On Security Research towards Future Mobile Network Generations

David Rupprecht*, Adrian Dabrowski*, Thorsten Holz, Edgar Weippl, and Christina Pöpper

***Abstract*—Over the last decades, numerous security and privacy issues in all three active mobile network generations have been revealed that threaten users as well as network providers. In view of the newest generation (5G) currently under development, we now have the unique opportunity to identify research directions for the next generation based on existing security and privacy issues as well as already proposed defenses. This paper aims to unify security knowledge on mobile phone networks into a comprehensive overview and to derive pressing open research questions. To achieve this systematically, we develop a methodology that categorizes known attacks by their aim, proposed defenses, underlying causes, and root causes. Further, we assess the impact and the efficacy of each attack and defense. We then apply this methodology to existing literature on attacks and defenses in all three network generations. By doing so, we identify ten causes and four root causes for attacks.**

Mapping the attacks to proposed defenses and suggestions for the 5G specification enables us to uncover open research questions and challenges for the development of next-generation mobile networks. The problems of unsecured pre-authentication traffic and jamming attacks exist across all three mobile generations. They should be addressed in the future, in particular to wipe out the class of downgrade attacks and, thereby, strengthen the users' privacy. Further advances are needed in the areas of inter-operator protocols as well as secure baseband implementations. Mitigations against signal denial-of-service attacks by smart protocol also design represent open research questions.

***Index Terms*—Security Research, Mobile Networks, GSM, UMTS, LTE, 5G, Systematization of Knowledge**

I. Introduction

OVER the past decades, mobile communication has become an integral part of our daily life. For instance, in 2016 the mobile network comprised 4.61 billion users [1] and the revenue of all mobile network operators totaled 1,331 billion USD [2]. On many markets, the number of mobile Internet subscribers has outnumbered the stationary ones. A vast and diverse mobile communication and application ecosystem has emerged. These applications include private as well as business communication, and even critical infrastructures. For example, payment services, energy infrastructure, and emergency services (e. g., FirstNet [3]) highly depend on mobile networks. As a consequence, the reliability and security of mobile networks have become a substantial aspect of our daily lives.

* These authors contributed equally to this work.

David Rupprecht and Thorsten Holz are with Horst Görtz Institute for IT-Security (HGI) at Ruhr-Universität Bochum, Bochum, Germany (email: david.rupprecht@rub.de; thorsten.holz@rub.de).

Adrian Dabrowski and Edgar Weippl are with SBA Research, Vienna, Austria (email: adabrowski@sba-research.org; eweippl@sba-research.org).

Christina Pöpper is with New York University Abu Dhabi, Abu Dhabi, United Arab Emirates (email: christina.poepper@nyu.edu).

However, over the last years, a large body of literature has revealed numerous security and privacy issues in mobile networks. There is a broad set of attacks [4], [5], [6], [7], [8], [9] that affect the users' privacy and data secrecy, the mobile network operators' revenue, and the availability of the infrastructure. Various countermeasures against these attacks have been proposed, some of which have become security features of new mobile generations. Besides the academic community, the non-academic community also substantially contributed to the comprehension of mobile network security. Unfortunately, attacks and countermeasures were mostly considered in an isolated manner and the research efforts have not been systematized or categorized into a big picture. However, these insights are necessary to develop generic countermeasures instead of separate fixes or mitigations. For example, messages being exchanged before the authentication and key agreement is the cause of multiple attacks [4], [10], [11]. Considering the attacks separately, one might not assume that this is a broader problem present in all three mobile generations.

As network standards tend to stay in use for decades, structural or backwards-incompatible changes are only possible for new network generations. We would like to use the window of opportunity with regards to 5G for the development of future mobile security specifications in order to eliminate insecure legacies. While considering the next mobile network generation, we systematized the research efforts of the last decades to improve and provide a basis for future security research and specifications. Since the contributions in mobile network security research are fragmented, we develop a methodology to categorize attacks and their countermeasures and thus provide an abstract overview on the topic. We project the design errors and attacks across the network generations to illustrate the specifications' development. Furthermore, we give an outlook on future developments in mobile communication and map the extracted issues to them. Finally, we identify open research questions regarding mobile network security and point out challenges for future specifications.

The scope of our survey is on the technical side of mobile networks (Figure 1) to fill a blank space between highly researched topics. There are surveys on mobile applications such as secure messaging systems [12] and mobile operating systems, e. g., Android [13]. On the other hand, there are generic Internet security surveys [14] and telephony security contributions focusing on fraud attacks [15], [16], [17]. Recently, Jover [18] pointed out 5G security challenges, but without systematizing prior work.

In summary, the main contributions of this article are as follows:

- We develop a **systematization methodology** for attacks and defenses in mobile networks. Starting from security requirements, we classify the attacks by their aims. We use attack characteristics for estimating the attack impact, e. g., different attacker capabilities. Defenses characteristics help us to describe the advancement for defenses. To gain an abstract overview on the topic, we logically group technical attacks and defenses into *causes* and high-level *root causes*.
- We **categorize and systematize** attacks and defenses on mobile networks using our systematization methodology to obtain a comprehensive picture of research in this field. To this end, we incorporate publications from the academic as well as non-academic communities to represent the big picture.
- We derive **open research questions and challenges** building upon our systematization for further studies in both offensive and defensive work. We do this to shape the future research in the field of mobile network security. In order to achieve this, we investigate the shortcomings of existing work, the implications of future technologies, and the concrete challenges of defenses. We underline the challenges of future technologies by mapping implications of 5G technologies to open research questions.

II. Mobile Network Background

In the following, we briefly describe the technical background of mobile networks, including an overview of the currently active generations and a generic overview of the network architecture.

A. Generations

Over the years, the requirements for mobile networks have shifted from rather single-purpose networks (voice service) to multi-purpose networks (data). In the following, we introduce the currently active network generations.

- **GSM (2G, Global System for Mobile Communications)** is the first digital mobile communication system and was designed for voice transmissions. It uses circuit-switched scheduling in which fixed slots are allocated for transmissions over the air and on network components along the transmission path. The General Packet Radio Service (GPRS) is a packet-switched extension on top of the circuit-switched architecture.
- **UMTS (3G, Universal Mobile Telecommunications System)**: In order to meet the increasing demand for data transmissions, the next generation was optimized for data transmission on the radio layer. Additionally, UMTS added new security features such as mutual authentication and new encryption algorithms. Although the network is packet-switched in its core, voice and SMS transmissions are still offered as distinct network services.
- **LTE (4G, Long Term Evolution)** uses a completely redesigned radio layer and a strict IP-based packet-switched architecture with guaranteed Quality of Service (QoS) classes. In contrast to its predecessors, voice and SMS transmissions are no longer network services, but IP-based services (SIP, VoIP) on top of a general-purpose IP data network.

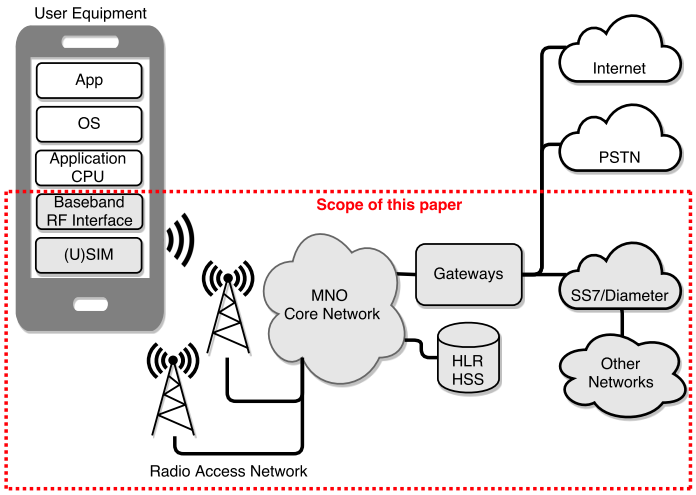

Fig. 1. Generic mobile network architecture and the scope of this paper.

Names and abbreviations for equivalent network components and concepts vary between the different network generations. Overall, we try to stay agnostic to the generations and access technologies. If we need to specially differentiate between different terms, we denote them with a ^{2G} for GSM, ^{3G} for UMTS, and ^{4G} for LTE.

B. Network Architecture

Figure 1 shows a generic network architecture including the scope of this paper. In general, the architecture consists of the following components:

1) User Equipment: The User Equipment (UE)^{4G} (e. g., smartphone) is the device utilized to communicate with the network and consume its services. It comprises different components, such as the application processor that runs the mobile operating system, the graphical user interface, and all its locally installed applications. The baseband processor implements the mobile protocol stacks for multiple network generations and thereby establishes the communication with the network. The SIM^{2G}/USIM^{3G,4G} (Universal Subscriber Identity Module) directly identifies a customer and stores the authentication information as a pair of the permanent identity (IMSI, International Mobile Subscriber Identity) and the secret long-term symmetric key used for encryption and authentication. From outside, a user is identifiable and thus callable via a public phone number (called Mobile Station Integrated Services Digital Network Number (MSISDN)). Besides permanent identities, for privacy reasons temporary identities are dynamically allocated to the UE, such as a Temporary Mobile Subscriber Identity (TMSI) that is used for paging and core network communication.

2) Radio Access Network: The purpose of the Radio Access Network (RAN) is to transmit data between the UE and the core network that provides service to the user. Therefore, the mobile phone establishes a radio connection to the base

station (BTS[2G], nodeB[3G], eNodeB[4G]) that acts as a network access point. Base stations are organized into cells which are in turn grouped into Location Areas (LAs)[2G,3G] or Tracking Areas (TAs)[4G] for mobility management.

3) Core Network: The core network's task is to manage the connection mobility and to deliver the services, e. g., phone calls and Internet connection. For this mobility management, several core network elements are utilized. A central database, the Home Location Register (HLR)[2G] or Home Subscriber Server (HSS)[3G,4G], stores the authentication, mapping, and other information about the users. Core network elements manage the mobility, connection, and security establishment. Signalling System #7 (SS7) is used within GSM and UMTS networks for signaling purposes such as mobility management and call setup as well as externally for roaming. SS7 was developed in the mid-1970s for landline networks and was later extended for mobile telephony networks. Unfortunately, the protocol only provides limited security mechanisms. Today, SS7 is mostly used as an SS7-over-IP adaptation. LTE introduced new IP-based protocols for the core-network infrastructure, e. g., the SIP-based IP Multimedia Subsystem (IMS) handles voice, video, and text messages.

4) Inter Network: Many services require a connection to other communication networks such as the Public Switched Telephone Network (PSTN) or the Internet leading to the introduction of subsystems and gateways.

Mobile networks are connected to each other via SS7 or its successor, the Diameter protocol for global inter-network operator roaming, text messages, and call forwarding. Diameter inherited most of the SS7 semantics, but offers improved authentication and confidentiality through the use of IPsec and Transport Layer Security (TLS).

5) Radio Channel: The radio layer shares some common design choices between GSM, UMTS, and LTE, whereas other characteristics like frequencies, modulation, or access technologies are highly individual. All generations incorporate three main types of logical channels into the physical radio channel: (i) Broadcast control channels carry information about the base station, its neighbors, and the network configuration. (ii) Paging channels are used to call out for specific UEs when the network wants to transmit data to them. (iii) Dedicated channels are used for traffic to and from each single device. These are the only channels that can be encrypted and integrity protected, if initiated by the network.

6) Pre-Authentication Traffic and Security Establishment: Unless initiated by the network, the traffic is unencrypted, not integrity protected and, thus, not authenticated. This means that only dedicated traffic to and from a specific device is secured. Thus paging, other broadcasts, most of the radio resource allocations, and low-level signaling traffic are always unprotected. All traffic that happens before the setup of an authenticated session is defined as *pre-authentication traffic*.

The authenticated session is established via an Authentication and Key Agreement (AKA) protocol which is a challenge-response protocol, that authenticates the partner(s) and derives a session key for the communication. While GSM only establishes user authentication, newer generations (UMTS, LTE) establish mutual authentication. The session keys are derived from a common long-term secret stored in the (U)SIM. The particular key derivation algorithm on the (U)SIM depends on the network generation.

7) Mobility Management and Paging: When no active data transmission or phone call is ongoing, the phone goes into the idle state. In this state, the network only knows the coarse Location Area where the subscriber is located. The phone listens to the paging channel as an incoming phone call, message, or data triggers a paging message of the subscriber in the Location Area. Upon receiving a paging message, the phone contacts the network and requests a dedicated (logical) channel for further communication. Thus, only if the phone switches to another Location Area, it has to inform the network using a *Location Update Request*. Additionally, the phone sends *periodic* location updates at a low interval (typically every 24h) to reassure the network of its continued presence. Each cell broadcasts a list of neighbor cells (e. g., their frequencies) to help the phone find these cells.

8) RAN Sessions and Data Tunnels: As most data services need stable addresses, tunnels are used between the UE and an IP endpoint. These tunnels hide the mobile network's mobility management and also allow to offer multiple connections to different IP networks, such as Internet access or private networks. Tunnels terminate at the packet gateways (Packet Data Network Gateway, P-GW[4G]). If necessary, Network Address Translation (NAT) middleboxes separate the mobile network from the Internet by translating the private IP address and port to a public IP address and port. Tunnels aim at guaranteeing certain QoS parameters, such as latency or bandwidth.

III. Methodology of Systematization

In this section, we introduce our systematization methodology that we apply to categorize attacks on mobile networks and their defenses. In the course of this article, we recognize and formulate research questions and challenges for future research based on this systematization.

A. Methodology

We structure the systematization process according to the flow depicted in Figure 2, beginning with the selection of particular security requirements, continuing with the assessment of recent attacks and defenses, and resulting in a set of research questions and challenges to shape future research in mobile network security. This process allows us to incorporate multiple aspects of offensive and defensive previous work resulting in a high-level perspective on essential root causes of security issues.

Security requirements define concrete features to protect mobile networks and their users. Such requirements are challenged by **attack aims**, i. e., the major interests of an attacker (Table I). Accordingly, **attacks** are instantiations of these attack aims and exploit existing vulnerabilities in the definitions and implementations of systems or system components. In order to assess the impact of attacks on the mobile network, we use a set of **attack characteristics** that give a precise definition of an adversary's technical and organizational capabilities, e. g., the preliminaries for an attack. We assess the

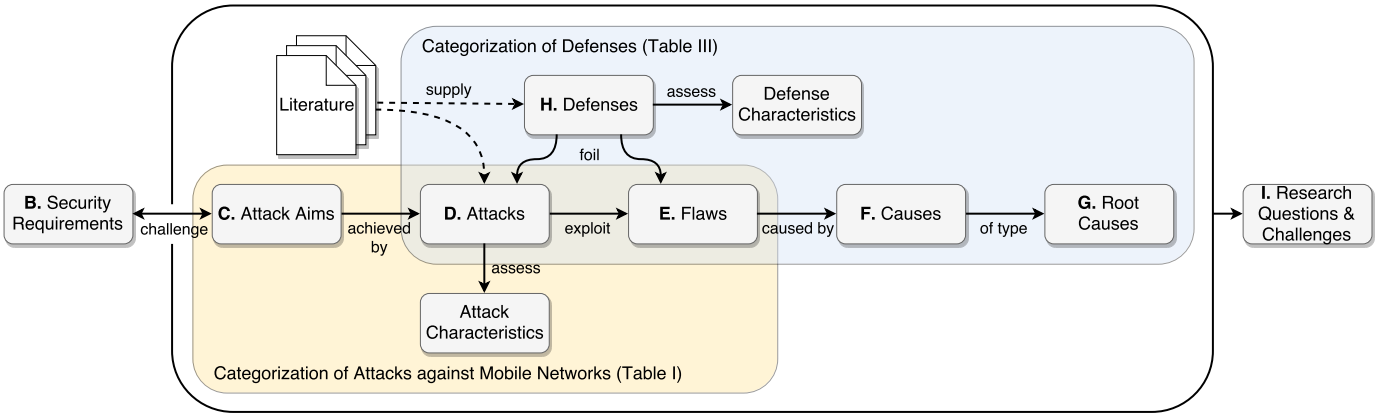

Fig. 2. Systematization methodology applied throughout this work. The letters correspond to the subsections of Section III where each aspect is described.

scope of existing **defenses** in relation to known attack vectors (Table III) and aggregate **defense characteristics** to assess their research and deployment status. However, multiple flaws are often manifestations of a broader problem that we define as a **cause**. Such causes facilitate the differentiation of attacks into distinct classes, thus allowing to derive open research questions and challenges in relation to the current state of the art. All causes are grouped into four fundamental **root causes**, which form the logical structure of our systematization.

Below, we give a short example to illustrate the application of this method.

> ***Example:*** *Radio Measurement Reports* are used for the maintenance of radio access networks and can be requested by a base station without authentication. This flaw can be exploited via the *Radio Measurement Report Request Attack* that allows an attacker with *active radio capabilities* to pinpoint a victim [4]. Hence, this attacks the user's privacy (*attack aim*) as it objects the location confidentiality *requirement*. The attack can be executed in the non-authenticated state of UEs, allowing an active attacker to fake measurement report requests. Therefore, the *flaw* is that requests for Radio Measurement Reports are part of the unsecured pre-authentication traffic (*cause*). As this is a legitimate request according to the specification, the *root cause* lies in the specification. A proposed *mitigation* is to require this specific request to be authenticated. However, this does not fix the underlying general problem of insecure pre-authentication traffic. A *generic solution* would be to eliminate pre-authenticated traffic completely, as it is the source of many other vulnerabilities as well. An *open research question* is how to develop a privacy-preserving specification while keeping the maintainability of mobile networks.

Coverage of Literature: We focus on academic research, i. e., scientifically peer-reviewed publications, as a foundation for the assessment. In addition, we use non-academic research (including publications, presentations, and demonstrations at hacker venues) and white papers from industry. Even though these publications are not peer-reviewed, they complement the academic body of the systematization with a comprehensive picture of mobile network security. In particular, the hacker community has contributed a lot to the understanding of mobile protocols [19] and has provided tools that academic researchers have built upon.

We require that the literature must present security- or privacy-related attacks and defenses and need to be unique to mobile networks and not focus solely on applications. We specifically exclude mobile operating systems security and common challenges of the public phone network. Preferentially, the literature should have a high impact, e. g., it affects many users, is operable from a large distance, or produces considerable damage.

Structure: We base the structure of our systematization (Sections V–VIII) on the root causes, and each section is further grouped into causes. Thus, attacks that are evoked by the same cause and root cause are logically grouped together. Mitigations and solutions are discussed directly within the respective subsections. Regarding the structure of this document, we traverse the systematization process (Figure 2) backwards from root causes, to causes, to attacks. Research questions originate from causes, root causes, and the implications of 5G technologies.

B. Security Requirements

Security requirements describe the demands that need to be met by the system in order to protect the interests of its stakeholders. For our systematization, we aim to establish generic and long-lasting security requirements spanning all three mobile network generations. However, the standardization bodies, e. g., 3rd Generation Partnership Project (3GPP), have issued diverging requirements over time, which is why, they fo not allow us to provide a holistic view and might not fit modern security concepts. In order to define generic and long-lasting security requirements, we therefore base our work on the publication of Avizienis et al. [20] who define a taxonomy of dependable and secure computing and general security requirements that we underpin with some more concrete requirements published by the 3GPP [21], [22], [23].

1) Confidentiality: Avizienis et al. [20] define confidentiality as the "*absence of unauthorized disclosure of information*". This statement is substantiated by the 3GPP with the following requirement: "*the network shall provide several appropriate*

levels of user privacy including communication confidentiality, location privacy, and identity protection" [21, p. 33]. In detail, this means [21]:

- Communication confidentiality: "[...] *contents, origin, and destination of a particular communication shall be protected from disclosure to unauthorized parties*".
- Identity protection: The network shall "*hide the identities of users from unauthorized third parties*".
- Location privacy: The network shall "*hide the user location from unauthorized parties*".

2) Availability: Availability denotes the readiness and the continuity of correct services [20]. With the pervasiveness of mobile communications in our everyday lives, availability becomes a crucial factor for customers as well as part of critical infrastructures [3], [24].

3) System Integrity: In contrast to data or transmission integrity, system integrity focuses on the hard- and software of the network components. Integrity is defined as the absence of unauthorized system alterations [20]. System integrity is an essential security requirement as it is crucial for the proper operation and trustworthiness of the system.

4) Unauthorized Service Access and Correct Charging: The service should only be accessible to authorized parties [21]. This requirement includes correct recording and offsetting call data records and other chargeable items [25]. In other words, a proper authorization and charging system should only allow subscribed services to be consumed and it should charge the *right* user for the *correct* volume [26].

Subsequently, we will use these high-level security requirements to assign an attack aim to each identified attack that challenges one or more of those requirements.

C. Attack Aims

Each attack has a clear primary aim that challenges one of the identified security requirements. An attacker might also pursue a secondary attack aim. For example, using side-channels, an attacker can obtain the shared key on the SIM card that undermines primarily the secrecy aim. However, the attacker might also clone the SIM card for free calls and thereby commit fraud attacks (secondary). We define five distinct attack aims:

- **Attacks on Privacy:** This aim covers all attacks that undermine the privacy of the user, including the *identity protection* and the *location privacy*.
- **Attacks on Secrecy:** This category includes attacks on *communication confidentiality*, e. g., the content of the transmission.
- **Denial of Service:** This attack aim contains all the objectives that impact the *availability* of services, or parts of them. Thus, *downgrade attacks*, such as disabling encryption or stepping back to less secure protocols belong here.
- **Attacks on Integrity:** This category comprises all the attempts which undermine the requirements for system integrity.
- **Fraud Attacks:** This aim covers attacks that aim towards directly or indirectly targeting financial benefits for the attacker or financial losses for others. *Direct under-billing* attacks dodge service charges at the expense of the operator, whereas *direct over-billing* produces financial loss to customers. *Indirect fraud* includes scams or spam via telephone.

D. Attacks

Attacks exploit system flaws under the defined attack aims. We use the following characteristics for an assessment of the attack impact (see Table I). In general, as for Table I, ● denotes a fully applicable attack for the characteristic, ◐ refers to limitations, and ○ characterizes attacks that are not applicable.

1) Attacker Capabilities: For mobile radio attacks, an attacker often combines several capabilities to perform an attack (e. g., retrieving session keys over SS7 and passively monitoring and decoding traffic); thus, we describe the attacker model as a set of distinct capabilities (i. e., building blocks). We assume that the attacker is a-priori not in possession of any *private* information (secret keys) of the victim, but might be in possession of *public* identifiers such as the phone number (MSISDN).

- **Passive Radio**: An attacker with passive radio capabilities is able to capture radio transmissions, decode signals, and read raw messages. The recent developments of Software Defined Radios (SDRs) and re-purposed hardware render this type of attack quite affordable [27], [28].
- **Active Radio**: An attacker with this capability has full control over radio transmissions and is therefore able to put arbitrary messages on the radio channel. This enables an attacker to setup a own base station or a fully controllable phone stack using an SDR [9], [27], [28], [29], [30], [31].
- **User Traffic**: The attacker is able to control or initiate traffic on a commodity mobile phone. The phone performs normal radio emissions, but the attacker accesses the higher (user-land controlled) network layers (e. g., IP). In most cases, this ability does not require a rooted or jail-broken phone.
- **SS7/Diameter Interface**: An attacker with access to SS7/Diameter is able to send and receive Signalling System #7 or Diameter messages to and from other networks. Some network providers even sell these services [32].
- **Nondestructive Physical**: A nondestructive-physical attacker temporarily has physical access to the victim's device, but neither destroys nor modifies hardware or software. Thus, the attack leaves no visible or measurable trace. We exclude the destructive attacker, because these visible traces would raise doubts by the users.
- **PSTN Interface**: An attacker has access to voice or text services of the Public Switched Telephone Network (PSTN).
- **Internet Traffic**: An attacker with the ability to access the Internet in a way that can specifically contact the victim's phone. That can be achieved by knowing the phone's public IP address and the TCP/UDP port mapping on the operator's packet gateway. Other possibilities include

identifiers of chat services, instant messaging apps, or cloud messaging services (such as Google Cloud Messaging (GCM) [33] or Apple's Push Notifications [34]), and the ability to transfer such messages.

2) Limitations of Attacker Capabilities: For our systematization, we assume that the operator's authorized personnel is trusted and thus exclude such attacker capabilities from systematization. However, such attacks have occurred in the past and are a threat to the mobile user's data secrecy and privacy [35], [36]. For instance, in the 2005 Vodafone Greece incident [35], a staff technician was suspected to have planted a backdoor in mobile switches that allowed copying traffic on government phones. In the Gemalto SIM key material theft [36], secret key material for the SIM cards was transferred by the use of unprotected means. However, such attacker capabilities are beyond the scope of this paper, as the attackers had the permissions in the first place and deliberately misused them.

3) Target: The target category depicts who is harmed by the attack, and if there is a relation to other categories, e. g., privacy attacks predominantly target the user. We focus on the primary goal and disregard secondary effects such as bad publicity due to data breaches.

4) Technology: This category maps the applicability of an attack to the three major access technology generations and assesses if there has been a security development, e. g., if defenses have been introduced in later access technologies, or if new technologies teared open new attack vectors. The former does not necessarily prevent attacks, as multiple downgrade attacks are known.

For example, only GSM lacks mutual authentication (*cause*), hence it is prone to Man-in-the-Middle (MitM) attacks. However, UMTS and LTE are open to various downgrade attacks; therefore the problem will not be resolved until phones stop to (unconditionally) support GSM. Downgrade attacks that trick or force a specific party to fall back on older and less secure access technology must be kept in mind when discussing fixes or mitigations for new access technology generations. We filed downgrade attacks as part of Denial of Service (DoS) attacks, as they deserve a separate review.

5) Range: The range of an attack is an indirect indicator of impact and cost. A higher range (e. g., a globally performable attack) increases its impact and versatility and might justify higher costs for an attacker. In contrast, an attack that requires more physical vicinity increases involvement of the attacker and reduces the set of victims. In Table I, we classify the range by technical boundaries: Physical access (**Phy**), same radio cell including simulated ones (**Cell**), same location area (**LA**), same network (**Net**), and globally executable attacks (**Glo**).

E. Flaw

For our systematization, we define a flaw as a specific and distinct vulnerability that is exploited by a particular attack. We coalesced attacks that exploit the same technical flaw or are otherwise very similar in their technical or operational principle. This leads to a 1:1 relationship between flaws and attacks.

F. Cause

We group flaws that have similar technical or organizational reasons via a common cause. A cause is a broader technical reason summarizing multiple individual flaws and, if dealt with appropriately, would foil an entire class of attacks.

G. Root cause

Root causes are the underlying reason for certain classes of attacks; they are defined on an abstract level and independent from technology. Each root cause summarizes particular flaws and vulnerabilities according to their structural or causal dependency (Table II) and is completely disjoint from other root causes. We use this abstract structure as the foundation for our systematization.

H. Defenses

In order to systematize and assess the defenses presented in the literature, we relate them to attacks, causes, and root causes. We show the coverage of the suggested defenses in Table III. If a defense encounters all the attacks of a cause, it can be considered a *generic* defense, otherwise it is a *specialized* defense. We differentiate between two kinds of defenses, namely, **detections** (◐) and **mitigations** (●). While the detection of an attack is an important step to impede losses or disadvantages, it does not ultimately prevent the attack. Mitigations foil attacks by straightening out the underlying flaw or by making attacks very unlikely to succeed.

Additionally, we evaluated the defenses according to a set of quality characteristics that help to assess the realization effort, the sustainability, and the current research status of a defense.

1) Realization Method: The realization method (Table III) specifies *how* a defense is achieved. A **specification defense** (S) needs to pass the 3GPP change-request process, such as protocol changes, to guarantee the interoperability. It has a higher realization effort time-wise, as it needs to pass the specification process. However, it will potentially reach more people in the long run, as new products are likely to implement such measures. In contrast, **implementation defenses** (I) do not depend on a specification and can be implemented directly into network components. While this task can be accomplished by a vendor, only users of an updated product benefit from it.

The realization method is an indicator of the *effort*, the *swiftness* with which it can be rolled out, and the *reachability*.

2) Affected Components: On the right hand side of Table III, we denote which network components need modifications to implement a particular countermeasure. On the one hand, it indicates who needs to take action to roll-out a defense. On the other hand, as a rough estimate, the less components are affected by a defense measure, the easier it can be implemented in practice, and vice-versa. However, particular updates on the UE are hard to roll out due to the high number of units and manufacturers involved.

3) Deployment Status: The deployment status has more a practical than a scientific value: It helps to evaluate the feasibility of a defense, if information about its deployment is available. A defense which has been deployed by at least one

TABLE I
CATEGORIZATION OF MOBILE SECURITY ATTACKS BY THEIR AIM

Aim	Attack	Attacker Capabilities							Target	Technology			Range					Section
		Radio Passive	Radio Active	User Traffic	SS7 Interface	PSTN Interface	Internet Traffic	Nondestructive Physical	User/Provider	2G	3G	4G	Phy	Cell	LA	Net	Glo	
Service	Signaling DoS [37], [38], [39], [40]	●	●	○	○	○	○	○	U,P	●	●	●	○	●	○	○	○	V-E1
	Attach Request Attack [41]	●	●	○	○	○	○	○	P	●	●	●	○	●	○	○	○	V-E1
	GPS Receiver Denial of Service [42], [43]	○	●	○	○	○	○	○	U	●	○	○	○	●	○	○	○	V-A1
	Continuous Wideband Jamming [44], [45], [46], [47]	○	●	○	○	○	○	○	U,P	●	●	●	○	●	○	○	○	VIII-A
	Protocol-Aware Selective Jamming [44], [45], [46], [48]	●	●	○	○	○	○	○	U,P	○	○	●	○	●	○	○	○	VIII-A
	IPv4/IPv6 Middleboxes Misconfiguration [39], [49]	○	○	●	○	○	●	○	U,P	○	○	●	○	○	○	●	○	VII-A1
	SMS Link Saturation [50], [51]	○	○	○	◐	○	●	○	U,P	●	●	●	○	○	○	○	●	V-E1
	Paging Response Race DoS [52]	●	●	○	○	○	○	○	P	●	?	?	○	●	○	○	○	V-A1
	DDoS HLR: Activate Call Forwarding Request [53]	○	○	●	○	○	○	○	P	●	●	○	○	○	○	◐	○	V-E1
	Insert/Delete Subscriber Data into the VLR/MSC [54]	○	○	○	●	○	○	○	U	●	●	●	○	○	○	○	●	V-D1
Secrecy	(U)SIM: COMP128v1 and MILENAGE Side-Channels [55], [56], [57]	○	○	○	○	○	○	●	U	●	●	●	●	○	○	○	○	VI-B1
	Baseband State Machine Exploits [58], [59], [60], [61]	○	●	○	○	○	○	○	U	●	●	●	○	●	○	○	○	VI-A1
	Encryption Downgrade [62], [63], [64], [65], [66], [67]	○	●	○	○	○	○	○	U	●	○	○	○	●	○	○	○	V-B1
	SIM Key Extraction via COMP128v1 Cryptoanalysis [68], [69], [70]	○	○	○	○	○	○	●	U	●	○	○	●	○	○	○	○	V-C1c
	Weak Key due to Inter-Technology Handover [71]	●	●	○	○	○	○	○	U	○	●	?	○	●	○	○	○	V-C1c
	Inter eNodeB User Plane Key Desynchronization Attack [72]	●	○	○	○	○	○	○	U	○	○	●	○	●	○	○	○	V-C1c
	Key Reusage Across Cipher and Network Generations [73]	●	●	○	○	○	○	○	U	●	◐	?	○	●	○	○	○	V-C1c
	MitM IMSI Catcher [62], [63], [64], [65], [66], [67]	●	●	○	○	○	○	○	U	●	○	○	○	●	○	○	○	V-B1
	Passive Over-the-Air Decryption of A5/1 and A5/2 [73], [74], [74], [75], [76], [77], [78], [79]	●	○	○	○	○	○	○	U	●	○	○	○	●	○	○	○	V-C1c
	Intercepting Calls with SS7/CAMEL [54]	○	○	○	●	○	○	○	U	●	●	?	○	○	○	○	●	V-D1
	Session Key Retrieval via SS7 [54], [64]	●	○	○	●	○	○	○	U	●	●	?	○	●	○	○	◐	V-D1
Privacy	AKA Protocol Linkability Attack [7], [80]	●	●	○	○	○	○	○	U	○	●	●	○	●	○	○	○	V-A1
	IMSI Paging Attack [7]	●	●	○	○	○	○	○	U	●	●	●	○	●	○	○	○	V-A1
	Location Leak by SIP Message [81]	○	○	●	○	○	○	○	U	○	○	●	○	○	○	○	●	VII-A1
	Location/Tracking Area not Allowed (Downgrade) [4], [6], [82]	●	●	○	○	○	○	○	U	○	●	●	○	●	○	○	○	V-A1
	Measurement Reports Localization [4], [10]	●	●	○	○	○	○	○	U	○	○	●	○	●	○	○	○	V-A1
	OTA SIM Card Update Key Reconstruction [83]	○	●	○	◐	○	○	○	U	●	●	●	○	○	○	○	●	V-C1c
	Unauthenticated IMEI Request [8], [62], [64], [65], [66], [67]	●	●	○	○	○	○	○	U	●	●	○	○	●	○	○	○	V-A1
	Unauthenticated IMSI Request (IMSI Catcher) [8], [9], [62], [63], [64], [65], [66], [67]	●	●	○	○	○	○	○	U	●	●	●	○	●	○	○	○	V-A1
	TMSI Deanonymization (Paging Attack) [4], [5]	●	○	○	◐	◐	◐	○	U	●	●	○	○	●	●	○	○	V-A1
	Cell-Level Tracking with SS7/MAP [54]	○	○	○	●	○	○	○	U	●	●	●	○	○	○	○	●	V-D1
	GPS Location with SS7/LCS [54]	○	○	○	●	○	○	○	U	●	●	●	○	○	○	○	●	V-D1
Integrity	ASN.1 Heap Overflow [84]	○	●	○	◐	○	○	○	U,P	●	●	●	○	●	●	●	●	VI-A1
	Binary Baseband Exploit [11], [85], [86]	○	●	○	○	○	○	○	U	●	●	●	○	●	○	○	○	VI-A1
	SMS Parsing [87], [88]	○	●	○	○	○	○	○	U	●	●	●	○	●	○	○	●	VI-A1
	SIM Card Rooting [83]	○	●	○	◐	○	○	○	U	●	●	●	●	○	○	○	●	VI-A1
Fraud	Fake Base Station SMS Spam [89], [90]	○	●	○	○	○	○	○	U	●	◐	○	○	●	○	○	○	V-B1
	LTE IMS-based SMS Spoofing [81], [91]	○	○	●	○	○	○	○	U	○	○	●	○	○	○	○	●	VII-A1
	Misbilling: TCP Retransmission or DNS Tunneling [92], [92], [93]	○	○	●	○	○	○	○	P	○	●	●	○	○	○	●	○	VII-B1
	Underbilling using VoLTE Hidden Channels [94], [95]	○	○	●	○	○	○	○	P	○	○	●	○	○	○	●	○	VII-B1
	Uplink IP Header Spoofing/Cloak-and-Dagger Misbilling [26], [96]	○	○	●	○	○	○	○	U	○	○	●	○	○	○	●	○	VII-A1
	Unblock Stolen Devices [97]	○	○	○	●	○	○	○	U	●	●	●	○	○	○	○	●	V-D1

● yes, applicable, needed for attack ◐ partially/supportive/optional ○ no, not applicable, or does not apply **?** property unknown

operator can naturally be considered feasible. The following notation is used:

- **No information** (?). No information about deployment.
- **Not deployed** (○). Not deployed by any operator.
- **Partially deployed** (◐). At least one operator or phone that partially implements the defense.
- **Fully deployed** (●). At least one operator or phone that fully implements the countermeasure.

4) Research Status: In the literature, defenses are discussed at vastly different levels of detail. Some papers about attacks conclude with rather vague defense proposals, while other works focus on the concrete realization and evaluation of a defense. The research status of a defense helps us to disclose possible shortcomings of the existing work. For this, we estimated the research status by examining the detail level and evaluation degree of a defense proposal and denote three status levels in Table III:

- **Vague Proposal** (○). A vague proposal mentions a defense without any precise scheme or architecture.
- **Concrete Proposal** (◐). A concrete proposal is a detailed scheme for a defense. However, the scheme is not evaluated.
- **Evaluated Proposal** (●). The security of the proposal was comprehensively evaluated—preferably by more then one literature source. The evaluation can be done either theoretically and/or practically.

I. Research Questions and Challenges

From the assessment of attacks and countermeasures, we derived open questions and challenges that should shape future security research in context of 5G mobile security. Following the systematization structure, we defined three leading questions or challenges for each cause:

Shortcomings of Existing Work. The limitations of prior research lead to individual sets of shortcomings for the different causes that we identified through our systematization. We define concrete starting points to address these shortcomings in future offensive and defensive work.

Concrete Challenge of Defenses. As we systematize the defenses in the context of causes, we emphasize the problems and challenges that all proposed defenses are trying to solve. We evaluate if the defenses are successful and might encounter multiple attacks in the cause. If they are not already solved successfully or just covering a small amount of attacks in a cause, we give starting points using literature of other related disciplines in which similar problems were solved.

Security Implications of 5G. When possible, we match these research questions onto the current 5G specification development. As the 5G is currently under development, we briefly refer to discussions and suggestions made within technical reports [98]. This matching assists us in finding the difference between current research and the specification process. From today's perspective, we point out security challenges of 5G technologies that should be addressed by future security research. To do this, we introduce the new technologies as well as the associated 5G challenges.

TABLE II
ROOT CAUSES RELATED TO CAUSES

Root Cause	Cause
Specification Issue	Unsecured Pre-Authentication Traffic
	Non-Existing Mutual Authentication
	Weak Cryptography
	Resource Usage Asymmetry
	Insecure Inter-Network Protocol
Implementation Issue	Insecure Implementation
	Leaky Implementation
Protocol Context Discrepancy	Cross-Layer Information Loss
	Accounting Policy Inconsistency
Wireless Channel	Channel Characteristics

IV. SYSTEMATIZATION OVERVIEW

In the following, we introduce the abstract *root causes* and their individual *causes* as used in this systematization (see Table II). Later, we present each cause in detail in relation to attacks, defenses, and open research questions, following the reverse process of Figure 2. The results regarding attacks are condensed in Table I and as graph in Figure 3 (see Appendix). Likewise, defenses are aggregated in Table III.

Specification Issues originate from incomplete, inaccurate, or faulty definitions of system behavior and comprise five individual causes: *Unsecured Pre-Authentication Traffic* allows to send messages to the phone or network prior to the key agreement and ciphering setup has taken place. *Non-Existing Mutual Authentication* relates to an attack vector exclusive to GSM networks, but is still an issue in recent technologies due to downgrade attacks. The use of *Weak Cryptography* significantly reduces the required effort for attacks on encrypted data, while *Insecure Inter-Network Protocols* undermine the users' privacy and confidentiality by poor protocol design choices. *Resource Usage Asymmetry* enables an attacker to perform cheap requests that result in intensive operations on the network side and hence can lead to DoS.

Implementation Issues are either caused by *Insecure Implementations* that open attack vectors in components of the mobile network, which can impair the system's integrity, or by *Leaky Implementations*, which means that sensitive information can be accessed through unintended side channels.

The root cause *Protocol Context Discrepancy* summarizes a class of security issues which use a protocol differently or in another environment than it was originally designed for. *Cross-Layer Information Loss* occurs at the interface of different layers in the network stack, e. g., when necessary, trustworthy security information is lost between network layers. *Accounting Policy Inconsistencies* result from different accounting schemes that can be played against each other, e. g., voice data is charged in minutes, whereas other data is charged by volume.

The *Wireless Channel* and its characteristics is essential for the transmission of information in mobile communication and comes with several physical limitations that impact the security.

Following the structure of root causes, we discuss offensive and defensive characteristics of specific causes and derive open

TABLE III
CATEGORIZATION OF DEFENSES

Countermeasure	References	ASN.1 Heap Overflow	Binary Baseband Exploit	SIM Card Rooting	SMS Parsing	Baseband State Machine Exploits	(U)SIM: COMP128v1 and MILENAGE Side-Channels	Misbilling: TCP Retransmission or DNS Tunneling	Underbilling using VoLTE Hidden Channels	LTE IMS-based SMS Spoofing	Uplink IP Header Spoofing/Cloak-and-Dagger Misbilling	Location Leak by SIP Message	IPv4/IPv6 Middleboxes Misconfiguration	Continuous Wideband Jamming	Protocol-Aware Selective Jamming	Unblock Stolen Devices	Cell-Level Tracking with SS7/MAP	GPS Location with SS7/LCS	Intercepting Calls with SS7/CAMEL	Session Key Retrieval via SS7	Insert/Delete Subscriber Data into the VLR/MSC	Fake Base Station SMS Spam	Encryption Downgrade	MitM IMSI Catcher	AKA Protocol Linkability Attack	IMSI Paging Attack	Location/Tracking Area not Allowed (Downgrade)	Measurement Reports Localization	TMSI Deanonymization (Paging Attack)	Unauthenticated IMEI Request	Unauthenticated IMSI Request (IMSI Catcher)	GPS Receiver Denial of Service	Paging Response Race DoS	Attach Request Attack	DDoS HLR: Activate Call Forwarding Request	Signaling DoS	SMS Link Saturation	OTA SIM Card Update Key Reconstruction	Inter eNodeB User Plane Key Desynchronization Attack	Key Reusage Across Cipher and Network Generations	Passive Over-the-Air Decryption of A5/1 and A5/2	SIM Key Extraction via COMP128v1 Cryptoanalysis	Weak Key due to Inter-Technology Handover	SIM	User Equipment	Base Station, (e)NodeB	Core Network	HLR, HSS	Packet Gateway	PSTN/Voice Gateway	Interconnection Gateway	Realization	Research Status	Deployment Status
Root Cause		Implementation Issue						Protocol Context Discrepancy						Wireless Channel		Specification Issue																												**Effected Components**										
Cause		Insecure Implementation					Leaky Implementation	Accounting Policy Inconsistency		Cross-Layer Information Loss				Channel Characteristics		Insecure Inter-Network Protocol						Non-Existing Mutual Authentication			Unsecured Pre-Authentication Traffic									Resource Usage Asymmetry				Weak Cryptography																
Frequent TMSI Reallocation	[99], [100]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	●	○	○	○	○	I	?	●
Pseudonymous IMSI and Non-Static Identifiers	[100], [101], [102], [103], [104]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	●	●	●	●	●	S	○	○
Asymmetric Cryptography with PKI	[100], [105], [106]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	●	●	○	●	●	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	○	●	S	◐	○
Base Station Fingerprinting	[62], [65], [66], [67], [89], [107], [108]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	◐	◐	○	○	○	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	I	●	●
Geographic Mapping of Network Infrastructure	[62], [65], [66], [67], [109]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	I	●	●
Passive Behavioral Analysis of Control Traffic	[67], [110]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	◐	○	○	○	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	I	●	●
Location Updates Inconsistency Check	[63]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	I	◐	?
Round-Trip Time Analysis	[63]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	I	◐	?
Check for Disappearing Phones	[111]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	I	○	?
Collect Neighbor Cells IDs by Phones and BTSs	[109]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	I	◐	?
Monitor Radio Vicinity for Changing BTSs w/ dedicated HW	[62], [107], [112], [113]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	I	●	●
Paging Repeat Statistics	[62]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	I	●	?
Retrofitting Mutual Authentication to GSM	[114], [115], [116], [117], [118], [119]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	◐	◐	◐	●	○	○	○	S	◐	○
Secure Key Derivation Function (e.g., MILENAGE)	[120]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○	●	○	○	○	S	●	●
Distinct Key Material and Key Derivation for Different Generations		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	●	●	●	○	◐	●	○	○	○	S	?	○
Increase Session Key Update Interval	[72]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	●	○	○	○	○	I	●	?
Disable Direct eNodeB Handover	[72]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	●	○	○	○	○	S	●	?
Introduction of Secure Cipher to GSM (e.g., A5/3)	[121]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	◐	○	○	○	○	S	●	●
Disable A5/1 on Network		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	◐	○	○	○	○	I	?	?
Disable A5/0 and A5/2 on Network	[122]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	◐	○	○	○	○	I	?	●
Disable A5/0 on UE for Non-Emergency Calls		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	S	?	○
Disable A5/1 on UE		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○	S	?	○
Disable A5/2 on UE	[122]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	○	○	○	○	○	S	?	●
GSM Random Padding	[123], [123]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	◐	○	◐	○	○	○	○	S	●	●
SS7 Penetration Tests	[124]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	◐	◐	◐	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	I	◐	◐
Stateful SS7 Firewall	[125], [126]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	I	◐	◐
Migration to Diameter		○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	S	◐	?
Statistical Attack Detection and Protection	[37], [41], [50], [51], [53]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	○	○	○	○	○	○	○	○	●	●	○	○	○	○	I	◐	?
SMS Parsing Test Framework	[86], [87]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	I	?	●
State Machine Test Framework	[59], [60]	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	I	?	●
Filtering Malicious SMS	[83]	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○	I	?	●
SMS Home Routing	[127]	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	◐	○	○	○	◐	S	●	●
Memory-Safe Languages and Runtime-Environments	[128], [129], [130]	◐	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	I	◐	●
Fully Machine-Readable Protocol Specifications		○	◐	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	S	○	◐
Fully Machine-Readable State Machine Specifications		○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	S	○	◐
Constant Time and Power Specification Requirements	[55], [56], [57]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	◐	○	○	○	○	○	○	S	●	?
Secure Binding Across Networks Layers	[26]	○	○	○	○	○	○	○	○	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	I	◐	?
Active Connection Deauthorization	[26]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	●	○	○	S	◐	?
Feedback-Based Mischarge Correction	[26]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	●	○	○	S	◐	?
Stateful IP Firewalls	[39], [49], [94], [95]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	I	◐	?
Deep Packet Inspection and Ratio Detection	[92], [92], [95]	○	○	○	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	I	◐	?
Spread-Spectrum Jamming Resiliency	[131]	○	○	○	○	○	○	○	○	○	○	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	S	○	?
Broadcast Encryption	[131]	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	◐	○	○	○	○	S	○	○
Beam-Forming Scheme for Selective Jamming Cancellation	[131]	○	○	○	○	○	○	○	○	○	○	○	○	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	I	○	?

Countermeasures: ● effective mitigation/solution ◐ detection, partial mitigation, probabilistic mitigation ○ not applicable
Components: ● implementation requires changes of that component ◐ optional or minor changes ○ no changes necessary
Realization Method: **S** by specification change/amendment/extension **I** by implementation (update)
Research Status: ○ vague proposal ◐ concrete proposal ● evaluated proposal
Deployment Status: **?** unknown ○ not deployed or deployable ◐ partially deployed ● deployed and known to work from at least one Carrier

research questions and challenges for future mobile network technologies.

V. Root Cause: Specification Issue

Specifications ensure the interoperability between implementations by specifying protocols, state machines, and interfaces. However, there may exists issues in the specification that might lead to flaws that can be exploited by attackers. In the specification-related root cause, we collate all flaws that are based on specification issues. The reasons for these problems range from technical trade-offs to political motivation.

A. Cause: Unsecured Pre-Authentication Traffic

The signaling traffic prior the security establishment with the AKA protocol is unprotected: it is neither encrypted nor integrity-protected and thus unauthenticated. This leads to implicit trust between the phone and the network. In this unauthenticated state, the phone fully obeys the network, even if the latter is not genuine. A malicious usage of messages in this unauthenticated state can serve for downgrade, track, or locate a specific user or handset.

1) Attacks: One prominent example for attacks based on unsecured pre-authentication is the deployment of *fake base stations*. Fake base stations (also known as *rogue* or *fraudulent base stations*, *IMSI Catchers*, *cell-site simulators*, a *DRT-Box*, or by product names such as *Stingray*) are active devices simulating a genuine base station to the phone by broadcasting genuine network identifiers. These fake base stations exploit the fact that mobile phones cannot verify the authenticity of the network prior to the AKA protocol.

In the unauthenticated state, the attacker is allowed to ask for the permanent identity, such as the IMSI or IMEI, and can thus undermine the user's identity and location privacy [6], [8], [9], [64], [65], [66], [80]. Besides obvious requests such as the *identity request*, an attacker can also use more subtle ways to determine the vicinity of a victim, e. g., with the AKA linkability attack [7]. Additionally, an attacker can repeatedly page the victim's IMSI [7] and, thereby, determine if a user is in radio range. Moreover, an attacker can retrieve a more precise location by requesting measurement reports from the victim's handset [4], [10] enabling an attacker to track a victim or to request the identity of people within radio range.

Furthermore, unsecured pre-authentication traffic allows *downgrade attacks* to a less secure access technology by denying service using the *tracking area update reject* or a combination of other messages [4], [6], [82]. This serves as a stepping stone for further attacks such as the GSM MitM attack (Section V-B1). Additionally, a fake base station can disable the location service on some phones by sending out the country code of Egypt, because GPS receivers were forbidden in Egypt [42], [43]. Furthermore, Golde et al. [52] showed that unsecured pre-authentication uplink traffic in GSM can be misused for a DoS attack dropping calls in the entire location area by winning the race answering paging requests. This is a problem of the GSM state-machine specification, as it can not recover once it proceeds to the ciphering setup.

The missing protection of broadcast and paging messages also enables attacks that retrieve the temporary identity of a victim by triggering the paging process multiple times and statically analyzing the paged TMSIs [4], [5]. An attacker can trigger the paging procedure in multiple ways: for example, with targeted Internet traffic, a short phone call and immediate hang-up, e. g., before the ring starts, or with a *Silent SMS* that is a text message which is silently discarded by the phone [132].

Assessment: Attacks based on unauthenticated uplink traffic or on passively exploitable downlink traffic are vastly outnumbered by active radio attacks based on pre-authentication traffic. While potentially having a very severe impact, an active radio attacker is limited to his/her radio vicinity. Most of these attacks undermine the victim's data or location privacy. Many commercially available products exploit unsecured pre-authentication traffic [133], [134], hence making it a high priority to be addressed.

2) Defenses: The research community proposed and implemented multiple detection and mitigation techniques against fake base stations. Detection schemes against the client include geographical mapping (e. g., via GPS) of the network structure to detect new—and possible fraudulent—base stations, finding unusual frequency or cell parameter configurations, and behavioral analysis of base stations. Some are implemented as smartphone apps [62], [66], [67], [89] others use dedicated smartphones with baseband firewalls [110]. Furthermore, a sensor network can detect such changes [62], [107], [135]. Recently, operator-based detection schemes were proposed [63], [109], [111]. Some of these approaches also detect large-scale paging race attacks [62].

Besides detection schemes, mitigations and fixes based on protocol changes have been proposed. An ephemeral identifier, e. g., dynamic IMSI or pseudonymic IMSI (P-IMSI) instead of the static IMSI has been proposed [90], [101], [102]. All of them protect against an unauthorized IMSI request by providing a new, seemingly unrelated number as the identifier for each request. However, the ephemeral identifier require severe changes to the network structure as the IMSI is used as a primary key to link all the subscriber-related information in a network. Additionally, protocol changes have been proposed against the paging response race attack and the AKA linkability attacks [7], [11].

Besides these specialized solutions, securing the paging and other broadcast traffic would eliminate the cause for all these attacks, e. g., using a source origin authentication scheme. Some proposed options are based upon asymmetric cryptography with a public key infrastructure [98], [105], [106] or upon broadcast authentication schemes [100].

Attacks that map a public identifier to the temporary identifier (TMSI de-anonymization) are currently countered by frequently changing TMSIs [4], [99], [100] even after unsuccessful calls. The GSMMap project [136] provides a rough estimation on the deployment of this workaround.

3) Research Questions and Challenges: The detection of fake base stations via the handset (e.g., behavioral analysis) or with externally deployed sensors only benefits a small number of people or a certain geographical area.

Countermeasures based on protocol changes often have a hard time to get through specifications for current network generations, as they introduce non-backward-compatible changes. For example, dynamic identifiers such as PMSI (as a replacement for TMSI and IMSI) require deep changes in many systems at once (VLR, HLR, Packet Gateways). The importance of such measures influenced the 5G design process and some of them might be included in the new specification [98, §5.7.4.3 ff.]. In contrast, moving measurement reports from an unauthenticated to an authenticated protocol state is possible in current network generations, as the functionality of currently deployed handsets is unaffected (but stay vulnerable). However, in recent years, new vulnerabilities based on pre-authentication traffic have been revealed [4]. In conclusion, none of the proposed protocol changes abandons non-protected pre-authenticated traffic in its entirety.

Thus, a more general approach is based on abandoning pre-authentication traffic in particular – or unprotected signaling in general – completely. Two main ideas have been proposed: Schemes based on asymmetric cryptography and broadcast-authentication schemes such as the TESLA protocol [100], [105], [106], [137]. For example, 5G currently explores ways to protect base station identity signatures using asymmetric cryptography [98, §5.4.4.8]. However, both were not extensively researched in the context of mobile networks with its limited bandwidth, power consumption restrictions, and low computational USIM card. Another related question is, if the protection of signaling uplink traffic from the UE to the network would increase the over-all security of the system. Such a general solutions would be desirable for future network generations as to remove the entire threat class.

Nevertheless, formal analysis of proposed protocols should prove the authenticity, confidentiality, privacy, and availability requirements [7], [120]. This can be either accomplished by manually proving the protocols or the use of automated tools.

Summary: Attacks based on pre-authentication traffic affect the privacy and aim to downgrade the service. Such attacks are possible across all three mobile generations. Defenses include either attack detection or protocol changes that aim to mitigate specific attacks or abandon the entire pre-authentication traffic. Future research must focus on completely abandoning pre-authentication traffic, e. g., with asymmetric cryptography. Automated and manual inspection aid the goal of provable security by identifying shortcomings.

B. Cause: Non-Existing Mutual Authentication

The specification of GSM does not include network authentication and, thus, allows a MitM attack. Although the fact of non-existing mutual authentication originally exploits a specific vulnerability of GSM networks, they are still a relevant threat in today's networks as the weakest-link-principle applies. Downgrade attacks via unsecured pre-authentication traffic on UMTS or LTE (Section V-A) still allow to exploit this GSM vulnerability on modern phones. The difference to pre-authentication traffic (Section V-A) is the lack of mutual authentication. In that sense, the non-existing mutual authentication is an extension of the unsecured pre-authentication traffic issue and has similarities in attacks and defenses with the former cause.

1) Attacks: If the phone cannot verify the authenticity of the network, an unconditional trust of the phone to the network and, thus, to a potential attacker is established. In a network-centric architecture, where most decisions are made by the network, an attacker faking a base station gains excessive power over the handset.

Fake base stations often employ additional techniques to keep a victim in the fake cell, such as not supplying information on neighboring cells or manipulating cell reselection thresholds [62]. The phone behaves inconspicuously and is able to make phone calls as well as send text messages and data to the fake network. However, without any further exploit, the attacker can not gain the possession of the cryptographic keys. Still, the attacker can downgrade the communication to the null-cipher or an easily attackable cipher (see Section V-C1a) for passing it to the real network. In this case, the phone remains reachable for the genuine network. Alternatively, calls, SMS, and data could be forwarded with additional modems or SIP, in which case the original caller-ID is lost, and the phone is not reachable from the outside. The impact of the attacks can be increased by an attacker with SS7 capabilities, e. g., she/he can directly inject the traffic into the phone network.

Similar to measurement reports on LTE, the GSM radio resource location service protocol enables the network to request GPS coordinates from the phone [138]. Developed for emergency services, most phones will answer the request even though it is not an emergency call [61]. Additionally, the non-existing mutual authentication has been a rich source for location-based SMS spam—mainly in China [89], [139]. Commercially available fake base stations with ready-to-use exploits are a reminder of the urgency with which this threat should be addressed.

2) Defenses: Similar to unsecured pre-authentication traffic, fake base stations that exploit the non-existing mutual authentication can be detected with mobile apps, baseband firewalls, sensors, or network-based sensors [62], [63], [64], [65], [66], [67], [107]. Nevertheless, mobile apps do not sufficiently protect against the threat of fake base stations [108]. Besides that, fake base stations that send out SMS spam can be detected based on the content of the SMS and meta-information (e. g., signal strength, duration of cell contact) [89]. Many defenses (and caveats) from unsecured pre-authentication (Section V-A2) traffic also apply here.

While UMTS and later network generations introduced mutual authentication, the literature urges retrofitting mutual authentication to GSM. Some of the proposed schemes need major changes in the specification [114], [115], while others focus on minimizing changes to ensure a fast roll-out [116], [117]. Even proposals to use the UMTS authentication scheme in GSM have been discussed within the 3GPP working group [118], [119]. However, none of the suggestions has been found appropriate for the GSM specification such that

the non-existing mutual authentication still remains a problem for future generations.

3) Research Questions and Challenges: Even the phase-out of GSM by some network providers does not protect users against MitM attacks, as the phone continues to "peak" GSM. Research can thus proceed into several directions. Modern authentication protocols could be retrofitted into GSM with a downgrade protection that prohibits legacy GSM operations if both the phone and the network can support newer methods. A downgrade protection scheme will also benefit future network generations with their security problems. For this, we refer to the causes *unsecured pre-authentication traffic* and *wireless channel*, as they are responsible for downgrade attacks.

Summary: GSM has no network authentication, which leads to privacy and confidentiality issues. Nevertheless, the GSM specification will not be addressed by any improvements. For future generations downgrade attacks to the insecure GSM standard open old attack vectors. Future research must suggest technologies for prevention downgrade attacks, e. g., by securing the pre-authentication traffic. Furthermore, the retrofitting network authentication to GSM provides protection in case of a downgrade attack.

C. Cause: Weak Cryptography

Cryptography provides the means to achieve data confidentiality. However, weak cryptography can lead to attacks revealing protected information. This can emerge from intentionally weakened algorithms or by evolving attack methods [140]. Cryptographic systems should be designed following Kerckhoffs' principle [141], which states that a system should only rely on the secrecy of the key and while everything else is publicly known. In the following, we describe attacks that aim specifically at weak cryptography.

TABLE IV
CIPHER OVERVIEW

	Cipher	Type	Effective (nom.) key length	Attackable
2G	A5/0	Null Cipher	–	●
	A5/1 + Comp128v1/2	LSFR keystream	54 (64) bits	●
	A5/1 + Comp128v3	LSFR keystream	64 bits	●
	A5/2	LSFR keystream	40 (64) bits	●
	A5/3	KASUMI	64 (128) bits	◐
	A5/4	KASUMI	128 bits	◐
	GEA1	LSFR keystream	64 (96) bits	?
	GEA2	LSFR keystream	64 (125) bits	?
	GEA3	KASUMI	64 (128) bits	◐
	GEA4	KASUMI	128 bits	◐
3G	UEA0	Null Cipher	–	●
	UEA1	KASUMI	128 bits	◐
	UEA2	SNOW 3G	128 bits	○
4G	EEA0	Null Cipher	–	●
	EEA1	SNOW 3G	128 bits	○
	EEA2	AES	128 bits	○
	EEA3	ZUC	128 bits	○

○ not attackable ◐ attacks known, but not practicable
● attacks with commodity hardware ? no Information

1) Attacks: Cryptography is used for the encryption algorithms on the air interface, for the handover, and initial key derivation. In all these parts, we identify attacks due to the use of weak cryptography. The found attacks undermine the data confidentially requirement, either by breaking the used session key or the shared key on the SIM card.

a) Encryption Algorithms: Table IV depicts the air interface encryption algorithms for all three generations, in particular the type of cipher, the effective key length, and if the cipher is attackable. All cipher suites in GSM except for A5/3 are breakable within minutes on commodity hardware for different reasons. A5/1 is a 64-bit cipher with major cryptographic vulnerabilities that have led to passive decryption attacks [73], [74], [75], [76], [77], [78]. A5/2 was designed as a stripped-down export version of A5/1 with less security, and Goldberg et al. [142] showed how to break this cipher in near real-time. Rainbow table approaches are further eased by the predictable padding of messages [79]. Theoretical attacks exist against A5/3, but they are impractical in terms of space requirements, as they require 2^{26} captured data frames [143]. GPRS ciphers GEAx basically mirror the weaknesses and development of their A5/x counterparts [144]. In GSM, the cipher-capabilities of the network and the user device are not integrity-protected and are therefore vulnerable to manipulation. An attacker can change the encryption handshake to block A5/3 and force a downgrade to A5/1.

In contrast to GSM, all UMTS and LTE ciphers underwent public development and thus followed Kerckhoffs' principle. As a consequence, only one attack against the KASUMI based UEA1 algorithm was revealed, but still requires a large amount of captured data and is unpractical [145], [146].

Additionally, each generation has a null cipher that offers no protection. Since the networks select the encryption algorithm, the user is unaware of sending data in clear text. A ciphering indicator should warn the user on the UE. However, just few vendors implement such a ciphering indicator [60], [147], [148], [149].

b) Interoperability of Access Technologies: Interesting problems arise due the usage of same key material within the same generation or due to the interconnection of network generations. Barkan et al. [73] describe that it is possible to downgrade to a less secure cipher for a short period of time or to reconstruct the key passively from over-the-air communication and later use it for all the other ciphers. In order to allow a GSM SIM to connect to UMTS, the key is extended to meet the UMTS key length [71], [150], [151]. Also, a USIM operating on GSM will simply use a shortened key. Thus, an attack on the much weaker A5/x series reveals parts of the key information for other access technologies during handover. Additionally, the LTE handover is vulnerable to the so-called "desynchronization" attack [72]. In this attack, an attacker can desynchronize the used key with the core network and, thus, an old session key is reused.

c) Key Derivation: Weak cryptography is also used for the initial key derivation algorithms. By reverse-engineering and breaking the COMP128v1 key derivation algorithm of GSM an attacker can reconstruct the shared secret key [68], [69]. In combination with side-channels, COMP128v1 attacks

can be brought down to nearly instant key recovery [70] (see Section VI-B). Another attack by Nohl et al. [83] on SIM cards can remotely reconstruct the SIM's software update key based on weak 3DES encryption. They leveraged the fact that the error messages concerning ciphering are sent encrypted with a known plaintext. As this attack is delivered via SMS, it is globally applicable. A reconstructed OTA key enables the attacker to install new applications on the SIM card, subsequently accessing secrets stored in other applications (see Section VI-A).

Assessment: All the attacks based on weak cryptography primarily undermine the data confidentially aim of mobile networks. The attacker might also pursue a secondary aim. For example, the shared key obtained through SIM attacks can later be used to decode encrypted transmissions or write the keys on a freely programmable SIM card. Such cards can be used to impersonate a subscriber, redirect calls, change settings, or commit fee fraud. While attacks on the air interface can be executed by an attacker with passive radio capabilities, the attacks on the SIM card require physical access— thereby are thereby either limited to the radio transmission range or to the physical range. The attacks on the session keys are possible using affordable methods such as rainbow tables on an ordinary PC. GSM is especially prone to cryptography attacks. In contrast, newer generations rely on secure algorithms following the Kerckhoffs' principle such that these attacks are not known for now.

2) Defenses: Because the specification follows the best practices in newer generations, most of the defenses concentrate on the weaknesses of GSM. After weaknesses of A5/{1,2} became apparent and attacks were feasible, two new ciphers were added which are backports of the UMTS KASUMI cipher, whereas A5/3 simply pads the GSM 64-bit key to 128 bits and A5/4 uses the full 128 bits [152]. The A5/3 usage is increasing [63], but as of 2017, there is no known network supporting A5/4. GSMA finally mandated the removal of A5/2 support from phones [122]. Besides A5/2, the A5/0 was a useful downgrade target, so some networks disabled both of them [63]. Disabling A5/1 is still not a viable option for operators. The key derivations and authentication algorithms are exchangeable and also follow the best practice. MILENAGE is based on AES and replaces COMP128 [153]. TURK, based on SHA-3 (Keccak), is another option for the authentication [154]. It is important the algorithms is provably secure and hold strong security assumptions [120].

The introduction of new encryption algorithms for old access technologies decreases the effectiveness of attacks. However, this introduction takes a long time as software/hardware needs to be updated and new algorithms must be specified.

3) Research Questions and Challenges: Standardization and implementation of cryptographic protocols for handover, initial key derivation, or encryption did not follow best practices. Advances in cryptanalysis have revealed various vulnerabilities in these algorithms. In the future, new algorithms need to be carefully analyzed following Kerckhoffs' principle. This is especially the case for the newly introduced device-to-device (D2D) communication. In the case of direct device communication, two devices agree on a common key by using two protocols that provide no forward secrecy and rely on one master key [155], [156], [157]. Such a scheme has different security implications [158]. If asymmetric cryptography is added to 5G or future generation, this introduces new attack surfaces if not designed and implemented carefully. Additionally, the to-be-introduced embedded SIM card comes with a complex security infrastructure and with protocols that have not yet been analyzed with respect to security [159]. Future research should prove the security of all the used cryptographic techniques in the mobile context to ensure overall security.

Summary: Weak cryptography has led to many attacks against the data confidentiality aim. In future generations, structural changes such as device-to-device communication challenge the use of secure algorithms. The system's security should continue to rely on well-known and proven secure cryptographic algorithms. Future research must match specified cryptographic algorithms with a realistic scope of attacker capabilities. Additionally, measures to protect against downgrade attacks to older and less secure ciphers and protocols must be developed.

D. Cause: Insecure Inter-Network Protocols

Nowadays the telecommunication industry is deregulated and SS7 has been ported to an IP-based network. Both developments make SS7 easily accessible. Thus, an attacker with SS7 capabilities becomes more likely. However, for interconnectivity with the SS7 networks, SS7 messages are translated to Diameter. This makes Diameter also vulnerable to SS7 attacks, as this inter-working function does not provide authenticity. Even though Diameter was designed with security features based on protocols like TLS and IPsec, researchers found vulnerabilities in the dedicated Diameter protocol that do not rest upon the inter-working function of SS7.

1) Attacks: The general idea of SS7 attacks is to request services on different layers of the home network or the serving network. As SS7 offers no authentication mechanisms, the network entities cannot decide if the request is legitimate. Thus, the entity replies properly, even though the request might not be legitimate.

An attacker can determine the user location on different levels of granularity—in the range of cells up to exact GPS coordinates [54], [160], [161]. Additionally, an attacker can map the temporary identity (TMSI) to the permanent identity (IMSI) of a victim by using the SS7 system. The permanent identity can then be mapped to the public telephone number. Both attacks are not compliant with the identity confidentiality aim. The misuse of SS7 can also lead to attacks that undermine the confidentiality of calls or of text messages [54]. This can be done by rerouting calls or by requesting the over-the-air encryption key. Besides this, the insecurity of SS7 can also be exploited for fraud attacks by unblocking a stolen device [97]. Additionally, an attacker can run a precise DoS attack against a distinct user by deleting subscriber data in the VLR [54]. Attacks that are possible due to the inter-working function between Diameter and SS7 are discussed by Holtmanns et al. [161] and Rao et al. [162].

Assessment: The insecurity of SS7 leads to a wide range of attacks. Most of them aim to undermine the (location) privacy of the user. Even commercial services were built upon the insecurity of SS7 allowing to pinpoint and track a victim [32], [54], [163]. This shows that the SS7 vulnerabilities are actively used and are thereby a serious threat to users. Most of the attacks require SS7 capabilities of the attacker. However, some attacks can be accomplished by using passive radio capabilities, e. g., an attacker can decrypt the traffic as soon as the over-the-air encryption key is revealed.

2) Defenses: The most sustainable long-term solution is the complete elimination of SS7. With the specification of Diameter in LTE, a more secure protocol is used for inter-networking functions. However, even Diameter is not free of flaws [162]. Additionally, the inter-working function between SS7 and Diameter still allows attacks via Diameter based on SS7 vulnerabilities, as long as not all the network providers migrate to Diameter.

Therefore, short-term solutions to mitigate the threats of SS7 and Diameter insecurity have been proposed. Most of them are based on validating the legitimacy of the request and then blocking the request itself or blacklisting certain classes of message types. For example, a request for the over-the-air encryption key is only allowed by a network that proves the user's registration within its range. Furthermore, certain requests are merely of network-internal interest and are discarded at the network border, e. g., the charging of the prepaid credit. The industry provides solutions for the mobile network operators ranging from SS7 scans [124] to state-full SS7 firewalls [125], [126].

3) Research Questions and Challenges: By now, it is known that SS7 is an insecure protocol and the backward-compatibility of Diameter rendering also newer systems vulnerable to SS7 attacks. The exclusive use of Diameter in the (inter)-core network communication would be a step forward in terms of security, but it will not entirely solve the security problems.

Thus, the open research question is to design a protocol that is proven secure and that holds the security requirements, especially the privacy requirements in the (inter)-core network while maintaining the functionality of the mobility management. Such a protocol must withstand an exhaustive security analysis. For example, such a protocol should enforce a proof from the remote network that the subscriber is actually present and only authorize such transactions. A solution explored for 5G is to bind keys to a public key identity of the serving network [98, §5.2.4.6]. Both would prevent attacks in which an attacker sends unauthorized requests to the home network, e. g., for the session key. The means of a privacy-preserving protocol are open topics for research.

Summary: Insecure inter-network protocols (e. g., SS7) allow privacy and fraud attacks, and will not be entirely switched off in the near future. Firewalls constitute only temporary solutions to the problem. Future research is challenged to design privacy-preserving inter-network protocols that keep the maintenance overhead low.

E. Cause: Resource Usage Asymmetry

Resource usage asymmetry occurs when an simple action on one side triggers a computationally or resource-wise expensive reaction on the other side. This—for example—leads to signaling DoS attacks, during which an attacker misuses signaling/control messages to trigger an expensive action. Thus, the network allocates the resources within different components and may eventually run out of them after repeated or coordinated requests.

1) Attacks: Unauthenticated messages like those used in the *attach procedure* can be utilized to overload the core network components [38], [41]. Additionally, they can impersonate legitimate subscribers. Similarly, Lee et al. [37] have presented signaling attacks for 3G networks and argue that low-volume but well-timed signaling attacks can have a major impact on the network components. By misusing multiple messages for establishment and release of radio connections, the authors caused a significant increase of message load in the network. Traynor et al. [53] evaluated network attacks targeting the $\text{HLR}^{2G,3G}$. They found an effective method to tear down an HLR by frequently switching the call forwarding service on and off. They suggest that a mobile phone botnet can disable the service of an HLR.

Similarly, a mobile phone botnet could attack a 911 response center, which would result in an outage of emergency services [164]. While this is not exclusively related to mobile-phone networks, the elevated priority of emergency calls makes it a unique mobile network problem: The network will drop other connections in favor of emergency calls if necessary. Enck et al. [50] evaluated attacks considering the to open SMS functionality on the Internet. They analyze an attacker model that uses open SMS centers on the Internet to saturate the wireless link downstream from the base stations, obstructing the service in the whole cell.

Assessment: All the attacks based on resource usage asymmetry focus on an exhaustive denial-of-service of the network. However, the impact of these attacks vary. While some attacks require active radio attacker capabilities, others already work with Internet capabilities. Besides intentional disturbance of the service, similar problems can occur due to misconfigured mobile apps or unexpected user behavior [165], [166].

2) Defenses: So far, most suggested detection and protection methods are statistical approaches [37], [51], [53]. Random connection drops might protect the network functionality as a whole, but inevitably they also deny legitimate requests. Even good statistical methods come with a non-negligible false-positive rate. The suggested protocol changes are unrealistic for currently rolled out networks.

3) Research Questions and Challenges: All the defenses suggest reactive schemes that come with a certain false-positive rate and do not prevent attacks. Future research should explore how to prevent resource exhaustion in the first place. This could require protocol changes and is, thus, only viable for new network generations.

Possible approaches can be borrowed from similar problems in the context of other computer networks. RFC5013 [167] proposes a TCP cookie against connection flood attacks. In

contrast, Dwork [168] and Back [169] suggested a proof-of-work-based method against flooding and email spam. Before the server or network processes a request, the client has to solve a (moderately hard) computational puzzle, proving its commitment. These puzzles have to be easy to generate, easy to check, but parametrizable hard to solve (e. g., finding bits of a hash-collision). Thus, equalizing the computational load on both sides and making flood-based DoS attacks much more resource-intense for the attacker. However, such schemes have to be adopted to and evaluated in the context of mobile networks. Challenges include the limited resources on mobile devices and low-latency requirements on some operations.

Summary: Resource usage asymmetry allows to flood networks with signaling messages and eventually a denial of service. Future research must aim for complete attack prevention, as current state of the art research can only provide probabilistic detection. This is possible through protocol designs with balanced resource usage.

VI. Root Cause: Implementation Issue

Deviations of the implementation from the original specification can open attack vectors and, thus, can have a security impact on otherwise securely defined systems. Such deviations can be introduced on purpose, e. g., for compatibility trade-offs, or result from faulty implementations. In the following, we discuss the implications of insecure and leaky implementations.

A. Cause: Insecure Implementation

While insecure implementations can open attack vectors in deployed systems, current research mainly focuses on attacks on the baseband and SIM cards. By sending malicious data to vulnerable devices, an adversary can exploit implementation issues. In the following, we discuss how attacks undermine the system integrity, availability, secrecy, and privacy including potential countermeasures.

1) Attacks: The lower layers of the protocol stack run on distinct baseband processors in the UE. Parser errors within the baseband processor can occur due to faulty implementations of parsing modules or libraries threatening the device's integrity. In 2016, a heap overflow in a widely used ASN.1 compiler was discovered [84], [170] affecting baseband implementations of multiple manufacturers. Weinmann [85] and Golde [11] demonstrated how to use baseband exploits to further target the application processor and its operating system.

Crashing-only flaws in the parsing and decoding stage of text messages [86], [87], [88] make the phone inoperable until the next reboot. Similar flaws on SMS parsing have been found on other processing levels [171].

Apart from attacks on the baseband, Nohl et al. [83] showed that the application isolation on the SIM card is so weak that processes can access foreign data including authentication credentials. Such applications can be remotely installed after reconstructing the over-the-air (OTA) update key (see Section V-C1c).

Implementation flaws in the protocol state machines of the baseband result in the acceptance of a fake base station as a genuine network endangering data secrecy and privacy [58], [59], [60], [61].

Assessment: On the one hand, we see that attacks can be launched globally and in a targeted manner that makes the impact of these flaws very high. On the other hand, the most dangerous ASN.1 heap overflow and the staged baseband-to-application-processor attacks required a fake base station with active radio capabilities and is thus locally bounded. The danger lies in the potential to take over the device at the lowest level.

2) Defenses: Intermediate workarounds for multiple of the aforementioned attacks are based on operator-side filtering. For example, operators filter out messages that might be used to infer the OTA-key of SIM cards. Such filtering can be easily and quickly deployed by the operator. However, intermediate workarounds are only effective against known attacks and, thus, are not very sustainable. Furthermore, network filtering only prevents attacks coming through the network. An attacker with active radio capabilities operating a fake base station can still deliver these exploits directly to the phone, albeit with reduced range.

More generic defenses in the field of insecure implementation focus on the detection and prevention of insecure implementations. For SMS parsing errors as well as for state machine errors, various security testing frameworks have been proposed [59], [60], [86], [87]. These frameworks automatically test for known vulnerability patterns based on predefined test cases. While automated approaches were used to find SMS parsing errors and state machine errors, many memory corruption vulnerabilities were manually found through reverse engineering [11], [85].

3) Research Questions and Challenges: All the attacks and mitigations stemming from *insecure implementation* have similarities to classic system security. We distinguish research questions between detection and prevention of vulnerabilities. Additionally, we discuss the shortcomings of the existing work which is the current scope.

a) Detection of Vulnerabilities: Although testing frameworks have been proposed [59], [60], [86], [87], they usually focus on one particular type of flaw, such as SMS parsing errors, state machine failures, or particular memory vulnerabilities. Basebands have complex state machines and exhibit a fragile behavior [11], thus, automated testing tools based on fuzz testing have problems achieving higher levels of code and state coverage. However, alternatives such as manual reverse engineering of the baseband scale poorly and are expensive.

Therefore, reliable detection methods for vulnerabilities in the decoding functions and state machines are needed. The decoding functions are important to protect against integrity and availability attacks. This can be supported by data for security testing that would allow better corner case testing, e. g., error states and illegal state machine transitions.

b) Prevention of Vulnerabilities: Control-flow hijacking, memory corruption, and state machine failures are well-known problems in the context of classic system security [128], [129], [130]. However, in mobile security, classic

system security defenses face certain challenges. Most notably, the real-time capability is a hard requirement for the baseband, as it needs to stay synchronized with the radio transmissions. In addition to the run-time overhead, many modern countermeasures come with a certain overhead, unreasonable for the baseband. Adapting classic system security countermeasures like memory-safe languages, memory address randomization, or control-flow integrity solutions in this constrained environment remain an open challenge [128], [129], [130].

Another way to reduce implementation bugs is to carefully choose the development framework based on their intrinsic security properties [172], [173]. Additionally, machine-readable protocol specifications and state machines would allow to generate parsers and state machines directly from the specification, cutting out the error-prone human interpretation of the specification. For parsing, part of the 3GPP specification already employs ASN.1. However, the parser libraries and compilers must be thoroughly tested and audited to avoid the fallout an ASN.1 compiler bug caused in 2016 [84], [170].

c) Current Scope: Within implementation security, the research community focuses mainly on the user equipment. However, it is very likely that other network components, e. g., the core network or base stations, suffer from similar vulnerabilities. For example, ASN.1 parsing is also implemented on the network side. Thus, it is not unlikely that the known ASN.1 vulnerabilities may also be present in network components. We therefore suggest the examination of network components as well.

Summary: Insecure implementations open attack vectors for adversaries with active radio capabilities or direct network access. Future research must provide more sustainable defenses of the classical system security context, e. g., control-flow integrity protection for basebands.

B. Cause: Leaky Implementation

Implementations in software and hardware can leak information about internal states in surprising or non-obvious ways. Besides using a provable secure, an implementation might leak enough information to circumvent the strong security measures due to the implementation insufficiencies.

1) Attacks: The SIM card stores the secret key for authentication and key derivation. Gaining access to this information breaks the security concept at its very core enabling decryption and impersonation.

Rao et al. [55] and Zhou et al. [56] have built a key reconstruction attack upon the cryptanalysis of Comp128v1 on Global System for Mobile Communications (GSM) SIM cards with chosen plaintexts and by using electromagnetic field probes. In 2015, Liu et al. [57] found that the AES-based *MILENAGE* algorithm on USIM implementations is susceptible to power-based side-channel analysis and were thus able to extract the secret key.

Assessment: The primary aim of such attacks is gaining access to the secret key and, thereby, undermining the confidentially requirement. However, once the key is known to the attacker, he/she might fulfill secondary attack aims. It may enable him/her to decrypt the radio communication with passive radio capabilities or to impersonate a subscriber by cloning the SIM card.

Even though the aforementioned attacks reveal one of the most valuable secrets in mobile networks, the attacks require temporary physical access to the SIM card. Thus, forging SIM card clones is more likely to happen through an internal attacker or through the device owners themselves than through external attackers.

2) Defenses: The proposed defenses for side-channel attacks are implementation-specific [55], [56], [57]. The common ground for all known defenses is to have constant time and power properties, thus not leaking information about the internal state and making it unfeasible to derive the secret key by non-invasive methods.

3) Research Questions and Challenges: The proposed countermeasures need to be adopted to SIM cards by the industry. Clear requirements for constant time and constant power properties in the specification would help to accelerate the process of adoption. Additionally, it could be helpful to require a third party certification regarding attack resistance. If asymmetric cryptography should make it into 5G USIMs, than this will pose additional challenges to side-channel prevention [98, §5.1.4.19].

An upcoming technology in the field of SIM cards is the *embedded SIM card* [159]. Embedded SIM cards enable the configuration of the users' credentials via the Internet and are permanently soldered into the user device. From a research perspective it is interesting to examine how embedded SIM cards are secured against side-channel attacks.

Summary: Leaky implementations reveal the secret key of the SIM card via unintended side-channel attacks. With the leaked key, an attacker can passively decrypt the communication or impersonate a victim. Future research needs to investigate new technologies with respect to their side-channel resistance, e. g., embedded SIM cards or asymmetric cryptography implemented on SIM cards.

VII. Root Cause: Protocol Context Discrepancy

This root cause is based on protocol context issues that are due to deploying a protocol that is not originally intended for the mobile network environment. Protocol properties are not harmful in a non-mobile network environment, but may be exploitable in a mobile environment if not adjusted properly.

A. Cause: Cross-Layer Information Loss

The layering of network stacks serves multiple important purposes such as implementation transparency (e. g., upper layers do not have to care about details of lower layers) and interoperability (e. g., upper layer applications can span or exchange data over multiple networks). However, such layering also means loss of information that might be needed at higher levels, e. g., at some point, IP addresses or connections need to be mapped to the subscriber identity.

1) Attacks: The lack of a strong binding between radio-level authentication and IP-service authentication is the source for multiple vulnerabilities. The literature show that the implementation of such mapping is vulnerable and can be tricked with simple IP-based attacks, such as spoofing of IP addresses [26], [96]. IP address spoofing can be exploited for over- and under-billing attacks and to reverse the isolation of the internals to the Internet network. IPv4 and IPv6 NAT middleboxes pose a threat to the users as well as for the mobile network operator [39], [49]. Similarly to the NAT middleboxes, the Packet Data Network Gateway (P-GW) rooting configuration seems to be a problem in cases that allow direct communication between two phones [94], [95]. Another related problem is the lack of security checks within the SIP-protocol. Manipulated SIP headers can be used to fake the caller ID with UE-originated SMS messages [91].

Assessment: All these attacks consider an attacker able to initiate user traffic and optional Internet traffic capabilities. Hence, all the attacks can be easily realized. The range of those attacks is network-wide, thus an attacker can be anywhere in the network and exploit the flaw. We see the trend that newer generations—especially LTE—are more prone to attacks that are based on cross-layer information loss. This happens because LTE aims to be a general-purpose network providing normal Internet connectivity, and the layering of stacks is more prominent in those networks.

2) Defenses: Higher-level services cannot solely rely on the transport layer security measures of the lower layers and their authentication. Since an attacker can access any network communication on the device, no data from the device should be trusted. A *secure binding* between the user's charging ID and the established connection suppresses any possible misuse [26]. Such a secure binding operates across the separated layers. Additionally, Peng et al. suggest active *de-authorization* of a connection and a *feedback-based mischarge correction* scheme for misbilling attacks [26]. Other mitigations built upon well-configured and maintained stateful firewalls to encounter threats due to misconfigured routers and NAT middleboxes [39], [49], [94], [95]. All defenses must be implemented at the core network by operator. While firewalls and the secure binding can by simply implemented, more advanced misbilling countermeasures, e. g., deauthorization or feedback-based mischarge correction need to be specified.

3) Research Questions and Challenges: The research question is, how protocols that were not originally designed for the use in mobile networks can be adapted in such a way that they prevent possible information loss across layers. For instance, instead of making it a duty of the higher service to connect the IP identity with the radio identity, some part of the core network could inject the radio identity into the IP stream. For all the countermeasures, it is important that no data from the user should be trusted, as it could be forged. However, such extensions must be carefully evaluated with respect to sustainability and performance. Additionally, currently discussed 5G additions such as software-defined networking and network virtualization, can introduce new ways for cross-layer information loss. Future research should evaluate whether new protocols introduce information losses.

Summary: Cross-layer information loss causes fraud or DoS attacks and is especially exploitable within newer generations. Countermeasures propose a secure binding between the separated network layers and firewalls. Future research must carefully observe new technological proposals, e. g., 5G network virtualization to avoid cross-layer information loss in the future generations to come.

B. Cause: Accounting Policy Inconsistency

Mobile networks come with a variety of billing methods. Some services are charged by time and geographical distance, others by data volume. In earlier networks, the different billing methods were straightforward to distinguish as they were based on different network services. However, data networks —such as the Internet—were originally not in mind when earlier networks were built. Another problem are transmission artifacts that occur on lower layers without the knowledge or control of higher layers, such as data retransmissions because of bad connectivity or packet loss. For example, some providers charge for TCP retransmissions while others do not. In addition, some providers have special charging policies for extra services such as music streaming. These policy inconsistencies lead to hidden channels that can be exploited for billing attacks (fraud attacks).

1) Attacks: Hidden channels for different protocols have been found, e. g., in the DNS protocol [174] or in TCP retransmissions [92], [93], both leading to under billing attacks. Additionally, TCP retransmission can also be exploited for over-billing attacks [92]. In this case, the attacker uses an existing connection to send unwanted TCP retransmissions to increase the victim's data usage. With the shift from the circuit voice to a packet-based voice switching, Voice over LTE (VoLTE) introduced a new attack surface for under-billing attacks using the RTP and the SIP protocol [94], [95]. As voice is traditionally charged according to call duration, the voice-related channels can be misused as a hidden channel to transport data and thereby circumvent the accounting mechanism.

Assessment: Most hidden channels are still exploited by an attacker with user traffic capabilities and optional Internet capabilities. Similar to the cross-layer information loss, these attacks are exploitable in the latest network generations and can be exploited everywhere in the network.

2) Defenses: To encounter the threat of accounting policy inconsistency, most countermeasures suggest the use of improved filtering at the gateway to detect possible misuses based on technologies like deep packet inspection, stateful protocol monitoring or ratio detection (of DNS packets or TCP retransmission) [92], [94], [95], [174]. These countermeasures need to be installed by the operators in the core network at the packet gateways to protect against revenue losses.

3) Research Questions and Challenges: In the future, more applications will utilize the IP connectivity for their service instead of using the special purpose services such as text messages and voice. These special purpose services originally generated a large proportion of the operators revenue.

To encounter revenue losses, operators have established new accounting policies, e. g., fixed rates for music or video streaming [175], [176]. Future research should evaluate how such new accounting policies lead to inconsistency and thus open hidden channels for billing attacks. Effective countermeasures against these hidden channels and thus a prevention of billing attacks are remaining challenges.

Summary: Inconsistent accounting policies open up the possibility for hidden channels, which allow to consume resources without being charged for the service. Future research must exclude the possibility for hidden channels by an early detection of conspicuous behavior, e. g., through anomaly detection.

VIII. Root Cause: Wireless Channel

The wireless channel is essential for realizing mobility in mobile networks. However, this versatility makes the channel also easily accessible by unauthorized persons within the range of the radio transmission. Additionally, the wireless channel has limited resources. Over time more effective modulations and transmission schemes have been developed to improve the wireless transmission performance by reducing transmission redundancies. The easy access to the wireless channel makes mobile networks prone to jamming attacks for which an attacker disturbs the communication between two parties in a targeted manner. Jamming attacks are DoS attacks and require an active radio attacker. As a result, the wireless channel is prone to several attacks and exhibits fundamental limitations such that we define it as a root cause.

A. Attacks

Jamming attacks disturb the communication by increasing the noise on the wireless channel. Most prior research has concentrated on the evaluation of different constant jamming strategies and their effectiveness [45], [46], [47], [177], [178]. While constant jamming attacks jam the entire communication bandwidth over time, smart jamming attacks are protocol-aware and intentionally jam certain control information that affect the rest of the communication. In general, smart jamming attacks are more cost-efficient. Lichtman et al. [44], [48], [179] demonstrated that LTE is particularly vulnerable to smart jamming.

Assessment: All jamming attacks require an active radio attacker who needs to be aware of the used frequencies and the bandwidth. For smart jamming attacks, the attacker requires knowledge of the protocol and needs to be synchronized with the cell to obtain the position of control information. Nevertheless, the hardware for such attacks is easily available [180], [181], in particular in the form of software defined radios such as USRPs [182]. While jamming attacks disturb the communication of all the victims, smart jamming attacks are more targeted. In all cases, the effective range of the attack is limited by the transmission power and location of the jammer. The motivation for jamming attacks is versatile. Besides simply obstructing the mobile service [183], jamming attacks can also serve as *downgrade attacks*.

B. Defenses

Different countermeasures against jamming have been proposed by the research community ranging from specification changes to smart implementations using different technologies, e. g., beamforming or spread-spectrum techniques [131]. So far, little effort has been devoted to implement or to evaluate jamming countermeasures in mobile networks. Furthermore, it is little known about jamming countermeasure implementations within commercial products and their deployment.

C. Research Questions and Challenges

Even though different defenses are proposed, none of them have been evaluated in detail for mobile networks. Such measures could negatively impact the transmission speed which is an important selling point for future network generations. Future research should explore the methods that were proposed or adopted by related fields [184], [185] and evaluate their fit and benefits to mobile network setups. The challenge is to integrate efficiently jamming countermeasures which typically linked to performance impairments, into the radio layer, still fulfilling quality of service requirements. This can be achieved by a specification that is dedicated for the use in critical networks with efficiency loss. Additional research should also consider new radio technologies like the narrowband LTE [186]. Hardening new generations against jamming attacks is especially important for the availability of safety-critical applications.

Summary: The wireless channel is open and easily accessible and, thus, can be exploited by jamming attacks. As a consequence, the adversary can impact the availability of services. So far, no strong defenses exist. Future research is challenged by the trade-off between efficient jamming countermeasures and high data rates to ensure the availability of safety-critical applications.

IX. Related Surveys

We finally compare our work to related surveys from a methodological perspective highlighting parallels and differences.

Unger et al. [12] compare messaging systems based on desired security features and usability aspects. In contrast to our work, their methodology does not include attacks. Tu et al. [15] directly map telephone spam attacks and their countermeasures, without an abstraction into causes and root causes. Acer et al. [13] identify research issues in the area of Android security and use a methodology that directly addresses the stakeholders who might fix the issues. Our approach has the most similarities with the recently published work by Sahin et al. [17] since they also categorize attacks and defenses into causes and root causes. However, they limit their considerations to telephony fraud. Unique to our approach is that we abstract attacks and defenses into causes and root causes for all the three mobile network generations and use this approach to derive research questions for future generations of mobile networks.

X. Conclusion

In this work, we introduced a systematization methodology for attacks and defenses in mobile networks. We derived technical causes and abstract root causes for existing vulnerabilities and discussed the impacts of attacks and defenses. We used this to derive challenges and research questions with respect to shortcomings of existing work and security implications for new 5G technologies. The results of our systematization have implications on future security research in mobile networks. We finally point to the major areas and challenges for future research on this topic.

Vulnerabilities in earlier generations of mobile networks were addressed through improvements in the following generations. However, the backward compatibility of systems and attack vectors for downgrade attacks render such vulnerabilities a continuing problem. Two factors are responsible for downgrade attacks: *unsecured pre-authentication traffic* and *openness of the wireless channel*. While protocol changes and new cryptographic methods (e. g., asymmetric cryptography) can address unsecured pre-authentication, the wireless channel requires more fundamental changes to provide security against jamming attacks. Future research must address the class of downgrade attacks to overcome these issues.

A related problem are *insecure inter-network protocols* (e. g., SS7 or Diameter) in such a way that these legacy systems represent a threat to users as well as network providers. While firewalls constitute a temporary solution, research should develop inter-network protocols that keep the misuse potential as low as possible by minimizing the number of trusted entities.

Insecure implementations of network components (e. g., smartphones or core network) are an attack vector that undermines the system's integrity and immediately affects many users. Research should focus on securing those implementations by adopting means of classical system security while considering the requirements of the mobile network.

Resource usage asymmetry led to the so-called signaling denial-of-service attacks. In future, the number of subscribers and thus the threat of such an attack increases (e. g., by a mobile phone botnet). Therefore, research should investigate protocol designs in which the resource usage is more balanced to mitigate the threat of signaling denial-of-service attacks.

Acknowledgment

This work has been supported by the Franco-German BERCOM Project (FKZ: 13N13741) co-funded by the German Federal Ministry of Education and Research (BMBF) and by the DFG Research Training Group GRK 1817/1.

This work was also sponsored by the *COMET K1* program by the Austrian Research Promoting Agency (FFG).

References

[1] The Statistics Portal, "Number of Mobile Phone Users Worldwide from 2013 to 2019," https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/, [Online; accessed 22-May-2017].

[2] ——, "Revenue Forecast Mobile Operators Worldwide," https://www.statista.com/statistics/371899/mobile-operator-total-revenue-forecasts/, [Online; accessed 22-May-2017].

[3] FirstNet, "FirstNet: First Responder Network Authority," http://www.firstnet.gov/, [Online; accessed 22-May-2017].

[4] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2016.

[5] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location Leaks on the GSM Air Interface," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2012.

[6] 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," 3rd Generation Partnership Project (3GPP), TS 24.301, 06 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/24301.htm

[7] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. K. Redon, and R. Borgaonkar, "New Privacy Issues in Mobile Telephony: Fix and Verification," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2012, pp. 205–216.

[8] Chris Paget, "Practical Cellphone Spying," in *DEFCON 19*, 2010.

[9] Mjølsnes, Stig F. and Olimid, Ruxandra F., "Easy 4G/LTE IMSI Catchers for Non-Programmers," in *Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS)*. Springer, 2017, pp. 235–246.

[10] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanärä, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2007.

[11] N. Golde and D. Komaromy, "Breaking Band," in *Recon*, jun 2016. [Online]. Available: https://comsecuris.com/slides/recon2016-breaking_band.pdf

[12] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2015, pp. 232–249.

[13] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. Mcdaniel, and M. Smith, "SoK: Lessons Learned from Android Security Research for Appified Software Platforms," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 433–451.

[14] J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, and E. Weippl, "IPv6 Security: Attacks and Countermeasures in a Nutshell," in *USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2014.

[15] H. Tu, Z. Zhao, and G.-J. Ahn, "SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 320–338.

[16] P. Gupta, B. Srinivasan, V. Balasubramaniyan, and M. Ahamad, "Phoneypot : Data-driven Understanding of Telephony Threats," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2015.

[17] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad, "SoK: Fraud in Telephony Networks," in *IEEE European Symposium on Security and Privacy (EuroSP)*. IEEE, 2017.

[18] R. P. Jover, "Some Key Challenges in Securing 5G Wireless Networks," *Electronic Comment Filing System*, Jan. 2017. [Online]. Available: https://www.fcc.gov/ecfs/filing/10130278051628

[19] S. Wagenknecht and M. Korn, "Hacking As Transgressive Infrastructuring: Mobile Phone Networks and the German Chaos Computer Club," in *ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW)*. ACM, 2016, pp. 1104–1117.

[20] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 1, no. 1, pp. 11–33, 2004.

[21] 3GPP, "Service requirements for the Evolved Packet System (EPS)," 3rd Generation Partnership Project (3GPP), TS 22.278, 10 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/22278.htm

[22] ——, "3GPP System Architecture Evolution (SAE); Security architecture," 3rd Generation Partnership Project (3GPP), TS 33.401, 06 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33401.htm

[23] ——, "3G security; Security architecture," 3rd Generation Partnership Project (3GPP), TS 33.102, 12 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33102.htm

[24] E. Thompson, "Army examines feasibility of integrating 4G LTE with tactical network," September 25, 2015, [Online; accessed 22-May-2017]. [Online]. Available: http://www.army.mil/article/87875/event16

[25] 3GPP, "Service aspects; Charging and billing," 3rd Generation Partnership Project (3GPP), TS 22.115, 04 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/22115.htm

[26] C. Peng, C.-Y. Li, H. Wang, G.-H. Tu, and S. Lu, "Real Threats to Your Data Bills: Security Loopholes and Defenses in Mobile Data Charging," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2014, pp. 727–738.

[27] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: an open-source platform for LTE evolution and experimentation," in *ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH)*. ACM, 2016, pp. 25–32.

[28] Osmocom, "OsmocomBB Open Source GSM Baseband Software Implementation," http://bb.osmocom.org, [Online; accessed 12-July-2016].

[29] B. Wojtowicz, "OpenLTE - An open source 3GPP LTE implementation," http://openlte.sourceforge.net/, 2015, [Online; accessed 05-April-2017].

[30] RangeNetworks, "Openbts," http://openbts.org/, [Online; accessed 05-April-2017].

[31] N. Nikaein, R. Knopp, F. Kaltenberger, L. Gauthier, C. Bonnet, D. Nussbaum, and R. Ghaddab, "OpenAirInterface: An Open LTE Network in a PC," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*. ACM, 2014, pp. 305–308.

[32] C. Timberg, "For Sale: Systems that can Secretly Track where Cellphone Users go Around the Globe," https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html, August 24, 2014, [Online; accessed 22-May-2017].

[33] Google Firebase, "Firebase cloud messaging," accessed 2017-04-09.

[34] Apple Inc., "Apple Push Notification service Overview," https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html#//apple_ref/doc/uid/TP40008194-CH8-SW1, [Online; accessed 06-April-2017].

[35] V. Prevelakis and D. Spinellis, "The Athens Affair," *IEEE Spectrum*, vol. 44, no. 7, pp. 26–33, 2007.

[36] J. Scahill and J. Begley, "The Great SIM Heist - How Spies Stole the Keys to the Encyption Castle," jan 2015. [Online]. Available: https://theintercept.com/2015/02/19/great-sim-heist/

[37] P. P. C. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G/WiMax Wireless Networks," *Computer Networks*, vol. 53, no. 15, pp. 2601–2616, 2009.

[38] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, "Effects of Signaling Attacks on LTE Networks," in *IEEE Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, 2013, pp. 499–504.

[39] W. K. Leong, A. Kulkarni, Y. Xu, and B. Leong, "Unveiling the Hidden Dangers of Public IP locationes in 4G/LTE Cellular Data Networks," in *ACM Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM, 2014, pp. 16:1–16:6.

[40] G. Kambourakis, C. Kolias, S. Gritzalis, and J. Park, "DoS Attacks Exploiting Signaling in UMTS and IMS," *Computer Communications*, vol. 34, no. 3, pp. 226–235, 2011.

[41] D. Yu and W. Wen, "Non-access-stratum request attack in E-UTRAN," in *IEEE Computing, Communications and Applications Conference (ComComAp)*. IEEE, 2012, pp. 48–53.

[42] C. Farivar, "Apple removes GPS functionality from Egyptian iPhones," 2008, http://www.macworld.com/article/1137410/Apple_removes_GPS_func.html.

[43] "Egypt tries to control the use of GPS by banning except with individual licences," 2008, http://www.balancingact-africa.com/news/en/issue-no-429/top-story/egypt-tries-to-contr/en.

[44] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to Hostile Interference," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2013, pp. 285–288.

[45] J. Xiao, X. Wang, Q. Guo, H. Long, and S. Jin, "Analysis and Evaluation of Jammer Interference in LTE," in *ACM International Conference on Innovative Computing and Cloud Computing (ICCC)*. ACM, 2013, pp. 46–50.

[46] R. P. Jover, "Security Attacks against the Availability of LTE Mobility Networks: Overview and Research Directions," in *IEEE Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE, 2013.

[47] F. M. Aziz, J. S. Shamma, and G. L. Stüber, "Resilience of LTE Networks against Smart Jamming Attacks: Wideband Model," in *IEEE Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2015, pp. 1344–1348.

[48] R. M. Rao, S. Ha, V. Marojevic, and J. H. Reed, "Lte phy layer vulnerability analysis and testing using open-source sdr tools," *arXiv preprint arXiv:1708.05887*, 2017.

[49] H. Hong, H. Choi, D. Kim, H. Kim, B. Hong, J. Noh, and Y. Kim, "When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks," in *IEEE European Symposium on Security and Privacy (EuroSP)*. IEEE, 2017.

[50] W. Enck, P. Traynor, P. McDaniel, and T. La Porta, "Exploiting Open Functionality in SMS-capable Cellular Networks," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2005, pp. 393–404.

[51] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 17, no. 1, pp. 40–53, 2009.

[52] N. Golde, K. Redon, and J.-P. Seifert, "Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks," in *USENIX Security Symposium (SSYM)*. USENIX Association, 2013, pp. 33–48.

[53] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. Mcdaniel, and T. L. Porta, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2009, pp. 223–234.

[54] T. Engel, "SS7: Locate. Track. Manipulate." in *Chaos Communication Congress*, ser. 31C3, 2014. [Online]. Available: https://berlin.ccc.de/{~}tobias/31c3-ss7-locate-track-manipulate.pdf

[55] J. R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, "Partitioning Attacks: or how to Rapidly Clone some GSM Cards," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2002, pp. 31–41.

[56] Y. Zhou, Y. Yu, F. X. Standaert, and J. J. Quisquater, "On the Need of Physical Security for Small Embedded Devices: a Case Study with COMP128-1 Implementations in SIM Cards," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2013, pp. 230–238.

[57] J. Liu, Y. Yu, F. X. Standaert, Z. Guo, D. Gu, W. Sun, Y. Ge, and X. Xie, "Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards," in *European Symposium on Research in Computer Security (ESORICS)*. Springer, 2015, pp. 468–480.

[58] A. Osipov and A. Zaitsev, "Adventures in Femtoland: 350 Yuan for Invaluable Fun," Black Hat USA 2015, 08 2015.

[59] B. Michau and C. Devine, "How to not Break LTE Crypto," in *ANSSI Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, 2016.

[60] D. Rupprecht, K. Jansen, and C. Pöpper, "Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness," in *USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2016.

[61] H. Welte, "OpenBSC - Running your own GSM network," 08 2009, talk at Hacking at Random 2009. Slides: https://openbsc.osmocom.org/trac/raw-attachment/wiki/FieldTests/HAR2009/har2009-gsm-report.pdf.

[62] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," in *ACM Annual Computer Security Applications Conference (ACSAC)*. ACM, 2014, pp. 246–255.

[63] A. Dabrowski, G. Petzl, and E. R. Weippl, "The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection," in *Symposium on Recent Advances in Intrusion Detection (RAID)*. Springer, 2016, pp. 279–302.

[64] K. Nohl, "Mobile Self-Defense," in *Chaos Communication Congress*, ser. 31C3, 2014. [Online]. Available: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

[65] L. Malette, "Catcher Catcher," 2015. [Online]. Available: https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher

[66] SecUpwN (Pseudonym, Maintainer), "Android IMSI-Catcher Detector," https://cellularprivacy.github.io/Android-IMSI-Catcher-Detector/, retrieved 2017-04-04.

[67] SR Labs, "Snoopsnitch," 12 2014, https://opensource.srlabs.de/projects/snoopsnitch, accessed Nov 12 2015.

[68] I. Briceno, Marc and Goldberg and W. David, "GSM Cloning," 2002. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[69] M. Briceno, I. Goldberg, and D. Wagner, "An implementation of the GSM A3A8 algorithm. (Specifically, COMP128.)," 1998, http://www.scard.org/gsm/a3a8.txt, accessed June 24th 2016.

[70] D. Kaljevic, "SIMSCAN v2.01," http://dejankaljevic.org/, accessed 2017-03-09, 2003.

[71] U. Meyer and S. Wetzel, "On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PRIMRC)*. IEEE, 2004, pp. 2876–2883.

[72] C.-K. Han and H.-K. Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks," *IEEE Transactions on Mobile Computing (TMC)*, vol. 13, no. 2, pp. 457–468, 2014.

[73] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communication," *Journal of Cryptology*, vol. 21, no. 3, pp. 392–429, aug 2008.

[74] M. Briceno, I. Goldberg, and D. Wagner, "A Pedagogical Implementation of A5/1." 1999. [Online]. Available: http://www.scard.org/gsm/a51.html

[75] S. Labs, "Kraken: A5/1 Decryption Rainbow Tables," via Bittorent, 2010, https://opensource.srlabs.de/projects/a51-decrypt, accessed Nov 12 2015.

[76] K. Nohl and C. Paget, "GSM – SRSLY?" in *Chaos Communication Congress*, ser. 26C3, dec 2009.

[77] J. D. Golić, "Cryptanalysis of Alleged A5 Stream Cipher," in *International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT)*. Springer, 1997, pp. 239–255.

[78] A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," in *International Workshop on Fast Software Encryption (FSE)*. Springer, 2000.

[79] K. Nohl and L. Melette, "Defending mobile phones," Chaos Communications Congress (28C3), 2011. [Online]. Available: https://events.ccc.de/congress/2011/Fahrplan/events/4736.en.html

[80] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert, "New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor," in *BlackHat*, 2017.

[81] S. Chalakkal, H. Schmidt, and S. Park, "Practical Attacks on VoLTE and VoWIFI," ERNW Enno Rey Netzwerke, Tech. Rep., 2017. [Online]. Available: https://www.ernw.de/download/newsletter/ERNW_Whitepaper_60_Practical_Attacks_On_VoLTE_And_VoWiFi_v1.0.pdf

[82] W. Zhang and H. Shan, "LTE Redirection: Forcing Targeted LTE Cellphone into Unsafe Network," in *Defcon*, 2016. [Online]. Available: https://media.defcon.org/DEFCON24/DEFCON24presentations/DEFCON-24-Zhang-Shan-Forcing-Targeted-Lte-Cellphone-Into-Unsafe-Network.pdf

[83] K. Nohl, "Rooting SIM cards," in *Blackhat*, 2013. [Online]. Available: https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf

[84] Ia-sadosky, "Heap memory corruption in ASN.1 parsing code generated by Objective Systems Inc. ASN1C compiler for C/C++," 2016. [Online]. Available: https://github.com/programa-stic/security-advisories/tree/master/ObjSys/CVE-2016-5080

[85] R.-P. Weinmann, "Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks," in *USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2012.

[86] F. van den Broek, B. Hond, and A. Cedillo Torres, "Security Testing of GSM Implementations," *Engineering Secure Software and Systems (ESSoS)*, vol. 8364, pp. 179–195, 2014.

[87] C. Mulliner, N. Golde, and J.-P. Seifert, "SMS of Death: from Analyzing to Attacking Mobile Phones on a Large Scale," in *USENIX Security Symposium (SSYM)*. USENIX Association, 2011, pp. 363–378.

[88] T. Court and N. Biggs, "WAP just happened to my Samsung Galaxy?" 2017, https://www.contextis.com/resources/blog/wap-just-happened-my-samsung-galaxy/, accessed 2017-02-05. [Online]. Available: https://www.contextis.com/resources/blog/wap-just-happened-my-samsung-galaxy/

[89] Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, and Y. Liu, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2017.

[90] vinatan Hassidim, Y. Matias, M. Yung, and A. Ziv, "Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats to BLE Beacons," 2016, https://developers.google.com/beacons/eddystone-eid-preprint.pdf.

[91] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2016, pp. 1118–1130.

[92] Y. Go, E. Jeong, J. Won, Y. Kim, D. F. Kune, and K. Park, "Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2014.

[93] Y. Go, D. F. Kune, S. Woo, K. Park, and Y. Kim, "Towards Accurate Accounting of Cellular Data for TCP Retransmission," in *ACM Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM, 2013.

[94] C.-Y. Li, G.-H. Tu, S. Lu, X. Wang, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Networks," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2015, pp. 316–327.

[95] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, "Breaking and Fixing VoLTE : Exploiting Hidden Data Channels and Misimplementations," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2015, pp. 328–339.

[96] Z. Wang, Z. Qian, Q. Xu, Z. Mao, and M. Zhang, "An Untold Story of Middleboxes in Cellular Networks," in *ACM SIGCOMM Computer Communication Review*. ACM, 2011, pp. 374–385.

[97] S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura, "Unblocking Stolen Mobile Devices using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR access," in *IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2015, pp. 1171–1176.

[98] 3GPP, "Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system," 3rd Generation Partnership Project (3GPP), TR 33.899, 08 2017. [Online]. Available: http://www.3gpp.org/ftp/specs/archive/33_series/33.899/

[99] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, "Privacy through Pseudonymity in Mobile Telephony Systems," in *Symposium on Network and Distributed System Security (NDSS)*. The Internet Society, 2014.

[100] 3GPP, "Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)," 3rd Generation Partnership Project (3GPP), TR 33.821, 06 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33821.htm

[101] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating IMSI Catchers," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2015, pp. 340–351.

[102] M. S. A. Khan and C. J. Mitchell, "Improving Air Interface User Privacy in Mobile Telephony," in *International Conference on Research in Security Standardisation (SSR)*, vol. 9497. Springer, 2015, pp. 165–184.

[103] G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik, "Untraceable Mobility or How to Travel Incognito," *Computer Networks*, vol. 31, no. 8, pp. 871–884, 1999.

[104] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Enhancing User Identity Privacy in LTE," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2012, pp. 949–957.

[105] G. Horn and B. Preneel, "Authentification and Payment in Future Mobile Systems," in *European Symposium on Research in Computer Security (ESORICS)*. Springer, 1998, pp. 183–207.

[106] G. Kambourakis, A. Rouskas, and S. Gritzalis, "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2004, no. 1, pp. 184–197, 2004.

[107] P. Ney, I. Smith, G. Cadamuro, and K. Tadayoshi, "Sea-Glass: Enabling City-wide IMSI-Catcher Detection," in *Privacy Enhancing Technologies Symposium (PETS)*. Springer, 2017.

[108] S. Park, A. Shaik, R. Borgaonkar, A. Martin, and J.-P. Seifert, "White-stingray: Evaluating IMSI catchers detection applications," in *USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2017.

[109] S. Steig, A. Aarnes, T. v. Do, and H. T. Nguyen, "A network based imsi catcher detection," in *2016 6th International Conference on IT Convergence and Security (ICITCS)*, Sept 2016, pp. 1–6.

[110] GSMK mbH, "Gsmk cryptophone," http://www.cryptophone.de/en/products/mobile/, 2017, [Online; accessed 03-April-2017].

[111] T. van Do, H. T. Nguyen, and N. Momchil, "Detecting IMSI-Catcher Using Soft Computing," in *Springer International Conference on Soft Computing in Data Science (SCDS)*. Springer, 2015, pp. 129–140.

[112] GSMK Gesellschaft für sichere Mobile Kommunikation mbH, "Gsmk debuts new security systems to protect mobile network operators against eavesdropping and fraud," http://www.cryptophone.de/en/company/news/gsmk-debuts-new-security-systems-to-protect-mobile-network-operators-against-eavesdropping-and-fraud/, 2017, [Online; accessed 03-April-2017].

[113] C. Technologies, "Protect yourself from cell phone interception," http://www.charontech.com/network_guard.html, accessed 2017-03-12.

[114] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, "Mutual Authentication and Key Agreement for GSM," in *IEEE International Conference on Mobile Business (ICMB)*. IEEE, 2006.

[115] C.-C. Chang, J.-S. Lee, and Y.-F. Chang, "Efficient Authentication Protocols of GSM," *Computer Communications*, vol. 28, no. 8, pp. 921–928, 2005.

[116] M. S. A. Khan and C. J. Mitchell, "Retrofitting Mutual Authentication to GSM using RAND Hijacking," in *International Workshop on Security and Trust Management (STM)*. Springer, 2016, pp. 17–31.

[117] C.-C. Lee, I.-E. Liao, and M.-S. Hwang, "An Efficient Authentication Protocol for Mobile Communications," *Telecommunication Systems*, vol. 46, no. 1, pp. 31–41, 2011.

[118] Ericsson, "Enhancements to GSM/UMTS AKA: 3GPP TSG SA WG3 Security, S3-030542," http://www.3gpp.org/ftp/tsg_sa/wg3_security/tsgs3_30_povoa/docs/pdf/S3-030542.pdf, [Online; accessed 06-April-2017].

[119] ——, "On the introduction and use of UMTS AKA in GSM: 3GPP TSG SA WG3 Security, S3-040534," ftp://www.3gpp.org/tsg_sa/WG3_Security/TSGS3_34_Acapulco/Docs/PDF/S3-040534.pdf, [Online; accessed 06-April-2017].

[120] S. Alt, P.-A. Fouque, G. Macario-rat, C. Onete, and B. Richard, "A Cryptographic Analysis of UMTS/LTE AKA," in *International Conference on Applied Cryptography and Network Security (ACNS)*. Springer, 2016, pp. 18–35.

[121] 3GPP, "3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification," 3rd Generation Partnership Project (3GPP), TS 35.202, 12 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/35202.htm

[122] *Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support*, GSM Association Std. SP-070 671, http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip.

[123] 3GPP, "Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification," 3rd Generation Partnership Project (3GPP), TS 44.006, 03 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/44006.htm

[124] P1Sec, "SS7 Security Map." [Online]. Available: http://ss7map.p1sec.com/

[125] M. Ashdown and S. Lynchard, "SS7 Firewall System," 2001. [Online]. Available: https://www.google.com/patents/US6308276

[126] T. Engel and H. Freyther, "Verfahren und eine vorrichtung zur sicherung einer signalisierungssystem- nr. 7-schnittstelle," DE Patent 102 014 117 713, 2016, also filed as US20160156647.

[127] 3GPP, "Study into routeing of MT-SMs via the HPLMN," 3rd Generation Partnership Project (3GPP), TR 23.840, 03 2007. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23840.htm

[128] N. Burow, S. A. Carr, J. Nash, P. Larsen, M. Franz, S. Brunthaler, and M. Payer, "Control-Flow Integrity: Precision, Security, and Performance," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, pp. 16:1–16:33, Apr. 2017.

[129] L. Szekeres, M. Payer, T. Wei, and D. Song, "SoK: Eternal War in Memory," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2013, pp. 48–62.

[130] P. Larsen, A. Homescu, S. Brunthaler, and M. Franz, "SoK: Automated Software Diversity," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2014, pp. 276–291.

[131] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the Security of LTE Networks against Jamming Attacks," *Journal on Information Security (EURASIP)*, vol. 2014, no. 1, p. 7, 2014.

[132] 3GPP, "Technical realization of the Short Message Service (SMS)," 3rd Generation Partnership Project (3GPP), TS 23.040, 09 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23040.htm

[133] PKI Electronic Intelligence GmbH Germany, "3G UMTS IMSI Catcher," http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/, 2017, [Online; accessed 03-April-2017].

[134] S. Biddle, "Long-Secret Stingray Manuals Detail how Police an Spy on Phones," pp. 1–10, sep 2016. [Online]. Available: https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/

[135] GSMK mbH, "Gsmk debuts new security systems to protect mobile network operators against eavesdropping and fraud," http://www.cryptophone.de/en/company/news/gsmk-debuts-new-security-systems-to-protect-mobile-network-operators-against-eavesdropping-and-fraud/, 2017, [Online; accessed 03-April-2017].

[136] "GSM security map," http://gsmmap.org/.

[137] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2005.

[138] 3GPP, "Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)," 3rd Generation Partnership Project (3GPP), TS 04.31, 06 2007. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/0431.htm

[139] P. Muncaster, "Chinese cops cuff 1,500 in fake base station spam raid," The Register, 26 Mar 2014, http://www.theregister.co.uk/2014/03/26/spam_text_china_clampdown_police/.

[140] S. K. Pell and C. Soghoian, "Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy." *Harvard Journal of Law & Technology*, vol. 28, no. 1, pp. 1–76, 2014.

[141] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, pp. 5–83, 1883.

[142] I. Goldberg, D. Wagner, and L. Green, "The (Real-Time) Cryptanalysis of A5/2," in *Rump session of Crypto'99*, 1999.

[143] O. Dunkelman, N. Keller, and A. Shamir, "A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony," 2010. [Online]. Available: http://eprint.iacr.org/2010/013

[144] K. Nohl and L. Melette, "GPRS Intercept: Wardriving your country," Chaos Communications Camp 2011, 2011.

[145] K. Jia, C. Rechberger, and X. Wang, "Green cryptanalysis: Meet-in-the-middle key-recovery for the full kasumi cipher," Cryptology ePrint Archive, Report 2011/466, 2011, http://eprint.iacr.org/2011/466.

[146] O. Dunkelman, N. Keller, and A. Shamir, "A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony," *Journal of Cryptology*, vol. 27, no. 4, pp. 824–849, 2014. [Online]. Available: http://dx.doi.org/10.1007/s00145-013-9154-9

[147] *Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features*, European Telecommunications Standards Institute Std. GSM 02.07, Rev. version 8.0.0 Release 1999, 1999.

[148] "Android Issue 5353: Ciphering Indicator," 2009, https://code.google.com/p/android/issues/detail?id=5353, accessed July 14th 2013.

[149] I. Androulidakis, D. Pylarinos, and G. Kandus, "Ciphering Indicator Approaches and User Awareness," *Maejo International Journal of Science and Technology*, vol. 6, no. 3, pp. 514–527, 2012.

[150] U. Meyer and S. Wetzel, "A Man-in-the-Middle Attack on UMTS," in *ACM Workshop on Wireless Security (WiSe)*. ACM, 2004, pp. 90–97.

[151] 3GPP, "SIM/USIM internal and external interworking aspects," 3rd Generation Partnership Project (3GPP), TR 31.900, 12 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/31900.htm

[152] ——, "3G Security; Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS," 3rd Generation Partnership Project (3GPP), TS 55.226, 02 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/55226.htm

[153] ——, "3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification," 3rd Generation Partnership Project (3GPP), TS 35.206, 12 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/35206.htm

[154] ——, "Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*;," 3rd Generation Partnership Project (3GPP), TS 35.231, 12 2015. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/35231.htm

[155] ——, "Proximity-based Services (ProSe); Security aspects," 3rd Generation Partnership Project (3GPP), TS 33.303, 12 2009. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33303.htm

[156] M. Groves, "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption," https://tools.ietf.org/html/rfc6507, [Online; accessed 12-July-2016].

[157] ——, "Sakai-Kasahara Key Encryption (SAKKE)," https://tools.ietf.org/html/rfc6508, [Online; accessed 12-July-2016].

[158] S. J. Murdoch, "Insecure by Design: Protocols for Encrypted Phone Calls," *IEEE Computer*, vol. 49, no. 3, pp. 25–33, 2016.

[159] GSM Association, "Remote Provisioning Architecture for Embedded UICC Technical Specification (27 May 2016)," http://www.gsma.com/iot/wp-content/uploads/2016/07/SGP.02_v3.1.pdf, [Online; accessed 06-April-2017].

[160] T. Engel, "Locating Mobile Phones using Signalling System 7," in *Chaos Communication Congress*, ser. 25C3, dec 2008. [Online]. Available: http://events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf

[161] S. Holtmanns, S. P. Rao, and I. Oliver, "User Location Tracking Attacks for LTE Networks using the Interworking Functionality," in *IFIP Networking Conference and Workshops*, 2016, pp. 315–322.

[162] S. P. Rao, B. T. Kotte, and S. Holtmanns, "Privacy in LTE networks," in *ICST International Conference on Mobile Multimedia Communications*, 2016, pp. 176–183.

[163] Verint, "Skylock Product Description 2013," 2013. [Online]. Available: http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/

[164] M. Guri, Y. Mirsky, and Y. Elovici, "9-1-1 DDoS via Malicious Baseband Firmware," in *IEEE European Symposium on Security and Privacy (EuroSP)*. IEEE, 2017.

[165] C. Yang, "Weather the signaling storm," Huawei, Tech. Rep. 61, 2011. [Online]. Available: http://www1.huawei.com/en/static/HW-094153.pdf

[166] Ericsson, "Handling of Signaling Storms in Mobile Networks: The Role of the User Data Management System," Ericsson, Tech. Rep., 2015. [Online]. Available: https://www.ericsson.com/res/docs/2015/handling-of-signaling-storms-in-mobile-networks-august.pdf

[167] W. Simpson, "RFC 6013: TCP Cookie Transactions (TCPCT)," 2011, [Online; accessed 22-May-2017]. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6013.txt

[168] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference (Crypto)*. Springer, 1992, pp. 139–147.

[169] A. Back, "Hashcash-a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002, [Online; accessed 22-May-2017].

[170] D. Goodin, "Software Flaw puts Mobile Phones and Networks at Risk of Complete Takeover," jul 2016. [Online]. Available: https://arstechnica.com/security/2016/07/software-flaw-puts-mobile-phones-and-networks-at-risk-of-complete-takeover/

[171] Aaron Brown, "WARNING: This text message will CRASH and reboot YOUR iPhone," http://www.express.co.uk/life-style/science-technology/580211/iPhone-Messages-iMessage-Bug-Text-Reboot-Crash, June 2015.

[172] V. D'Silva, M. Payer, and D. Song, "The Correctness-Security Gap in Compiler Optimization," in *IEEE CS Security and Privacy Workshops*. IEEE, 2015. [Online]. Available: http://spw15.langsec.org/papers/dsilva-gap.pdf

[173] E. Jaeger and O. Levillain, "Mind your language (s): A discussion about languages and security," in *IEEE Security and Privacy Workshops (SPW)*. IEEE, 2014, pp. 140–151.

[174] C. Peng, C.-y. Li, G.-H. Tu, S. Lu, and L. Zhang, "Mobile Data Charging: New Attacks and Countermeasures," in *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2012, pp. 195–204.

[175] Telekom, "StreamOn Optionen," https://www.telekom.de/unterwegs/tarife-und-optionen/streamon, [Online; accessed 06-April-2017].

[176] T-Mobile, "Binge On," https://www.t-mobile.com/offer/binge-on-streaming-video.html, [Online; accessed 06-April-2017].

[177] S. Bhattarai, S. Wei, S. Rook, W. Yu, R. F. Erbacher, and H. Cam, "On Simulation Studies of Jamming Threats Against LTE Networks," in *IEEE International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2015, pp. 99–103.

[178] G. Philippe, F. Montaigne, J.-c. Schiel, E. Georgeaux, C. Gruet, P.-y. Roy, P. Force, and P. Mège, "LTE Resistance to Jamming Capability," in *Military Communications and Information Systems Conference (MCC)*, 2013, pp. 7–9.

[179] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-a Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[180] Jammer-Store.com, "Jammer-Store," http://www.jammer-store.com/, 2016.

[181] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *arXiv*, 2016. [Online]. Available: http://arxiv.org/abs/1607.05171

[182] Ettus Research, "Universal Software Radio Peripheral," https://www.ettus.com/product, [Online; accessed 22-May-2017].

[183] Andrew Dalton, "Florida man fined 48k for jamming cellphones while driving," https://www.engadget.com/2016/05/25/florida-man-fined-48k-fcc-jamming-cellphones/, May 2016, [Online; accessed 22-May-2017].

[184] S. Khattab, D. Mosse, and R. Melhem, "Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?" in *ACM International Conference on Security and Privacy In Communication Netowrks (SecureComm)*. ACM, 2008.

[185] C. Pöpper, M. Strasser, and S. Čapkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, Jun 2010.

[186] 3GPP, "Standardization of NB-IOT completed," 2016, [Online; accessed 06-April-2017]. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete

Mobile Communications Acronyms

3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
EDGE	Enhanced Data Rates for GSM Evolution
eNodeB	Evolved NodeB
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
GCM	Google Cloud Messaging
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSS	Home Subscriber Server
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IMS	IP Multimedia Subsystem
LA	Location Area
LTE	Long Term Evolution
MAC	Message Authentication Code
MitM	Man-in-the-Middle
MSISDN	Mobile Station Integrated Services Digital Network Number
NAT	Network Address Translation
OTA	Over-the-Air
P-GW	Packet Data Network Gateway
PSTN	Public Switched Telephone Network
PKI	Public Key Infrastructure
QoS	Quality of Service
RAN	Radio Access Network
RTP	Real-Time Transport Protocol
SDR	Software Defined Radio
SIP	Session Initiation Protocol
SS7	Signalling System #7
TA	Tracking Area
TMSI	Temporary Mobile Subscriber Identity
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
VoLTE	Voice over LTE

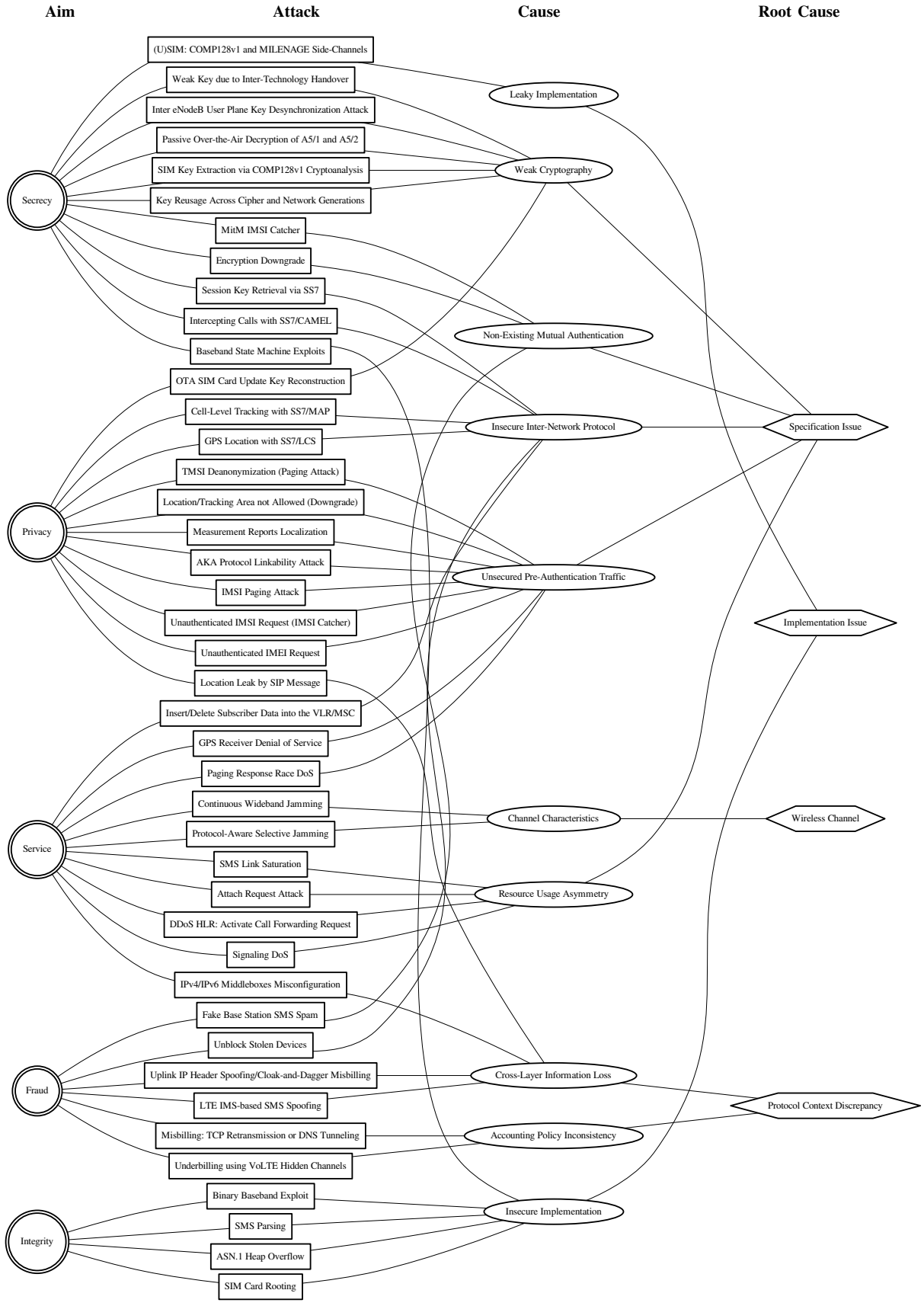

Fig. 3. Visualization of Systematization including Attack Aims, Attacks, Causes, and Root Causes.