Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-3, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

SS7 Network and Its Vulnerabilities: An Elementary Review

Mamta B. Savadatti[1] & Divya Sharma[2]
[1]M.Tech Communication Systems
[2]Senior Assistant Professor, ECE department
[1&2]New Horizon College of engineering, Bangalore, 2017.

***Abstract**: This paper provides an overview of the SS7 network and protocol. SS7 (Signaling System Number 7) is a set of protocols that describes a means of communication between telephone switches in public telephone networks. SS7 is a powerful and highly sophisticated form of Common Channel Signaling (CCS). SS7 establishes a framework by which data can be exchanged between systems in the network via dedicated signaling channels. It examines vulnerabilities present within SS7 networks whose threat has been magnified by deregulation and emerging trends in network technology. This paper presents few threats into 4 broad categories so the impact to the subscriber and ultimately the network operator can be easily determined.*

1. Introduction

There are two essential components to all telephone calls. The first is the actual content which is our voices, faxes, modem data, etc. The second is the data that instructs telephone exchanges to establish connections and route this content to an appropriate destination. Telephony signaling works for the creation of standards for the latter to achieve the former. These standards are known as protocols. SS7 (Signaling System Number 7) is simply another set of protocols that describes a means of communication between telephone switches in PSTN (public telephone networks). They have been controlled and created by various bodies around the world, which has led to some specific local variations, but the principal organization with responsibility for their administration is the International Telecommunications Union (ITU-T). Originally designed for conveying information related to call establishment and call teardown from different exchanges, the protocol architecture has been extended to cover a variety of tasks associated with collecting and reporting information necessary for the transmission of telephone calls. The SS7 standards include specifications for a wide diversity of telephony management tasks and have been proven to be extremely successful and flexible in it. Due to convergence between packet-switched IP world and public circuit-switched telephone network, SS7 has become the subject of significant attention as developers seek to integrate the two worlds and to hold the best of both. An understanding of SS7 is thus an important component of an understanding of the current and next generation of public networks.

The SS7 network and protocol are used for: Setting up a basic call, management and tear down, wireless services such as personal communications services- PCS, mobile subscriber authentication and wireless roaming, local number portability- LNP, toll-free e.g. 800/888 and toll 900 wireline services, improved call features such as call forwarding, calling party name or number display, and three-way calling, secure and efficient worldwide telecommunications.

2. Background and Historical Perspective

To understand SS7 we must first understand the basic inefficiency of traditional signaling methods used in the Public Switched Telephone Network (PSTN). In the early days of telephony, there was a single wire dedicated to each customer. Switching meant connecting customers together via intermediary pieces of wire. In addition to carrying the conversation or bearer “content,” all telephone bearer trunks also carried the signaling information necessary to control the telephone call concerned. This is known as “Channel Associated Signaling,” or CAS.

The above method is fundamentally inefficient, as it means that even if the destination phone is unable to accept an incoming call, a complete bearer channel is fully occupied, from the point of source to the point of destination, in the attempt to connect to it. Far better would be a way to signal to the destination phone without using the valuable bearer circuit until necessary. This mode of signaling, where the information is carried separately from the bearer channels is known as “Common Channel Signaling,” or CCS.

CCS can also result in the allocation of a single, dedicated resource to signaling and allow it to be responsible for the control of large numbers of individual voice circuits.

SS7 is simply a highly sophisticated and powerful form of CCS. Today, SS7 is responsible for routing calls across countries, between countries, and has a central role in mobile networks.

2.1 SS7 Signaling defined

Signaling System No. 7 - SS7 is a set of telephony signaling protocols, which is used to set up and tear down most of the world's public switched telephone network -PSTN telephone calls. It performs number translation, local number portability, prepaid billing, Short Message Service -SMS and other mass market services.

3. SS7 Architecture

SS7 is built as layered architecture as depicted in figure 1. Each layer plays a specific role. The lowest 3 layers form the Message Transfer Part (MTP) which is responsible for the secure and reliable routing of messages, the content of which is provided by higher layers. MTP uses signaling links for routing messages to their destinations. Higher layers have different functionalities and are implemented as required by the network. Call control (i.e. establishment and disconnection of calls) is handled by one of a series of Layer 4 Protocols, like ISUP or TUP. Other functions are built on top of another layer called SCCP.

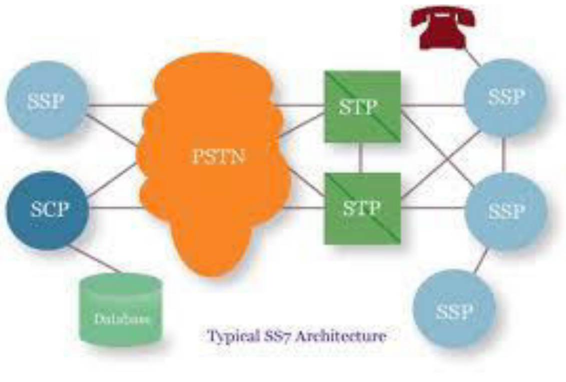


Figure 1. SS7 Architecture.

3.1 SS7 architecture entities

Architecture consists of three different entities:

- SSP -Service Switching Point
- STP -Signal Transfer Point
- SCP -Service Control Point

3.1.1 Service Switching Point (SSP)

The Service Switching Point is the local exchange in any telephone network. An SSP can be a combination voice switch and SS7 switch, or an adjunct computer connected to the local exchange's voice switch. SSPs setup, manage and release voice circuits required to make a call. The main function of SSP is to use the information provided by the calling party and determine how to connect the call. An SS7 message must be sent to this adjacent exchange requesting a circuit connection on the specified trunk. There are few features required from an SSP, to be able to send messages using the ISUP protocol and the TCAP and the network management. SSP's uses a global title to determine how to connect a call using its routing table.

3.1.2 Signal Transfer Point (STP)

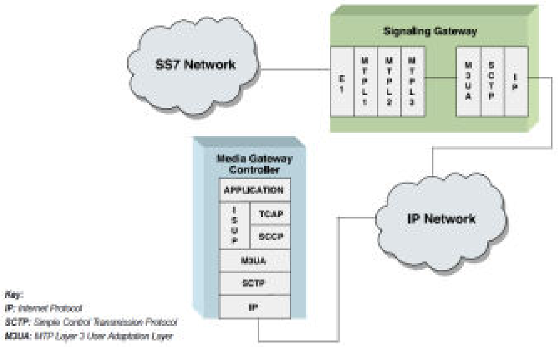
STPs are the SS7 network routers, directing signaling units to the destination signaling points. They are large, specialized devices that often incorporate several racks. Messages to outside destinations must travel through dedicated gateway **STPs.** Messages are not originated by an STP. If an originating SSP does not know the address of a destination SSP, the STP must provide it using Global Title Translation.

3.1.3 Service Control Point(SCP)

SCPs provide database access needed for advanced services. They directly connect to STPs (like SSPs). SCPs are usually software running on a commercial operating system. The address of an SCP is a point code and the database address it interfaces with is a subsystem number. The database is an application entity which is accessed through TCAP protocol. It accepts a query for information from a subsystem at different node. STP performs Global title translation using SCP.

4. SS7 over IP

IP based data transfer is fast growing in the telephony industry. Long distance routing of telephone calls over an IP network is more cost effective than routing using conventional methods. IP access standards are emerging that offer greater flexibility. The SIGTRAN standards, describe a way of presenting SS7 signaling information over an IP transport in such a way that all the benefits of SS7 are maintained. These standards allow next generation IP-based networks to be interfaced with existing SS7 networks and to exchange information with no loss of service capability. SIGTRAN decomposes the original SS7 stack and allows its different layers to communicate using an IP transport layer. The architecture is shown in figure 2. Instead of using MTP as a transport protocol, SIGTRAN separates this from the user parts and transfers the information that would be passed to each layer of an IP infrastructure. A new IP transport protocol i.e. the Simple Control Transmission Protocol (SCTP), has been defined that improves upon previous ones to ensure reliable transfer of information in a way that meets the requirements of SS7 systems. Currently, SIGTRAN is primarily used at the interface between PSTN and IP networks, transferring information from a Signaling Gateway to Media Gateway Controller.

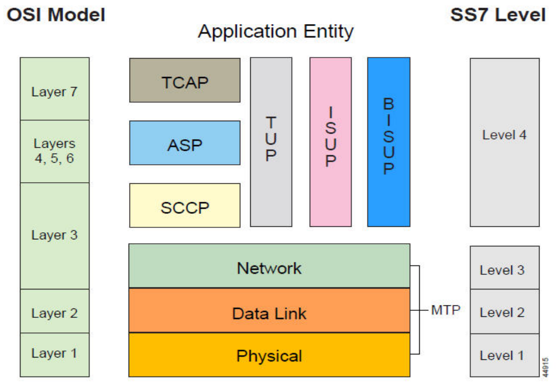


Key:
IP: Internet Protocol
SCTP: Simple Control Transmission Protocol
M3UA: MTP Layer 3 User Adaptation Layer

Figure 2. SIGTRAN Architecture.

5. SS7 protocol stack

Figure 3 shows the SS7 protocol stack. The different levels are as explained below-



TCAP: Transaction Capabilities Application Part
ASP: Application Service Part
SCCP: Signaling Connection Control Part
TUP: Telephone User Part
ISUP: ISDN User Part
BISUP: Broadband ISDN User Part
MTP: Message Transfer Part

Figure 3. SS7 protocol stack.

5.1 SS7 Level 1

The lowest level is MTP Level 1 which is equivalent to the OSI Physical Layer. SS7 Level 1 defines the physical, electrical and functional characteristics of the digital signaling link. Physical interfaces are **E-1** (2048 kb/s with 32 64 kb/s channels), **DS-1** (1544 kb/s with 24 64 kb/s channels), **V.35** (64 kb/s), **DS-0** (64 kb/s), and **DS-0A** (56 kb/s).

5.2 SS7 Level 2

The SS7 level 2 provides the network with sequenced delivery of all SS7 message packets. Like the OSI data link layer, this layer is only concerned with the transmission of data from one node to the next but not to its destination in the network. Sequential numbering is used to determine loss of any messages during transmission. Each link uses its own message numbering type independent of another links. SS7 uses CRC-16 error checking of data and requests retransmission of lost or corrupted messages. Length indicators allow SS7 Level 2 to determine what type of signal unit it receives and how it is processed.

5.3 SS7 Level 3

SS7 level 3 or MTP Level 3 routes messages based on the routing label in the signaling information field (SIF) of message signal units. The routing label is made up of the three fields – the destination point code (DPC), the originating point code (OPC) and signaling link selection (SLS) field. Point codes are nothing but unique numeric addresses, which identify each signaling point in the SS7 network. When the DPC in a message indicates, the receiving signaling point, the message is distributed to the appropriate user part indicated by the service indicator in the SIO. Messages which are destined for other signaling points are transferred if the receiving signaling point has message transfer capabilities (like an STP). The selection of outgoing link is based on information provided by the DPC and SLS.

5.4 SS7 Level 4

Level 4 consists of several protocols, user parts and application parts as shown in figure 4.

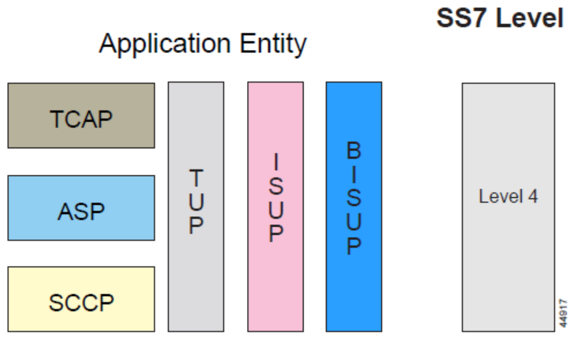


Figure 4. SS7 level 4 protocols.

TCAP
Transactional Capabilities Application Part (TCAP) helps to connect to an external database. Data received is sent back in the form of a TCAP

message. TCAP also supports remote control ability to invoke the features available in another remote network switch.

OMAP
Operations, Maintenance and Administrative Part is an applications entity that uses TCAP services for communication and control functions through the network via a remote terminal.

MAP
Mobile Application Part is used to share cellular subscriber information among different networks. It includes information such as the mobile identification number i.e. MIN, and the serial number of the cellular device handset. This information is used by the IS-41 protocol during cellular roaming.

ASP
Application Service Part (ASP) provides the functions of layers from 4 to 6 of the OSI model. These functions are not presently required in the SS7 network. However, the ITU-T and ANSI standards do reference ASP as viable.

SCCP
Signaling Connection Control Part (SCCP) is a higher-level protocol than MTP that provides end-to-end routing. SCCP is required for routing TCAP messages to their proper database.

TUP
Telephone User Part (TUP) is a protocol that performs basic telephone call connect and disconnect. It has been replaced by ISUP but is still used in some parts of the world like China.

ISUP
ISDN User Part (ISUP) supports basic telephone call connect and disconnect between end offices. It is used primarily in North America, ISUP was basically derived from TUP it supports ISDN and intelligent networking functions. ISUP links the cellular and PCS network to the PSTN. BISUP i.e. Broadband ISUP will gradually replace ISUP.

BISUP
Broadband ISDN User Part (BISUP) is an ATM protocol which is intended to support services such as high-definition television i.e. HDTV, multilingual TV, voice and image storage and retrieval system, video conferencing, high-speed LANs and multimedia systems.

6. Vulnerabilities in SS7 Networks

This paper presents few threats into 4 broad categories so the impact to the subscriber and ultimately the network operator can be easily determined. These categories are:

- Obtaining Subscriber Information
- Eavesdropping on subscriber like SMS and calls – incoming and outgoing
- Financial theft
- Disruption of subscriber service

6.1. Obtaining Subscriber Information

The subscriber information can be used by the attacker or sold on the open market as a source of revenue. There are two types of information gained in this category: The International Mobile Subscriber Identity (IMSI) and the location of the subscriber whether at home or roaming.

6.1.1. Vulnerability 1 Obtaining the Subscriber IMSI
The IMSI identifies a subscriber within the mobile network which is unique. Since the IMSI can lead to other threats it is not transmitted over the Air Interface rather a randomized Temporary Mobile Subscriber Identity (TMSI) is used over the air. However, if an attacker can obtain the TMSI over the air interface and has access to the SS7 network, then the SS7 protocol can be used to ask what the IMSI is associated with the TMSI. An attacker can use the SS7 MAP and its normal procedure for delivering a text message to a subscriber to obtain the IMSI. Once the attacker knows the IMSI due to its format they can also know the home country of the subscriber and home mobile network operator. All the attacker had to have is the telephone number of the target subscriber and access to the SS7 network and a little knowledge about the target subscriber's home SS7 network.

6.1.2. Vulnerability2 Determining the subscriber's location
There are at least two SS7 methods for determining a subscriber's location within the global mobile network. The first utilizes a message and procedure known as *Any Time Interrogation*, which would return the subscribers location parameters. However, many network operators have stopped their equipment from responding to these messages. In the second procedure, the attacker poses like a Fake Home Location Register and uses the normal MAP messages and procedures known as Provide Subscriber information. The information received from this process yields the Cell ID, the Mobile Country Code, Mobile Network Code and the Location Area Code all related to the target subscriber's current location.

6.2. Eavesdropping on subscriber calls (incoming and outgoing)

The vulnerabilities in this category would allow the intruder to listen or to record a subscriber's conversation on incoming or outgoing calls or to intercept and/or modify incoming text messages to a targeted subscriber. Each of these attacks could be performed without the knowledge of the targeted subscriber. The initial information required by the intruder is the mobile telephone number of the target subscriber, little knowledge of the target subscriber's home network and access to an SS7 network. The remainder of the information required can be accessed from the network using the initial information. The attacker can be located anywhere in the world – they do not have to be part of the targeted subscribers network.

6.2.1. Vulnerability 3 Intercepting and monitoring an outgoing call

This is a multi-stage attack where the attacker poses as different mobile network element to implement different scenarios at each stage. This threat uses the Customized Applications for Mobile Networks Enhanced Logic Application Part (CAP) protocol and some logic that allows network operators to define services which are over and above the standard Global System for Mobile communications (GSM) and Universal Mobile Telecommunication Systems (UMTS) standard services. In this threat the intruder has the outgoing call routed to their bridging system or monitoring or recording system and then places a second call path to the original called party and subsequently bridges the two call paths together with the intruder being in the Middle.

6.2.2. Vulnerability 4 Intercepting and monitoring an incoming call

This threat uses the SS7 MAP messaging and procedures for subscriber call forwarding feature. However, it is activated at the SS7 level without the knowledge of the target subscriber. This vulnerability is also a multi-staged attack. It also uses a bridging, monitoring or a recording system to bridge two calls. The intruder call forwards (at the SS7 MAP Message level) the targeted subscriber calls to their bridging, monitoring or recording system. The intruder then cancels call forwarding (at the SS7 MAP Message level) and then places a second call path to the original called party. The intruder bridges the two call paths together with their bridging, monitoring or recording system all without the knowledge of either party involved in the call.

6.3 Financial theft

6.3.1. Vulnerability 5 Intercepting a subscribers SMS (Text) Messages

In this attack the intruder will act like an MSC/VLR and sends an MAP-Update-Location (UL) Request message directly to the HLR subscribers. Upon completion of this procedure SMS messages will be sent to the intruder acting as a Fake MSC serving the targeted subscriber. This attack can be used to obtain targeted subscribers passwords, reset their passwords and once the passwords are reset the intruder can play around with the targeted subscribers accounts.

6.3.2. Vulnerability 6 Manipulating USSD Request

Unstructured Supplementary Service Data (USSD) is currently being used for applications like mobile prepaid, online banking and other financially sensitive applications. Fraud linked to USSD can cause severe financial impacts to subscribers/ to network operators/ to financial institutions and many others. In this multi-staged attack the intruder first acts like a Short Message Service Centre (SMSC) to obtain the Global Title Address (GTT) of the targeted subscribers Home Location Register (HLR), the IMSI of the targeted subscriber and the current serving Mobile Switching Centre (MSC). In the second stage the intruder acts like MSC acting on behalf of the targeted subscriber and requests the subscribers current account balance. After receipt of the account information the intruder acts like the MSC acting on behalf of the subscriber and requests a transfer of funds from the targeted subscribers account to the intruders account. Normally a message is sent to the subscriber indicating the transfer. But if this attack is coupled with Vulnerability 5 then the SMS never reaches the target subscriber.

6.4. Disruption of subscriber service

The two vulnerabilities here can be used to interrupt service to any subscriber or to activate or change billing, thus enabling fraudulent calls to be made from the mobile station. Any of these scenarios cause a significant financial impact on the mobile network operator. One for the fraud and the other for loss of subscriber due to a perceived lack of service.

6.4.1. Vulnerability 7 Disruption of subscriber availability

In this attack the intruder will act like a MSC/VLR and send MAP Update Location (UL) Request message directly to the HLR subscribers. Once the Update Location procedures are complete the Subscriber will not be able to receive any incoming messages or calls until they move to another MSC/VLR or reboot the phone or make an outgoing call. These procedures are part of the usual mobility management in which the subscriber moves to a new area served by different MSC. The intruder spoofs the network into believing that they are now the new MSC.

6.4.2. Vulnerability 8 Manipulating a subscriber's profile in the Visitor Location Register (VLR)

Any time an intruder has access to the subscriber identity i.e. MSIDN and IMSI the address of the serving MSC/VLR and the format of the subscriber profile they can alter billing routing allowing disruption of the subscriber service and use of the subscriber's mobile station to make fraudulent calls.

In this attack, the intruder acts like an HLR and sends fraudulent details of subscriber to the serving MSC/VLR invoking intruder desired services. These services can include bypassing billing services, turning on or off call forwarding, barring calls to the targeted subscriber and many more.

7. Future of SS7

SS7 requirements continue to grow and access to SS7 signaling remains as essential as ever. Indeed, with a growing set of service providers and operators emerging, its importance is certainly increasing. SS7 allows a service provider to maximize their connectivity options and it remains the best way to access the large number of subscriber base stations that connect to the PSTN.

Indeed, for most operators it is the best preferred way of network connectivity and not a matter of choice. SS7 is destined to play a vital role in next generation mobile networks. In the network core, it is likely to remain unchallenged for some quantitative time and with the advent of new IP-based SS7 networks, it is also more likely to play an important role in the next generation of public networks.

The evolution of SS7-based signaling network infrastructure to SIP based signaling infrastructure, or IMS networking does not involve just changing from SS7 to SIP protocols and procedures. It requires a fundamental shift in the network's design to accommodate more types of services, devices and customer preferences. But operators aren't willing to give up the billions of dollars already invested in their existing networks to achieve these changes overnight.

8. Acknowledgements

This work was supported in part by a grant from the National Science Foundation.

9. References

1. Michael Tuxen, *SCTP/SIGTRAN & SS7 Overview*, Foothill College, April 2nd, 2008.

2. Y. Lin, et al., *Wireless and Mobile Network Architecture,* John Wiley and Sons, New York, 2000

3. T. Moore, T. Koslofi, J. Keller, G. Manes, S. Shenoi, *SIGNALING SYSTEM 7 (SS7) NETWORK SECURITY, 2002*

4. Guy Redmill, *An Introduction to SS7*, Brooktrout technology, July 2001.

5. T. Russell, *Signaling system #7*, McGraw-Hill, New York, 2000.