5GMap: User-Driven Audit of Access Security Configurations in Cellular Networks

Andrea Paci, Matteo Chiacchia, Giuseppe Bianchi
University of Rome "Tor Vergata" & CNIT Natl. Network Assurance & Monitoring LAB

***Abstract*—In the realm of cellular networks, security vulnerabilities often result from misconfigurations within their protective mechanisms. Typically, the responsibility for ensuring proper configuration and security checks lies with the network operator. The tool described in this paper, named 5GMap, aims to enable also legitimate subscribers in gaining insights into how data protection mechanisms are configured. By actively manipulating user device security settings during multiple processes of connection setup, and analyzing the relevant network responses, 5GMap enables auditing of the encryption and integrity protection algorithms set by the provider at both radio interface and Core Network access (NAS) protocol. 5GMap has been preliminary assessed over three out of the four major Italian operators, revealing instances where customers could not only negotiate "null" encryption but also where, for two of the three audited operators, "null" encryption was the only current option configured at the NAS layer.**

I. Introduction

Over the last four decades, personal communication systems have evolved dramatically, with mobile telephony and data communication tightly integrated in our smartphone applications playing a pivotal role in our lives. This surge in technology usage, both personally and in businesses, underscores the crucial importance of addressing security and privacy concerns.

Research in the field has unveiled numerous vulnerabilities in mobile communications, spanning confidentiality breaches, encryption weaknesses and protocol gaps exploited by attackers [1]–[4]. While the absence of protection in the first cellular network generation and naive security design in GSM systems were the root causes of early security and privacy concerns, modern cellular network generations have systematically improved security. This progress includes the adoption of more robust cryptographic algorithms since 3G and the implementation of a comprehensive security architecture since 4G.

Unsurprisingly, and apart from a few notable exceptions like [5] that exploited a severe design flaw (now corrected since Release 15), most recent attacks documented by the research community target the implementation or (mis)configuration of protection mechanisms within the network architecture and deployments.

This work was partially supported by the EU under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership "Telecommunications of the Future" (PE00000001 - program "RESTART") and "SEcurity and RIghts In the CyberSpace" (PE00000014 - program "SERICS").

Often, vulnerable configurations, which may eventually account also for the disabling of whole security features, are the result of learned risk-based or cost-based decisions. For a striking example, the absence of integrity protection until the 4G/LTE specification (included) was a deliberate 3GPP choice, primarily motivated by concerns about the extra overhead it would impose on the radio layer. It is only since 5G that such a decision was changed, perhaps in part also motivated by the emergence of practical attack scenarios [4] demonstrating how lack of integrity could be effectively exploited in real-world scenarios.

But perhaps more often, misconfigurations can unexpectedly occur and may stem from various sources, such as human errors, misinterpretations of security guidelines, or simply the improper application of 3GPP standard rules which, in some cases, are affected by a significant degree of looseness and optionality, as a recent thorough report from ENISA duly analyzes and highlights [6][1]. Misconfigurations become particularly critical when paired with a limited visibility of security configurations, i.e., when there's no clear way to monitor and confirm the status of security measures set forth.

The research presented in this paper centers on a motivating question: Besides the operator, who else should have the capability to monitor and confirm security settings within a cellular network and evaluate the adequacy of the protection offered? While it's evident that this responsibility does not fall within the domain of the average user, we argue that, motivated by the principles of transparency and self-assurance, a tech-savvy consumer should have the means to acquire this knowledge. Specifically, she should be able to verify the specific security settings that can be configured for her connectivity. This issue has been tackled on other consumer-related protocols already, yet it remains unresolved on cellular networks.

To fulfill this goal, this paper introduces 5GMap, a tool designed to enable users to conduct a range of assessments, with a specific focus on verifying the protection measures in their network connections. 5GMap is designed to assess

[1]As an enlightening example of how loose a specification might ultimately be, let's directly quote an example from the ENISA report on page 24: [in clause 5.3.9 of the 3GPP security specifications TS 33.501] there is a requirement regarding 5G that says that "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane*", there is also a NOTE which says: "*The above requirements allow to have F1-U protected differently (including turning integrity and/or encryption off or on for F1-U) from all other traffic on the CU-DU (e.g. the traffic over F1-C)*".

ISBN: 978-3-903176-61-4

© 2024 International Federation for Information Processing (IFIP).
ISBN: 978-3-903176-61-4

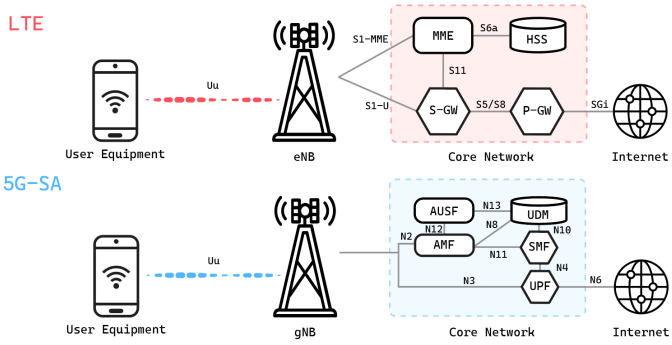

Fig. 1: 4G/5G Network Architecture.

security parameters within operational cellular networks (either LTE and 5G) and uncover instances of misconfiguration. Through an active methodology, 5GMap actively manipulates the security settings of the user device during connection to gauge the network's response and tolerance.

In this preliminary work, our emphasis mainly lies on the network selection of the encryption and integrity algorithms, and on the relevant possibility of downgrade attack conditions. However, as described in section III, 5GMap is already engineered to permit the exploration of a larger space of configuration parameters.

To assess the effectiveness of 5GMap, we acquired commercial SIM cards and connected as regular subscribers to three out of the four primary operators in Italy. In our tests, we assessed the way in which these operators support encryption and integrity on two specific layers: access stratum (i.e. PDCP/RRC layers) as well as Non-Access Stratum (NAS layer). Experimental findings are quite interesting, and demonstrate that "null" encryption not only can be negotiated by the customer, but in some cases, and specifically for two out of the three operators audited, is the only current option configured at the NAS layer.

The rest of the paper is organized as follows. Section II offers an overview of LTE and 5G network architecture, including secure communication setup. Section III outlines 5GMap's objectives and methodology. Sections IV and V detail design decisions and implementation choices. In Section VI, we present experiments and outcomes. Related work is discussed in Section VII. Finally, Section VIII draws conclusions and discusses open issues and future work.

II. Background

In this section we provide a background on *4G LTE* and *5G New Radio* architectures (Fig. 1 and Section II-A), with emphasis on the protocol stack (Section II-B) and especially on the *Attach Procedure* (Section II-C), i.e., the procedure responsibile to establish a secure communication.

A. 4G & 5G Network Architectures

The development of the various generations of mobile networks adheres to the technical specifications outlined by 3GPP, a consortium responsible for standardizing design, protocol specifications, and security aspects to facilitate global coordination among various technology manufacturers and mobile service providers [7]. The mobile network, and more specifically 4G and 5G networks, consists of three main components: the **User Equipment** (UE), the **Base Station** (BS), and the **Core Network** (CN)[2].

User Equipment (UE). The UE, a device at the user end, comes equipped with a Universal Subscriber Identity Module (USIM), a critical component that contains the *user credentials* to access the network (user identifiers, master secret key, etc.). These elements are crucial for mutual Authentication and Key Agreement (AKA) between the user and the network. Common UEs include cell phones, tablet computers, and IoT devices with cellular connectivity.

eNodeB. In the 4G architecture, the eNodeB (eNB) acts as the base station or mobile network tower. It serves as an intermediary in establishing and maintaining connections, implementing the Radio Resource Control (RRC) and lower layers.

gNodeB. The gNodeB (gNB), also known as the Next-Generation NodeB, is an upgraded version of the eNodeB responsible for transmitting and receiving signals to and from the UE in a 5G Network.

4G Core Network. The 4G Core Network (also known as Evolved Packet Core) architecture includes key components such as the Home Subscriber Server (HSS), responsible for user authentication and authorization, the Packet Data Network (PDN) Gateway (P-GW), providing access to external IP networks, the Serving Gateway (S-GW), routing data between the base station and the PDN gateway, and the Mobility Management Entity (MME), central for user management. It facilitates two-way authentication for the UE, chooses security algorithms, and monitors user locations.

5G Core Network. The 5G Core Network includes various functional components like the Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), Authentication Server Function (AUSF), and more. The the core network elements in 4G and 5G, despite having different labels, are comparable in their roles and responsibilities.

B. Protocol Stack

The LTE and 5G technologies encompass a complex protocol stack (Figure 2) that defines the rules and protocols for the transmission and reception of data between mobile devices and network infrastructures.

The three lower layers are not of specific interest for what concerns security configuration. On the air interface, the

[2]The transition from 4G to 5G networks brings many benefits, but it does not affect the main features that are relevant for this study. Therefore, we describe both 4G and 5G networks without differentiating their protocol behavior.

ISBN: 978-3-903176-61-4

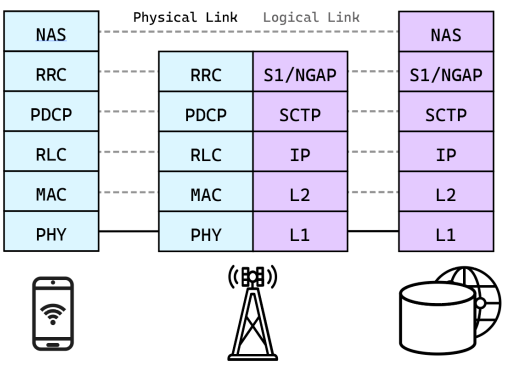

Fig. 2: 4G/5G Network Stack.

Physical layer handles radio signals and enables stable UE to eNB/gNB communication through diverse channels. The **Medium Access Control (MAC)** Orchestrates radio resource access managing channel multiplexing and demultiplexing, differentiates UEs in the same cell using identifiers (RNTI) acquired through a Random Access Procedure [8], and ensures reliability. The **Radio Link Control (RLC)** segments and reassembles packets to/from the PDCP sublayer, oversees packet retransmission, and offers different transmission modes (Transparent Mode (TM), Acknowledged Mode (AM), and Unacknowledged Mode (UM) [9]).

Security configurations instead take place and influence the upper layers in the protocol stack. These layers are briefly described in what follows.

Packet Data Convergence Protocol (PDCP): The primary role of the PDCP sublayer revolves around ensuring the Access Stratum (AS) security functions. Precisely, it delivers encryption and integrity protection for control and/or data plane messages. The PDCP protocol offers a variety of functionalities to better such as improving data rate efficency (i.e. Robust Header Compression), facilitate Handover procedures and orders received *Packet Data Units* (PDU) [10].

Radio Resource Control (RRC): As implied by its name, primarily oversees radio session management and radio bearer control within the LTE/5G protocol stack. This includes tasks such as initiating, sustaining, and terminating radio sessions. The RRC protocol is responsible for managing UE radio measurements, Access Stratum (AS) session key agreements, transparent transmission of Non-Access Stratum (NAS) messages, and other relevant functions [11]. It's noteworthy that while RRC messages are encrypted and integrity protected, messages exchanged before the AS security activation may be transmitted without any protection.

Non-Access Stratum (NAS): This layer serves as the endpoint for control plane signaling messages and it is used for the communication between the UE and the Core Network. The NAS protocol is dedicated to managing the mobility and sessions of User Equipment (UE). Its responsibilities encompass user identification, authentication, and security control through the *Autentication and Key Agreement*(AKA) protocol.

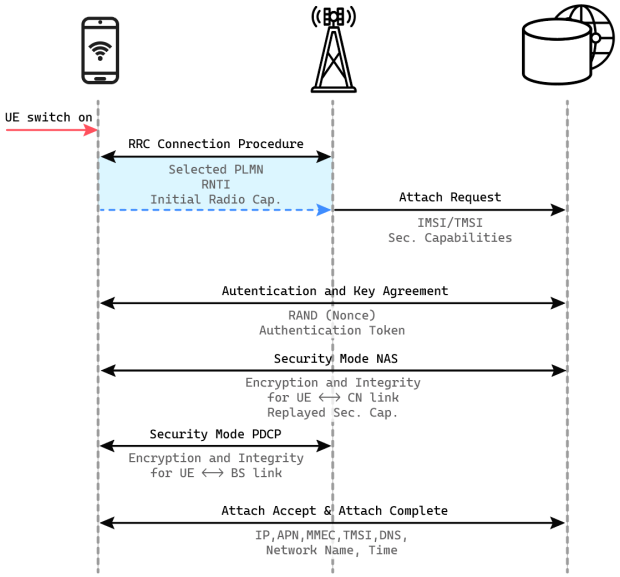

Fig. 3: 4G/5G Attach Procedure.

Additionally, the NAS sublayer handles tasks such as updating the UE's tracking area location, facilitating network-originated paging processes, and assigning temporary network identifiers and IP addresses. Security features provided by the NAS sublayer include *mandatory integrity protection and optional encryption for NAS signaling messages* [12], [13].

C. Security Procedures

Security of Mobile Networks rely on multiple mechanism in order to guarantee confidentiality and autenticity to its end user. Among those mechanism there are Mutual Authentication, Anti-Replay protection, Public Key Infrastructure and Encryption/Integrity. All of these mechanism have to function correctly or even if one of these mechanism fail, the whole security of the system is compromised. Since this preliminary work focuses on Encryption and Integrity, this section will delve into Encryption and Integrity algorithms and how they are negotiated during the *Attach Procedure*.

Once an RRC Connection is established with the Base Station, the user initiates the Attach Procedure by communicating with the Core Network, particularly with the MME, exchanging control messages. In the "Attach Request" message, the UE identifies itself by sending the IMSI or the TMSI and includes the *UE Capabilities* (i.e. the encryption/integrity algorithms supported by the device connecting to the network and other radio access parameters). The subsequent Authentication and Key Agreement (AKA) establishes mutual authentication and guarantees that the user is connection to a legitimate Base Station/Core Network: The MME dispatches an Authentication Request carrying a random nonce and an authentication token. The UE verifies the authentication token, computes the RES and packs it in the Authentication Response, which is then validated by the network. To enable the security mechanisms, the Core Network transmits the NAS Security Mode

ISBN: 978-3-903176-61-4

Command, which is integrity protected, indicating the selected security algorithms to be used for NAS layer messages, along with the replay of the original UE Security Capabilities to prevent algorithm downgrade attacks [3]. The UE confirms with a Security Mode Complete. Similar to this, the eNB (or gNB) transmits an RRC Security Mode Command message to the UE, specifying the encryption and integrity algorithms to be used at the PDCP layer[3], and subsequently awaits an RRC Security Mode Complete message from the UE. In the concluding steps, the network allocates an IP address to the UE, incorporating it into the Attach Accept, and the UE verifies this assignment by sending an Attach Complete, finalizing the establishment of the connection.

LTE and 5G support many encryption and integrity protection algorithms [14] known as EPS Encryption Algorithm (EEA) and EPS Integrity Algorithm (EIA) for LTE and NR Encryption Algorithm (NEA) and NR Integrity Algorithm (NIA) for 5G. The most commonly used and widely supported algorithm are the one shown in Table I. EIA1 and EEA1 operate with the Snow3G cipher, while EIA2 and EEA2 rely on AES. Every UE, eNB, and Core is mandated to support both Snow3G and AES. A subsequent LTE version introduces optional support for ZUC (EIA3, EEA3). The null algorithms EIA0/NIA0 and EEA0/NEA0 are used respectively for null integrity and null encryption. While protecting the integrity of the signaling plane is mandatory during normal operation, encryption remains optional but highly recommended [14].

III. Approach

While the long-term objective is to explore the whole configuration of the cellular networks, in this work we focus in exploring the supported security (encryption and integrity) algorithms employed by the Base Station and Core Network of different operators. Along with the security configuration, the tool we aim to devolop has to be capable of collecting various cell information, including crucial identification values like MCC, MNC, TAC, and CellID.

We sought to confirm whether these entities truly supported encryption and integrity, and also to observe the network's response under specific challenging situations. Since direct physical access to the Base Station and Core Network is not feasible, we simulate the role of a regular user, executing various attach procedures and querying the network to gather these informations.

To conduct this verification, it is essential to carefully examine the messages transmitted between the UE, the Base Station and the Core Network. In particular, we must focus on two key types of messages:

- *RRC Messages*: These messages are fundamental for configuring communication with the Base Station. Through the analysis of RRC messages, we can identify the security algorithms supported by the base station and evaluate those actually chosen during communication.

[3]AS and NAS are not compelled to select the same algorithms.

TABLE I: Mobile Security Algorithms

Algorithm	Type
EEA0/NEA0 EIA0/NIA0	Null
128-EEA1/NEA1 128-EIA1/NIA1	Snow3G
128-EEA2/NEA2 128-EIA2/NIA2	AES
128-EEA3/NEA3 128-EIA3/NIA3	ZUC

- *NAS Messages*: These messages are central to the communication between the UE and the Core Network. By analyzing NAS messages, we can determine which security algorithms are supported by the CN and which are preferred during security negotiation.

We have sought to make the application as automate as possible, allowing it to control the UE by initiating it, modifying some of its configuration parameters, extracting and analyzing the information, disconnecting the UE, changing its configurations, and re-executing the procedure to observe how the mobile network behaves and to provide a summary analysis of what the framework has been able to extract. During the algorithm negotiation phase within the attach procedure, the UE reports its supported algorithms through the capabilities sent in the attach request message. Both the Base Station and Core Network select two of these algorithms (one for encryption and one for integrity) based on their availability.

A. Methodology

In order to gain a comprehensive understanding of the supported algorithms, we employ an active approach that entails conducting a series of iterations. Each iteration involves distinct attach procedures and configurations, including the use of null encryption (or integrity) alongside specific algorithms. The reason why it is necessary to establish multiple connection to gather all the supported security algorithms is described in Section II-C: since it is the network that selects the security algorithms based ones supported by the user, it is necessary to iterate multiple attach procedure with different security capabilities ans closely monitor the responses of the Base Station and the Core Network in each scenario. This process is repeated until a comprehensive mapping of all the algorithms is achieved. Moreover, we aim to verify the feasibility of establishing insecure communication, specifically without utilizing any security algorithms, thus allowing us to observe network behavior in these particular scenarios. To obtain the algorithms, we need to retrieve the Security Mode Commands from both the RRC and NAS messages and analyze the algorithms sent by the network.

To ensure that each iteration is independent of previous ones and does not rely on data previously stored by the operator, the tool has to perform attach procedures using the International Mobile Subscriber Identity (IMSI), avoiding the use of the Temporary Mobile Subscriber Identity (TMSI). This is crucial to ensure that the information exchange is as comprehensive as possible.

ISBN: 978-3-903176-61-4

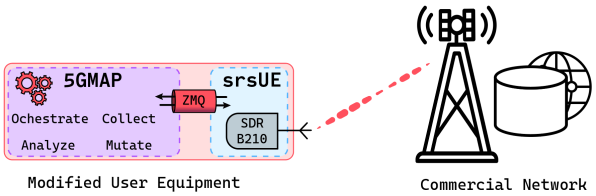

Fig. 4: 5GMap Architecture.

IV. Design

Since Commercial User Equipment don't offer the possibility to thinker with the inner functionalities of the protocol and to inject/manipulate message flow, it is required to design an architecture that simulates the UE protocol stack and is capable to interact with a radio frontend to send and receive signal from real Base Stations. To establish the radio connection with a real Base Station, the setup involved the use the following equipment:

- **Software Defined Radio USRP B210**: A type of software-defined radio (SDR) that provides a flexible platform for designing, prototyping, and deploying wireless communication systems. It is capable of transmitting and receiving a wide range of radio signals, making it suitable for various applications [15].
- **SIM Card Reader with real SIM**: Security algorithms are transmitted within the Security Mode Command, which comes after the *authentication phase*. Therefore, to access these algorithms and retrieve them it is necessary to pass the authentication phase as a legitimate user [16].
- **Workstation Laptop**: Signal processing and protocol implementation is done on a off-the-shelf computer. The decoding/encoding of the radio spectrum can be a demanding operation with general purpose hardware. To compensate such limit, a laptop with adequate performance is required. Along with it, a proper tuning of the OS helps to ensure the processing stays within the time window allowed for resource block processing. For protocol implementation of both 4G and 5G we use *srsUE*, one of the tool offered by the srsRAN software suite [17][4], to impersonate the UE and retrieve the data of interest. srsUE implements all the protocols and procedures that compose a proper User Equipment, in both 4G and 5G scenarios.

It is crucial to note that while 5GMap was primarily tested on LTE networks, it is highly adaptable and can be easily tailored to operate on 5G networks. The decision to initially test it on an LTE network was motivated by several factors:

- *Infrastructure Availability*: LTE networks are more widely available and accessible compared to 5G networks, enabling easier access to a real LTE base station for testing purposes.
- *Relevance of LTE Testing*: Given that LTE technology is a widely used and established communication standard, testing the software on an LTE network is still relevant. This validation helped showcase the software's effectiveness in a significant context.
- *Gradual Transition*: The transition from LTE to 5G networks is a gradual process. Conducting initial software testing on 4G networks ensured compatibility and stability on a solid technological foundation before tackling the complexities of 5G networks.

A summary of the design can be seen in Figure 4.

V. Implementation

In the following chapter, we will explore the implementation choices, providing a detailed insight into the decisions made.

A. Hook

In order to force specific behaviours and retrieve the desired information sent from the Base Station, we properly modified the source code of srsRAN and added code snippets, known as "*hooks*", that enable the extraction of exchaged messages between the UE and the BS. Through these hooks, messages exchanged in regular mobile communication are directed toward 5GMap by establishing a communication bridge with srsue.

After a careful study of 4G and 5G protocols, it was made the decision made to insert the hooks at the following points:

- The MIB, carried by the PBCH (Physical Broadcast Channel), is managed through the handle present in the dedicated control flow for this channel. The hook is inserted into this handle, specifically after the process of decoding the data contained in the packet.
- SIB1, SIB2, and SIB3 are RRC messages, The hooks were inserted into thefunctions that individually handled each SIBs.
- To retrieve RRC messages, it was made the decision insert the hook at the PDCP level as this layer acts as a connection point for all upper layers.
- Each NAS message is associated with its dedicated handler, and therefore the hooks are inserted within these specific handlers.

For the last two types of messages (RRC and NAS) hooks, they have to be inserted at two distinct points, one for *uplink* messages and one for *downlink* messages and the decoding phase is done in 5GMap directly. [5]

To establish a communication channel between the hook and 5GMap, the ZMQ library [18] has been employed, implementing the inter-process ordered Request-Reply pattern.

Since the 5GMap is capable of extracting messages related to radio synchronization as well as those exchanged during the attach procedure, it can be configured to retrieve other types of parameters that are not directly exchanged in RRC Messages. An example is the Physical Cell ID, a parameter

[4]The srsRAN software suite is an open-source collection of 4G and 5G software radio implementations from SRS. srsRAN is designed to serve as a development framework for researching and implementing software-based radio solutions in mobile communication networks.

[5]In UL, messages are retrived before the encryption, and in DL after the decryption

ISBN: 978-3-903176-61-4

that is exchanged with the Primary synchronization signal (PSS) and Secondary synchronization signal (SSS). In our case study, we focused on security configuration parameters and cell identification parameters.

B. Experimental setup

Once the setup outlined in section IV has been completed, we developed a process to successfully establish a radio connection to a real network.

This procedure consists of the following phases:

1) *Verification of available frequencies*: Network Signal Guru [19] is used on an Android device to check frequencies of the avaliable cells of the chosen network operator in the area. From the list, the EARFCN (E-UTRA Absolute Radio Frequency Channel Number) that returns the highest Signal-to-Noise Ratio (SNR) value is selected.
2) *Signal quality verification*: To assess the actual quality of the signal received by the SDR, various operations are performed. Firstly, the "*uhd_fft*" command, part of the GNU Radio suite [20], is executed to manually evaluate the spectrogram of the received signal. Subsequently, "*cell_search*" and "*pdsch_ue*" executables, part of the srsRAN example scripts, are executed. The former is used to determine if the SDR can detect cell and syncronize with it, while the latter, among other factors, reports the Block Error Rate (BLER) of the received signal.
3) *Modification of the ue.conf configuration file*: The srsue configuration file is properly modified to reflect the cell configuration parameters gathered in the previous steps: EARFCN, Access Point Name (APN) and Gains. Other required changes include updating Radio Frontend driver to enable the connection with the USRP B210, setting the "USIM mode" to "pcsc" in order to enable the usage of the SIM Reader with the legitimate SIM of the chosen network operator [16], and eventually, as mentioned in section III-A, enforcing the use of IMSI for every attach procedure. Finally, we tuned SDR parameters to maximize device performance and ensure optimal reception and transmission of radio signals.
4) *Execution of 5GMap and data collection*: Once all the steps before are correctly carried out, 5GMap is executed. After 5GMap has finished all its iteration, it is shown a summary of the results.

Since 5GMap only needs the exchange of few messages to gather all the information it needs, there is no need to ensure a high throughput and highly reliable connection, partly achieved with features like MIMO and Automatic Gain Control. Those features provided a more unstable connection, and as a consequence they have been disabled by lowering the *UE Category*.

VI. Results

We conducted experiments on real networks using the 5GMap, and in this section, we will outline the types of experiments conducted and present the preliminary results obtained.

A. Experiments

We performed experiments in various areas of the city of Rome, connecting to three different operators and testing two different Tracking Area Codes (TACs) for each of them. To ensure privacy, we will refer to the operators as "Operator 1", "Operator 2" and "Operator 3". The 5GMap was developed to extract the security algorithms supported by Base Stations and Core Networks. Additionally, it was employed to determine the default algorithms chosen by these entities. This involved including support for all security algorithms in the capabilities to ascertain which algorithms Base Stations and Core Networks would choose by default if the selection were complete. In this manner, we created tables representing this information. Furthermore, we examined how the system behaves in certain edge cases:

- Whether a connection is established or not when only the null encryption or integrity algorithm is included in the capabilities.
- Whether a connection is established or not when the capabilities include the null encryption (or integrity) algorithm along with an algorithm that seems to be unsupported by the Base Station and/or Core Network. The goal is to verify if the network establishes a connection even when it cannot support the security requested by the user.

We have successfully created a comprehensive mapping of the supported algorithms in both the AS (Access Stratum) (Table II) and the NAS (Non-Access Stratum) (Table III) by these three operators.

B. Discussion

Our tests have revealed some differences in algorithm choices among the various operators examined. In particular, it has been observed that two out of three operators appear to exhibit no support for any NAS-level encryption algorithm.

Regarding differences in configurations among different physicall cells, this experiment has shown that the analyzed cells are configured with the same security parameters. It is worth noting that those cells are located in an higly urbanized area and are quite near to each other.

In addition, we have observed variations in default algorithm choices depending on the operator, highlighting the effective diversity in network configurations and/or vendor of equipment. It is noteworthy that the same two operators, lacking support for NAS-level encryption, accept establishing an unencrypted connection when the user includes only EEA0 in the capabilities, or when the user include EEA0 and a non-supported algorithm.

In specific instances, the UE incorporates a cryptographic algorithm pair within its capabilities, consisting of a null algorithm and one unsupported by the tested BS and Core Networks. Consequently, these entities establish an unencrypted connection, notwithstanding the user's explicit specification of support for certain encryption algorithms. In contrast, the third

ISBN: 978-3-903176-61-4

TABLE II: AS supported algorithms

	EEA0	EEA1	EEA2	EEA3
Operator 1	✓	✓	✓	
Operator 2	✓	✓	✓	
Operator 3		✓	✓	
	EIA0	**EIA1**	**EIA2**	**EIA3**
Operator 1		✓	✓	
Operator 2		✓	✓	
Operator 3		✓	✓	

Supported ✓, Preferred ✓

TABLE III: NAS supported algorithms

	EEA0	EEA1	EEA2	EEA3
Operator 1	✓			
Operator 2	✓			
Operator 3		✓	✓	
	EIA0	**EIA1**	**EIA2**	**EIA3**
Operator 1		✓	✓	
Operator 2		✓	✓	
Operator 3		✓	✓	

Supported ✓, Preferred ✓

operator, under the same conditions, responds with an Attach Reject, always ensuring user confidentiality.

Another significant aspect that has emerged is that all the examined operators do not appear to support null integrity, or at least, they never activate it during the establishment of regular communication, i.e., non-emergency scenarios.

In addition to the critical security algorithms that are negotiated during the attach request, we have observed other differences among different operators, such as:

- The Attach Reject message due to unsupported security capabilities had different cause values for different operators.
- The Access Point Name was mandatory for some operators, but optional for others.
- Some cells only allowed the UE to connect with the cause ”Mobile Originating Signaling” instead of the appropriate ”Mobile Originating Data”.
- Some networks sent an *EMM Information* message at the end of the Attach Request procedure, containing Network Name, Date, Time, Timezone and other information.

These differences, which are not related to security configuration, can be used to identify and cluster Base Station/Core Network manufactured by different vendors.

VII. Related Work

Since the inception of LTE and now with the emergence of 5G, research into the security of cellular network protocols has surged. On one side, formal approaches have been utilized for the security and privacy analysis of 4G/5G protocols. These methods ensure rigorous verification and validation, and often provide insights into potentially exploitable weaknesses - for instance, the potential to track users despite 5G's IMSI encryption, recently demonstrated in [21], builds upon a linkability issue initially revealed by [22] through the formal analysis of the 5G-AKA protocol.

On the other side, implementations invariably widen the scope of potential threats, demanding practical methods like fuzzing [23] to uncover vulnerabilities. Fuzzing methods specifically devised for 5G systems require the generation of data patterns and protocol messages tailored to the specificities of 5G protocols [24]–[26]. Furthermore, since access to the source code is frequently restricted, fuzzing methods must be formulated as black-box tests, capable of operating remotely or even through the air interface [27], [28].

With respect to the above methods, our approach is orthogonal, as we offer a tool that comprehensively identifies supported ciphersuites and default configurations. Our goal is to uncover (mis)configuration issues rather than focusing on design or implementation flaws. When it comes to the methodology for conducting tests the execution of certain tasks might require a special role. For instance, the execution of most of the 3GPP standard security assurance (SCAS) tests mandates direct access to the network function under examination. This access is only feasible within the core network infrastructure itself or within its suitable replica in a testing platform [29].

On the other side, testing UEs ”just” requires to program a suitable ”fake” base station to which UEs can be connected and then exposed to spoofed protocol messages to observe their reaction [30], [31].

In our specific scenario, testing the operator's access network mandates access credentials, specifically a valid SIM card. The feasibility of integrating a commercial SIM into an SDR-based UE was first provided by [32], a paper which appears closest to our work due to a similar testing methodology. However, our approach differs in three key aspects. First, our implementation choices and tools are different[6]. Second, our objective is to comprehensively explore and report the entire configuration space. This entails mapping all algorithms supported by networks and identifying the default usage (in both the Access Spectrum and Non-Access Spectrum), rather than merely verifying the network's support for null encryption/integrity. Third, and perhaps most importantly, while in this preliminary work we concentrate on ciphersuite negotiation, 5GMap is already designed to readily expand its scope to retrieve a multitude of potential parameters and configurations exchanged between UEs and Base Stations or the Core Network. Additionally, 5GMap is also ready to test 5G-SA networks, although we haven't done so yet due to the unavailability of deployments in our region.

[6]Among the reasons, one is that were unfortunately unaware of this work when we started the development of 5Gmap

ISBN: 978-3-903176-61-4

VIII. Conclusions

The tool introduced in this paper, 5GMap, is motivated by the opportunity of providing tech-savvy users with means to access detailed insights into the security configurations of the access networks they are connected to.

In the current preliminary version, 5GMap allows users to audit encryption and protection mechanisms by actively manipulating connection setup requests and analyzing network responses during connection setup. However, 5Gmap is already designed to incorporate in future releases a broader range of access network configuration parameters beyond just security aspects. While the extension of 5GMap's capabilities in terms of configuration gathering is our current focus, an open challenge is whether our active probing methodology may be ported on commercial devices.

Initial assessments on major Italian operators revealed concerning instances of "null" encryption at the NAS layer, being the only configured option for two out of the three tested. As per responsible disclosure, some involved operators have been informed by our findings and at the time of writing are making their internal controls.

We plan to further improve 5GMap with the following features, in order to allow a finer-grained study of 4G/5G cellular networks:

- Gather other relevant information exchanged during the Attach Procedure: MME/AMF Code, IP Subnet, Roaming capability, DNS addresses, preferred 5G NSA/SA capabilities.
- Test impromper usage of security related procedure: IV/RAND Generation, TMSI randomicity, Emergency registration.
- Test improper network configuration: Open services in the cellular subnet, DNS Caching (DNS Poisoning).

Moreover, we intend to extend this research with more scenarios:

- Test configuration among cells belonging to different Tracking Area Codes, MME/AMF Code and geographical region
- Evaluate whether in particularly crowded events (i.e. concerts, sport matches, etc.) security configuration get "relaxed" in order to guarantee a higher throughput
- Test against virtual operators

References

[1] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4g/5g air interface security: A survey of existing attacks on different lte layers," *Computer Networks*, vol. 201, p. 108532, 2021.

[2] B. Karakoc, N. Fürste, D. Rupprecht, and K. Kohls, "Never let me down again: Bidding-down attacks and mitigations in 5g and 4g," WiSec '23, p. 97–108, 2023.

[3] R. Zhang, W. Zhou, and H. Hu, "Towards 5g security analysis against null security algorithms used in normal communication," *Security and Communication Networks*, vol. 2021, 10 2021.

[4] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking lte on layer two," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121–1136, IEEE, 2019.

[5] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4g and 5g cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, p. 221–231, 2019.

[6] ENISA, "Security in 5g specifications, controls in 3gpp security specifications (5g sa)," 2021. Accessed on November 4, 2023.

[7] P. Moorhead, "Why 3gpp just works – multiple generations of global cellular standards and solid execution," September 9 2021.

[8] 3GPP, "Medium access control (mac) protocol specification, release 15," 2019. Accessed on November 2, 2023.

[9] 3GPP, "Radio link control (rlc) protocol specification, release 15," 2018. Accessed on October 27, 2023.

[10] 3GPP, "Packet data convergence protocol (pdcp) specification, release 15," 2018. Accessed on October 15, 2023.

[11] 3GPP, "Radio resource control (rrc) protocol specification, release 15," 2019. Accessed on October 29, 2023.

[12] 3GPP, "Non-access-stratum (nas) protocol for 5g system," 2018. Accessed on November 4, 2023.

[13] 3GPP, "Evolved universal terrestrial radio access network (e-utran), s1 application protocol (s1ap)," 2014. Accessed on October 28, 2023.

[14] 3GPP, "Security architecture and procedures for 5g system," 2018. Accessed on November 5, 2023.

[15] E. Research, "Usrp b210 overview." Accessed on November 9, 2023.

[16] L. Rousseau, "pcsc-tools: Tools for testing PC/SC functions of smart cards and readers." https://github.com/LudovicRousseau/pcsc-tools. Accessed on November 3, 2023.

[17] SRS, "srsRAN_4G: An Open Source 4G LTE and 5G NR Software Radio Implementation." https://github.com/srsran/srsRAN_4G. Accessed: 2023.

[18] "ZeroMQ." https://github.com/zeromq. Accessed: 2023.

[19] Q. Technologies, "Network signal guru," 2023.

[20] "Gnu radio." Accessed on November 11, 2023.

[21] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, "5g suci-catchers: Still catching them all?," in *Proc. 14th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, pp. 359–364, 2021.

[22] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 1383–1396, 2018.

[23] B. Miller, L. Fredriksen, and B. So, "An empirical study of the reliability of unix utilities.," *Commun. ACM*, vol. 33, pp. 32–44, 12 1990.

[24] D. Rupprecht, K. Jansen, and C. Pöpper, "Putting {LTE} security functions to the test: A framework to evaluate implementation correctness," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.

[25] I. Karim, S. R. Hussain, and E. Bertino, "Prochecker: An automated security and privacy analysis framework for 4g lte protocol implementations," in *2021 IEEE 41st Int. Conf. on Distributed Computing Systems (ICDCS)*, pp. 773–785, IEEE, 2021.

[26] C. Park, S. Bae, B. Oh, J. Lee, E. Lee, I. Yun, and Y. Kim, "{DoLTEst}: In-depth downlink negative testing framework for {LTE} devices," in *31st USENIX Security Symp. (USENIX Security 22)*, pp. 1325–1342, 2022.

[27] M. E. Garbelini, Z. Shang, S. Chattopadhyay, S. Sun, and E. Kurniawan, "Towards automated fuzzing of 4g/5g protocol implementations over the air," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 86–92, IEEE, 2022.

[28] H. Wang, B. Cui, W. Yang, J. Cui, L. Su, and L. Sun, "An automated vulnerability detection method for the 5g rrc protocol based on fuzzing," in *4th Int. Conf. on Advances in Computer Technology, Information Science and Communications (CTISC)*, IEEE, 2022.

[29] F. Mancini and G. Bianchi, "Scasdk-a development kit for security assurance test in multi-network-function 5g," in *Proc. 18th Int. Conf. on Availability, Reliability and Security*, pp. 1–8, 2023.

[30] E. Bitsikas, S. Khandker, A. Salous, A. Ranganathan, R. Piqueras Jover, and C. Pöpper, "Ue security reloaded: Developing a 5g standalone user-side security testing framework," in *Proc. 16th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, pp. 121–132, 2023.

[31] C. Yu, S. Chen, Z. Wei, and F. Wang, "Secchecker: Inspecting the security implementation of 5g commercial off-the-shelf (cots) mobile devices," *Computers & Security*, p. 103361, 2023.

[32] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "Lte security disabled: misconfiguration in commercial networks," in *Proc. 12th conf. on security and privacy in wireless and mobile networks*, pp. 261–266, 2019.

ISBN: 978-3-903176-61-4