Security Analysis of 4G LTE Networks

Venkatesh Chinta Rambabu Atmakuri

Abstract— The goal of 3GPP Long Term Evolution/System Architecture Evolution (LTE/SAE) is to move mobile cellular wireless technology into its fourth generation. The main unique challenges of fourth-generation technology is how to close a security gap through which a single compromised or malicious device can jeopardize an entire mobile network because of the open nature of these networks. This paper, however, identifies and details the vulnerabilities because the EPC architecture inherits most of the IP-specific security vulnerabilities and also vulnerability in handover key management. So attackers can jeopardize secure communication between users and mobile networks. In this paper, to overcome these key exposures, attacks on IP layer can eliminate by implementation of IPSec.

Index Terms— Attacks, authentication and key agreement, ip layer, ipsec, lte networks, security in lte, security analysis, vulnerabilities

1 INTRODUCTION

The Evolved Packet System (EPS) brings two new major ingredients into the 3rd Generation Partnership Project (3GPP) environment: the radio network Evolved Universal Terrestrial Radio Access Network (E-UTRAN) with a new radio interface, and the Internet Protocol (IP)-based core network Evolved Packet Core (EPC). The flat all-IP architecture allows all radio access protocols to terminate in one node called evolved NodeB (eNodeB). In the Universal Mobile Telecommunications System (UMTS), the functionality of eNodeB was divided into NodeB and the Radio Network Controller (RNC). The placement of the radio access protocols in eNodeB makes them vulnerable to unauthorized access because eNodeB is located in unattended place. Further, internetworking with radio access networks exposes the vulnerability of these networks to direct external threats and carries grave implications for LTE security. Aside from the obvious security risk of intercepted wireless communications transmitted to and from user equipment (UE), there are security risks traditionally associated with the fixed line Internet now pertinent to 4G mobile network operators. This is a significant departure for mobile operators because in prior generations of cellular networks, security was baked into standard network functions and integral to the whole system.

In the LTE networks the main threats are the IP networks open the doors for intruders, hackers, and other malicious traffic generators. The core network is exposed could be exposed due to flatter IP topology. Sniffing on communication between EPC & and other components in the LTE. The style will adjust your fonts and line spacing. Use italics for emphasis; do not underline.

To over come the above mentioned threats the components in the LTE share information between them by implementing confidentiality, integrity and authenticity. The data or traffic must be authenticated in network to over come denial of service vulnerabilities.

In this paper we identified the security vulnerabilities in LTE networks and it leads to defacing network and future key exposure due to desynchronization attacks in handover key management. We provide a solution to eliminate all these vulnerabilities including desynchronization attacks by implementing IPSec protocol. IPSec protocol is designed by Cisco and Microsoft and it has a feature of long term security directional.

2 EPS SECURITY

2.1 Design of EPS Security

The EPS architecture contains mainly Evolved Universal Terrestrial network (E-UTRAN) and the Evolved packet core (EPC). The E-UTRAN supports IP network architecture to deliver data services. EPC will serve as the equivalent of GPRS networks (via the Mobility Management Entity, Serving Gateway and PDN Gateway subcomponents). EUTRAN consists only of enodeBs on the network side. The enodeB performs tasks similar to those performed by the nodeBs and RNC (radio network controller) together in UTRAN. The aim of this simplification is to reduce the latency of all radio interface operations. eNodeBs are connected to each other via the X2 interface, and they connect to the packet switched (PS) core network via the S1 interface. The architectural change has shifted the termination point of the air interface from the RNC in the UMTS to eNodeB in the EPS. Such a termination point would constitute a security weakness.

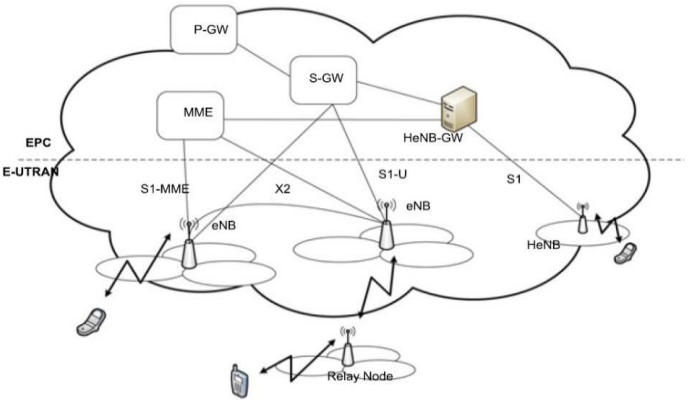
The eNodeB is located at different geographical exposed location and connected to the core network over the IP layer. To make eNodeB secure, there are two layers of LTE security protect traffic passing through it. The first layer, called the Access Stratum (AS) layer (see (a) in Fig. 1), it enables security between the UE and eNodeB. This layer is created when data in radio links need to be exchanged and protects the signaling and user data. In contrast, the second layer, called the Nonaccess Stratum (NAS) layer (see (b) in Fig. 1), remains active whenever the UE is registered to the network and is responsible for securing the signaling in the region between the UE and the Mobility Management Entity (MME). Concerns about insecure links beyond the MME are the responsibility.

A C-plane signaling traffic path, designated as S1-C, is established between a UE and an MME, and a path for the U-plane data traffic, designated as S1-U, is set up between a UE and a Serving Gateway (S-GW). This new change implies not only physically separate paths for these two types of traffic but also separate key management for encryption and

integrity protection.

.

[3] Fig.1: EPS Architecture

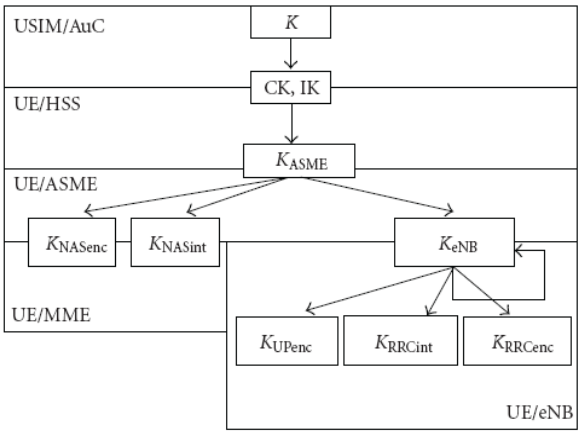


2.2 Key Hierarchy in EPS-AKA

The key hierarchy in the EPS is considerably elaborate and extended for efficient managements of the increased number of keys. The MME hosts the Access Security Management Entity (ASME) to handle access security and acts as a key distributor in the EPS security. The first intermediate keys are derived and distributed to the MME to protect the NAS layer. Further, the second intermediate keys are derived in the MME and distributed to eNodeB to protect the AS layer.

Each time a UE registers itself with an EPS network, an Authentication and Key Agreement (EPS-AKA), occurs between a UE and the MME on behalf of the Home Subscriber Server (HSS)/Authentication Center (AuC). The EPS-AKA is the EPS security mechanism to execute 1) authentication between a UE and an MME on behalf of the HSS/AuC, and 2) a key agreement between a UE and an MME as well as between a UE and eNodeB. Once mutual authentication succeeds the two parties generate the first intermediate key, KASME, from the permanent master key, K. In the course of performing EPS-AKA, the HSS/AuC delivers the first intermediate key to the MME after binding to the serving network identity. Clearly, the evolution to LTE and its flat all-IP core network emphasizes the urgent need for a revision of the trust relationships between operators and network components. Any threats arising from untrusted networks are alleviated in the EPS by a new feature, namely cryptographic network separation. Network separation tries to isolate the impact of any security breach in the local network and prevent its spillover to other networks. This is achieved by binding any cryptographic keys to the identity of the serving network for which the keys are intended. The UE can ensure that it communicates with the intended serving network by authenticating an identity in the current network. In the UMTS, a UE was unable to authenticate a serving network. The local master key, KASME, also called the first intermediate key, is valid at a maximum interval determined by the timing of the next EPS-AKA procedure. The UE can choose to invoke the EPS-AKA protocol whenever the serving MME changes because of roaming to another serving network. In the same situation, the UE also can choose to transfer the security context between the old and new MMEs in an effort to lower the overhead of the full EPS-AKA. The UE may, of course, also need to run the EPSAKA protocol periodically without interrupting service. Hence, the frequency of EPS-AKA runs is rather random or configurable by a network operator. In general, the lifetime of KASME varies from a few hours to a couple of days. As shown in Fig. 2, the MME derives three keys from KASME. The two transient keys, denoted as K_{NASenc} and K_{NASint}, are used for encryption and integrity checks, respectively, of signaling traffic in the NAS. The third key, denoted as K_{eNB}, is the second intermediate key and is specific for an eNodeB and a UE. After being transferred to eNodeB, K_{eNB} is used to derive another three transient keys (see Fig. 2). Among these three keys, two are used to encrypt and check the integrity of Radio Resource Control (RRC) signaling traffic in the AS (i.e.,K_{RRCenc} and K_{RRCint}). The last key is used to encrypt U-plane data traffic in the AS (i.e., K_{UPenc}). The UE should be able to derive from the permanent master key the two intermediate keys, the two transient keys for the NAS, and the three transient keys for the AS.

The key used for the AS protection keys (i.e., K_{eNB}) requires updating whenever a UE serves a different eNodeB as a result of an inter-eNodeB handover. The EPS security uses only a single set of KASME and defines the handover key update without involving an MME. MME involvement at every inter-eNodeB handover levies excessive computational and signaling loads and causes communication delays in the EPC. To avoid these MME problems, the EPS permits the K_{eNB} update to occur directly between eNodeBs.



[5] FIG.2: KEY HIERARCHY

3 SECURITY ANALYSIS

The LTE networks uses flat IP protocol to connect the components such as between eNodeB's or between EPC core and eNodeB's. The0.n EPC inherits the IP Specific Vulnerabilities in LTE networks

3.1 LTE Security Threats

The main threats which are inherited from IP Protocol

1) Eaves Dropping

The attacker knows the information between communication entities.

2) Data Modification

The attacker can tamper or modify the data between the communication entities

3) Identity Spoofing

The attacker can spoof identity and acts as a legitimate entity.

4) Man-in the-middle Attacks

The attacker sniffs the information and gains sensitive information which can achieve by a spoofing attack.

5) Denial-of-Service attacks

The attacker can generate malicious large traffic and it leads to unavailability of resources or network down.

3.2 Attacks

A compromised eNodeB or fake base station is placed in network and then attacker sniffs the user data because IP protocols communicate among the parties in plain-text. Further home eNodeB keys i.e K_{eNB} can be derived by performing only horizontal key derivations. Horizontal keys are derived from old K_{eNB}. Hence the future communications are also exposed. It occurs when by sending spoofed NCC values to target eNodeB at a high value so it only performs horizontal key derivation. The keys are also exposed with out launching desynchronization attacks because all the data are in plain text between eNodeB and MME.

3.2.1 Spoofing Attack

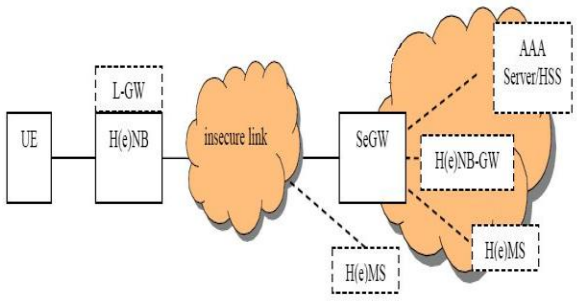
The attacker can spoof and acts as a legitimate eNodeB's or MME then gains user's credentials and exploit it.

3.2.2 Denial of Service

Generation of malicious t1raffic from non authenticated devices leads to network down.

3.2.3 Sniffing

The intruder can intercept all the data among networks by launching a Man-in the-Middle attack which exposes the victim's data. By this attack the attacker knows passwords and



other sensitive information.

[6] Fig.3 Insecure link in LTE network

4 Overview of IPSec

Source [4]: The IPSec standard provides a method to manage authentication and data protection between multiple crypto peers engaging in secure data transfer. IPSec includes the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley and two IPSec IP protocols: Encapsulating Security Protocol (ESP) and Authentication Header (AH)[4].

IPSec uses symmetrical encryption algorithms for data protection. Symmetrical encryption algorithms are more efficient and easier to implement in hardware. These algorithms need a secure method of key exchange to ensure data protection. Internet Key Exchange (IKE) ISAKMP/Oakley protocols provide this capability.

This solution requires a standards-based way to secure data from eavesdropping and modification. IPSec provides such a method. IPSec provides a choice of transform sets so that a user can choose the strength of their data protection.

4.1 How It Works

As with the TCP/IP protocol suite, IPSec protocols work in unison to create a secure communication. The whole process can be broken down into three phases:

- Determine if a communication requires IPSec
- Negotiate and establish a secure connection
- Transmit the data

4.1.1 Step 1: Policy, Selector, and Action

The active IPSec policy and its selectors determine if a communication requires IPSec. If a packet matches a selector within the active policy then the specified action is performed. If that action is only to block or permit a packet then steps 2 and 3 are skipped. The process only proceeds to step 2 if a selector's action is to use AH and/or ESP. It is important to note that if IPSec is enabled on a host then **every** packet goes through this step.

Usually, it is very important to create a mirror of each selector. In other words, if one selector permits traffic from any address to any address on TCP 80 then another rule is required to permit traffic from any address on TCP 80 to any address. This permits the two-way flow of communication. Under W2K, checking Mirrored automatically creates the mirrored selector. Other platforms may require that the mirrored selector be entered.

4.1.2 Step 2: IKE

IKE creates the keys that the subsequent steps will use to encrypt and sign packets. However, IKE is faced with a problem. If those keys are sent over an insecure connection then someone could "steal" those keys and view or modify the packets we are attempting to secure. In essence, IKE is faced with a chicken and egg problem: a secure connection requires keys but it can't send the keys until it has a secure connection. To tackle this problem IKE is broken in to two phases. Phase 1 solves the problem of creating a secure channel over an insecure connection with a mathematical algorithm that permits anyone to view the communication occurring between the hosts and yet be unable to capture or predict the key that results from this communication. This algorithm is called the

Diffie-Hellman (DH) key exchange.

When configuring Windows 2000 IPSec, there are two DH groups to select from: Low and Medium (there is no High). The important thing to know about DH groups is that it determines the strength of the phase 1 keys that are generated. It is strongly recommended that Medium be selected.

Unfortunately, DH is extremely CPU intensive. As a compromise W2K, as recommended by the RFC, only generates a DH key at the start of a communication and not for each packet sent. In fact, the same DH keys can be used for multiple, independent communication streams between two devices. If necessary, IPSec can be configured to generate new DH keys for each communication and periodically recreate those keys during a communication.

Phase 2 uses the DH keys to create a secure channel. This secure channel is used to create a subsequent set of keys that AH and ESP will use to encrypt and sign packets. It is important to note that phase 2 requires the phase 1 keys to work.

1. Device A communicates to Device B using IKE on UDP 500
2. Each side generates a Diffie-Hellman key
3. Device A and Device B create an encrypted connection using the keys from step 2
4. Device A and Device B negotiate the highest level of security supported on both devices
5. Device A and Device B create phase 2 keys for use with IPSec (AH and/or ESP)
6. IPSec communication (AH and/or ESP) begins using phase 2 keys created in step 5

Step 1 deserves some special attention. As mentioned earlier IPSec can act as a packet filter: passing packets that match a selector or dropping packets that do not match. IKE is treated specially by IPSec: UDP 500 is automatically accepted. If it were not then a chicken and egg problem would arise: device A needs to negotiate a secure channel with device B, to do so it must connect on UDP 500, in order to make that connection it must establish a secure connection, to do so it must connect on UDP 500…. Obviously this is unacceptable. The IPSec RFCs require that IKE packets are recognized as such and processed appropriately.

4.1.3 Step 3: AH and ESP

AH and ESP perform separate but similar functions. AH verifies the identity of the sender using IKE Phase 2 keys to sign the IP packet (authentication and integrity) and keeps track of the packet sequence and lifetime of the phase 2 keys (anti-replay). AH does not encrypt the packet (confidentiality) and it works at the network layer. ESP can verify the identity of the sender, sign the transport layer, and keep track of the packet sequence. However, it also has the ability to encrypt the packet, but only encrypts the transport layer and higher.

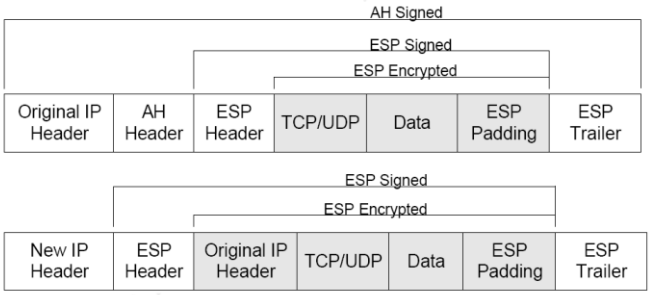
Both AH and ESP are available in Transport and Tunnel mode. As discussed previously, Tunnel mode encapsulates the entire packet. Although AH supports tunnel mode, in practice it is not usually deployed in this fashion since it provides no additional protection over Transport mode. If tunnel mode is required, ESP is typically used. Since ESP tunnel mode protects the entire original packet AH is not necessary.

As can be seen, the header and trailer are not encrypted. AH keeps its HMAC in the header and ESP stores its HMAC in the trailer. When the destination device receives the packet it calculates the HMAC and compares it to the HMAC in the trailer. Not encrypting the HMAC allows IPSec to quickly determine if the packet has been modified and, if so, discard the packet.

4.1.4 Interacting With IPSec

Years of experience with IPv4 have exposed us to various aspects of TCP/IP communication: transport protocols have port numbers, NAT and proxy servers have become standard networking features, we have learned to accept replay attacks as vulnerability, and Network IDS is considered a requirement by many security professionals. IPSec changes the rules on how and what we deploy in our networks and in some cases we no longer need accept certain limitations of TCP/IP.

Figure 4 The IPSec Transport mode and tunnel mode



Unlike many transport layer protocols, such as TLS, TCP, and UDP, ESP uses only a protocol number. AH also uses a protocol number as is typical of network layer protocols. Specifically, AH uses protocol number 51 and ESP uses protocol number 50. If the two are used together then the protocol number of the outer most protocol is exposed. AH and ESP in transport mode will expose protocol 51 whereas ESP in tunnel mode and AH in transport mode will expose protocol 50.

As was mentioned in previous sections, AH and ESP may not work with a proxy server or NAT. More generically, IPSec, in either transport or tunnel mode, does not work with a device that modifies an IP packet. This is because AH and ESP sign their portions of each packet. AH signs the entire IP packet with the exception of a few fields that must change in normal IP communication (such as TTL). Tunnel mode allows the new IP header to be modified enroute, unless AH in transport mode is also used, but the rest of the packet is still off limits. The result is that regardless if you use AH or ESP the payload is always off limits for modifications, tunnel or transport, and the IP and transport header information may also be off limits.

Recently Network and Host IDS have become an important tool in the security professional's toolbox. NIDS are basically protocol analyzers. They capture packets on the network, analyze the packets to determine if it is malicious, alert security administrators of malicious packets, and in some cases will terminate communication containing malicious packets.

All IDS' work on the premise that the packet is transparent

and that the contents are in an expected position. IPSec complicates this by encrypting portions of the packet, ESP, or moving the location of parts of a packet, tunnel mode. The solution will depend on the organization. Tunnel mode moves the original IP header and Transport layers from the expected location within the packet. However, tunnel mode is almost exclusively used between gateways. NIDS will need to be located inside of each gateway, prior to IPSec tunneling being applied, to permit the NIDS to work. Since transport mode does not relocate important packet information, in principle NIDS will work with transport mode. If ESP is used with encryption there is no simple solution, however. One solution is to not use ESP with encryption on a network that requires NIDS. Another solution is to use ESP in tunnel mode to a gateway. Once at the gateway the IPSec is decrypted and available for inspection by NIDS before reaching the next gateway, which encrypts the packet before sending it to the final destination. Potentially a Host IDS that provides packet analysis can be used. This solution only works if the HIDS is able to inspect the packet after the packet has been decrypted. HIDS solutions can quickly become extremely expensive since every host in the network requires the software. Replay and man-in-the-middle attacks are difficult to protect against. Fortunately, they are somewhat difficult to carry out since they require direct access to the network the systems use. Replay attacks capture the packets of a real session, alter the packets, and then retransmit the packets. The end-point hosts believe they are communicating directly with each other, but in fact they are communicating with a server in between. This is attack is extremely difficult to detect. As has been mentioned many times, IPSec provides anti-replay protection. This is done by using a sliding window. IPSec gives each packet a sequence number. If a 64- packet sliding window is used then a host will accept packets 1 – 64 without problem. When packet 65 arrives the host will no longer accept packet number 1. Likewise, when packet 100 arrives, any packets below number 36 are dropped. In addition, IPSec does not accept duplicate sequence numbers. In other words, once packet 125 arrives for a given IPSec session, IPSec does not permit another packet 125. This also means that IPSec keys must be renegotiated and a new IPSec session established before IPSec sequence numbers wrap. This scheme makes replay attacks very difficult since the attacker only has a narrow window of time to retransmit the packet. IPSec provides only limited man-in-the-middle protection. This protection is dependent on authentication method selected. In W2K, 3rd party certificates, Kerberos, and shared secret are supported. Of these, only 3rd party certificates provide strong man-in the- middle protection.

5 Simulation

In NS3 (Network Simulator), it has a lot of modules, known as networking models. We consider LENA module which is used for LTE Simulation in ns3 simulator. LENA was developed by CTTC and it is open-source project.

By using LENA module we ran a simulation with enabling traces and packet capture i.e: pcap in LTE simulation code. After simulation the LTE code, it produces pcap files, traces and stats. By these results we can understand the complete message flow in LTE networks. Pcaps is a library function in ns3 that captures all packets in network.

To understand pcap a special tool, Wireshark is used. It analyzes the packets from top layer to bottom layer. LTE uses flat IP and due to this all the data in the network is in plain text. We can read information what the user or entities send. All the data is exposed in pcap file. In the same manner the attacker also captures in LTE network and exploits the results.

5.1 Implementation of IPSec

We simulated IPSec protocol in GNS3 or in Cisco Packet Tracer. Every eNodeB and other components in LTE network such as MME, HSS and other components consists of networking devices like router, switches and etc. Now we are considering two routers at two eNodeB's and IPSec protocol between them was established as show in figure below. In order to establish IPSec in their routers we have to configure IOS commands in those devices. We selected Diffie-Hellman Key exchange protocol for encryption and authentication, for integrity we selected a HMAC signature mechanism.

Fig 5 Simulation output in Cisco Packet Tracer

In GNS3 tool we can capture packets in network and we can understand by the Wireshark tool. All the data between entities is encrypted and protected with integrity. If an attacker sniffs the traffic then the data can't decrypt with out a key.

By this implementation of IPSec the communication between peers is encrypted and protected by HMAC signature. The IPSec protocol *protect* from following attacks they are:

1) Eaves Dropping
2) Data Modification
3) Identity Spoofing
4) Man-in the-middle Attacks
5) Denial-of-Service attacks

6Conclusion

We were concerned that forward key separation in handover key management in the 3GPP LTE/SAE network can be threatened because of what are known as rogue base station attacks. Although by implementing IPSec between base stations minimizes the effect of the attacks.

Acknowledgments

Our work is mainly derived from "Security Analysis of Handover Key Management in 4G LTE/SAE Networks" by Chan-Kyu Han and Hyoung-Kee Choi and "IPSec" by Scott Cleven-Mulcahy.

REFERENCES

[1] "3GPP System Architecture Evolution (SAE); Security Architecture (Release 11)," 3GPP TS 33.401, Version 11.2.0, Dec. 2011.

[2] "Security Analysis of Handover Key Management in 4G LTE/SAE Networks" Chan-Kyu Han and Hyoung-Kee Choi

[3] "A Robust Secure DS-AKA with Mutual Authentication for LTE-A M. Prasad and R. Manoharan

[4] "IPSec Tutorial" by Scott Cleven-Mulcahy,SANS Instiute.
[4] CISCO IOS for more information refer www.cisco.com.
[5] A USIM-Based UniformAccess Authentication Framework inMobile Communication Xinghua Li,1 JianfengMa,1 YoungHo Park,2 and Li Xu3
[6] Cisco Packet Tracer Software available at www.cisco.com
[7] Source Internet

Venkatesh Chinta received Bachelor of Technology in 2011. He is pursuing his M.Tech programme in Computer Networks and Information Security, Malla Reddy College of Engineering,Hyderabad.

A.Ram Babu M.Tech working as a Assistant Professor in CSE Department at Malla Reddy College of Engineering, Hyderabad.