International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

SS7 Signaling Protocol – Security

Garima Sharma [1], Dr. Harish Mittal[2]

[1]Research Scholar, Sat Priya Group of Institutions, MD University, Rohtak, India

[2]Director, Sat Priya Group of Institutions, MD University, Rohtak, India

Abstract: ***In this era of mass surveillance and cybercrimes, numerous attacks are conducted by government agencies and evil hackers on mobile users. Recent report in the media revealed that one of the major government surveillance agencies is collecting bulk information from the mobile traffic. Yet another leaked report from Ukrainian communication regulators (NKRZ) and Ukrainian Security Services (SBU) disclosed that suspicious mobile network packets from one of the telecommunication partners from Russia was revealing location of mobile users and there were high chances that their voice calls were being intercepted. The attacks are serious because SS7, despite its age, remains the main signaling protocol in the mobile networks and will still long be required for interoperability and background compatibility in international roaming.***

Keywords: Attack Mitigation, Attack Analysis, Protocol Stack, SS7, Security, Vulnerabilities, Mobile Network.

1. Introduction

With the vast coverage of cellular networks and more affordable smart phones, the number of mobile users is increasing day by day. The telecommunication sector is growing continuously with a total of 3.6 billion unique mobile subscribers at the end of year 2014 [3]. At present, half of the world population is using mobile phones and subscriptions in their day to day life, and it is estimated that an additional of one billion mobile subscribers will be using telecommunication services at the end of year 2020.

In today's world, mobile networks have not only become the most vital part of communication infrastructure but also a major driving force behind global economic progress and welfare. Repeated incidents of private calls, messages or pictures of government officials, celebrities and businessmen being leaked over the Internet have demonstrated concrete evidence about vulnerability of telecommunication systems. These incidents not only question the capability and responsibility of mobile operators, but also agitate common laymen about their personal privacy. While most attacks in the public eye have exploited weaknesses in the end-device software, less known attacks that exploit weaknesses of the mobile network have also become an everyday problem. This thesis focuses on such attacks against the mobile backbone and signaling systems.

The attackers were able to locate the mobile users and intercept voice calls and text messages.

The attacks are presented in a uniform way, in relation to the mobile network protocol standards and signaling scenarios.

The attacks are serious because SS7, despite its age, remains the main signaling protocol in the mobile networks and will still long be required for interoperability and background compatibility in international roaming. Moreover, the number of entities with access to the core network, and hence the number of potential attackers, has increased significantly because of changes in regulation and opening of the networks to competition.

2. SS7

Signaling System No. 7 is one of the most widely used network architecture and a protocol used for commutations purposes in telephony world. SS7 is standardized by International Telecommunication Union Telecommunication Standardization Sector (ITU-T). This standard articulates specific set of protocol about information exchange over a digital signaling network in the public switched telephone network (PSTN) systems. SS7 is widely used in cellular (wireless) and fixed-line (wire line) for call establishment, billing, routing and information exchange. Though it is not going to last in the industry for various outdated methods and security vulnerabilities, many aspects of SS7 will be replicated in the signaling networks.

3. Application of SS7

Being the backbone of Public Switched Telephone Network (PSTN), SS7 protocol suite has its diverse application across the global telecommunication network. SS7 is also needed each time we make a telephone call which goes beyond local exchange. Despite being used in daily routine for mobile telephony, many of the end users are unaware of its existence or diverse applications.

- Call establishment, management and release.
- Short Message Service (SMS)
- Supplementary services by the mobile operators such as Call Number Display (CND) call waiting and call forwarding.
- Local Number Portability (LNP)
- Toll-free numbers for telemarketing
- Enhanced Messaging Services (EMS) such as logos and ringtone delivery.
- Call blocking (Do-not-call enforcement)

Besides its applications in telecommunication networks, it also acts as a connection to the data communication world by providing features like Internet call-waiting, games based on locations, services which uses browser based telecommunication, Hotspot billing, etc.

4. SS7 Network

Signaling Network Architecture

Definition of signaling according to ITU-T is as follows "The exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls, and network management, in automatic telecommunications operations" [4].

Subscriber signaling happens on the link between subscribers (end users) and the nearby local switch; whereas the signaling that takes place between the nodes of core network is known as network signaling. Network signaling is complex compared to subscriber signaling as it supports various database-driven functionalities such as calling plan validation, Local Number Portability and roaming. Since the SS7 protocol stack comes under the network signaling, the rest of this thesis will consider only network signaling.

Implementation of network signaling is possible by two methods namely Channel Associated Signaling (CAS) and Common Channel Signaling (CCS). In CAS systems, most of the signaling takes place in a deterministic manner. Major disadvantage of CAS based systems is that signaling cannot be done in the in the call connection phase, which imposed limits on signaling states. Another drawback is that the resource allocation is inefficient because of its deterministic nature.

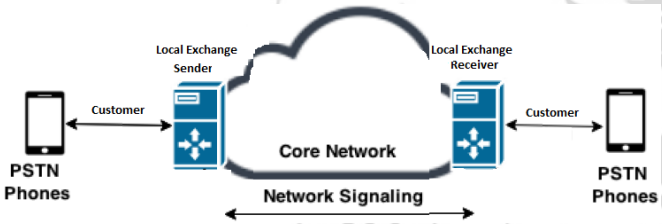

Figure 1: SS7 network signaling

SS7 is a purely CCS based protocol and is packet based carrying 200 bytes of information in each SS7 packet. The advantage of being a packet based approach is that it can support two different ways of signaling:

1) **Circuit based signaling**: This indicates the primary purpose of signaling such as set up, management and dropping telephone calls.
2) **Non-circuit based signaling**: This type of signaling facilitates data transfer between network entities for purpose other than telephone calls.

Since SS7 is based on CCS, it indeed makes sense to know more about it. Signaling mode refers to the type of relationship that the network traffic and signaling path holds. This matters to CCS mainly because of the reason that it is not a fixed path. So the efficiency and performance would matter on the relationship between the signaling modes. The brief description of signaling modes of CCS follows:

Associated mode
Non – Associated mode
Quasi – Associated mode

Figure 2: Switch base signaling

5. Signaling Architecture

SS7 uses bi-directional channels called signaling links where it transfers the messages. These signaling links connect the building blocks of the network known as signaling points. There are three signaling points namely Signal Switching Point (SSP), Signal Transfer Points (STP) and Signal Control Points (SCP). Each of these points is identified by a unique code, and that code will be carried in the signaling message between such the signaling points. This code identifies the source and destination.

Brief descriptions of the signaling points are as follows:

Signal Switching Point (SSP): These are the telephone switches which initiate, switch or terminate calls. They communicate with other SSPs to establish, manage and release voice circuits. They are capable of communicating with SCP's database to check the routing information in case of a toll-free number.

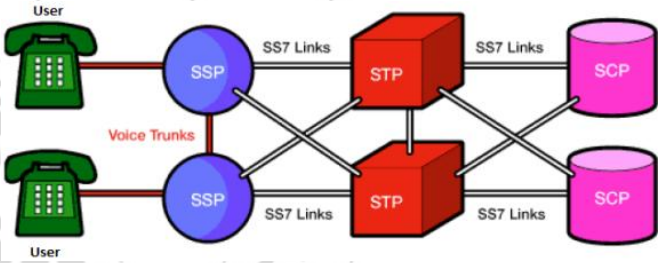

Figure 3: SS7 link

Signal Transfer Points (STP): These are the packet switches which perform routing of incoming signaling message from the source towards the destination based on the information contained in the SS7 message.

Signal Control Points (SCP): These are nothing but databases which aid the services that are supplementary to normal calling. Usually SCPs are deployed in pairs with the STPs for reliability.

6. SS7 Protocol Stack

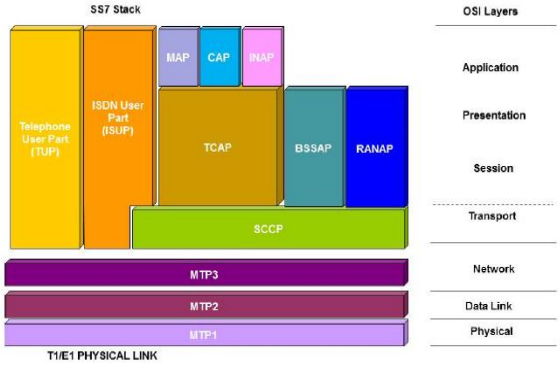

Figure 4: SS7 protocol stack

7. Attacks in SS7

Entry Points to Core Network

The number and complexity of interfaces between heterogeneous network entities pose major vulnerabilities to the SS7 mobile core network. Additionally, expanding interdependence and interconnectivity between the telecommunication networks and Internet has elevated the threats. Changes in the regulation and opening of the telephony industry to competition have given rise to easier ways to get into the mobile core network. For example, the United States "Telecommunications Act of 1996" [5] enforces laws to "*let anyone enter any communication business – to let any communication business to enter any market against any other*" [6]. It also mandates the implementation of Legal Interception Gateways (LIGs) [7] which allows government agencies to lawfully intercept mobile communication. The "Telecommunications Act of 1996" allowed the small scale Competitive Local Exchange Carriers (CLECs) to introduce new trends in telecommunication industry by breaking the monopoly business of Incumbent Local Exchange Carriers (ILECs). Any of the CLECs, including ones established by malicious attackers, can gain access to the SS7 core network at a reasonably low cost [5]. Since STPs and SCPs have human facing frontend systems, an attacker can compromise them in a CLEC environment and thus gain control over the core networks.

By injecting malicious ISDN (ISUP) messages, an attacker can connect to SSPs, which bridges end users to SS7 entry points and hence enter the core network. The attacker can also execute Distributed Denial of Service (DDoS) attacks by overloading the SSP entities beyond its capabilities and harm interconnection between SSPs and STPS [8].

Yet another threat of attacker gaining access to the core network comes from Local Number Portability (LNP) [9]. The Application Programming Interface (APIs) to SCPs to incorporate LNP has been exploited by the attackers to gain knowledge of secret subscriber information and mobile user location

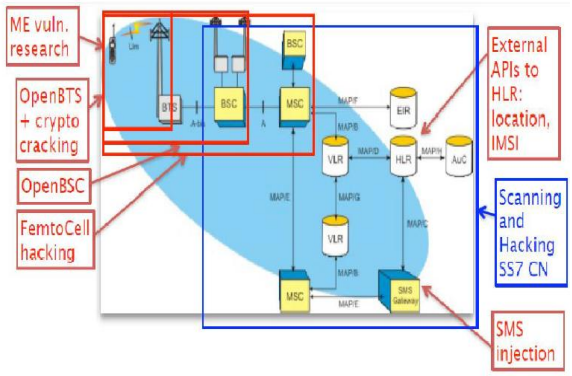

Figure 5: SS7 attacks entry points

8. Attacks Based On Communication Networks

8.1 Attacks based on the GSM networks

The attacker may try to break the encryption of the mobile network. The GSM network encryption algorithms belong to the family of algorithms called A5. Due to the policy of security through obscurity it has not been possible to openly test the robustness of these algorithms.

8.2 Attacks based on Wi-Fi

Access Point spoofing – An attacker can try to eavesdrop on Wi-Fi communications to derive information (e.g. username, password). This type of attack is not unique to smartphones, but they are very vulnerable to these attacks because very often the Wi-Fi is the only means of communication they have to access the internet.

8.3 Bluetooth-based attack

Security issues related to Bluetooth on mobile devices have been studied and have shown numerous problems on different phones. One easy to exploit vulnerability: unregistered services do not require authentication, and vulnerable applications have a virtual serial port used to control the phone.

9. Attacks Based On Vulnerabilities in Software Application

9.1 Web Browser

The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, mobile web browsers are extended from pure web navigation with widgets and plug-ins, or are completely native mobile browsers.

9.2 Operating system

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself.

10. Attacks Based On Hardware Vulnerabilities

In 2015, researchers at the French government agency ANSSI demonstrated the capability to trigger the voice interface of certain smartphones remotely by using "specific electromagnetic waveforms".

10.1 Juice Jacking

Juice Jacking is a method of physical or a hardware vulnerability specific to mobile platforms.

10.2 Password cracking

In 2010, researcher from the University of Pennsylvania investigated the possibility of cracking a device's password through a smudge attack.

11. Future Work

Lots of concepts are left which plays an important role in providing security to the SS7 protocol. As SS7 is still widely used and we can say that SS7 is the largest used protocol in the communication purposes. Thus to provide security to our communication a techniques can be developed in this field. New possible attacks are discovering which can affect the security. To block all such attacks lots of development is needed.

References

[1] A. &. G. B. Soltani, "New documents show how the NSA infers relationships based on mobile location data," Washington Post, [Online]. Available: http://wapo.st/1hrSi9F.
[2] "Taking up the Gauntlet: SS7 Attacks, " Adoptive Mobile, 16 December 2014. [Online]. Available: http://bit.ly/13VDJdi.
[3] G. Association, "The Mobile Economy 2015, " [Online]. Available: http://bit.ly/1Gh19cQ.
[4] International Telecommunication Union, "Vocabulary of switching and signaling terms".
[5] "Telecommunications Act of 1996," US government Publication Office, Public Law 104-104 section 301, 104th Congress, 1996.
[6] "Telecommunications Act of 1996," Federal Communications Corp, 1996. [Online]. Available: https://transition.fcc.gov/telecom.html.
[7] "ETSI TR 101.943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture, " European Telecommunications Standards Institute.
[8] T. Moore, T. Kosloff, J. Keller, G. Manes and S. Shenoi, "Signaling system 7 (SS7) network security," in *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. {MWSCAS}-2002.* 2002.
[9] 3GPP, "3GPP TS 23.066: Support of Mobile Number Portability (MNP); Technical realization; Stage 2".

Author Profile

I, Garima Sharma received the degree of B.Tech (CSE) in 2015 from Sat Priya Group of Institutions, MD University, Rohtak. Presently pursuing M.Tech (CSE) from Sat Priya Group of Institutions, MD University, Rohtak, India.

Dr. Harish Mittal, Director, Sat Priya Group of Institutions, MD University, Rohtak, India