ystem$_2$017.pdf

[78] Andrew Paul Pridmore, Paul Maxwell Martin, and Riki Benjamin Dolby. 2015. Acquiring identity parameters by emulating base stations. US Patent 9,215,585.

[79] Privacy International. [n.d.]. Surveillance Industry Index. https://sii.transparencytoolkit.org

[80] Qualcomm. 2012. Bandwidth Support in LTE Standards. https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting71612/PANEL2.3-Gaal-Qualcomm.pdf

[81] Quanzhou Kingtone Optic and Electronic Technology Co., Ltd. [n.d.]. kingtone Successfully Attend The HongKong Global Sources Consumer Electronics Show at month October. http://www.kingtone.cc/m/newsshow.aspx?id=218

[82] Muhammad Taqi Raza, Fatima Muhammad Anwar, and Songwu Lu. 2018. Exposing LTE Security Weaknesses at Protocol Inter-layer, and Inter-radio Interactions. In *SecureComm*. 312–338. https://doi.org/10.1007/978-3-319-78813-5$_1$6

[83] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Pöpper. 2017. On Security Research Towards Future Mobile Network Generations. (oct 2017). arXiv:1710.08932 http://arxiv.org/abs/1710.08932

[84] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on Layer Two. In *2019 IEEE Symposium on Security and Privacy (SP).*

[85] SecUpwN. [n.d.]. Android IMSI-Catcher Detector. https://secupwn.github.io/Android-IMSI-Catcher-Detector/.

[86] Septier. [n.d.]. Septier IMSI Catcher. https://www.septier.com/product-item/septier-imsi-catcher/

[87] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. (2015). http://arxiv.org/abs/1510.07563

[88] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In *Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19).*

[89] Shogi Communications Ltd. [n.d.]. Semi Active GSM Monitoring System. https://assets.documentcloud.org/documents/409296/160-shogi-2006-semiactive-gsm-monitoring.pdf

[90] Trent Smith. 2017. Project Overwatch: Multi-National Effort to Combat IMSI Catchers.

[91] SRLabs. 2014. SnoopSnitch. https://opensource.srlabs.de/projects/snoopsnitch. [Online, accessed 01-12-2018].

[92] Simen Steig, Andre Aarnes, Thanh van Do, and Hai Thanh Nguyen. 2016. A Network Based IMSI Catcher Detection. In *2016 6th International Conference on IT Convergence and Security (ICITCS)*. IEEE, 1–6. https://doi.org/10.1109/ICITCS.2016.7740306

[93] Stratign FZCO. [n.d.]. Stratign GSM Monitoring System. https://assets.documentcloud.org/documents/810511/1172-stratign-product-description-gsm-monitoring.pdf

[94] Daehyun Strobel. 2007. IMSI-Catcher. (2007).

[95] Swapnil Udar and Ravishankar Borgaonkar. 2014. Understanding IMSI Privacy.

[96] Unwired Labs. [n.d.]. OpenCellID. https://www.opencellid.org

[97] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. 2015. Defeating IMSI Catchers. *CCS '15* (2015), 340–351. https://doi.org/10.1145/2810103.2813615

[98] Kenneth van Rijsbergen. 2016. The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF. *University of Amsterdam* (2016).

[99] Ash Wilson. 2016. SITCH: Situational Information from Telemetry and Correlated Heuristics. *DEF CON 24* (2016). https://sitch.io

[100] Muxiang Zhang. 2003. Provably-Secure Enhancement on 3GPP Authentication and Key Agreement Protocol. Cryptology ePrint Archive, Report 2003/092. https://eprint.iacr.org/2003/092.

[101] Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu, Zhenhua Li, and Yunhao Liu. 2018. FBSleuth: Fake Base Station Forensics via Radio Frequency Fingerprinting. *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (2018), 261–272. https://doi.org/10.1145/3196494.3196521