Detection of Signaling System 7 Attack in Network Function Virtualization using Machine Learning

Tooba Qasim[1], M. Hanif Durad[1], Asifullah Khan[1], Farhan Nazir[2], Tehreem Qasim[3]
[1]Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan
[2]Xflow Research, Islamabad, Pakistan
[3]Quaid-i-Azam University, Islamabad, Pakistan
toobaqasim0191@gmail.com, hanif@pieas.edu.pk, asif@pieas.edu.pk, farhan.nazir@xflowresearch.com,
tehreemqasim@ele.qau.edu.pk

***Abstract*—The mass popularization of telecommunication services has led to a heavily loaded Signaling System No. 7 (SS7) network. SS7 was originally well protected because the communication networks were controlled by trusted state-owned telecom operators. Switching to the IP technology and deregulation has made it fairly easy for third parties to gain access to the once protected SS7 network. For many vendors, Signaling Transfer Points (STPs) have already evolved from TDM (Time Division Multiplexing) proprietary hardware to an IP proprietary hardware solution. So the next step is moving to a virtualized solution such as Network Function Virtualization (NFV). The intersection of SS7 and NFV has also introduced several new security challenges. In this work, we present the vulnerabilities of SS7 messages to cyber-attacks in a virtualized environment. A network simulation model under SS7 attack is developed. In order to mitigate these attacks machine learning techniques are applied to the gathered network traffic.**

Keywords—SS7 Security; Network Function Virtualization; Cyber security; Machine Learning; Mobile System Security

I. INTRODUCTION

Our society is more reliant on telecommunications than ever before. The Internet of Things (IoT) and the growing use of Machine to Machine (M2M) solutions add to the pressure on mobile carriers to ensure network security and continuity of service.

This mass popularization of telecommunications services has led to a heavily loaded Signaling System number 7 (SS7). SS7 is protocol used in Second and Third Generations (2G and 3G) mobile networks. Initially SS7 network was well protected and it didn’t require as such security. But as the industry is continuously moving towards Internet Protocol (IP) technology, it is much easier to get access to the enclosed SS7 network. The SS7 network, in general has been marked as vulnerable and susceptible to exploits by researchers [1]. Intruders can get all the information about the subscribers once they get access to the SS7 network. They can track phone users globally, deny service to subscribers, intercept SMS messages and calls and can commit fraud.

The intersection of SS7 and Network Function Virtualization (NFV) has also introduced several new security challenges. With operators opening the SS7 network to offer third-party access as a commercial offering, vulnerabilities are exposed and attacked are being launched.

Different intrusion detection solutions have been developed for these vulnerabilities but most of them only gather information about the system under attack. However, it is equally important to obtain knowledge about the attacker [2]. Distinguishing anomalous and normal network traffic is difficult and wearisome. A human analyst has to analyze huge chunks of data to identify anomalous sequences in data. To make the analyst's job easier, an application is required to utilize machine learning techniques and create rules for an intrusion detection expert system [3].

This study therefore focuses on the security of SS7 network in virtualized environment. The study aims at demonstrating vulnerabilities of SS7 network to cyber-attacks which can make SS7 messages susceptible to attacks. A mechanism for the security of SS7 network has been proposed using machine learning techniques to classify the incoming network traffic into normal and abnormal. The efficiency of the proposed mechanism is tested in a simulated network.

The rest of this paper is organized as follows. Section II highlights the related work. Section III introduces SS7 vulnerabilities. Section IV presents the methodology adopted for applying machine learning to SS7 attack. Section V presents the experimental setup. Results are presented in section VI. Conclusions and Future Work is given in section VII and VIII, respectively.

II. RELATED WORK

Security of Signaling System No. 7 has been given an increasing amount of attention in the past few years. It’s increasingly becoming clear that SS7 is fraught with serious vulnerabilities that compromise the privacy of cellular customers.

In [4], authors discuss several issues and challenges faced by Stream Control Transmission Protocol (SCTP), which is used in SS7 over IP called SIGTRAN [5]. In [6] several vulnerabilities in SS7 network are presented. In [7] different threats as a result of the intersection between SS7 and IP are described, provided by SIGTRAN protocol and MTPSec, IPsec, and enhanced firewall combined with intrusion detection are proposed as a solution. Authors in [8] discuss various types

978-1-5386-3564-3/18/$31.00 ©2018 IEEE

of SS7 attacks like entry points to the core network, location privacy breach, call interception and SMS based attacks.

In [9] authors present the Diameter-based attacks in LTE networks using Interworking Function (IWF). They also propose protection approaches for these attacks. In [10] Kristoffer Jensen, apply machine learning to improve the security of SS7 and secure subscribers identity.

These approaches suffer several shortcomings e.g. in [7], [8] and [9], the authors just exposed the vulnerabilities of SS7 network and proposed some protection techniques, no detection mechanism is implemented to provide a proof of the concept. In [10] artificial traffic is generated using a simulator in a controlled environment.

In this paper, we generate close to real SS7 traffic in virtualized environment by using open source Dialogic SIGTRAN protocol stack software[1]. Message intercept attack and DoS attacks are launched on the network and suitable machine learning classifiers are used to detect the attack.

III. SS7 Vulnerabilities

SS7 vulnerabilities can be divided into four main categories [11]:

- Breach of user information
- Eavesdropping
- Financial thievery
- Misuse of service

A. *Breach of user information*

Subscriber's unique information like International Mobile Subscriber Identity (IMSI), Location Area Code (LAC) and Mobile Country Code (MCC) and can be illegally accessed using legitimate functions associated with SMS. This can lead to other serious security concerns.

1) Acquiring the IMSI: Every user in a network has a unique IMSI. The IMSI isn't transmitted directly on the physical channel, instead a randomly selected Temporary Mobile Subscriber Identity (TMSI) is utilized to transmit it. This is because the IMSI can pave the way for several other threats. However, if the attackers can somehow obtain TMSI, they can easily get the IMSI as well. This enables the attacker to find out the user's home country and the mobile network.

2) Finding the subscriber's location: The location of the subscriber can be obtained by using "Any Time Interrogation", a message that is used to provide the location details of the subscriber. The equipment used by the network operators is usually not configured to not respond to these messages.

Subscriber's location can also be obtained by attacker using the normal Mobile Application Part (MAP) messages and by acting as a Faux Home Location Register. This procedure is known as Provide Subscriber information. Device ID, Mobile Country Code, Mobile Network Code and the Location Area Code can be obtained through this procedure.

B. *Eavesdropping*

Attacker can eavesdrop on subscriber's data, can wiretap and send/modify text messages to a victim by acting as a "man-in-the-middle", with the victim totally unaware of the attack.

1) Wiretapping outgoing calls: In this attack, the attacker intercepts all the communication between two users by using the Customized Applications for Mobile Networks Enhanced Logic Application Part (CAP) protocol. The intruder bridges himself between the two calling parties and directs all the calls to its monitoring system.

2) Wiretapping incoming calls: For this purpose, MAP messages and a call-forwarding function are used. The target user is not aware of this attack. The attacker sends the victim calls to the monitoring system at the SS7 MAP Message level. Consequently, the attacker establishes another call to the user to whom call is being made.

C. *Financial thievery*

In this attack the victim's Mobile Switching Centre (MSC) is impersonated. The aim is to get text messages or to receive information about the victim's bank account etc. Unstructured Supplementary Service Data (USSD) is used for this purpose. Finally, victim's account can be misappropriated for monetary transactions.

D. *Misuse of service*

In this attack, subscriber's billing is exploited. This leads to significant fiscal repercussions for the network operator. Increase in these attacks causes inaccessibility of services, and decrease in the gross income.

IV. Methodology

This section presents the methodology we adopt for the development of the simulated experiment. Detection of SS7 attack is carried out that has been launched in a network simulation model. Two of the mentioned SS7 vulnerabilities in previous section are exploited in the simulation model i.e. eavesdropping on subscriber traffic and disruption of subscriber service.

In the proposed model Dialogic SS7/SIGTRAN Protocol Stack[1] is installed on signaling gateways. A virtual Signaling Transfer Point (STP) is used between SS7/SIGTRAN nodes to route SMS. Windows Server 2012 with Routing and Remote Access Service (RRAS) is configured as vSTP. The attacker machine intercepts the text messages transferred between SIGTRAN nodes and launches Man-in-the-Middle (MITM) attack using Ettercap tool and DOS attacks with the help of Scapy tool.

As a result of the DoS attack, router becomes busy in handling the invalid packets and can't route legitimate packets to the destination. The network activity can be seen in Fig. 1.

[1] Available at https://www.dialogic.com/signaling-and-ss7-components/download/dsi-interface-protocol-stacks

X-axis shows time and Y-axis shows packet/second. The peak values show a large number of packets being transmitted per second. It could be legitimate or anomalous packets that may result in disruption of service.

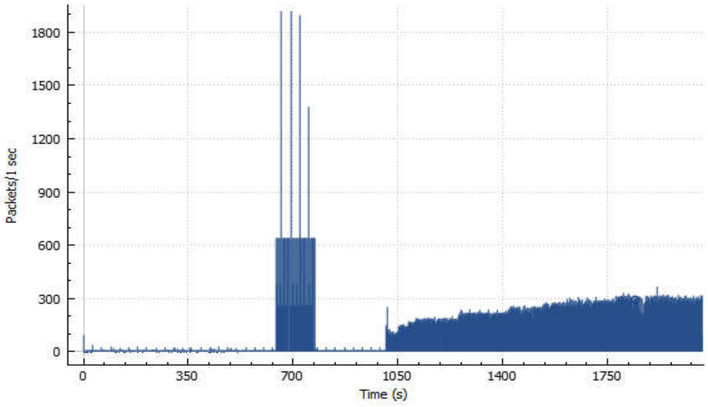

Fig. 1. Network Activity

In order to determine whether the peak value represents anomalies or normal traffic, machine learning is used. Pre-processing of the collected data is done using python scripts. Different machine learning classifiers are used to classify the traffic between normal and abnormal based on the feature set. Perceptron [12], Decision Tree [13], Support Vector Machine (SVM) [14] and Random Forest [15] are used for data classification. With the help of data classification, suspicious packets can be blocked from entering the network in the future. Also the attacker can be barred from joining the network.

V. Experimental Setup

The network tested to analyze the potential of the proposed approach to circumvent SS7 attack consists of four machines. Static IP addresses are assigned to these machines. SIGTRAN network setup is shown in Fig. 2.

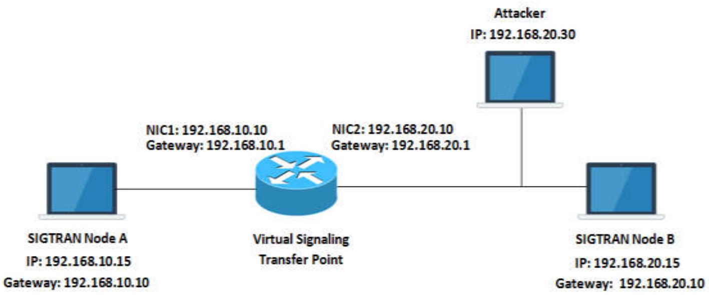

Fig. 2. SIGTRAN Simulation Setup

Implementation of detection of SS7 attack in network function virtualization using machine learning techniques includes the following steps:

- Creating virtual machines for SS7/SIGTRAN Signaling Gateways, VSTP and attacker using Virtual Box.
- Configuration of Dialogic SS7/SIGTRAN protocol stack on two signaling Gateways.
- Configuration of Windows Server 2012 R2 as VSTP between two SIGTRAN Signaling Gateways.
- Configuration of Routing and Remote Access Server on Windows Server 2012 to route SMS between two SIGTRAN nodes.
- Installation of Python, Scapy, Wireshark and Ettercap tools on Attacker machine.
- Exchange of SMS between two SIGTRAN nodes through vSTP.
- Network scanning for hosts by attacker using Ettercap.
- Launching MITM attack on the router and one of the SIGTRAN node using python script in scapy.
- Launching DoS attack on the router using Scapy.
- Network traffic capture through Wireshark on router.
- Preprocessing, normalization and labeling of data.
- Use of Machine Learning classifiers on Packet Capture file to classify the traffic between normal and anomalous traffic.
- Generating Reports and analyzing results.

Once an attacker gains access to a private or public IP networks transporting SS7 signaling messages, he can use freely available packet manipulating software packages to disrupt the whole SS7 signaling network. The attacker can eavesdrop on all the communications between any two participants and can launch DoS attack later to bring down the communication links between those participants.

VI. Machine Learning For The Detection Of Ss7 Attack

In order to find out how feasible it is to apply machine learning in SS7 network, the network data obtained through Wireshark and exported to CSV file, passes through a series of steps as shown in Fig. 3 and the machines learning techniques are applied to it.

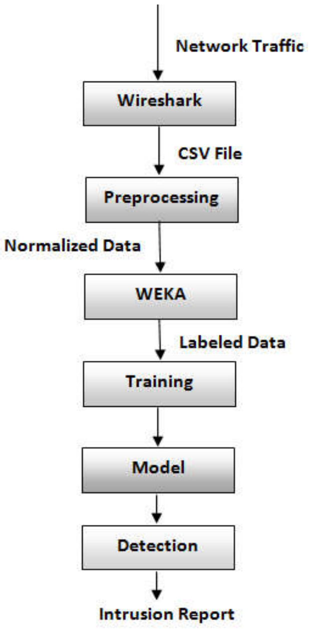

Fig. 3. Machine Learning Process

The data is preprocessed using python scripts in order to covert nominal data to numeric. Preprocessed data is normalized by removing any negative values and normalizing very small decimal values. The preprocessed and normalized data is then taken as input in Weka.

To detect attacks, a suitable algorithm must be chosen according to the type of the data selected. Two most commonly used approaches to detect anomalies are Supervised and Unsupervised learning.

In supervised learning approach there are a large number of labeled normal and abnormal data events. In unsupervised learning, the dataset consists of many known normal events but only few abnormal events are unknown.

In our experiment, dataset was labeled as normal and abnormal based on some of the known features as shown in Table I, consisting of the normal and abnormal traffic. Therefore the algorithms chosen were supervised learning algorithms.

TABLE I. FEATURES SELECTED TO DETECT ANOMALIES IN TRAFFIC

Description	Variable Type
Throughput	Numeric
Timing	Numeric
Byte Length	Numeric
MAC-IP Mapping	Nominal
Time to live	Numeric
SCTP verification tag	Numeric
IPv4 Header Checksum	Numeric

A. *Use of Machine Learning Classifiers in Weka*

Weka[2] is a collection of machine learning algorithms for data mining tasks. The algorithms can either be applied directly to a dataset or called from our own Java code. Weka contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization.

Four classifiers are used on our dataset which are Perceptron, Decision Tree, Support Vector Machine (SVM) and Random Forest. A model for each classifier was generated and evaluated with a 10-fold cross validation. Each classifier performance was observed while building a model.

The results obtained by each classification algorithm are analyzed and evaluated with the training set. It is important that these classifiers produce good and reliable results during classification of new traffic. It is better not to use the best classifier, but to choose faster algorithms. Therefore, the faster algorithm with good results is chosen.

VII. RESULTS AND DISCUSSION

A dataset of 23859 samples was used out of which 12286 were normal instances and 11573 were labeled anomalous. Results obtained by each classifier after building the model are shown in the Table II:

TABLE II. PERFORMANCE AND EVALUATION OF DIFFERENT CLASSIFICATION ALGORITHMS

Classifier	TP Rate	FP Rate	Correctly Classified Instances	Time taken to build model
Perceptron	0.848	0.150	84.77%	22.58 sec
Decision Tree	0.920	0.077	92.03%	8.81 sec
Support Vector Machine	0.791	0.215	79.05%	942.15 sec
Random Forest	0.898	0.102	89.77%	1.42 sec

It can be observed from Table II that Decision Tree has the highest accuracy among the implemented classifiers with a TP rate of 0.920 and FP rate of 0.077. Random Forest despite slightly degraded performance is the most efficient one in terms of time overhead.

Fig. 4 shows the model performance chart or ROC curve for each classifier and compares the true positive rate of the four algorithms as a function of the false positive rate at different prediction thresholds. We observed that Decision Tree yielded the highest cross-validation prediction performance of the four compared methods.

[2] Available at http://prdownloads.sourceforge.net/weka/weka-3-8-1jre-x64.exe

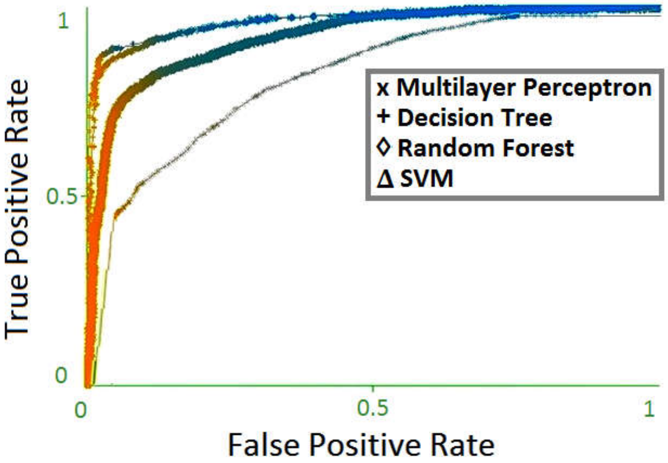

Fig. 4. Model Performance Chart

VIII. Conclusion

In this research paper we described how SS7 network is exposed to vulnerabilities and threats due to the intersection of IP technology and deregulation. Also the intersection of NFV and SS7 has introduced some threats. Different categories of SS7 vulnerabilities are presented. In order to detect attacks against SS7 network, machine learning techniques are proposed as a detection mechanism. An experimental setup has been established in order to provide proof of concept. SS7 traffic is generated in a virtualized environment. MITM and DoS attacks are launched on the network. Different machine learning classifiers are used to detect attack by classifying traffic into normal or malicious.

IX. Future Work

The results obtained in this research work have raised many other questions and concerns. There are several lines of research arising from this work which should be pursued.

In future, experiment can be carried out in a real life SS7 network using real life data so that the feasibility of the proposed detection methods can further be proved. Different machine learning techniques other than those used in this paper can be used. Virtual routers or Soft switches can be used as part of NFV in future along with the real traffic from a telecom network to detect and mitigate the vulnerabilities in SS7 protocol.

References

[1] Jiang Lingling, Ma Hong, “New trends of attack and prevention technologies in telecommunication”, IEEE Information Technology and Applications, May 2009.

[2] P. Fruehwirt, S. Schrittwieser and E. R. Weippl, “Using machine learning techniques for traffic classification and preliminary surveying of an attackers profile”, Proc. of Int. Conf. on Privacy, Security, Risk and Trust, 2014.

[3] Chris Sinclair, Lyn PierceSara, Matzner, “An application of machine learning to network intrusion detection”, ACSAC '99 Proceedings of the 15th Annual Computer Security Applications Conference, December 06 - 10, 1999.

[4] Shaojian Fu and Mohammed Atiquzzaman, “SCTP: State of the art in research, products, and technical challenges”, IEEE Communications Magazine, April 2004.

[5] L. Ong, et al., Framework Architecture for Signaling Transport, RFC 2719, October 1999.

[6] G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi, “Securing SS7 telecommunications networks” IEEE Workshop on Information Assurance and Security, 5–6 June 2001.

[7] Hemant Sengar, Ram Dantu, Duminda Wijesekera and Sushil Jajodia, “SS7 over IP: signaling interworking vulnerabilities”, IEEE Network: The Magazine of Global Internetworking, November 2006.

[8] Garima Sharma, “SS7 signaling protocol – Attacks against privacy”, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol 3, Issue 7, July 2016.

[9] Silke Holtmanns, Siddharth Prakash Rao, Ian Oliver, “User location tracking attacks for LTE networks using the interworking functionality”, IFIP Networking Conference (IFIP Networking) and Workshops, 2016.

[10] Kristoffer Jensen, Thanh van Do, Hai Thanh Nguyen, André Årnes, “Better protection of SS7 networks with machine learning”, IT Convergence and Security (ICITCS), 2016 6th International Conference, November 10, 2016.

[11] Mamta B. Savadatti, Divya Sharma, “SS7 network and its vulnerabilities: An elementary review”, Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-3, 2017.

[12] Ruck, Dennis W., et al. "The multilayer perceptron as an approximation to a Bayes optimal discriminant function." IEEE Transactions on Neural Networks 1.4 (1990): 296-298.

[13] Quinlan, J. Ross, and Ronald L. Rivest. "Inferring decision trees using the minimum description lenght principle." Information and computation 80, no. 3 (1989): 227-248.

[14] Platt, J. "Fast training of support vector machines using sequential minimal optimization, In, B. Scholkopf, C. Burges, A. Smola,(eds.): Advances in Kernel Methods-Support Vector Learning." (1998).

[15] Breiman, Leo. "Random forests." Machine learning 45.1 (2001): 5-32.