Analysis and application of SS7 network threats detection

Zuobing Xu*, Yu Wang, Xiaoyue Ge
School of Space Information, Space Engineering University, Beijing, China

ABSTRACT

Signaling System No.7 (SS7) Network was designed with a focus on reliability and efficiency, with a high degree of trust between communication entities and no encryption or defense against attacks. With the development of the network, the vulnerability of SS7 network is increasingly exposed. This paper comprehensively analyzed the security threats existing in SS7 network, and extracted the characteristics of the threats such as location tracking, interception of calls and interception of SMS. On the basis of feature extraction, threat modeling is carried out to extract threat detection rules, and the threat detection model is applied to the experimental network.

Keywords: SS7, threats, detection, analysis, application

1. INTRODUCTION

SS7 network is one of the three supporting network of modern communications, SS7 is internationalization, standardization of the general public channel signaling system, SS7 network is an important support of telecommunication network. it was designed with a focus on reliability and efficiency, with a high degree of trust between communication entities and no encryption or defense against attacks. If the network is highly closed, the possibility of being attacked is very small. However, with the development of the network, SS7 network is no longer completely closed, and the vulnerability of the SS7 is increasingly exposed. There is no authentication mechanism between elements, and any elements which is connected to the network can send message to other elements which have roaming relationships around the world. Some countries have lax supervision on the access of the network, so attackers can easily enter the network, which greatly reduces the security of the network and the threshold of attack.

This paper firstly analyzes the security threats of SS7 network, then extracts the characteristics of attacks such as location tracking, interception of calls and interception of SMS. On the basis of feature extraction, threat modeling is carried out to extract threat detection rules. Finally, the threat detection model is applied to the experimental network.

2. THE THREATS OF SS7 NETWORK

At present, the calls and SMS services runs in 2 generation mobile communication protocol. For the non_Internet services such as voice and SMS, the service enters the network and runs on the SS7 network. Subscribers can use the service exchange of SS7 to complete the communication between GSM networks and other communication networks, and managing subscribers' data and mobility database. Some elements of SS7 involved in this paper include Moblie Switch Center (MSC), Visitor Location Register (VLR) and Home Location Register (HLR), Short Message Center (SMSC), and International Mobile Subscriber Identity (IMSI), Mobile Station International ISDN number (MSISDN), Global Title (GT), etc. The architecture of the international SS7 network is shown in Figure 1. The SS7 network is mainly faced with potential threats such as subscriber location tracking, interception of call and interception of SMS, as shown in Figure 2.

* 578866528@qq.com

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 125061J

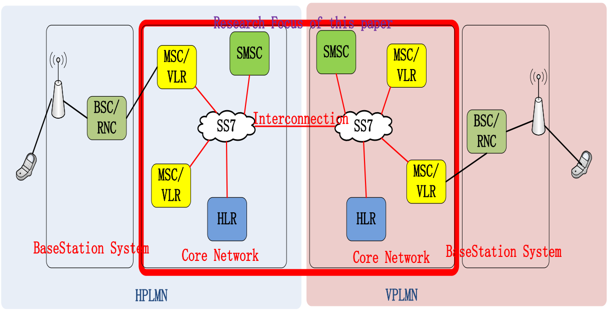


Figure 1. SS7 network architecture.

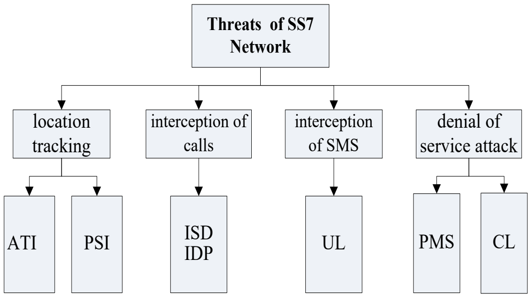


Figure 2. Threats of SS7 network.

Table 1. Analysis of the SS7 network threats.

Threat category	Involved in the message	Major parameter	Characteristics and research status
Information disclosure	SRI, PRN	MSC, IMSI	Based on the SS7 protocol flow, the characteristics of SRI message are analyzed. The IMSI and MSC information returned by SRI response message which leads to subscriber information disclosure[1].
Information disclosure	SRIFSM	MSC, IMSI	Because the elements do not authenticate the initiator of the SRIFSM message, the subscriber information is leaked when the IMSI and MSC of the subscriber are contained in the return SRIFSM message[2].
Location tracking	ATI, PSI	LAC, CI	Due to the high degree of trust between the elements, the attacker can counterfeit gsmSCF or HLR to sends ATI or PSI message to obtain subscriber's cell location[3,4].
Interception of calls	ISD, IDP	MSISDN, IMSI, gsmSCF	Taking advantage of the defect of CAMEL protocol in international roaming, the attacker inserts false gsmSCF address by sending ISD message to achieve the purpose of call interception[5].
Interception of SMS	UL	IMSI	Using the update location mechanism of SS7 network, the attacker inserts the fake MSC address by sending UL message to the subscriber's HLR, while sending the SRIFSM message, the HLR will return the fake MSC address, and any SMS sent to the subscriber will be intercepted through the false MSC[5,6].
Denial of service	PMS	IMSI	The attacker impersonates VLR to send PMS messages to HLR, which are used to mark the current subscriber unreachable in the HLR, so that the subscriber cannot make calls and receive SMS messages[7].
Denial of service	CL	IMSI	The attacker impersonates HLR to send CL messages to the subscriber's VLR, which are used to clear the current subscriber's information in VLR. When the subscriber receives call or SMS, the VLR considers that the subscriber is unreachable and unable to provide services.

In view of the threats in SS7 network, this chapter conducts research and analysis from the aspects of protocol defects and elements vulnerabilities. Location tracking mainly involves message such as SRI, PRN, SRIFSM, ATI and PSI, Call interception mainly involves ISD and IDP message. SMS interception mainly involves UL and SRIFSM message. Parameters in each message involve IMSI, MSISDN, MSC, LAC, and CI (Table 1).

3. THREATS DETECTION MODELLING

The SS7 network threats are mainly based on the SS7 protocol characteristics of subscribers' home and roaming places, and the attacker's methods of attack and technical principles are analysed. the characteristics of the threats which are extracted from the data are used to form a threat detection model. Some concepts need to be defined in threat modeling in this chapter, as shown in Table 2:

Table 2. Definition.

Name	Description	Name	Description
Inbound message	Roaming message	HPLMN	Home network operator
Opcode	Message type	VPLMN	Visit network operator
messagetype	The messagetype value of the request message is 98, and the messagetype value of the reply message is 100.	time_message	Indicates the time when the message was sent.
imsi_cc	Imsi_cc means the country that imsi belongs to, for example: imsi=4600113036777 and its mcc=460 means China.	ogt_cc	ogt_cc means the country that the original GT belongs to, for example: ogt=8613822811 and its cc=86 means China.
msisdn_cc	msisdn_cc means the country that msisdn belongs to.	dgt_cc	dgt_cc means the country that the destination GT belongs to.
eventtypebsm_cc	eventtypebsm_cc means the country that msisdn belongs to.	callingpartynumber_cc	callingpartynumber_cc means the country that msisdn belongs to.
gsmscf_cc	gsmscf_cc means the country that msisdn belongs to.		

3.1 Location tracking

The main reason for location tracking is that the attacker sends illegal messages with MSISDN or IMSI to obtain the cell ID of the subscriber. Based on the cell ID, the attacker can track a subscriber with accuracy down to street level. The analysis of the attack is shown in Figures 3 and 4.

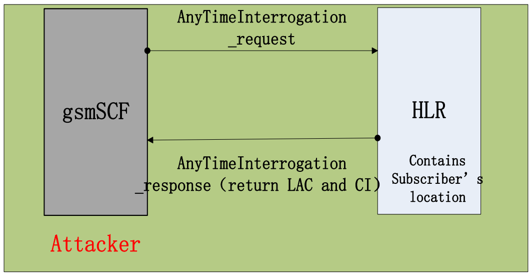

AnyTimeInterrogation _request
gsmSCF
HLR
AnyTimeInterrogation _response (return LAC and CI)
Contains Subscriber’ s location
Attacker

Figure 3. ATI location tracking.

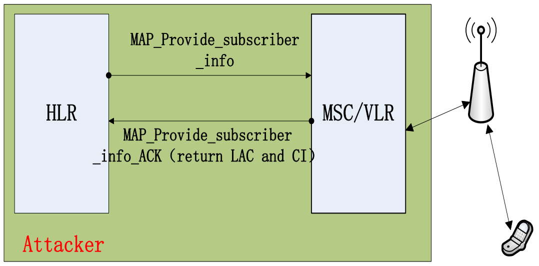

MAP_Provide_subscriber _info
HLR
MSC/VLR
MAP_Provide_subscriber _info_ACK (return LAC and CI)
Attacker

Figure 4. PSI location tracking.

According to the message flow of location tracking, relevant characteristics and detection rules are extracted as shown in Table 3:

Table 3. Characteristics and detection rules of location tracking.

Message	Characteristics	Detection rules
AnyTimeInterrogation (ATI)	opcode is 71. Elements that do not belong to the country of the subscriber send ATI message to subscriber	For each massage, If Opcode='71'and messagetype=98 and (ogt_cc<>msisdn_cc or ogt _cc<>imsi_cc) Then block
		For each massage, If Opcode='71' and messagetype=100 and (dgt_cc<>msisdn_cc or dgt _cc<>imsi_cc) Then block
ProvideSubscriberInfo (PSI)	opcode is 70. Elements that do not belong to the country of the subscriber send PSI message to subscriber	For each massage, If Opcode='70' and messagetype=98 and (ogt_cc<>imsi_cc) Then block

3.2 Interception of calls

The main principle of call interception is that the attacker impersonates HLR to send ISD messages to subscriber and inserts fake gsmSCF addresses. When the subscriber initiates a call to the peer subscriber, the subscriber registers the calling party service and sends an IDP message to the fake gsmSCF to ask for the handling measures. After receiving the IDP message, the fake gsmSCF changes the called number to the elements which is under the control of attacker and the attacker records the content of the call as an intermediary. The analysis of the attack is shown in Figure 5.

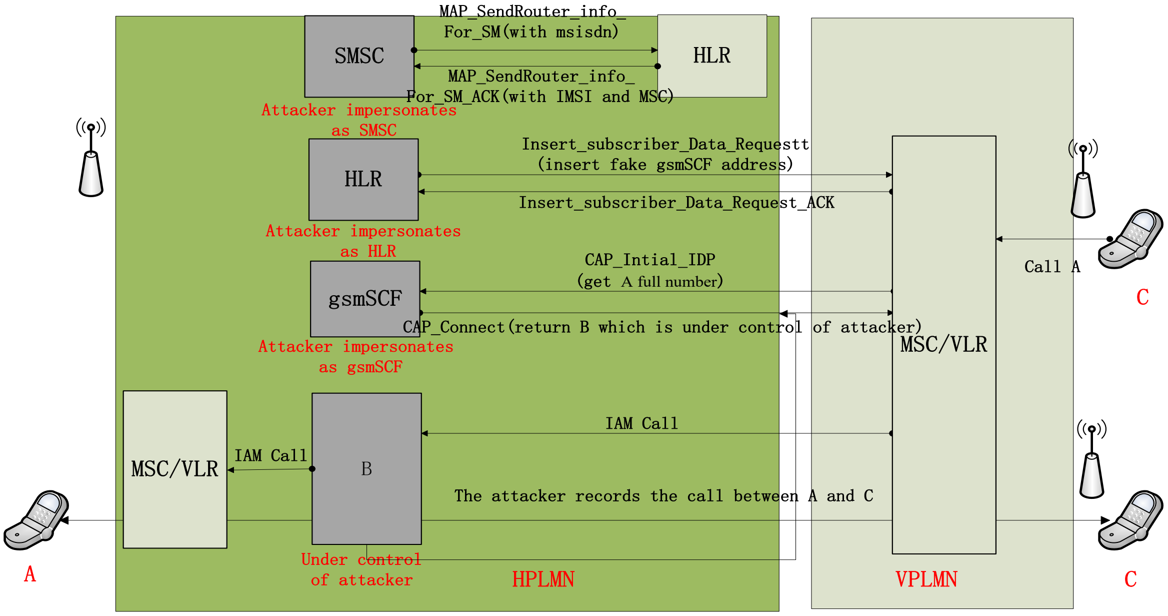


Figure 5. Interception of calls.

According to the message flow of the interception of calls, relevant characteristics and detection rules are extracted as shown in Table 4:

Table 4. Characteristics and detection rules of location tracking.

Message	Characteristics	Detection rules
InsertSubscriberData (ISD)	opcode is 7, and the gsmSCF address inserted does not belong to the subscriber's country	For each massage, If Opcode='7' and messagetype=98 and (gsmscf_cc <> imsi_cc or gsmscf_cc <> msisdn_cc) Then block
InitialDP	opcode is 0, and dgt address does not belong to the subscriber's country	For each massage, If Opcode='0' and messagetype=98 and eventtypebsm=2 and (dgt_cc <> callingpartynumber_cc) Then block

3.3 Interception of SMS

The MAP updateLocation messages are used to inform HLR that the subscriber has moved to a new MSC area, and the interception of SMS works by using a false updateLocation message. Since SMSC sends SRIFSM to HLR which returns the attacker's fake MSC, any SMS sent to the subscriber will be intercepted by the fake MSC. The attacker is now controlling the message and can store it, change it, and possibly forward it to the original subscriber[8]. Specific attack flow analysis is shown in Figure 6:

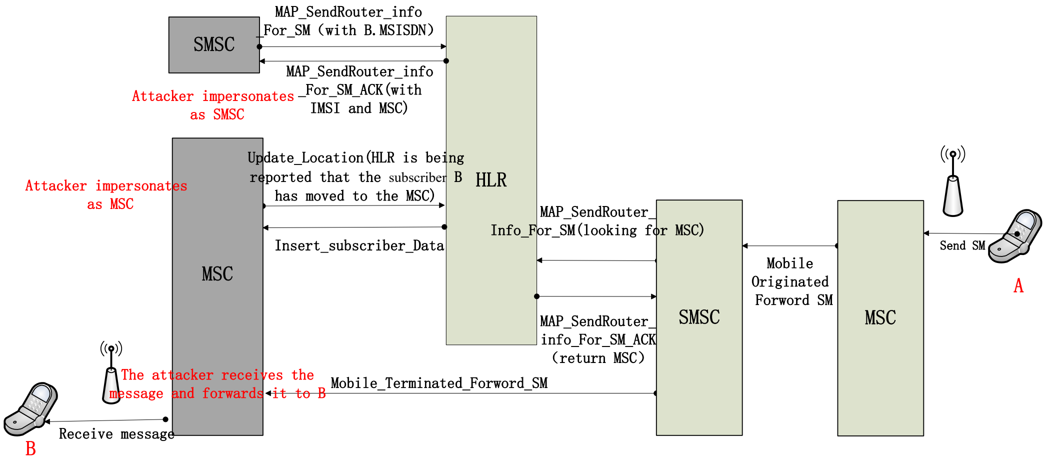

SMSC
MAP_SendRouter_info _For_SM (with B.MSISDN)
MAP_SendRouter_info _For_SM_ACK(with IMSI and MSC)
Attacker impersonates as SMSC
HLR
Attacker impersonates as MSC
MSC
Update_Location(HLR is being reported that the subscriber B has moved to the MSC)
Insert_subscriber_Data
MAP_SendRouter_ Info_For_SM(looking for MSC)
MAP_SendRouter_ info_For_SM_ACK (return MSC)
SMSC
Mobile Originated Forword SM
MSC
Send SM
A
The attacker receives the message and forwards it to B
Mobile_Terminated_Forword_SM
Receive message
B

Figure 6. Attack flow analysis of the intercepting SMS.

According to the principle of SMS interception, relevant characteristics and detection rules are extracted as follows as shown in Table 5:

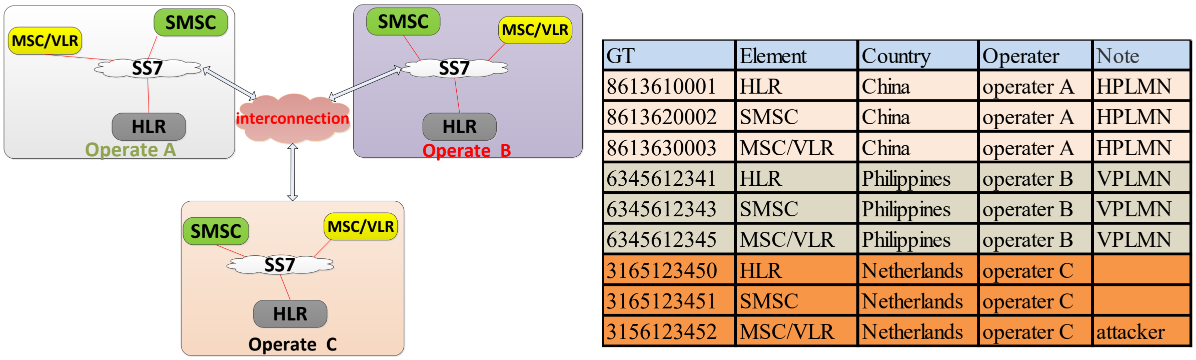
Table 5. Characteristics and detection rules of SMS interception.

Message	Characteristics	Detection rules
Updatelocation (UL)	opcode is 2, MSCS in different countries send updatelocation messages to subscriber's HLR in a short period of time (this method is used to extract subscriber's position jump in a short period of time)	For each massage, If Opcode='2'and messagetype=98 then If |time_message2- time_message1|<60min and ogt1_cc <> ogt2_cc Then block

4. APPLICATION

4.1 The experimental network

Mobile operators must recognize the fact that SS7 is no longer secured. The SS7 network threat detection model need apply as soon as possible. Considering that the SS7 data involved subscriber privacy, the data which used in test modified based on real network, and simulated in the communication among the operate A, B, C. Each operator represents a network connected to the international SS7, the network architecture and the information of the elements are shown in Figure 7.



GT	Element	Country	Operater	Note
8613610001	HLR	China	operater A	HPLMN
8613620002	SMSC	China	operater A	HPLMN
8613630003	MSC/VLR	China	operater A	HPLMN
6345612341	HLR	Philippines	operater B	VPLMN
6345612343	SMSC	Philippines	operater B	VPLMN
6345612345	MSC/VLR	Philippines	operater B	VPLMN
3165123450	HLR	Netherlands	operater C	
3165123451	SMSC	Netherlands	operater C	
3156123452	MSC/VLR	Netherlands	operater C	attacker

Figure 7. The experimental network architecture.

The simulated attack data are generated on the experimental network. All the simulated data are derived from real data and conformed to the MAP message specification. In addition to simulating the normal data, we also simulated the attack data which is initiated by the element of the operate C, and there are five main types : (1) SRIFSM message is used to obtain subscriber's imsi and MSC information; (2) PSI message is used to obtain **subscriber** location information; (3) ATI message is used to obtain subscriber's location information; (4) UL messages is used to Intercept SMS; (5) ISD messages and IDP message are used to Intercept calls. Msisdn and IMSI are used to uniquely represent subscribers in these data.

To test the capability of threat detection model in an SS7 network, we defined that the Person A belongs to Chinese operator A, and roaming in the Philippines operator B. In order to facilitate mobile management, mobile operators need to track the location information of mobile terminals at all times. When person A moves to a new location in startup state, it will report its MSC to HLR through updateLocation message.

4.2 Threat detection application

To detect abnormal data on the network, Tshark is used to collect and parse the original traffic. After the data is preprocessed, it will be imported to the HDFS and be loaded to the Hive warehouse. Then the abnormal attack behavior will be extracted by loading the threat detection model, and the threat alarm information is formed. The detection process is shown in Figure 8.

Through the application of threat detection model in SS7 original traffic, we can extract some abnormal structured messages, as shown in Figures 9-11, and the attack traffic is visualized on the map, as shown in Figure 12.

In the data of location tracking, we can find that the attacker (GT:3165123452) sends SRIFSM message to the subscriber to obtain the imsi of the subscriber, and then the attacker sends PSI message to the subscriber to obtain the cell-level location of the subscriber by imitating HLR.

In the data of call interception, we can find that the attacker (GT:3165123452) sends ISD message to the subscriber to insert fake gsmSCF address (GT:3165123452). When the subscriber initiates a call, the MSC asks gsmSCF for the real phone number of the called subscriber. The fake gsmSCF rewirtes the number to 3165123452 which is under the control of attacker. Both subscribers can talk to each other, while the attacker records the conversation.

In the data of SMS interception, we can find that the attacker (GT:3165123452) sends a false updateLocation message to HLR after the subscriber initiates a updateLocation message in the roaming place, telling HLR that the subscriber has moved to the current MSC (GT:3165123452), then all of the SMS messages sent to subscribers will be routed to the attacker.

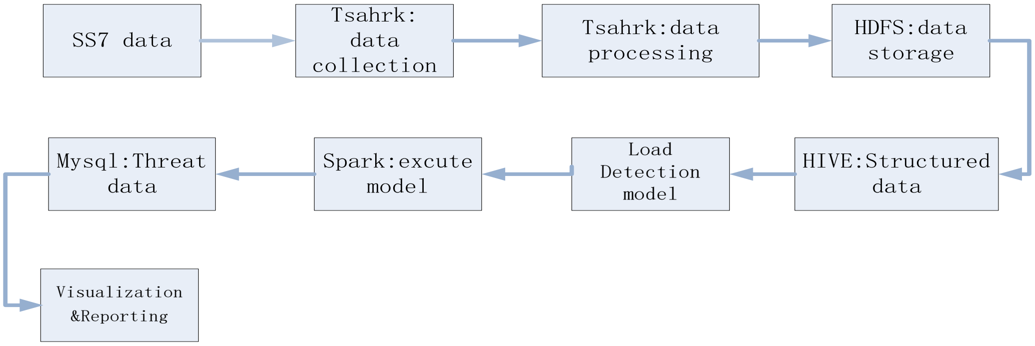
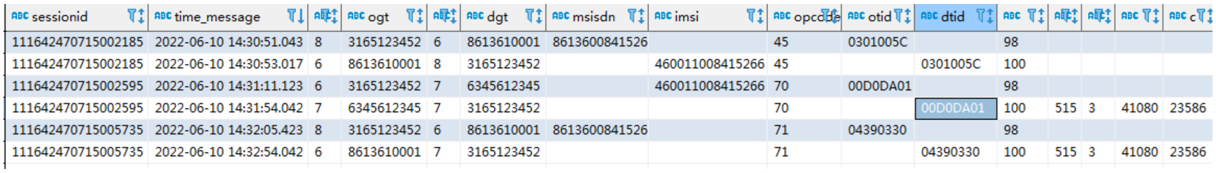
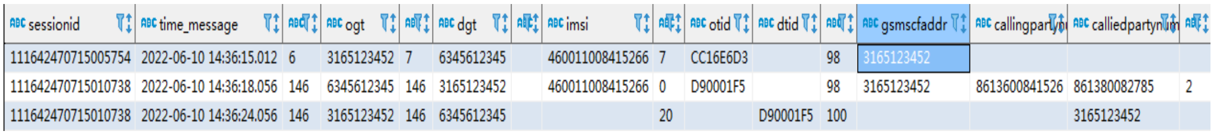


Figure 8. The detection process.



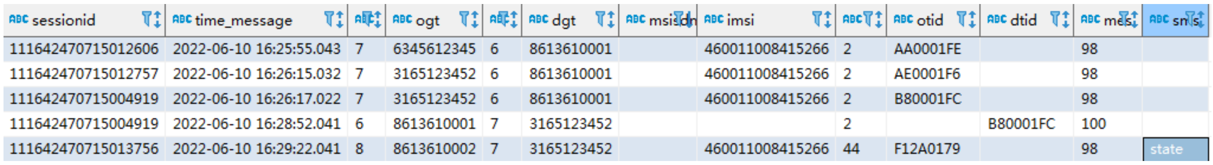
sessionid	time_message		ogt		dgt	msisdn	imsi	opcode	otid	dtid					c
111642470715002185	2022-06-10 14:30:51.043	8	3165123452	6	8613610001	8613600841526		45	0301005C		98				
111642470715002185	2022-06-10 14:30:53.017	6	8613610001	8	3165123452		460011008415266	45		0301005C	100				
111642470715002595	2022-06-10 14:31:11.123	6	3165123452	7	6345612345		460011008415266	70	00D0DA01		98				
111642470715002595	2022-06-10 14:31:54.042	7	6345612345	7	3165123452			70		00D0DA01	100	515	3	41080	23586
111642470715005735	2022-06-10 14:32:05.423	8	3165123452	6	8613610001	8613600841526		71	04390330		98				
111642470715005735	2022-06-10 14:32:54.042	6	8613610001	7	3165123452			71		04390330	100	515	3	41080	23586

Figure 9. The data of location tracking.



sessionid	time_message		ogt		dgt		imsi		otid	dtid		gsmscfaddr	callingparty	calliedpartynum	
111642470715005754	2022-06-10 14:36:15.012	6	3165123452	7	6345612345		460011008415266	7	CC16E6D3		98	3165123452			
111642470715010738	2022-06-10 14:36:18.056	146	6345612345	146	3165123452		460011008415266	0	D90001F5		98	3165123452	8613600841526	861380082785	2
111642470715010738	2022-06-10 14:36:24.056	146	3165123452	146	6345612345			20		D90001F5	100			3165123452	

Figure 10. The data of call interception.



sessionid	time_message		ogt		dgt	msisdn	imsi		otid	dtid	mes	sms
111642470715012606	2022-06-10 16:25:55.043	7	6345612345	6	8613610001		460011008415266	2	AA0001FE		98	
111642470715012757	2022-06-10 16:26:15.032	7	3165123452	6	8613610001		460011008415266	2	AE0001F6		98	
111642470715004919	2022-06-10 16:26:17.022	7	3165123452	6	8613610001		460011008415266	2	B80001FC		98	
111642470715004919	2022-06-10 16:28:52.041	6	8613610001	7	3165123452			2		B80001FC	100	
111642470715013756	2022-06-10 16:29:22.041	8	8613610002	7	3165123452		460011008415266	44	F12A0179		98	state

Figure 11. The data of SMS interception.

Figure 12. The visual interface displays the attack traffic information sent by the attacker.

5. CONCLUSION

In this paper we have described some of the current threats towards the SS7 network, and built threat analysis and detection models for location tracking, interception of calls, interception of SMS, etc. and extracted threat features to form threat detection rules. Based on the simulated network, we generated normal traffic and attack traffic, and carried out the application of threat detection models. These models can also be applied to the real SS7 network to reduce the threat of SS7 network. In future work, we will apply machine learning and other knowledge to further discover unknown threats in SS7 network.

REFERENCES

[1] Tobias, E., “Locating mobile phones using signalling system #7,” 25th Chaos Communication Congress 25C3, 7 (2008).

[2] Eustratios, M., [Attacks on SS7], University of Piraeus, chapter 2, 29 (2019).

[3] Ullah, K., Rashid, I., Afzal, H., Iqbal, W., Bangash, Y. A. and Abbas, H., “SS7 vulnerabilities—A survey & implementation of machine learning vs rule based filtering for detection of SS7 network attacks,” IEEE Communications Surveys & Tutorials, 15 (2020).

[4] Division, “Study paper on SS7 security”, Telecommunication Engineering Centre, (2019).

[5] Tobias, E., “SS7: Locate. track. Manipulate,” 31st Chaos Communication Congress 31C3, 32-37 (2014).

[6] Sergey, P., “Stealthy SS7 attacks,” Positive Technologies, 46-47 (2017).

[7] Kristoffer, J., [Improving SS7 Security Using Machine Learning Techniques], Norwegian University of Science and Technology, chapter 4, 27-28 (2016).

[8] Poornima, P. and Subrata, A., “Signaling system 7: Limitations and resolutions,” IEEE International Conference on Advanced Networks and Telecommunications Systems, 3 (2018).