Adversarial Trends in Mobile Communication Systems: From Attack Patterns to Potential Defenses Strategies

Hsin Yi Chen[1] and Siddharth Prakash Rao[1,2(✉)]

[1] Aalto University, Espoo, Finland
hsin-yi.chen@aalto.fi
[2] Nokia Bell Labs, Espoo, Finland
sid.rao@nokia-bell-labs.com

Abstract. Understanding attack patterns and attacker behavior has always been a prominent security research topic to provide insights into adversarial trends and defense strategies. In this paper, we demonstrate the process of analyzing adversarial trends in mobile communication systems using a conceptual threat modeling framework combined with graph analysis methodologies. We model 60 attacks using the Bhadra framework [30] and conduct graph-theory-based analysis to deduce insights. We observed the attack patterns, the diversity of attack paths given an attacker's ability or target impact, and the importance of each technique from a network graph viewpoint and discussed potential defense strategies that mobile operators can deploy accordingly. Our main contribution is demonstrating the potential of Bhadra for analyzing the security posture of an operator's network and simplifying the complexity of the mobile networks to communicate the security analysis results.

Keywords: Threat modeling · Mobile networks · Attack patterns

1 Introduction

As the threat landscape of mobile communication systems expands with the broader adoption of newer technologies and the involvement of more parties, threat intelligence sharing has become essential. As a response, the industry partners, including standardization and regulatory bodies (e.g., 3GPP, ENISA) and academia, have conducted many security analyses. However, there is a lack of common taxonomy and conceptual framework to gather all the knowledge in one place. In this work, we argue that such a framework is essential in understanding adversarial trends. It forms the first step in security communication towards threat intelligence sharing.

To our best knowledge, the recently proposed Bhadra framework [30] is the only conceptual threat and attack modeling framework that captures attack vectors in the end-to-end mobile communication systems from 2G to 4G. In this work, we demonstrate how a framework like Bhadra can be used to gain

N. Tuveri et al. (Eds.): NordSec 2021, LNCS 13115, pp. 153–171, 2021.
https://doi.org/10.1007/978-3-030-91625-1_9

insights on adversarial trends and provide potential defense strategies for mobile operators. In particular, we model individual attacks with Bhadra and apply graph-theoretic analysis on the modeled attack data. By visually representing our analysis, we discuss how operators can use similar methods to discover attack patterns, analyze the importance of techniques to the attackers and explore the possible impact given the attackers' capability. Our main contribution is to demonstrate how to use a framework like Bhadra for analyzing the security posture of an operator's network using readily available graph algorithms and simple visualizations.

Although threat modeling has always been an integral part of system security, it is mostly confined to using well-known frameworks – such as STRIDE [39] or MITRE ATT&CK [6] in recent years – on different types of systems. However, research on how to communicate threat modeling findings, especially graph analysis techniques, is far less explored. Some of the recent works [1,44] have used the MITRE ATT&CK framework for enterprise systems that initiated such a line of research. We continue to extend the research in the context of mobile communications systems and with the Bhadra framework. In this realm, one of our contributions is to explore Bhadra's potential in simplifying the complexity of mobile network security while building narratives for security communication.

The rest of the paper is organized as follows. Section 2 presents an overview of the mobile communication networks, the Bhadra framework, and existing research that summarizes analysis methods in attack patterns. Section 3 describes the methodology we used to collect attacks and conduct graph analysis. Section 4 presents the graph analysis results. Section 5 discusses limitations of our work and potential research directions in overcoming them. Finally, Sect. 6 contains concluding remarks.

2 Background

This section gives a high-level overview of mobile network topology to show the attack surface covered in the Bhadra framework. We discuss some of the known security weaknesses, specifically mobile network protocols, to illustrate the types of attack techniques that can be modeled using Bhadra. Then, we briefly introduce Bhadra and its design philosophy. Finally, we present related work in finding attack patterns and attack graph analysis.

2.1 Mobile Network Topology

Figure 1 shows a simplified version of mobile network topology that consists of the following components. *User Equipment (UE)* contains a Subscriber Identification Module (SIM) card that supports the identification of the subscriber to its mobile operator with the International Mobile Subscriber Identity (IMSI) stored in the SIM card. *Radio Access Network (RAN)* is the air interface that connects UEs to operators' networks. *Core Network (CN)* comprises components

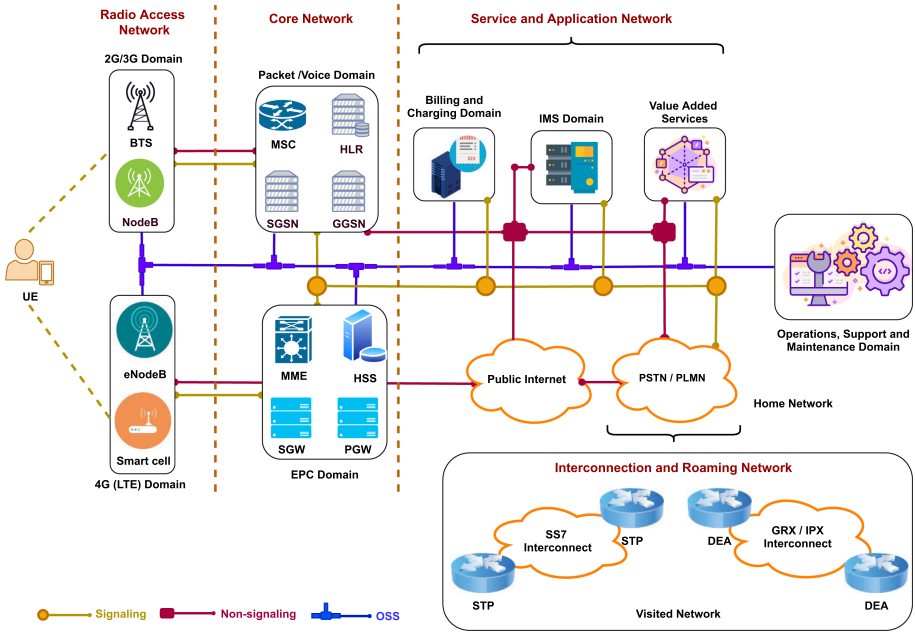

Fig. 1. Overview of mobile networks topology [4]

that are responsible for managing subscribers' authentication and mobility, initiating connections, and providing core telephony services such as SMS, voice calls, and Internet data.

Service and Application Network includes components that are responsible for billing and charging of the mobile service used by the subscribers. It also includes IP multimedia subsystem (IMS) and Value-added Services (VAS) that provide supplementary services to mobile subscribers on top of the core telephony services. In addition, *Interconnection and Roaming Network* enables roaming scenarios when a subscriber is outside their operator's serving area (i.e., home network). In a roaming scenario, the visited operator is connected to the subscriber's home network over the General Packet Radio Service (GPRS) roaming exchange or IP exchange carrier and retrieves the subscriber's profile from the Home Location Register (HLR) using signaling protocols.

2.2 Security Weaknesses

This section briefly describes some of the known security weaknesses in different mobile generation and communication protocols. Although these weaknesses are not exhaustive, we intend to help the readers to understand the techniques defined in the Bhadra framework or the attacks analyzed in this paper.

The 2nd generation (2G) or GSM networks offers three main security features, namely, subscriber authentication, encryption at the radio interface for

communication, and the use of temporary identities for identity confidentiality [9]. Nevertheless, they are susceptible to active eavesdropping attacks on the radio interface because there is no mutual authentication between the subscriber and base stations of the connected operator. Security design of the 3G networks improves such weaknesses in 2G by introducing mutual authentication between UE and the base stations, along with mandatory integrity protection for signaling messages that the mobile and network exchange.

While the security features on the RAN have improved between generations, the 3G core network still uses legacy communication protocols such as the Signalling System 7 (SS7) that raise security concerns. SS7 was developed in 1975, where mobile networks were run by a closed network of mutually trusted and government-owned operators. Therefore, security was not a top priority in the design considerations. Eventually, the number of mobile operators and other service providers from the private sector in the mobile communication network increases, and SS7 become an attractive target to exploit. Due to the lack of authentication to verify the message origin, SS7 can be abused for obtaining subscriber information, eavesdropping, financial theft, and disruption of subscriber service [29,43].

Another often exploited protocol is GPRS Tunnelling Protocol (GTP), a suite of IP-based communication protocols that transport user data over the mobile network. The GPRS network connects many internal network elements and other external networks such as the public Internet and other network operators, thus providing broad attack surfaces for attackers. However, since no built-in security mechanism is supported in GTP, operators are suggested to implement security protection such as IP Security (IPsec) at their network interfaces. Failing to do so may path the way for attackers to successfully carry out GTP attacks that leads to data interception, billing frauds, DoS against the network or user, and privacy leaks [41].

Session Initial Protocol (SIP) is yet another protocol with many known vulnerabilities. SIP is the underlying session control protocol used in IMS to provide multimedia communications services. Exploiting the vulnerabilities in SIP allows the attackers to, for example, send spoof SMS and perform Denial of Service (DoS) on SMS clients [42]. Commonly targeted IMS services include IMS-based Voice over IP (VoIP), Voice over LTE (VoLTE), SMS [42].

The 4G LTE network inherits several security weaknesses from 2G and 3G, mainly because it has to support backward compatibility. Also, since LTE contains several IP-based systems, attackers can now use IP-based penetration tools or exploit network components (e.g., DNS servers) they are more familiar with. This would naturally increase the attack surface and undermines the overall security. Among several other threats against Evolved Packet System (EPS) [9], jamming or flooding the radio channels of the mobile users to cause DoS is one of the common threats to LTE networks.

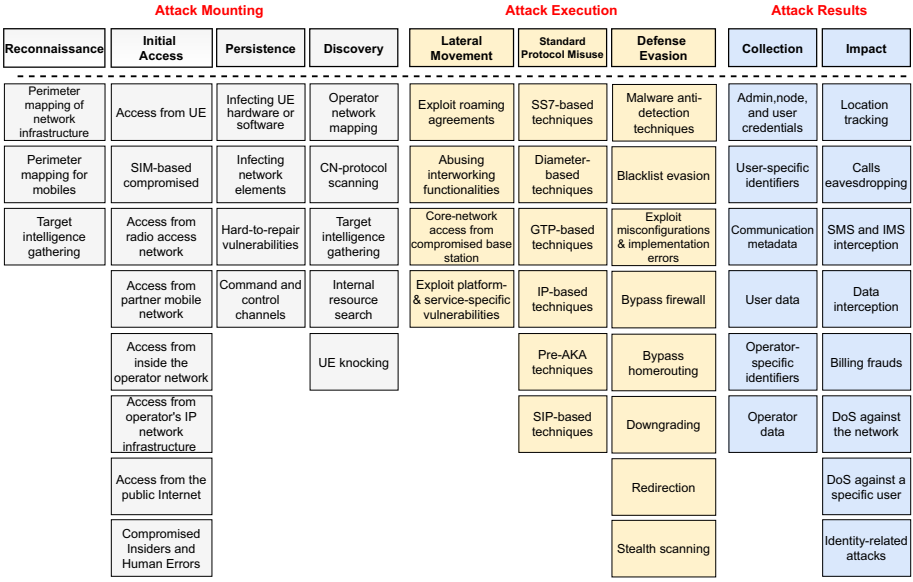

Fig. 2. Bhadra threat modeling framework [30]

2.3 Bhadra Framework

Bhadra is a conceptual threat and attacks modeling framework that captures attack vectors in end-to-end mobile communication systems. Bhadra provides a taxonomy to map attacks and threats to 2G, 3G, and 4G mobile networks, where it describes the adversarial behaviors in terms of tactics and techniques. For more details about Bhadra, refer to the original paper [30].

Similar to the MITRE ATT&CK framework, Bhadra's taxonomy is arranged as a matrix (as shown in Fig. 2). The column titles are called *Tactics*, and they are essentially categories of *techniques*. Tactics are the attacker's intermediate or final goals, and techniques are the methods to accomplish those goals. Bhadra takes inspiration for its design philosophy from the ATT&CK framework and hence, shares several commonalities. Nevertheless, Bhadra's taxonomy covers techniques specific to network environment and protocols used in telecommunication systems, which are missing from the ATT&CK framework. For more complex mobile network attacks, one can use both Bhadra and ATT&CK in conjunction. This work solely uses the Bhadra framework.

Bhadra can be used for both attack and threat modeling. While modeling, the modeler would manually express the attack or threat as a set of tactic and techniques pairs which is referred to as *models* in this paper. Depending on the complexity of the attack, models may contain all or only a few tactics, and each tactic selected may contain more than one technique.

2.4 Attack Pattern and Graph Analysis

As network topologies are of graph-based structure, researchers have explored the possibility of using graph analysis methods to simulate and predict the attackers' behavior, assess risk in the network, and harden network security in, for example, enterprise network and cyber-physical systems. The graph analysis methods include graph algorithms, Bayesian networks, Markov models, cost optimization algorithms like game theory, and uncertainty algorithms [46]. However, we have not found any existing research in attack graph analysis focusing on mobile communication networks.

Research also exists that extracts attack patterns observed with threat modeling frameworks. In recent work, Al-Shear et al. investigated the MITRE ATT&CK techniques associations using hierarchical clustering to represent interdependencies among the techniques. These relations can help predict adversarial behavior based on observed attacks and support threat mitigation [1].

3 Methodology

This section explains the methodology we use to collect and model attacks. Moreover, we introduce the graph algorithms we use to associate with different aspects of the adversarial trends.

3.1 Attack Collection and Sampling

First, through a thorough literature review, we collected different types of attacks for modeling with the Bhadra framework. We mainly reused the broad literature presented in Bhadra's original paper [30]. It contains two groups of literature: *Group I* includes peer-reviewed papers that describe one or multiple attacks scenarios. *Group II* consists of security reports from standardization bodies (e.g., 3GPP, GSMA) and regulatory agencies (e.g., ENISA).

Out of this pool, we used the following three criteria for sampling the attacks for our study. (1) We selected multi-staged attacks that contain mounting, execution, and result collection stages. (2) We prioritized attacks where their descriptions clearly state at least the initial access and final impact along with some details on the attack procedures. (3) We picked attacks that cover different initial accesses, protocols, and network components for variety. The first and second criteria ensured that we could model the selected attacks using Bhadra as per its threat modeling procedure. At the same time, the third criteria allowed us to imitate a real-life scenario of an operator – where the observed attacks often consist of a variety of attack vectors – while seeking insights from the analysis. Our sampling yielded us 30 sources (i.e., attack papers) in total.

After the sampling, we further reviewed the selected attacks and found many similar ones with minor variants. In such attacks, the end goals and some intermediate steps were the same. However, the only varying aspect was the message types used for attacks, such as different Radio Resource Control (RRC) procedure messages in Pre-AKA techniques. We decided to count those as separate

attacks while modeling even though they have a partially similar pattern. This way, we keep the graph analysis weighting more realistic as using different message types can be seen as different paths with which an attacker can reach the same end goals. We populated 60 attacks primarily from 30 of the sources that we had sampled. Table 2 in the appendix lists all the attacks that we considered.

It is important to note that the mobile operators rarely discuss actual attacks on their networks in public forums. Due to the lack of such attack data, we treat our collection of 60 attacks as if they were observed on a single operator's network premise for the rest of the paper. We believe that the attacks in our collection represent real-world scenarios (in terms of their practicality and variety), and an actual audit of an operator's network might yield a similar collection. This reasonable generalization helps us communicate our observations from graph analysis and potential defense strategies from an operator's point of view.

3.2 Attack Modeling

From our previous threat modeling experience with Bhadra, we observed that even with the clear technique description and examples that Bhadra provides, people may still come up with different models given the same attack scenario. This is because the results of any threat or attack modeling would vary based on the expertise (domain knowledge) of the person modeling it and of the details provided about the attack/threat. To minimize this effect, our modeling process involved the following two stages.

1. **Independent modeling**: In this stage, all the authors of this paper independently modeled all the attacks from our sample using Bhadra. While doing so, we first understood the attack and mapped their steps to the tactical objective as per Bhadra. We then tried to select at least one technique. Nevertheless, in some cases, depending on the details available about the attack, we had to select either all applicable techniques or none based on our reasoning.
2. **Discussion**: All the authors participated in a discussion where we jointly reviewed the attacks from our sample. Here, when conflicts were found (e.g., mismatch of techniques), we discussed until all the authors were convinced about the techniques applicable to the attack for final analysis. We found that such discussions helped us improve the reliability of our results as they collectively utilized the independent expertise of each author and compensated for the lack of details (if any) about a specific attack.

3.3 Graph Analysis

Our goal from graph analysis is to discover common attack patterns, importance, and diversity of techniques from our modeled attacks. After reviewing different methods, we chose graph algorithms because they had readily available algorithms that matched goals. We explain them in detail as follows. We used Python `Networkx` [12] package for our graph analysis.

Common Subpaths—Association of Techniques. We derived common subpaths (as an attack pattern) among the attack models to understand how the techniques are associated with each other. Networkx does not contain any readily available function to calculate common subpaths among paths. Hence, we wrote a simple python script to find common subpaths containing three to five nodes.

Connectivity—Importance of Techniques. Researchers have used graph connectivity to measure the communication network survivability [7]. We associate the similar idea to quantify the importance of a technique with the loss of average node connectivity after removing all the edges to and from the individual node. The more average connectivity loss, the lower the possibility an attacker would successfully finish all the tactics to finish his final goal covered in the impact tactical category.

Following the definition [2], we calculate average node connectivity $\bar{K}$ of a graph G as the average of local node connectivity over all pairs of nodes of G:

$$\bar{K}(G) = \frac{\sum_{u,v} K_G(u,v)}{\binom{n}{2}} \tag{1}$$

where $K_G(u,v)$, the local node connectivity for two non-adjacent nodes u and v, is the minimum number of nodes to be removed to disconnect the two nodes.

Unique Paths—Diversity of Attack Techniques. The number of unique paths to reach a certain goal has been used to infer the diversity of attack methods an attacker can choose [18]. We are particularly interested in visualizing the diversity of attack methods from a particular initial access point to a specific impact. Therefore, we calculate the number of simple paths between two nodes [38] given the attack graph built from our attack models using the built-in function in `NetworkX` [26].

4 Results

This section presents the graph analysis results based on the 60 attack models. We constructed an attack graph (as shown in Fig. 3) with the Python `Networkx` package.

Each node represents a technique, and each edge represents the connection of adjacent techniques used in the same attack. The thickness of each edge represents its weight, meaning how many times two nodes are connected in the attack models. We calculated and presented the weight in and out of a technique node in the figure. Also, each node is color-coded based on the number of unique connections where the node links next.

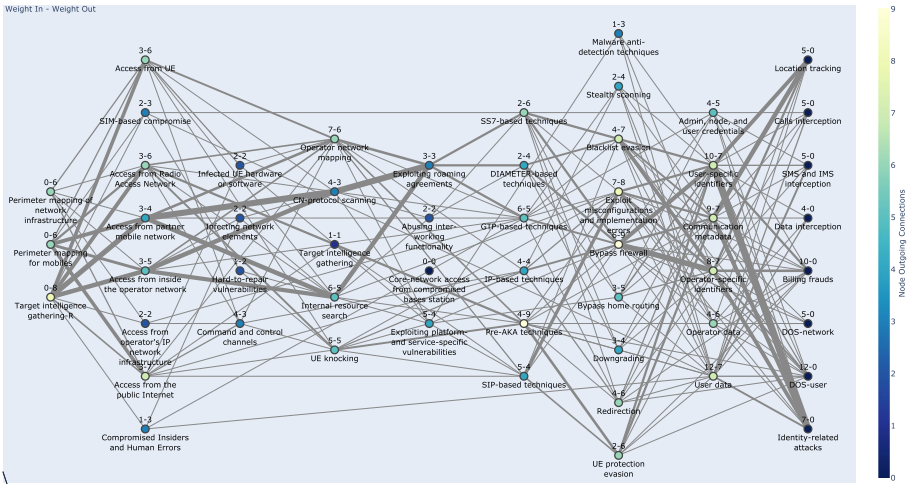

Fig. 3. Attack graph of the 60 modeled attacks

Strategy 1: By visualizing basic graph analysis results, a security analyst can identify the strong association of techniques and the highly connected nodes as an information source to prioritize their defense. In Fig. 3, thickest edges represent the strong association of techniques. Similarly, the node with the highest value for the (weight-in, weight-out) pair represents the highly connected nodes.

If Fig. 3 is treated like a real-life scenario of visualization of attacks observed on an operator's network, the operator's goal is to build defense strategies such that it either eliminate or reduce the thickest edges or reduce the (weight-in, weight-out) of the highly connected nodes.

We now highlight some insights derived from other results and explain the reason behind them with examples from the collected attack scenarios. Similar to the above example, we first describe our observation and then present a potential defense strategy.

4.1 Common Attack Patterns

Table 1 shows the common sub-paths of the modelled attacks. We observed a strong association of techniques that are used before and after exploiting roaming agreements. For example, attackers often use internal resource search or CN-protocol scanning in the discovery phase to gain information on the target network nodes. After initial access and discovery, attackers often misuse GTP, Diameter, and SS7 protocols and send crafted messages to exploit their target.

Since the attackers are connected to the target network through an interconnection network or spoof as a partner network node, they can easily bypass the firewall and evade blacklisting to reach their target. It is worth noting that the initial access point and impact are not highly associated since an attacker can access the roaming network using different techniques. Also, these core network attacks can target more broad attack surfaces and lead to various types of impact.

Another such association is the techniques used in attacks originated from the radio access network. In these attack scenarios, threat intelligence gathering is often required in the reconnaissance phase. Attackers need to gain some knowledge on the target UE (e.g., which operator it subscribes to) and its operators' network characteristics to find some operator-specific vulnerabilities, such as GUTI allocation mechanism [16].

Moreover, in LTE, signal strength is not the only factor in tricking UE to connect to the BS. An attacker might need to perform operator network mapping by, for example, listening to the base station broadcast message that includes frequency priority to adjust the fake BS configuration [25]. After the target UEs connect to the fake BS, an attacker often use the UE knocking technique that triggers the paging message by silent calls and messages to identify the location of a subscriber or spoof other paging message content and metadata. As we observed, Pre-AKA protocols are usually misused in radio attacks. For example, an attacker can send an identity request to the target UE to get the IMSI that links to identity-related attacks and location tracking. Besides, an attacker can also craft the RRC connection message or trigger NAS Detach Procedure to achieve denial of service or downgrading.

We observe some strong association in the attack patterns. Note that the distribution of the technique selection may not represent the actual number of incidents seen in the wild since we only modeled publicly available attack scenarios mostly from academic publications. Nevertheless, these associations can help prioritize defense deployment.

Strategy 2: Exploiting roaming agreements can be seen as a bottleneck that, if succeeded, could lead to a broader attack surface that allows an attacker to exploit signaling protocols such SS7, Diameter, or GTP. These protocols that do not have a secure mechanism to verify the sender and attacker can impersonate a benign roaming partner.

In this case, the operator's strategy would be to deploy the edge agents (if not already deployed) and impose strict policies for any traffic coming from the interconnection network for filtering the message content [13,32]. Authenticating the benign roaming partners would be another possible strategy if the operators can run a public-key infrastructure.

Table 1. Common subpaths

# of nodes	Count	Path
3	6	(Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	5	(Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques)
	5	(Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking)
	4	(Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	4	(UE knocking, Pre-AKA techniques, UE protection evasion)
	4	(Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques)
	4	(Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	4	(Access from Radio Access Network, Operator network mapping, Pre-AKA techniques)
4	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	3	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	3	(Internal resource search, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	3	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
5	2	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Location tracking)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Identity-related attacks)
	2	(Target intelligence gathering-R, Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Redirection)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
	2	(Target intelligence gathering-R, Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Exploit misconfigurations and implementation errors)

4.2 Loss of Connectivity

Figure 4 shows the loss of average connectivity after removing edges to and from a particular technique node. As shown in the figure, operator network mapping and internal resource research, the two most commonly used discovery techniques, have a significantly higher percentage in loss of connectivity than the rest. Our prior network analysis experience confirms that operator network mapping and internal resource techniques are commonly observed. These techniques help the attackers learn information about the target node, such as IP address and open port. The attacker then effectively uses them in the later stages of an attack, such as lateral movement techniques.

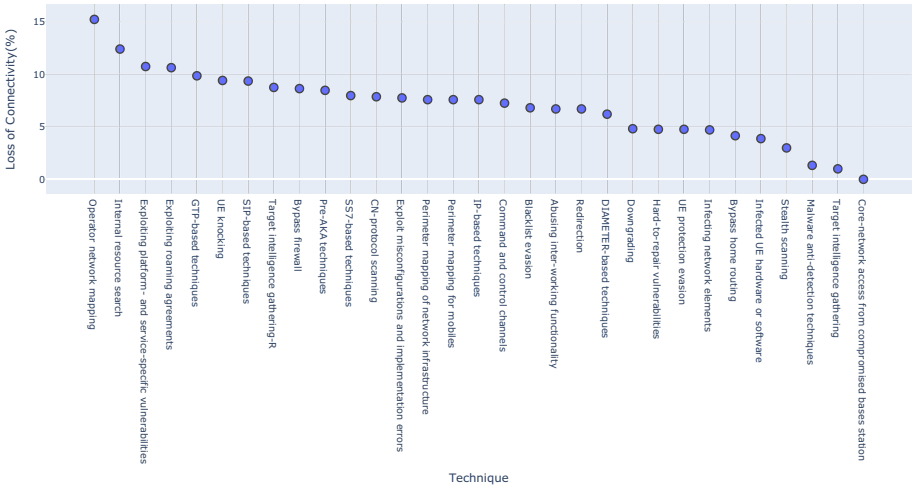

Fig. 4. Loss of connectivity after removing edges to and from individual technique

On the other end, malware and anti-detection techniques, target intelligence gathering in the discovery phase, and core-network access from the compromised base station are the ones with the most negligible loss of connectivity. This result is also consistent with the impression we got from our reviewing and attack modeling process since not many publicly available attacks that gain access to core networks through compromised based stations or perform malware anti-detection techniques were found, and target intelligence sharing is primarily already used in the reconnaissance phase.

Strategy 3: An operator can use the loss of connectivity result to prioritize the defense against those techniques that are more important to attackers. In Fig. 4, the most important technique would be "operator network mapping". So, the operator has to deploy defense mechanisms that hinder the attackers from mapping their network, or at worst case, alerts them if any network-wide mapping activity is observed. It could also imply that the operators audit their network regularly, for example, to close any ports that are left open.

4.3 Unique Paths

Figure 5 shows the result from the unique paths calculation. From the initial access dimension, we found that attacks from UE, radio access networks, inside the operator network, and public Internet have more diverse paths to reach the target impacts. The result is predictable as we did not find many attacks involving compromised insiders and human errors, access from operators' IP network infrastructure, and SIM-based compromise.

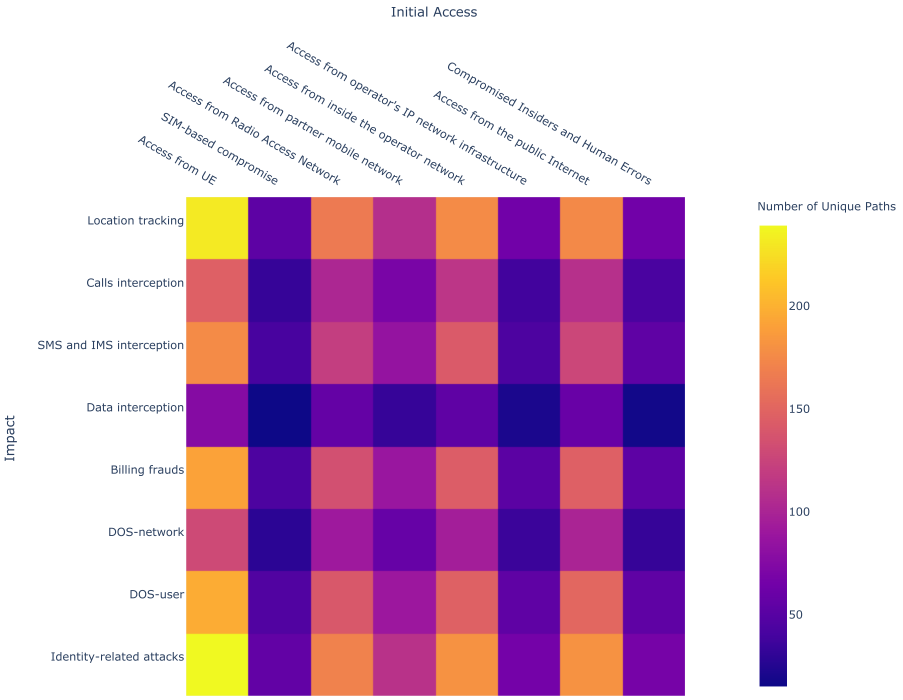

Fig. 5. Number of unique paths from initial access to impact

From the impact dimension, there are more unique paths to reach location tracking, SMS and IMS interception, billing frauds, DOS-user, and identify-related attacks. We can interpret that these impacts are relatively easy to achieve than call or data interception since call interception is only possible in lower generation (e.g., 2G) where the communication is not required to be encrypted.

Strategy 4: From the result of the unique path, the operator can prioritize their defense effort in two ways. One is to evaluate from the attackers' point of view, based on the potential threat actors' capability to gain initial access and their final target impacts. Another is to analyze the operator's own system to identify the weakest points in the network that an attacker might gain access to and the most impacted assets. Once focused on specific initial access or impact combination, the operator can investigate each unique path and strengthen their defense.

5 Discussion

Our results demonstrate potential uses of the framework—to form defense strategies or prioritize threats—by providing insight on the attack patterns, diversity of attack paths given an attacker's ability or target impact, and the importance of techniques from a network graph viewpoint. It is important to note that the analysis presented in this work does not provide any insight into the expected adversarial trends in 5G. On the one hand, this limitation comes from Bhadra's taxonomy that covers only 2G, 3G, and 4G mobile networks. On the other hand, since most public 5G attacks are still theoretical, we decided to limit our analysis strictly to only practical attacks while creating our sample. Nevertheless, with a taxonomy covering the 5G attack surface, similar analysis as shown in this work could potentially help uncover new attack patterns. We aim to explore it in our future work.

We sampled publicly available literature to collect various types of attacks that are indicative of an operator's network premises because there is hardly any information on the attacks observed in the wild. Hence, we could only present mostly high-level results that may seem trivial to readers with strong mobile network backgrounds. Nevertheless, while analyzing real-world attacks, the operators would have access to intrinsic details of the security incidents (e.g., in the form of network logs and configuration settings of their nodes). We argue that applying the methodology presented in our work in such cases would provide more in-depth insights. Similarly, adding more sub-techniques to Bhadra would help add more details while modeling, offering potentially concrete insights.

Furthermore, we had to make assumptions either about missing techniques or about specific details of attack procedures. In particular, we model reconnaissance, discovery, and defense evasion tactics with assumptions based on our domain expertise due to the lack of descriptions about the actual procedure in the sources we referred to. Our sources from the attack collections are mostly

experiments conducted in academic lab setup or high-level reports on observed attacks in the wild. We missed knowing how exactly an attacker would perform reconnaissance, discovery, and defense evasion in either case. Therefore, we admit that some of our results may be skewed. For instance, even though operator network mapping and internal resource search are the two highest in terms of connectivity loss, they may not be representative of real-world scenarios.

The lack of real-world attack data of the mobile communication networks is a major barrier for academic research. Although sometimes the attacks and lessons learned from defending them are discussed in 3GPP and GSMA meetings, operators rarely share any specific data about attack incidents, even among themselves. One of the reasons for the hesitance to openly discuss security issues could be that operators seem to believe that any such discussions would affect their business and reputation. Nevertheless, we argue that sharing information about security incidents and learning from each other's failures could be beneficial. In this direction, Bhadra would provide a suitable abstraction for sharing threat- or attack-related incidents. We urge that the operators utilize such abstractions, apply a similar analysis as shown in this work, and release it in the public domain to inculcate future research efforts.

6 Conclusion

Our work demonstrated that a conceptual framework like Bhadra establishes a common taxonomy to describe adversarial behaviors and provides valuable insights when combined with analysis methodologies to find relations between different attacks. In particular, our work provides high-level insights into the adversarial trends in mobile communication systems. Using Bhadra, we model 60 attacks that are carefully chosen as a representative sample of different kinds of attacks on the mobile network. We analyze the modeled attacks using graph analysis techniques to understand the importance of the techniques to attackers, the diversity of attack paths an attacker can choose, and the common attack patterns. We also discuss how these insights on different adversarial trends can help the operators prioritize defense strategies. We demonstrated the potential of Bhadra for analyzing the security posture of an operator's network and explored how Bhadra can help simplify the complexity of mobile network security for security communication (such as threat intelligence sharing). Given the initial results and the potential use of the analysis presented in this work, we hope future research efforts can extend a similar study on a large scale and include more diverse attacks (e.g., 5G). Also, we hope our work initiates wider adoption of Bhadra and more collaboration on threat intelligence sharing.

Acknowledgement. The authors would like to thank Professor Tuomas Aura for providing constructive feedback and Nokia Bell Labs for funding the research work.

Appendix

Table 2. Attacks collected from different sources for modeling

Title	Attack name (as per the source)
Billing Attacks on SIP-Based VoIP System [47]	– SIP-based VoIP Billing Attack
Survey of network security systems to counter SIP-based denial-of-service attacks [8]	– SIP message payload tempering – SIP message flooding – SIP message flow Tempering
Mobile data charging: new attacks and countermeasures [27]	– Toll-free data access attack – Stealth Spam Attack in UDP-based Services - VoIP – Stealth Spam Attack with Malicious Link Connection
SIM cards are prone to remote hacking [22]	– Remote SIM hacking
Unveiling the hidden dangers of public IP addresses in 4G/LTE cellular data networks [23]	– Data Quota Drain – Battery Drain
Gaining control of cellular traffic accounting by spurious TCP retransmission [11]	– TCP retransmission attacks - Usage Inflation – TCP retransmission attacks - Free riding
On Her Majesty's Secret Service: GRX & A Spy Agency [34]	– GTP Data Session Hijacking
Analysis and mitigation of recent attacks on mobile communication backend [29]	– Location disclosure using call setup messages
LTE and IMSI catcher myths [3]	– Simple IMSI Catcher
Unblocking stolen mobile devices using SS7-MAP vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access [31]	– Unblocking stolen mobile devices using SS7-MAP
Breaking and fixing volte: Exploiting hidden data channels and mis-implementations [20]	– VoLTE Mis-implementation: Permission model mismatch – VoLTE Mis-implementation: Direct Communication in P-GW
Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege [19]	– Illegitimate Surveillance
User location tracking attacks for LTE networks using the interworking functionality [15]	– IMSI catcher with interworking functions – Location disclosure using CAMEL messages
New security threats caused by IMS-based SMS service in 4G LTE networks [42]	– IMS-based SMS - Silent SMS abuse – IMS-based SMS - client DoS – IMS-based SMS - SMS spoofing – IMS-based SMS - SMS spamming towards IMS
Subscriber profile extraction and modification via diameter interconnection [13]	– Extraction and Modification of Subscriber Profile
Diameter Security: An Auditor's Viewpoint [24]	– DoS on subscriber via S6a messages – Location tracking via Sh User-Data-Request
Threats to packet core security of 4G networks [40]	– EPC Tunnel Endpoint Identifier Thief – GTP-based IMSI catcher – GTP-based billing evasion - Create session Request – Exploit Charging Gateway Function – Connection Hijacking with GTP messages – GTP-based DoS attack on subscribers – GTP-based DoS attack on the operator's equipment – Control packets inside a user tunnel: GTP-in-GTP
SMS and one-time-password interception in LTE networks [14]	– Diameter-based SMS Interception
GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier [16]	– Location Tracking Attack on VoLTE User – Smart Tracking Attack
How Criminals Recruit Telecom Employees to Help Them Hijack SIM Cards [10]	– SIM Swap Attack
LTEInspector: A systematic approach for adversarial testing of 4G LTE [17]	– 4G LTE Paging Channel Hijacking – 4G LTE Authentication Relay Attack
Touching the untouchables: Dynamic security analysis of the LTE control plane [21]	– BTS resource depletion attack – Blind DoS attack
Understanding How IMSI- Catchers Exploit Cell Networks [25]	– IMSI Catcher - Communication Interception – Basic Location Area Test – Smart Paging Test – Active GPS location tracking – TAU Reject - Communication Interception – TAU Reject - DoS
Breaking LTE on layer two [35]	– LTE User Data Manipulation Attack – Passive Layer 2 Attack - Identity Mapping Attack
MESSAGETAP: Whofis Reading Your Text Messages? [33]	– MessageTap
LTE security disabled: misconfiguration in commercial networks [5]	– Impersonation Attack based on Misconfiguration
LTE Phone Number Catcher: A Practical Attack against Mobile Privacy [45]	– LTE Phone Number Catcher
Hidden Agendas: bypassing GSMA recommendations on SS7 networks [28]	– SS7 - Use ACN for illegitimate component – SS7 - Modify user profile with InsertSubscriberData Message – SS7 - Operation Cod Tag Misuse
Simjacker - Next Generation Spying Over Mobile [37]	– SimJacker
IMP4GT: IMPersonation Attacks in 4G NeTworks [36]	– IMPersonation Attacks in 4G Networks

References

1. Al-Shaer, R., Spring, J.M., Christou, E.: Learning the associations of MITRE ATT&CK adversarial techniques. In: 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1–9. IEEE (2020)
2. Beineke, L.W., Oellermann, O.R., Pippert, R.E.: The average connectivity of a graph. Discret. Math. **252**(1–3), 31–45 (2002)
3. Borgaonkar, R., Shaik, A., Asokan, N., Niemi, V., Seifert, J.-P.: LTE and IMSI catcher myths. BlackHat Europe (2015)
4. Chen, H.-Y.: Domain-specific threat modeling for mobile communication systems. Master's thesis, Department of Computer Science and Engineering, Aalto University School of Science and Technology, Espoo, Finland (2021)
5. Chlosta, M., Rupprecht, D., Holz, T., Pöpper, C.: LTE security disabled: misconfiguration in commercial networks. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 261–266. ACM (2019)
6. The MITRE Corporation. The MITRE ATT&CK. https://attack.mitre.org/
7. Duque-Anton, M., Bruyaux, F., Semal, P.: Measuring the survivability of a network: connectivity and rest-connectivity. Eur. Trans. Telecommun. **11**(2), 149–159 (2000)
8. Ehlert, S., Geneiatakis, D., Magedanz, T.: Survey of network security systems to counter SIP-based denial-of-service attacks. Comput. Secur. **29**(2), 225–243 (2010)
9. Forsberg, D., Horn, G., Moeller, W.-D., Niemi, V.: LTE Security. Wiley, Chichester (2012)
10. Franceschi-Bicchierai, L.: How criminals recruit telecom employees to help them hijack SIM cards (2018). https://www.vice.com/en/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam. Accessed 25 Apr 2021
11. Go, Y., Jeong, E., Won, J., Kim, Y., Kune, D.F., Park, K.: Gaining control of cellular traffic accounting by spurious TCP retransmission. In: NDSS. Internet Society (2014)
12. Hagberg, A., Swart, P., Chult, D.S.: Exploring network structure, dynamics, and function using NetworkX. Technical report, Los Alamos National Lab. (LANL), Los Alamos, NM (United States) (2008)
13. Holtmanns, S., Miche, Y., Oliver, I.: Subscriber profile extraction and modification via diameter interconnection. In: Yan, Z., Molva, R., Mazurczyk, W., Kantola, R. (eds.) NSS 2017. LNCS, vol. 10394, pp. 585–594. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64701-2_45
14. Holtmanns, S., Oliver, I.: SMS and one-time-password interception in LTE networks. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2017)
15. Holtmanns, S., Rao, S.P., Oliver, I.: User location tracking attacks for LTE networks using the interworking functionality. In: 2016 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 315–322. IEEE (2016)
16. Hong, B., Bae, S., Kim, Y.: GUTI reallocation demystified: cellular location tracking with changing temporary identifier. In: NDSS. Internet Society (2018)
17. Hussain, S., Chowdhury, O., Mehnaz, S., Bertino, E.: LTEInspector: a systematic approach for adversarial testing of 4G LTE. In: NDSS. Internet Society (2018)
18. Idika, N., Bhargava, B.: Extending attack graph-based security metrics and aggregating their application. IEEE Trans. Dependable Secure Comput. **9**(1), 75–85 (2010)

19. The Intercept: Massive hack of 70 million prisoner phone calls indicates violations of attorney-client privilege (2015). https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/. Accessed 25 Apr 2021
20. Kim, H., et al.: 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 (2015)
21. Kim, H., Lee, J., Lee, E., Kim, Y.: Touching the untouchables: dynamic security analysis of the LTE control plane. In: 2019 IEEE Symposium on Security and Privacy (SP), pp. 1153–1168. IEEE (2019)
22. Security Research Labs: SIM cards are prone to remote hacking. https://srlabs.de/bites/rooting-sim-cards/. Accessed 17 June 2021
23. Leong, W.K., Kulkarni, A., Xu, Y., Leong, B.: 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 (2014)
24. Mashukov, S.: Diameter security: an auditor's viewpoint. J. ICT Stand. **5**(1), 53–68 (2017)
25. Nasser, Y.: Gotta Catch ′Em All: Understanding How IMSI-Catchers Exploit Cell Networks. White paper, Electronic Frontier Foundation (2019). https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf
26. NetworkX: Network Analysis in Python. A generator that produces lists of simple paths (2019). https://networkx.org/documentation/stable/reference/algorithms/generated/networkx.algorithms.simple_paths.all_simple_edge_paths.html. Accessed 25 Sept 2021
27. Peng, C., Li, C., Tu, G., Lu, So., Zhang, L.: Mobile data charging: new attacks and countermeasures. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 195–204 (2012)
28. Puzankov, K.: Hidden agendas: bypassing GSMA recommendations on SS7 networks. In: Hack in the Box Conference (2019)
29. Rao, S.P.: Analysis and mitigation of recent attacks on mobile communication backend. Master's thesis, Department of Computer Science and Engineering, Aalto University School of Science and Technology, Espoo, Finland (2015)
30. Rao, S.P., Holtmanns, S., Aura, T.: Threat modeling framework for mobile communication systems. arXiv preprint arXiv:2005.05110 (2020)
31. Rao, S.P., Holtmanns, S., Oliver, I., Aura, T.: 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, pp. 1171–1176. IEEE (2015)
32. Rao, S.P., Kotte, B.T., Holtmanns, S.: Privacy in LTE networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, pp. 176–183 (2016)
33. Leong, D.P.R., Dean, T.: MESSAGETAP: Who's Reading Your Text Messages? (2019). https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html. Accessed 25 Apr 2021
34. Corelan Cybersecurity Research: On Her Majesty's Secret Service: GRX & A Spy Agency. https://www.corelan.be/index.php/2014/05/30/hitb2014ams-day-2-on-her-majestys-secret-service-grx-a-spy-agency/. Accessed 25 Apr 2021
35. Rupprecht, D., Kohls, K., Holz, T., Pöpper, C.: Breaking LTE on layer two. In: 2019 IEEE Symposium on Security and Privacy (SP), pp. 1121–1136. IEEE (2019)

36. Rupprecht, D., Kohls, K., Holz, T., Pöpper, C.: IMP4GT: impersonation attacks in 4G networks. In: Symposium on Network and Distributed System Security (NDSS). ISOC (2020)
37. AdaptiveMobile Security: New Simjacker vulnerability exploited by surveillance companies for espionage operation (2019). https://simjacker.com/. https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile. Accessed 25 Apr 2021
38. Sedgewick, R.: Algorithms in C, Part 5: Graph Algorithms. Pearson Education, Boston (2001)
39. Shostack, A.: Experiences threat modeling at microsoft. MODSEC@ MoDELS (2008)
40. Positive Technologies: Threats to Packet Core Security of 4G Network. White paper, GSMA (2017)
41. Positive Technologies: Threat vector: GTP (2020). https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf. Accessed 24 May 2021
42. Tu, G.-H., Li, C.-Y., Peng, C., Li, Y., Lu, S.: 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 (2016)
43. Welch, B.: Exploiting the weaknesses of SS7. Netw. Secur. **2017**(1), 17–19 (2017)
44. Xiong, W., Legrand, E., Åberg, O., Lagerström, R.: Cyber security threat modeling based on the Mitre enterprise ATT&ACK matrix. Softw. Syst. Model., 1–21 (2021)
45. Yu, C., Chen, S., Cai, Z.: LTE phone number catcher: a practical attack against mobile privacy. Secur. Commun. Netw. **2019** (2019)
46. Zeng, J., Shuang, W., Chen, Y., Zeng, R., Chengrong, W.: Survey of attack graph analysis methods from the perspective of data and knowledge processing. Secur. Commun. Netw. **2019** (2019)
47. Zhang, R., Wang, X., Yang, X., Jiang, X.: Billing attacks on SIP-based VoIP systems. WOOT **7**, 1–8 (2007)