How to diagnose SS7 Protocol Vulnerability in Roaming Networks

Seongmin Park

Korea Internet & Security Agency, Republic of Korea,

smpark@kisa.or.kr

Received: September 30, 2023; Revised: November 25, 2023; Accepted: December 14, 2023;
Published: December 21, 2023

Abstract

As cellular networks spread to various operators in various countries, access to roaming networks by operators in other countries has become easier than before. As security attacks pretending to be roaming operators increased as the number of security attacks increased as the number of hours that were closed between trusted operators was gradually operated openly. By analyzing SS7 vulnerabilities in roaming networks and reenacting them through simulation, this study establishes a security threat scenario in a real commercial communication environment and builds a pre-simulation test environment that can identify and respond to the presence or absence of proactive measures through security analysis. The simulation test environment can be applied to the actual operational environment to reduce attack damage through pre-defense measures by preparing countermeasures against possible security attacks.

Keywords: Roaming network attack, SS7 protocol, Mobile security threats.

1 Introduction

Early mobile communication networks were closed structures centered on voice calls. It was difficult for attackers to attack and had a limited impact even if the attack was successful because a small number of mutually trusted operators opened communication channels only when needed and operated in a disconnected form to the outside world.

However, since the introduction of smartphones, the global mobile communication market has shifted from voice-oriented to data-oriented, and data traffic has soared, making it an environment prone to malicious attacks due to its connection with heterogeneous networks such as the Internet.

In particular, if you use roaming services not only in South Korea but also when you go abroad, you can connect wherever you are in the world, so you are more likely to be exposed to threats.

In roaming networks, each operator communicates with each other using the SS7 protocol. The SS7 protocol became an international standard in the 1980s, and at the time of its initial design, there was no process called inter-operator authentication because the communication channel was opened only when necessary and kept closed normally between small numbers of mutually trusted subscribers [1]. Even today, when the number of roaming operators increases, the SS7 protocol does not have an authentication process, and users are inevitably exposed to attacks disguised as roaming operators [2].

2 Preliminary

2.1 SS7

SS7 is a telephone network signal protocol developed in 1975 and is used to make or disconnect calls on public switched telephone networks (PSTNs) used worldwide. In addition, services such as number transfer, prepaid plans, and text messages can be performed using SS7.

In North America, SS7 is also called Common Channel Signaling System 7 (CCSS7) and in the UK, it is also called CCITT No. 7 (CCITT No. 7) or CCIS7. In Germany, it is called ZZK-7 (Zentraler Zeichengabekanal Number 7). The SS7 protocol was included in the Q.700 series recommendations issued by ITU-T in 1988 and became used internationally [3]. SS7 has several variants, most of which follow standardized content in ANSI [4] and ESTI [5], and China and Japan operate independently unlike this.

Since the SS7 protocol is also used for roaming, it may also be used for roaming in which a user outside the home network connects to another external network. Both ends of the signaling link are called signaling points (SP). Each SP of the SS7 is uniquely identified by a point code (PC) number. When a signal is exchanged between the SP and the SP, the PC is used to identify the source and destination of the signaling message. Each SP uses a routing table to find a suitable path for each message. The hardware and software functions of the SS7 protocol are divided into functional abstractions called "layers". This level is mapped to the OSI 7 layer defined by ISO, as shown in Figure 1 [6].

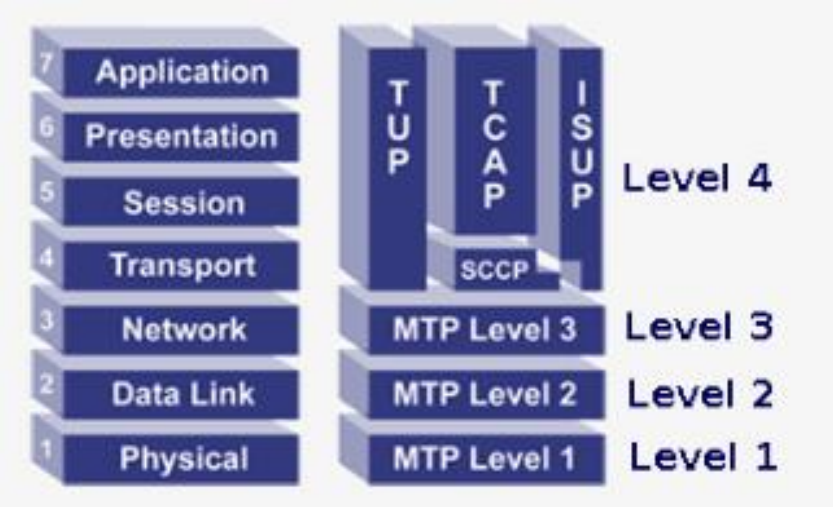

Figure 1. SS7 protocol and OSI layer 7

As shown in Figure 2, the SS7 protocol stack has four layers. Message Transfer Part (MTP) occupies Level 1 to Level 3 and is stable signal transmission using a PC. MTP Level 1 defines requirements for the physical, electrical, and functional characteristics of digital signal links.

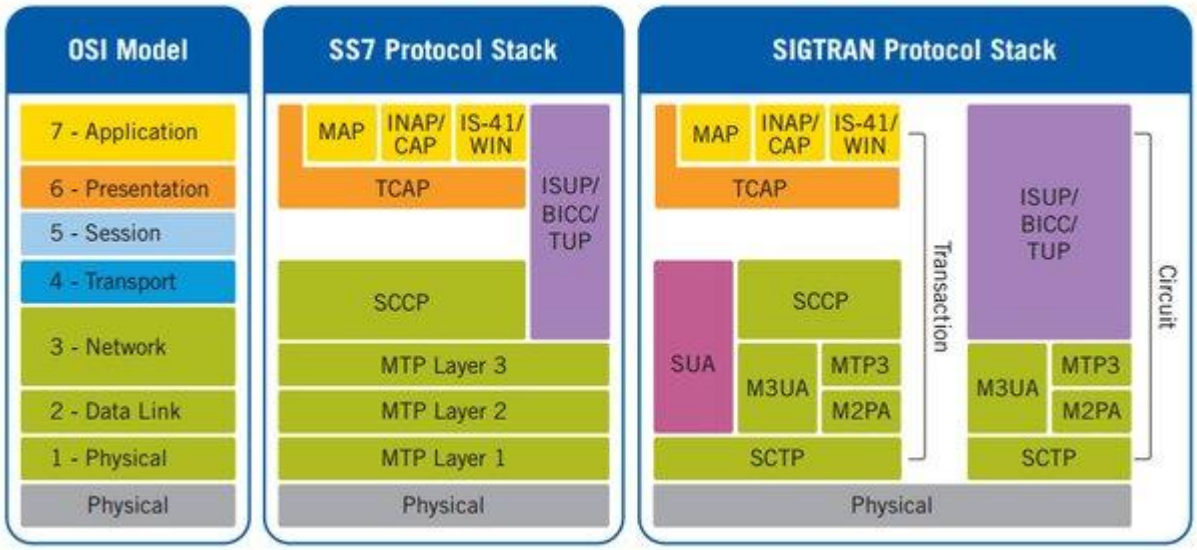

Figure 2. SS7 and SIGTRAN Protocol Stacks

MTP Level 2 specifies signal link functions such as message isolation, error detection, error correction, and supervision. Therefore, it ensures accurate end-to-end message transmission over the signal link. MTP Level 3 provides message routing between SPs in the SS7 network. If a link or SP fails, it is rerouted to a path that avoids it, and if congestion occurs, traffic is controlled. Level 4 is responsible for various services such as SCCP (Signaling Connection Control Part), Mobile Application Part (MAP), and Integrated Services Digital Network User Part (ISUP). Based on the functions of the lower MTP layer, SCCP provides more powerful signal message processing functions such as connection-oriented control, non-connection control, routing, and network management.

TCAP is responsible for processing multiple applications (MSC, HLR, etc.) on a node on an SCCP-based basis. The MAP provides an application layer for communicating with each node of the cellular core network. ISUP defines a protocol used to establish, manage, and release trunk circuits that carry voice and data between end-line exchanges (e.g., between sender and receiver). ISUP is used for both ISDN and non-ISDN calls.

As the Internet develops, IP has become an important means of communication. In accordance with this trend, the SS7 protocol for IP was developed. The SIGTRANS protocol is an extended IP version of the SS7 protocol and enables the same application and call management as SS7. The core of SIGTRANS is to transmit the PSTN signal to the IP using the Stream Control Transmission Protocol (SCTP) protocol. The SCTP also specifies the user adaptation (UA) part to link the PSTN and IP. M3UA (MTP 3 User Adaptation) exchanges signaling messages with MTP Level 3.

2.2 Roaming Interconnection

As can be seen in Figure 3, several nodes in the cellular core network interact with each other to provide roaming services. In a non-LTE network, a Home Location Register (HLR) is a database that includes subscription profile, service data, the current state and location of the subscriber. It also has information that maps IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Station International Subscriber Directory Number). A VLR (Visitor Location Register) has a copy of HLR data, and a Mobile Switching Center (MSC) is responsible for routing calls and text messages. A Short Message Switching Center (SMSC) is responsible for storing and delivering SMS messages [7].

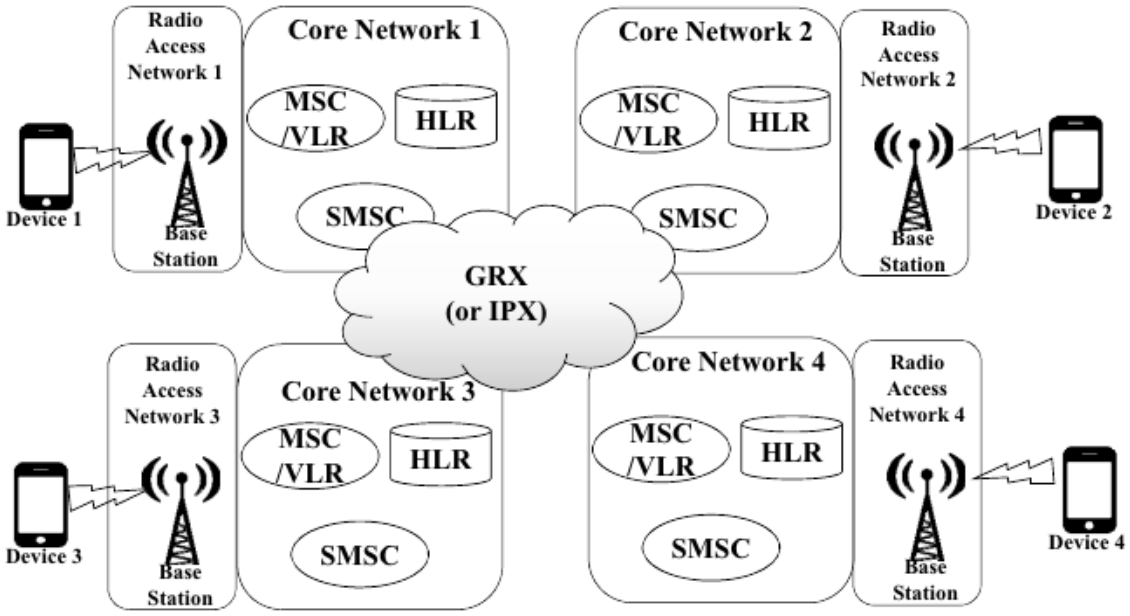

Figure 3. Roaming Connection in a Non-LTE Network

These nodes are identified by Global Title (GT) numbers, and GT is used to route MAP messages in SS7 networks. Each operator's core network is connected by General Packet Radio Service Roaming Exchange (GRX) or IPX (IP Packet Exchange). Roaming services are provided through this interconnection. On the other hand, in LTE networks, the Diameter protocol is used instead of SS7. In a Diameter-based network, all nodes are connected through the IP interface, and operators generally deploy Diameter Edge Agent (DEA) at the network boundary. DEA will be the first location to receive the first message in the part where the network is interconnected. In addition, in LTE networks, Home Subscriber Server (HSS) is used instead of HLR and Mobility Management Environment (MME) is used instead of MSC [8].

2.3 Restcomm jSS7 platform

2.3.1 Restcomm jSS7 Overview

Restcomm jSS7 is an SS7 protocol stack based on Java open source. It provides implementations for MTP2, MTP3, ISUP, SCCP, TCAP, CAMEL, and MAP protocols for dedicated equipment. It also supports SIGTRAN (M3UA) over IP by default and strictly complies with the standard specifications defined by the ITU and ANSI. The platform makes SS7 applications simple and easy to develop because it hides details about sublayers to developers and provides a flexible set of APIs.

Restcomm jSS7 supports TDM equipment that is widely used in the field. If you only want to use M3UA, you can install jSS7 on any operating system that supports Java. However, it is recommended to use Linux to use drivers for SS7 cards, SCTP, etc. Restcomm jSS7 comes with JSLEE TCAP, MAP, CAP, and ISUP resource adapters (RAs) to help developers easily build SS7 applications. Developers only need to understand resource adapters, and the SS7 stack takes care of the rest.

2.3.2 Compliance with implemented protocols and standards

Restcomm jSS7 is a software implementation of the SS7 protocol. It provides implementation of level 2 or higher in the SS7 protocol stack. Restcomm jSS7 does not provide the application itself but

supports users to build their own applications using the API. Table 1 shows related standards for each protocol.

Table 1. Table description

Protocol	Compliance
ISUP	ITU-T Q.761 to Q.764 and Q.767
SCCP	ITU-T Q.711 to Q.716, ANSI T1.112-2000
TCAP	ITU-T Q.771 to Q.775, ANSI T1.114-2000
MAP	GSM 09.02, GSM 29.002, GSM 03.40
CAP	GSM 09.78 - CAMEL Phase - I, II, III and IV
M3UA	RFC 4666

2.3.3 Key Features of the jSS7 Protocol

A. Based on JAVA

Restcomm jSS7 is the only Java - based SS7 protocol stack. It can be installed on any operating system that is powerful, reliable, and supports Java.

B. Open sauce

Software is open source, so it can be modified freely to meet corporate needs.

C. SS7 Hardware Card

Restcomm jSS7 can be used in Intel Family Board (Dialographic SS7 Cards) or Zaptel/Dahdi compatible TDM devices.

D. SIGTRAN (M3UA)

It has built-in support for SIGTRAN (M3UA using SCTP).

E. Flexible and consistent API

It provides an API that abstracts lower layers to support the rapid and efficient development of SS7 applications.

F. Standalone or JSLEE RA

It can also be used as a standalone, and JSLEERA (Resource Adaptor) can be used to manage the stack and develop applications.

2.3.4 Architecture

Restcomm jSS7 is logically divided into two sections, bottom and top. The subsection provides implementations for SS7 level 2 and level 3. Therefore, this section is affected by the type of SS7 hardware used (level 1). The top section provides implementations for SS7 level 4 and above. The top section is the same regardless of hardware, and this structure makes it easy to port other hardware-based applications. The jSS7 protocol stack can be operated independently on one computer as shown in Figure 4, or it can be operated in a form that connects two computers [9].

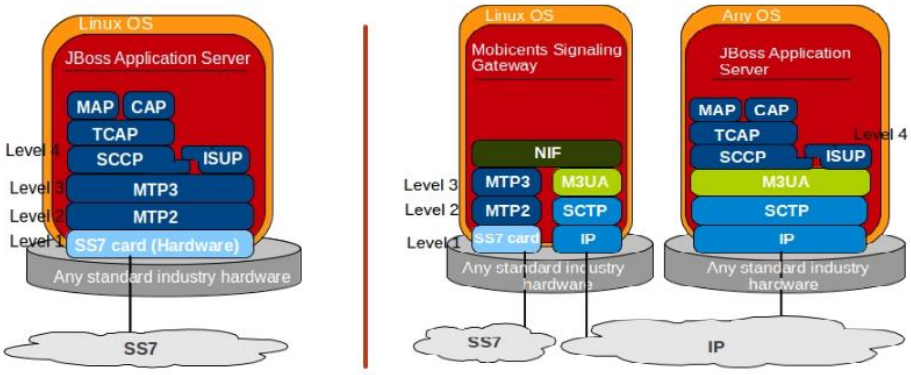

Figure 4. jSS7 Protocol Stack Operations Example

2.3.5 jSS7 Simulator

Restcomm jSS7 is provided with a simulator module that can test and analyze the functionality of the stack. Multiple instances of the simulator can also be run in one folder, and each instance can be given its own option. The set options are saved as xml files. Each simulator instance may have a unique host name, and the simulator may be executed locally or remotely.

3 How to diagnose security threats

Based on the previous analysis, an SS7 roaming network is implemented to perform security measurements in the SS7 roaming network.

3.1 Implementing a Security Measurement Framework

The security measurement framework for SS7 roaming networks may be implemented in an SS7 stack. Implementing an SS7 stack requires considerable time and resources, so we used an open source SS7 stack. Among several open source stacks, we utilized jSS7, a RestComm Java SS7 stack and service that can communicate with Java application legacy SS7 communication equipment. jSS7 provides an open source source implementing M3UA, SCCP, TCAP, CAMEL, MAP and ISUP protocols for dedicated equipment (Dialographic) and M3UA (SIGTRAN) over IP. Based on this protocol stack, messages with security issues are set and implemented to be tested.

In the framework, parameters were reset for each security diagnosis, and the latest MAP message version was set as the default. The version of the MAP message can also be selected, and the overall source code was implemented in the JAVA language. In order to operate the implemented framework, it must run on an operating system that supports SCTP. This is because the SIGTRAN protocol uses SCTP over IP, and for this reason, it may not work on Windows.

3.2 Testing the Security Diagnostic Framework

Security measurement was performed on the test bed of the SS7 roaming network to confirm that the security measurement framework was working properly. As shown in Figure 5, the test bed is configured such that the roaming network is connected by each gateway location register (GLR). A GLR is a VLR or a node between the SGSN and the HLR and may be used by the subscriber across network boundaries to optimize the processing of the profile data. When subscribers roam, GLRs play

the role of HLRs for VLRs and SGSNs in the visiting network, and VLRs and SGSNs for HLRs in the home network. In this case, the MAP message cannot be sent directly to the network nodes of the roaming network such as HLR, MSC, VLR, and SMSC. Job messages that are not supported by GLRs are ignored or deleted from GLRs. Therefore, operators can use GLRs to protect roaming networks and optimize network performance. For security measurements, it is assumed that an attacker is connected to the testbed network through GLR and has a roaming contract with the testbed network. Security measurements were performed under this configuration and assumption.

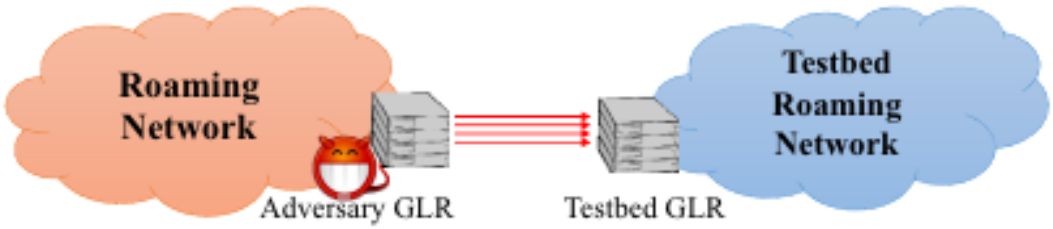

Figure 5. Setting up a test bed for security measurements

Figure 6 shows the result of the security measurement. Most of the security problems found in the security measurement can be targeted at outbound roaming subscribers using IMSI or MSIDSN or both. However, if the MAP-UPDATE-LOCATION message is abused, it targets all subscribers, so in this case, the attacker can intercept the victim's call and text or make the victim DoS state. Therefore, operators should prevent this problem in advance [10-14].

MAP message	Threat Category	Target	Prerequisites
MAP-UPDATE-LOCATION	DoS, Interception	All the subscriber	IMSI
MAP-CANCEL-LOCATION	DoS	Roaming subscriber	IMSI
MAP-PURGE-MS	DoS	Roaming subscriber	IMSI
MAP-INSERT-SUBSCRIBER-DATA *MAP-DELETE-SUBSCRIBER-DATA*	DoS	Roaming subscriber	IMSI and MSISDN
MAP-RESTORE-DATA	Identity leak, DoS	Roaming subscriber	IMSI
MAP-SEND-IMSI	Identity leak	Roaming subscriber	MSISDN
MAP-PROVIDE-SUBSCRIBER-INFO	Location tracking	Roaming subscriber	IMSI

Figure 6. Diagnostic Framework Test Results

4 Security Diagnostic Tool Implementation Results

4.1 Building a Security Diagnostic System

The diagnostic system for security diagnosis of roaming networks was built with Kali Linux, which can install the SCTP library. Restcomm SS7 Simulator provided by Restcomm was used to diagnose the security of the roaming network.

4.2 Network Configuration

The environment for security diagnosis of the roaming network was configured in the vmware virtualization environment as shown in Figure 7 [15].

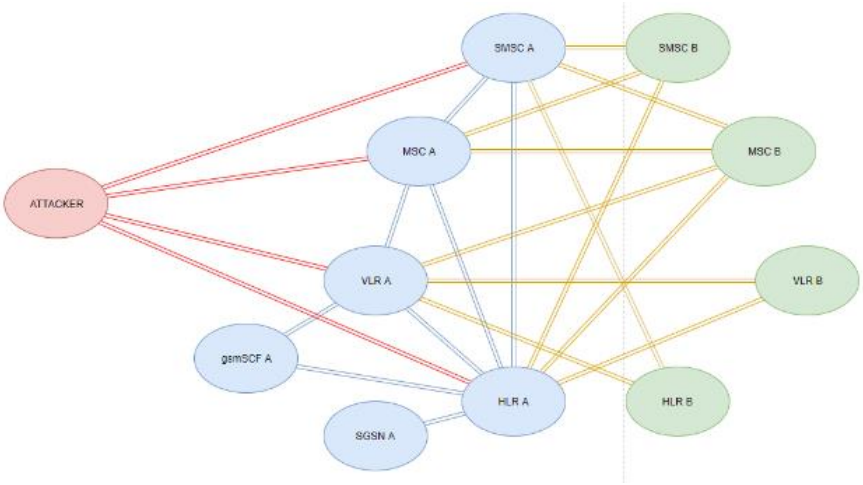

Figure 7. Network Configuration

4.3 Protocol Settings

The Restcomm jSS7 protocol stack is largely composed of four layers, and a common environment is set for each layer, and an environment in which vulnerability tests can be conducted is established. The following shows the settings for each layer for vulnerability execution.

A. Layer 1

Layer 1 uses the M3UA method and uses SCTP as a type to support IP channels. Figure 8 shows the settings for the test.

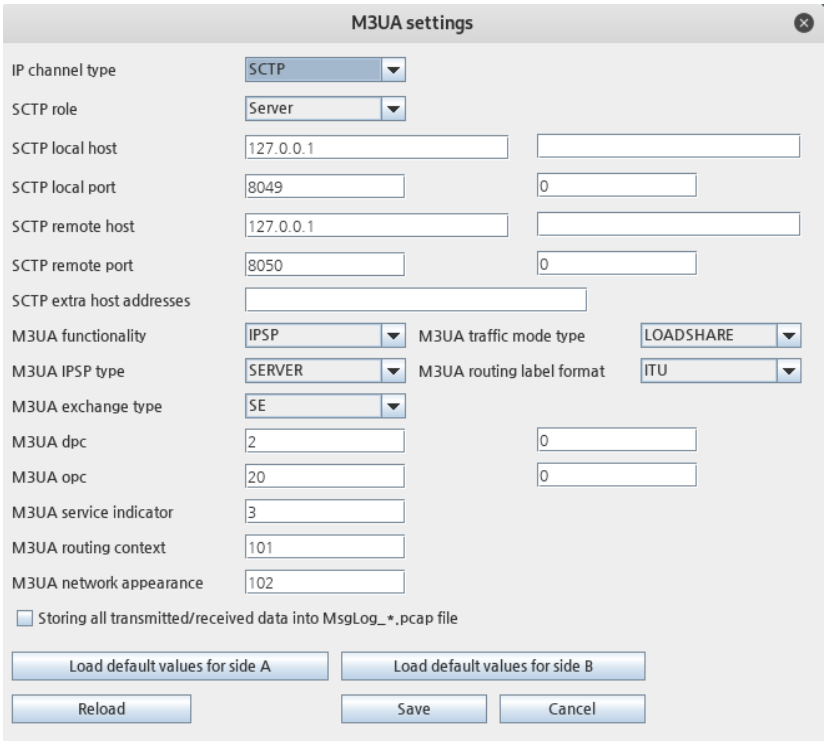

Figure 8. Configuration in Layer 1

B. Layer 2

Layer 2 uses the SCCP protocol, and SCCP specifies two addressing methods. It supports the Point Code + Subsystem Number method and the Global Title method and provides an input interface that may be changed and applied according to information on types and values provided in an actual environment. Figure 9 shows an example of a configuration value for Layer 2.

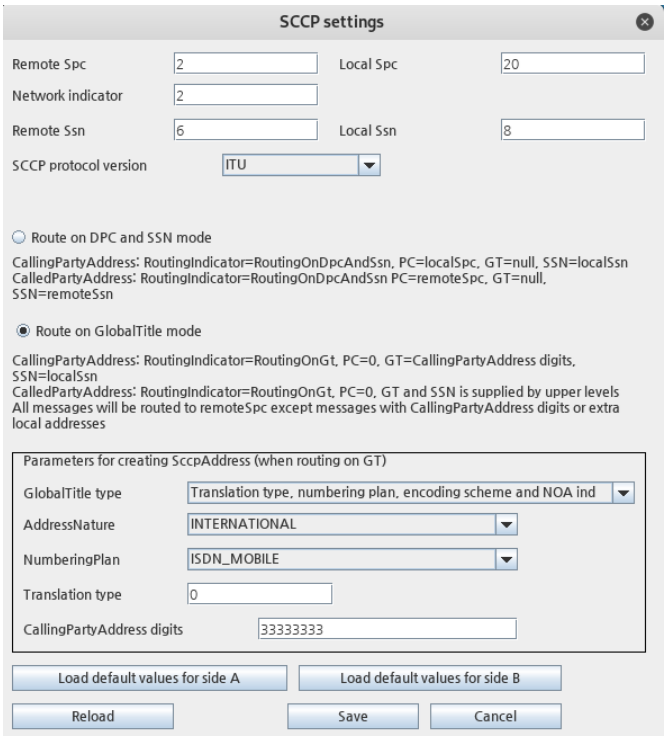

Figure 9. Configuration in Layer 2

C. Layer 3

Layer 3 supports the TCAP+MAP method and the TCAP+CAP method. The environment described as a security vulnerability is the TCAP+MAP method, and Figure 10 shows the configuration values for vulnerability testing.

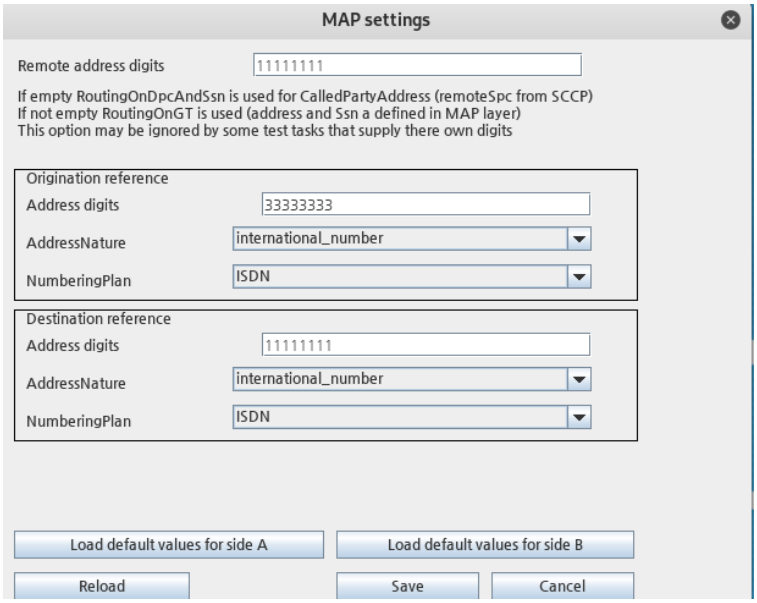

Figure 10. Configuration in Layer 3

5 Conclusion and Future Work

The security problem found in this document is caused by the omission of the authentication part from SS7. Authentication can be provided in several ways. First, public key infrastructure (PKI) based authentication can be considered. When end-to-end encryption using PKI is applied to SS7, most security problems can be prevented. This paper comprehensively investigates security issues in cellular roaming networks. To this end, MAP messages used in roaming networks were analyzed and messages with security issues were extracted. We also found important security issues in these messages [16-18].

In addition, in order to design a filtering mechanism, it was classified as an internal-only or externally available message. The results of this analysis were utilized to implement a security measurement framework for roaming networks. We implemented this framework and performed measurements on the testbed of the roaming network to ensure that the framework worked properly. As a result of the measurement, we found that outbound roaming subscribers can be vulnerable to multiple attacks even if the filtering rules are set correctly at the boundary nodes. In addition, we have proposed a variety of effective measures to mitigate the problems found.

References

[1] De Oliveira, A. and P.-O. Vauboin, Worldwide attacks on SS7 network. Hackito Ergo Summit, 2014.
[2] Engel, T. Locating mobile phones using signalling system 7. in 25th Chaos communication congress. 2008. Citeseer.
[3] ITU-T. Specifications of Signalling System No. 7. Recommendation Q.700, International Telecommunication Union, 1994.
[4] ANSI. American National Standards Institute. .
[5] ETSI. European Telecommunications Standards Institute. .
[6] Ong, L., et al., Framework architecture for signaling transport. 1999.
[7] USSD. Unstructured Supplementary Services Data (USSD). .
[8] Fajardo, V., et al., Diameter base protocol. 2012.

[9] jSS7. RestComm Java SS7 Stack and Services. .
[10] Engel, T. SS7: Locate. track. manipulate. in Talk at 31st chaos communication congress. 2014.
[11] Holtmanns, S., S.P. Rao, and I. Oliver. User location tracking attacks for LTE networks using the interworking functionality. in 2016 IFIP Networking conference (IFIP Networking) and workshops. 2016. IEEE.
[12] Moore, T., et al. Signaling system 7 (SS7) network security. in The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002. 2002. IEEE.
[13] Rao, S.P., B.T. Kotte, and S. Holtmanns. Privacy in LTE networks. in Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. 2016.
[14] Sengar, H., et al., SS7 over IP: signaling interworking vulnerabilities. IEEE Network, 2006. 20(6): p. 32-41.
[15] Lorenz, G., et al. Securing ss7 telecommunications networks. in Workshop on Information Assurance and Security. 2001.
[16] SS7map. SS7map: SS7 country risk ratings. .
[17] Timberg, C., For sale: systems that can secretly track where cellphone users go around the globe. Washington Post, 2014. 24.
[18] Nohl, K. Mobile self-defense. in 31st Chaos Communication Congress 31C3. 2014.