Rao, Siddharth Prakash; Chen, Hsin Yi; Aura, Tuomas

Threat modeling framework for mobile communication systems

Published in:
Computers and Security

DOI:
10.1016/j.cose.2022.103047

Published: 01/02/2023

Document Version
Publisher's PDF, also known as Version of record

Computers & Security 125 (2023) 103047

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Threat modeling framework for mobile communication systems

Siddharth Prakash Rao [a,*], Hsin-Yi Chen [b], Tuomas Aura [b]

[a] Nokia Bell Labs, Espoo Finland
[b] Aalto University, Espoo, Finland

ARTICLE INFO

Article history:
Received 9 June 2022
Revised 12 October 2022
Accepted 1 December 2022
Available online 5 December 2022

Keywords:
Threat modeling
Security framework
Mobile communication

ABSTRACT

This paper presents a domain-specific threat-modeling framework for the cellular mobile networks. We survey known attacks against mobile communication and organize them into attack phases, tactical objectives, and techniques. The *Bhadra framework* aims to provide a structured way to analyze and communicate threats on a level that abstracts away the technical details but still provides meaningful insights into the adversarial behavior. Our goals are similar to existing threat modeling frameworks for enterprise information systems, but with a focus on mobile operator networks. The framework fills a gap that has existed in tools and methodology for sharing of threat intelligence within and between organizations in the telecommunications industry. The paper includes concrete case studies of applying the framework. It can also be read as a survey of attacks against mobile networks.

CCS CONCEPTS

Security and privacy → Security requirements; Mobile and wireless security; **Networks**→ Networks Mobile networks

1. Introduction

The goal of mobile telecommunication networks is to establish ubiquitous, reliable and ever faster communication while maintaining interoperability between the industry players and backward compatibility with previous technology generations. Security of the user communication and network infrastructure are also critical requirements. It is, however, difficult to form a comprehensive picture of the security architecture and the threats against it. This is because, after over three decades of evolution, the mobile networks have become a complex ecosystem of businesses, components and interfaces that combines communication and security technologies and trust models from different eras.

Mobile network security evolved in a closed environment where the standards are agreed between technology companies, where software components are proprietary, and where the networks were initially run by a small number of trusted national or regional operators. In the early years, the designers focused on encryption on the radio interface, and security in the rest of the network was achieved by restricting access and knowledge to a closed group of professionals. Over the last decades, the telecommunications market has gradually opened to new players, the networks have adopted IP network technology, and they have been connected to the Internet at both the control and data layers. Nevertheless, in many ways, the old security model still prevails. There is no consistently deployed security architecture or security protocols for the operator core networks and interconnections between operators. Moreover, security failures are not discussed openly or even between close business associates. There are no shared tools for conducting security audits and no public datasets about security threats or known vulnerabilities. There is clearly a need for a more open discussion of the security threats against mobile communication and tools for sharing information about them.

One approach to sharing information about threats and potential attacks against complex information systems is *threat modeling*, i.e., methods for the description and characterization of known threats and attacks. On the one hand, the goal of threat modeling is to provide a conceptual framework, abstractions, and tools for analyzing threats with the view of mitigating them. On the other hand, it can be used for communicating information about the threats to engineers, managers, industry partners, and customers. The best-known approach to threat modeling is the MITRE ATT&CK (Strom et al., 2018) framework for modeling threats against enterprise information systems.

* Corresponding author.
E-mail addresses: sid.rao@nokia-bell-labs.com (S.P. Rao), hsin-yi.chen@aalto.fi (H.-Y. Chen), tuomas.aura@aalto.fi (T. Aura).

https://doi.org/10.1016/j.cose.2022.103047

There is currently no domain-specific threat modeling framework for mobile communications. Threat landscape studies and best-practice guidelines by standards and other governance bodies (ENISA, 2020; GSM Association, 2019) use generic threat models. Also, information about attacks is communicated mainly in the form of message sequence charts. While the charts are an industry-standard way to document case studies, they do not capture much insight on the high-level adversarial behavior.

This article surveys the threat landscape in mobile telecommunications and present a domain-specific threat modeling framework. The framework aims to be an immediately useful tool for the analysis and description of attacks within organizations, and it defines terminology and concepts for communicating meaningful high-level information about threats to management, customers and partners. We also hope that the framework is a starting point for an industry-wide shift towards a more open discussion of threats and attacks in the telecommunications systems. We have already contributed the work to GSM Association for this purpose. The structure and terminology of the MITRE framework has been reused where possible. However, there are substantial differences dues to the different architecture, attack surfaces, and trust models in mobile telecommunication networks compared to enterprise information systems. The framework is built on publicly available knowledge. The attack examples are mostly from the research literature, consulting reports, and public presentations. The reason is that there is currently little public information available about the attacks that have been observed in the real world.

The framework focuses on the 2G, 3G and 4G technologies based on 3GPP standards. This is partly because these are still the most widely deployed mobile communications systems, and partly for the goal of documenting domain-specific knowledge that is not receiving sufficient attention. 5G networks will combine telecommunications protocols with the more general web and cloud platforms and layers of virtualization, and industry discussion of 5G security has focused on such new aspects. Nevertheless, the mobile-specific threats that motivate our framework are still relevant in 5G and beyond. Thus, our telecommunications-focused work provides necessary background information for the design of the future technology generations.

Contributions— The contributions of our work are the following. The article provides a comprehensive overview of different components of mobile communications and identify the potential threat actors. Based on a systematic methodology, we present the *Bhadra framework* (name based on a Sanskrit word for *secure*) that models the threats against mobile communication systems. The framework categorizes publicly known attacks into nine tactical categories and, in the current version, 55 different techniques. We also show with case studies how the framework captures adversarial behavior. The article can also serve as a survey of publicly known threats against mobile telecommunication.

Structure— Section 2 describes the motivation for this work. Section 3 explains the mobile network architecture and potential entry points for adversaries. Section 4 introduces the Bhadra framework and the methodology used in its construction. Sections 5, 6 and 7 dive into the attack mounting, execution and results phases, respectively. Section 8 presents the case studies. Section 9 discusses the significance and also the limitations of our work, and Section 10 concludes the article.

2. Motivation

Threat modeling and analysis is an essential part of designing a secure system. It is a systematic, iterative process that involves identifying critical assets that need to be protected, identifying threats and assessing risks, defining security requirements, and recommending steps to mitigate the threats and to reduce the risks. There are various generic threat modeling and analysis frameworks (Shostack, 2014) (e.g., STRIDE, DREAD and PASTA), each with its own advantages and disadvantages (Bodeau et al., 2018; Selin, 2019). The frameworks and tools can be used for *threat analysis* where the goal is to enumerate previously unknown threats and find potential vulnerabilities in a system. They can also be used for *threat modeling* as a process of describing, characterizing and communicating known threats and attacks. The focus of our work is on the latter.

Applying the generic frameworks to a specific domain requires careful adaptation and combination. For instance, STRIDE is intended for analyzing software vulnerabilities and assumes access to the source code. However, STRIDE is often applied also to other types of distributed systems based on only a high-level specification. As the target system becomes more mature and the focus shifts from the generic threats to domain-specific ones, there arises the need for a domain-specific threat modeling framework with its own taxonomy of threats, vulnerabilities, and attacks. Such dedicated threat models exist, e.g., for storage systems (Hasan et al., 2005) and industrial control systems (Schlegel et al., 2015).

Despite the age of mobile communication systems and the growing number of threats against them, there are no threat modeling frameworks explicitly dedicated to them. The thesis by Kotapati (2008) from 2008 was one of the few attempts to define a threat model for GSM networks. The 2G network now coexists with later generations of technology with various components and features that did not exist in GSM. The systematization of knowledge (SoK) genre of academic literature about mobile communication as a whole (Rupprecht et al., 2018) or as subsystems (Ferrag et al., 2018; Rupprecht et al., 2018; Sahin et al., 2017; Spensky et al., 2016) points to the growing need of the community for systematic organization of knowledge. Our primary motivation is to create a domain-specific threat modeling framework for mobile communication systems. It should be focused on the mobile domain but sufficiently agnostic to the specific underlying technologies to model domain-specific threats against both current and future generations of technology.

Our other motivation comes from the requirements of a large mobile network technology vendor. The company comprises a wide range of employees: engineers who build end-to-end mobile communication systems, technical sales and marketing who sell the products and services to mobile operators, researchers who contribute to both existing and future solutions, standardization experts who exchange knowledge with other industry players by participating in standards committees, and technical support that assists customers with day-to-day deployment and operations. All these teams share the responsibility for securing the deployed systems. Despite having in-depth technical knowledge required for their respective roles, one problem they currently face is the lack of a common conceptual framework to capture the security of the entire system on a high level. The company already uses enterprise threat modeling frameworks, including MITRE ATT&CK (Strom et al., 2018; 2017) on the enterprise IT side, and they believe a dedicated framework for mobile communication systems that can co-exist with the existing enterprise ones will be useful.

Due to the complex nature of the mobile communication systems, we also believe that a common conceptual framework is needed to communicate security-related issues between industry players in the mobile sector. These companies rely heavily on the resources produced by the 3rd Generation Partnership Project (3GPP) in the form of normative technical specifications (TS) and informative technical reports (TR). For example, series 33 (3rd Generation Partnership Project, 1999–2022b) and 35 (3rd Generation Partnership Project, 1999–2022a) provide in-depth knowledge of the security of the individual subsystems. Other regulatory bod-

ies such as the GSM Association (GSMA), the National Institute of Standards and Technology (NIST), and European Union Agency for Cybersecurity(ENISA) produce security studies and guidelines that complement the 3GPP efforts. They also produce resources that summarize attacks on mobile communication systems (ENISA, 2020; Franklin et al., 2016; GSM Association, 2019). While these documents provide a lot of useful information, they do not replace systematic threat models as engineering and communication tools.

Furthermore, the technical specifications and security literature rely on *message sequence charts* (also known as *sequence diagrams*) as a standard format for communicating network protocols and related vulnerabilities. Given the protocol-heavy nature of the mobile communication systems, the charts are valuable as an unambiguous, message-by-message description of the potential attacks. However, they fail to capture the full life cycle of adversarial behavior and do not provide high-level insights that help to avoid similar security failures in other protocols or technology generations. We believe that a threat modeling framework can provide a level of abstraction that will reveal such relations.

To this end, our goal is to design a domain-specific framework that includes a common conceptual framework, taxonomy and categorization for threats and attacks against mobile communications systems. The threat models should be simple and easy to understand by the different technical roles in the sector, and yet they should retain enough information to be a useful engineering and communication tool.

3. Background

Step changes in mobile communication network technology and architecture are called *generations*, while the incremental development of the standards by the 3GPP is staged in *releases*. Each release and generation is expected to overcome the limitations of the previous generation with improved capabilities, such as bandwidth, latency, and security. The first generation (1G) used analog network signals and only supported voice calls. Digital signals have dominated since the second generation (2G) or Global System for Mobile Communications (GSM). The digital signaling channels in GSM enabled the revolutionary Short Message Service (SMS) service. The network gradually gained mobile data and Internet access capabilities: the General Packet Radio Service (GPRS) and Enhanced Data rates for GSM (EDGE). These networks are connection-oriented, i.e., they use circuit switching with a dedicated route between the source and destination for both voice and data, with handovers to enable mobility. The Multimedia Messaging Service (MMS) tried to build on the success of SMS by introducing value-added services, such as multimedia messaging and video calls, over these data services. The third generation (3G) or Universal Mobile Telecommunications System (UMTS) introduced connectionless packet switching for improved speed and reliability for data. With that, mobile users could finally access Internet services such as streaming media. The fourth generation (4G) or Long Term Evolution (LTE) increased the bandwidth and lowered the latency of the mobile Internet connection, which contributed to the growth of mobile broadband as a ubiquitous alternative to fixed Internet access. In the most up-to-date 4G networks, both voice (Voice over LTE) and data are transmitted over the IP protocol. We refer the reader to Rost et al. (2016) for more details about the evolution of the mobile network architecture.

3.1. Mobile network topology

This section gives an overview of modern mobile network architecture (Fig. 1) and its subsystems as technical background for the rest of the article. Note that we will mainly discuss the currently co-existing generations from 2G to 4G.

3.1.1. User equipment (UE)

User Equipment (or mobile station in GSM) is the mobile device used by a mobile subscriber for accessing the network. The Subscriber Identification Module (SIM), called Universal Integrated Circuit Card (UICC) in the latest standards, is an embedded smart card inside the phone. The UE provides the hardware and software, while the SIM card contains a mobile subscription profile and cryptographic keys needed for connecting to mobile networks. Each SIM card has a unique identifier, International Mobile Subscriber Identity (IMSI). Furthermore, each SIM card slot is associated with another unique identifier, International Mobile Equipment Identity (IMEI).

Both IMSI and IMEI are transmitted over the air to establish radio channels between the UE and the mobile network, and they are not visible to the user. The Mobile Station International Subscriber Directory Number (MSISDN) is the user's phone number. The IMSI, MSISDN, and IMEI are unique long-term identifiers in mobile device or user, and they will change only when the user changes the mobile subscription or equipment. Mobile networks frequently check that the user has a valid subscription. To avoid the repetitive use of IMSI, the network gives the UE an alternative short-lived identifier such as Temporary Mobile Subscriber Identity (TMSI) or Globally Unique Temporary ID (GUTI).

3.1.2. Radio access network (RAN)

The radio access network (RAN) is the first point of network access. It wirelessly connects the UE to the core network, which then provides the telecommunication services. The RAN comprises base stations, i.e., cell towers. The standard names for these are Base Transceiver Station (BTS) in 2G and NodeB 3G. Furthermore, the evolved NodeB (eNodeB) and smart cells of the 4G domain provide air connectivity with additional features such as support for voice over Wi-Fi.

The radio access network is responsible for maintaining the UE's connection to the network when the user is moving, and handover mechanisms transition the UE between base stations and even between different generations of RANs. The UE keeps the cellular network informed about its location by sending location updates and responding to paging by the network.

3.1.3. Core network (CN)

The core network (CN) is responsible for managing mobility of the users by interacting with the RAN, for initiating connections with other network operators, and for delivering telecommunications services, such as voice calls, SMS, and data connections. Figure 1 shows the critical nodes in the 2G and 3G packet/voice domains and in the 4G Evolved Packet Core (EPC) domain as parts of CN.

Home Subscriber Server (HSS) in the 4G EPC domain is the master database that maintains user and subscription information (e.g., IMSI and MSISDN). HSS is responsible for user authentication and access authorization based on the user's subscription plan. HSS is also in charge of mobility management and supporting call and data session establishment, for example, by keeping track of the user's location. *Home Location Register (HLR)* and Authentication Center (AuC) perform the equivalent functions in the 2G and 3G packet/voice domain.

Serving Gateway (SGW) and *Packet Data Network Gateway (PGW)* in the EPC domain are the user-plane gateway nodes that route and filter the IP traffic between the UE and external networks. More specifically, SGW is the point of interconnection between RAN and CN, whereas PGW connects CN to external networks, including the public Internet and other mobile operators. They both support accounting and charging, user mobility, and lawful interception on the user plane. *Gateway GPRS support node (GGSN)* and

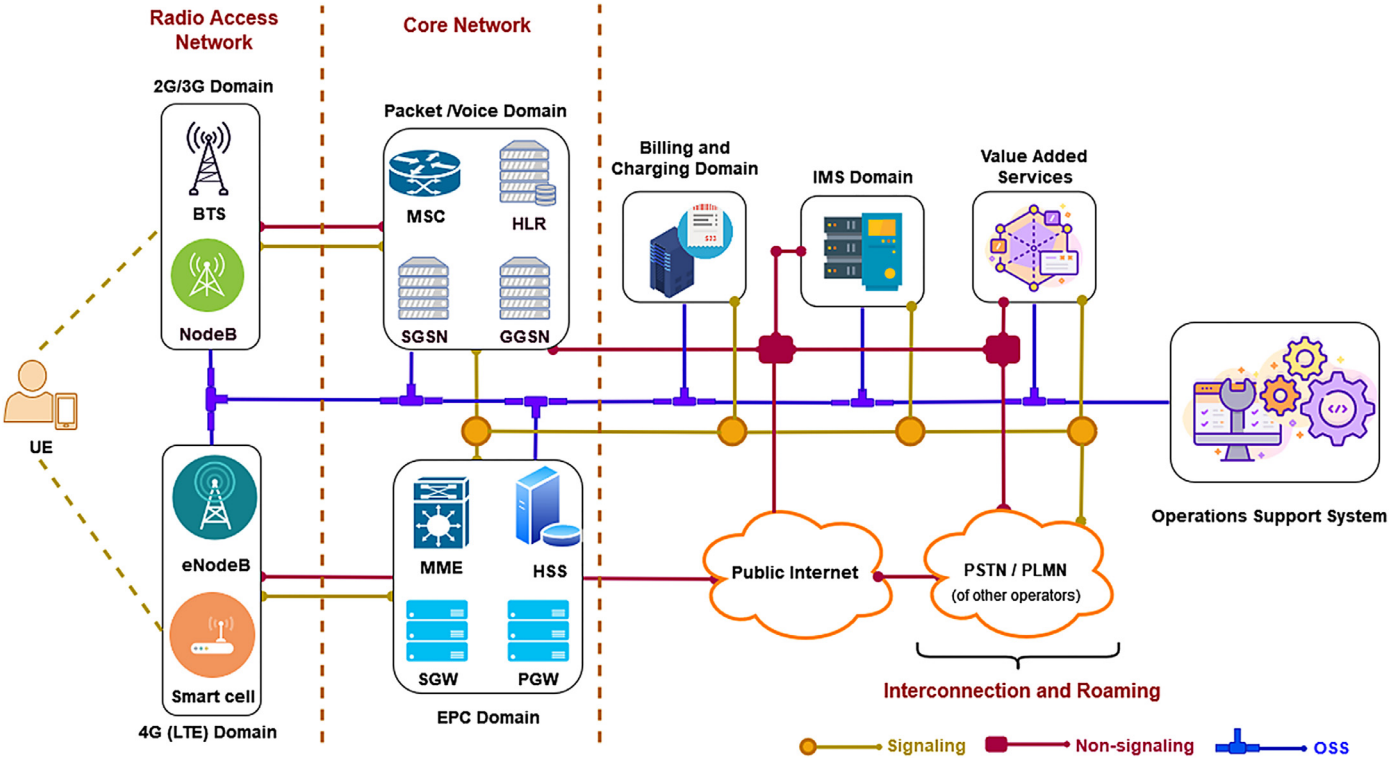

Fig. 1. Mobile network architecture.

Serving GPRS support node (SGSN) provide similar functionality in the 2G and 3G networks.

Mobility Management Entity (MME) handles the control plane traffic in 4G networks. More specifically, it handles signaling related to session and mobility management, user authentication with the help of HSS, and selection of the gateways. MME is also responsible for the lawful interception on the control plane. The *Mobile Switching Center (MSC)* provides similar functionality in 2G and 3G networks.

3.1.4. IMS and value-added services

The operator network additionally comprises the IP multimedia subsystem (IMS), value-added services, and billing and charging domain. The IMS domain integrates mobile and fixed voice communications with Internet technologies. IMS builds on the Session Initiation Protocol (SIP) (Handley et al., 1999), which establishes voice calls and other media connections over IP networks. Moreover, the mobile operators partner with third-party vendors to offer value-added services, such as missed-call and answerphone services, mobile commerce and advertisements, gaming, and on-demand streaming.

3.1.5. Billing and charging

The billing and charging domain was earlier a part of the core network (Kuhne et al., 2011) but has been moved to a separate domain so that it can be used for billing other services such as those provided by IMS and value-added services. With mobile payment or direct carrier billing, mobile users can make purchases from registered third-party vendors offline and online, and the value of the purchase is charged to the user's mobile bill.

3.1.6. Operations support systems (OSS)

Most operators support multiple generations of mobile network infrastructure from 4G all the way back to 2G. They also combine equipment from multiple manufacturers. Given the heterogeneous and complex nature of the networks, the mobile operators collaborate with external OSS vendors to manage, configure, and monitor their networks. OSS features have not been standardized and thus depend on the vendor. OSS requires a connection to every supported node in the RAN, CN, and IMS, and billing and charging for managing, troubleshooting, and maintenance purposes.

3.1.7. Interconnection and roaming

So far, we have described the network subsystems that belong to a single mobile operator. These network subsystems are collectively referred to as a Public Land Mobile Network (PLMN). Each operator owning such a PLMN, possibly along with their fixed Public Switched Telephone Network (PSTN), communicates with other operators to provide seamless mobile communication. Also, operators cooperate to enable roaming, i.e., vising another operator's network. Each mobile network also connects its users to the public Internet, for example, for mobile browsing and applications. We use *interconnection and roaming* as a generic term to refer to the operator-to-operator communication.

3.2. Communication between the networks

This sections gives a high-level overview of how the subsystems communicate with each other or within themselves.

3.2.1. UE to RAN

User equipment connects to the base stations in RAN over radio channels. In GSM, only the UE authenticates itself to the network, whereas in 3G and 4G, the Authentication and Key Agreement (AKA) protocol provides mutual authentication. The created session keys protect the communication between the UE and the network.

3.2.2. Core network to other networks

The 2G and 3G networks have Signalling System 7 (SS7) as the control-plane protocol. SS7 was developed in the days of fixed

landlines to exchange information between signaling points and then adapted to mobile networks. SS7 historically had its own protocol stack. The modern SS7 stack, SIGTRAN, has been run over IP. In 4G, the natively IP-based Diameter protocol is replacing SS7. Both SIGTRAN and Diameter have Stream Control Transmission Protocol (SCTP) as the transport layer. SCTP is a reliable transport layer like TCP but message-oriented, and it supports failover in case of endpoint failure. Inter-generation signaling between 2G/3G and 4G is facilitated by Inter Working Functions (IWF) in the mobile networks.

SIGTRAN and Diameter are also used for signaling between operators. The IR.34 guidelines for inter-service-provider IP backbone (GSM Association, 2018) recommend Internet Protocol Security (IPsec) or other VPN technologies for protecting the connections. However, it is unclear how widely these technologies are deployed, and many operators may still rely on non-cryptographic techniques to isolate the control plane from potential attackers.

GPRS Tunnelling Protocol (GTP), which tunnels user data to the Internet in 2G and 3G, has its own control-plane protocol GTP-C for maintaining data paths. These protocols are IP-based.

3.2.3. OSS to other networks

OSS relies mainly on the Common Management Information Protocol (CMIP) and Simple Network Management Protocol (SNMP) for remote configuration and management of the network nodes. As the OSS is not standardized, operators may use other protocols for network management, including Secure Shell (SSH), File Transfer Protocol (FTP), Simple Object Access Protocol (SOAP), and Representational State Transfer (REST).

3.3. Potential adversaries

This section outlines the threat actors against mobile communication. They may be outright malicious adversaries, such as cybercriminals and rogue governments, or from honest organizations and systems that were compromised on the technical or human level. Since our threat model is primarily technical, we group the potential attackers based on their technical capabilities and not by their motivation.

3.3.1. External attacker on the radio link

The radio interface has historically been the weakest link in wireless communication. However, ever since digital communication and encryption in GSM prevented casual interception of phone calls, the radio link has received relatively little attention. In recent years, inexpensive hardware (Ettus Research, 2022), software-defined radio, and open-source software modules (Gomez-Miguelez et al., 2016) have made it possible for researchers to experiment with radio interfaces without access to expensive telecommunications labs and test equipment. The same technology gives adversaries with limited resources the opportunity to build attack tools that undermine the security of the radio channels. These tools can exploit weaknesses in the radio interface, such as the lack of network authentication in 2G (Jover, 2016; Park et al., 2019; van Rijsbergen, 2016).

3.3.2. Compromised mobile operator

Communication between the UE and radio access network is authenticated and encrypted with keys stored on the SIM card. The mobile service operator manages these keys. The network operator routes the decrypted communication to other operators, and as explained above, the relayed traffic should be protected with IPsec or VPN. Both the local network operator and the remote one have full access to the traffic, and the user's home or service operator has access to the keys. This trust in the operators originates from the days of landline phones and national telecom operators. As the telecommunications market has opened to new entrants, the basis of such absolute trust has disappeared, but the system architecture remains unchanged. There are no technical protections against the network or service operator intercepting and spoofing voice or data communication.

3.3.3. Human insider

Humans are always one of the weakest links in system security because they are prone to break the rules and make mistakes. Employees of the mobile operators or OSS systems could misuse their position to access sensitive data (Jordan and Lee, 2015) for personal reasons, for financial gain (Brandom, 2017), or due to external pressure or misinformation. Weaknesses in the security culture and education can make human insiders vulnerable to social engineering, misconfiguring the systems, and disregarding operational security guidelines.

3.3.4. Hardware and SIM manufacturers

The manufacturers of network equipment and user equipment are potential sources of attacks and can compromise the hardware supply chain. Bugs at the hardware level are challenging to trace and may stay hidden for years (Robertson and Riley, 2018). SIM cards may similarly have security flaws or backdoors. The SIM cards contain the keys for encrypting the over-the-air radio communication, and the key-generation infrastructure requires top-level security. Technical flaws and compromised organizations pose a serious threat to secure key management (Scahill and Begley, 2015).

3.3.5. Compromised software and OS vendors

Mobile networks involve a large number of proprietary and open-source software components to enable the regular functioning of the systems. Similar to hardware, the software supply chain is prone to intentional and accidental vulnerabilities. Due to its complex and closed nature, breaking into the core network requires in-depth knowledge and skills, whereas, with publicly available forensic tools, attackers can exploit common vulnerabilities (e.g., SQL injection (Tung, 2014)) in the software stack of routers and other network equipment (Checkoway et al., 2016; Hau et al., 2015). Since software and OS vendors may become a medium of software supply chain infiltration, we consider them as potential adversaries.

3.3.6. Law enforcement and governments

Law-enforcement agencies have standard interfaces for lawful access to mobile communication systems ((ETSI), 2020; Li et al., 2018), and every mobile operator is required to support them based on the local laws. The governmental entities have also exploited mobile communication data outside the lawful interfaces, e.g., in mass surveillance programs (Gellman and Soltani, 2013) and malware campaigns (Kaspersky Lab Report, 2014). Considering the power and interest of nation-state actors in obtaining access to the internal networks of mobile operators, including infiltrating the hardware or software supply chains, they are some of the most potent attackers against mobile systems.

3.3.7. Mobile users

Most mobile phones contain an application processor for running the mobile OS and user applications and a baseband processor for the radio software stack. The former is usually based on open specifications, and the users are free to write and install any software on top of the provided application programming interfaces (API). The baseband processor, on the other hand, is proprietary, and accessing it requires insider knowledge or reverse engineering. Nonetheless, mobile users have physical access to the hardware and may be able to bypass any sandboxes or access controls in the

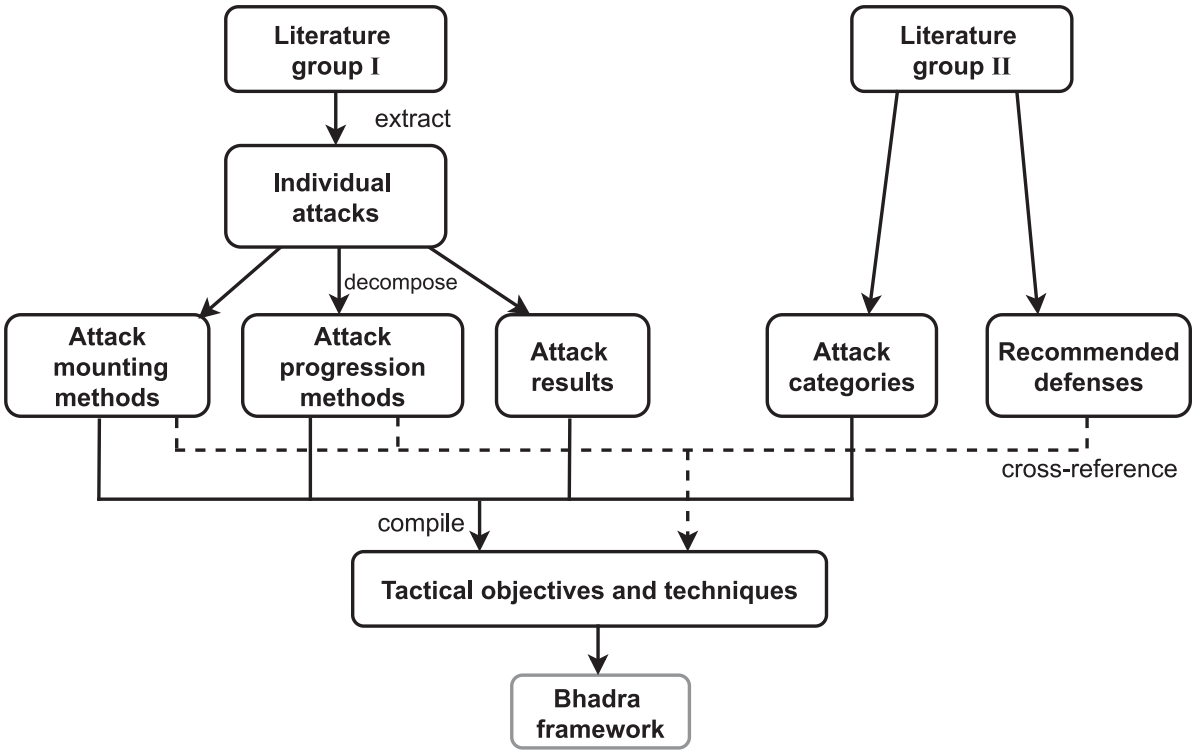

Fig. 2. Overview of methodology.

user equipment. This is commonly called *rooting*. It is conceivable that the user tampers with the mobile OS or with the baseband processor, e.g., to avoid billing, to spoof their identity, or to hinder network access by other users.

4. Threat modeling framework

In this section, we introduce the *Bhadra* threat modeling framework and explain the methodology and design choices in its development.

4.1. Methodology

The methodology is outlined in Fig. 2. We used literature from the following two sources:

- *Group I* consists of peer-reviewed academic publications, technical reports, white papers, and presentations at information security events. They offer a rich resource on individual attacks and their root causes.
- *Group II* comprises publications by standards bodies in the mobile communication sector (mainly 3GPP, GSMA, ETSI) and government agencies (*e.g.*, ENISA and NIST). These publications describe classes of threats, as well as best practice guidelines and recommendations for defensive strategies.

We extracted individual attacks from literature group I, which often describes them as message sequence charts accompanied by a textual description. Then, the attacks were decomposed into phases from mounting to progression and to results. From literature group II, we found various attack categories and classifications. This wealth of information was used to compile the tactical objectives and techniques, resulting in the Bhadra framework. Recommended defenses and best practices in the literature group II were cross-referenced with the attack descriptions.

Relation to the MITRE ATT&CK framework. The tactical categories have been aligned with the MITRE framework when possible. As a trade-off in favor or readability of the models, each technique was placed under just one fixed tactical objective. Some modifications were necessary to match the mobile communication context. These will be explained in the relevant sections.

Another difference between the frameworks is the type of data used in their construction. The MITRE framework focuses on documenting common tactics, techniques, and procedures of malware and advanced persistent threats to build a knowledge base of adversary's offensive behaviors throughout attack life cycles against particular platforms (e.g., Windows). It is based on real-world observations gathered, e.g., through malware samples, penetration testing, and threat intelligence reports. The behavioral modeling helps in attack attribution (The MITRE Corporation, 2019a) and in prioritizing the development and deployment of defenses.

In comparison to enterprise IT systems, mobile networks do not appear to regularly experience attacks and compromises — at least ones that are publicly documented. Most known attacks have been presented by academic researchers and information security professionals whose main motivation is to understand and mitigate *potential* vulnerabilities. Thus, we consider a broader range of potential attackers and motivations than might seem realistic, and we also model attacks that have not occurred in the wild. While not as firmly grounded in experience as the MITRE framework, our framework should nevertheless be useful for understanding the possible weaknesses of the systems and for developing rigorous security defenses.

4.2. Tactics, techniques, and assets

We will now define the key components of the framework: tactics and techniques. Additionally, we will discuss the assets that need protection.

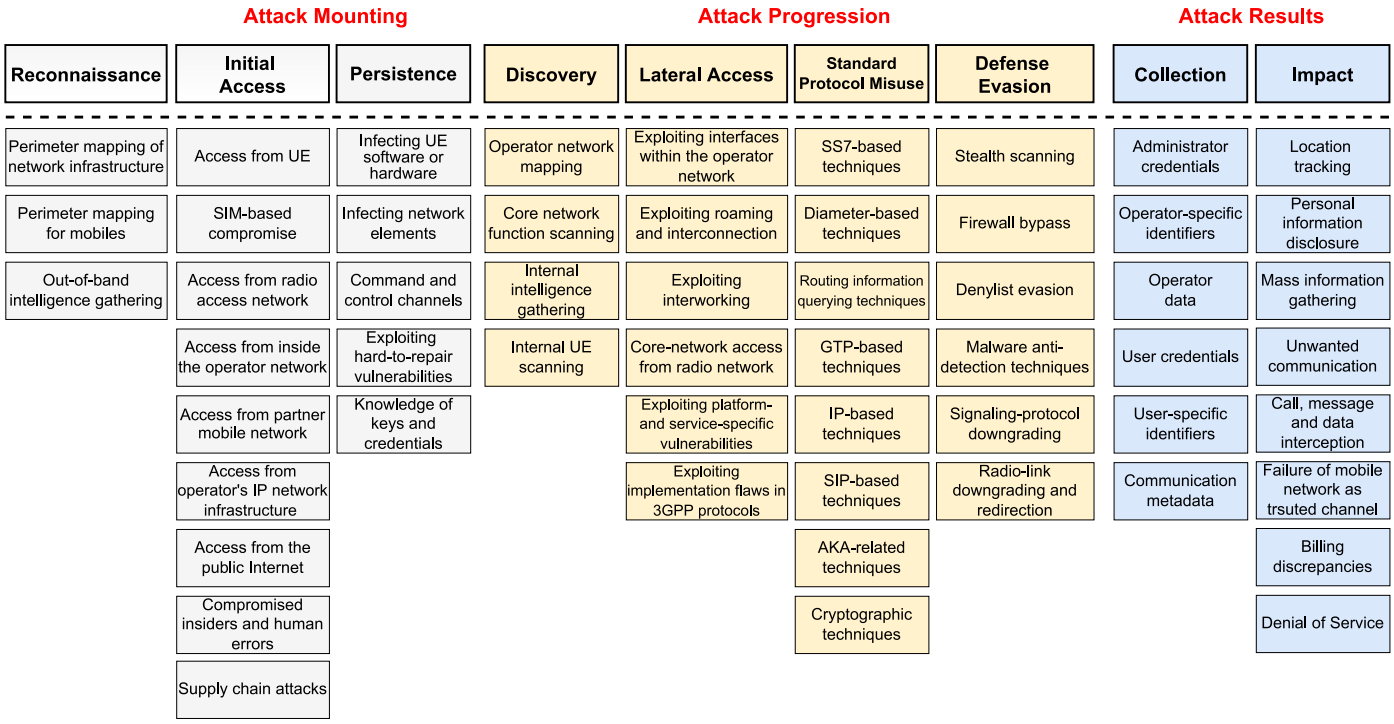

Fig. 3. Bhadra threat modeling framework.

Tactics represent the adversary's tactical objectives, i.e., the reason ("why") for performing a particular action during an attack. In most of the studied attacks, there are similar phases and intermediate objectives of the adversarial actions during the course of the attack. Thus, the tactics are ordered in the way they represent the natural attack life cycle. Of course, not all attacks include all the tactics.

Techniques are specific actions or technical means by which the adversary achieves the tactical objectives. They refer to the "how" and "what" aspects of the adversarial strategy. While some techniques may serve multiple tactical objectives, they have been grouped under the tactics which they most commonly serve.

Assets are things of value that need protection. The most important asset in the mobile communication system is its *continuous operation* and the mobile user's ability to use it for communication. Since all entities and subsystems in the mobile network (Fig. 1) exist to facilitate this communication, they are also assets that need protection. From the operator's point of view, another important asset is the *revenue* generated by the services. Thus, any scenarios that could result in financial or accounting discrepancies are significant threats. For mobile users, the content of the communication is often as valuable as the service availability. Therefore, users are concerned with attacks that could violate the *integrity, confidentiality and privacy* of their communication or incur a fee for services that they have not used. These are the primary assets that need protection in the system. On the other hand, the model does not include threats from malicious apps or malware on the user equipment that steal sensitive information (*e.g.*, banking credentials, or passwords to online services) but which are not dependent on the underlying communication network.

Below, the discussion of tactics and techniques has been organized to three phases in the attack life cycle: mounting, progression, and result (Sections 5, 6 and 7, respectively). Figure 3 summarizes the Bhadra framework. The assets will be visible mostly in the results phase of the framework; however, having them in mind throughout the process will help us focus the threat modeling on relevant threats.

5. Attack mounting phase

The attack life cycle starts with the attack mounting phase, in which the adversary finds a weak point in the target, gains initial access to the target, and establishes a persistent presence. The adversary may also discover information that will be useful in the following phases of the attack. We recognize three tactical objectives in the attack mounting phase: reconnaissance, initial access, and persistence.

5.1. Reconnaissance

The tactical objective *reconnaissance* represents adversarial techniques used to gather information about a target system or network before mounting the actual attack. It is a preparatory step where the adversary, from outside the network, collects details about the target organization, infrastructure, and devices. The techniques used for reconnaissance may appear harmless to the victim, or they may be lost in the network noise. However, the attacker gains information that enables it to narrow down the target and to proceed with the more dangerous steps; hence, reconnaissance should be considered a serious issue. We identify the following three techniques towards this tactical objective.

Perimeter mapping of network infrastructure is a generic technique where the adversary gathers information on the target network infrastructure before mounting the attack. Examples are DNS enumeration, AS lookup, and IP and port scanning. The scanning can find both gateway nodes and services that are visible to the Internet due to misconfiguration.

Moreover, there are dedicated search engines (e.g., *Shodan* Matherly, 2015 and *Censys* Durumeric et al., 2015) for finding Internet-connected devices and networks. Similar information can be found on normal search engines with advanced search

options, popularly known as *Google dorking* (Toffalini et al., 2016). Real-time information on the exposed nodes and their known vulnerabilities (Li et al., 2019; Tounsi and Rais, 2018) is essential for network operators and owners of Internet-of-Things (IoT) devices to track the public visibility of their systems. However, the adversary can use the same information sources for finding targets within the operator's network.

The radio network, including cell-tower locations, frequency bands, and other network parameters, can be mapped by scanning the frequencies and by connecting to the mobile networks.

Perimeter mapping for mobiles covers methods for collecting information on target user equipment. The most common method of information collection is tracking of the mobile user's access on public websites. Carrier-grade NATs (CGN) make it challenging to perform IP and port scanning of the mobiles. Nevertheless, the adversary can perform an exhaustive enumeration of IPv4 addresses and ports in the CGN, and IPv6-enabled mobiles are directly exposed to the Internet. If the mobile has a public IP address, it may be discoverable from dynamic DNS. On the wireless link, the attacker may use an IMSI catcher (Nasser, 2019) to find subscriber and device identifiers, such as IMSI, IMEI and MSISDN. The user's MSISDN is often public information or available from various sources.

Out-of-band intelligence gathering refers to the gathering of business and technical information about the target organization, network and users, e.g., from out-of-band sources, such as technical documentation, roaming contracts, cell-tower databases, and subscriber geolocation data from the operator or from mobile applications. The adversary could be assisted by an insider with access to the operator's internal technical and business documents.

An important source of information for the adversary is the IR.21 roaming database, which contains standardized information about each operator's network infrastructure for interconnection and roaming. GSMA administers the global IR.21 database, and every GSM, 3G, or LTE operator has access to it. The IR.21 database provides comprehensive information about the external interfaces and parameters of the operator network that are visible to other operators. This includes IP addresses of all operator network nodes that connect to the GPRS roaming exchange, such as GGSNs, SGSNs, MMSCs, AAA servers, and DNS Servers. The operators use this information for configuring their firewalls and border gateways. Moreover, the database describes the signaling protocols and protocol versions supported by the operator network at these endpoints. For the older SS7 protocols, the database reveals the Global Titles of the SCCP gateways and Point Codes of underlying MTP signaling points. For WLAN roaming, the database lists the RADIUS server addresses. The database also includes the contact information of both administrative and technical troubleshooting, including person names and direct phone numbers and email addresses.

Many of the above techniques allow an adversary to discover network topological information, such as addressing, router and gateway filtering, firewall rules, and addressing-based trust relationships that are useful for the subsequent phases of the attack.

The techniques under the reconnaissance tactical objective are performed from outside the network. Section 6.1) will discuss similar techniques when the attacker is already inside the operator network and wants to discover more details or to fine-tune its attacks.

5.2. Initial access

The tactical objective *initial access* represents techniques or attack vectors used as entry points to the systems, such as exploiting technical or human weaknesses.

Access from UE refers to attacks that originate from software or hardware components on the user equipment. The reader should keep in mind that, while a compromised UE is a serious and immediate threat to its user, our goal is to model attacks that make further use of the mobile network or target the network itself.

The most common security concern in mobile phones is malicious applications. Ostensibly fun or useful applications published on the app stores may hide Trojan features (Felt et al., 2011). There is often no clear boundary between outright malicious applications and those that push the limits on data collection or monetization.

Vulnerabilities in mobile applications could also be exploited to take control of the UE. The known examples of such attacks have been mostly in mobile web browsers, which are exposed to untrusted web sites (Kurtz and Alperovitch, 2012). We can expect more mobile applications to be hacked as they gain richer features and are exposed to untrusted data and servers.

More serious compromises of the user equipment require the attacker to have control of the device's operating system. *Rooting* or *jailbreaking* refers to users intentionally compromising the access-control features on mobile operating systems (Sun et al., 2015). The motivation may be to install third-party applications not authorized by the device vendor (Goodwin, 2020) or even to replace the device operating system with a customized one. Historically, breaking the *SIM lock* (i.e. carrier lock) has been the most common reason for such tampering. These attacks require user cooperation, but they also open the path for untrusted software to gain full control of the phone. Even more alarmingly, recently discovered mobile malware, called Pegasus, can compromise the phone without the user's cooperation by exploiting software flaws (Marczak et al., 2018; Pegg and Cutler, 2021).

There has also been discussion of attacks where the baseband modem on the phone could be compromised (Weinmann, 2012) and then used for attacks against the network. There are few known examples of such attacks. Also, while there have been projects for developing an open-source baseband modem (Burgess et al., 2008; Welte and Markgraf, 2010), they rarely have produced fully functional hardware and software.

SIM-based compromise refers to various attack techniques that gain access to the system via the subscriber identity module. The purpose of the SIM (or USIM in 3G and later generations) is subscriber identification and authentication. The SIM card is a cryptographic token that represents the subscriber identity. The subscriber's authentication is based on a shared secret key stored in the SIM. Thus, if the SIM card is in the wrong hands, this can lead to impersonation of the subscriber's phone number (MSISDN) or to billing fraud.

The subscription was bound to the physical phone in some early mobile networks. *Phone cloning* allowed the user to have two phones with one subscription or to steal someone else's subscription. After the introduction of SIM cards in GSM, *SIM cloning* could potentially achieve the same. The attack has been demonstrated on SIM cards that use outdated cryptographic algorithms (Anwar et al., 2016).

The SIM as an authentication token has become even more significant because other applications build their security on the authentication provided by the mobile network. For example, mobile and online applications (e.g., WhatsApp and Facebook) may authenticate the user by sending a text message to their phone numbers. The banking sector has mostly moved away from such vulnerable phone-number-based authentication, but more informal financial services, such as Bitcoin wallets, have been compromised by obtaining access to the victim's SIM card. In *SIM swapping*, the attacker fraudulently obtains a replacement (or second) SIM from the operator, thus taking control of the user's phone number (Lee et al., 2020), possibly with the help of insiders working for the operator (Franceschi-Bicchierai, 2018).

The SIM is also a programmable platform that can run simple applications based on the SIM Application Toolkit (STK)

(3rd Generation Partnership Project, 2020b). These are mostly menus to operator services, such as telephone directory, but may also include security-critical applications like mobile money-transfer system M-Pesa (Jack and Suri, 2011) and mobile signature based on the ETSI MSS standard (ETSI(2022). The SIM applications communicate with the operator's backend services over SMS, Unstructured Supplementary Service Data (USSD) (3rd Generation Partnership Project, 2020c), or in some cases, over HTTP. These interfaces to the SIM present another attack surface. We will discuss *SIMjacker* (AdaptiveMobile Security, 2019a) further in Section 8.2.

Another security-critical feature is over-the-air (OTA) updates to the SIM profiles and firmware. The updates may be sent over binary SMS messages or HTTP. If there are weaknesses in the OTA protocol or keys, the updates can be used to compromise the SIM card (Nohl, 2013).

New phones and IoT devices have replaced the physical SIM card with an embedded hardware module, *eUICC*, in the UE. The hardware is expected to have the same level of security as the physical SIM card. The SIM profiles are provisioned to the eUICC with the Remote SIM Provisioning (RSP) protocol, which could have vulnerabilities either on the protocol or human level.

Access from radio access network covers techniques where the adversary gains access to the radio communication between the UE and the network. It could achieve this by breaking the cryptographic protection on the radio link, by physically compromising the base station, or by establishing a fake base station.

A well-known example in this category is the *IMSI catcher*, which pretends to be a base station and captures identifiers (IMSI, IMEI, MSISDN) from the UEs within its vicinity (Borgaonkar et al., 2011; Park et al., 2019; Shaik et al., 2015; 2016). The attacker may also learn SIM- and UE-specific parameters, such as supported mobile generations and cipher suites. The newer protocol versions provide incrementally better protection against IMSI catchers, but the attack is still possible in some cases (Borgaonkar et al., 2015). The IMSI catchers can be used for tracking the presence of UEs in a given location (Nasser, 2019) or for selectively jamming a specific UE.

In addition to tracking the user, the adversary may want to intercept the calls and data communication. 2G networks were vulnerable due to weak encryption algorithms. More importantly, it was easy to route the calls and data through a *fake 2G base station* because GSM had no network authentication and because enabling the encryption was up to the base station. Since the interception is easiest in 2G, the adversary may try to *downgrade* 3G and 4G connections to 2G. Moreover, roaming agreements mean that there is a vast number of RANs around the world that can legitimately provide cellular service to a given subscriber, and this could be misused for setting up fake base stations.

Due to their large number and distributed locations, base stations are vulnerable to physical compromise. For this reason, 3G standards moved the encryption endpoint from the base station to RNC, but in 4G, it was moved back to the eNodeB. Femtocells (home nodeB) are particularly exposed to physical attacks (Borgaonkar et al., 2011; Golde et al., 2012).

Access from inside the operator network describes the techniques that require access to the mobile operator's network. The attack could originate from a rogue or compromised operator or from misuse of legal interception capabilities. The attacker may gain access to the subscriber's personal details and location and call history, as well as real-time data. It may also be possible to intercept calls and data traffic.

Access from partner mobile network covers similar techniques that are launched from a partner mobile operator's network via the interconnection and roaming mechanisms. Known attacks mainly exploit the standard roaming functions. Similar to insider attacks, the attacker's goal can be real-time location tracking or communication interception. Additionally, it could be a denial of service or billing fraud (Rao, 2015). Examples of potential attacks have been reported, particularly in the context of GPRS after mobile data gained popularity (Positive Technologies, 2017; Xenakis, 2006; 2008). The interconnection and roaming are fundamentally based on mutual trust between the operators, and it is difficult to know whether a received request was made with the honest intent to provide a service to the mobile or for a malicious purpose. The attacks that exploit the interconnection can be done remotely from anywhere in the world, and *roaming brokers* or *aggregators* make it possible to hide the origin of the requests. Both of these factors reduce accountability for the misuse of the interconnection and roaming mechanisms.

Access from operator's IP network infrastructure covers techniques where the attacker gains access through compromised routers and middle-boxes and other underlying IP network equipment or data links. These breaches can result from vulnerabilities and neglected security updates in network equipment, and there have been suspicions of built-in backdoors (Armasu, 2018; Pancevski, 2020). The signaling traffic within the operator's network and even between operators is not always cryptogprahically protected, which leaves it open to interception by the network infrastructure. The same is true for the user data traffic. User data is vulnerable to further attacks when it leaves the operator network and traverses the public Internet. Weaknesses in inter-domain routing (Butler et al., 2009) could potentially be used to divert and intercept inter-operator signaling and user traffic, but there are no publicly known examples of such attacks.

Access from the public Internet refers to attack techniques that originate from the public Internet and target the mobile network or its users. The attacker could try to compromise public-facing elements of the mobile operator network. For example, the SIP gateways in VoIP and VoWiFi services may be hacking targets (Chalakkal et al., 2017). Such techniques aim for billing fraud (Zhang et al., 2007) and traffic interception. For another example, GPRS gateways (GRX) have been found to have unnecessary and vulnerable services exposed to public Internet.

The mobile network infrastructure and users may be targets of DDoS attacks from the Internet, also using SIP or VoIP protocols (Ehlert et al., 2010; Gauci, 2021; Keromytis, 2011; Sisalem et al., 2006). Earlier technology generations (e.g., GPRS) had very limited data bandwidth to the UEs, which could be easily overwhelmed. Individual mobile users can still be targeted with DDoS; the well-known examples are from the competitive gaming community (Nexusguard, 2020).

Note that attacks against the UE software and mobile applications are mostly outside the scope of our framework, but they can be relevant when the network operator should take action to mitigate them. This is the case with packet-flooding attacks (Anagnostopoulos et al., 2016).

Compromised insider and human errors refer to techniques where the adversary takes advantage of human insiders to compromise components of the mobile network. The insiders could be operator employees with a lack of security awareness, who are prone to social engineering attacks (Lee et al., 2020; Mitnick and Simon, 2003). Former employees, whistleblowers and political activists are sometimes seen as potential risk factors (Amine, 2021; Kirchgaessner, 2020). Regardless of whether such actors have good or bad intentions, it is the operator's duty to protect subscriber data from unlawful access. In more sinister scenarios, the insider may be coerced or corrupted by criminal or foreign entities. Insider threats have also been studied from the human-centric point of view (Nurse et al., 2014).

The parts of the mobile system that are most exposed to insider attacks and human errors are naturally the customer service (Franceschi-Bicchierai, 2018; Lee et al., 2020), which has ac-

cess to the subscriber's personal data, and the Operations Support System (OSS), which has comprehensive access to both data and network equipment in the mobile system (Bhorkar et al., 2017). Unintentional human errors, such as insecure system configuration or careless handling of confidential information, can also lead to vulnerabilities. The previously discussed technical methods of initial access often depend on such human vulnerabilities, and threat modeling should identify both the technical and human factors in the initial access.

Supply chain attacks are techniques where the adversary gains initial access by compromising network hardware or software in the supply chain before it is delivered to the operator. There have been concerns about network hardware compromised either during manufacturing or during delivery to the operator (Hau et al., 2015). While the possibility of tampered chip designs has received a lot of attention (Lee and Moltke, 2019), the most vulnerable part is the updatable firmware on the devices. Software supply chains can be similarly vulnerable. Modern software is always built on an extensive ecosystem of outsourced and open-source components, such as libraries and frameworks. It may be impractical to comprehensively audit the security of all new software versions. Furthermore, information systems — including operator networks — make use of third-party infrastructure for communication and data processing so that this infrastructure becomes a part of the telecommunications supply chain. The supply chain attacks overlap with the other initial access techniques, and threat modeling should identify both the supply chain vulnerability and the targeted architectural components.

5.3. Persistence

After the initial access, the next tactical objective for the attacker is *persistence*, i.e., retaining a foothold on the target system. While one-off access may be sufficient for achieving some objectives, others require the attacker to retain control of the target even if the vulnerabilities that enabled the initial access are fixed.

Infecting UE software or hardware are the techniques where the adversary installs hard-to-detect malware on the phone or even infects the phone operating system or firmware. If the malware is installed in the supply chain, it may be impossible to remove it with a security update. There is also an example of a vulnerability that enables the installation of malware on the SIM card (AdaptiveMobile Security, 2019a).

Infecting network elements allows adversaries to retain control over the nodes in the operator's core network. For example, the MessageTap (Leong et al., 2019) malware infects the SMS center. Physical access or administrative rights are usually required to install such a backdoor or malware. However, the large number of network functions from different manufacturers makes it difficult to gain assurance that no attacker has a foothold in the core network. The threat of this kind of attacks may increase further as physical network nodes are replaced with virtual network functions, unless sufficient measures are taken to ensure their integrity.

Advanced persistent threat (APT) refers to attacks where an advanced adversary installs particularly undetectable backdoors or malware on the target system and remains there for extended periods of time. Telecommunications systems are naturally among the targets of such attacks (Cybereason, 2019; 2021). Recently, APT-like malware has also been found on UE (Pegg and Cutler, 2021).

Command and control channels refers to techniques that enable the attacker to control the infected system components remotely. In the simplest case, this means listening to connections on a network port or polling a command-and-control server in the Internet for new instructions. Researchers have also shown that a botnet can be controlled via SMS messaging (Geng et al., 2012; Zeng et al., 2012).

A command and control channel is also needed for controlling mobile malware in the UE (Kocialkowski, 2014). Network operators provided network-based malware detection as a service (Khatri and Abendroth, 2015) to warn the users of the infected mobiles.

Exploiting hard-to-repair vulnerabilities refers to situations where the operator or user may be aware of security vulnerabilities but is unable to patch them. These may be caused by hardware flaws or by insufficient software or firmware updates. For example, old SIM cards or phones may only support outdated cryptographic protocols, but the operator cannot mandate maintenance or replacement of the UE hardware. Similarly, operators in low-income countries sometimes reuse outdated network equipment that is no longer secure, but the users may be unaware of that. The need to interoperate with the older technology also means that other operators in the global interconnection and roaming system must continue supporting older, less secure protocols and algorithms, leading to downgrading attacks (see Section 6.4).

Knowledge of keys and credentials enables another type of persistence. If the attacker learns the long-term cryptographic key on the user's SIM card, they can use it for passive eavesdropping. On the backhaul and interconnection, compromised IPsec credentials could give an attacker who is present on the underlying network persistent access to signaling and data, although an active attack is required to intercept IPsec. Possession of long-term access credentials to any network nodes can also be considered a form of persistence.

6. Attack progression

In the second phase of the attack, which we call *attack progression*, the adversary exploits vulnerabilities in the system to expand its control from the initial foothold towards its objectives. We recognize four tactical objectives in this phase: discovery, lateral access, standard protocol misuse, and defense evasion.

6.1. Discovery

The tactical objective *discovery* means learning more information about the operator network and its users after gaining a foothold inside the system. The knowledge gained by discovering the surrounding environment will decide the attacker's next steps. The techniques for discovery overlap with those used for reconnaissance (Section 5.1). The difference is in that discovery takes place inside the network.

Operator network mapping represents network-scanning techniques deployed from inside the operator network. Once behind the operator's firewall and NAT, the attacker can use IP-based scanning tools like *nmap* to find nodes and services on the operator's private network. In particular, it would look for open SCTP ports in the network address space. Depending on the internal structure of the operator network and on the location of the attacker's foothold, the attacker may scan the core network, radio access networks, IMS and other service domains, and OSS. Internal network boundaries and firewalls will, however, limit the reachable nodes and services. Also, network and port scanning is relatively noisy activity that puts the attacker at the risk of being detected.

Another way to map the network is to query the operator's *internal DNS* service for the network functions. For example, the names of GPRS support nodes follow a well-known structure so that they are not difficult to guess. Moreover, an attacker with access to one operator's network can find the gateway nodes of peer operators for interconnection and roaming. The operators provide *external DNS* servers for GGSN discovery, and the attacker can exploit them for mapping the peer network boundaries (Electronic Communications Committee (ECC), 2003).

Core network function scanning aims to find 3GPP-specified network interfaces on the core network. After discovering the reachable network nodes and open ports, the attacker may connect to them in order to identify the network functions to which they belong. At open SCTP ports, it will look for 3GPP-specified signaling interfaces, and on open UDP ports, for services related to GPRS tunneling. There are specialized tools like *SCTPScan* (Langlois, 2009) and *GTPScan* (Mende and Rey, 2011) for discovering these services. The interfaces should be protected by IPsec or VPN tunnels, but in the core network, operators do not always see the need for such protection. OSS or billing functions may be similarly found by scanning TCP ports.

Older networks may still use the SS7 protocol stack without IP transport. Instead of IP addresses, the legacy signaling nodes have point codes and Global Titles (GT). Although these numeric addresses are routed similarly to IP addresses, different tools are needed for scanning the address space *GTScan* (Abdelrazek, 2018). For the scan, the adversary needs access to one signaling node in the network.

Internal intelligence gathering refers to gathering of information about the target network by exploiting the functions and data to which the attacker already has access. The attacker wants to learn the internal structure of the operator network, how it supports the operator business, which functions are accessible, and who are the customers. In comparison, the IR.21 roaming database discussed earlier in Section 5.1) provided only information about the external interfaces of the operator network.

Internal UE scanning is a technique where the attacker connects directly to the mobile device from inside the operator network. An adversary could mount such attacks from compromised core network nodes. Known examples of the technique, however, take place on the data plane between mobile devices. For example, a UE behind a carrier-grade NAT or operator firewall is relatively well protected against scanning from the Internet, but the same protection may not exist between mobile nodes within the same 100.64.0.0/10 network (Qing and Guangdong, 2017). This may enable the attacker to scan for vulnerable services in phones and Internet-of-Things devices. The situation is similar to being connected to the same local WLAN network without isolation between the stations.

6.2. Lateral access

The tactical objective *lateral access* refers to the ways in which the attacker expands its influence to other network nodes beyond the initial foothold. In most known attacks, the adversary does this by sending or manipulating signaling messages from the compromised node. This is a broader concept than *lateral movement* in the MITRE framework, where the attacker aims to compromise additional nodes.

Exploiting interfaces within the operator network refers to accessing 3GPP network functionality from a compromised node inside the operator network. The attacker may have a foothold either on one of the 3GPP network nodes or on some other computer or device on the operator network. Often, control of any network-connected device inside the operator's firewall is sufficient to access the nodes and interfaces in the network. To prevent such unauthorized connection requests, the legitimate network nodes should authenticate each other with IPsec or some other means. Additionally, they should enforce access control rules so that each interface on a network node can only be accessed by the intended peers. While the trend in 5G is towards zero-trust networking (Rose et al., 2020) between virtual network functions, many operators still assume that the core network is sufficiently protected by boundary firewalls.

Exploiting roaming and interconnection refers to an attacker using its control of a node in one operator network to attack the users or infrastructure of other operators. It can do this by connecting to them over the roaming and interconnection mechanisms. For example, *LightBasin* is a targeted intelligence gathering operation that uses compromised nodes in one operator network to target servers in other operator networks (Harries and Mayer, 2021). The adversary does not need to build its own mobile network to gain access to the roaming and interconnection interfaces; it can create a service operator that rents RAN capacity from others.

The interconnection between operators typically takes place in an Internet packet exchange (IPX) or a specialized GPRS roaming exchange (GPX) (GSM Association, 2018). IP-layer access between operators is controlled by firewalls or border gateways. Alternatively, there may be a direct connection between two operators, in which case IPsec or some other type of VPN should be deployed to protect the interconnection. This limits the number of nodes in each operator's network that can access the interconnection. Thus, the attacker that has a foothold in one operator network can reach other operators mainly through the services intentionally available to other operators. Many of these services are accessible via the Gateway GPRS Support Nodes (GGSN), which implement signaling and data transfer between operators for the packet-switched and circuit-switched domains. The signaling is handled by the Diameter edge agent (DEA) or SS7 Signaling Transfer Point (STP). In the IMS domain, Interconnect Session Border Controller (I-SBC) implements the interconnect functions including SIP proxy and a layer-3 or 4 firewall. Firewalls also exist for the signaling protocol level, but they have not been widely deployed (ENISA, 2018) and the filtering policies may not be fully developed.

Exploiting interworking refers to an adversary in control of one generation or type of technology extending the attack to another. The interworking can take place between operator core networks, between radio networks, and with non-3GPP networks.

Interworking functions (3GPP TS 29.305 3rd Generation Partnership Project, 2022) enable interoperability between core networks of 4G and older generation networks by translating signaling messages from one protocol stack to another, i.e., SS7 messages of 2G/GSM to Diameter for 4G. This functionality enables roaming between networks of different generations. Unfortunately, interworking also means that vulnerabilities of the older signaling protocols are retained in the newest networks (Holtmanns et al., 2016).

The same operator may have radio networks based on different generations from technologies ranging from 4G eUTRAN to 3G UTRAN and 2.5G GERAN. *Inter-generation handovers* enable mobility between the different radio access networks. The handovers to older technologies may result in downgrading of authentication and cryptographic mechanisms (Dabrowski et al., 2016). In any case, the inter-generation handovers add complexity to the communication system. Formal modeling has provided some clarity to the security properties of the handovers (Copet et al., 2015; 2017; Peltonen et al., 2021).

Finally, 4G networks supports roaming in *non-3GPP access networks* (3GPP TS 24.302) (3rd Generation Partnership Project, 2020a; Rajavelsamy et al., 2015), which in practice means WLAN data and calling. The integration with WLAN technology lowers the bar for attacks because IEEE 802.2.11 access points and software stacks are much more widely available. For example, they have been used for implementing a WLAN-based IMSI catcher (OHanlon and Borgaonkar, 2016).

Core-network access from radio network is a technique where an adversary who has compromised a base station or some other part of the radio network accesses the core network functions. Base stations are likely points of first access for the attacker be-

cause they are physically distributed and exposed to physical compromise. Thus, the attacker can be expected to misuse the X2 and S1 signaling interfaces that are accessible from the base station. A compromised MME could request authentication tuples for a mobile that is not present in the area. It has also been demonstrated that the attacker could hack *femtocells*, small low-power cellular base stations placed at homes or small businesses (Borgaonkar et al., 2011; Golde et al., 2012).

Exploiting platform and service-specific vulnerabilities means exploiting vulnerabilities in the software implementations and computing platforms. While the operator network is relatively well isolated from outside, once the attacker is in the network, it can exploit flaws or misconfiguration of software frameworks, operating systems, and services like databases and file storage. The attacker will try to gain access to additional network nodes as well as administrator accounts. In addition to the CN, the attacker could find such flaws in the operations and support system software and services. It may also look for vulnerabilities in the underlying network infrastructure including routers, switches, and network controllers. For more details, we refer the reader to the *lateral movement* and *privilege escalation* techniques in the MITRE framework (Strom et al., 2018).

Exploiting implementation flaws in 3GPP protocols refers to the fact that, just like any software, the 3GPP control and data-plane can have security vulnerabilities that arise from implementation flaws or weak administrative practices. First, the implementation may violate the specification, for example, by allowing downgrading to an insecure mode (Rupprecht et al., 2016). In one study, fuzz testing uncovered several vulnerabilities in the LTE radio interface caused by ambiguous specifications or implementation flaws (Kim et al., 2019).

Second, even an implementation that complies with the specification may have a flaw like a buffer overrun or an injection vulnerability. Since the internal functions of the CN have not been exposed to the public Internet, they may not have been thoroughly analyzed for latent flaws. However, there is little public information about the types or prevalence of software errors in the CN components.

6.3. Standard protocol misuse

Standard protocols play a crucial role in telecommunications networks. In the mobile networks, they enable network access, mobility, voice and data communication, and other telephony services. Most reported attacks against the mobile networks arise because the standard protocols have a weakness that can be exploited or feature that can be misused. For this reason, we have promoted *standard protocol misuse* to its own tactical objective. Often, the most serious attacks are enabled by legacy protocols that are supported for backward compatibility with the older technology generations.

SS7-based techniques refer to misuse of the legacy Signalling System 7 (SS7) protocol stack that was adopted from traditional telephone networks to GSM and still continues to be the predominant signaling protocol today. It provides almost no cryptographic security in terms of authentication, confidentiality, or integrity. Misuse of SS7 messages has been discussed by the mobile security community for over a decade (Engel, 2008; 2014; Rao, 2015). Various solutions to the vulnerabilities have also been proposed, such as secure tunneling (Lindskog and Brunstrom, 2008; Sengar et al., 2005), firewalls (Ashdown and Lynchard, 2001; Mehra et al., 2019) and machine learning (Jensen et al., 2016). However, operators are reluctant to deploy the solutions at scale. One reason is that they create operational and management costs, especially when agreement between operators would be required on the global level. Additionally, network engineers are typically reluctant to deploy security measures that could disrupt the operation of a production system. Thus, SS7 continues to be a source of threats, and finding hidden features of SS7 and turning them into attack vectors is an active security research theme (Rao et al., 2015). There are also open-source tools that scan for well-know vulnerabilities and implement attacks (Abdelrazek and Azer, 2018).

3G introduced SIGTRAN, which is SS7 signaling over IP and thus enables the use of IPsec for protecting the messages. There is no public data on how widely IPsec has been deployed. Moreover, the hop-by-hop authentication between signaling points does not prevent misuse of the SS7 features from compromised nodes the belong to the network.

Diameter-based techniques refer to similar vulnerabilities in the more modern protocol stack. Diameter is the successor of SS7 for interconnection in 4G networks, and it supports encryption and authentication with IPsec or DTLS. Diameter also allows operators to hide internal structure of their network from others. While this provides a good starting point for security, the security is implemented hop-by-hop in the signaling network, which means that, just like in SIGTRAN, corrupt nodes in the network can still inject signaling messages.

Many of the attacks that rely on SS7 have been replicated using Diameter due to improper deployment of the security features (Abdelrazek and Azer, 2018; Kotte et al., 2016; Mashukov, 2017; Positive Technologies, 2018). While operators adopt best practices over time, the issue of backward compatibility remains. That is, SS7-based attacks can be translated into Diameter attacks using GSM-to-LTE interworking functions (Holtmanns et al., 2016) even if the adversary has limited knowledge of LTE networks.

Routing information querying techniques make use of the fact that calls and text messages between two mobiles are routed directly between the serving networks. Establishing calls to the callee's current location is the responsibility of the network from which the call originated, and they can query the callee's home network for the callee's location. Similarly, the sender's network delivers SMS directly to the recipient and, thus, needs to have access to the routing information. A compromised operator can query the mobile's location without establishing any actual call or without having an SMS to deliver. SS7 and Diameter have different but equivalent signaling messages that can be used for this attack. The attacker first queries the target's IMSI based on the phone number and then the routing information based on the IMSI. There is evidence of such rogue queries in the wild SS7ExposureReport2018.

SMS home routing is a defense mechanism (3rd Generation Partnership Project, 2007) where the mobile user's home operator always responds with a fixed location in the home network and forwards the SMS from there to the mobile's current location. This hides the fact that the mobile may be roaming. However, adversaries have been able to bypass some implementations of home routing by hiding the location queries within other messages (Puzankov, 2019). A similar home routing mechanisms could be implemented for calls, but it is not part of the standards.

GTP-based techniques exploit the GPRS tunneling protocol. It is yet another protocol with no built-in encryption for user data (GTP-U) or authentication for signaling (GTP-C). Thus, an attacker at the right location in the network can either spy on the communication or spoof control messages even if it is not a legitimate participant. For example, an attacker at the GPRS roaming exchange (GRX) network can passively spy on the user data in GTP-U packets, and it can track the user's location by monitoring in the packet headers (Kho and Kuiters, 2014). Attacker at the GRX can also actively query information about the mobile from the SGSN. It may even be able to spoof PDP Context Request messages to redirect the tunnelled user data (GTP-U) to itself (Positive Technologies, 2017) or Delete PDP Context Request to disconnect the mobile from the Internet.

IP-based techniques target the TCP/IP family of protocols. The documented attacks comprise mainly denial of service and misuse of the DNS protocol.

The mobile nodes and GPRS gateways are vulnerable to ICMP flooding, SYN flooding, and UDP flooding attacks from the Internet. This was especially the case for early generations where the data bandwidth to the mobiles was very limited. Naturally, an attacker with a foothold inside the operator network or interconnection and roaming system could mount similar packet-flooding attacks against the network nodes. The noisy attack would, however, reveal the presence of the attacker.

One DNS-based attack is DNS spoofing — or poisoning, as it is also called. If the attacker is able to manipulate DNS responses, e.g., within the operator network or at a GRX, it can divert traffic flows to attacker-controlled nodes (Positive Technologies, 2017). Another way to misuse DNS is to use it as an unmetered communication channel to bypass charging or data caps (see Section 7.2).

SIP-based techniques exploit the hop-by-hop nature of the Session Initiation Protocol (SIP). SIP is used to setup voice or video calls (e.g., VoLTE and VoWIFI) and for controlling other IMS multimedia communication sessions. 3GPP defines security mechanisms (3rd Generation Partnership Project, 2021) for authenticating the SIP signaling between the UE and P-CSCF, which is a SIP proxy in the operator network, and signaling between the IMS core network elements. Each of the SIP proxies on the path between the end users needs to be trusted to maintain the signaling integrity. The media stream between the UEs can be protected end-to-end; however, the security of the end-to-end connection typically depends on hop-by-hop authentication by the intermediate proxies. When the IMS session takes place between two operator networks, each users is authenticated by their own operator. In roaming situations, the security depends on SIP proxies in the visited network.

Consequently, compromised SIP proxies can spoof IMS communications including text messages, which have been used as a secure channel for various applications (Tu et al., 2016a). An on-path attacker could also tamper with the signaling to redirect and capture the communication. Moreover, it has been suggested that forged SIP messages can enable billing fraud (Zhang et al., 2007) or free service. Even limited access to the SIP proxies may enable denial-of-service attacks against IMS, and the proxies themselves could be used to amplify DoS (Ehlert et al., 2010; Sisalem et al., 2006).

AKA-related techniques refer to attacks that exploit limitations of the access authentication and authorization between the UE and the radio network. 3GPP protocol specifications define several versions of the authenticated key exchange (AKA) (Nakarmi, 2021). The original GSM networks had one-sided authentication: only the network authenticated the UE. Moreover, it was up to the network to enable or disable encryption on the radio interface. This means that a technologically advanced attacker could set up a false base station and capture calls made through it. 3G introduced mutual authentication between the UE and network, so that the phone would only connect to radio access networks that were authorized roaming partners of the user's home operator. 4G further binds the network authentication to a specific serving network identifier (SNID), which is a numerical network identifier. However, the network name and timezone information presented to the user are not linked securely to the authenticated SNID. Moreover, it is not clear how the home operator is supposed to use the authenticated SNID. It could be compared with other signaling messages or charging records to detect discrepancies.

The limitations discussed above are not accidental but, rather, known compromises made when designing the architecture and trust model of the mobile networks. It is also possible that the complex protocol specifications have inadvertent flaws. Such mistakes in the protocol design may be discovered by formal analysis (Alt et al., 2016; Basin et al., 2018; Borgaonkar et al., 2019; Cremers and Dehnel-Wild, 2019). One recurring issue is that, while each technology specification addresses the perceived security weaknesses of the previous generations, the UEs and networks remain backward compatible with previous AKA versions.

One important goal of the AKA protocol is to hide the identity and location of the UE from an adversary on the radio link. The location update and authentication process has been designed to prevent passive sniffing of the IMSI and other identifiers. Thus, attackers have resorted to setting up fake base stations, so-called *IMSI catchers*, that actively trick the mobile into revealing its identity. The 3GPP radio network generations provide progressively stronger protection against such tracking; nevertheless, IMSI catchers have been demonstrated for all generations of the radio network (Borgaonkar and Shaik, 2021; Golde et al., 2013; Kune et al., 2012; Nohl, 2014; Park et al., 2019; Shaik et al., 2016). In addition to location and presence tracking, identification of the UE can lead to selective denial-of-service attacks.

Cryptographic techniques aim to find weaknesses in cryptographic algorithms and their implementations. The main target of such attacks in mobile networks has been the radio interface, where cryptography is used for authenticated key agreement (AKA) and for encryption and integrity protection.

The early encryption and key derivation algorithms (A5/1, A5/2) were stream ciphers designed for very constrained hardware, and they can now be broken in real-time (Barkan et al., 2008; Biryukov et al., 2000; Goldberg et al., 1999; Golić, 1997; Nohl and Melette, 2011a). These algorithms were proprietary and deliberately weakened due to export control regulations. The same weak algorithms are used for GPRS encryption with the name GEA/1 and GEA/2 (Nohl and Melette, 2011b). The later A5/3 and A5/4 are based on the KASUMI block cipher, which has some theoretical weaknesses but no known practical attacks (Dunkelman et al., 2010; 2014; Jia et al., 2011). The latest algorithm EEA2 is based on AES in counter mode. The main remaining weaknesses are due to backward compatibility, i.e., that a new UE may connect to an older generation network, and that news phones allow the use of older SIM cards that derive weak keys (Meyer and Wetzel, 2004a; 2004b).

The original GSM radio link had no integrity protection as the voice compression was designed to tolerate bit errors. Integrity protection was introduced in 3G for the signaling between the UE and core network. In 5G, the protection has been optionally extended to user data; however, real-world networks still rarely support the integrity protection. There are well-known attacks against data integrity on stream ciphers with no strong integrity check. It has been demonstrated in controlled settings that the attacker can modify DNS responses to the mobile (Rupprecht et al., 2019). Key stream reuse by broken implementations may enable call and data decryption and modification (Rupprecht et al., 2020a; 2020b). The alternative integrity algorithm ZUC suffers from similar issues (Wu and Gong, 2013).

Even strongly encrypted communication is vulnerable to traffic analysis. It may be possible to classify encrypted connections based on the timing and size of data. For example, both passive fingerprinting and active traffic watermarking have been used to identify accessed web sites and mobile users (Kohls et al., 2019).

Cryptographic attacks could also be targeted at the tunneling of user data and signaling on the core network on in interconnection and roaming. However, since these tunnels use strong encryption algorithms and integrity protection, cryptogprahic attacks are less likely than on the radio link.

6.4. Defense evasion

Adversarial techniques used for bypassing protection mechanisms, including evading detection of an adversary's presence, are grouped into the defense evasion tactical category.

Stealth scanning covers ways to avoid detection in the reconnaissance and discovery phases of the attack. Mobile operators deploy intrusion detection systems (IDS) and audit event logs, which could reveal the presence of the attacker. A common method is slow and randomized scans originating from a large number of source IP addresses (e.g., from a botnet or cloud), so that the scan looks like network noise. In the discovery phase, when the scanning source is within the operator network, even a single connection attempt could be detected. In that case, techniques such as TCP half-open scan may help the attacker avoid creating log events (SANS Institute: Global Information Assurance Certification Paper, 2002).

Firewall bypass refers to any techniques by which the adversary can get through the operator network boundary and avoid traffic filters.

The easiest targets are the UEs that have public IP addresses. Even if the UE does not accept incoming connections, it is vulnerable to denial-of-service and over-billing attacks (Leong et al., 2014). When SGSN or SGW implements a NAT or stateful firewall, the attacker could target the ports that are open on the gateway at any given time.

The operator core networks are protected from the Internet by strict firewalls. Nevertheless, the filtering defence allow some unwanted traffic through (Wang et al., 2011), for example, with spoofed source addresses. Moreover, the firewall itself could be a target of resource exhaustion attacks. Other vulnerabilities may lie in the address mapping logic of the NAT or IPv4-to-IPv6 translation (Hong et al., 2017). The IP firewalls may incorporate network intrusion detection systems (NIDS) that aim to detect anomalous activity in the network. Malware may try to evade the detection by using *covert channels* for its command and control traffic.

Signaling firewalls can analyze the signaling traffic for interconnection and roaming to detect patterns of malicious behavior (Kacer and Langlois, 2017). Studies show that only a small fraction of operators deploy such defences (ENISA, 2018). Even when they are deployed, attacks could be hidden by layers of encoding or encapsulation, such as nested tunneling (Whitehouse and Murphy, 2004). The malicious actors may avoid anomaly detection by hiding the unwanted activities among large quantities of legitimate SS7, Diameter and GTP signaling and by making only gradual changes to their behavior (Puzankov, 2017). Machine learning can help the detection of malicious behavior (Jensen et al., 2016), but machine learning algorithms themselves are vulnerable to new attack techniques such a generative adversarial network (GAN) (Creswell et al., 2018).

Denylist evasion refers to techniques for bypassing filtering defences at the endpoints of control-plane communication. Mobile operators have an allowlist of IP addresses and GTs of the signaling nodes in their own infrastructure and at partner operators, and they only accept SS7 and Diameter traffic from the authorized nodes. The nodes that should communicate with partner operators are listed in the IR.21 roaming database. There may be a similar allowlist of value-added service providers. In addition, the operator maintains a denylist to block unwanted traffic that it knows to be caused by either configuration errors and malicious activity. However, signaling between partner operators is often not authenticated, and the connections come through a third-party-maintained exchange (IPX or GRX). Thus, attackers may be able to to bypass the deny and allowlists by spoofing the sender addresses (Positive Technologies, 2017).

Malware anti-detection techniques are used to avoid detection of compromised network nodes and devices. The operating systems, software, and services on the network nodes could be compromised by malware or backdoors. Although operators conduct routine security audits to detect such compromises, it is unknown if hidden issues such as advanced persistent threats (APT) (Harries and Mayer, 2021), rootkits (Positive Technologies, 2021), or undiscovered backdoors remain. The UEs have been similarly targeted by stealth malware (Bickford et al., 2010; Marczak et al., 2018).

Signaling-protocol downgrading refers to techniques that trick the operator into using older and less secure signaling mechanisms. The hop-by-hop security on signaling protocols can be bypassed if the operator accepts also unauthenticated connections. The attacker could initiate the connections itself or cause legitimate access to be downgraded by blocking secure connections. Moreover, the attacker may prefer the older SS7 signaling protocol over the newer Diameter, either because hop-by-hop security is not deployed for the older protocol or because it wants to use old attacks that exploit SS7 features. Interworking functions for inter-generation communication translation could also be used to bypass authentication for Diameter (Holtmanns et al., 2016).

Radio-link downgrading and redirection techniques are used to force the phone into using insecure technologies or networks. Attacks on the radio access networks are well-studied, and newer network generations address weaknesses in the previous generations. However, radio link attackers can block service to the newer protocols and thus force the target UE to fall back to the older protocols and cryptographic algorithms. The attacker can then exploit weaknesses such as lack of integrity protection or one-sided authentication that no longer exist in the latest protocols. This downgrading attack is aided by the fact that most UEs can be configured to refuse the newer generations but the user typically cannot prevent the fallback to the older ones.

Even within the same network generation, the attacker can block the mobile's access to trusted radio networks, such as the user's home operator network. The UE may then connect to an unsafe roaming network where the calls and data can be intercepted (Zhang and Shan, 2016). This technique could also be used for capturing the UE to a network with high roaming charges.

7. Attack results phase

In the ultimate phase of the attack life cycle, the adversary hopes to achieve its main goals. The tactical objectives in this phase are thus related to information collection and other attack impact.

7.1. Collection

The tactical objective of information collection is about stolen and gathered sensitive data. The data may have inherent value to the attacker, or it may enable persistence and future attacks. While some of this data may have already been used in the previous phases, it is informative to summarize the data collected by the attacker throughout the attack life cycle.

Administrator credentials: One goal of the adversary is to obtain administrator and node credentials, such as usernames and passwords, master keys, access tokens, and API keys, for the network nodes and services. The privileged credentials may give the attacker persistent access to sensitive data and control over the system. The techniques used for obtaining the credentials are similar to those in enterprise information systems (The MITRE Corporation, 2019b).

Operator-specific identifiers are node and service identifiers and addresses of critical system components that give the adversary insider information about the operator network. For example, these include GTs and IP addresses of critical nodes as well as the Tunnel Endpoint Identifiers (TEID) of GTP tunnels.

Operator data includes information about the network architecture and configuration, such as the network topology, the trust relationship between nodes and operators, routing metadata, statistical information about network usage, as well as historical or live data about connections and mobility events. Naturally, the attacker would also want to get hold of sensitive technical and business documents. This data is mainly obtained with the discovery tactics and used for lateral movement in the system. However, it may also have long-term value to the adversary because it reveals weak points in the critical infrastructure or provides a competitive advantage.

User credentials in the mobile network are mainly the SIM card or profile and the secret key stored in the SIM. It is usually not possible to extract the secret key from the SIM, and it is more likely that the adversary either steals the SIM or gains indirect access to it. There have also been cases where the key leaks from the SIM supply chain (Scahill and Begley, 2015). In the remote SIM provisioning (RSP) protocol, the trusted subscription manager data preparation (SM-DP) entities become a part of the supply chain.

If the adversary gets access to the credentials, it can impersonate the user on the mobile system level as well as in applications that depend on the phone network for their security (Mulliner et al., 2013; The MITRE Corporation, 2022). The credentials also authorize the adversary to use telephony services and to charge them to the user's subscriber account.

User-specific identifiers in the mobile network comprise the subscriber identifier IMSI, user equipment identifier IMEI, and the phone number MSISDN. Each one of these identifiers uniquely identifies the UE and user, and the adversary needs to known them for location and presence tracking as well as for various SS7 and Diameter based attacks. The phone number is meaningful to human users, while IMSI identifies the user in signaling messages. An adversary with access to the signaling network can map the IMSI to the MSISDN and back. It has also been demonstrated that 2G radio networks can be exploited to discover this mapping for mobiles in the area (Yu et al., 2019). The IMEI is collected for logging and troubleshooting purposes. The logs enable law enforcement — and perhaps also the adversary — to trace a specific physical phone even when the SIM card and IMSI changes.

Communication metadata in the mobile network includes call detail records or charging data records (CDR), SMS and IMS metadata, and roaming information. Adversaries could obtain live data from a compromised serving network or UE, or it could exploit the SS7 and Diameter signaling protocols to query the data. Historical data can be found in home and roaming network logs and in log files on the UE. Billing records and other data in the OSS is another potential source of call logs and information about the mobile users and their affiliations.

Another interesting piece of metadata is the IP address and port number allocated to the UE at any given time. This can be used to link data connections from the mobile to Internet servers to the subscriber identity. There is regulation that requires operators to retain the address-allocation log for law-enforcement purposes. The data has been used, for example, to trace mobile Internet users who made libellous statements or shared copyrighted content online. The DNS queries and Internet connections from the mobile could be logged as well. Historically, operators were able to collect access logs from DNS servers and web proxies, but encryption now makes such data collection less reliable, and the server IP addresses identify the cloud platform rather than a specific service. Therefore, the user's Internet traffic reveals less meaningful information to the operator networks than it used to. Nevertheless, researchers have shown that, in some cases, the IMSI and other identifiers captured on the radio link can be correlated with the user's online activities and identities (Shaik et al., 2016).

7.2. Impact

This tactical category summarizes the impact which the attacks have on the users and network operator.

Location tracking is the privacy issue in mobile networks that has received the most attention. Cellular networks by their nature need to know about the mobile user's location and movements. Adversaries may exploit this for violating the user's privacy, either to tracking the users' locations and movements or to detect their presence at a specific area.

Adversaries with access to the SS7 (Engel, 2008; 2014), Diameter (Holtmanns et al., 2016; Rao et al., 2016b), or SIP (Kim et al., 2015b) signaling protocols can query the mobile's location from its home network or from the radio access network. The location granularity ranges from the location area (e.g., country or region) to the current cell identifier. The cellular networks also implement Location Based Services (LBS), which are used by emergency services and other authorized clients to obtain more accurate coordinates with trilateration based on signal timing and strength.

The IMSI catchers are fake base stations that collect UE identifiers in their vicinity (Jover, 2016; Kune et al., 2012; Park et al., 2019; Shaik et al., 2016). The attacker can increase the accuracy of the location information with trilateration from multiple observation points. The cleartext timing information present in the LTE radio-link signaling between the mobile and legitimate base stations can also be used to calculate the mobile's location (Roth et al., 2017).

Temporary identifiers (e.g., TMSI and GUTI) are used to avoid sending permanent identifiers like IMSI over the radio channel. While researchers have identified some weaknesses (Arapinis et al., 2014; Hong et al., 2018), it is impractical to track the mobile with only passive interception of the radio signals.

Personal information disclosure refers to leaks of the user's personal information from the operator network or information systems. This includes the identifying and contact information from the billing system as well as communication metadata, such as charging data records, message logs, and Internet access logs. As mentioned earlier, operators collect call and message metadata for charging and billing purposes, and they are also obligated to retain the records for a specific time for law-enforcement access. If an unauthorized party gets hold of such personal data, it is a violation of the users' privacy. Furthermore, data protection regulation requires the operators to take special care to protect such personal data; thus, potential data breaches create legal and business risks to the operator.

Mass information gathering uses the methods of information gathering already discussed above but targets the population at large rather than individual mobile users. Mass information gathering is commonly attributed to intelligence agencies (Fidler and Ganguly, 2015) or advertisers (Christl et al., 2017; Vanrykel et al., 2016). The call and message metadata could be used for large-scale data mining and algorithmic social network analysis (Gellman and Soltani, 2013; Rao et al., 2016a). Location data could be used to to trace people's movements and meetings on the population scale. Billing data could be used as an indicator or the subscriber's financial status. Users could also be fingerprinted to correlate their activities across networks and media. Extensive government and law-enforcement access to the data becomes a concerns when automated data collection and big-data mining methods replace manual investigations.

Unwanted communication is an everyday problem with which mobile phone users are familiar. The phone is part of the user's private space, and unwanted calls and messages can feel like a privacy invasion. Probably the most common type of unwanted communication is unsolicited sales calls including cold calling. The problem is aggravated by robocalls and predictive dialers (Tu et al., 2016b). In addition to legitimate marketing, unsolicited calls may be entirely fraudulent, such as phishing and technical support scams (Miramirkhani et al., 2016). Unwanted text messages may be simple advertising, or they may try to trick the user into replying and subscribing to fraudulent infotainment services. Sometimes, the unwanted calls and messages may be intentional harassment.

The primary defense against unwanted calls is the caller id, i.e, the caller's telephone number or name displayed to the callee before answering. The caller id may, however, be spoofed, or the caller may use variable and unlisted numbers. In North America, there has been an effort to authenticate the caller id (Internet Engineering Task Force (IETF), 2022). Another defense mechanisms against unwanted calls is unlisted and secret phone numbers. These are often used by public figures and those who have been targeted for harassment. However, the number may leak accidentally or intentionally (Snyder et al., 2017). For information on these and other defense mechanisms, such as the caller name lookup service (CNAM), we refere the reader to (Tu et al., 2016b).

Call, message and data interception is the ultimate goal for the adversary in a mobile telephone network. While mobile networks encrypt calls and data over the air, the encryption terminates right at the edge of the network, i.e., at the base station. This allows efficient routing of the calls to their destination, as well as local breakout of data traffic to the Internet, but also makes it possible for the adversary perform targeted interception of user traffic from compromised base stations or roaming networks.

For mass surveillance, the adversary would prefer central locations in the network where it can observe most connections. We will list some such locations. Within a 2G or 3G operator network, the mobile switching center (MSC) acts as a telephony switch. Calls between operators and international calls may be routed through the public switched telephone networks (PSTN). Many of the international calls are routed though satellite links and sea cables, which are vulnerable to espionage (Gellman and Soltani, 2013; Webb, 2007). Data and IMS between operators typically goes through exchanges like GRX an IPX (Kho and Kuiters, 2014). Data destined to the Internet will naturally be exposed to the same threats as any Internet traffic.

Another approach to interception is to manipulate the routing of calls or data. A compromised mobile operator that has access to the interconnection and roaming system could intercept calls or SMS by spoofing signaling messages (Holtmanns and Oliver, 2017; Puzankov and Kurbatov, 2014). Also, SMS home routing or Customised Applications for Mobile networks Enhanced Logic (CAMEL) (Engel, 2014) could potentially be misused for traffic interception.

Mobile networks have not embraced the idea of end-to-end encryption for phone calls or text and multimedia messages. While there exists a 3GPP specification for end-to-end confidentiality in the IMS media plane (3rd Generation Partnership Project, 2021), it has not been deployed. This may be due to the deployment complexity or the need for law enforcement to intercept the communication. Moreover, any universally deployed end-to-end security mechanisms would depend on the endpoint authentication provided by the operators or some third party, which could become the weak link in the system.

Failure of mobile network as trusted channel can happen when mobile applications and online services use the phone to bootstrap their security. Applications often rely on text messages sent or robot calls made to the user's phone as the second factor in two-factor authentication (2FA). The phone number is also used as a trusted recovery channel when users lose or forget credentials, in which case it becomes the only authentication factor. These authentication methods are vulnerable to an adversary that is able to intercept the messages, for example, because it has compromised the radio link or a node on the operator network. For this reason, the trend in security-critical applications is away from relying on the user's phone number and text messages for authentication.

Billing discrepancies refers to any inconsistencies on the charging and billing data and processes in the mobile network. In the 3GPP context, *charging* is the collection of information about chargeable events, such as calls, message, data or roaming, and *billing* means transforming this information into a bill that requires payment. The discrepancies can occur at both stages, and both under and over billing are potential problems. We refer the reader to Sahin et al. (2017) for a classification of fraud in telephony networks.

An obvious threat from the subscriber's point of view is that they might be overcharged or billed for services they did not use. In such disputes, the adversary is typically a value-added service provider or a roaming partner. The home operator is often in the difficult position that is being billed for services which the subscriber disputes.

The subscriber might also be billed for services that were really used but unintentionally and for fraudulent reasons. The user may be fraudulently enrolled for value-added services, or they may be misled to subscribe to services that are excessively expensive and difficult to cancel. A malicious smartphone app may call or message a premium-rate number or subscribe to value-added services without the user's consent (Tu et al., 2016a). In the missed call scam, the adversary takes advantage of the user's habit of returning missed calls: the user is tricked into dialing a premium rate number or expensive international number. Inadvertent roaming mostly takes place in border regions where a phone might accidentally connect to a roaming operator and incur high roaming charges. This can even be intentionally caused by antenna placement by the roaming operator.

In SMS payment and direct operator billing, the telephone operator effectively becomes a payment services provider for non-telephony services and products. This opens the possibility for new types of crime, such as fraudulent billing by the service providers or making fraudulent purchases that are billed to the victim. In general, when the phone is used to make payments for other services or goods, it becomes easier for cybercriminals to covert their control of the phone or the operator network to money or tangible goods.

The origins of telephone network security are in ensuring that the subscriber always pays for the calls and services. The user should not be able to evade charges for the usage, and they should not be able to shift the charges to another user. These were bigger concerns in the past, before flat-rate mobile subscriptions. However, some subscribers still have metered connections or data caps, and they may try to evade the charges. Potential loopholes in mobile networks arise from free services, such as DNS name resolution or TCP re-transmission, which could be used for tunneling data (Go et al., 2014; Peng et al., 2012), and IP-based signaling in VoLTE, which may bypass charging (Kim et al., 2015a; Li et al., 2015).

Denial of service attacks (Jover, 2013) can target either the network or a specific user. The attacks can originate from external interfaces, most significantly the radio interface and the gateways that connect the operator network to the Internet. They can also originate from compromised nodes within the operator network or, more likely, from interconnection and roaming.

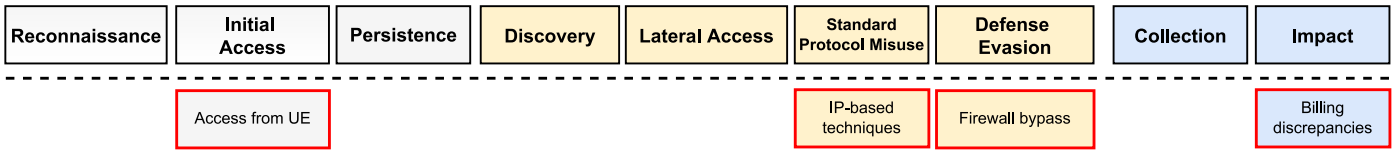

Fig. 4. Case study 1: Free Internet access by tunneling over DNS (Peng et al., 2012).

Many reported DoS attacks against the RAN abuse radio channel allocation requests (Bassil et al., 2012; 2013; Golde et al., 2013; Kambourakis et al., 2011; Lee et al., 2009; Ricciato et al., 2010). More generally, the attacker can cause DoS by repeatedly triggering resource allocation or revocation requests. Another major category of DoS arises from the IP-based interfaces, which are the IMS domain and the connections to the public Internet (Croft and Olivier, 2007; Enck et al., 2005; Traynor et al., 2008; Tu et al., 2016a). Such attacks could be launched by cellular botnets (Khosroshahy et al., 2013; Traynor et al., 2009).

Radio signal jamming can obviously cause local DoS within the radio range (Aziz et al., 2014; Jover, 2013; Lichtman et al., 2016; 2013; Xiao et al., 2013). There are open-source tools which the radio-link adversaries can use (Rao et al., 2017). The typical goal of the DoS would be to enable interception and tracking attacks (Shaik et al., 2015).

Adversaries who have access to the SS7 and Diameter protocols (Engel, 2014; Kotte et al., 2016) can misuse them to target a specific user for DoS. For example, they can spoof location updates to prevent the user from receiving calls or messages.

8. Case studies of applying the framework

This section presents two case studies of the Bhadra threat modeling framework. The first is a relatively simple attack, and the second shows how the framework allows us to model a more complex attack and compare its different variants.

8.1. Case study 1: Free mobile internet access

Peng et al. (2012) describe how a mobile subscriber can obtain free internet access by tunneling the data over DNS queries and responses. This works because mobile operators often do not charge for DNS access, which is also needed to access free pages such as the operator's online shop. In some cases, the malicious subscriber can connect to a VPN server in the internet that is listening in the TCP or UDP port 53, and the operator will assume it to be DNS traffic. Most operators limit the free access to their own DNS server. In that case, the malicious subscriber can encapsulate the user data into recursive DNS queries, which the operator's DNS server forwards to the user's specially crafted DNS server. These techniques have been observed in the wild and implemented as VPN mobile app. Similar techniques have previously been used to obtain free internet in wireless hotspots and hotel networks Hex (2020).

This relatively simple attack makes use of the following techniques (see Fig. 4):

Initial access — The attack is based on *access from UE*.

Standard protocol misuse — The attack misuse DNS, which falls into *IP-based techniques*.

Defense evasion — The goal of the attack is to bypass the filtering of unpaid internet access from the mobiles. Additionally, the malicious subscriber may have to adjust its behavior to the data formats and rate limits allowed for outbound DNS requests. Thus, the attack involves *firewall bypass*.

Impact — The goal of the attack is to avoid paying for the service. The impact is thus categorized *billing discrepancy*.

8.2. Case study 2: Simjacker

The *Simjacker* attack was disclosed by AdaptiveMobile Security in September 2019 (AdaptiveMobile Security, 2019b). *Simjacker* is a large-scale espionage attack on mobile users, presumably by a competent adversary group on behalf of a nation-state actor, whose adversarial behavior we want to characterize through the lens of our framework.

The adversary exploited a vulnerability in a software application that exists on many SIM cards: the S@T browser. It is a microbrowser application for accessing the operator's value-added services. The browser communicates with the operator backend over binary SMS messages, which are not seen by the phone user (3rd Generation Partnership Project, 2020b). The operator can send push messages to the S@T application. The phone routes the received binary SMS to the specific application on the SIM, and the SIM authenticates them before processing the contents. The vulnerability in this case was that many operators had misconfigured the S@T application to accept also unauthenticated push messages.

The adversary could thus send unauthenticated commands to the S@T browser. In the most common form of the attack, the adversary used the S@T application functionality to query the IMEI and location of the phone. The application processes the commands without interaction with the user. The adversary could launch the attack from the SS7 signaling network, a commercial SMS gateway, or even from an ordinary mobile phone.

We now model the *Simjacker* attack with the Bhadra framework (see Fig. 5). There are two interesting variants of the attack. In the *phone-based* attack, the malicious SMS messages are sent from an ordinary mobile phone. This attack is not suitable for tracking large numbers of subscribers over time. In the *interconnection-based*, the attack originates from an unscrupulous operator network that allows the adversary to send high volumes of suspicious SMS messages, either with an SMS gateway or with direct access to the SS7 signaling network.

Reconnaissance — SIM cards with misconfigured S@T browsers were distributed by operators in at least 29 countries. To find the vulnerable operators and the phone numbers of their subscribers, the adversary would have resorted to *out-of-band intelligence gathering*. It may also have scanned the operator's number space, which is *perimeter mapping for mobiles*.

Initial access — The adversary gains access to the target through the SIM card with misconfigured S@T browser functionality. Thus, the initial access technique is *SIM-based compromise*. For the interconnection-based attack, the adversary also needs *access from inside the operator network* at some operator in the world.

Persistence — The S@T browser configuration is embedded in the SIM card firmware and cannot be modified by the user. Therefore, the adversary achieves a level of persistence by *exploiting hard-to-repair vulnerabilities*. The operator can, however, modify the security settings with an over-the-air (OTA) update.

Lateral movement — Analysis of the detected attacks revealed that the messages originated from both phones and from the SS7 interconnection. In the latter case, the adversary *exploits roaming and interconnection* to mounted the attack remotely from another operator network and country. To be precise, the phone-based at-

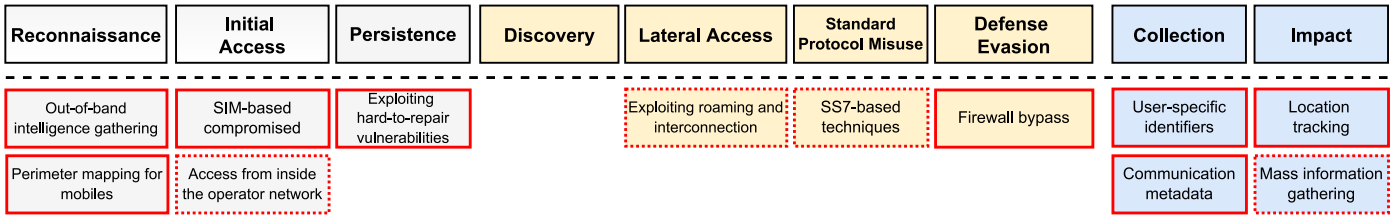

Fig. 5. Case study 2: *Simjacker* attack (AdaptiveMobile Security, 2019b). Phone-based attack uses the techniques marked with solid lines. Interconnection-based attack additionally includes the techniques marked with dotted lines.

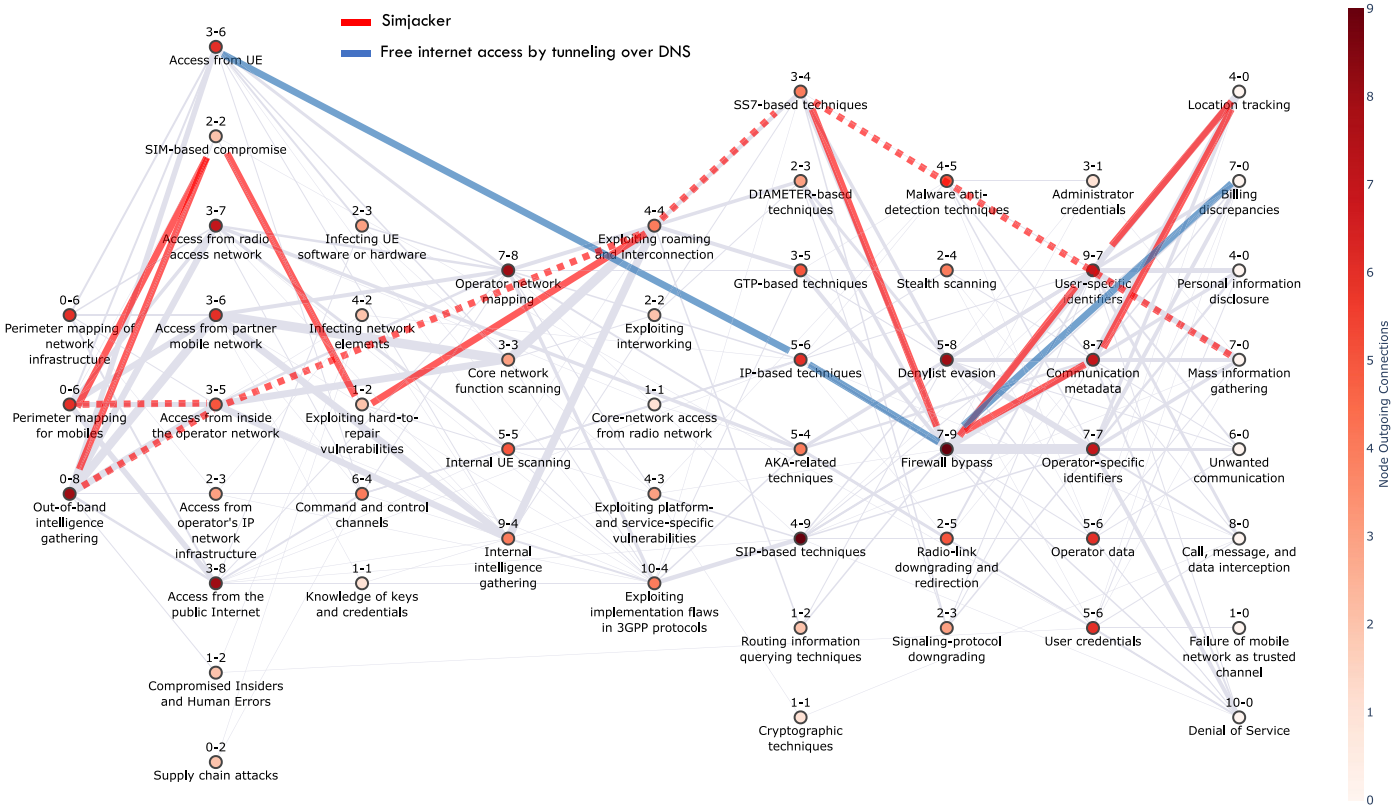

Fig. 6. Case studies 1 and 2 in the context of total 65 modeled attacks.

tack can also be mounted from another country, but that is not an essential part of the phone-based attack.

Standard protocol misuse — For the interconnection-based attack, *SS7-based techniques* were used for sending the SMS messages. The SS7 access may have been implemented by the attacker or by an unscrupulous SMS gateway.

Defense evasion — Attacks based on binary SMS have been demonstrated before (Alecu, 2013; Nohl, 2013), and they have also been observed in the wild (Marczak and Scott-Railton, 2016; Spiedgel International, 2014). It is therefore possible that operators detect or filter unusual binary SMS activity. It appears that *Simjacker* circumvented such filtering by varying the binary SMS header format. This is a form of *firewall bypass*.

Collection — The targeted SIM card returns to the adversary the IMEI (*user-specific identifier*)) and serving cell-ID (*communication metadata*). The collected information is sent back to the adversary in another binary SMS.

Impact — The goal of the observed attacks was *location tracking*, although there could be other variants that exploit the same vulnerability for a different purpose. Given the large scale of the interconnection-based attacks, the impact included *mass information gathering*.

Figure 6 shows the two case studies in the context of 65 attacks that we have modelled using the framework.

9. Discussion

The Bhadra framework is a threat modeling framework for the mobile telecommunication networks. It adopts the structure of the MITRE ATT&CK (Strom et al., 2018) framework for enterprise information systems, which is already a familiar tool for enterprise IT security in the telecommunications sector. Unlike the MITRE framework, Bhadra focuses on threats that target or exploit the mobile communication infrastructure.

The threat modeling framework provides a structured way to talk about threats and attacks against the system. On one hand, it provides a conceptual framework and common terminology for discussing the attacker behavior. The conceptualization helps to see the threats in a somewhat technology-independent way, e.g., across network generations. On the other hand, the framework is a knowledge base of known attacker tactics and techniques. The knowledge is systematized following the attack phases from target discovery all the way to impact, which makes is easy to communicate observed or potential threats.

The framework provides a language for security professionals to analyze and communicate incident and vulnerability information with sufficient context. During incident investigation, it helps security analysts to see the technical details within a bigger picture and to provide actionable summary information for colleagues and management. The common vocabulary is also useful for threat intelligence sharing across organizations. The level of abstraction aims to be such that it is possible to share meaningful information without disclosing confidential details about the operator's network. Since the framework is structured to model the attacker behavior, it can help in attack attribution. We have experimentally used the framework for quantitative threat intelligence, i.e., to detect trends in attacker behavior (Chen and Rao, 2021).

As a knowledge base, the framework supports preemptive threat analysis. It can be used by red teams and penetration testers to ensure coverage of all stages in the attack kill chain and for reporting their findings. System designers can use the framework as a reference to map their current defense posture, to search for potential security issues, and to understand how new defensive measures would prevent attacker activity.

Why is a separate threat modeling framework needed for mobile communication networks? The mobile operator networks can be seen both as collections of IT services and as a communication network. From both perspectives, their technology differs considerably from the enterprise information systems and networks. The internal interfaces in the communication systems are based on different protocol standard, such as SS7 and Diameter, as opposed to HTTP APIs. In addition to the ubiquitous Internet connections, the mobile operator networks have two additional external boundaries: the radio interface accessed by millions of untrusted users and devices, and the interconnection and roaming between operators to form a world-wide telecommunications system. Compared the Internet, the trust model in the mobile networks is still partly based on the idea of trusted operators and closed networks.

Recently, the discussion of telecommunication network security has been dominated by the new threats created by cloud computing and virtualization technologies in 5G (Ahmad et al., 2017; Khan et al., 2019). In the current version of Bhadra, we have chosen to model threats that are specific to telecommunication and exist across network generations. There are many significant and interesting threats that originate from the current and older generations of cellular networks and are not the focus of the 5G security discussion. Yet, these issues will continue to be relevant in 5G because the interfaces and trust model remain essentially the same.

The Bhadra framework has so far been used for company-internal threat modeling in product development and for communicating the threats and mitigation techniques to partner organizations. We have implemented threat modeling and visualization tools (Chen and Rao, 2021) to support this work. The Bhadra framework has already influenced an industry-wide effort (Donegan, 2017). Formal work on a threat modeling framework has started in the GSMA Fraud and Security Group (FASG). The Bhadra knowledge base will be made available to the community by via contributions to this effort.

The information for the framework has been curated from publicly available sources that primarily include peer-reviewed academic publications, white papers, news items, and reports from security auditors. We have only used sources where sufficient technical details have been published for understanding the attack process, required attacker capabilities, and potential impact on the communication systems. It is quite common for online articles to make claims about possible security breaches while providing only vague descriptions of the attacker's tactics for achieving them, and the curators of the knowledge base have to be careful to dissect such claims to their technical components. One limitation in compiling threat intelligence from the telecommunications sector is that it is not feasible for the curators to try to reproduce all the claimed attacks. Another limitation is that there is little public information about which attacks have occurred in the wild; the incident data remains exclusive to mobile operators, and it is rarely shared between companies. Thus, in most cases, it is not possible for the curators to differentiate between potential attacks based on vulnerability analysis, attacks confirmed with laboratory experiments, and techniques that are used by real-world adversaries. Nevertheless, all vulnerability reports can point out potential weaknesses, and addressing them can lead to more robust system design.

The telecommunications industry and operators are aware of this lack of communication, and it is often attributed to the fact that there is no common language or conceptual framework that could be used for the information sharing. We believe that the Bhadra framework is a step towards providing a unified language for sharing information about security incidents and attacker behavior among industry players and that the framework, together with follow-up community efforts, can lower the barriers for addressing mobile communications security on the industry level.

Comparison with the MITRE ATT&CK framework The techniques in our framework are specific to mobile communications. This often means adapting and reinterpreting the tactical objectives as well. Firstly, the *execution, privilege escalation, command and control* tactical objectives have been dropped because there is little public information on attack techniques that would fall under them. Instead, we grouped the first two into a single technique called *exploit platform- and service-specific vulnerabilities* and demoted *command and control* into a technique. Secondly, *lateral movement* was renamed *lateral access* because reported attacks in mobile networks rarely involve more than one compromised network node. Instead, attackers use the signaling protocols to access the necessary services across the networks. Thirdly, *standard protocol misuse* was added as a new tactical objective due to the high importance of the protocols in mobile operator networks and in the attacks against them. Fourthly, *credential access, exfiltration* have been merged into the *collection* tactical objective. Finally, *network effects* and *remote service effects* from the mobile domain matrix have been merged into the *impact* tactical objective, which was redefined to include all end results achieved by the adversary.

10. Conclusion

This article presents a threat modeling framework that is specific to mobile communication systems. The *Bhadra framework* aims to provide a unified conceptual framework for analyzing and communicating security threats that specifically target or make use of the mobile operator infrastructure. Following prior work on threat modeling in the enterprise IT area, the framework focuses on attacker behavior at different stages of the attack life cycle. The goal is to find a level of abstraction that makes it possible to describe the attack in a meaningful way without having to understand all the technical details, to analyze common patterns and trends in attacks, and to share information within and between organizations. We describe case studies of the framework on modeling individual attacks and understanding the commonalities and differences in related attacks. The Bhadra framework has already been influential in initiating industry-wide discussion on threat modeling frameworks for mobile communication networks.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

References

Abdelrazek, L., 2018GTScan: the Nmap scanner for telcohttps://www.github.com/SigPloiter/GTScan [Online] Accessed: 2020-03-31

Abdelrazek, L., Azer, M.A., 2018. SigPloit: a new signaling exploitation framework. In: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, pp. 481–486.

AdaptiveMobile Security, 2019a. New simjacker vulnerability exploited by surveillance companies for espionage operationAccessed: 2020-03-15

AdaptiveMobile Security, 2019b. Simjacker next generation spying over mobile https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile [Online]Accessed: 2020-03-15

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A., 2017. 5G Security: analysis of threats and solutions. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, pp. 193–199.

Alecu, B., 2013. SMS fuzzing–SIM toolkit attack, Vol. 21. DEF CON.

Alt, S., Fouque, P.-A., Macario-Rat, G., Onete, C., Richard, B., 2016. A cryptographic analysis of UMTS/LTE AKA. In: International Conference on Applied Cryptography and Network Security. Springer, pp. 18–35.

Amine, Y. E., 2021Former softbank employee alleged to have leaked 5G data to Rakuten https://www.insidetelecom.com/former-softbank-employee-leaks-5g-secrets-to-rivals/ [Online] Accessed: 2021-09-29

Anagnostopoulos, M., Kambourakis, G., Gritzalis, S., 2016. New facets of mobile botnet: architecture and evaluation. Int. J. Inf. Secur. 15 (5), 455–473.

Anwar, N., Riadi, I., Luthfi, A., 2016. Forensic SIM card cloning using authentication algorithm. Int. J. Electron.Inform. Eng. 4 (2), 71–81.

Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M., 2014. Privacy through pseudonymity in mobile telephony systems. NDSS.

Armasu, L., 2018Backdoors keep appearing in Cisco's routers https://www.tomshardware.com/news/cisco-backdoor-hardcoded-accounts-software,37480.html [Online]Accessed: 2021-09-29

Ashdown, M., Lynchard, S., 2001. SS7 Firewall System. US Patent 6,308,276.

Aziz, F.M., Shamma, J.S., Stüber, G.L., 2014. Resilience of LTE networks against smart jamming attacks. In: 2014 IEEE Global Communications Conference. IEEE, pp. 734–739.

Barkan, E., Biham, E., Keller, N., 2008. Instant ciphertext-only cryptanalysis of GSM encrypted communication. J. Cryptol. 21 (3), 392–429.

Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V., 2018. A formal analysis of 5G authentication. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383–1396.

Bassil, R., Chehab, A., Elhajj, I., Kayssi, A., 2012. Signaling oriented denial of service on LTE networks. In: Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access, pp. 153–158.

Bassil, R., Elhajj, I.H., Chehab, A., Kayssi, A., 2013. Effects of signaling attacks on LTE networks. In: 2013 27th International Conference on Advanced Information Networking and Applications Workshops. IEEE, pp. 499–504.

Bhorkar, G., et al., 2017Security analysis of an operations support system.

Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., Iftode, L., 2010. Rootkits on smart phones: attacks, implications and opportunities. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, pp. 49–54.

Biryukov, A., Shamir, A., Wagner, D., 2000. Real time cryptanalysis of A5/1 on a PC. In: International Workshop on Fast Software Encryption. Springer, pp. 1–18.

Bodeau, D., McCollum, C., Fox, D., 2018. Cyber Threat Modeling: Survey, Assessment, and Representative Framework. HSSEDI, The MITRE Corporation.

Borgaonkar, R., Hirschi, L., Park, S., Shaik, A., 2019. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. Proc. Privacy Enhancing Technol. 2019 (3), 108–127.

Borgaonkar, R., Redon, K., Seifert, J.-P., 2011. Security analysis of a femtocell device. In: Proceedings of the 4th International Conference on Security of Information and Networks. ACM, pp. 95–102.

Borgaonkar, R., Shaik, A., 2021. 5G IMSI Catchers Mirage. BlackHat Briefings.

Borgaonkar, R., Shaik, A., Asokan, N., Niemi, V., Seifert, J.-P., 2015. LTE and IMSI catcher myths, Vol. 2015. BlackHat Europe.

Brandom, R., 2017For $500, this site promises the power to track a phone and intercept its texts https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime [Online] Accessed: 2020-03-15

Burgess, D. A., Samra, H. S., et al., 2008The OpenBTS project http://openBTS.org [Online] Accessed: 2022-01-10

Butler, K., Farley, T.R., McDaniel, P., Rexford, J., 2009. A survey of BGP security issues and solutions. Proc. IEEE 98 (1), 100–122.

Chalakkal, S., Schmidt, H., Park, S., 2017. Practical Attacks on VoLTE and VoWiFi. Tech. Rep. ERNW Enno Rey Netzwerke.

Checkoway, S., Maskiewicz, J., Garman, C., Fried, J., Cohney, S., Green, M., Heninger, N., Weinmann, R.-P., Rescorla, E., Shacham, H., 2016. A systematic analysis of the juniper dual EC incident. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 468–479.

Chen, H.Y., Rao, S.P., 2021. Adversarial trends in mobile communication systems: from attack patterns to potential defenses strategies. In: Nordic Conference on Secure IT Systems. Springer, pp. 153–171.

Christl, W., Kopp, K., Riechert, P.U., 2017. Corporate surveillance in everyday life 6.

Copet, P.B., Marchetto, G., Sisto, R., Costa, L., 2015. Formal verification of LTE-UMTS handover procedures. In: 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE, pp. 738–744.

Copet, P.B., Marchetto, G., Sisto, R., Costa, L., 2017. Formal verification of LTE-UMTS and LTE–LTE handover procedures. Comput. Standards Interfaces 50, 92–106.

Cremers, C., Dehnel-Wild, M., 2019Component-based formal analysis of 5G-AKA: channel assumptions and session confusion.

Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., Bharath, A.A., 2018. Generative adversarial networks: an overview. IEEE Signal Process Mag 35 (1), 53–65.

Croft, N.J., Olivier, M.S., 2007. A silent SMS denial of service (DoS) attack. Information and Computer Security Architectures (ICSA) Research Group South Africa, Vol. 29.

Cybereason, 2019Operation soft cell: a worldwide campaign against telecommunications providers https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos [Online] Published on: June 25, 2019

Cybereason, 2021DeadRinger: Exposing chinese threat actors targeting major telcos https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos [Online] Published on: August 3, 2021

Dabrowski, A., Petzl, G., Weippl, E.R., 2016. The messenger shoots back: network operator based IMSI catcher detection. In: International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, pp. 279–302.

Donegan, P., 2017An ATT&CK-Like framework for telcos https://www.hardenstance.com/wp-content/uploads/2020/09/HardenStance-Briefing-on-An-ATTCK-Framework-For-Telecom-Final.pdf [Online] Accessed: 2022-01-10

Dunkelman, O., Keller, N., Shamir, A., 2010. A practical-time attack on the a5/3 cryptosystem used in third generation GSM telephony. IACR Cryptol. ePrint Arch 2010, 13.

Dunkelman, O., Keller, N., Shamir, A., 2014. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. J. Cryptol. 27 (4), 824–849.

Durumeric, Z., Adrian, D., Mirian, A., Bailey, M., Halderman, J.A., 2015. A search engine backed by internet-wide scanning. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 542–553.

Ehlert, S., Geneiatakis, D., Magedanz, T., 2010. Survey of network security systems to counter sip-based denial-of-service attacks. Comput. Secur. 29 (2), 225–243.

Electronic Communications Committee (ECC), 2003(Report 30) technical briefing: mobile access to the internet https://docdb.cept.org/download/286 [Online] Accessed: 2022-01-10

Enck, W., Traynor, P., McDaniel, P., La Porta, T., 2005. Exploiting open functionality in SMS-capable cellular networks. In: Proceedings of the 12th ACM conference on Computer and communications security, pp. 393–404.

Engel, T., 2008. Locating mobile phones using signalling system 7. 25th Chaos communication congress.

Engel, T., 2014. Ss7: Locate. Track. Manipulate. Talk at 31st Chaos Communication Congress.

"ENISA", 2018. Signalling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation. Technical Report.

European Union Agency for Cybersecurity (ENISA), 2020Enisa threat landscape for 5g networks 2019 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [Online] Accessed: 2021-01-15

European Telecommunications Standards Institute (ETSI),. Technical Report

European Telecommunications Standards Institute (ETSI), 2020Technical committee (TC) lawful interception (LI) https://www.etsi.org/committee/1403-li [Online] Accessed: 2022-03-15

Ettus Research,. USRP Software Defined Radio (SDR) On-Line Catalog https://www.ettus.com/products/ [Online] Accessed: 2022-08-15

Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D., 2011. A survey of mobile malware in the wild. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 3–14.

Ferrag, M.A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H., 2018. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. 101, 55–82.

Fidler, D.P., Ganguly, S., 2015. The Snowden Reader. Indiana University Press.

Franceschi-Bicchierai, L., 2018How criminals recruit telecom employees to help them hijack SIM cards https://www.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam [Online],Accessed: 2020-03-15

Franklin, J., Brown, C., Dog, S., McNab, N., Voss-Northrop, S., Peck, M., Stidham, B., 2016. Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue. Technical Report. National Institute of Standards and Technology.

Gauci, S., 2021Massive DDoS attacks on VoIP providers and simulated DDoS testing https://www.rtcsec.com/post/2021/09/massive-ddos-attacks-on-voip-providers-and-simulated-ddos-testing/ [Online], Accessed: 2021-09-29

Gellman, B., Soltani, A., 2013NSA tracking cellphone locations worldwide, Snowden documents show https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [Online],Accessed: 2020-03-15

3rd Generation Partnership Project, 1999–2022. Security Algorithms. 3GPP Technical Specification Series TS 35.

3rd Generation Partnership Project, 1999–2022. Security Aspects. 3GPP Technical Specification Series TS 33.

3rd Generation Partnership Project, 2007. Study into routeing of MT-SMs via the HPLMN. 3GPP Technical Report TR 23.840.
3rd Generation Partnership Project, 2020. Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks. 3GPP Technical Specification TS 24.302.
3rd Generation Partnership Project, 2020. Universal Subscriber Identity Module (USIM) Application Toolkit (USAT). 3GPP Technical Specification TS 31.111.
3rd Generation Partnership Project, 2020. Unstructured Supplementary Service Data (USSD) using IP Multimedia (IM) Core Network (CN) subsystem IMS; Stage 3; Release 16. 3GPP Technical Specification TS 24.390.
3rd Generation Partnership Project, 2021. IP Multimedia Subsystem (IMS) Media Plane Security; Release 16. 3GPP Technical Specification TS 33.328.
3rd Generation Partnership Project, 2022. Technical Specification Group Core Network and Terminals; InterWorking Function (IWF) between MAP based and Diameter based interfaces (Release 17). 3GPP Technical Specification TS 29.305.
Geng, G., Xu, G., Zhang, M., Guo, Y., Yang, G., Wei, C., 2012. The design of SMS based heterogeneous mobile botnet. JCP 7 (1), 235–243.
Go, Y., Won, J., Kune, D.F., Jeong, E., Kim, Y., Park, K., 2014. Gaining control of cellular traffic accounting by spurious TCP retransmission. In: Network and Distributed System Security (NDSS) Symposium 2014. Internet Society, pp. 1–15.
Goldberg, I., Wagner, D., Green, L., 1999. The real-time cryptanalysis of A5/2. Rump Session of Crypto 99, 16.
Golde, N., Redon, K., Borgaonkar, R., 2012. Weaponizing femtocells: the effect of rogue devices on mobile telecommunications. NDSS.
Golde, N., Redon, K., Seifert, J.-P., 2013. Let me answer that for you: exploiting broadcast information in cellular networks. In: Presented as Part of the 22nd USENIX Security Symposium (USENIX Security 13), pp. 33–48.
Golić, J.D., 1997. Cryptanalysis of alleged A5 stream cipher. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 239–255.
Gomez-Miguelez, I., Garcia-Saavedra, A., Sutton, P.D., Serrano, P., Cano, C., Leith, D.J., 2016. srsLTE: an open-source platform for LTE evolution and experimentation. In: Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization, pp. 25–32.
Goodwin, C., 2020. Why Sideload? User behaviours, interactions and accessibility issues around mobile app installation. In: Proceedings of the 33rd International BCS Human Computer Interaction Conference 33, pp. 27–30.
GSM Association, 2018IR.34 guidelines for IPX provider networks https://www.gsma.com/newsroom/wp-content/uploads//IR.34-v14.0-3.pdf [Online] Accessed: 2020-03-15
GSM Association, 2019Mobile telecommunications security threat landscape 2020 https://www.gsma.com/security/resources/mobile-telecommunications-security-threat-landscape-report/ [Online] Accessed: 2020-09-15
Handley, M., Schulzrinne, H., Schooler, E., Rosenberg, J., 1999. SIP: Session Initiation Protocol. RFC 2543.
Harries, J., Mayer, D., 2021LightBasin: a roaming threat to telecommunications companies https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/ [Online] Published on: October 19, 2021
Hasan, R., Myagmar, S., Lee, A.J., Yurcik, W., 2005. Toward a threat model for storage systems. In: Proceedings of the 2005 ACM workshop on Storage security and survivability, pp. 94–102.
Hau, B., Lee, T., Homan, J., 2015SYNful knock-a Cisco router implant-Part I https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html [Online] Accessed: 2020-03-15
Hex, P., 2020Part 1: free unlimited internet trick DNS settings for all ISPs in the world https://www.techfoe.com/2020/10/part-1-free-unlimited-internet-trick.html [Online] Accessed: 2022-01-10
Holtmanns, S., Oliver, I., 2017. SMS and one-time-password interception in LTE networks. In: 2017 IEEE International Conference on Communications (ICC). IEEE, pp. 1–6.
Holtmanns, S., Rao, S.P., Oliver, I., 2016. User location tracking attacks for LTE networks using the interworking functionality. In: 2016 IFIP Networking conference (IFIP Networking) and workshops. IEEE, pp. 315–322.
Hong, B., Bae, S., Kim, Y., 2018. GUTI reallocation demystified: Cellular location tracking with changing temporary identifier. NDSS.
Hong, H., Choi, H., Kim, D., Kim, H., Hong, B., Noh, J., Kim, Y., 2017. When cellular networks met IPv6: Security problems of middleboxes in IPv6 cellular networks. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, pp. 595–609.
Internet Engineering Task Force (IETF), 2022Secure telephone identity revisited (STIR) https://datatracker.ietf.org/wg/stir/about/ [Online] Accessed: 2022-01-10
Jack, W., Suri, T., 2011. Mobile Money: The Economics of M-PESA. Technical Report. National Bureau of Economic Research.
Jensen, K., Van Do, T., Nguyen, H.T., Arnes, A., 2016. Better protection of SS7 networks with machine learning. In: 2016 6th International Conference on IT Convergence and Security (ICITCS). IEEE, pp. 1–7.
Jia, K., Rechberger, C., Wang, X., 2011. Green Cryptanalysis: Meet-in-the-Middle key-Recovery for the Full KASUMI Cipher. Report 466. International Association for Cryptologic Research (IACR), Cryptology ePrint Archive.
Jordan, S., Lee, M., 2015Not so securus: massive hack of 70 million prisoner phone calls indicates violations of attorney-client privilege https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/ [Online] Accessed: 2020-03-15
Jover, R.P., 2013. Security attacks against the availability of LTE mobility networks: overview and research directions. In: 2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC). IEEE, pp. 1–9.
Jover, R. P., 2016LTE security, protocol exploits and location tracking experimentation with low-cost software radio arXiv preprint arXiv:1607.05171.
Kacer, M., Langlois, P., 2017. SS7 Attacker Heaven Turns into Riot: How to make Nation-State and Intelligence Attackers Lives Much Harder on Mobile Networkss. BlackHat, USA.
Kambourakis, G., Kolias, C., Gritzalis, S., Park, J.H., 2011. DoS attacks exploiting signaling in UMTS and IMS. Comput. Commun. 34 (3), 226–235.
Kaspersky Lab Report, 2014The Regin Platform: Nation-State Ownage of GSM Networks https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07185213/Kaspersky_Telecom_Threats_2016.pdf [Online] Accessed: 2020-03-15
Keromytis, A.D., 2011. A comprehensive survey of voice over ip security research. IEEE Commun. Surv. Tutor. 14 (2), 514–537.
Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M., 2019. A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. IEEE Commun. Surv. Tutor. 22 (1), 196–248.
Khatri, V., Abendroth, J., 2015. Mobile guard demo: network based malware detection. In: 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1. IEEE, pp. 1177–1179.
Kho, S., Kuiters, R., 2014Hitb Conference: On Her Majesty's Secret Service - GRX & A Spy AgencyAccessed: 2021-11-24
Khosroshahy, M., Qiu, D., Ali, M.K.M., 2013. Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface. In: 2013 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT). IEEE, pp. 30–35.
Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., Kim, T., Kim, Y., 2015. Breaking and fixing volte: exploiting hidden data channels and mis-implementations. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 328–339.
Kim, H., Lee, J., Lee, E., Kim, Y., 2019. Touching the untouchables: dynamic security analysis of the LTE control plane. In: 2019 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 1153–1168.
Kim, S., Koo, B., Kim, H., 2015. Tracking location information of volte phones. In: 2015 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, pp. 703–708.
Kirchgaessner, S., 2020Revealed: Saudis suspected of phone spying campaign in US https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us [Online]
Kocialkowski, P., 2014Replicant developers find and close Samsung Galaxy backdoor https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor [Online] Accessed: 2019-12-30
Kohls, K., Rupprecht, D., Holz, T., Pöpper, C., 2019. Lost traffic encryption: fingerprinting LTE/4G traffic on layer two. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 249–260.
Kotapati, K., 2008Assessing security of mobile telecommunication networks.
Kotte, B., Holtmanns, S., Rao, S., 2016. Detach Me Not–DoS Attacks Against 4G Cellular users Worldwide from Your Desk. blackhat Europe 2016.
Kuhne, R., Huitema, G., Carle, G., 2011. Charging and billing in modern communications networks–a comprehensive survey of the state of the art and future requirements. IEEE Commun. Surv. Tutor. 14 (1), 170–192.
Kune, D. F., Koelndorfer, J., Hopper, N., Kim, Y., 2012Location leaks on the GSM air interfaceISOC NDSS (Feb 2012).
Kurtz, G., Alperovitch, D., 2012Hacking exposed: mobile rat edition http://docs.huihoo.com/rsaconference/usa-2012/Hacking-Exposed-Mobile-RAT-Edition.pdf [Online] Accessed: 2022-01-10
Langlois, P., 2009SCTPscan: SCTP network and port scanner https://www.p1sec.com/corp/research/tools/sctpscan/ [Online] Accessed: 2020-03-31
Lee, K., Kaiser, B., Mayer, J., Narayanan, A., 2020An empirical study of wireless carrier authentication for SIM swaps
Lee, M., Moltke, H., 2019Everybody does it: the messy truth about infiltrating computer supply chains https://theintercept.com/2019/01/24/computer-supply-chain-attacks/ [Online] Published on: Jun 24, 2019
Lee, P.P., Bu, T., Woo, T., 2009. On the detection of signaling dos attacks on 3G/WiMax wireless networks. Comput. Netw. 53 (15), 2601–2616.
Leong, R., Perez, D., Dean, T., 2019MESSAGETAP: whos reading your text messages? https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html [Online] Accessed: 2020-03-31
Leong, W.K., Kulkarni, A., Xu, Y., Leong, B., 2014. Unveiling the hidden dangers of public ip addresses in 4G/LTE cellular data networks. In: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, pp. 1–6.
Li, C.-Y., Huang, C.-C., Lai, F., Lee, S.-L., Wu, J., 2018. A comprehensive overview of government hacking worldwide. IEEE Access 6, 55053–55073.
Li, C.-Y., Tu, G.-H., Peng, C., Yuan, Z., Li, Y., Lu, S., Wang, X., 2015. Insecurity of voice solution volte in LTE mobile networks. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 316–327.
Li, V.G., Dunn, M., Pearce, P., McCoy, D., Voelker, G.M., Savage, S., 2019. Reading the tea leaves: a comparative analysis of threat intelligence. In: 28th USENIX Security Symposium (USENIX) Security 19), pp. 851–867.
Lichtman, M., Jover, R.P., Labib, M., Rao, R., Marojevic, V., Reed, J.H., 2016. LTE/LTE-a jamming, spoofing, and sniffing: threat assessment and mitigation. IEEE Commun. Mag. 54 (4), 54–61.
Lichtman, M., Reed, J.H., Clancy, T.C., Norton, M., 2013. Vulnerability of LTE to hostile interference. In: 2013 IEEE Global Conference on Signal and Information Processing. Ieee, pp. 285–288.

Lindskog, S., Brunstrom, A., 2008. An end-to-end security solution for SCTP. In: 2008 Third International Conference on Availability, Reliability and Security. IEEE, pp. 526–531.

Marczak, B., Scott-Railton, J., 2016. The Million Dollar Dissident: NSO Groups iPhone Zero-Days used Against a UAE Human Rights Defender. The Citizen Lab.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., Deibert, R., 2018. HIDE AND SEEK: Tracking NSO Groups Pegasus Spyware to Operations in 45 Countries. Technical Report.

Mashukov, S., 2017. Diameter security: an auditor's viewpoint. J. ICT Stand. 5 (1), 53–68.

Matherly, J., 2015. Complete Guide to Shodan, Vol. 1. Shodan. LLC (2016-02-25)

Mehra, K., Evans, J. F., Sexson, J., 2019Contextual signaling system 7 (SS7) firewall and associated method of useUS Patent App. 16/242,630

Mende, D., Rey, E., 2011Practical security research on 3G and 4G mobile telecommunications networksAccessed: 2020-03-31

Meyer, U., Wetzel, S., 2004. A man-in-the-middle attack on UMTS. In: Proceedings of the 3rd ACM workshop on Wireless Security, pp. 90–97.

Meyer, U., Wetzel, S., 2004. On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. In: 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No. 04TH8754), Vol. 4. IEEE, pp. 2876–2883.

Miramirkhani, N., Starov, O., Nikiforakis, N., 2016. Dial one for scam: analyzing and detecting technical support scams. 22nd Annual Network and Distributed System Security Symposium (NDSS, Vol. 16.

Mitnick, K.D., Simon, W.L., 2003. The Art of Deception: Controlling the Human Element Of security. John Wiley & Sons.

Mulliner, C., Borgaonkar, R., Stewin, P., Seifert, J.-P., 2013. SMS-based one-time passwords: attacks and defense. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp. 150–159.

Nakarmi, P. K., 2021Cheatsheets for authentication and key agreements in 2G, 3G, 4G, and 5G arXiv preprint arXiv:2107.07416.

Nasser, Y., 2019Gotta catch 'Em all: Understanding how IMSI-catchers exploit cell networks https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks#Spoofing [Online] Accessed: 2020-03-15

Nexusguard, 2020Threat report: online gaming is a hotbed for DDoS attacks https://www.nexusguard.com/hubfs/2020Q3_Threat%20Report_Final.pdf [Online] Accessed: 2021-09-29

Nohl, K., 2013. Rooting SIM cards. BlackHat Briefings. Accessed: 2020-03-15

Nohl, K., 2014. Mobile self-defense. 31st Chaos Communication Congress 31C3.

Nohl, K., Melette, L., 2011. Defending mobile phones. The 28th Chaos Communication Congress.

Nohl, K., Melette, L., 2011. GPRS intercept: wardriving your country. Chaos Communications Camp 2011, 2011.

Nurse, J.R., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R., Whitty, M., 2014. Understanding insider threat: a framework for characterising attacks. In: 2014 IEEE Security and Privacy Workshops. IEEE, pp. 214–228.

OHanlon, P., Borgaonkar, R., 2016. WiFi-based IMSI catcher. In: Proccedings of the Black Hat Europe 2016 Conference, London, 3rd November, Vol. 2016.

Pancevski, B., 2020U.S. officials say Huawei can covertly access telecom networks https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256 [Online] Accessed: 2021-09-29

Park, S., Shaik, A., Borgaonkar, R., Seifert, J.-P., 2019. Anatomy of commercial IMSI catchers and detectors. In: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society. ACM, pp. 74–86.

Pegg, D., Cutler, S., 2021What is Pegasus spyware and how does it hack phones? https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [Online] Published on: July 18, 2021

Peltonen, A., Sasse, R., Basin, D., 2021. A comprehensive formal analysis of 5G handover. In: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM.

Peng, C., Li, C.-y., Tu, G.-H., Lu, S., Zhang, L., 2012. Mobile data charging: new attacks and countermeasures. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security. ACM, pp. 195–204.

Positive Technologies, 2017Threats to packet core security of 4G networks https://positive-tech.com/research/epc-research/#Fraud [Online] Accessed: 2020-03-15

Positive Technologies, 2018Diameter vulnerabilities in the spotlight https://positive-tech.com/research/diameter-2018/ [Online] Accessed: 2020-03-31

Positive Technologies, 2021Rootkits: evolution and detection methods https://www.ptsecurity.com/upload/corporate/ww-en/analytics/PT_Rootkit_ENG.pdf [Online] Published on: November 3, 2021

Puzankov, K., 2019. Hidden agendas: bypassing GSMA recommendations on SS7 networks. In: Hack In The Box Conference.

Puzankov, S., 2017. Stealthy SS7 attacks. J. ICT Stand. 5 (1), 39–52.

Puzankov, S., Kurbatov, D., 2014How to intercept a conversation held on the other side of the planetPHDays (August 2014), http://2014.phdays.com/program/tech/36930.

Qing, Z., Guangdong, B., 20173G/4G Intranet scanning and its application on the wormhole vulnerability https://www.blackhat.com/docs/asia-17/materials/asia-17-Bai-3G-4G-Intranet-Scanning-And-Its-Application-On-The-WormHole-Vulnerability.pdf [Online] Published on: March 31, 2017

Rajavelsamy, R., Choudhary, M., Das, D., 2015. A review on evolution of 3GPP systems interworking with WLAN. J. ICT Stand. 133–156.

Rao, R.M., Ha, S., Marojevic, V., Reed, J.H., 2017. LTE PHY layer vulnerability analysis and testing using open-source SDR tools. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, pp. 744–749.

Rao, S., Holtmanns, S., Oliver, I., Aura, T., 2016a. The known unknowns of SS7 and beyond https://ernw.de/download/TSD2016_Known_Unknowns_of_SS7.pdf [Online]

Rao, S. P., 2015Analysis and mitigation of recent attacks on mobile communication backend.

Rao, S.P., Holtmanns, S., Oliver, I., Aura, T., 2015. Unblocking stolen mobile devices using SS7-MAP vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access. In: 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1. IEEE, pp. 1171–1176.

Rao, S.P., Kotte, B.T., Holtmanns, S., 2016. Privacy in LTE networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, pp. 176–183.

Ricciato, F., Coluccia, A., DAlconzo, A., 2010. A review of DoS attack models for 3G cellular networks from a system-design perspective. Comput. Commun. 33 (5), 551–558.

Robertson, J., Riley, M., 2018. The Big Hack: How China Used a Tiny Chip to Infiltrate US Companies Vol. 4.

Rose, S. W., Borchert, O., Mitchell, S., Connelly, S., 2020Zero trust architecture.

Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M.A., Samdanis, K., Sayadi, B., 2016. Mobile network architecture evolution toward 5G. IEEE Commun. Mag. 54 (5), 84–91.

Roth, J., Tummala, M., McEachen, J., Scrofani, J., 2017Location privacy in LTE: a case study on exploiting the cellular signaling plane's timing advance.

Rupprecht, D., Dabrowski, A., Holz, T., Weippl, E., Pöpper, C., 2018. On security research towards future mobile network generations. IEEE Commun. Surv. Tutor. 20 (3), 2518–2542.

Rupprecht, D., Jansen, K., Pöpper, C., 2016. Putting LTE security functions to the test: a framework to evaluate implementation correctness. 10th USENIX Workshop on Offensive Technologies (WOOT 16).

Rupprecht, D., Kohls, K., Holz, T., Pöpper, C., 2019. Breaking LTE on layer two. In: 2019 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 1121–1136.

Rupprecht, D., Kohls, K., Holz, T., Pöpper, C., 2020. Call me maybe: Eavesdropping encrypted LTE calls with ReVoLTE. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 73–88.

Rupprecht, D., Kohls, K., Holz, T., Pöpper, C., 2020. IMP4GT: impersonation attacks in 4G networks. ISOC Network and Distributed System Security Symposium (NDSS). ISOC.

Sahin, M., Francillon, A., Gupta, P., Ahamad, M., 2017. SoK: fraud in telephony networks. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, pp. 235–250.

SANS Institute: Global Information Assurance Certification Paper, 2002Stealth port scanning methods https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446 [Online] Accessed: 2022-01-10

Scahill, J., Begley, J., 2015The great SIM heist: how spies stole the keys to the encryption castle[Online]. The Intercept, Accessed: 2020-03-15.

Schlegel, R., Obermeier, S., Schneider, J., 2015. Structured system threat modeling and mitigation analysis for industrial automation systems. In: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN). IEEE, pp. 197–203.

Selin, J., 2019Evaluation of threat modeling methodologies.

Sengar, H., Wijesekera, D., Jajodia, S., 2005. MTPSec: customizable secure MTP3 tunnels in the SS7 network. In: 19th IEEE International Parallel and Distributed Processing Symposium. IEEE, pp. 8–pp.

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J.-P., 2015Practical attacks against privacy and availability in 4G/LTE mobile communication systems arXiv preprint arXiv:1510.07563.

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J.-P., 2016. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. 23rd Annual Network and Distributed System Security Symposium (NDSS 2016). Internet Society.

Shostack, A., 2014. Threat Modeling: Designing for Security. John Wiley & Sons.

Sisalem, D., Kuthan, J., Ehlert, S., 2006. Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms. IEEE Netw. 20 (5), 26–31.

Snyder, P., Doerfler, P., Kanich, C., McCoy, D., 2017. Fifteen minutes of unwanted fame: detecting and characterizing doxing. In: Proceedings of the 2017 Internet Measurement Conference, pp. 432–444.

Spensky, C., Stewart, J., Yerukhimovich, A., Shay, R., Trachtenberg, A., Housley, R., Cunningham, R.K., 2016. SoK: privacy on mobile devices—its complicated. Proc. Privacy Enhancing Technol. 2016 (3), 96–116.

Spiedgel International,2014 http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html [Online], Accessed: 2022-01-10. Inside TAO: Documents reveal top NSA hacking unit

Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B., 2018. MITRE ATT&CK: Design and Philosophy. Technical report.

Strom, B.E., Battaglia, J.A., Kemmerer, M.S., Kupersanin, W., Miller, D.P., Wampler, C., Whitley, S.M., Wolf, R.D., 2017. Finding Cyber Threats with ATT&CK-Based Analytics. Technical Report MTR170202. MITRE.

Sun, S.-T., Cuadros, A., Beznosov, K., 2015. Android rooting: methods, detection, and evasion. In: Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 3–14.

The MITRE Corporation, 2019a. MITRE ATT&CK Adversary groups https://attack.mitre.org/groups/ [Online] Accessed: 2020-04-04

The MITRE Corporation, 2019b. MITRE ATT&CK: Credential Access https://attack.mitre.org/tactics/TA0006/ [Online] Accessed: 2020-04-04

The MITRE Corporation, 2022MITRE ATT&CK: Capture SMS Messages https://attack.mitre.org/techniques/T1412/ [Online] Accessed: 2022-01-10
Toffalini, F., Abbà, M., Carra, D., Balzarotti, D., 2016. Google dorks: analysis, creation, and new defenses. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp. 255–275.
Tounsi, W., Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 72, 212–233.
Traynor, P., Enck, W., McDaniel, P., La Porta, T., 2008. Mitigating attacks on open functionality in SMS-capable cellular networks. IEEE/ACM Trans. Netw. 17 (1), 40–53.
Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., La Porta, T., 2009. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 223–234.
Tu, G.-H., Li, C.-Y., Peng, C., Li, Y., Lu, S., 2016. New security threats caused by IMS-based SMS service in 4G LTE networks. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1118–1130.
Tu, H., Doupé, A., Zhao, Z., Ahn, G.-J., 2016. SoK: everyone hates robocalls: a survey of techniques against telephone spam. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 320–338.
Tung, L., 2014Hackers access 800,000 orange customers data https://www.zdnet.com/article/hackers-access-800000-orange-customers-data/ [Online] Accessed: 2020-03-15
van Rijsbergen, K., 2016. The Effectiveness of a Homemade IMSI Catcher Build with YateBTS and a BladeRF. University of Amsterdam.
Vanrykel, E., Acar, G., Herrmann, M., Diaz, C., 2016. Leaky birds: exploiting mobile application traffic for surveillance. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 367–384.
Wang, Z., Qian, Z., Xu, Q., Mao, Z., Zhang, M., 2011. An untold story of middleboxes in cellular networks. ACM SIGCOMM Comput. Commun. Rev. 41 (4), 374–385.
Webb, D., 2007. Echelon and the NSA. In: Cyber Warfare and Cyber Terrorism. IGI Global, pp. 453–468.
Weinmann, R.-P., 2012. Baseband attacks: remote exploitation of memory corruptions in cellular protocol stacks. In: WOOT, pp. 12–21.
Welte, H., Markgraf, S., 2010. Running your own GSM stack on a phone. 27th Chaos Communication Congress (27C3).
Whitehouse, O., Murphy, G., 2004. Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks. Atstake Inc.. Mar
Wu, T., Gong, G., 2013. The weakness of integrity protection for LTE. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 79–88.
Xenakis, C., 2006. Malicious actions against the GPRS technology. J. Comput. Virol. 2 (2), 121–133.
Xenakis, C., 2008. Security measures and weaknesses of the GPRS security architecture. IJ Netw. Secur. 6 (2), 158–169.
Xiao, J., Wang, X., Guo, Q., Long, H., Jin, S., 2013. Analysis and evaluation of jammer interference in LTE. In: Proceedings of the Second International Conference on Innovative Computing and Cloud Computing, pp. 46–50.
Yu, C., Chen, S., Cai, Z., 2019. LTE phone number catcher: a practical attack against mobile privacy. Secur. Commun. Netw. 2019.
Zeng, Y., Shin, K.G., Hu, X., 2012. Design of SMS commanded-and-controlled and P2P-structured mobile botnets. In: Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 137–148.
Zhang, R., Wang, X., Yang, X., Jiang, X., 2007. Billing attacks on SIP-based VoIP systems. WOOT 7, 1–8.
Zhang, W., Shan, H., 2016. Lte redirection: Forcing targeted lte cellphone into unsafe network. In: Proc. Defcon. Accessed: 2020-01-04

Siddharth Prakash Rao is a research scientist (security and privacy) at Nokia-Bell Labs and a doctoral candidate at Aalto University, Finland. He holds double master's degrees from Aalto University, Finland (Information and network security) and the University of Tartu, Estonia (Cryptography). As a Ford-Mozilla Open Web Fellow at European Digital Rights (EDRi) during 2016-17, he contributed to various EU-level policies as a technology expert. His research interests include security analyses of different kinds of networked systems and understanding human factors of security.

Hsin-Yi Chen graduated from the Security and Cloud Computing (SECCLO) Erasmus Mundus Joint Master Degree program, holding double master's degrees from Aalto University, Finland (Technology) and The Norwegian University of Science and Technology, Norway (Security and Cloud Computing). During her master's studies, she grew her research interest in telecommunication security through her 6 months internship with Ericsson Security Manager and did her master thesis on threat modeling and analysis for mobile communication systems with Nokia Bell Labs. Besides security, she is also interested in Human-Computer Interaction (HCI)studies. She currently works as a security solution manager at Ericsson.

Tuomas Aura received the MSc and PhD degrees from Helsinki University of Technology, Espoo, Finland, in 1996 and 2000, respectively. His doctoral thesis was on authorization and availability in distributed systems. He is a Professor of computer science and engineering with Aalto University, Espoo, Finland. Before joining Aalto University, he worked with Microsoft Research, Cambridge, U.K. He is interested in network and computer security and the security analysis of new technologies.