ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

SS7 Signaling Protocol – Attacks Against Privacy

Garima Sharma
M.Tech. Student, Sat Priya Group Of Institutions, MD University, Rohtak ,India
garima.sargam@gmail.com

***Abstract*—: With this era of mass surveillance & cybercrimes, large number of attacks is 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. 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. SS7 is vulnerable to large number of attacks based on number of platforms and factors. Some of them are considered in this research paper.**

***Keywords:* Attacks, Location Tracking, Privacy, Security, SS7.**

I. 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 [2]. 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.
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. The attackers were able to locate the mobile users and intercept voice calls and text messages. 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.

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. 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.

II. 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.

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

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.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

III. 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" [3] enforces laws to "let anyone enter any communication business – to let any communication business to enter any market against any other" [4]. It also mandates the implementation of Legal Interception Gateways (LIGs) [5] 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 [3]. 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.

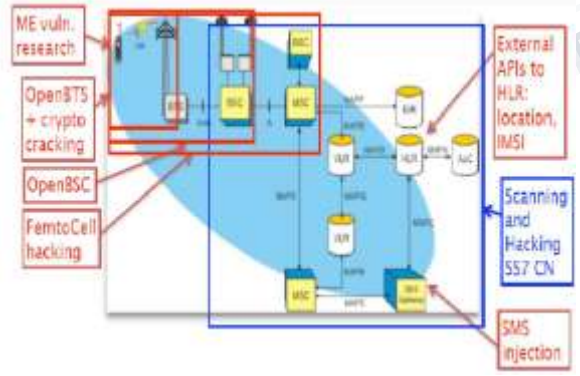


Fig. 1: SS7 attacks entry points

IV. VULNERABILITIES IN COMMUNICATION NETWORKS.

4.1 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. There were originally two variants of the algorithm: A5/1 and A5/2 (stream ciphers), where the former was designed to be relatively strong, and the latter were designed to be weak on purpose to allow easy cryptanalysis and eavesdropping. Since the encryption algorithm was made public, it was proved it was possible to break the encryption: A5/2 could be broken on the fly and A5/1 in about 6 hours.

4.2 Wi-Fi

Access Point spoofing – An attacker can try to eavesdrop on Wi-Fi communications to derive information. 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. Initially wireless networks were secured by WEP keys. The weakness of WEP is a short encryption key which is the same for all connected clients. In addition, several reductions in the search space of the keys have been found by researchers. For small networks, the WPA is a "pre-shared key" which is based on a shared key. Encryption can be vulnerable if the length of the shared key is short.

4.3 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. A phone must be within reach and Bluetooth in discovery mode. The attacker sends a file via Bluetooth. If the recipient accepts, a virus is transmitted.

V. VULNERABILITIES IN SOFTWARE APPLICATION

5.1 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. The exploitation of the vulnerability is importance of the Web browser as an attack vector for mobile devices. Vulnerability in the web browser for Android was discovered in October 2008. As the iPhone vulnerability, it was due to an obsolete and vulnerable library. A significant difference with the iPhone vulnerability was Android's sandboxing architecture which limited the effects of this vulnerability to the Web browser process

5.2 Operating system

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. Vulnerabilities in virtual machines running on certain devices were revealed. It was possible to bypass the byte code verifier and access the native underlying operating system. In theory smartphones have an advantage over hard drives since the OS files are in ROM, and cannot be changed by malware. However, in some systems it was possible to circumvent this: in the Symbian OS it was possible to overwrite a file with a file of the same name. On the Windows OS, it was possible to change a pointer from a general configuration file to an editable file.

VI. LOCATION PRIVACY BREACH

With growing number of mobile phone users, number of services that the mobile user demands is increasing. There exists many location based services in which user allows the application vendors to learn about their location. Mobile phones have become a major part of our daily lives and hence a vital component of our communication and commutation. Since we carry our mobile phones almost everywhere and any time [6], the location information that can be learnt poses as one of the biggest privacy threats. Location and International Mobile Subscriber Identity (IMSI) are co-related and they are protected from outer world as far as technically feasible. Using IMSI catchers the active attackers can collect IMSIs on Radio Access Network (RAN) or air interface. Besides, home network operator can fully track the user location whereas the visited network operator can partially track user location.

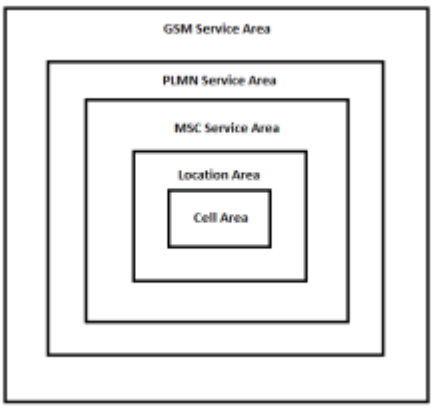


Fig. 2: Location proximity

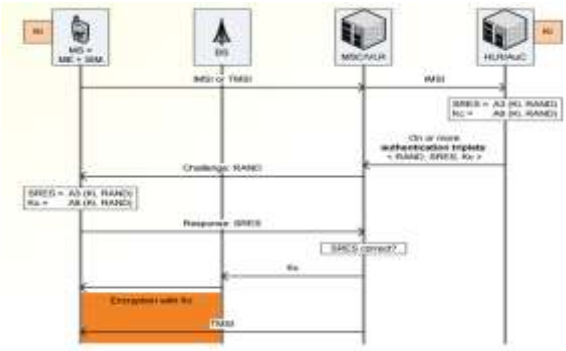
To serve cellular services to appropriate mobile users, mobile networks have a specific geographic hierarchical structure. Such a structure for GSM consists of cell, Location Area, MSC service area, Public Land Mobile Network service area and GSM Service area. Cell being the smallest area of GSM location hierarchy, it ranges from 100 meters to 35 Kilometers. Each cell is identified by Cell Global Identity and it is used for positioning. Multiples of such cells constitute a Location Area. Every time a mobile user moves to a new location area, it will be updated in the VLR database. An MSC Service Area comprises of many such location areas that the MSC can serve. HLR stores the in-formation about MSC that serves a particular mobile station. MSCs are recognized by Global Title (GT).

VII. CALL INTERPRETATION GSM/UMTS AUTHENTICATION MECHANISM

According to GSM/UMTS specification [7], "an intruder cannot deduce whether different services are delivered to the same user". TMSI is used for encrypting over the air traffic for voice calls. However, a new TMSI should be assigned at each change of location. The GSM security model relies on a shared secret between HLR and subscriber's SIM. The security mechanism contains following elements:

1. A 128-bit key shared secret- Ki
2. A 32-bit Signed Response- SRES
3. A Random challenge - RAND
4. A 64-bit session key- Kc

When a mobile is switched on, it reports to the network. HLR sends one or more authentication triplets <RAND, SRES, Kc> to the serving MSC/VLR. Then the MSC chooses a RAND and sends it to the mobile. Using ki stored in the SIM card, the MS generates SRES and sends back to MSC. MSC compares the SRES provided by MS and HLR, and if it matches, session key Kc is provided to base station. This key is used for encryption for every cellular activity thereafter. TMSI is used along with the session key instead of IMSI until a next location update is received.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

Fig. 3: GSM Authentication Mechanism

VIII. SMS BASED ATTACKS

SMS protocol includes two parts [9]. When an SMS is initiated from subscriber A, the MS will contact its MSC which in turn connects to SMSC using Mobile Originated Forward SM message. SMSC looks up for MSC GT and IMSI of the SMS receiver, and dispatches Mobile Terminated Forward SM message towards destination MSC. Below figure explains the two faceted SMS mechanism.

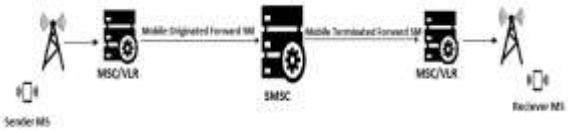


Fig. 4: SMS Mechanism

Since Mobile Originated Forward SM and Mobile Terminated Forward SM messages are not checked for their authenticity, loophole in the SMS protocol leverages the chances of SMS based attacks.

IX. ATTACKS COMMON NOW DAYS

With advancement of recent mobile manufacturing technologies the number of mobile users is increasing day by day as mobile phones are becoming more affordable. According to the World Bank's report [10] in 2012 close to three-quarter of world's population including the developing countries have access to mobile phones. With the increase in mobile phone users, flourishing business in the black market is rising substantially. In United States, 113 phones per minute are stolen or lost; which amass about $7 million worth of smart phones on a daily basis. Recent survey [11] by Lookout, Inc. - a mobile security company revealed that about 25% of the missing phones are left in a public place, where 14% are taken from house or vehicles. Surprisingly the numbers of phone thefts happen through pickpocketing which represents 28% of missing devices.

In 2004, GSM Association (GSMA) has started a Central Equipment Identity Register (CEIR) for methodical recovery or tracking of stolen devices. In spite these advancements by technologists to fortify the mobile phone users, attackers have competitively grown to exploit the vulnerabilities in existing mobile network communication backend to gain illegal control over stolen/missing devices and the private information on them. There exists a growing black market [12] where such devices are sold with least possibility of tracing them.

X. COMMON ADOPTED SOLUTIONS

Some of the best practices that are implemented by various mobile network operators are enlisted below, they are collected & found from various sources over internet:

a. High priority messages like Any Time Interrogation and MAP Send Parameters is purely internal. Hence any such message from an external network should be filtered out.

b. Mobile network operators should completely remove dependency on handing over subscriber IMSI and MSC GT to external networks.

c. Messages like Insert Subscriber Data should be processed only after authenticating the origin of the message. In case if they are originated from external networks or APIs, such requests should be denied.

d. During handovers, it is observed that the attacker exploits the system by intercepting network internal messages before the completion of TCAP handshake. By enforcing MSC/VLR to prosecute the changes requested by the MSCs only after the TCAP handshake completion [13].

e. Any information being sent out of HLR should be filtered based on checking the origin of requester. Messages such as Update Location have to be checked with the previous MSC/VLR to confirm the legitimacy of new VLR.

f. Network operators without roaming agreements should be blocked at interconnect STPs. Transport layer firewalls (Layer 2 firewalls) as part of SCCP Routing Control (SCRC) to enforce legitimate GT and SSN routing [14] can be implemented to provide more security to the system.

g. Mobile operators should educate their subscribers to be aware of RAN network attacks such as IMSI catchers, fake base stations and silent SMS by enforcing them to use user applications such as 'SnoopSnitch' [15] and 'Darshak' [16].

XI. 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] G. Association, "The Mobile Economy 2015," [Online]. Available: http://bit.ly/1Gh19cQ.

[3] "Telecommunications Act of 1996," US government Publication Office, Public Law 104-104 section 301, 104th Congress, 1996.

[4] "Telecommunications Act of 1996," Federal Communications Corp, 1996. [Online]. Available: https://transition.fcc.gov/telecom.html.

[5] "ETSI TR 101.943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture," European Telecommunications Standards Institute.

[6] Y.-C. Hu and H. J. Wang, "A framework for location privacy in wireless networks," inACM SIGCOMM Asia Workshop, 2005.

[7] 3GPP, "3GPP TS 33.102: 3G security; Security architecture," 3rd Generation Security Project.
[8] T. Aura, Lecture notes: Network Security- GSM and 3G Security, Aalto University, 2010.

[9] 3GPP, "3GPP TS 23.040: Technical realization of the Short Message Service (SMS)," 3rd Geneartion Partnership Project.

[10] World Bank, "Information and Communications for Development 2012: Maximizing Mobile," World Bank, Washington, DC., 2012.

[11] "Phone Theft in Europe: What Really Happens When Your Phone Gets Grabbed," Lookout, Inc, May 2014. [Online]. Available: https://www.lookout.com/resources/reports/phone-theft-in-UK.

[12] "The secret world of stolen smartphones, where business is booming," Wired.com, December 2014. [Online]. Available: http://www.wired.com/2014/12/where-stolen-smart-phones-go/.

[13] 3GPP, "3GPP TS 33.204: 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security," 3rd Generation Partnership Project.

[14] Informit.com, Signaling System No. 7 | SCCP Routing Control (SCRC) | InformIT.

[15] SR Labs, "SnoopSnitch," Security Research Lab.

[16] S. Udar and R. Borgaonkar, "Understanding IMSI Privacy," Blackhat USA 2014.