Chapter 7

Identifying and Mitigating Security and Privacy Threats in Modern Telecommunciation Infrastructure

Abdulrahman Yarali, Nagaraju Pureti, Nisha Ganster, Justin Davidson

Telecommunication Systems Management, I.E., Murray State University

ayarali@murraystate.edu, npureti@murraystate.edu, nganster@murraystate.edu, jdavidson5@murraystate.edu

Abstract

There has been a tremendous change in technologies and businesses. These changes forces the companies to come up with new models and compelling new ways to attract customers and reach new markets. Personal information is not protected by businesses, governments, or unethical private information seekers. When users plug in, log on, connect, agree to the "terms and conditions" on any technical device with internet access, GPS, networking capabilities, or merely swipe a customer loyalty card, leaves data traces of every aspect of you. This data is collected (mined) and data of this data (metadata) is also collected, analyzed, and turned into the most powerful and precious resource available, information. This chapter examines the power of information and personal power over personal information, collected through telecommunications systems without protection from arbitrary or unlawful interference by commercial, governmental, or civil violations of user privacy in regards to family, home, or correspondence. Threat and security of modern IP- based 4G LTE mobile communication networks which are expected to provide novel applications such as streaming video and conferencing, Web 2.0 and mobile TV are discussed. 3GPP algorithms and security functions into the overall EPS, SAE architecture of 4G LTE are discussed.

Keywords:
Information and communication, Privacy and threat, 4G Wireless and mobility, security algorithms and functions

Introduction

Industry environment:

At an increasing rate consumers and business are each utilizing networks to accomplish everyday tasks. Some of these networks exist strictly within the parameters of the home or office building, while others are public networks found within the community; in either case these networks typically have access to the outside world or have the ability to be joined by those with malicious intentions. Add to the network the use of wireless routers and access

Email:ayarali@murraystate.edu

points, along with mobile devices such as tablets and cell phones, and the threat to have information and data stolen or corrupted increases. A lost handheld device which set to access internal data and services can be a very serious security risk. Providing high levels of security is crucial within a provider's network. Applications traditionally supported in the desktop environment are penetrating the market for mobility. All sorts of mobile devices now use software just as commonly as any other fixed device. The growth rate is extremely fast. Many steps should be taken to ensure communication remains secure as new features, networks, and devices are added to the conglomerate. From 2010 to 2019 the worldwide shipments of laptops, tablets and desktop PCs (in million units) as shown in figure 1 [1]. Users are consuming more data every year, and as the reliance on the Internet continue to grow, so too will the demands for higher data capacity. The tremendous data demand by mobile consumers and operators commitment to provide quality of services and user experience have been the main driving forces of deployment of multiple cellualr networks augmented with small cells and wifi to cope with capcity increase demand and to provide relaible coverage throughout the service area. Mobile users should not worry about dealing with a comlicated procedure to access wireless networks seamlessly and securly.

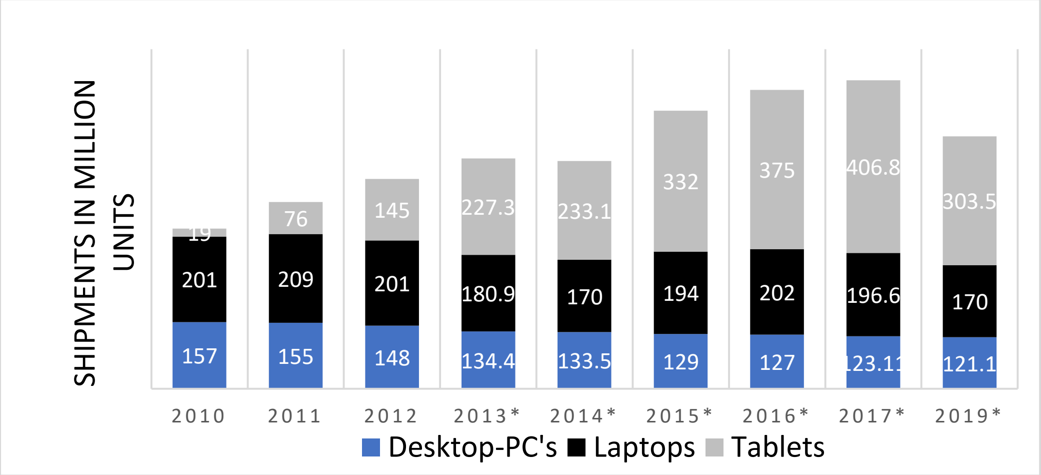

Figure 1) Number of Desktop-PCs (blue) versus Laptops (Black) versus Tablets (Grey)

Commercial:

Consumers are more demanding for services and applications. They depend on providers to handle the security component of their service just as much as the service itself. Recently, the number of security breaches from other industry segments have done harm to some organizations. A record of a security breach with leaked consumer information is devastating to operations and eventually, the bottom line. No organization wants to have a botched name from such an event. Are Mobile Network Operators (MNOs) taking the right approach? Taking a proactive stance to ensure infrastructure meets and exceeds the industry standard for security should be the ultimate goal. Other organizations who have taken a reactive approach to security threats suffered some serious losses. In some cases the damage may be irreversible. I will identify some problem areas in mobile network operations and some approaches providers can take to optimize security to protect the ones who keep the lights on, the consumer.

A. Google

Industry giant, Google, captures a wide range of data in the form of online behaviour. In the development of their location-based service Google Maps, a fleet of vehicles (bicycles and cars) collected data in the form of photographs from the street level and uploaded images to a database that creates a virtual 360 degree street view. People, automobiles, and private residences were captured as well as payload data (personal email, passwords, and passwords) collected from unsecured wireless networks [2].

B. Social Media

Each social media platform establishes its own dynamic privacy policy and terms and conditions of use. There are various privacy threats that common users of social media are exposed to whether they are cautious of information broadcast in status updates or not.

1) Facebook: Of the estimated 7.2 billion people in the world [3], Facebook reports, as of September 30, 2014, an average of 1.35 billion monthly active users and 1.12 billion mobile monthly active users, collecting both personal and usage data [4]. The personal data (demographics, status, email, location, media, etc.) users willing disclose can be used maliciously to determine personal and private information. Third-party companies, allowed access to personal and usage data by Facebook and users, predict personality and actions then use this information to manipulate decision-making and influence behaviour such as purchases through targeted advertisements.

2) The Virtual Market*:* The Digital Age has created a market for research and development in terms of adding networking features to every device that requires a power source, including; refrigerators, Smart TVs, game consoles, digital watches, automobiles, surveillance systems, smart heating, ventilation, and air conditioning systems, fitness and health monitoring products, home phones, cellular phones, and micro computing devices and accessories. These advancements in technology allow users to connect but allow for intrusions against online attacks.

Government:

The fact is, privacy is expected when it comes to communication. Call records were previously difficult to obtain. With the modern telecommunications networks voice, video, and data communications travel together over the same pathways. As telephony and data networks have converged, the black and white has become gray in terms of differentiating the two. Even law enforcement has had less trouble intercepting traffic since the voice traffic, now packetized, is treated the same as the data traffic. Even though wiretapping is illegal when targeting traditional wired telephony system for private users, some software companies are selling eavesdropping software legally. They can record a multitude of things on mobile devices. How would it feel to have your call recorded without your consent? I suspect with the development of such software, the expectation of privacy is going to be pressed. It is one thing to have records released to a government entity for the protection of its citizens, but the availability of end users to see my emails, applications I use, or anything else is horrifying. Such software should be banned in the consumer market.

The United States of America, founded on the principles of a government for the people by the people, has strayed in its founding vision of a promised land in which citizens hold this government accountable for its actions. When addressing the nation, US Secretary of State, Hillary Clinton stated, "We stand for a single internet where all of humanity has equal access to knowledge and ideas." Clinton further states that it is "our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building. And every generation of Americans has worked to protect the values etched in that stone." Those words, although they promote equality in information exchange over a single internet, do not reflect the actions of the federal government, nor do those civil liberties protect people that exchange information regarding government interference in civilian privacy over this free internet for enlightenment [5].

A. NSA

Edward Snowden, during contractual work at National Security Agency (NSA) facilities, collected tens of thousands of classified documents pertaining to various government surveillance programs and leaked them to the public in piecemeal fashion in June of 2013. The NSA surveillance programs target different aspects and different areas of the Internet. The surveillance project, upstream, uses fiber-optic cables to collect communications. Another NSA surveillance project, MUSCULAR, processes data collected from the internal cables that link the data centers for Google and Yahoo.

1) Boundless Informant: Used as a data mining tool, Boundless Informant has "the ability to dynamically describe GAO's [Global Access Operations] collection capabilities (through metadata record counts) with no human intervention and graphically display the information in map view, bar chart or simple table [6]."

2) TURMOIL: Used to capture data packets, TURMOIL is the fiber based wire-tap system used by the NSA [7].

3) X-KeyScore: The query system and database, X-KeyScore, allows NSA analysts to 'select' criteria of data extracted by TURMOIL, such as user IP or email address and initiate live interception of internet activity on a targeted individual. Over 150 X-KeyScore sites exist worldwide in the form of wiretaps at telecommunications companies' peering sites, foreign intelligence agencies' collections sites are connected by systems in allying countries, and fiber-optic cable taps in mid-ocean. Searches performed by the query system can target all VPN (virtual private network) start-ups or all encrypted word documents in a given country as long as the X-KeyScore plugin exists. The system was created to store the data packets solving the problem of storage from the 10-gigabit network tap collecting 129.6 terabytes per day [6].

4) Telephony Metadata: The mass surveillance of telephone data and metadata of US citizens by the NSA, suspected from leaked documents later confirmed by the federal government, were provided by Verizon as court ordered by FISC (Foreign Intelligence Surveillance Court) to produce daily electronic detailed call records. This telephony Meta data consisted of to and from whom calls are placed, duration, time, and place [8]. Susan Landau, Senior Staff Privacy Analyst at Google, states in her in-depth analysis of the impact of Edward Snowden's leaked NSA documents that it wasn't unusual the decision to permit the bulk collection of telephony metadata was a secret interpretation of the US Patriot Act, but "the [FISC] operates in secret and without anyone to argue against the government's position [8]."

Several organizations, including Verizon Business customers the ACLU (American Civil Liberties Union), filed lawsuits in federal court against the federal government on the grounds that the NSA used the Patriot Act to violate the freedom Americans are constitutionally guaranteed security from unwarranted search and seizures from the federal government in June of 2013. The ACLU has also filed a Freedom of Information Act lawsuit, which demands the government provide information about the use of Executive Order 12333 to intercept and collect the communications of Americans.

7) Piecemeal: Used as a data mining tool, Boundless Informant has "the ability to dynamically describe GAO's [Global Access Operations] collection capabilities (through metadata record counts) with no human intervention and graphically display the information in map view, bar chart or simple table [8]."

8) Tempora: The leaked NSA documents also showed access to the network of cables which carry international phone calls and internet traffic and shared information with the NSA gained by Britain's intelligence agency, the Government Communications Headquarters (GCHQ) in the covert operation Tempora. The transatlantic fiber-optic cables carry data at 10 gigabits per second with the potential of delivering more than 21 petabytes per day to watch and store.

9) Prism: The NSA classified documents revealed the operation, Prism allows access to collect communications directly from the servers of global internet service providers. The NSA has been granted court approved access to Google, Facebook, and Yahoo user accounts.

10) SIGINT: According to leaked classified NSA documents.

The project enabling by SIGINT engages effectively in the US and foreign IT industries to secretly impact and/or excessively influence their commercial products' designs. These changes in design make the systems being referred to exploitable through SIGNIT collections (e.g., Endpoint, Midpoint, etc.) with foresight adjustments to the consumer and other adversaries nonetheless, the systems' security remains in place. In this way, the enabling approach of the SIGNIT utilizes commercial technology and knowledge to deal with increasing expense and discovering technical challenges and exploiting the systems interest successfully within the ever-more security-focused and integrated global communication environment [9].

.

The excerpt from the NSA's fiscal year 2013 budget request exposed the planned compromise of the National Institute of Standards and Technology (NIST) cryptographic standard, Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC-DRBG), a random-bit generator to allow back doors in security products, Landau states "the NSA sabotage of a cryptography standard harmed communications security... [And] also hurt the industry."

C. Healthcare

Figures Healthcare systems are notorious producers of big data. Mass data collections include both patient and provider information. The US Government mandated in the American Recovery and Reinvestment act of 2009 that all healthcare providers adopt the use of electronic medical records (EMR) to continue their reimbursements from Medicare and state Medicaid programs [10].

Wireless Network Security and Privacy

The existence of communication has always called for a need for privacy and security. In the information age, security measures must be upgraded and adapted for the mobile user. Users spend more time traveling and mobile device usage has increased exponentially. Many users work from home, travel frequently as part of their business, or spend the majority of their time away from a stationary desk. The younger generations use their mobile devices everywhere, from vehicles, to lobbies in doctors' offices to school buses to concerts and expect their data transmissions to have privacy protection without having to setup their own.

After many decades of successful commercial implementation and operation of wireless communication systems many countries, organizations, manufacturers and different user groups are driven to work together to develop new standards due to the rise and demands in the wireless systems, applications and technologies. When deploying a wireless systems there are a number of areas in the systems both at access point and at user handheld device side must be taken into account in order to deploy a secure wireless communication system. The standardization groups for short and long range wireless networks and services have issued wireless standards and protocols including the Home RF, Hyper LAN, IEEE 802.11, 802.16,20 and 3GPP standards for 3G and 4G.

The technologies used in4G networks varies from WiMAX to HSPA to LTE and LTE-A. For example WiMAX and LTE have two different network architectures as an ITU requirement. And for that reason they use different security features. For WiMAX, IEEE 802.16 introduced the sub-layer in the MAC layer and the different handles like authentication and authorization to verify and identify the device connecting to the network which can be EAP-based or RSA-based, key management distribution to share traffic using private key management (PKM) and encryption used for data after exchanging keys [11]. So in general, the communication in WiMAX is secured with keys such as Authorization, encryption, Downlink hash function-based message authentication code (HMAC), Uplink HMAC key, and Traffic encryption.

Security features kept improving through mobile generations because of some security issues or weaknesses. It has varied from authentication to encryption to using integrity keys.

For LTE networks, the improvements occurred to 3GPP by using abstraction and associating on temporary ID for each SIM card to avoid IDs theft. Also LTE network has a new entity called Mobile Management Entity that signals securely the UE which is another way to secure communications.

Many countries, organizations, manufacturers and different user groups are driven to work together to develop new standards due to the rise in the wireless systems, applications and technologies. These standardization groups have issued wireless standards including the Home RF, Hyper LAN and the IEEE 802.11 standards. This section focuses on the IEEE 802.11 wireless standards. For remain of this chapter we discuss different security standards for various wireless mobile communication systems. This section focuses on the IEEE 802.11 wireless standards.

The IEEE 802.11 wireless standards

Existing solutions to wireless connectivity and data communication have been exposed to increased security issues and hence affects their performance and effectiveness. There is an increasing demand for wireless data communication and networks in the current technological age. Consequently, there is need for more efficient and effective wireless communication platforms. The IEEE 802.11 wireless networks have recently become so popular in the industry due to their ability to provide mobility, flexibility and security in the access to information and information resources. This report provides a detailed description and elaboration of the IEEE 802.11 Wireless LAN's security mechanisms and begins by providing an introduction to wireless networks, their vulnerabilities and how the IEEE 802.11 architecture can be used to employ security to the wireless networks. In this section, it is evident that IEEE 802.11 security mechanisms are the first and most effective and reliable ways to secure wireless networking. With the consistent and rapid evolution in technology and ways of computing, mobile computing and other wireless forms of data processing and computation will soon take over. Therefore, there is need for reliable and efficient security control mechanisms for wireless networks.

IEEE 802 committee approved the 802.11 Direct Sequence Spread Spectrum (DSSS) in 1997 to be used as a standard for wireless LANs that allows a bandwidth through put of 1 to 2 Mbps. The IEEE DSSS standard offers a wireless connectivity that allows quick network setup in a limited time zone. The 802.11 standards support ISM radio frequency as well as the infrared as transmission media. The throughput was increased developing three 802.11's extensions based on the new RF transmission techniques [12]. They include;

i) 802.11a; this extension increased the throughput to 54Mbps. It also operates in the 5 GHz frequency wavelength that uses the unlicensed-National Information Infrastructure (U-NII) band.

ii) 802.11b; this is a standard that increased the throughput to 11Mbps and is similar to the Ethernet 10baseT. It operates in the 2.4GHz frequency.

iii) 802.11g; this is the standard extension that is viewed as a go between the 802.11a and 802.11b. This standard offers a theoretical throughput of 54Mbps and is compatible with both the 802.11a and 802.11a standards. Additionally, the 802.11g standard will be the most used standard suitable for implementation of wireless network technologies.

The Relationship between the IEEE 802.11 and Wireless Technology

WI-FI (Wireless- Fidelity) certification is given to the 802.11 products that are compatible and interoperable with other Wi-Fi products. Their main concern is to ensure the interoperability of the products from all the 802.11 standards and all other wireless products from other standards. This certification is normally given by the Wi – Fi alliance, which also defined the WPA (Wi – Fi protected Access) and the Wi – Fi Zone for the expanding market for wireless networks and connectivity. These specifications, standards, and certifications are relevant for the 802.11 wireless connectivity. Therefore, the next section will identify the IEEE 802.11's security mechanisms for the wireless networks.

IEEE 802.11 Security standards and mechanisms for wireless connectivity

With the increase in popularity of the wireless networking and communication, there are also major challenges in roaming, configuration and security. Most of the data are subjected to security threats ranging from eaves dropping, through the radio frequencies [13].

Therefore, these wireless networks must be secured to enhance reliability and security in data communication. Conventionally, wireless traffic is transmitted through the open air via the radio waves, consequently, proper security mechanisms must be installed to prevent against possible security threats. The IEEE 802.11 has developed a set of security standards and mechanisms to secure wireless connectivity and networks. These set of mechanisms and security features include:

- Virtual Private Networking (VPN) across radio frequency
- Service set identifier (SSID)
- MAC Address Filtering
- Wireless Equivalent Privacy (WEP) Algorithm
- Access Control list

These mechanisms can be deployed individually but deploying all four mechanisms ensures a more secure and reliable security framework.

VPN

An alternative to the three mechanisms is the incorporation of the VPN solution to a high security network. This mechanism provides a dedicated and secure channel over an un-trusted network particularly the internet. The VPN has a server and a VLAN interfacing the access point and the VPN server. The VPN server acts as a gateway to the private network and provides full encryption as well as authentication.

The VPN mechanism is mainly develop to provide users with a more secure way of connecting to the network using the internet. This connection is established through a secure VPN using the different tunneling protocols [13]. Additionally, the VPV mechanism provides a logical solution to wireless networks due to the fact that it provides an access control that protects against unauthorized routes to the network [14].

Service Set Identifier (SSID)

This is an identity verification mechanism that is often used in the access point or group of access points that is used to identify which subnet mask one exists in. it works by segmenting the wireless network in multiple networks and using it as a form of authentication. In case the wireless station doesn’t know the value of the SSID then, access to the access point is denied. The SSID acts as some form of password hence providing security [15].

However, if the SSID is used alone the security is weak due to the fact that the value is known by all network cards and access points; hence it is easily accessed through radio waves and the air because of lack of encryption. Access points are configured to broadcast the SSID hence any client can be able to receive it and hence access the access point. Additionally, users can be able to configure their own client systems with appropriate SSID, because SSIDs are easily shared and are widely known.

MAC Address Filtering

Client computers in a wireless network have different MAC address for its IEEE 802.11 network card. Every access point in a network has a list of authorized MAC addresses that are only allowed to access the Access point. This list is inputted manually and must always be kept up to date. Due to this cumbersome process of creating and maintaining the list, it is suitable for smaller networks. The security of such a network can further be reinforced by using the IEEE 802.11 WEP and the SSID together with the MAC address filtering.

WEP Algorithm

The WEP security protocol and mechanism provides security against eavesdropping and physical security attributes. This is the encryption standard that has been specified by the IEEE 802.11 network architecture. Essentially, the WEP algorithm encrypts data and information and protects it from unauthorized users. The mechanism uses a 40- bit secret key for encryption and authentication. Other IEEE 802.11 standards allow the 104 – bit secret key encryption [15].

Encryption

Once WEP is enabled, all the data is encrypted using the Ron Rivest code 4(RC4) to provide security for data to be transmitted. WEP also protect the wireless traffic using a 24-bit initialization vector (IV) that is randomly generated. This IV is combined with 104-bit or 40-bit shared secret key. The encryption process involves:

First, the 40-bit shared key is concatenated with the 24-bit IV. The IV introduces cryptographic variance to the shared secret key hence increasing security. Now there is a new 64- bit key that is fed to the RC4 algorithm hence creating the encryption key. The data is protected against modification by checking for integrity using the cyclic redundancy Chech-32(CRC-32). This process generates 4 bytes CRC that will be used together with the encryption key to generate an encryption output. This output is sent to transmission where the recipient will use reverse steps to decrypt the data.

Authentication

WEP authentication mechanism uses the same secret key that was used in the encryption process. There are two possible authentication ways namely open system authentication and Shared Key authentication.

Open system Authentication

This is the default authentication mechanism that works in two steps:

i) The client that wishes to join the wireless network sends an authentication request.

ii) The Access point in turn checks the shared secret key and replies with a positive or negative answer.

In this mechanism, neither the client nor the Access point has the privilege of authenticating each other.

Shared Key Authentication

In this mechanism, the access point issues an encrypted challenge packet to clients once encryption is enabled [13]. Each of this is broadcasted to any client that is attempting to connect to the access point. The client then uses the key to encrypt the correct response so as to authenticate itself. Both the client and the access point use the same key for encryption and subsequent decryption of data.

All the encryption keys in the WEP algorithm that are used in a wireless network should be manually managed since there are no protocols for managing the keys in WEP and for distribution as well.

One of WEP limitations is that it can only be implemented on a client /server wireless network having an access point but cannot work on a peer-to-peer network.

The other weaknesses associated with the WEP algorithm is that the WEP keys encryption and authentication is static thus making it susceptible to traffic injection, statistical attacks and password replays among other threats. Regular change of WEP key reduces the risks of unauthorized access to the access point, and eaves dropping among other security threats [16]. Hackers have exploited this security loop hole in the past by intercepting the traffic and flipping the bits and injecting modified packets into the network. The IEEE 802.11 WEP security mechanism is mainly concerned with three goals; Data integrity, access control and confidentiality. For better effectiveness in securing wireless networks WEP mechanism is deployed together with the SSID security standards.

MAC Address Filtering

Client computers in a wireless network have different MAC address for its IEEE 802.11 network card. Every access point in a network has a list of authorized MAC addresses that are only allowed to access the Access point. This list is inputted manually and must always be kept up to date. Due to this cumbersome process of creating and maintaining the list, it is suitable for smaller networks. The security of such a network can further be reinforced by using the IEEE 802.11 WEP and the SSID together with the MAC address filtering.

Security weaknesses in the IEEE 802.11 security mechanisms

The security mechanisms defined by IEEE 802.11 are intended to provide security to wireless networks through authentication, access control and data encryption. However, these mechanisms have some limitations and cannot provide maximum security against some sophisticated attacks.

SSID Weaknesses

SSIDs are periodically broadcasted by the Access Point to all the wireless devices that are in range. The wireless devices with the correct SSIDs can automatically discover and join the wireless network. Consequently, this makes it easy for attackers to find the SSID and access the network without authorization. The broadcast feature of the Access Point can be disabled and the SSID configured manually by each client. With the broadcasting off, attackers can still gain access to the SSID during the association phase. The SSID will then be transmitted during the association request between the client and the access point and hence an attacker may intercept the transmission and gain access to the SSID.

Attackers may also gain easy access to a default SSID, this happens when the client or user does not change the default SSID which in this case makes it easy for the attacker to guess and gain access to the wireless network.

MAC address Filtering Weaknesses

The ACL or in this case MAC address filtering has some vulnerabilities that result from the possibility of an attacker identifying the authorized MAC addresses. This is possible due to the fact that ACL or MAC address filtering allows the Access point and the network administrator to maintain a list of authorized address. Hence, the attacker can use one of the MAC addressed and deceive the Access point into gaining authorization into the wireless network.

WEP Weaknesses

The WEP mechanism has vulnerabilities both on authentication and encryption. The major cause of these vulnerabilities is the fact that every component has possible security weaknesses.

First, the shared security secret keys are configured manually during installation and are rarely changed. Secondly, the use of RC4 algorithm is susceptible to various security threats that can expose the WEP shares secret key. Thirdly, there is possibility of repeating the IV hence causing IV collision. This opens a loop through which the attacker can collect enough data to depict the secret key. Finally, the CRC-32 can be modified by an attacker in a manner that the recipient won’t realize since it will appear valid.

Higher Generation of Mobile Communication Systems

With the emergence of mobile and wireless networks, devices, the amount of data that can be transmitted, the distance that data can be transmitted over, and the massive amount of users that access this data daily, the need for security has multiplied. Information is being transmitted today in ways that mankind hasn’t seen before. Mobile devices, tablets, wearable wireless technology such as watches, heart rate monitors, medical devices, laptops, and even smart cars transmit data. On an even larger scale, the world’s governments, militaries, and financial institutions absolutely must utilize some form encryption or security to protect the secrets, policies, information communication channels, and financial channels from unwanted adversaries.

Hospital and medical staff carry laptops with them from patient to patient instead of pen and paper and physical charts and records. They can look up and update patient information while talking with the patient. The data is wirelessly transmitted to servers and stored remotely. Smart cars can connect to mobile phones to make phone calls, access the Internet, use GPS (Global Positioning System) for directions, and even transmit data from one smart vehicle to another.

Mobile devices utilize operating systems such as Apple’s iOS or Google’s Android software and available applications to access the internet. Users can play online games, utilize productivity software for work purposes, and watch instant streaming through services like Netflix, Hulu, and Amazon Prime, in addition to the older services like text messaging and making phone calls. Wearable technology is becoming more popular. Smart watches allow users to connect to the Internet through a wireless network, or connect to a user's mobile or cellular device to access data. GPS watches enable athletes to track their exercise like running or walking. Many smart watches and GPS watches even have the ability to track a user's heart rate for medical purposes. Some of these data uses may seem more mundane and the need for security may seem less or not needed at all. But as users become more connected to their devices, and their devices to the Internet, the need for security has never been greater.

In 4G and beyond systems the Security requirements is an important essential. It comprise of security requirements on the followings:

- ME (Mobile Equipment) for protection of integrity of the hardware, software and OS in mobile platform for data control access, maintenance of confidentiality and integrity of the stored data and user identity privacy retention
- Security requirements on radio interface and network operator for entity authentication and mutual authentication between user and switch, confidentiality of traffic and signaling data, and confidentiality of user traceability.
- Security visibility, configurability and scalability for transparency, acceptable level and scalability of security mechanism for a roaming visitor to a network.

4G LTE Architecture

The LTE network architecture is based on three levels which are: the communication protection between the UE and E-UTRAN or MME, provision a protection among the wireline network elements and the provision of a secure access to the mobile station.

However, even with all these security features in the network, there is still some vulnerabilities in the system especially in the physical layer such as interference and scrambling attacks. The interference would be a man made to disturb the communication and possibly lose it because of the high level of signal to noise ratio. But it's also easy to detect.

Scrambling attack is also a form of interference or jamming but it occurs for a short specific period of time in order to disrupt a channel like control channel. Attackers can easily detect the control channel because it has a fix duration and it's always located at the beginning of a frame. Also there is the risk of the Denial of service attack that can happens at the level of eNodeB and affect a specific UE.

Designing of the Long Term Evolution (LTE) architecture supports packet-switched service to give consistent Internet Protocol (IP) connectivity between the packet data network (PDN) and User Equipment (UE), without any interruption to the end users applications during mobility. The combination of long term evolution (LTE) and the system architecture evolution (SAE) is called evolved packet system (EPS). LTE covers the evolved UMTS terrestrial radio access network and evolution of non-radio access network [17].

Evolved packet system (EPS) is combination of the core network (CN) and the access network E-UTRAN. In which core network consists of number of logical nodes and access network consist of single node i.e. evolved NodeB (eNB), which connects to UE. The network elements in the EPS is interconnected by standardized interfaces to allow multi-vendor interoperability. The interconnectivity of EPS network elements are shown in figure 2 [17].

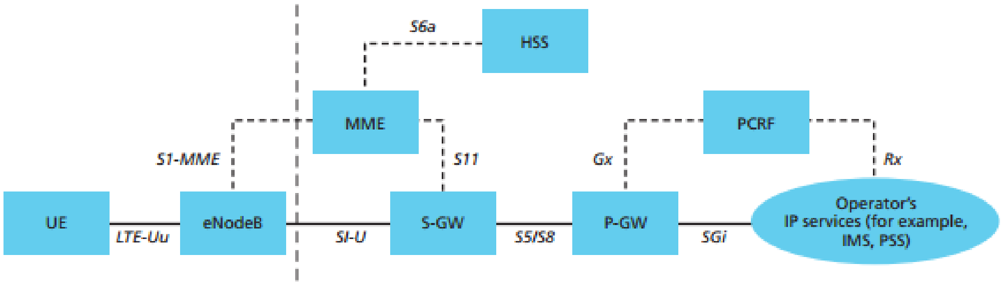

Figure 2) The EPS network elements

The core network

The core network called evolved packet core (EPC) in system architecture evolution (SAE) is responsible for the overall user equipment (UE) control and bearer's establishment. The core network consists of following logical nodes:

- Mobility Management Entity (MME)
- Serving Gateway (S-GW)
- PDN Gateway (P-GW)

Along with these nodes, EPC also includes Home Subscriber Server (HSS) and Policy Control and Charging Rule Function (PCRF). The logical nodes and their functions are explained as:

Home Subscriber Server (HSS): The HSS in the network holds the users subscription data, which contains the Quality of Service profile and roaming restrictions for accessing the network. It also contains the PDNs information to connect the user. Along with these information the HSS holds the dynamic data such as the MME identity.

Policy Control Charging Function (PCRF): It is responsible for the policy control and decision making, control of the flow based charging functionalities and it also provides QoS authorization.

PDN Gateway: It is responsible for IP allocation for the UE and user IP packets in the downlink are filtered based on the distinct QoS bearers. It performs QoS implementation for ensured bit rate (GBR) bearers.

Serving Gateway: All the user IP packets in the network are transmitted through the Serving Gateway and when the UE moves among the eNodeBs, it acts as local mobility anchor for the information bearers. Downlink data is buffer when the MME initiates the paging of the user entity to restore the bearers. Notwithstanding these functions it does some administrative functions in the visitor network.

Mobility Management Entity (MME): It is the control node and the signaling between the UE and the CN is processed by the control node. In this Non Access Stratum (NAS) protocols are working between the UE and the CN. The MME functions are identified with the connection management and bearer management. In bearer management, which includes the establishment, maintenance and release of the bearers. In connection management, which is used for the establishment of the security and connection between the network and UE.

The access network

LTE access network, E-UTRAN comprises of network of eNodeBs, where there is no controller in E-UTRAN for normal user traffic. Hence the architecture of the E-UTRAN is flat, it is shown in figure [18].

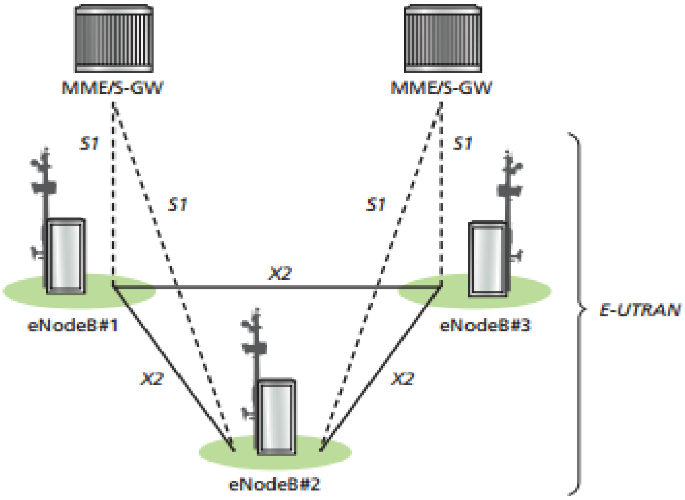

Figure 3) E-UTRAN architecture

From the above figure the eNodeBs are interconnected through the X2 interface and to the EPC by S1 interface- more accurately connected to the MME through the S1-MME interface and to the S-GW through the S1-U interface. The Access Stratum (AS) protocols are function between the eNodeBs and the UE.

All radio related functions are managed by the E-UTRAN in the LTE network, such as Radio Resource Management (RRM), security, header compression and network to the EPC. Radio Resource Management (RRM), which extends all the functions identified with the radio bearers including radio admission control, radio mobility control, radio bearer control, scheduling and dynamic allocation of resources to UEs in both uplink and downlink. Header compression, which is used to reduce the overhead of the IP packets by compressing headers of the IP packet. Security, which is encryption of the data that sent over the radio interface. All of the network functions are reside in the eNodeBs, these functions are responsible for managing multiple cells and all the radio control function incorporated into an eNodeB [18].

Security technology for SAE/LTE

The architecture design of LTE is different to an extraordinary degree from the scheme utilized by the existing 3G network. That distinction between the architecture design brings with it need to adjust and enhance the security function. The most essential necessity is that level of security in 3G network must be ensured in LTE [18]. The necessity additions and changes are made to fulfill security in LTE are listed below.

- The hierarchical key framework is introduced in which keys can be changed for distinctive purpose.
- Distinctive security functions for the NAS and AS. NAS security functions are processed between a Mobile Management Entity (MME) and a mobile terminal (UE), from those functions for the AS, which incorporate between the eNB and the UE.
- The forward security concept is introduced, which confines the scope of damage when a compromised key is utilized.
- The security functions expansion for interconnection between a 3G system and a LTE system.

Security requirements for LTE

The security functions of 3G networks are widely used, providing 3G network with user ID confidentiality, authentication, Control plane (C-plane) and User plane (U-plane) confidentiality as well as integrity protection of C-plane at a security level correspondence in form with other standards.

Essential requirements for security functions in LTE are:

- Provision of the same level of security in LTE as the 3G network without influencing the user comfort.
- Give resistance against current attacks from the web.
- The security functions gave by LTE should not influence the step-wise move from 3G to LTE.
- Permit continued utilized of the Universal Subscriber Identity Module (USIM).

The last two requirements of LTE are fulfilled by reusing the 3GPP Authentication and Key Agreement (3GPP AKA) mechanism.

Network Domain Security (NDS) is applied to fulfill the security necessities for the evolved packet core (EPC) i.e., the LTE core network on the IP layer as standardized in TS33.210.

Nevertheless, the 3G security architecture cannot be re utilized as is for the RAN in LTE because some of the RNC functions are coordinated into eNB in LTE. Evolved NB stores the key for encryption and integrity protection while UE is in the associated state. Moreover, the evolved NBs in LTE may be installed in open areas to guarantee scope for indoor, for example, work places and ample wireless capacity, a measure that is required to expand the danger of unapproved access to eNB. In this way, the measures portrayed below are pointed out to minimize the damage that may come about when a key is stolen from an eNB [19].

LTE security architecture

The complete overview of the LTE security architecture is shown in figure 4 [21]. The stratums in the network are identified and each stratums addressing the isolated category of the security threats in the LTE system.

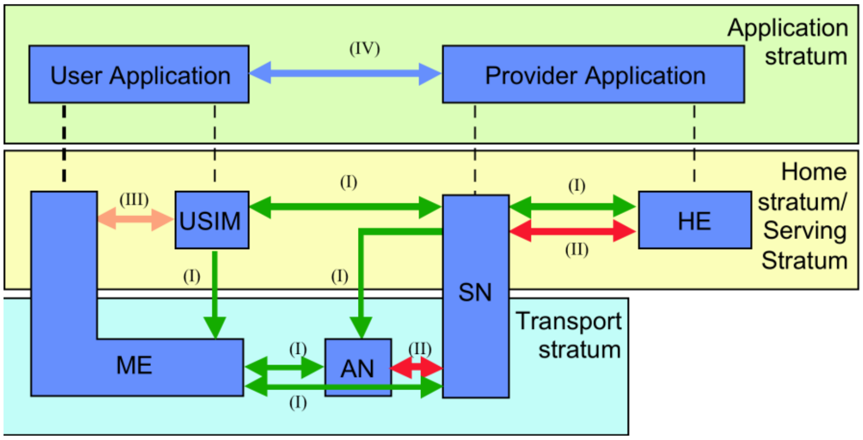

Figure 4) Overview of the Security architecture

From the above figure there are five security feature groups in the LTE security architecture.

(I) Network access security: Network access security gives services with secure access to the users and protect from the radio link attacks. Security features on the primary radio link are:

- RRC signaling encryption and integrity protection
- NAS signaling encryption and integrity protection
- Radio bearer data encryption
- Mutual Authentication between the Access Network and UE

(II) Network domain security: Network domain enables node to exchange user data and signaling data in a secure manner and protect from the wireline network attacks. It performs the following functions:

- Internet Key Exchange (IKE) is used for the key negotiation
- Setting up the security association between the Security Gateways (SEG) using Internet Security Association and Key Management Protocol (ISAKMP).
- Encryption, data integrity and Authentication are done by using Tunnel-mode Encapsulation Security Protocol (ESP).

(III) User domain security: It gives secure access to mobile device and the mutual authentication between the ME and USIM before the USIM access to the UE. The following set of security is provided by the user domain security:

- It requires IMSI and IMEI should be protected confidentially.
- Authentication between the user and USIM, PIN is used to authenticate the user to access the USIM.
- Authentication between the USIM and terminal, this is used for SIM locked mobiles. In SIM locked mobile devices are stored the IMSI of the USIM.

(IV) Application domain security: It enables the UE applications and exchanging messages between the USIM and the network in a secure manner.

(V) Visibility and configurability of security: Which allows the user to know about the feature of the security is in operation or not and whether the services utilize and provision should depend on the security feature. This security provides following security functions:

- Access network encryption indication
- Security level indication
- User-USIM authentication enabling or disabling
- Accepting or rejecting incoming non-ciphered calls

Vulnerabilities in system architecture

There is an increase with the security risks in the 3GPP LTE networks because of its flat IP-based architecture. A directed path to the base station is provided by the all-IP network for the malicious attackers because of the various eNBs in the flat architecture are managed by an MME. Along with these security risks there is also an existing security risk because of the mobility of UE from an eNB/HeNB to a HeNB/eNB. Bandwidth consumption as well as signaling overhead authentication among the HN and the SN will arise due to the SN requests authentication vectors set from the HN when the UE remains in the SN for a long time and consumes its authentication vectors set for the authentication [39].

Security in a LTE Cellular System

In a LTE cellular security, the important scheme is the mutual authentication between the user entity (UE) and the evolved packet core (EPC). The mutual authentication between the UE and the EPC is achieved by using the Authentication and Key Agreement (AKA) procedure and it shown in figure 5 [21].

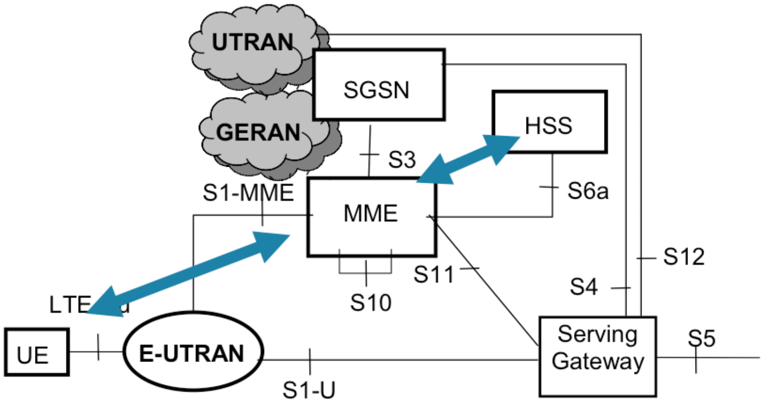

Figure 5) Authentication and Key Agreement

In Authentication and Key Agreement (AKA) procedure the authentication data generated by Home Subscriber Server (HSS) provided to the Mobility Management Entity (MME). Different session keys are used for the encryption and the integrity protection, which are derived by the integrity key (IK) and ciphering key (CK) that are generated in the AKA procedure.

In the LTE system, when UE interfaces with the EPC over the E-UTRAN, the MME represents the EPC in the network to perform mutual authentication with the UE. The mutual authentication between the MME and the UE is done by using the EPS AKA. The EPS AKA authentication procedure is shown in figure 6 [22].

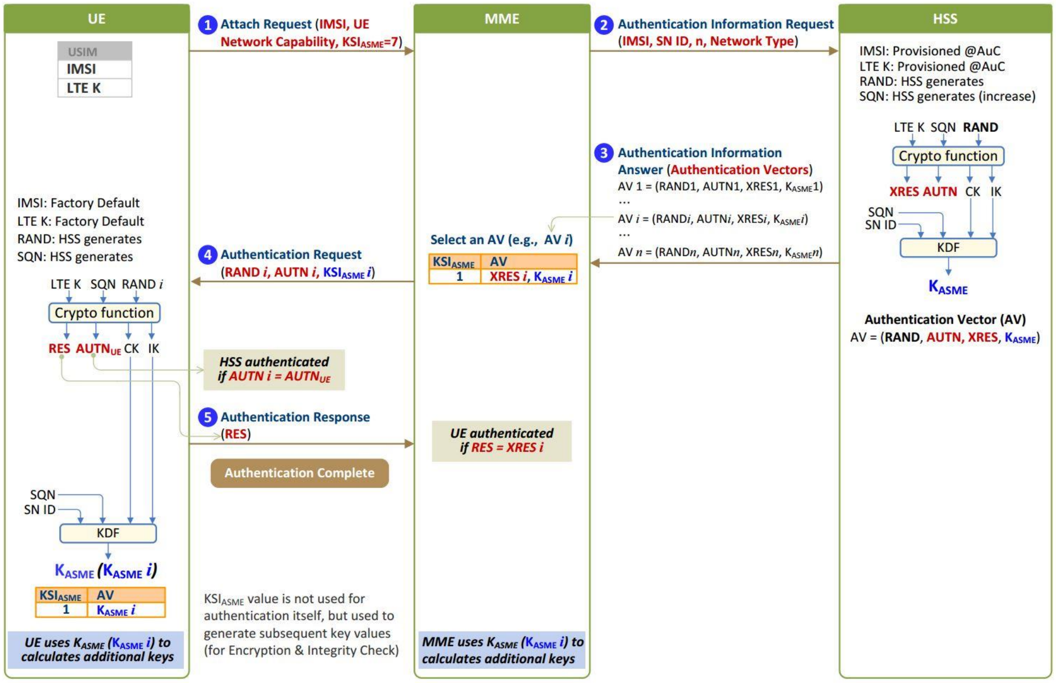
UE
MME
HSS
USIM
IMSI
LTE K
1 Attach Request (IMSI, UE Network Capability, KSIASME=7)
2 Authentication Information Request (IMSI, SN ID, n, Network Type)
IMSI: Provisioned @AuC
LTE K: Provisioned @AuC
RAND: HSS generates
SQN: HSS generates (increase)
LTE K SQN RAND
Crypto function
XRES AUTN CK IK
SQN
SN ID
KDF
KASME
Authentication Vector (AV)
AV = (RAND, AUTN, XRES, KASME)
3 Authentication Information Answer (Authentication Vectors)
AV 1 = (RAND1, AUTN1, XRES1, KASME1)
…
AV i = (RANDi, AUTNi, XRESi, KASMEi)
…
AV n = (RANDn, AUTNn, XRESn, KASMEn)
Select an AV (e.g., AV i)
KSIASME AV
1 XRES i, KASME i
IMSI: Factory Default
LTE K: Factory Default
RAND: HSS generates
SQN: HSS generates
4 Authentication Request (RAND i, AUTN i, KSIASME i)
LTE K SQN RAND i
Crypto function
RES AUTNUE CK IK
HSS authenticated if AUTN i = AUTNUE
5 Authentication Response (RES)
UE authenticated if RES = XRES i
Authentication Complete
SQN
SN ID
KDF
KASME (KASME i)
KSIASME AV
1 KASME i
KSIASME value is not used for authentication itself, but used to generate subsequent key values (for Encryption & Integrity Check)
UE uses KASME (KASME i) to calculates additional keys
MME uses KASME (KASME i) to calculates additional keys

Figure 6) EPS AKA (Evolved Packet System Authentication and Key Agreement)

Two steps are processes in the evolved packet system authentication and key agreement (EPS AKA) procedure. In first step, authentication vectors such as RAND, AUTN, XRES, and K_{ASME} are generated by Home Subscriber Server (HSS) and those are delivers to an MME. In the second step, one of the received authentication vectors selected by the MME and uses this selected vector for mutual authentication with a UE and the same authentication key (K_{ASME}) is shared each other. In LTE networks, authentication vectors generation requires user's serving network ID (SNID). In addition to user authentication by the network it also performs network authentication by the user.

Top-level security keys are received by the Access Security Management Entity (ASME) from HSS are used in an access network. An MME in the EPS acts as ASME and K_{ASME} key is utilized as the top level key to be utilized in the access network. In the EPS, instead of HSS, MME conducts mutual authentication with a UE. Once the mutual authentication between the UE and MME is completed using key K_{ASME}, they both share the same K_{ASME} as an authentication key. Several distinctive AKA procedures are carried out for the non-3GPP access.

In LTE cellular security, there are few outstanding features are named in security access of the user. To prevent the LTE networks from the attacks such as false base station and redirection attacks, the SNID (serving network identity) added to the EPS AKA procedure. A new key hierarchy is initiated to defend the signaling security as well as the data traffic of the user [22].

Another outstanding features in cellular security is that supporting of the non-3GPP access authentication among the AAA server and the UE. An Extensible Authentication Protocol-AKA (EAP-AKA) is carried by the AAA server and UE to complete the authentication of the access.

Key Hierarchy

Stream encryption method is used in LTE for data encryption, in which exclusive OR of the data and key stream in the same way as is carried out in 3G to encrypt the data. It is essential in that system that the key stream will never be reused. The finite length of key stream is used for algorithms in 3G and LTE. Therefore, the key stream is changed consistently to prevent the reuse of the key stream, e.g. during handovers. The execution of AKA is important to create a key in the 3G network. Accomplishing AKA may take a few several milliseconds to key calculation on the USIM and for association with the HSS. To accomplish higher data rate as in LTE, allows key upgrading function must be added without executing the Authentication and Key Management (AKA).

Moreover, to reduce the damage that may come about if one of the keys utilized for encryption or integrity protection becomes compromised, it is desirable that the compromised key isn't stored and utilized at numerous places on the network. So in LTE a key hierarchical system is introduced to solve the issue in 3G network. The Key hierarchical system in LTE is shown below figure 7 [21].

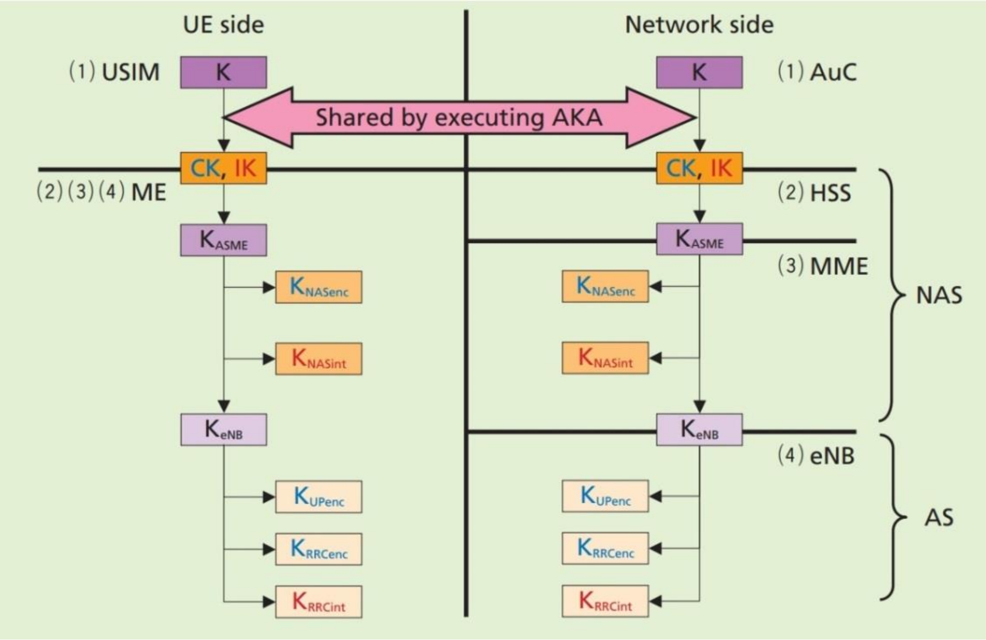

Figure 7) Hierarchical keys and method for key generation between entities in LTE

The USIM and Authentication Centre (AuC) in the key hierarchical system share secret information (key k) in advance similarly as the key shared in the 3G network.

- Mutual authentication between the network and user executed by using Authentication and Key Management (AKA), keys are generated for integrity protection (key IK) and encryption (key CK) and respectively keys are passed from USIM to mobile equipment (ME) and AuC to HSS.
- Key generation function used to generate K_{ASME} by ME and HSS from the key pair CK, IK based on the ID of the visited network. HSS in the network side ensures that K_{ASME} can be used by the visited network by building the correspondence of K_{ASME} key. To serve as essential data on the key hierarchy K_{ASME} is exchanged from the HSS to MME of the visited network.
- Keys K_{NASenc} and K_{NASint} for NAS protocol encryption and integrity protection between the MME and the UE are generated from K_{ASME}.
- MME generates K_{eNB} key when the UE is associated to the network and passes key to the eNB. The K_{UPsec} key for user plane encryption, the K_{RRCenc} and K_{RRCint} keys for Radio Resource Control (RRC) encryption and integrity protection are generated from the K_{eNB}.

Separation of AS and NAS security functions

Huge amount of data in the LTE network transmitted only when the UE is connected to the network. So the LTE network build security associations between the UE and eNB only when UEs are connected in the network. Consequently, there is no need to preserve state in an eNB for UEs in idle mode. Because NAS messages are transferred with idle mode UEs, NAS security associations are laid down between the UE and the MME.

After completion of UE authentication, K_{ASME} key is retained by the MME, which is the highest priority key of the key hierarchy in the visited network. By using K_{NASenc} and K_{NASint} keys the NAS security command manages the encryption and integrity protection algorithms for NAS communication between UE and the MME. Right now, the MME must find from which UE the authentication request message arrived so as to discover the right key to use for decryption and to verify data integrity. Nevertheless, a temporary ID called the GUTI (Global Unique Temporary Identity) introduced in LTE network to identify the UE instead of using the IMSI because the UE ID should be protected in the radio link. It is not possible to trace which GUTI the UE is using because of this GUTI changed periodically.

When UE enters in to the connected state, eNB switches on the AS security functions with the AS security mode command. Thereafter, AS security is connected to all communication between the UE and eNB. AS security algorithm is negotiated independently from the NAS security algorithm.

In LTE, standardized Snow 3G and Advanced Encryption Standard (AES) algorithms are used for encryption and integrity protection. These two standard algorithms are provide full security to the network and these are differ in basic structure are used in 3GPP so that even if one algorithm is collapsed, the other algorithm can be used for continued secure use of the LTE system [23].

LTE access procedure vulnerabilities

The ability to protect the privacy of the system deficiencies in the EPS-AKA procedure. The prevention of the DoS attacks cannot be done in LTE cellular security because of the MME, which forwards the requests from the UE's to the HSS even before the authentication of the UE by the MME. The ability of the online authentication lacks in the EPS-AKA protocol. The inadequacy in the EPS-AKA protocol have which are user identity disclosure, synchronization of sequence number (SQN), bandwidth consumption as well as vulnerability to MitM attacks. The inadequacy has been identified in the LTE system because of the reusing the EAP-AKA to give authentication for the secure access [39].

LTE handover security

Handover is the mode of mobility in the network occurs when the UE is active and the mobility can occur when the UE is in the active or the UE is idle. There are different types of handovers in the LTE both for active and idle UE. These handovers can be categorized as follows.

- Intra-SAE/LTE
    - X2 Handover: This handover occurs when the UE moves from source eNB to target eNB
    - S1 Handover: This occurs when the handover leads to change in MME
    - Intra-eNB handover: This handover occurs when the UE moves from one cell of a given eNB to other cell in the same eNB

- Inter-RAT handover: This handover occurs when the UE moves from E-UTRAN to different RAT

X2 Handover

This Handover occurs when User Entity (UE) moves from source eNB to the target eNB, where eNBs connected to the same MME. In this case a new key is provided to the target eNB in the core network and unknown key in the source eNB, these keys are used after handover. Next Hop (NH) parameter is the arbitrary value at the UE and eNB, this parameter is sent to the target eNB by the MME. If the source eNB is compromised by attacker have the ability to effect the services of the given UE at the target eNB however UE services will be secured from the following handover onwards by assuming the target eNB is not compromised. X2 handover mechanism shown in below figure 8 [24].

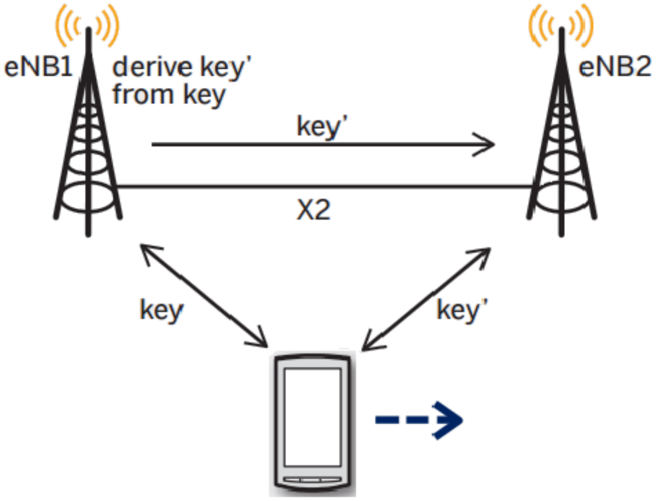

Figure 8) X2 Handover: backward security

To secure the handovers in LTE networks and to support global mobility and secure 4G wireless communication systems a hybrid authentication and key agreement scheme was proposed. The scheme was proposed a non-repudiation service and lightweight authentication by associating a dynamic password with a public key. Likewise, as a part of the scheme broadcast protocol designed by adopting the public key, without using the certificate a mutual authentication between the foreign network (FN) and the UE is achieved. However, using the public cryptography brings a lot of trouble to support the consistent handovers because public cryptography may incur a great deal of computational costs and storage cost. 4G wireless networks proposed security roaming and vertical handover scheme among different technologies. The 3GPP committee has detailed the security procedures and features on the mobility inside E-UTRAN and additionally between the E-UTRAN and the UMTS Terrestrial Radio Access Network (UTRAN)/GSM EDGE Radio Access Network (GERAN)/non-3GPP access networks. The security procedures in handover explained in detail as follows [24].

Intra E-UTRAN mobility: LTE networks provides new key management mechanism to achieve secure handover within E-UTRAN. Based on the vertical or horizontal key derivations new eNB keys are derived in different ways by using new key management mechanism. K_{eNB} and Next Hop parameter (NH) are derived from the K_{ASME} to achieve a secure communication between an eNB and an UE. After an initial authentication procedure K_{ASME} is derived from the UE and the MME. Each K_{eNB} and NH parameter are associated with the NH chaining counter (NCC). In handovers, new session keys K_{eNB} are utilized between the UE and the target eNB and these keys will be derived from the either the currently active K_{eNB} or from the NH parameter.

Mobility between the E-UTRAN and UTRAN/GERAN: To achieve handover between the E-UTRAN and UTRAN/GERAN, the UE and MME might first derive a CK' and IK' from the K_{ASME} and these are called the mapped UTMS security context because they are derived (or mapped) from KASME. After getting IK' and CK' with KSI' from the MME, the general radio packet service (GPRS) K_c is derived by using CK' and IK' at the target service GPRS supporting node (SGSN) and the UE. To achieve handover from the UTRAN/GERAN to the E-UTRAN, K'_{ASME} derived from IK and CK or received GPRS K_c from the SGSN at the target MME. Along with the target eNB the UE should also follow the same procedure as MME to derive K'_{ASME}. By following key hierarchy mechanism the target MME and the UE might drive K_{eNB} and relating NAS keys.

Mobility between the E-UTRAN and non-3GPP access networks: To attain secure consistent handovers among the E-UTRAN and non-3GPP access networks, the 3GPP committee proposed several different mobility approaches for the evolved packet core. By looking at the proposed 3GPP specifications, full access authentication procedure will be implemented at the UE, the target access network and the EPC before the UE moves to the new access network. Distinctive procedures of access authentication will be implemented in different mobility scenarios, such as EPSAKA is implemented when handover to the E-UTRAN, when handover to trusted non-3GPP access networks the EAP-AKA or the EAP-AKA' are implemented and when handover to untrusted non-3GPP access networks IKEv2 with EAP-AKA or the EAP-AKA' are implemented [25].

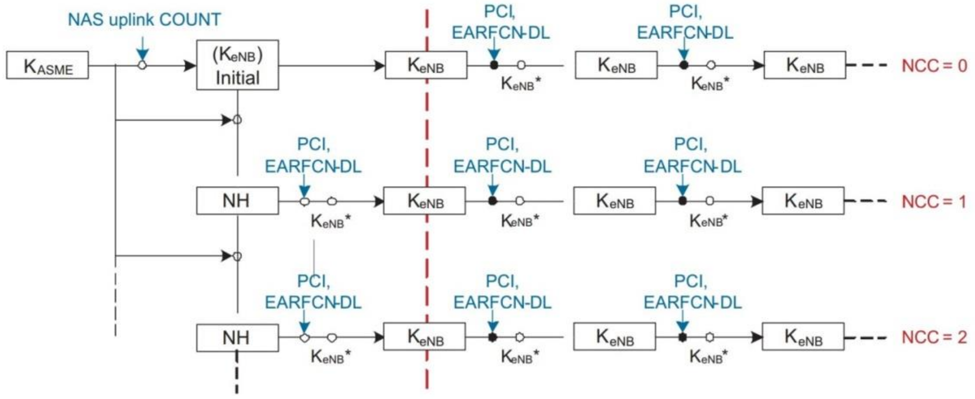

Figure 9) Handover Key Chaining

S1 Handover

This handover occurs when the s1 interface involved in the handover key management. S1 handover occurs when the UE moves between the source eNB and target eNB, and these are connected to distinct MMEs but it can also occur when both eNBs are under the same MME. Unlike X2 handover, even if the source eNB is compromised the communication from the next hop is secured. The secured communication from the next hope happens because of fact that the source MME sends new NH to the target eNB with NCC incremented by 1, which further forwards the new NCC, NH pair to the target eNB. The new NCC, NH pair provide K_{eNB} to the target eNB. The UE is informed that key derivation obtained from the NCC. Therefore, NH value used at UE and target eNB is unknown to the source eNB giving a way to a K_{eNB} that cannot be known to an adversary of the compromised source eNB [24].

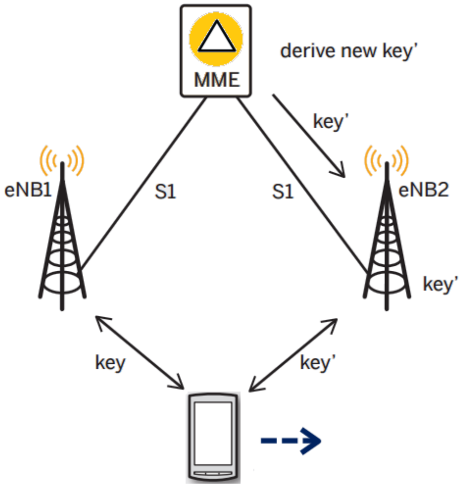

Figure 10) S1-handover: forward and backward security

Vulnerability in LTE Handover procedure

There are several security threats posed due to the malicious base stations so to mitigate these security threats a new handover key management scheme is provided by the LTE security mechanism. Whenever the UE moves from one eNB to another eNB this scheme is used to refresh the material keys between an UE and an eNB. Furthermore, to support mobility secure between heterogeneous systems the 3GPP committee has defined the necessity securities, threats and solutions to the security issues. Nevertheless, there are lot of vulnerabilities still found in the handover key mechanism and the LTE mobility management procedure. Some key vulnerabilities in handover procedure are explained below.

Lack of backward security: Since LTE key management mechanism used the key chaining architecture, new keys are derived at the current eNB by chaining the current key with the eNB specific parameters for multiple target eNBs. An attacker has the ability to obtain the subsequent session keys after source eNB is compromised. Thus, backward security achievement in the current LTE networks fails by using the handover key management.

Vulnerabilities to DE synchronization attacks: By deploying a rogue eNB, an attacker manipulate the request message for the handover between eNBs or acknowledgement message from the s1path switch as shown figure, by disrupting the NCC value refreshing. In this situation, the NCC value is desynchronized by the target eNB and it can only perform horizontal handover key derivation, and thus there is possible vulnerabilities to compromise the future session keys [25].

Vulnerability to the reply attacks: The establishment of secure link between an UE and a target eNB is destroyed by the reply attacks. Firstly, an encrypted handover request message is destroyed by an attacker as shown in figure between an UE and source eNB. The collected previous handover request messages are sent by the adversary instead of the legitimate one to the target eNB, when the UE wants to move into a target eNB. K_{eNB} in the previous message is received as link key at the target eNB and sends back the previous message NCC value to the UE. After the target eNB sends the NCC value, the UE checks if the received NCC value is equal to the stored NCC value in the UE. Since the received NCC value is comes from the previous message, the check is failure. Thus, the establishment of security link between the UE and target eNB won't be set and the UE needs to launch new handover procedure [26].

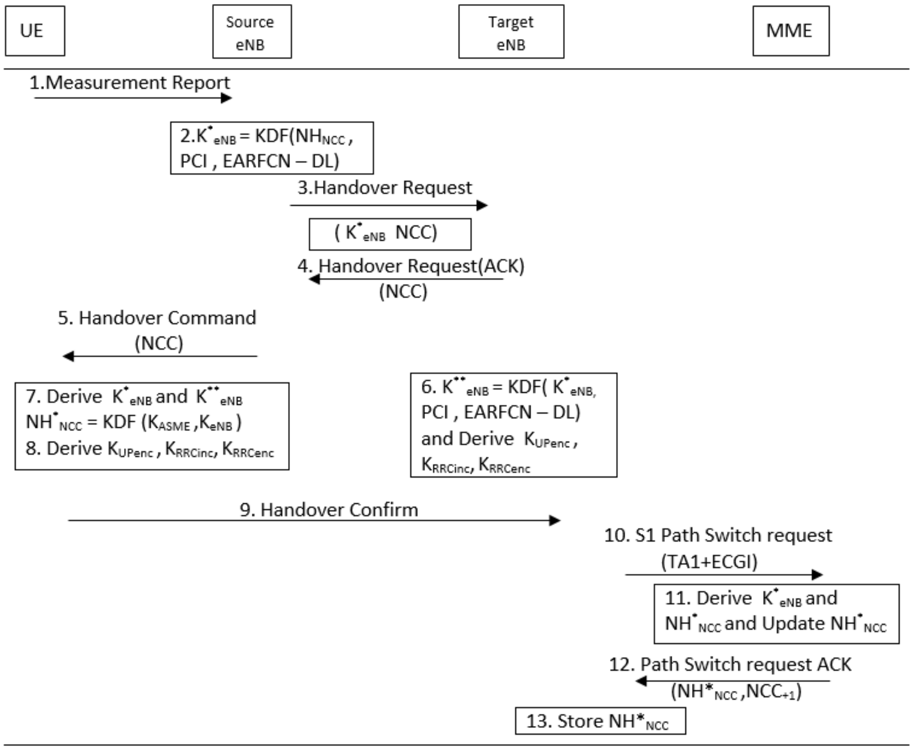
UE
Source eNB
Target eNB
MME
1.Measurement Report
2.K^{*}_{eNB} = KDF(NH_{NCC} , PCI , EARFCN – DL)
3.Handover Request
(K^{*}_{eNB} NCC)
4. Handover Request(ACK) (NCC)
5. Handover Command (NCC)
7. Derive K^{*}_{eNB} and K^{**}_{eNB}
NH^{*}_{NCC} = KDF (K_{ASME} ,K_{eNB})
8. Derive K_{UPenc} , K_{RRCinc}, K_{RRCenc}
6. K^{**}_{eNB} = KDF($K^{*}_{eNB,}$ PCI , EARFCN – DL) and Derive K_{UPenc} , K_{RRCinc}, K_{RRCenc}
9. Handover Confirm
10. S1 Path Switch request (TA1+ECGI)
11. Derive K^{*}_{eNB} and NH^{*}_{NCC} and Update NH^{*}_{NCC}
12. Path Switch request ACK ($NH*_{NCC}$,NCC_{+1})
13. Store $NH*_{NCC}$

Figure 11) Inter-eNB Handover

Security in IMS (IP Multimedia Subsystem)

There are three different types of attackers to attack IP Multimedia Subsystem (IMS). First type of attackers are script kiddies, they are curious but they don’t ability to write advanced hacking programs on their own and their attacks are simple and initiated on the proposed security problems. Second type of attackers are well educated and their goal is to attack on financial issues. Third type of attackers have good knowledge but their attacks on the modern secret activities. The potential dangerous attackers are the IMS employees because they possess incredible knowledge of the system [27].

Security threats to IMS

The scope of the amount of data transformation, data links and problems with security are increasing in number because of the increase in IMS users, mobile subscription and web users. The security threats to IMS are categorized as follows.

External threats: Because of continuous growth in the mobile wireless technology IMS posed security threats are becoming increasingly critical. There are number of groups to support hacking in the IMS. The motivation behind this hacking is not only limited to the profit based but some of the organizations take hacking as prestige. These security threats largely on the databases of the corporate customers by listening through the network, and completed by destroying the material of communication system [27].

Internal threats: internal attacks are more dangerous than the external attacks. These attacks are posed by the employees, consultants, contractors and service providers inside an organization i.e. the information security is breaches by the insiders. These are range from the administrative mistakes and careless behavior to consider actions made by displeased employees, such as providing authorized information to the authors in terms of giving passwords to others and unintentionally releasing sensitive data.

Compliance requirements: Security standards, such as Sarbanes-Oxley (SOX), and IEC/ ISO international standards are developed for the security and privacy in IMS. These requirements are caused to respond IMS operators or providers on security problems in IMS. So these standard organizations frequently take a lot of effort and time to organize issues, development policies and proper control, and monitor compliance [28].

Along with these major threats there are some more threats on services offered by the IMS.

- Services are accessed by unauthorized users
- Network service misusing or disturbing, which leads to denial of service
- Sensitive data is accessed by unauthorized users, which is violation of confidentiality
- Manipulation of sensitive data by unauthorized users, which leads to integrity violation

The IMS system protection is achieved by carrying out of distinctive security services: authentication, authorization, integrity, confidentiality and availability.

The following security areas are proposed for IMS security:

Access security: It provides secure accessing of the IP Multimedia Systems and services to the end user.

Network domain security: The core network of the IMS operators and the traffic flow between visited and home networks is protected by the network domain security. It is used to give hop-by-hop security and it is also provide node protection.

Operation and Maintenance (O&M) Security: O&M security providing control access for the management operations furthermore security of O&M, provisioning and charging interfaces.

Security management: Security functions and attributes are managed by security management [29].

Security architecture in IMS

To protect the IMS system elements with respect to integrity, confidentiality, non-repudiation, availability and authentication a secure IMS system architecture is required. The IMS security architecture is shown below figure 12 [30].

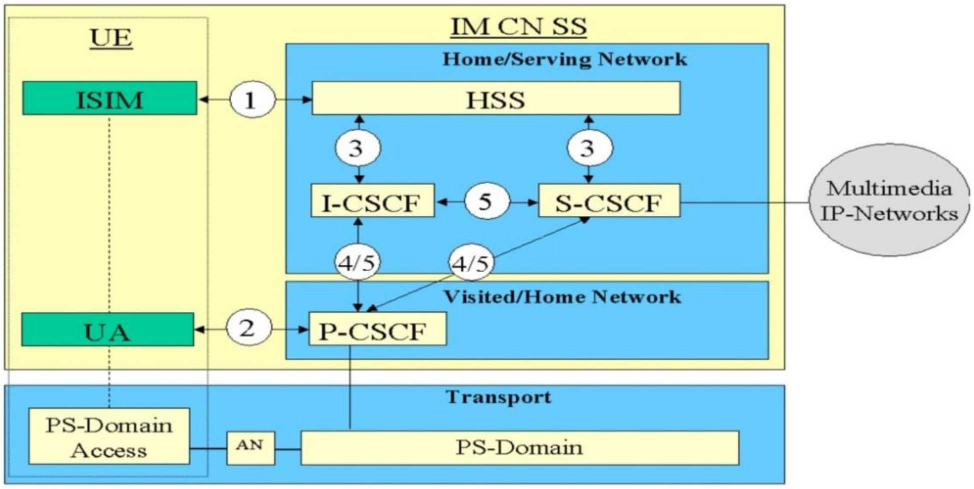

Figure 12) IMS security architecture

The diagram shows the interactions among the CSCFs and both external and internal elements of the IMS and the architecture describes the 5 distinct security associations and necessity for the IMS security protection.

1. Mutual authentication between the IM Services Identity Module and Home Subscriber Server (HSS). Authentication of subscriber ISIM with the HSS is provided by the mutual authentication process and the HSS assigns the performance of subscriber authentication to the Serving Call Session Control Function (S-CSCF).

2. A security association and a secure connection between the UE and a Proxy Call Session Control Function (P-CSCF) is established by network access (Gm) for the Gm reference point protection.
3. The network domain security is allowed for the network domain (Cx) between HSS and Interrogating Call Session Control Function (I-CSCF) and between HSS and S-CSCF for Cx interface protection. TS 33.210 cover this security association.
4. Security between distinctive networks is provided by network domain (Mw) for Session Initiation Protocol (SIP) capable nodes. This security association is provided by TS 33.210 and applicable only when the P-CSCF resides in the Visited Network.
5. Security is provided within the network internally by network domain (Mw) among the SIP capable nodes. This security association enforces when the P-CSCF resides in the home network.

IMS access security-IMS AKA

The purpose of access security in IMS is to address the security between the IMS network and the UE. IMS access security provides following features [30].

- Access security in the IMS is allowing the network to authenticate with the user and it provides authentication of network and the subscriber.
- Access security provides IMS signaling confidentiality and integrity protection.
- Access security provides policy control system, which is used to control the traffic to and from the UE by allowing the network.

The mutual authentication between the UE and the home network is provided by using the IMS AKA procedure. The UMTS AKA procedure concepts and principles are used as same in the IMS AKA procedure. The figure 13 [30] shows the IMS AKA procedure for an unregistered IMS user. The UE register with the IMS CN by sending SIP messages to the IMS CN, Then IMS CN is routed to the S-CSCF.

To access IMS services in the network the IMS users must be authenticated and authorized and these functions are resided in the Universal Integrated Circuit Card (UICC) that is inserted in the UE. To provide multimedia services for the users UE needs a new ISIM (IMS subscriber module) resided in the UICC. IMS functions and authentication keys at the user side might be stored in the ISIM.

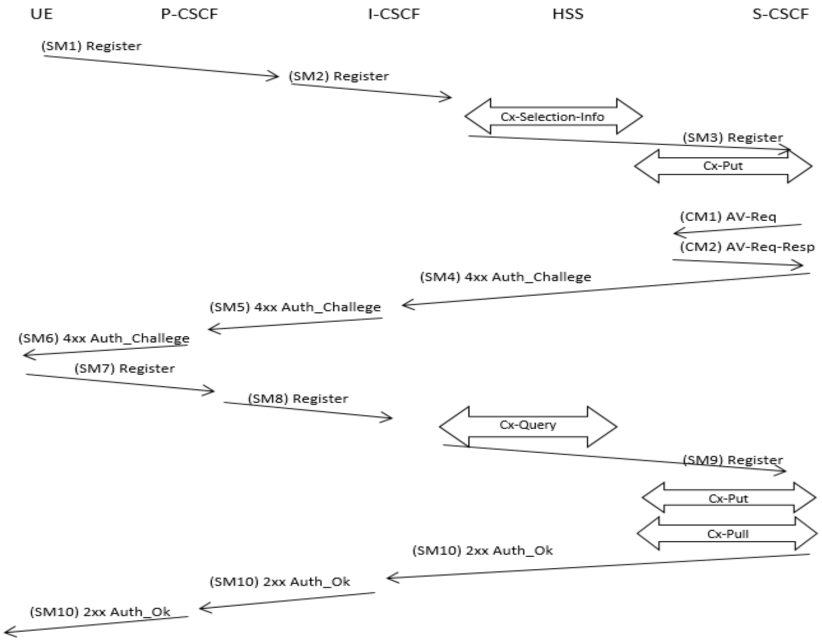

Figure 13) IMS AKA procedure

Security vulnerabilities in IMS

- The system complexity and the UE energy consumption is increased because the IMS UE needs to perform to protocols, one is for the LTE authentication by using EPC AKA protocol and another one is IMS authentication by using the IMS AKA protocol.
- The IMS AKA protocol in the IMS security is vulnerable to the Man in the Middle attacks, lack of sequential (SQN) synchronization and extra bandwidth consumption [29].
- IMS security is vulnerable to the various types of Denial of Service (DOS) attacks. This type of attacks occur when the registration of UE with the network, access authentication is implemented when the P-CSCF sends received registration request from the IMS UE to the core network. In this process an adversary could flood the core network by sending correct packets with invalid IMSI [39].

HeNB security

A HeNB in LTE network is considered as a 4G femtocell for the 3GPP. It is access point of the femtocell installed by a subscriber either in small office or residence to expand the voice coverage as well as high speed data service.

HeNB security architecture

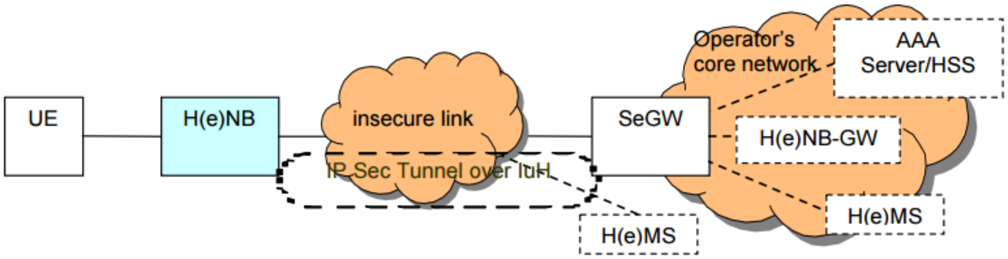

Figure 14) Security architecture of HeNB

In HeNB security architecture there is an E-UTRAN air interface among the UE and HeNB [31]. The core network of the operator in the security network can accessed by HeNB via a Security Gateway. May be there is an insecure link among the HeNB and Security Gateway. The mutual authentication among the operator's core network and HeNB can be performed via Security Gateway. The data transmitted in backhaul link is protected by the security tunnel among HeNB and Security Gateway.

HeNB security threats

The common security threats to HeNB are:

- HeNB causes physical tampering because these are placed in open place and streets.
- Communication among the HeNB and network is secured by the credentials can be compromised if the weak credentials of the authentication are used in the network. These credentials can be broken by brute force attack.
- The attacker performs Man-in-middle attacks at HeNB, when it makes contact to the operator's core network.
- Reply attacks at HeNB can performed by delaying or repeated fraudulently of the valid data transmission.
- The denial of service attacks performed against core network by deny the services to the actual users in the network.
- Eavesdropping of the other user's user data at E-UTRAN.
- The HeNB authentication token is duplicated by the user [32].

Security requirements to HeNB

- Unprotected data inside HeNB should never leave a secure domain.
- HeNB configuration changes and software updates might be verified and signed cryptographically and changes in the configuration shall be authorized by HeNB operator.

- Unauthenticated traffic on the links among the core network and the HeNB shall be filtered out.
- New users should be called for to confirm their acceptance ahead being joined to a HeNB.
- Authentication credentials at HeNB shall be stored inside a secure domain.

Security threats mitigation of HeNB

- Strong authentication algorithms might be used for authentication, confidentiality protection and integrity protection.
- Before securing association with the core network the integrity of HeNB must be validated.
- HeNB software and configuration updates must be in a secure way.
- Unauthorized users cannot access the data at the HeNB in plaintext such as sensitive data including authentication credentials, cryptographic key, information of the user, control plane data and user plane data.
- The HeNB location shall be reliably transmitted to the network.
- IKEv2 is used for establishing a secure backhaul link among the Security Gateway and core network and communication on the backhaul link is based on the IPsec security tunnel [32].

Security vulnerability in HeNB

Security vulnerabilities at HeNB comes because of the unreliable wireless connections in the network. The connections between the HeNB and the UE and the backhaul between the EPC and HeNB, which are sensitive to several kinds of attacks because conversations and information are vulnerable to eavesdropping and interception over them. Lack of robust mutual authentication among the HeNB and the UE and it is vulnerable to many types of DoS attacks [39].

MTC security

The MTC is also called Machine to Machine (M2M) communication and it is viewed as the one of the next developed techniques for future wireless networking. Now a days, the M2M communication is used in many areas such as smart home technology, e-health, factories that are equipped with the sensor networks, education, safety and protection [30] etc. With increase in number of applications in mobile communication provides rapid growing in Machine-Type Communication. Machine-Type Communication is the communication between the different devices and the core network and it is the communication between the devices, where there is no need for the human interaction to communicating with the devices. The MTC devices must possess certain requirements based on the operating conditions. The improvements required in MTC devices are [34]:

- Allowing MTC devices for very low energy consumption for data transmission to ensure long battery life for MTC applications [30].
- Allowing MTC devices for very low cost and they should have low complexity.
- Providing better coverage for MTC devices in challenging locations.
- Covering a very large number of MTC devices per cell [34].

Majority of the communication between the MTC devices carried out by using the LTE channel because of the limitations in the Conventional CSMA/CA-based short range technologies when handling traffic in MTC. The increase in number of MTC devices does the increase in network load even though MTC devices transmit and receive the small amount of data. Primarily MTC used for the collecting and delivering data for measurements. The security architecture of the MTC includes the three different security features as shown in figure 15 [35].

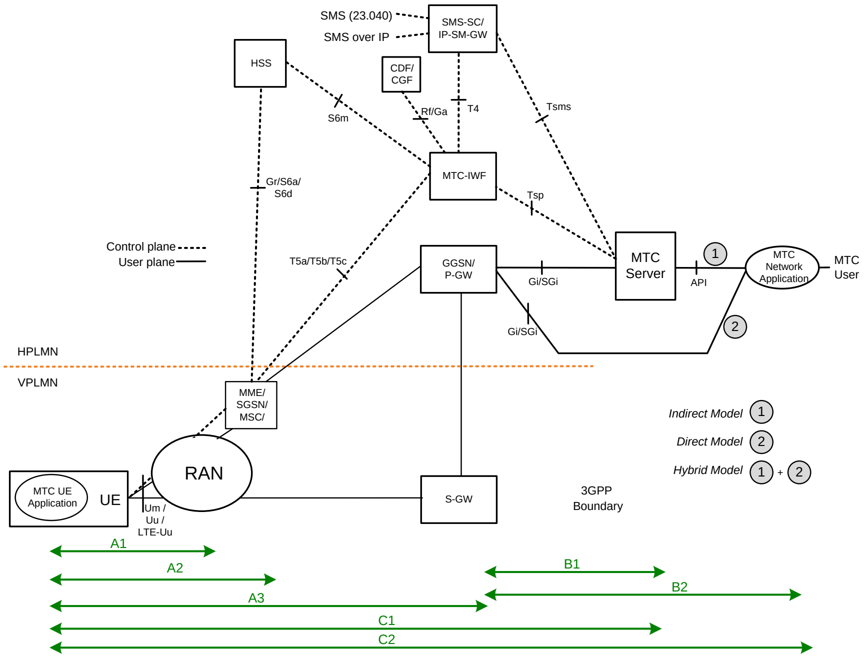

Figure 15) Potential high level security architecture for MTC Architecture for 3GPP Architecture for Machine-Type Communication.

Three security areas of MTC security architecture are:

A. MTC security communication between the MTC device and 3GPP network, which can be further separated to:

A1. MTC security communication between RAN (Radio Access Network) and the MTC device.

A2. MTC security communication between the MTC device and the MME (Mobile Management Entity) or NAS (Non Access Stratum).

A3. MTC security communication among the MTC device and MTC interworking function for 3GPP access and between the MTC device and ePDG for non-3GPP access.

B. MTC security communication between the 3GPP network and MTC server/MTC user, MTC application can be further separated to:

B1. Communication security among the MTC server and 3GPP network and it is further divided based on the MTC server, whether it is outside the 3GPP network and within the 3GPP network for the security aspects in MTC communication.

B2. MTC security communication between the MTC application and 3GPP network.

C. MTC security communication between the entity outside 3GPP network i.e. MTC device/ MTC server device, MTC application and 3GPP network can be further divided to:

C1. MTC security between the MTC server and MTC device.

C2. MTC security between the MTC user, MTC application and MTC device [36].

Security issues in MTC

- The key issue in the MTC security is device triggering, which has three possibilities for the indication of the device triggering i.e. triggering indication when MTC device in detached state, MTC device in attached state and the device has a no connection to the PDN, and MTC device in attached state and device has a connection to the PDN. There are different triggering's such as SMS based triggering, NAS signaling based triggering and user plane based triggering [37].
- Another issue in MTC security is the secure link between the MTC server and MTC device. The intention of the secure connection is to exchange keys between the MTC device and MTC server. The data encryption between the MTC device and MTC server would happen at application layer.
- Rejection of message without integrity protection when the overload occur in MTC communication.
- Congestion control in MTC i.e. block the traffic of the UEs used for MTC device causing the congestion, without restricting the other MTC devices that are not causing a problem.
- External interface security i.e. the communication link between the MTC server and core network (CN) is not over the secure link.
- Restricting the USIM to specific MEs/MTC devices based on the machine type modules associated with the specific billing plan.
- The major issue in the MTC is the concern for privacy because MTC devices are may be controlled by the third party when MTC devices are connected to the individuals.

Security threats in MTC

False network attack: This threat is happened when MTC device is disconnected state, this threat occurs, the attacker posing as a network device to send a trigger indication to the MTC device. In a network MTC devices are different from the UEs because MTC devices are needs through the use of a single rechargeable battery power, without running for a long time. Because of the false network triggering in the network waste the power of the MTC device by awaking it when in detached state. So the false network threat is serious to the MTC devices compared to non-MTC communication [37].

Tamper attack: In this type of threat, the trigger indication which contain IP or TCP application port server that the MTC device should contact. If the IP or TCP application port server is tampered by the attacker, then MTC device may be rejected by the MTC server or establish PDN connection to the wrong MTC server. It will causes the MTC device not to communicate with the correct MTC server and it will also waste the power utilization of the MTC device.

MTC devices and the network causes denial of service attack, if the rejection message is sent without the integrity protection. Because the false base station can duplicate the rejection causes values in the MM such as illegal ME and IMSI unknown in HLR.

Enabled indicators to the network to access the mobile network should be protected to minimize the security threats. In this the attacker can tamper the network by letting many devices connect in the network setup congestion control mechanism with low priority indicators or delay tolerant access to the normal state [37].

Collection of MTC device location information that can be connected individual cause security breaches in the network.

Privacy sensitive information sent by a MTC device and requested by or sent towards a MTC server causes security breaches in the network.

Security requirements

- A mechanism should provide by the system such that only trigger indications received from authorized network entities such as MTC server and MTC application will lead to triggering of MTC device and also to the MTC user to provide a set of authorized network entities. The MTC devices in the network should be responds to genuine trigger messages and only the authentic trigger will be carried to the UEs used for MTC [38].
- Denial of Service (DoS) attack is prevented by using security mechanism in the network.
- According to the rules provided by the 3GPP standard the low access priority should be integrated and protected.
- Mutual authentication among the 3GPP network and the MTC user.
- The authorization of MTC server could be determined by the 3GPP network to send the control plane requests and to send the given trigger to the given MTC device.
- The signaling message between the 3GPP network and MTC server should be integrity protected and confidentiality protected.
- Protection level of security should not be lower when the MTC device within the operator domain.
- Security mechanisms provided by the mobile network are used to:
  Ensure that an MTC server can only communicate with certain MTC devices.
  Ensure that only authorized PDN entities can communicate with the MTC devices.

Ensure that a MTC device can only communicate with the MTC servers of its subscriber and it is not possible to communicate with any other entities.

- The first point of entry into a secure operator network is MTC security GW could be used between the MTC server and core network.
- The use of USIM in the network must be restricted to the specific MEs/MTC devices.

Vulnerability in MTC security

- Security schemes for the communication among the MTC device and the ePDG and for non-3GPP access, which among the MTC applications and the MTC devices and among the MTC applications and for the 3GPP networks are lacks in the Machine-Type Communication (MTC).
- The MTC devices are vulnerable to various attacks such as protocol attacks, physical attacks, credentials compromise and the attacks to the core network.
- Signaling overhead incur between an HSS and the MME when a number of MTC devices are authenticate simultaneously [39].

Conclusion

Rapid growth in telecommunications and development of new technologies did not allow for proper growth and development of new privacy laws to protect users. In the US, there is currently no standard curriculum or program implemented in the public education system to formally teach and train users of the Internet and web enabled devices or promote safe and secure use of telecommunications systems and technology. Until a remarkable advancement in education and privacy laws protecting the essential liberties of civilians are implemented, telecommunications will continue to diminish privacy. Keeping good security high on the requirements list is of utmost importance. When using technology for common tasks, it is easy to store passwords and remove some security barriers to make accessing information faster. Unfortunately, that mindset may not change for the end user, but as for technology professionals and network engineers, the security should be the first thing that comes to mind. Every bit of information that is transmitted needs protection from unauthorized access. There will always be malicious users trying to get what information they can. As new technology advances our networks and devices, so will the need for advancements in user’s security methods. The “bad guys” are constantly looking for the next big break to gain access to end users data and personal information. Strong authentication, devices protection, data stream encryption and verification that security measures are active avoid aby risk to communication network and its user community. Future trends and many evolved security measures and standardization that will shape the next phases of wireless mobile communication infrastructure for better protection, integrity and user experience were discussed. Many of these new features and requirements in 4G and beyond networks are different than their predecessors (2G and 3G) in EPS, eNB, UE, and user privacy by applying new key hierarchy in EPS, permanent security association between UE/USIM and home location register, protection of IMSI, and eNB and device validation. Device security, network security, malware defense, threat intelligence, network access control, advanced data encryption, and over-the-air capabilities are some of many required control mechanisms embedded into 4G and beyond generation of wireless networks.

References

[1] Statista, “Forecast for global shipments of tablets, laptops and desktop PCs from 2010 to 2019 (in million units),” 2015.

[2] Dwyer, “Privacy in the Age of Google and Facebook," Technology and Society Magazine, IEEE, vol.30, no.3, pp.58-63, fall 2011.

[3] US Census Bureau. (2014) International Data Base World Population Summary. [Online]. Available: https://www.census.gov/population/international/data/idb/worldpopinfo.php

[4] Facebook. (2014) Statistics. [Online]. Available: http://newsroom.fb.com/company-info/

[5] Boundless Informant: NSA explainer – full document text, Guardian, June 8, 2013. [Online] Available: http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text

[6] S. Landau. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations," Security & Privacy, IEEE , vol.12, no.1, pp.62,64, Jan.-Feb. 2014

[7] Clement. (2013) "IXmaps — tracking your personal data through the NSA's warrantless wiretapping sites," Technology and Society (ISTAS), 2013 IEEE International Symposium on, pp.216, 223, 27-29 June 2013.

[8] The New York Times (2013). "Secret Documents Reveal N.S.A. Campaign Against Encryption " [Online] Available: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

[9] S. White. (2014). "A review of big data in health care: challenges and opportunities." Open Access Bioinformatics, 6. [Online]. Available: http://www.dovepress.com/a-review-of-big-data-in-health-care-challenges-and-opportunities-peer-reviewed-article-OAB

[10] US Department of State. (2010). Remarks on Internet Freedom. The Newseum, Washington, DC, January21, 2013.

[11] A Yarali, S Rahman, B Mbula, “WiMAX: the innovative broadband wireless access technology,” Journal of Communications 3 (2), 2008, p. 53-63.

[12] Alicia, L, “The Security Mechanism for IEEE 802.11 Wireless Networks,” November 24, 2001.

[13] Gast, M, “802.11 Wireless networks: The definitive guide,” O'Reilly Media, Inc, 2005.

[14] Stephane, G, “Wireless Security and the IEEE 802.11 standards,” London: SANS Institute, 2004.

[15] Baghaei, N., & Hunt, R, “IEEE 802.11 wireless LAN security performance using multiple clients in networks,” 12th IEEE International Conference. 1, PP. 299-303, IEEE, 2004.

[16] Karen, s., Derrick, D., Matthew, S., & Tibbs, C, “Computer Security: Guide to Securing Legacy IEEE 802.11 Wireless Networks,” National Institute of Standards and Technology, Department of Commerce, Gaithersburg: NIST.

[17] Yang CHEN, Xavier LAGRANGE, “Architecture and Protocols of EPC-LTE with relay”, Telecom Bretagne, 13360, 2013, pp.25.

[18] Suyash Tripathi., Vinay Kulkarni, Alok Kuma, “LTE-UTRAN and its Access Side protocols”, Radisys White paper, PP 1-17, September 2011.

[19] Anastasios N. Bikos, Nicolas Sklavos, “LTE/SAE Security Issues on 4G Wireless Networks,” IEEE Security & Privacy March/April 2013 p. 55-62.

[20] Alf Zugenmaier, Hiroshi Aono, "Security Technology for SAE/LTE", NTT DOCOMO Technical Journal, Vol. 11 No. 3, PP 27-30.

[21] 3GPP TS 33.102 version 8.2.0 Release 8, "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Security architecture," 2009.

[22] Net manias Technical Document, "LTE Security 1: Concept and Authentication", July 31, 2013.

[23] Daksha Bhaskar, "4G LTE Security for Mobile Network Operators", CSIAC Journal, 2013.

[24] Ericsson, "Security in the Evolved Packet System," PP 4-8, 2010.

[25] Murtadha Ali Nsaif Shukur, "Review of the LTE and LTE-A Security in Handover Technology," 2013, PP 1-6.

[26] Allouch, Hamid, and mostafa Belkasmi, "Design of distributed IMS by classifications and evaluation of costs for secured architecture", Second International Conference on the innovative Computing technology, 2012.

[27] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks," Computer Networks, Vol. 56, No. 8, PP. 2119-2131, May 2012.

[28] Dubravko Priselac, Miljenko Mikuc, "Security risks of pre-IMS AKA access security solution."

[29] Nauris Paulins, Peteris Rivza, "Vulnerability Analysis of IP Multimedia Subsystem (IMS)," International Conference on Applied Information and Communication Technologies (AICT2012), 26, 27, April 2012.

[30] 3GPP2 S.S0086-B, "IMS Security Framework," February 2008.

[31] 3GPP TS 33.320, "Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B (HNB)/Home evolved Node B (HeNB)," 2010.

[32] Hughes Systique Corporation, "H (e) NodeB Security", 2010.

[33] Oleg Dementev, "Machine-Type Communications as part of LTE-Advanced Technology in Beyond-4G Networks," Proceeding of the 14th conference of fruct association.

[34] Zhang, Yueyu, Jie Chen, Hui Li, Jin Cao, and Chenzhe Lai, "Dynamic Group Based Authentication protocol for machine-type communication", 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, 2012.

[35] Ericsson White Paper, "LTE Release 12-Taking another step toward the networked society," January 2013.

[36] 3GPP, "Machine Type Communications (MTC): Architecture, Features, Standards (Release 10)," October 2012.

[37] 3GPP TR 33.868, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type Communications; (Release 11)," 2012.

[38] 3GPP TS 33.187, "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements (Release 12)," 2015.

[39] Maode Ma, "Security Investigation in 4G LTE Networks," Nanyang Technological Univerity, Singapore.