SS7 & LTE Stack Attack

Ankit Gupta
Black Hat USA 2013

akg0x11@gmail.com

Introduction

With the evolution of IP network, Telecom Industries are using it as their core mode of communication for their network elements too. This approach has posed threat to their network by allowing the attacker to get into their network by using common internet tools. LTE is the new generation network which is all IP-based with better performance, scalability and capability. But with the deployment of its new architectural units, the telecom operator engineers lacked the ability for their NGN to be closed and non-penetrable one as it was in the PSTN network. Though the GSM encrypted calls were cracked back in 1998. Now the Telecom Industries have come up with new idea for SIP or Voip calls and other new protocols. This paper illustrates the penetrable techniques into the LTE stack, attacks involving SIP protocols, information gathering, imsi catching and ways to be more secure.

Architectural Elements

IP Multimedia Subsystem (IMS)

In 1990's, captain crunch's blue box came into public's attention when it was used to make free calls over the AT&T networks. The signalling used was in-band in which control and voice signals were sent on the same channel simultaneously. The same way IMS has come up with all-IP networking concept in which core control communication and media services are both done on the IP networks and thus its access to the intruders availed.
IMS mainly utilizes SIP (Session Initiation Protocol) protocol for call setup,

Diameter for AAA (Authorization, Authentication and Accounting) and other protocols like Service Delivery Platform(SDP) and RTP for media control. As it is a new infrastructure added and Voip being the insecure from very beginning it comes up with bugs and vulnerabilities issues. As its core elements are laid on the IP communication architecture with its services can be accessed from any IP network external to IMS for the purpose of calls and data accessibility.

Home Subscriber Server (HSS)

The Home Subscriber Server (HSS) is a master user database that supports the IMS network entities that actually handle calls. It contains subscribers' profiles and subscription details , performs authentication and authorization of the user, and can provide information about the subscriber's location and IP information. It is similar to the Home Location Register (HLR) in GSM.

Proxy-Call Session Control Function (P-CSCF)

This is the first entry point for user equipment(UE) to the IMS. The P-CSCF forwards incoming SIP signalings to UEs and forwards outgoing SIP signalings to the Interrogating-CSCF (I-CSCF). It provides subscriber authentication and may establish an IPsec or TLS security association with the IMS terminal. This prevents spoofing attacks and replay attacks and protects the privacy of the subscriber.

Multimedia management Entity (MME)

It is the first entity which is contacted by enodeB to receive data.Initial authentication of the user by interacting with the HSS and tracking of user takes place over here. It has been merged into MSC/VLR.

Signalling Connection Control Part (SCCP)

It is protocol used for routing packets for internodes communication. It uses Point code and Global Title address to direct the packet to a specific network elements. By default it works on a port 2000 and it is devised by Cisco for their equipments.

Point Code

A Unique number given to each nodes in SS7 network which communicate with each other.
It is of two types-

- OPC Originating Point Code
- DPC Destination Point Code

Global Title and its translation

Global title is unique number used for routing in telecommunication network. It is a number which is used to identify the subscribers internationally.

It is of 3 types-
1. E.164 or MSSIDN which is the standard for North America.
MSSIDN = Country code(CC) + National Destination Code(NDC) + Subscribers Number(SN)

2. E.212 or IMSI is used internationally for identification of subscribers over different mobile operators.
IMSI= Mobile Country Code(CC) + Mobile Network Code(MNC) + Mobile Subscriber Identification number(MSIN)

3. E.214 or Mobile Global Title(MGT) is the combination of both and it is used in rest of the world except North America

The Global title is needed to be converted from E.164 to E.214 when call is made outside to North America and vice versa and also into point code when it enters into the core network to route the signals to the network elements by *Global Title Translation.*

Signalling

The Signaling used in SS7 network is out of band unlike the native signalling technique which was in-band type. Out of band signalling is the signalling which does not takes place on the same path as the conversation. Signalling architecture essentially consist of three components-

Signal Switching Points (SSPs) - are the telephone switches with SS7 software and terminating links. This is used for switching, call setup and termination purpose.

Signal Transfer Points (STPs) - These are the packet switches in SS7 signalling system. They work as a router to relay the packets to the proper destination.

Service Control point (SCPs) - This holds the database and directory to forward the call to the ultimate geographical destination of the number.

Diameter

LTE uses diameter protocol for Authentication, Authorization and Accounting signalling purpose over its network. It is specially made to handle session data on IP-based network and made more reliable by using TCP and SCTP instead of UDP. Diameter security is provided by IPsec and TLS.

SIGTRAN

Signalling Transport is the standard telephony protocol used to transport SS7 signal over internet. A Telephone Company which transmits SS7 signal to a signalling gateway. This gateway, in turn, converts the signal into SIGTRAN packets for the transmission over IP. It is made up of SCTP.

Stream Control Transmission Protocol (SCTP)

SCTP is like TCP with multiple advantages like DoS resilient, 4-way handshake and reliable transport. It is specially designed for easier telephone connection over internet.

Transaction Capability Application Part (Tcap)

Tcap is a protocol used in SS7 network to query an SCP to receive the routing number through messages. Visitor location register(VLR) requests service profile information from the subscriber's home location register (HLR) using mobile application part (MAP) information carried within TCAP messages.

IMSI Catching

IMSI numbers with the help of cell ID (CID) and Location area code(LAC) can help us to track down the user’s current location detail. “Chaos” is an android fully stealthy botnet developed by me which is capable of stealing these details when installed by trick on victims android device. By sending the message with keyword “DED” followed by “imsi” and “cid”, the attacked device replies with these details through message to the attacker without the victim’s any knowledge.
“Chaos” is capable of stealing other private details like IP, messages etc. too.

After we get the imsi, by extracting starting 3 digits we get Mobile country code (MCC), next two digits gives us Mobile Network Code (MNC).
After that putting these details in **http://www.cell2gps.com/** you could track down the users current location.

Capturing SS7 and SIGTRAN packets with Wireshark

To capture SS7, you would need special hardware and a version of libpcap/WinPcap modified to support that hardware.

To capture SIGTRAN you need no hardware as these are the traffic over IP and wireshark supports all these protocols SCTP, M3UA etc.

GSM Sniffing

When someone talks of the security threats in his mobile phone ,the ultimate thought which comes into someone's mind is whether he is been phone tapped or whether his messages is been read by someone nearby.

GSM was created in 1991 providing confidentiality to the users voice with the help of ciphering the voice signal with A5 encryption. Later in the same decade it was cracked and eavesdropping of gsm data is possible with the help of equipments available in the market.
To sniff the gsm packets we need a Fake Base Station available on the Range over networks or Ettus which would communicate with the gsm devices and eventually routing them to the mobile operator's BTS receivers. This is more like a Man in the middle attack. In order to make the subscribers get connected to you, the power of the radio antenna capable of listening GSM traffic is made more than the power of the operator's base station nearby and using no encryption on your antenna that is A5/0.

This makes the all the UE gets connected to it rather than to the legitimate one. Secondly we need OpenBTS which is a software implementation for radio interface which forms the soft PBX like asterisk and soft SIP. After capturing the packet file we could demodulate and decode it in the sniffing tool wireshark to listen to the communication ultimately.

Penetration Testing the LTE

LTE core network and local IP's are visible to UE. By running the traceroute command you can find out the the IPs associated to your ISPs core network.Using scanning tools like nmap, hping, firewalk, netcat it is possible to scan the IMS network to get the knowledge of operating system running on different architectural elements and other open ports and services running on DNS servers, P-CSCF. Hence its possible to get the structure topology of the service provider. The open ports like 22,23, for ssh that could be exploited to get the remote shell by brute forcing both the username and passwords.

SIP attacks

Vulnerability into Voip networks with 5060,5061 ports opened on their network interface could give an entry point to the company's network and also to the IMS network.The SIP servers on the IMS are called P-CSCF and S-CSCF which run on the port 5060 by default. IMS has absence of IPsec protection between user equipment and P-CSCF. There are various ways with which servers running SIP services could be compromised by eavesdropping, masquerading, modifying and denial of service types of attacks. These attacks use the man in the middle methodologies. Since the SIP messages are transferred without integrity and confidentiality protection, the servers running SIP protocol could be potentially scanned and sniffed to he messages exchanged between two users during the setup phase of SIP session in order to get the dialog parameter. By inserting the attacker's IP address in the field "contact" of the SIP header of the 302 response, the attacker redirects

towards himself the successive requests emitted by the victim.

Botnets could be used to get the IP address of the users and thereafter scanning them to find out the services running on the open ports. Then, the SIP applications running on the computers and mobile phones once scanned could be tampered with the help of sniffing tools Wireshark and Cain & abel and its possible to listen their conversation too.
There are number of Voip softphones that are vulnerable to buffer overflow attacks too. By exploiting this vulnerability its possible to enter into someones device after getting the remote shell to the victims device.

Security measures

The deployment of LTE has been done with the thought of its implementation will be carried for long time in future so it is major need for it to be secure. This paper presented the weaknesses of the LTE infrastructure and some of the possible attacks that are needed to be eradicated. Implementation of IPsec protocol between enodeB and evolved packet core could provide better security to the data transferred. Intrusion Detection Systems and deep packet inspection on the SEcurity Gateways(SEG) could keep the network protected from malicious data.