

Implementation of a Malicious Traffic Filter Using Snort and Wireshark as a Proof of Concept to Enhance Mobile Network Security

Rafia Afzal and Raja Kumar Murugesan

School of Computer Science and Engineering, Taylor's University, Malaysia

<https://doi.org/10.26636/jtit.2022.155821>

Abstract—In the 1970s, roaming interconnections for cellular networks were designed for a few trusted parties. Hence, security was not a major concern. Today, the SS7 (Signaling System no. 7) solution that is several decades old is still used for many roaming interconnections. SS7 has been proven vulnerable to serious threats due to deregulation, expansion, and convergence with IP-based Long Term Evolution (LTE) networks. The limitations of the SS7 network that it is unable to check the subscriber's authentic location, verify their identity and filter illegitimate messages, makes the system vulnerable to attacks. Adversaries taking advantage of these shortcomings can inflict threats such as interception of calls and text messages, subscriber tracking and denial of service attacks. Although LTE and Diameter signaling protocols promise enhanced security keeping up with the latest attack vectors, their inherent flaws related to roaming interconnections are still there and continue to make the networks vulnerable. Hence, a highly secure signaling network is required to protect the operators and the subscribers from a diverse range of security attacks. SS7 network protocol layers, such as signaling connection control part (SCCP), transaction capabilities application part (TCAP), and global system for mobile Communications – mobile application part (GSM MAP), manage connectivity between networks and subscribers. An analysis of the parameters of these layers may provide a clear insight into any anomalies present. Unfortunately, these parameters are not validated and verified at the network's edge. The major contribution of this research is a methodology for detecting anomalies by checking malformed parameters and intra-layer parameter discrepancies at the abovementioned protocol layers. This paper provides an insight into the severity of SS7 network security vulnerabilities. Furthermore, it provides a proof of concept for the analysis of SS7 network traffic using the Wireshark packet capture tool and the Snort intrusion detection system (IDS) capable of detecting malicious traffic patterns.

Keywords—mobile network, signaling network security, SS7.

1. Introduction

In telecommunication networks, a signaling system is used to manage call set-up and termination processes in order

to connect and manage both ends. SS7 was designed five decades ago, in the 1970s, when only a few operators were providing telecommunication services and had access to the core network [1]. Since then, SS7 has been used for call establishment/termination, mobility management, user security information, billing information, and access/service authorization [2]. As it was considered that mutual trust existed between operators, no inherent security controls were incorporated in the SS7 core network. Operators being national or multinational corporations were assumed to be trustworthy, making the SS7 network a walled garden [3], [4]. The merger of packet-switched IP networks and circuit-switched telephone networks attracted more subscribers, resulting in an increase level of competition and in the expansion of coverage, thus creating high demand and allowing new competitors to enter the market. The number of core network entry points increased due to the introduction of new technologies and interfaces with the legacy SS7 network, boosting the number of operators accessing the system [5].

Network exposure results from the design and the architecture of the solution that needs to support the roaming of peers, making the system vulnerable to attacks. Vulnerabilities faced by users may be grouped into five major categories: obtaining information on the subscriber's location, spying or snooping, monetary mugging, account fraud, and interruption and denial of service [3]. Liberalization of the telecommunications domain and shifting to IP based communications exposed SS7 to severe threats, such as interference between calls and text messages, tracking the location of subscribers, deception/spamming, denial of service, and subscriber account frauds [6]. Several commercial signaling firewalls are currently available and much effort has been taken by the Global System for Mobile Association (GSMA) to mitigate such attacks. However, the commercial firewalls are not fully secure, as they focus solely on home public land mobile network level protection to mitigate the risks faced. They are still not adequate and are hardly accepted by telcos, since there are several ways in which the security measures may be evaded. This issue arises mainly

because of the lack of protection while the subscribers are roaming, and due to the possibility of spoofing messages in the SS7 signaling connection control part (SCCP) and in the Diameter protocols. Taking into consideration the fact that present defensive procedures, such as the use of firewalls, filtering and blacklisting, regrettably are not capable of ensuring satisfactory levels of safety for SS7 [4], a rule-based intrusion detection system has been proposed. In this research, the proof of concept for the rule-based intrusion detection system is provided to demonstrate that it improves detection accuracy and reduces the false alarm rate.

This paper is organized into the following sections. Section 2 highlights the causes of security vulnerabilities affecting the SS7 network. Section 3 presents the proof of concept for the rule-based intrusion detection system, and Section 4 concludes the paper and specifies future directions.

2. Related Work

2.1. Causes that Lead to SS7 Network Vulnerability

SS7 firewalls are currently breached and exposed to a wide range of vulnerabilities and threats that jeopardize the security of the telecommunications networks. Liberalization of the telecommunications sector has resulted in relaxation of the rules and regulations that are applied to manage the SS7 network. The deregulation has resulted in the SS7 network being more easily accessible to network providers and users alike.

In the early twenty-first century, a series of signaling transport protocols, known as SIGTRAN, was established to meet the new requirements for mobile connections and to support the emerging services. SIGTRAN is an SS7 extension that enables messages to be transmitted over IP networks. Because of this advancement, the signaling network is no longer isolated. Many entry points to the network were formed due to attempts to integrate the SS7 network with other solutions, for interoperability purposes. The emergence of numerous entry points to the SS7 network has become a major source of weakness. This helps attackers write, intercept and change SS7 posts via multiple mobile network and subscriber attacks [1], [2].

2.2. How Vulnerable is the SS7 Network?

Stealthy attacks made possible by the vulnerabilities of the SS7 system are discussed by Puzankov [7]. He feared that due to misconfiguration errors, SMS home routing may be by-passed and the IMSI of the subscriber may be disclosed, thus helping in the launch of further sophisticated security attacks. In his study, he also examines how an intruder can connect using a bogus MSC, while VLR remains legal. Although genuine MSC is used for voice calls and short messages, fake MSC will be used to intercept incoming messages [7]. In their research, Savadatti and Sharma explain signaling system no. 7 with a brief discussion of

SS7 attacks [8]. Holtmanns demonstrates that SS7 vulnerabilities endanger LTE users as well as GSM/UMTS subscribers. Because of their internet-working capabilities, the attacker can monitor LTE subscribers through the Diameter protocol, taking advantage of SS7 vulnerabilities [9]. In [10], Jensen gave a summary of SS7 attacks, including a section on entry points to the SS7 core network. Such attacks relied on the use of machine learning algorithms to detect SS7 attacks. His most significant contribution to SS7 research was the development of an open-source simulator called “SS7 Attack Simulator” that generates simulated SS7 regular and abnormal traffic.

Similarly, experts at Positive Security explained the entry points to SS7 and explained or demonstrated some attack plots [2]. A white paper released by the SANS Institute gives an insight into potential SS7 attacks. It also proposes how essential security monitoring may be deployed to secure the SS7 network more effectively [2]. Exploiting MAP messages can lead to several security attacks and research done by Rao *et al.* explains the methods relied upon to accomplish such attacks [11]. In another research, Rao *et al.* demonstrate SS7 location tracking attacks exposing vulnerabilities linked to the network’s entry points. They also provide recommendations on how to secure such entry points [12]. Engel gave a live demonstration of location monitoring and DoS attacks at the Chaos Communication Congress. He also described a wide range of other attacks [13]. Karsten Nohl from Security Research Labs showed how access to the SS7 network makes the calls and SMS interceptions possible, at the Chaos Communication Congress mentioned in [14]. At the Hackito Ergo Summit, security experts from P1 labs demonstrated user location tracking and showed how spoofed messages may be used as a security exploit [15].

Keeping in view the current cyber threat environment and the known SS7 vulnerabilities, further studies on this topic are needed to help protect the public’s privacy and to ensure personal protection. Attackers may cause billions in losses suffered by network operators. Hence, it is equally important for operators to help close these gaps in the fence of what once used to be a “walled garden”. It is the need of the hour to gear up against signaling vulnerabilities by understanding the major attacks that were recently carried out using these exploits, and by grasping their severity. This would help us develop methods to safeguard mobile networks from adversaries before any catastrophic security attacks take place.

3. Proposed Proof of Concept

3.1. Intrusion Detection Systems

A software system that detects malicious activities and behaviors is known as the Intrusion Detection System (IDS). An IDS usually detects data-driven attacks against applications, network-based attacks on vulnerable services, attacks against hosts, such as unauthorized logins, privilege escalation, and access to sensitive data files.

3.1.1. Types of Intrusion Detection Systems

Intrusion detection relies on two fundamental techniques, namely anomaly detection and signature detection. In the former method, the normal working conditions or the standard profile of a system is defined, meaning that any deviations from that profile may be detected [16]. In other words, the desired action is defined, and unwanted or undesired behaviors are identified using this technique. Stored data sets and behaviors are two different things. In the case of stored data, a single bit altered may be detected easily, whereas differentiating anomalous behaviors from those that are acceptable is not an easy task [16]. The method relying on characterizing the known ways of penetrating a system is called misuse detection and constitutes another approach to intrusion detection. These known ways are termed patterns. Unambiguous patterns are monitored by a misuse detection system. Patterns may vary from a static bit string to a suspected set of actions. Although both techniques have their advantages, some systems rely on both of these approaches, taking advantage of a hybrid intrusion detection system.

3.1.2. Anomaly-Based Detection

Anomaly-based detection is also well-known as statistical or profile-based intrusion detection. In this approach, a “regularity” is defined and any irregular or abnormal traffic deviating from that regularity profile is declared as intrusive [17]. Whatever differs from the normal profile can be comfortably considered as intrusive. Classifying a normal activity as intrusive or abnormal is considered false positive, whereas classification of an abnormal activity as normal is known as false negative. False negative identifications are considered more harmful than their false positive counterparts, as they involve a failure to detect harmful activities. What makes anomaly-based intrusion detection systems hard to implement is the requirement of not only complying with protocols and understanding the inner workings of an application, but also added with expert level users with their preferences, and date and time [17]. Anomaly-based IDS requires computationally intensive behavioral models for construction and tuning [18].

3.1.3. Snort-IDS

Snort is one of the most famous, free, and well-known open-source network IDS solutions. It utilizes a rule-based language combined with signature, protocol, and anomaly verification techniques to detect malicious activities, such as denial of service (DOS) attacks and stealth port scan attacks. The best thing about the program is the flexibility of its rule language. It is also suitable for writing rules concerning new attacks, meaning that the creation of new rules is reasonably simple. Rules are the major entities on which Snort relies to differentiate between regular Internet activities and malicious behaviors. In comparison with Wireshark, the program lacks a good GUI and is terminal-based.

3.2. Packet Sniffing and Analysis using Wireshark

Wireshark is a network packet analyzer. It has the form of data capturing software that understands the abstraction (structure) of different networking protocols. It captures live packet data from a network interface, or from a file of the packets already collected. It can parse and view fields and their definitions defined by various networking protocols. Data from various types of networks can be read in real-time and stored for later use. The program can export some or all the packets in many file formats available. It helps search the saved packets based on numerous criteria. The GUI version or terminal (command line) version of the utility, TShark, can be used to search the network data captured. A display filter may help refine the captured data. Wireshark is capable of color marking the code packets displayed, based on filters. It also helps create various statistics. Filtering wireless connections is also possible if they move through the controlled Ethernet network. Other options, such as timers and filters, may be used to aid in the filtering of output traffic.

3.3. SS7 Attack Simulation

Due to privacy and ethical considerations, using real SS7 network data is not plausible. As such, a simulation setup was realized using the open-source SS7 Attack Simulator [10] to produce the required data set that reflects a practical scenario of an SS7 network in operation. This tool can be used to produce both normal and attack traffic to study SS7 security vulnerabilities. Network traffic is created using MAP in the SS7 stack, according to 3GPP-defined MAP technical specifications.

The simulator generates both normal and anomalous traffic that is used to detect abnormalities. Three network operators, namely A, B and C, are built using the SS7 network simulator’s complex mode. The first network operator (A) is a victim, the second network operator (B) is a roaming network, and the third network operator (C) is an adversary. These operators communicate with one another through thirteen common messages. In addition to the usual communications, call/SMS intercept and location tracking attacks are carried out using anyTimeInterrogation (ATI), sendRoutingInfo (SRI) (-SM, -LCS) and ProvideSubscriberInfo (PSI). An attacker who is a subscriber of network operator C will imitate the attacks.

In this research, the two most debated and critical attacks, namely location tracking and interception attacks [2], are simulated. To demonstrate these attacks, one type of a message request from each category of SS7 MAP messages has been selected. Home network messages are categorized as category 1, inbound roamers’ messages as category 2, and outbound roamers’ messages as category 3. An ATI from category 1 was selected, as it could only be used within the home network. Similarly, a PSI message could only be sent by the home location register (HLR) to the current visitor location register (VLR). However, the attacker can bypass the HLR and can send this PSI message request di-

rectly to VLR through its MSC/VLR. In order to do this, the attacker needs to have international mobile subscriber identity (IMSI) and current VLR address information of the target. Therefore, the attacker performs another attack by sending SRI-SM to HLR which sends, without verifying and validating the requires, all crucial information to the attacker. This SRI-SM message request is a category 3 message and needs to be verified and validated at network borders or edges. An SRI-SM message request can also be used for other types of attacks, such as SMS interception attacks. The selected attack messages are marked in bold in Table 1.

Table 1
SS7 MAP messages with attack types

Category	Message	Attack
1	provideSubscriber Location (PSL)	Tracking
1	anyTime Interrogation (ATI)	Tracking and interception
2	insertSubscriber Data (ISD)	Interception, DoS
2	provideSubscriber Info (PSI)	Tracking
3	updateLocation (UL)	Interception, DoS
3	sendRoutingInfo (SRI)(-SM, -LCS)	Multiple attacks i.e. IMSI disclosure, SMS interception
3	sendAuthentication Info (SAI)	Interception

3.4. Proposed Anomaly Detection Scheme

To demonstrate location tracking and interception attacks, three types of map message requests: ATI, PSI and SRI-

SM are used. The simulator generates a data set for attacks and for normal traffic. This traffic is then captured on the loopback interface (lo) using the Wireshark packet capturing tool that generates pcap files. Anomalies are detected using Snort and customized SS7 anomaly detection rules. The proof-of-concept is presented, in the form of a flow diagram, in Fig. 1, and the model or the template of the anomaly detection rules is given in Fig. 2.

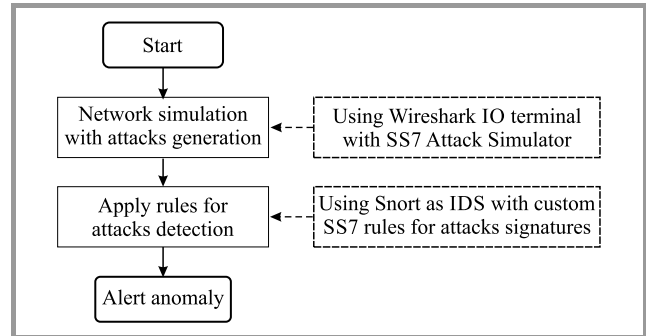


Fig. 1. Anomaly detection and alert generation flow.

3.5. Anomaly Detection and Alert Generation

As shown in Fig. 4, the first or the upper window shows live packet capturing. The middle or the second window shows the protocols underneath. The lower or the third window is the one that offers the information in “hexadecimal” form – a direct translation of the “bits” circulating through the communication channel. This tool’s window is crucial, as it helps collect signatures of traffic patterns in the form of hexadecimal figures. Bits are the deepest level of signatures, as any other form of analysis in the higher-level protocols will always be more densely packaged. Information circulating at the lowest level, in the form of bits, cannot avoid detection. During this experiment, Wireshark was helpful in identifying and analyzing attack packets from the captured traffic. Differentiating at-

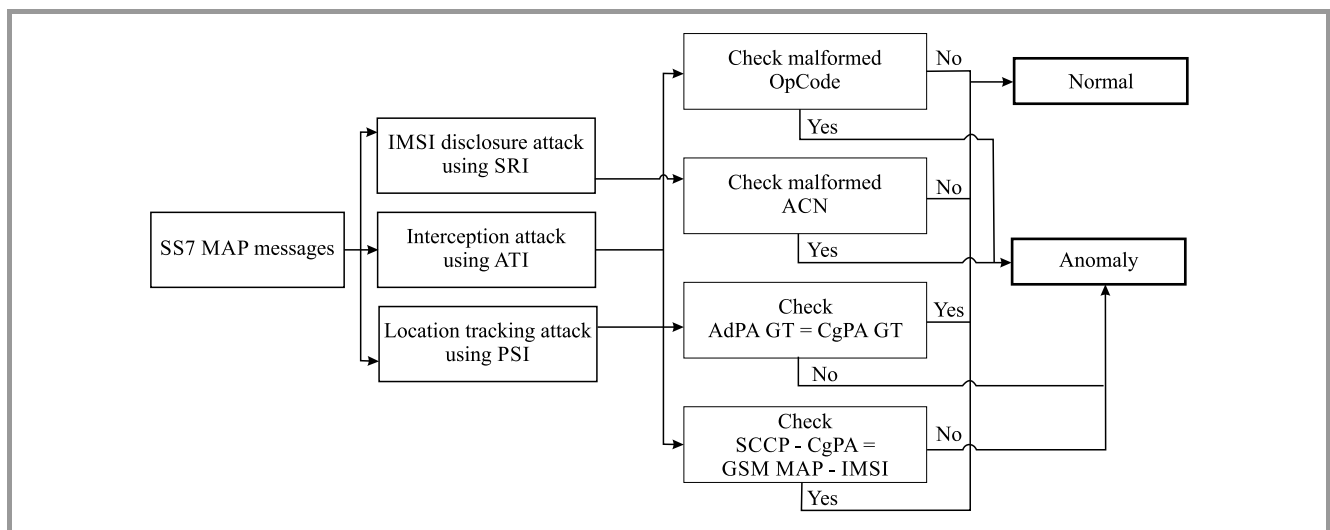


Fig. 2. Model of SS7 anomaly detection rules.

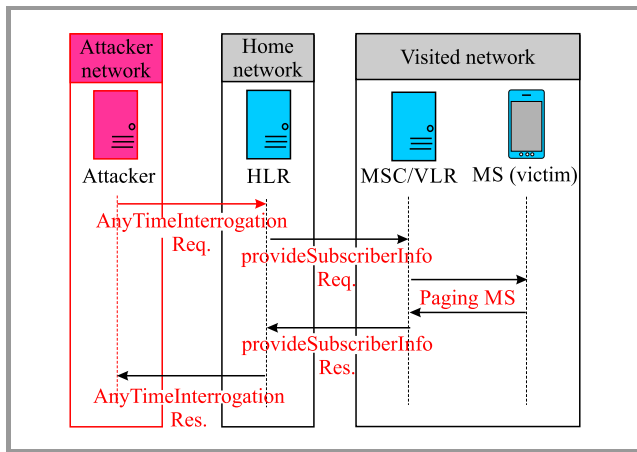


Fig. 3. SS7 attack using a MAP ATI message request.

tack packets manually by analyzing each packet is difficult and is not a recommended approach.

Attack using anyTimeInterrogation (ATI) request. The use of SS7 MAP ATI messages to perform a location tracking attack is presented in Figs. 3 and 4.

Attack using provideSubscriberInfo (PSI) request. Figures 5 and 6 show how SS7 MAP PSI message exploitation is carried out to perform location tracking attacks. Unfortunately, only the HLR could send the MAP PSI message to the current VLR. However, the attacker can send this MAP PSI message request straight to VLR via its MSC/VLR,

bypassing the HLR. To do so, the attacker will require the target’s IMSI and current VLR address information. As a result, the attacker launches a new attack by sending MAP SRI-SM to HLR, which provides all the critical information to the attacker without checking or validating it. This SRI-SM message request belongs to the category 3 message type and must be inspected and validated at the network node. This SRI-SM message request can potentially be exploited for other attacks, such as SMS interception.

Wireshark supports the SCCP protocol, and the tool offers the option of applying visualization filters for SCCP elements. It allocates different subsystem numbers (SSNs) to each entity, making it easier to use them as a filter. It helps

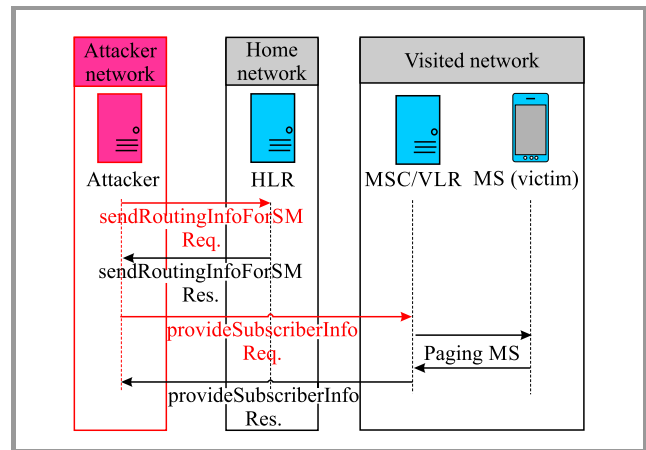


Fig. 5. Example of a PSI signaling message being exploited.

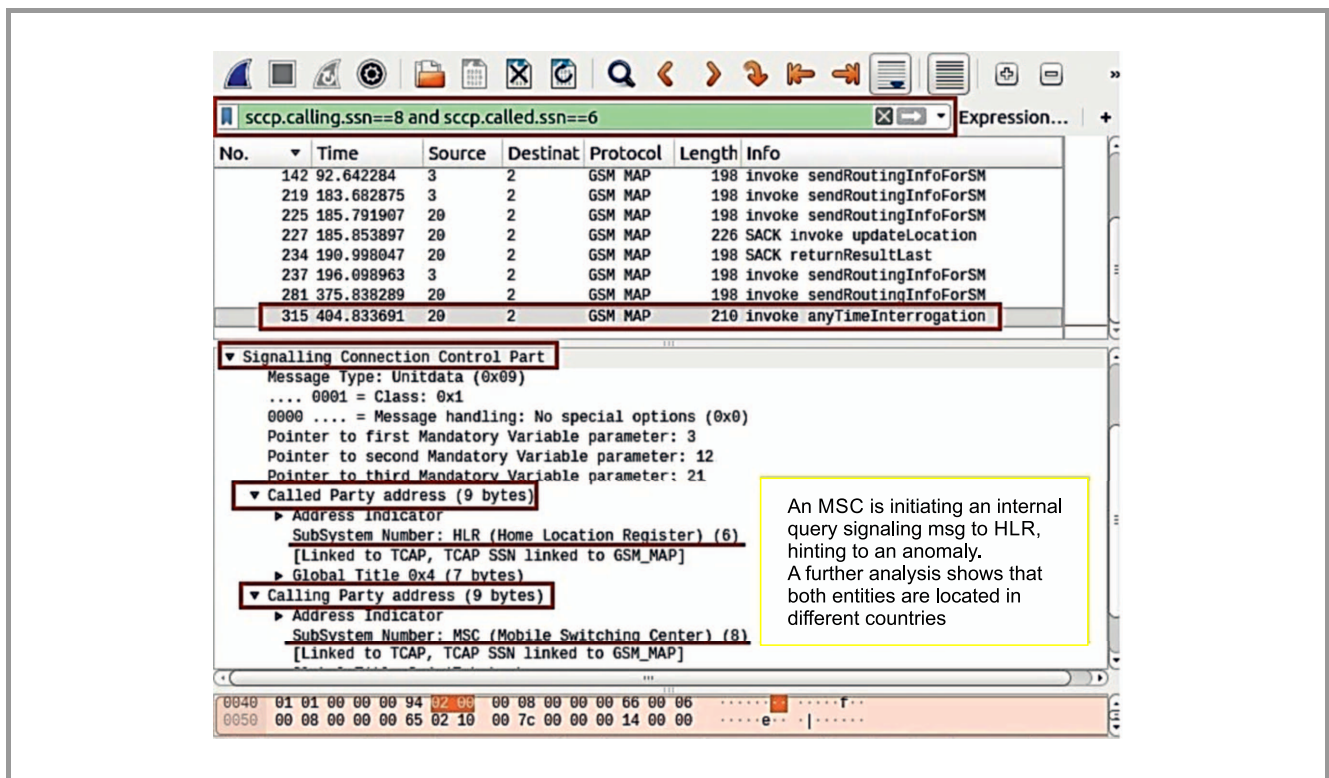


Fig. 4. Identification and analysis of attack packets captured in Wireshark

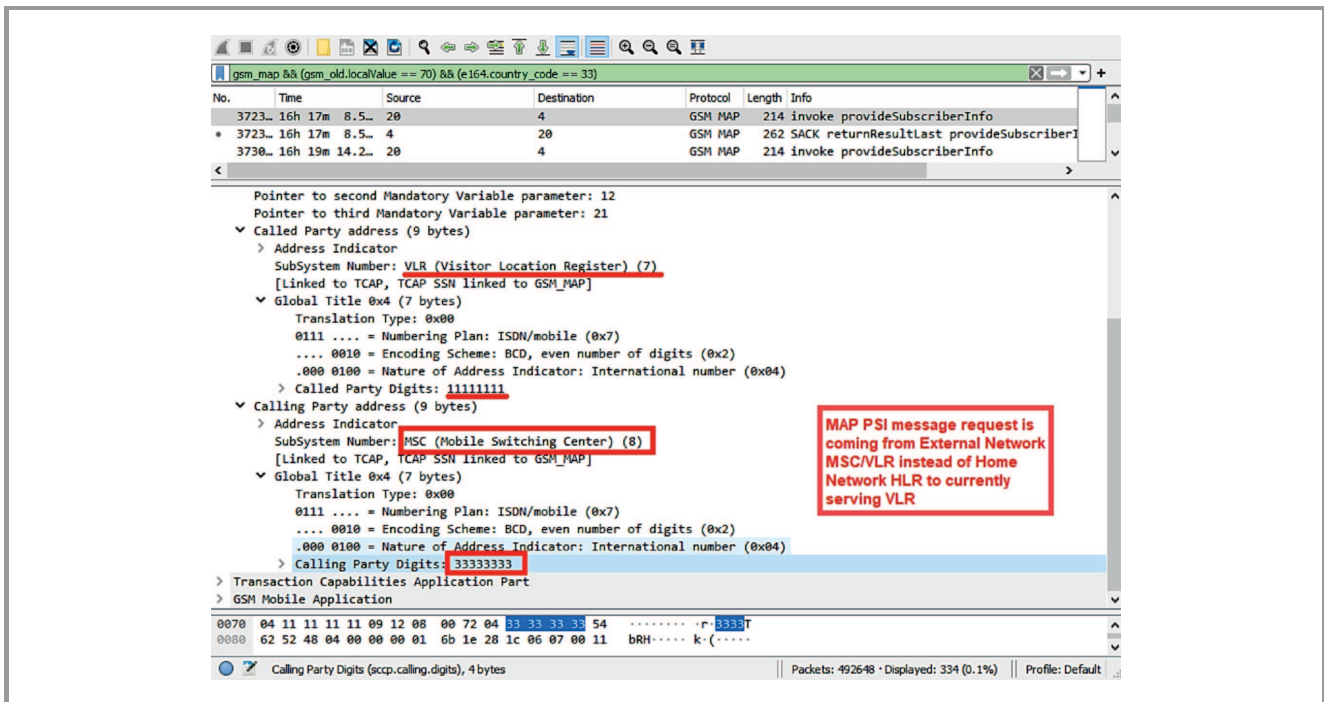


Fig. 6. SS7 attack using a MAP PSI message request.

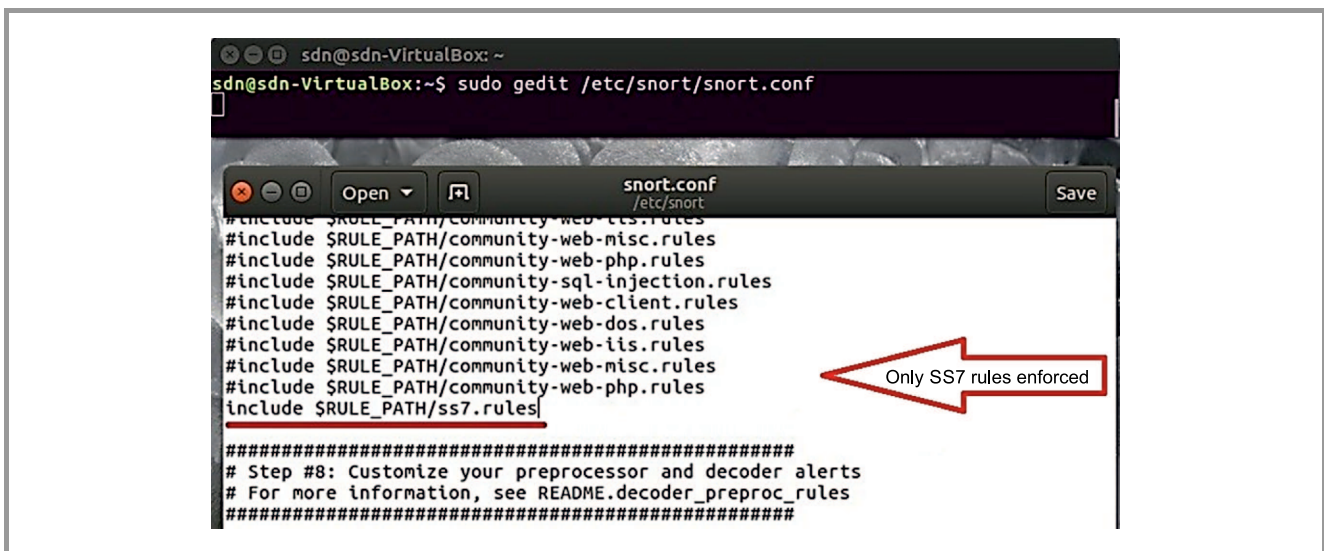


Fig. 7. Snort using an SS7 rules file.

deduce that if this attack packet is provided as an input to a detection tool, then all attack-related packets can be detected live or during the attack, should it reoccur. The data is presented in hexadecimal form, which is the primary representation of the packet's bits circulating across the communication channel. These bits could be helpful for the detection of signatures if provided as an input to some content-matching tool that is capable of matching all the packets against these bits to help detect all attack-related packets.

Acting in the capacity of an IDS, Snort provides hundreds of pre-loaded rules classified into different families, such

as HTTP, telnet, ssh, etc. All these rules, if enforced, can help detect hundreds of attacks. However, the tool must be kept up to date for standard usage, as new rules are published and regularized on a regular basis. With its great flexibility, Snort allows the addition of custom rules in its configuration file.

In this research, as shown in Fig. 7, custom rules named SS7 rules were added to the configuration file of Snort. This rules file contains all three types of rules covering all simulated attacks, with hexadecimal bits from the third window of Wireshark added as content matching information. After adding these rules, all other rules were disabled

using the hash symbol. The generated pcap file is given as input to Snort to test the SS7 rules. The tool detected the attacks without any false negatives.

4. Results

The results demonstrate that by relying on the knowledge of the SS7 network and its operation, traffic anomalies can easily be detected and, hence, attacks can be mitigated. Furthermore, from the results shown in Table 2, one may infer that filtering SS7 data with the use of a rule-based algorithm should be performed as the first defensive layer for all MAP SS7 messages.

Table 2
Confusion matrix for MAP UL, MAP PSI, SRI-SM, and ATI

	MAP PSI		MAP SRI		MAP ATI	
	TP	TN	TP	TN	TP	TN
Predicted positive	96	4	10	2	10	4
Predicted negative	0	4605	0	2946	0	4600
Accuracy	0.9998		0.9997		0.9998	
Detection rate	99.980%		99.997%		99.998%	
False positive	1		1		1	
False discovery	0.04		0.1667		0.2857	
False negative	0.9796		0.9966		0.9978	
Sensitivity	0.0204		0.0034		0.0022	
Specificity	0.9998		0.9997		0.9998	
Precision	0.96		0.833		0.7143	

A dataset of 12,279 samples was generated using the SS7 attack simulator. Out of these samples, 16 were detected as anomalies related to a MAP anyTimeInterrogation (ATI) message request, and 100 were detected as anomalies related to MAP provideSubscriberInfo (PSI) message requests. Similarly, for the MAP sendRoutingInfoSM (SRI-SM) message request, 12 samples were detected as anomalies. Based on the dataset for a particular MAP ATI message request, 10 of the detected anomalies were actual attacks, i.e. true positives, leaving 6 false positives. Similarly, for the MAP PSI message request, 96 of the detected anomalies were actual attacks, i.e. true positives, leaving 4 to be false positives. Likewise, in the case of MAP SRI-SM message requests, 10 of the detected anomalies were actual attacks, i.e. true positives, leaving 2 to be false positives. As shown in Table 2, the overall anomaly detection accuracy (related to all three types of message requests) is 99.98%.

4.1. Evaluation Matrix

The anomaly detection model is evaluated using the following metrics:

- True positive (TP), the number of instances correctly predicted as attacks.
- False positive (FP), the number of instances incorrectly predicted as attacks.
- True negative (TN), the number of instances correctly predicted as non-attacks.
- False negative (FN), the number of cases incorrectly predicted as non-attacks.
- Accuracy = $\frac{TP + TN}{TP + FP + FN + TN}$.
- False alarm rate = $\frac{FP}{FP + TN}$.
- Detection rate = DR = $\frac{TP}{TP + FN}$ is the ratio between the total number of attacks detected by the proposed model and the total number of attacks present in the dataset.

5. Conclusion

SS7 networks have become open and exposed to a multitude of vulnerabilities, degrading the level of security of telecommunication systems. Relaxation in the rules and regulations that governed the telecommunications market has rendered the networks vulnerable. Interoperability-driven attempts to merge networks have added additional concerns regarding breaches of SS7 security measures. The addition of new signaling messages for telephone mobility and advanced telecommunication services has led to further abuses and attacks, such as subscriber tracking, call interception, SMS spamming, and denial of service. Although the advantages of Diameter, a new protocol gradually replacing the SS7 signaling protocol in the next generation telecommunication networks are numerous, the default level of security provided by Diameter is not sufficient to make LTE an attack-resistant solution.

It is worth mentioning that traffic analysis is a useful tool for monitoring networks and detecting anomalies, and it has been relied upon for a long time now. In order to enable the adoption of this approach for detecting SS7 attacks, Snort and Wireshark tools were deployed on a simulated SS7 attack traffic data set to show that the deployment of Snort is a feasible solution mitigating the problem of network security. The approach adopted analyses SS7 attack traffic using Wireshark (a packet capture tool), as well as identifies malicious patterns and signatures to create Snort IDS rules allowing to detect common types of attacks. Test results related to the proposed intrusion detection method show that Snort detects all 3 types of attacks that the simulator can generate, relying on rule-determining signatures stored in its configuration file. This method allows us to analyze and identify the flow of bits that circulate through the network during a simulated attack, and to detect such potential traffic patterns. This scheme uses tools with open-source licenses to avoid the huge costs of custom development. It will be useful for small- and medium-sized networks with manageable volumes of traffic to filter.

Acknowledgment

This research project was supported by Taylor's University, Malaysia, through Taylor's Ph.D. Scholarship Program.

References

- [1] "5G-ready next-generation signaling firewall", Positive Technologies, 2019 [Online]. Available: <https://positive-tech.com/storage/Signaling-NgFW.pdf>
- [2] S. P. Rao, S. Holtmanns, and T. Aura, "Threat modeling framework for mobile communication systems", arXiv:2005.05110, 2020.
- [3] B. Welch, "Exploiting the weaknesses of SS7", *Network Secur.*, vol. 2017, no. 1, pp. 17–19 (DOI: 10.1016/S1353-4858(17)30008-9).
- [4] K. Ullah *et al.*, "SS7 vulnerabilities – a survey and implementation of machine learning vs rule based filtering for detection of SS7 network attacks", *IEEE Commun. Surv. and Tutor.*, vol. 22, no. 2, pp. 1337–1371, 2020 (DOI: 10.1109/COMST.2020.2971757).
- [5] I. Ahmad *et al.*, "Security for 5G and beyond", *IEEE Commun. Surv. and Tutor.*, vol. 21, no. 4, pp. 3682–3722, 2019 (DOI: 10.1109/COMST.2019.2916180).
- [6] H. Zhang and L. Dai, "Mobility prediction: A survey on state-of-the-art schemes and future applications", *IEEE Access*, vol. 7, pp. 802–822, 2019 (DOI: 10.1109/ACCESS.2018.2885821).
- [7] S. Puzankov, "Stealthy SS7 attacks", *J. of ICT Standard.*, vol. 5, no. 1, pp. 39–52, 2017 (DOI: 10.13052/jicts2245-800X.512).
- [8] M. B. Savadatti and D. Sharma, "SS7 network and its vulnerabilities: An elementary review", *Imperial J. of Interdiscip. Res. (IJIR)*, vol. 3, no. 3, pp. 911–916, 2017 [Online]. Available: <http://www.onlinejournal.in/IJIRV3I3/153.pdf>
- [9] S. Holtmanns, I. Oliver, and Y. Míche, "Mobile subscriber profile data privacy breach via 4G diameter interconnection", *J. of ICT Standard.*, vol. 6, no. 3, pp. 245–262, 2018 (DOI: 10.13052/jicts2245-800X.634).
- [10] K. Jensen, H. T. Nguyen, T. V. Do, and A. Arnes, "A big data analytics approach to combat telecommunication vulnerabilities", *Cluster Comput.*, vol. 20, no. 3, pp. 2363–2374, 2017 (DOI: 10.1007/s10586-017-0811-x).
- [11] S. P. Rao, B. T. Kotte, and S. Holtmanns, "Privacy in LTE networks", in *Proc. 2nd Int. Worksh. on 5G Secur. – 9th EAI Int. Conf. on Mob. Multimed. Commun. MOBIMEDIA 2016*, Xi'an, China, 2016, pp. 176–183 (DOI: 10.4108/eai.18-6-2016.2264393).
- [12] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, "We know where you are!", in *Proc. 18th Int. Conf. on Cyber Conflict CyCon 2016*, Tallinn, Estonia, 2016, pp. 277–293 (DOI: 10.1109/CYCON.2016.7529440).
- [13] T. Engel, "SS7: Locate. Track. Manipulate", in *Proc. 31th Chaos Commun. Congr. 31C3 2014*, Hamburg, Germany [Online]. Available: <https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf>
- [14] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: the root of all evil", in *Proc. of the 12th Conf. on Secur. and Priv. in Wirel. and Mob. Netw. WiSec 2019*, Miami Florida, USA, 2019, pp. 1–11 (DOI: 10.1145/3317549.3323402).
- [15] A. D. Oliveira and C. D. Nguyen, "Tids: A framework for detecting threats in telecom networks", Hack.lu 2017, 2017 [Online]. Available: http://archive.hack.lu/2017/Hacklu_POST.TIDS_framework.pdf
- [16] R. Panigrahi, S. Borah, A. K. Bhoi, and P. K. Mallick, "Intrusion detection systems (IDS) – an overview with a generalized framework", in *Cognitive Informatics and Soft Computing*, P. Mallick, V. Balas, A. Bhoi, and G. S. Chae, Eds. *AISC*, vol. 1040, pp. 107–117. Springer, 2020 (DOI: 10.1007/978-981-15-1451-7.11).
- [17] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks", *Future Gener. Com. Syst.*, vol. 110, pp. 148–154, 2020 (DOI: 10.1016/j.future.2020.04.013).
- [18] H. Hindy *et al.*, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems", *IEEE Access*, vol. 8, pp. 104650–104675, 2020 (DOI: 10.1109/ACCESS.2020.3000179).



Rafia Afzal received her B.Sc. in Computer Science in 2012 and M.Sc. in Computer Science in 2016 from COMSATS University (CU), Islamabad. She is currently pursuing a Ph.D. degree in Computer Science at Taylor's University Lake Side Campus, Subang Jaya, Malaysia. Between 2015 and 2018 she worked as a Teaching

Associate with the COMSATS University Islamabad, Campus, Pakistan. She also worked as Senior Computer Teacher at F. G. Model High School For Girls I/8-1 Islamabad, Pakistan from Jan 2018 to Dec 2018. Her research interests include artificial intelligence, machine learning and mobile network security.


 <https://orcid.org/0000-0002-5299-1366>

E-mail: afzalrafia@sd.taylors.edu.my
School of Computer Science and Engineering
Taylor's University
47500 Subang Jaya
Selangor, Malaysia



Raja Kumar Murugesan is an Associate Professor of Computer Science, and Head of Research for the Faculty of Innovation and Technology at Taylor's University, Malaysia. He holds a Ph.D. in Advanced Computer Networks from the Universiti Sains Malaysia. His research interests include IPv6, future of Internet, Internet governance,

computer networks, network security, IoT, blockchain, and machine learning. He is a member of the IEEE and IEEE Communications Society, Internet Society (ISOC), and is associated with IPv6 Forum, Asia Pacific Advanced Network Group (APAN), Internet 2, and Malaysia Network Operator Group (MyNOC) member's community.

 <https://orcid.org/0000-0001-9500-1361>

E-mail: rajakumar.murugesan@taylors.edu.my
School of Computer Science and Engineering
Taylor's University
47500 Subang Jaya
Selangor, Malaysia