Bachelor's thesis

Information and Communications Technology

2020

Minh Le

SECURING MOBILITY MANAGEMENT ENTITY IN MOBILE TELECOMMUNICATION NETWORK

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

BACHELOR’S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2020 | 34

Minh Le

SECURING MOBILITY MANAGEMENT ENTITY IN MOBILE TELECOMMUNICATION NETWORK

Mobility Management Entity is playing an indispensable role in the evolution of Evolved Packet Core – the core of the 4G LTE network architecture. This is a key control node for the Evolved Packet Core/Long-term Evolution network with many different significant functions. As the number of Mobile Telecommunication Network’s subscribers has been growing significantly, it has to deal with a huge amount of new security concerns. As a result, securing this component has developed into a serious challenge, leading to the creation of various security standards, recommendations, or frameworks.

Following this development of security, the objective of this thesis was to design a solution to appropriately secure Mobility Management Entity, contributing to securing the core of the 4G LTE network. This study was commissioned by a multinational networking and telecommunications company and consists of researching a solution to meet the security requirements and the implementation of this solution. In terms of the research method, the qualitative analysis is involved in the research process. The final result was established based on the security controls recommended by the National Institute of Standards and Technology (NIST) and the security architecture defined by the International Telecommunication Union (ITU).

KEYWORDS:

Evolved Packet Core, Mobility Management Entity, NIST standards, ITU standards

CONTENTS

FIGURES

TABLES

LIST OF ABBREVIATIONS

0G/1G/2G/3G/4G/5G	0th, 1st, 2nd, 3rd, 4th, 5th Generation – Wireless Telephone Technologies
3GPP	3rd Generation Partnership Project
8-PSK	Eight Phase Shift Keying
AAA	Authentication, Authorization, Accounting
AuC	Authentication Center
BGP	Border Gateway Protocol
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity, Availability
CLR	Cancel Location Request
CSPs	Communication Service Providers
CVEs	Common Vulnerabilities and Exposures
DEAs	Diameter Edge Agents
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EDGE	Enhanced Data rate for Global Evolution
eNB	evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSDPA	High-speed Downlink Packet Access
HSPA	High-speed Packet Access

HSS	Home Subscriber Server
HSUPA	High-speed Uplink Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDR	Insert Subscriber Data Request
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia System
IMSI	International mobile subscriber identity
IMT	International Mobile Telephone
IMTS	Improved Mobile Telephone Service
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T SG 17	ITU Telecommunication Standardization Sector Study Group 17
LDAP	Lightweight Directory Access Protocol
LTE	Long-term Evolution
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MSISDN	Mobile Station International Subscriber Directory Number
MTS	Mobile Telephone Service
NAS	Network Authentication Server
NB	Node B
NIST	National Institute of Standards and Technology
NVD	National Vulnerabiliy Database
OAM&P	Operations, Administration and Management
OS	Operating System
OSI	Open Systems Interconnection model

OSPF	Open Shortest Path First
PDN	Packet Data Network
P-GW	Packet Data Network Gateway
PTT	Push to Talk
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RNC	Radio Network Controller
S-GW	Serving Gateway
SIMs	Subscriber Identity Modules
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSK	Gaussian Minimum Shift Key
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
SSH	Secure Shell
STCP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UTRAN	UMTS Terrestrial Radio Access Network
W-CDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microware Access
WLAN	Wireless Local Area Network
WWW	World Wide Web

1 INTRODUCTION

After almost 60 years since the invention of the cellular network and 20 years since the first packet-switched domain was applied in General Packet Radio Services network, the telecommunication operators have been in a race to upgrade their systems to adapt with the creation of incoming Fifth Generation (5G) technology and the use of Telecommunication network in the Internet of Things (IoT). Although a considerable amount of money has been invested into the Security of Telecom network, there has existed a variety of telecom fraud leading to the loss of 32.7 billion USD annually, according to the Europol’s European Cybercrime Centre. This fraud is the abuse of telecom products and services to take advantage of the operators or their customers. Despite the rapid development of the hardware and software, the latest Telecommunication Generation (Fourth Generation) is still vulnerable to Denial of Service (DoS), tracking, spoofing, or spamming.

There are plenty of reasons for a successful attack from hackers such as software bugs, hardware failures, physical causes or even undiscovered reasons. Providing suitable methods for the whole systems and suitable security implementations on each network component seems to be the necessity to strengthen the network security although it would cost extravagantly. Have been studying in the Telecommunication Security field, the author wants to investigate the solutions to improve the telecommunication network security. Based on the work the author has done, the combination of ITU-T X.805 and NIST800-53 has been chosen as the main approach to develop the security settings that should be applied, thanks to its reliability, scalability and the well-designed security set defined by well-known security organizations.

The Mobility Management Entity (MME) acts as the ”brain” of the Evolved Packet Core in the Fourth Generation/Long-term Evolution Network (4G/LTE), controlling the network flow inside the core network, managing traffic and authenticating subscribers. As a result, the need to secure MME is prioritized due to its crucial role as well as being perceptive to hacker’s attacks. The thesis focuses on enhancing the security of MME by analyzing and implementing X.805 and NIST800-53 Recommendations on the specific node. The configuration on the MME node will be selected based on necessary controls from these two standards, working in different security planes inside the network. The proper configuration will improve the security baseline of the node, minimizing the security risks that it has to face in a secure manner.

The thesis's research will focus on finding the answers to the following questions:

- Why do we need to secure the Mobility Management Entity?
- What are X.805 and NIST800-53 Recommendations and why should they be chosen?
- How can X.805 and NIST800-53 be implemented in order to secure Mobility Management Entity?

The thesis comprises five main chapters: Mobile Wireless Technology, Evolved Packet Core, Mobility Management Entity's Operation and its security, X.805 and NIST800-53 Recommendation, Implementation. The author will begin the first chapter by giving an overview of the Telecommunication Network, the development of the technology from the beginning. Next, the Evolved Packet Core will be illustrated including its components, functions and protocols. Following the Evolved Packet Core, the details of the Mobility Management Entity will be given, focusing on its function and its related security concerns. Then, the thesis continues with the analysis of ITU-T X.805 and NIST800-53 security Recommendations to give an overview of methods that will be applied in the thesis. Lastly, based on the Recommendation, the author will suggest a security implementation for the MME to strengthen the node's security.

2 MOBILE WIRELESS TECHNOLOGY

Mobile Telecommunication Network, also known as a cellular network, is a communication network in which the connections between the User Equipment and the Base Stations are wireless. The network is distributed over land through cells which served by one fixed-location transceiver known as a base station.

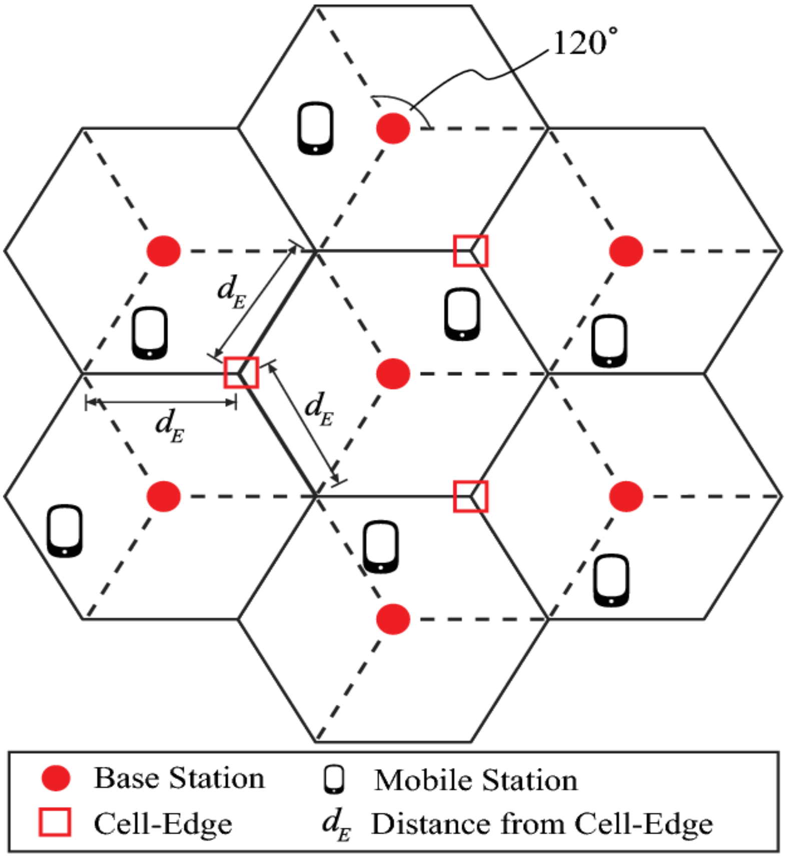


Figure 1. Base station Radio Coverage (IEEE, 2011).

The form of each cell is varied between hexagons, squares or circles; however, the conventional one is hexagons since it covers the most efficient radio signal (Figure 1). These cells, provided by base stations, together can cover a vast geographical area all over the world, building a stable network system for the transmission of voice, network and other types of data. When joined together, these cells can enable a great amount of portable transceivers such as mobile phones, tablets, laptops with a mobile broadband modem. These devices communicate with each other through fixed transceivers over the network, via base stations. Typically, each cell site is able to cover the range from 14 to 34 kilometers (Techopedia). The base stations are responsible for managing the level of signal for devices using Mobile Network. They can make a request to Mobile Switching Center, asking to transfer the control to other Base Station which is receiving the stronger signal from the portal devices. This process is called ”handover”. As a result, even if the equipment is moving between different cells during the transmission, it is supported to maintain the connection, resulting in the consistency and flexibility of the cellular network.

The development of mobile broadband radio access and the expeditious convergence of Mobile Service and the Internet play an important role since the necessity for communication between people all around the world has been evolved significantly. In the area of Mobile Telecommunication Network, the release of a new generation is likely to offer some development in the services, bit rate improvement, new frequency bands, more extensive frequency bandwidth of channels and the development in the quality of simultaneous data transmission rate. From the 1960s, we have been seeing the evolution of Mobile Cellular Network which has been progressed from Zero Generation (0G) to the First Generation (1G) followed by the Second and Third Generation (2G and 3G), and now the Fourth Generation (4G) systems are being deployed worldwide with more than 5 billions subscribers (GSMA Intelligence, 2017).

2.1 Zero Generation (0G)

After World War-II, the Zero Generation of the Wireless telephone was invented which is known as the predecessors of the first generation of cellular telephones. In this pre-cell phone mobile telephony technology, there is a small limited channel to communicate which was established by a small number of operators. Some outdated technologies had been used in the 0G system such as Push to Talk (PTT) which had been using by police and fire personnel, Mobile Telephone Service (MTS) offered by AT&T which was later developed into Improved Mobile Telephone Service (IMTS). The primary users for this generation were policemen, construction foremen, celebrities and others who need basic communication.

2.2 First Generation (1G)

1G is the first generation of cellular telephony networks which was commercially launched in Tokyo, Japan by Nippon Telephone and Telegraph in 1979 (Chinavasion, 2008). In 1980, Nordic Mobile Telephone and Total Access Communication System were introduced which were known as the most popular analog systems in Europe at this time. The main technical development of 1G in comparison with 0G was the use of multiple cell sites and the ability to transfer calls from one site to other sites during the transmission, which is known as ”handover”. In this system, the signal between the base stations and the transceivers (cell phones) needs to be strong enough to establish and maintain the connection between the two, which allows the use of the same channel at the same time in different cells. Due to the significant increase of the demand, a large quantity of new cells were added in order to increase the number of the cells as well as smaller the side of each cell, resulting in providing higher capacity and increasing the quality of transmission which was up to 2.4kbps. However, this 1G faced some drawbacks such as the inability to interoperate between countries, poor voice links and lack of security leading to the susceptibility to unauthorized transceivers.

2.3 Second Generation (2G, 2.5G, 2.75G)

Based on digital technologies, the Second Generation (2G) of wireless cellphones has emerged using the Global System for Mobile Communications (GSM) as the primary standard. Rather than only phone call service as the 1G, 2G has been providing many more services such as picture messages, text messages and Short Message Service (SMS). Furthermore, the technology made the usage of digital transmission instead of analog transmission used in 1G which supported the improvement of voice clarity, noise reduction, environmentally friendly, secrecy and privacy by digital encryption. 2G was first deployed in Finland in 1991 and had been being explosive all over the world, reaching 1 billion customers in February 2004 thanks to the incredible rise of mobile phone usage (OECD, 2004). Since the number of subscribers kept increasing dramatically, some advanced technologies were required to be developed leading to the invention of General Packet Radio Service (GPRS) which is a part of 2.5 generation.

GPRS was a non-voice cellular wireless technology that extended the existing 2G network. In addition to the circuit-switched domain, the 2.5G had been implementing a packet-switched domain which is the main difference in comparison with the 2G. Packet Switching in this development, the data rate was provided from 56 kbit/s to approximately 170 kbit/s as the maximum (Mishra, 2007). This technology allows the interconnection between the Mobile Telephony network and the Internet which viewed phones as ”mobile hosts”. With the connection to the Internet, at this time, the 2G subscribers were able to use multiple internet communication services as the World Wide Web (WWW) and the email services, however, with limited bandwidth and slow data rate.

The limitation of the GPRS system necessitated the development of the Enhanced Data rate for Global Evolution (EDGE) which is also known as 2.75G technology. With the introduction of Eight Phase Shift Keying (8-PSK) modulation to replace the Gaussian Minimum Shift Key (SMSK), EDGE became the complementary technology for Universal Mobile Telecommunications Service (UMTS) which would be known as the Third Generation later. EDGE was first deployed on the GSM network in 2003 in the United States, achieving a rate up to 500 kbit/s theoretically (Mishra, 2007) by implementating the 8-PSK method. EDGE is considered as a subset of GPRS technology and compatible to work over the GSM system because of its flexibility in transferring both circuit switch data and packet switch data. Although there were plenty of developments applied to the Second Generation technology, it still had some limitations such as global roaming, service quality, limited throughput, and capacity, leading to the requirement for a momentous evolution of the Mobile Wireless Communication Network.

2.4 Third Generation (3G, 3.5G, 3.75G)

Since 2G had been widespread and the demand to go online with cell phones increased, it was clear there was a demand of improving the data services and better transmission speed. The Third Generation Cellular networks, known as 3G technology were defined by the International Telecommunication Union (ITU) under the initiative International Mobile Telephone 2000 (IMT-2000) standard. In this evolution, 3G technology was believed to support a significantly higher speed of data rate with the ranges of 144 kbps to greater than 2Mbps (Mishra, 2007). 3G technology, offered a large number of advanced services including video calls, broadband wireless data, mobile television, a global positioning system (GPS), video-conferencing support which brought the world to the new era of the Internet.

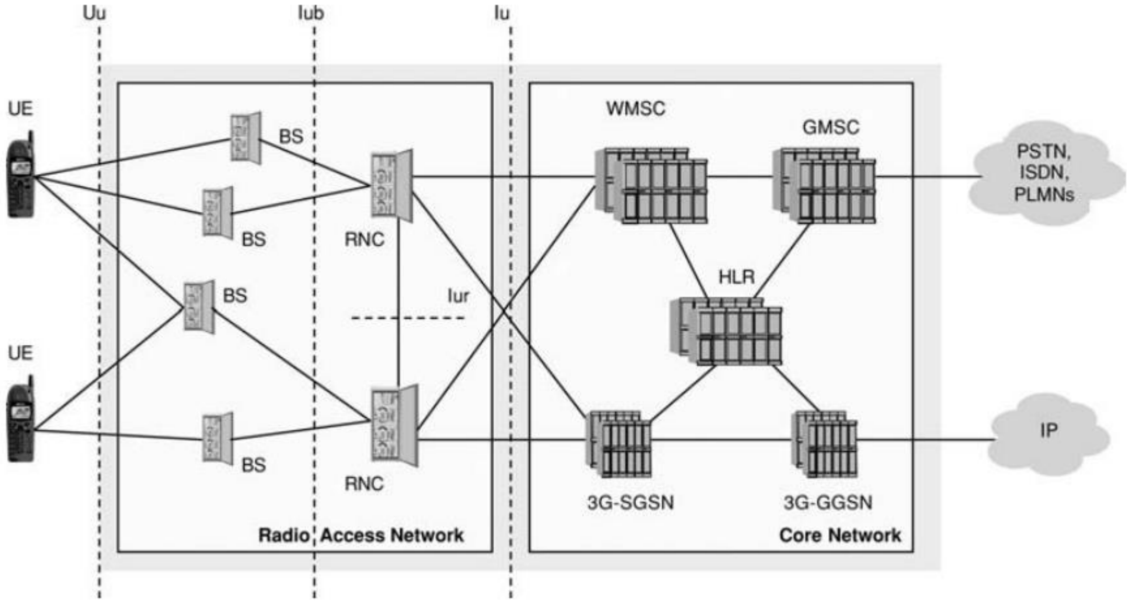


Figure 2. UMTS Infrastructure (Mishra, 2007).

Based on the GSM network, Wideband Code Division Multiple Access (W-CDMA) was accepted as a part of the IMT-2000 family of 3G standard which has been the underlying standard for UMTS. There are 3 domains in the infrastructure of the UMTS network: User Equipment (UE), UMTS Terrestrial Radio Access Network (UTRAN) and the Core Network (Figure 2).

High-speed Downlink Packet Access (HSDPA) is a mobile telephony protocol which can support to upgrade the downlink to reach a much higher speed up to 8-10 Mbps over the 5 MHz bandwidth (Mishra, 2007). The implementation of this technique, with the use of Multiple Input Multiple Output (MIMO) has been increasing the data speeds about 4-5 times in comparison with WCDMA which is referred to as 3.5 Generation. Moreover, 3.75G technology is referring to the implementation of High-Speed Uplink Packet Access (HSUPA) which is known as the UMTS/WCDMA evolution technology. This enhancement boosting the uplink to 1.4Mbps, is related to HSDPA and they should be appreciative of one another.

2.5 Fourth Generation (4G)

4G is the next generation of wireless network which has been developed based on the UMTS architecture of 3G technology. With 4G technology, the concept of ”interoperability” was introduced which meant that devices can be switched to some other alternative wireless access networks such as 3G and 2G (Mahjabeen et al., 2010). For example, if a mobile device lost the connection to a 4G Radio Access Network (RAN), then it can look automatically for some other signal from 3G or 2G infrastructure which provides a higher guarantee for the internet connection wherever it goes. Moreover, in this advanced technology, developers eliminated the use of circuit switching and only use packet switching to transfer the data.

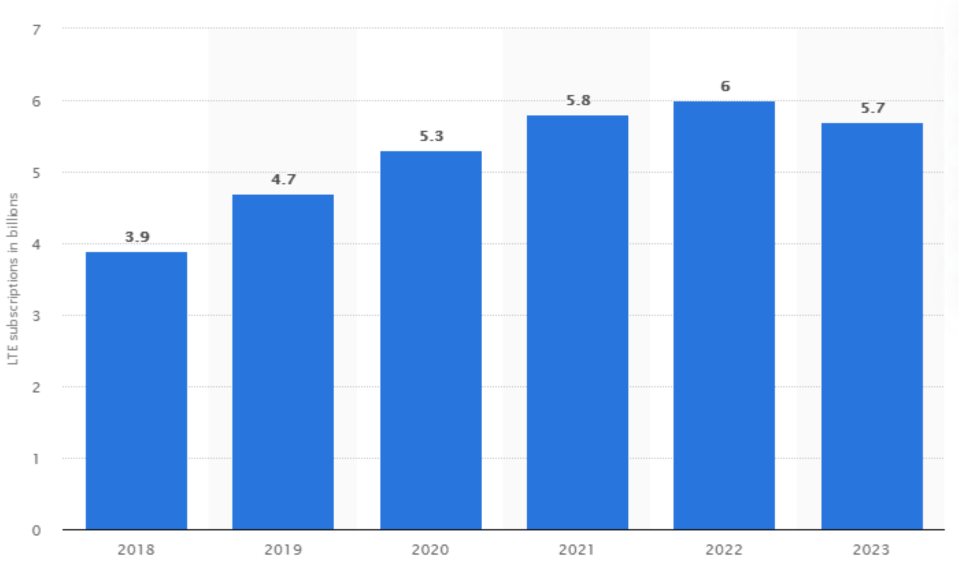


Figure 3. Number of LTE subcriptions worldwide forecast from 2018 to 2023 (Statista, 2018).

As a result, the data transfer speed can reach a much higher rate: 0-100 Mbps when moving at a speed of 60 Kmph or it could be even reached at least 1Gbps if the transceivers are stationary (Meraj & Kumar, 2015). The first-release Long Term Evolution (LTE) standard for 4G was deployed in Sweden in 2009 (Ericsson, 2009) and has been deployed all over the world with billions of subscribers (Figure 3).

3 EVOLVED PACKET CORE

3.1 Overview

The Evolved Packet Core (EPC) is the core network of the Long-term Evolution (LTE) System which is the evolution of the packet-switched architecture used in GPRS and UMTS. Through the development of cellular telephony networks, we have seen many different radio standards have been created and deployed where the GSM, CDMA, WCDMA/HSPA were the most popular (Olsson et al., 2009). In a GSM system, circuit switching was the only method to establish the calling and called parties throughout the telecommunication network which allow all services to be transported over the circuit-switched domain, including SMS and data. In the next system evolution, GPRS offered Packet Switching added beside a developed version of circuit switching in GSM which provides flexibility and efficiency. In this system, circuit switching is still responsible for the voice and SMS transportation; however, packet switching has the responsibility for data and further development of Packet Core network.

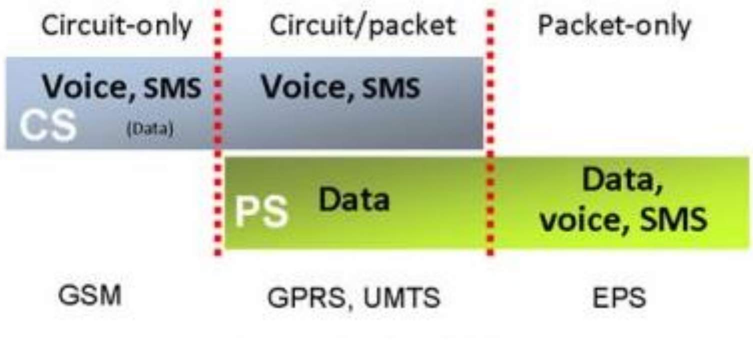


Figure 4. Circuit and packet domains (Firmin, F.).

After few years, UMTS was built over GPRS to be the core system of 3G network with some elements and function evolution but still keep the dual-domain concept as using both Circuit and Packet domains (Figure 4). The Third Generation Partnership Project (3GPP) community which has been developed multiple protocols and standards for mobile telecommunications, has been decided to develop the cellular telephony network to become the ”Mobile Internet” with the purpose ”Internet services that could be accessed from an end user’s mobile device” (Olsson et al.,2009). With this developing orientation, the target for the mobile network is to use the Internet Protocol (IP) to build the network architecture for all network functions and services transportations in which voice can be operated as one IP application. In order to satisfy this requirement, in the 4G LTE network architecture, the Packet-switched technology was decided to be used completely in the core architecture, entirely replacing the Circuit-switched part which still appeared in the UMTS system.

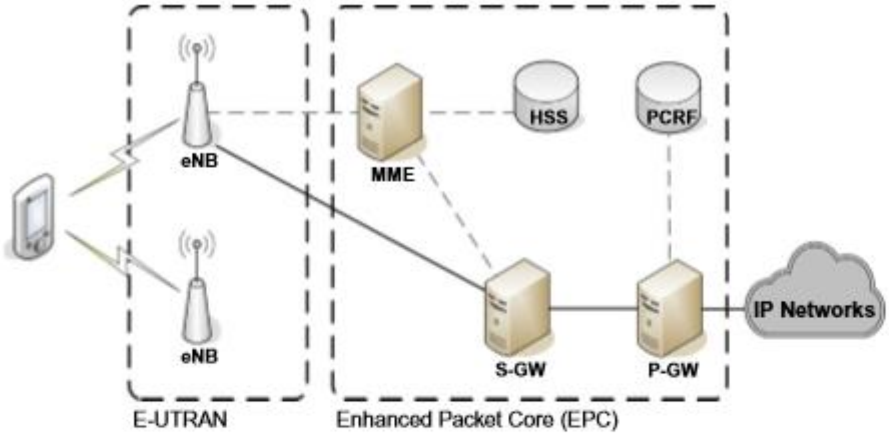


Figure 5. Evolved Packet System (EPS) in LTE Network (Obaidat, Nicopolitidis, &Zarai, 2015).

EPC was first introduced by 3GPP in their Release 8 which is considered as the legitimate solution for the Core network evolution. The development of this architecture seems to be the ”cornerstone” of the mobile broadband revolution in which ”without it, neither the RANs nor mobile Internet services would realize their full potential” (Olsson et al.,2009). In this network architecture, the user data (user plane) and signaling (control plane) are separated which provide the independent scalability between them, resulting in easier network dimension and management. Moreover, high-bandwidth services which are the impeccable combination of IP infrastructure and Mobility is the main concept of the new core network development, enabling the mobile broadband services and applications. Besides that, the ability to broadcast, connect and transfer data over multiple different radio access technologies such as WiMax, Wireless Local Area Network(WLAN), IEEE 802.11ac (Wi-Fi), GSM (2G), UMTS (3G) can provide higher quality and a better experience for end-users and also the operators. Alongside the development of the core network, the evolved version of RANs was also introduced by 3GPP by their Release 10 known as the Evolved UMTS terrestrial radio access network (E-UTRAN) (Obaidat, Nicopolitidis, &Zarai, 2015). With the new air interface system, the

4G LTE network can offer a higher peak rate, shorter round trip time, high flexibility in bandwidth and frequency (Kakadia, Yang, &Gilgur, 2017). Inside E-UTRAN, there is only one component call evolved Node B (eNB) which is the evolution of Node B (NB) in the UMTS system, combining the function of NB and Radio Network Controller (RNC). Together, E-UTRAN and EPC provide the whole 4G LTE infrastructure network known as Evolved Packet System (EPS) which is the standard and deployed all over the world (Figure 5).

3.2 EPC components

The Evolved Packet Core architecture has different components depending on the network operators. However, with the Standard defined by 3GPP, the architecture includes four main components: Mobility Management Entity (MME), Home Subscriber Server (HSS), Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW) which play the crucial roles in the system operation.

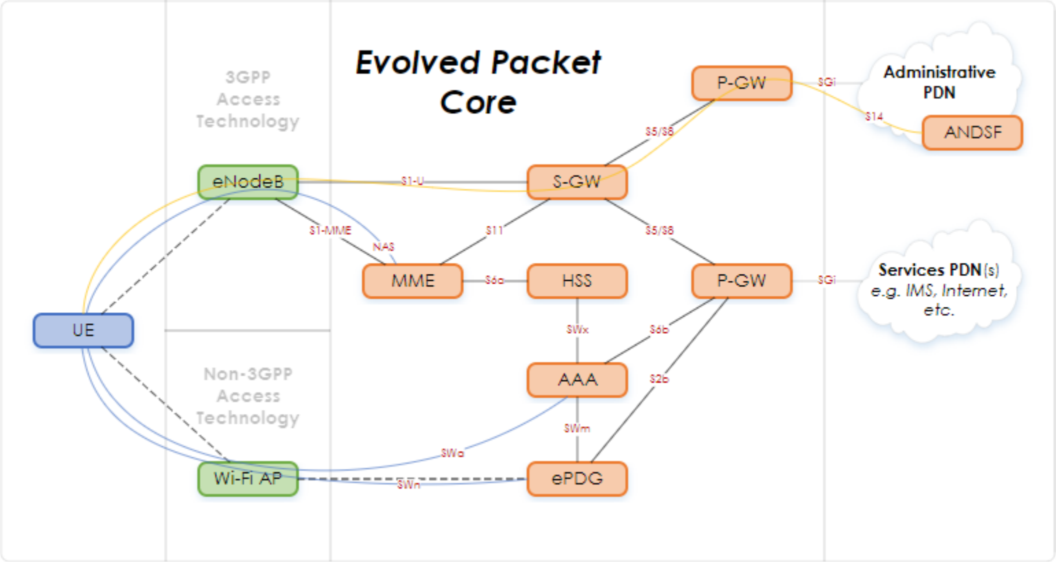


Figure 6. EPC components and their connections (Wikipedia).

- Mobility Management Entity (MME)

Mobility Management Entity is one of the most important nodes in the EPC infrastructure which deals with the control plane. This node has been emerged in the LTE network with the functions to control eNB, MME, S-GW and P-GW selection, playing the crucial role in the Mobility Management (Kakadia, Yang, &Gilgur, 2017). In there, MME has control over session setup, authentication and network access control ensuring the user tracking and security signaling. In addition, MME also has the responsibility to manage other network elements inside EPC like S-GW, HSS and P-GW by the use of signaling messages as well as control the mobility between LTE and other 3GPP networks.

- Home Subscriber Server (HSS)

Home Subscriber Server is a central database containing subscribers' information, playing an important role in the EPC infrastructure. The server is working as a single node and is the combination of the Home Location Register (HLR) and Authentication Center (AuC). Due to these functions integrated, HSS has the ability to authenticate valid Subscriber Identity Modules (SIMs), who are trying to connect to the system, validating their authorization and providing Quality of Service (QoS) to connect to LTE network. Moreover, HSS allows Communications Service Providers (CSPs) to perform management functions such as SIMs card activation and deactivation, hierarchical discrimination based on customer's subscription. HSS also supports the roaming to non-3GPP networks, making the flexibility of network connection and authentication by combining with Authentication, Authorization, Accounting (AAA) server (Figure 6).

- Serving Gateway (S-GW)

Serving Gateway is an important component of EPC infrastructure which deals with the user plane. This node works as a router having the responsibility for routing and forwarding user data packet between UEs and the packet data network (PDN) (Obaidat, Nicopolitidis, &Zarai, 2015). Moreover, S-GW is the ”anchor point” for the LTE network, working for ”handover” when the users keep moving between different radio cells and internetworking with other 3GPP accesses. The component allocates IP address for UE, have responsible for IP data packets transmission and can be switched to another S-GW when a mobility event occurs, providing the flexibility of network connection.

- Packet Data Network Gateway (P-GW)

Packet Data Network Gateway is the node between the EPC infrastructure and the external network, working as a bridge for the communication between the LTE network and other PDNs such as the Internet. This node function is to also manage the quality of service (QoS), filtering packets, applying policy rule, IP allocation,.. for UEs. In detail, P-GWs are able to perform dynamic host configuration protocol (DHCP) functionality or it can query and transfer from a nearby external DHCP server. Moreover, This is the anchor for mobility between 3GPP technologies and non-3GPP technology such as Wi-fi and WiMax. In some cases, the S-GW and S-GW can be implemented together in one node to perform the function combination.

3.3 Diameter Protocol

Diameter is the main protocol used in the interfaces between HSS, MME, S-GW, and P-GW in the LTE infrastructure, replacing the Signalling System No. 7 (SS7) which was the foundation for signaling in 2G and 3G circuit switch networks. It is an authentication, authorization and accounting protocol used in the LTE network and IP Multimedia System (IMS) network. This protocol is an upgrade path for Remote Authentication Dial-In User Service (RADIUS) and the improvement of Lightweight Directory Access Protocol (LDAP), strengthening the reliability, flexibility and security of the connection between EPC elements.

There are significant reasons for the emergence of Diameter that network operators switch to, most of them relating to security issues. In 2014, there were several SS7 vulnerabilities had been published which allowed attackers to keep track of cell phone users from virtually anywhere which the success rate of 70% (Wikipedia). Due to the ”SS7 vulnerabilities and attack exposure report” from Positive Technology in 2018, there were many other threats that were considered the security flaws in the mobile network such as Subscriber information disclosure, Network information disclosure, Subscriber traffic interception, fraud and Denial of service with high potential risks as shown in Table 1. These threats, when appeared in the Network, will generate reputational and financial risks for the operators due to financial losses, loss of customer’s faith, privacy violation and may put the companies at risk of collapsing (Positive Technology, 2018). Although the ratio of Network information disclosure, Subscriber traffic interception and Fraud had been decreased from 2015 to 2017, the risk of these network vulnerabilities remained so tremendous, meaning that the SS7 interfaces were pretty prone to these vulnerabilities. Because of this fact, the necessity to utilize other protocol standards to maintain the transmission inside the network was highly appreciated. Furthermore, the orientation of the LTE network is to move the telecommunication network forward ”all IP” connections and the Diameter could meet the requirement of that since this is an IP-based protocol. With the use of this new protocol, the interfaces will be provided with sufficient security than SS7 since the Diameter has the usage of Internet Protocol security (IPsec) by default to authenticate the network connection. Besides that, with the development over AAA functionality from RADIUS and the use of Network Authentication Server (NAS), the authentication process in Diameter went smoothly and lead to the security assurance. With the implementation of Transport Layer Security (TLS), Diameter is also offering a proper and credible method to encrypt the data flow inside the network, enhancing the reliability of the data transmission since with the data encrypted, hackers cannot intercept the transmission between network entities even when they are inside the core network. Also, one of the key measures to protect the core LTE network and strengthen security is the ability to hide the network components. With the usage of Diameter, the IP address of internal components cannot be revealed since the IP has been changed by an interconnected router, preventing attackers who are trying to gain access to the core network as well as the man-in-the-middle attacks.

Table 1. Vulnerabilities in Telecommunication Networks (Positive Technology, 2018).

Threat Type/Year	2015	2016	2017
Subscriber information disclosure	100%	100%	100%
Network information disclosure	100%	92%	63%
Subscriber traffic interception	100%	100%	89%
Fraud	100%	85%	78%
Subscriber denial of service	100%	100%	100%

Although there has been a huge amount of money and effort from the developers and operators to progress with Diameter protocol as the new one for the mobile telecommunication network, the protocol unfortunately still kept almost the same risks as SS7. With proper methods, the mobile network is still visible for attackers to investigate and exploit some high potential threats as Subscriber location discovery, Interception of SMS messages, DoS attack against a subscriber and fraud although they are not straight forwarded as the same in SS7 (Positive Technologies, 2017). These facts could prove that the operators need to implement some other techniques rather than the Protocol to make the whole Core network securer.

4 MOBILITY MANAGEMENT ENTITY’S OPERATION AND ITS SECURITY

4.1 Functions and Operations

Mobility Management Entity which is the key control node for the LTE network is also the primary signaling node in the EPC. Besides the main function - Mobility Management, MME also has the responsibilities for Network Access Control, Mobile devices’ authentication, Roaming Management, Tracking Area Management, Load Balancing between S-GWs (RCR Wireless, 2014).

Management Entity seems to be the most complex function that MME performs which provides the inter-working of UEs, S-GW, P-GW, connecting them and doing the ”handover” if needed. The node, acting as the ”referee” to control the load balancing between S-GWs, directing UEs to more suitable S-GWs to connect. It also performs the tracking area management which keeps track of user devices in ”connected” mode at eNB level and in idle mode at tracking area level (a group of eNBs) (Kakadia, Yang, &Gilgur, 2017). Moreover, MME will create and manage the tracking area list of idle-mode UEs, recording their locations periodically or when occurring the movement across different areas. As a result, the mobile network can be connected immediately with the accurate profiles of subscribers wherever the devices are in the range of radio transmission.

Network access control and subscriber management are also the crucial functions of MME in the EPC core network. When the UEs first register to the network, MME is responsible for initiating the subscriber authentication, communicating with HSS to provide UEs with the rigorous connection and activity-related information. Moreover, MME supports to generate and allocate temporary identities to UEs, supporting outbound and inbound roaming among other EPC systems and also some other networks such as 2G or 3G (Obaidat, Nicopolitidis, &Zarai, 2015). Furthermore, MME is the node in EPC which can retrieve the subscribers’ profile from UE’s home network to determine the QoS, data rate, packet network connection, and roaming restriction should be applied to UEs.

4.2 MME’s security

Since MME is the key control node in the EPC architecture with Mobility management, authentication and some other functions mentioned in the previous part, it has become the ideal target for hackers to attack the core network infrastructure. With the use of Diameter as the signaling protocol as other components in the core network, MME is visible for almost all the threats that appear from the protocol such as DoS attacks and fraud.

- DoS attacks

A DoS attack is a type of attack that interrupts the customers to use some normal functions of services or even collapse the whole system. In the case of MME, two DoS methods had been discovered in the event “Black Hat Europe 2016” (Sheridan, 2016). They were deploying DoS using Cancel Location Request (CLR) and DoS using Insert Subscriber Data Request (IDR). In both methods, the attackers need to investigate to have the information for the victim’s international mobile subscriber identity (IMSI). To achieve this information, they need to obtain the victim’s Mobile Station International Subscriber Directory Number (MSISDN) and the Diameter Edge Agents (DEAs) that the victim is connecting to (Lucian, C., 2016). After that, they would send a routing information request through the DEA they achieved to the targeted HSS server, gaining the information for IMSI and the identity of MME that the victim is currently connecting to. Once the prepared information compassed, in the first method, the attackers can masquerade as an HSS and send a CLR message to MME, causing the MME to disconnect with the targeted subscribers. There is a fact that, when a subscriber attempts to re-attach to the telecom network, their device has to send about 20 messages to the MME (Lucian, C., 2016). With that, by detaching thousands of virtual devices, the attackers are able to flood a huge number of messages into MME, which may lead to the collapse of MME and the whole network. In the second method, the attackers will imitate as an HSS server and send the IDR to the victim’s MME to set the “no services” value, preventing user to connect to the network permanently until they contact and ask the operators to fix.

- Fraud

The fraud in the telecommunication network is the abuse of telecommunication services or products to illegally take advantage of the operators or their subscribers (Europol).

Since the MME has the responsibility to authenticate the users and authorize, generate their profile with HSS, it will be the target for this kind of attack. Attackers will change their subscriber profile to gain more or even unlimited usage of services without paying any fee. With the pre-required as the same as in DoS attacks, the attackers need to achieve IMSI to begin any exploit. With that, attackers will continue to acts as an HSS server, sending IDR messages to MME to change the rule applied to the specific subscriber (Positive Technology, 2017).

Furthermore, LTE has been operated as an “all IP” network connected to the Internet which makes the base station visible directly for the attackers. The MME, with the main function of Mobility Management, has the responsibility to manage a large number of eNB which acts as the interconnected point between two different eNB. This fact could lead to the problem that, if attackers can invade an existed eNB or they can counterfeit one and get the connection to MME, they can compromise the whole system (Zhong et al., 2019). Moreover, in 2019, there was a Common Vulnerabilities and Exposures (CVE) had been found. Due to the CVE-2019-16026 detail description from National Vulnerability Database (NVD), this new CVE has been emerged from the implementation of the Stream Control Transmission Protocol (SCTP) on Cisco’s MME, allowing attackers to perform DoS attacks. In this case, the attackers would leverage as a man-in-the-middle between the transmission of eNB and MME, modifying or sending the crafted SCTP message, which then, can stop MME to send SCTP message to eNB, interrupting the connectivity from users.

The protection for the core network should be performed for all layers of the network as well as every component node inside the network. Protecting MME properly will not prevent the attacks completely but can contribute a positive manner in the security of the whole system. The world currently has been changed dramatically, the development of hardware or software is inevitable with some threats hole inside, leading to the requirement of applying security standards which contains the information security policies investigated to support the systems maintained securer. MME is the key control node in EPC because of its function of mobility management, user authentication,… As a result, if the hacker can go inside this node, they can use free services, steal the data from the HSS database, or even collapse the whole EPC infrastructure, harming both operators and their customers. In the next chapters, I will have investigated NIST800-53 and X.805 standard, applying them into MME’s configuration to enhance not only the node’s security but also the whole system’s.

5 X.805 AND NIST800-53 RECOMMENDATION

In the world, where the cybercriminal has been increased significantly since the past few years, the telecommunications and information technology industries have been seeking for cost-effective security solutions to make their service safer and stable. According to the International Telecommunication Union (ITU), ”A secure network should be protected against malicious and inadvertent attacks and should have high availability, appropriate response time, reliability, integrity, scalability, and provide accurate billing information”. The security in the products and services offering to the customers is crucial to the overall network security. Since the Telecommunication services have been growing expeditiously, the security for them should catch up with these developments to provide the appropriate solutions. In order to achieve the final security solution for a multi-vendor environment, the standard security architecture should be investigated and applied properly to provide secured end-to-end connections.

5.1 ITU-T X.805 Recommendations

The X.805 Recommendation Security architecture for systems providing end-to-end communications had been developed by ITU Telecommunication Standardization Sector Study Group 17 (ITU-T SG 17) and was published in 2003 (ITU-T, 2003). The group has been developing many sets of well-recognized Recommendations on security such as X.509 for cybersecurity, Y.3172 for machine learning and some other sets for specific purposes that have been appreciated and applied in a large number of systems all over the world (Wikipedia). The X.805 Recommendation is the one that has been the updated provision from X.800 – Security Architecture for Open Systems Interconnection for Consultative Committee for International Telephony and Telegraphy applications published from 1991. It was created to solve the security concerns about the management, control, use of network architecture and their services with the mission to detect, predict and correct security vulnerabilities (ITU-T, 2003). The architecture has the responsibilities to address the following essential issues:

- What kind of protection is needed and against what threats?
- What are the distinct types of network equipment and facility groupings that need to be protected?

- What are the distinct types of network activities that need to be protected?

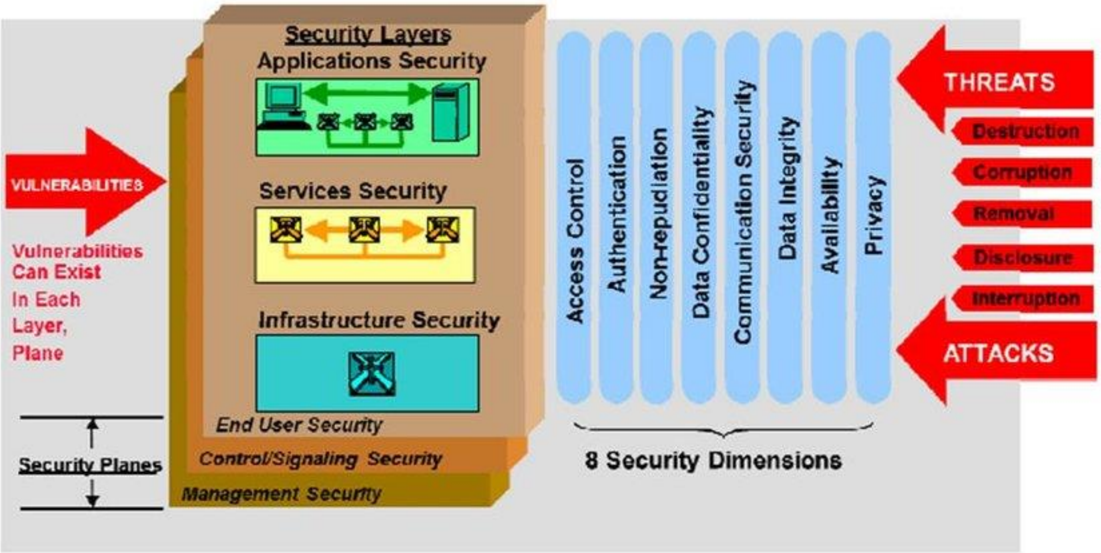


Figure 7. X.805 Security Architecture (O'Hanlon, P.).

To have a detailed answer to these questions and to build a convenient solution for a wide variety of different networks, they have investigated and separated the architecture into 3 components: Security Planes, Security Dimensions and Security Layers (Figure 7).

5.1.1 Security Planes

In the security planes, ITU-T has defined 3 different planes as End-User Security, Control/Signaling Security and Management security. These planes specify the activities through the network classified by their functions and responsibilities on the end-to-end connection from the operators to the customers.

- Management Security plane

In the telecommunication network, the management plane has the potential responsibility for configuring, monitoring, providing management through the network. As a result, management security planes should ponder on securing the Operations, Administration and Management (OAM&P) function of network elements, transmission facilities,... Some protocols included in the Management Security plane are Simple

Network Management Protocol (SNMP), Secure Shell (SSH), File Transfer Protocol (FTP).

- Control/Signaling Security plane

This plane has concerns about the flow of the network, the communication between network elements, the way to deliver the services, applications across the network. It contains the information security for routing and switching machines that need to determine the best routes or switches inside the network transmission. The traffic of this security plane contains some following protocols: Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Session Initiation Protocol (SIP), etc.

- End-User Security Plane

End-User Security Plane concerns the security of access and the availabilities of services and applications offered by the network operators to their customers. Many protocols are working on this plane such as Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Transmission Control Protocol (TCP), etc.

5.1.2 Security Layers

Security Layers are the separate categories that have different security vulnerabilities concerned. The method used in this end-to-end security solution is the hierarchical approach, where each layer will have to be considered with several security dimensions based on the network equipment and facility grouping.

Table 2. Security Layers.

Security layers	Description
Infrastructure security layer	- Represents building blocks of networks, services and applications
Services security layer	- Security of services which are offered to customers - For example: Internet Connection, Domain name Services
Applications security layer	- Security of network-based applications accessed by customers

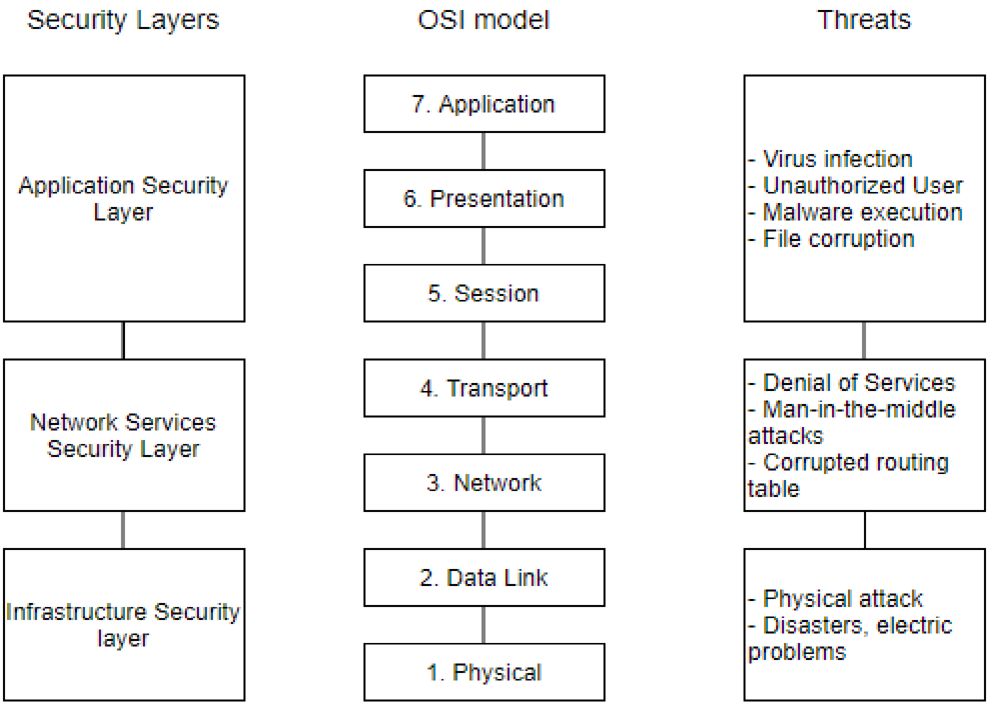


Figure 8. Security Layers, OS model relationship and their threats.

The security layers identify how network security should be implemented in products and where to apply the proper solution. There are 3 different security layers in each security plane: Infrastructure Security Layer, Services Security layer, Application Security Layer with the description provided in table 2. Figure 8 shows the relationship between Security Layers and OSI reference Layers.

5.1.3 Security Dimensions

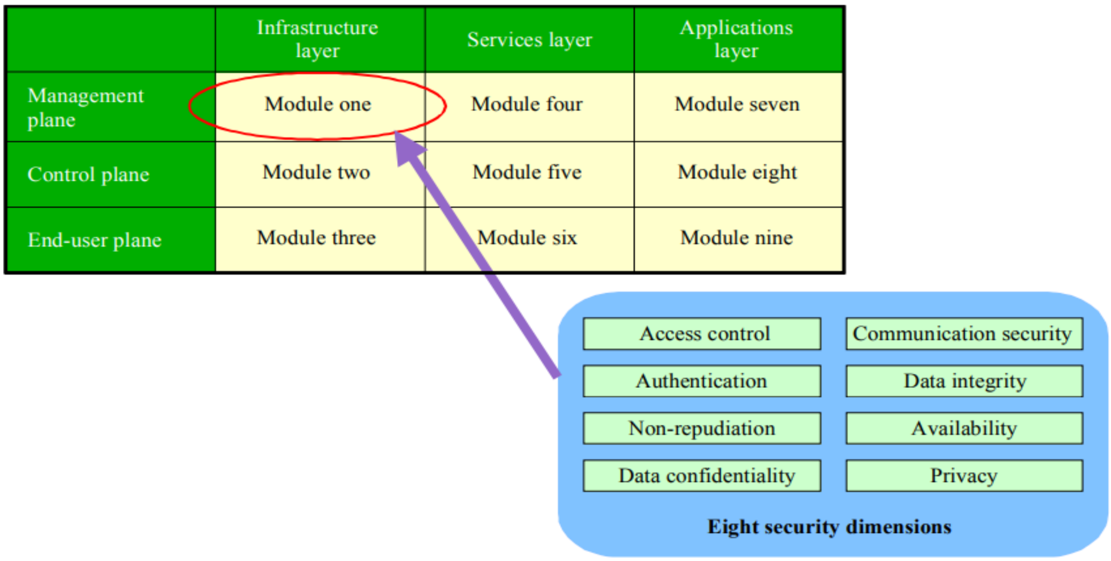
Each security dimension defined by ITU-T is a set of security measures that are designed to present a network security aspect. There are 8 security dimensions introduced in the X.805 Recommendation which cover almost all forms of network security; however, they are not limited to the network and can be extendable. The dimensions and their description will be represented in Table 3.

Table 3. Security Dimensions.

Security Dimension	Description
Access Control	Prevent unauthorized use of network elements, data, services and applications
Authentication	Ensure the validity of claimed identities
Non-repudiation	Prevent an individual or entity from denying having performed an action on the resources (data, services, applications)
Data confidentiality	Protects data from unauthorized disclosure
Communication	Ensure the data flow just only transferred between authorized end points
Data Integrity	Assurance of the accuracy and consistency of data
Availability	Ensure that information can be accessed by authorized users
Privacy	Having ability to protect personally sensitive information from the observation of network activities

5.1.4 Security Module Intersection

Defining the overview of each security component can give us in detail of security planes, layers and dimensions that the X.805 Recommendation concerns. To provide the final solution, we have to connect these components defined together to provide the connection between them in a secure manner which has been illustrated in Figure 9. From there, we can see the way to apply the security policies, rules through the network to finalize the completed security solution.



	Infrastructure layer	Services layer	Applications layer
Management plane	Module one	Module four	Module seven
Control plane	Module two	Module five	Module eight
End-user plane	Module three	Module six	Module nine

Figure 9. Security Module, Layer and Plane Intersection (ITU-T, 2003).

5.2 NIST800-53

NIST800-53 provides a catalog of security and privacy controls to support the secure and resilient federal system security which has been developed and published by the National Institute of Standards and Technology (Nate Lord, 2018). These controls are the operational, technical protection with the purpose to maintain the confidentiality, integrity and availability (CIA) of the network system. They are focused on the risk management framework outlined in the 800-37 provision, security requirement in Federal Information Processing Standard (FIPS) 200 and the solution for other organizational risk assessments (Wikipedia). There are 18 security control Families available in the NIST800-53 Recommendations: Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), System and Communication Protection (SC), Awareness and Training (AT), Configuration Management (CM), Contingency Planning (CP), Incident Response (IR), Maintenance (MA), Media Protection (MP), Personnel Security (PS), Physical and Environmental Protection (PE), Planning (PL), Program Management (PM), Risk Assessment (RA), Security Assessment and Authorization (CA), System and Information Integrity (SI), System and Services Acquisition (SA) (NIST, 2013). The process of applying these security controls does not require all of them, the key is to select a subset of controls that are necessary to protect the assets properly from different types of attacks.

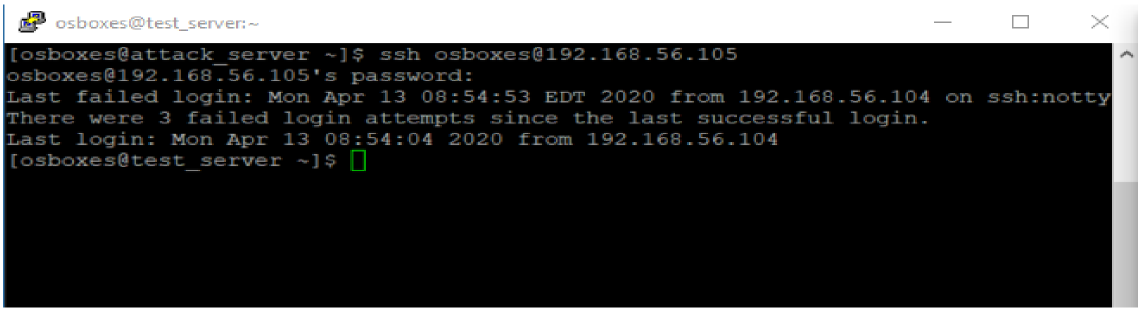
6 IMPLEMENTATION

Over the world, MME nodes have been built based on many different Operating Systems (OS) such as Windows Server, Linux, MacOS. However, the Linux Operating System seems to be the most popular one due to its Open Source Nature, better security, customization, better communication support and some other advantages. Because Linux is an open-source OS, there are many modifications based on the Linux kernel around the world, leading to a huge number of different distributions that share the same mechanism of Linux kernel but still have their characteristics. In this study, the author is going to have the implementation of security controls based on CentOS distribution which will be virtualized by VirtualBox – an open-source hosted hypervisor for x86 virtualization. Since there are thousands of Controls available, each of them requires one or more configurations to reach the highest security, two configurations will be implemented in the lab, which will take an important part in the Boundary Protection and Session Lock Control to show the ways they will affect the server performance.

6.1 Environmental Setup

In this lab, there are 3 servers created (test_server, attack_server, normal_server) for testing by using VirtualBox (VDI) images available at https://www.osboxes.org/centos/. ”test_server” will be the one where to apply the control policies while ”attack_server” will be the one where to exploit the Brute-force attacks over SSH or other kinds of accessing forward test_server. Besides, “normal_server” will be used to verify the correct configuration on the policy control in some cases. They are sharing the same network from where, by default, they can have SSH connection towards each other. The ”test-server” will have the IP address of 192.168.56.105, IP address of ”attack_server” is 192.168.56.104 and for the ”normal_server” is 192.168.56.103. Here is the example of using SSH to connect from ”attack_server”, ”normal_server” to ”test_server” to verify the connection.

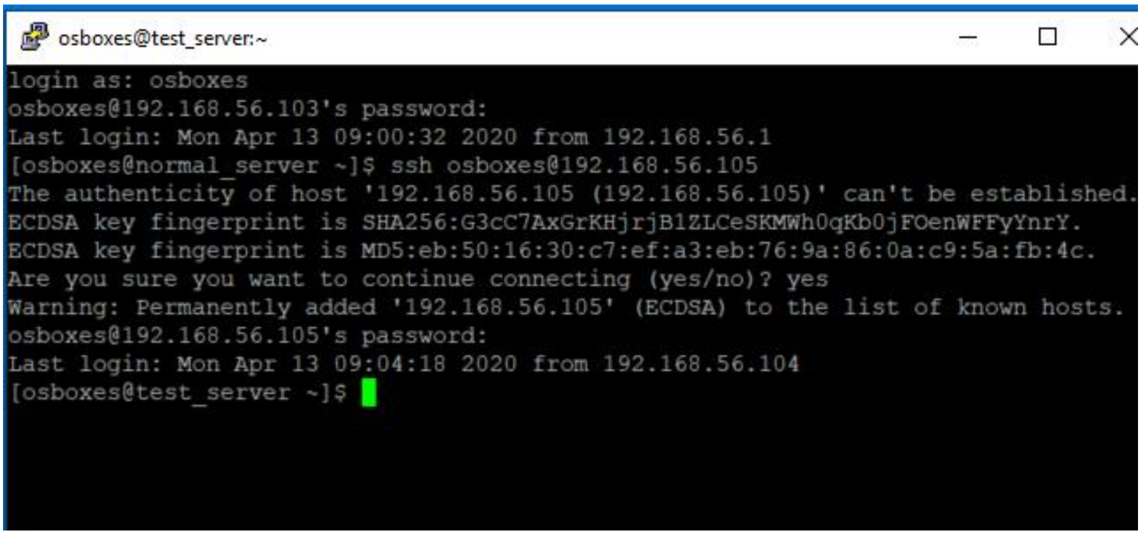
- ”attack_server” to ”test_server”: successful



```
[osboxes@attack_server ~]$ ssh osboxes@192.168.56.105
osboxes@192.168.56.105's password:
Last failed login: Mon Apr 13 08:54:53 EDT 2020 from 192.168.56.104 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Mon Apr 13 08:54:04 2020 from 192.168.56.104
[osboxes@test_server ~]$
```

Figure 10. Testing SSH connection between ”attack_server” and ”test_server”.

- ”normal_server” to ”test_server”: successful



```
login as: osboxes
osboxes@192.168.56.103's password:
Last login: Mon Apr 13 09:00:32 2020 from 192.168.56.1
[osboxes@normal_server ~]$ ssh osboxes@192.168.56.105
The authenticity of host '192.168.56.105 (192.168.56.105)' can't be established.
ECDSA key fingerprint is SHA256:G3cC7AxGrKHjrjB1ZLCeSKMWh0qKb0jFOenWFFyYnrY.
ECDSA key fingerprint is MD5:eb:50:16:30:c7:ef:a3:eb:76:9a:86:0a:c9:5a:fb:4c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.105' (ECDSA) to the list of known hosts.
osboxes@192.168.56.105's password:
Last login: Mon Apr 13 09:04:18 2020 from 192.168.56.104
[osboxes@test_server ~]$
```

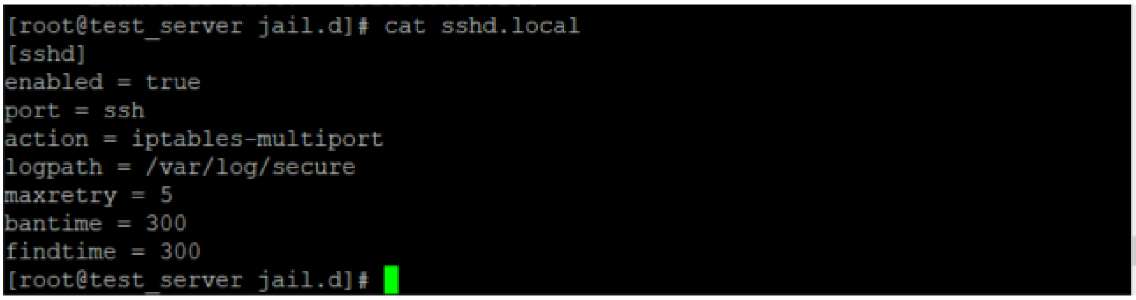
Figure 11. Testing SSH connection between ”normal_server” and ”test_server”.

6.2 Secure SSH Connection from Brute-force attacks (SC-7)

Defined in the System and Communications Protection Control Family, the Boundary Protection Control (SC-7) is applied to ensure that the connection to external networks can be established and managed through interfaces that have the Boundary Protection. Traffic flow would be applied to these interfaces to allow or restrict incoming connection.

In the configuration, to secure the SSH connection from Brute-force attacks (the attacker try to guess the correct password of authorized users by submitting a plenty of different passwords), “Fail2ban” software will be used. This software will scans log files and bans the IPs where request a variety of logins but with password failure. As a result, the use of this software can reduce the rate of incorrect attempts and log the malicious IPs with a defined amount of time. This implementation will improve the ”Access control”, ”Authentication” and ”Privacy” from security dimensions, taking part in the Application Security Layers in the Management Security Plane.

The installation of Fail2ban software can be found from https://www.evoluso.com/how-to-install-fail2ban-on-centos-7/. When the software successfully installed, we can set our rules for the SSH connection from /etc/fail2ban/jail.d/sshd.local file:



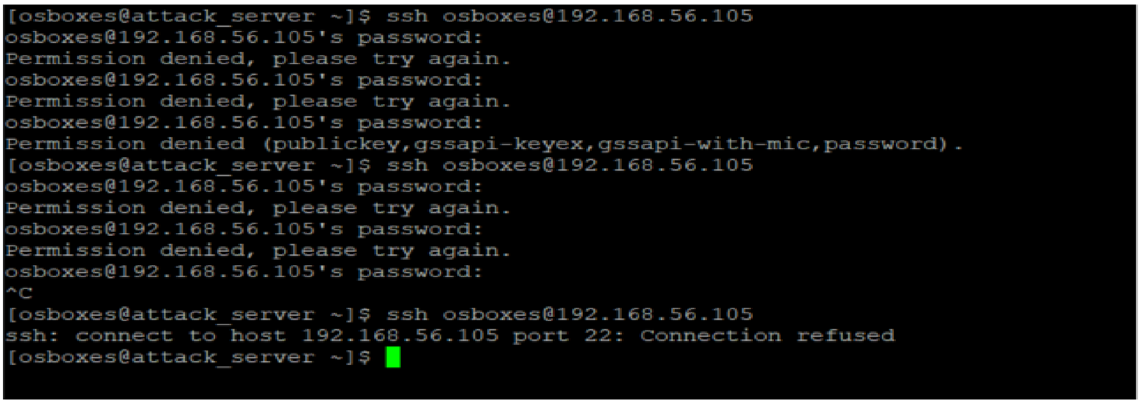
```
[root@test_server jail.d]# cat sshd.local
[sshd]
enabled = true
port = ssh
action = iptables-multiport
logpath = /var/log/secure
maxretry = 5
bantime = 300
findtime = 300
[root@test_server jail.d]# 
```

Figure 12. Fail2ban Configuration for SSH.

In this sshd.local configuration file (Figure 12):

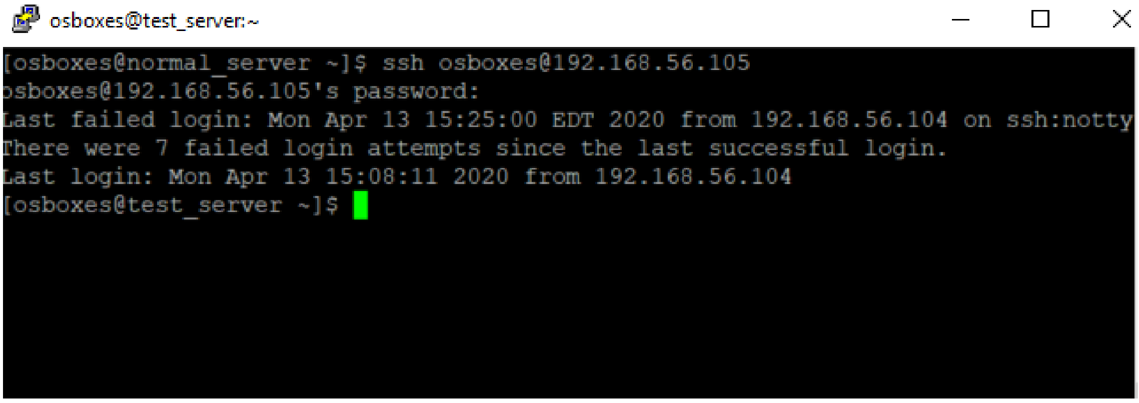
- ”enabled = true” means that the SSH protection is on
- ”port = ssh” means the port that using ssh access (ssh option is the port 22 by default)
- ”action = iptables-multiport” describes that the software will ban a matching IP address (this is the ”default” ban action)
- ”maxretry” parameter means the number of attempts can be made to access the server from a single IP before a ban (the value configured is 5)
- ”bantime” parameter means the time (in seconds) that the host will be banned after reaching ”maxretry” in the amount of ”findtime” (the value configured is 300s)
- ”findtime” parameter describes the length of time (in seconds) between login attempts before a ban is set

At first sight, the SSH connection was good as in Figure 10 and Figure 11. The rules from “Fail2ban” will be triggered by attempting to connect to the ”test_server” by ”attack_server” 5 times with wrong passwords.



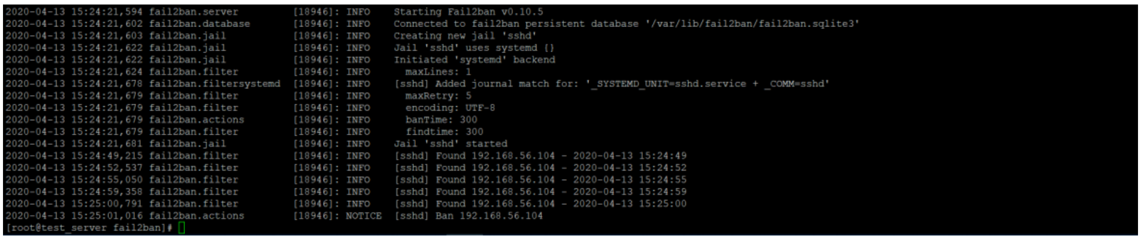
```
[osboxes@attack_server ~]$ ssh osboxes@192.168.56.105
osboxes@192.168.56.105's password:
Permission denied, please try again.
osboxes@192.168.56.105's password:
Permission denied, please try again.
osboxes@192.168.56.105's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[osboxes@attack_server ~]$ ssh osboxes@192.168.56.105
osboxes@192.168.56.105's password:
Permission denied, please try again.
osboxes@192.168.56.105's password:
Permission denied, please try again.
osboxes@192.168.56.105's password:
^C
[osboxes@attack_server ~]$ ssh osboxes@192.168.56.105
ssh: connect to host 192.168.56.105 port 22: Connection refused
[osboxes@attack_server ~]$
```

Figure 13. ”Connection refused” after 5 wrong password attempts.



```
[osboxes@normal_server ~]$ ssh osboxes@192.168.56.105
osboxes@192.168.56.105's password:
Last failed login: Mon Apr 13 15:25:00 EDT 2020 from 192.168.56.104 on ssh:notty
There were 7 failed login attempts since the last successful login.
Last login: Mon Apr 13 15:08:11 2020 from 192.168.56.104
[osboxes@test_server ~]$
```

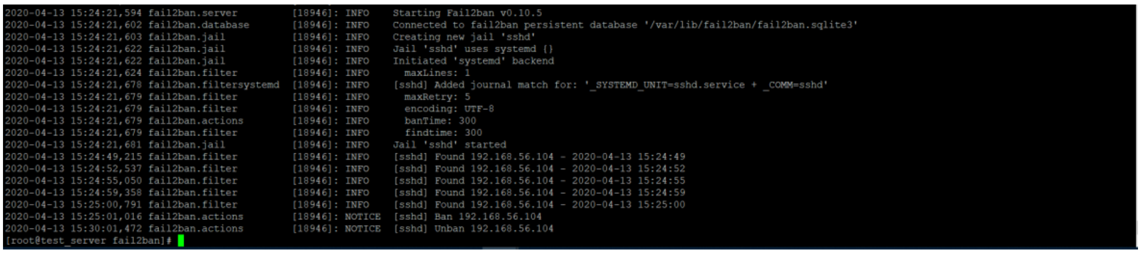
Figure 14. The connection from ”normal_server” to ”test_server”.



```
2020-04-13 15:24:21,594 fail2ban.server         [18946]: INFO    Starting Fail2ban v0.10.5
2020-04-13 15:24:21,602 fail2ban.database       [18946]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2020-04-13 15:24:21,603 fail2ban.jail           [18946]: INFO    Creating new jail 'sshd'
2020-04-13 15:24:21,622 fail2ban.jail           [18946]: INFO    Jail 'sshd' uses systemd {}
2020-04-13 15:24:21,622 fail2ban.jail           [18946]: INFO    Initiated 'systemd' backend
2020-04-13 15:24:21,624 fail2ban.filter         [18946]: INFO      maxLines: 1
2020-04-13 15:24:21,678 fail2ban.filtersystemd  [18946]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      maxRetry: 5
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      encoding: UTF-8
2020-04-13 15:24:21,679 fail2ban.actions        [18946]: INFO      banTime: 300
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      findtime: 300
2020-04-13 15:24:21,681 fail2ban.jail           [18946]: INFO    Jail 'sshd' started
2020-04-13 15:24:49,215 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:49
2020-04-13 15:24:52,537 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:52
2020-04-13 15:24:55,050 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:55
2020-04-13 15:24:59,358 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:59
2020-04-13 15:25:00,791 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:25:00
2020-04-13 15:25:01,016 fail2ban.actions        [18946]: NOTICE  [sshd] Ban 192.168.56.104
[root@test_server fail2ban]#
```

Figure 15. The IP of ”attack_server” had been banned.

Then for the 6th time, SSH port was tried to connect again but at this time, it refused the connection (Figure 13). However, the connection from ”normal_server” to ”test_server” was still good (Figure 14) since the fail2ban just block the IP of ”attack_server” (not log the user) which can be checked from /var/log/fail2ban file (Figure 15).



```
2020-04-13 15:24:21,594 fail2ban.server         [18946]: INFO    Starting Fail2ban v0.10.5
2020-04-13 15:24:21,602 fail2ban.database       [18946]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2020-04-13 15:24:21,603 fail2ban.jail           [18946]: INFO    Creating new jail 'sshd'
2020-04-13 15:24:21,622 fail2ban.jail           [18946]: INFO    Jail 'sshd' uses systemd {}
2020-04-13 15:24:21,622 fail2ban.jail           [18946]: INFO    Initiated 'systemd' backend
2020-04-13 15:24:21,624 fail2ban.filter         [18946]: INFO      maxLines: 1
2020-04-13 15:24:21,678 fail2ban.filtersystemd  [18946]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      maxRetry: 5
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      encoding: UTF-8
2020-04-13 15:24:21,679 fail2ban.actions        [18946]: INFO      banTime: 300
2020-04-13 15:24:21,679 fail2ban.filter         [18946]: INFO      findtime: 300
2020-04-13 15:24:21,681 fail2ban.jail           [18946]: INFO    Jail 'sshd' started
2020-04-13 15:24:49,215 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:49
2020-04-13 15:24:52,537 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:52
2020-04-13 15:24:55,050 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:55
2020-04-13 15:24:59,358 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:24:59
2020-04-13 15:25:00,791 fail2ban.filter         [18946]: INFO    [sshd] Found 192.168.56.104 - 2020-04-13 15:25:00
2020-04-13 15:25:01,016 fail2ban.actions        [18946]: NOTICE  [sshd] Ban 192.168.56.104
2020-04-13 15:30:01,472 fail2ban.actions        [18946]: NOTICE  [sshd] Unban 192.168.56.104
[root@test_server fail2ban]# 
```

Figure 16. The notice of ”Unban” IP of ”attack_server”.

After 5 minutes (300 seconds) the IP was unbanned and the ”attack_server” can have access to the ”test_server” which means the test was successfully deployed (Figure 16).

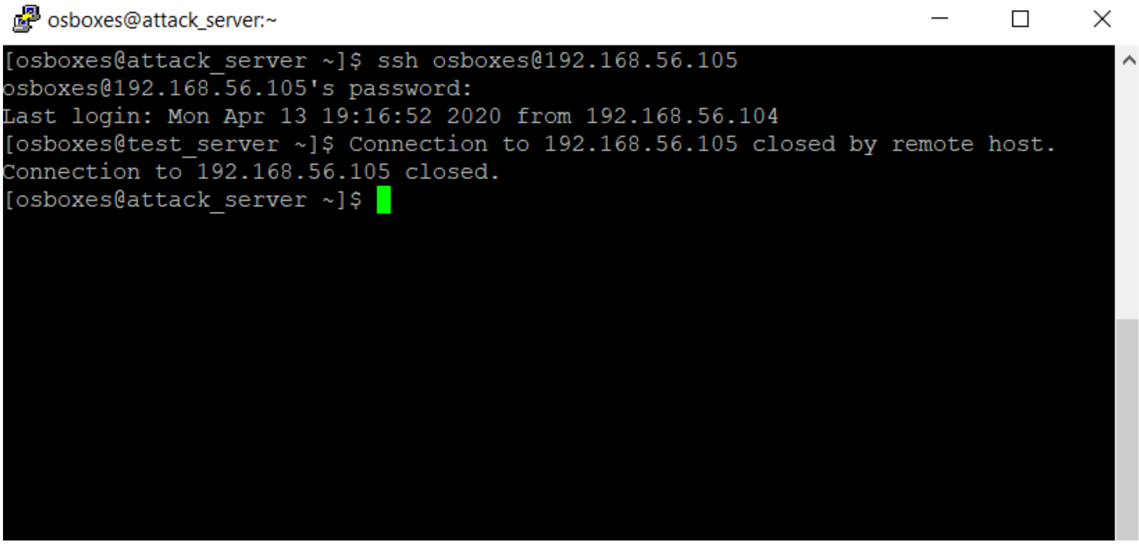
6.3 Force user to lock out of Session after defined inactive amount of time in SSH

In the Access Control Family from NIST800-53, there is a control ”Session Lock” which will prevent further access to the system by locking session client after inactivity amount of time. This control can prevent the physical attacks when the employees forget to lockout before they move away from the server which can give a high risk that someone unauthorized can access the system. In the case of X.805 security Recommendation, this can be referred to as securer the Access Control, Data Confidentiality and Privacy dimensions from the Application Security Layers in the Management Security Plane.

The configuration for SSH access can be done by putting these 2 lines inside the /etc/ssh/sshd_config:

- ClientAliveInterval 100
- ClientAliveCountMax 1

After the configuration, we need to restart SSH service to apply these changes into the active state by executing the command: systemctl restart sshd.service



```
[osboxes@attack_server ~]$ ssh osboxes@192.168.56.105
osboxes@192.168.56.105's password:
Last login: Mon Apr 13 19:16:52 2020 from 192.168.56.104
[osboxes@test_server ~]$ Connection to 192.168.56.105 closed by remote host.
Connection to 192.168.56.105 closed.
[osboxes@attack_server ~]$
```

Figure 17. Session closed after the time reached.

The ”ClientAliveInterval” defines the amount of time (in seconds) that the server will wait before sending a ”null packet” to the client to keep the connection alive while the ”ClientAliveCountMax” parameter defines the number of times that the server will wait if there is no response from Client for ”null packet”. With the configuration above, the client will lose the connection to the server after 100*1 = 100 (seconds). The result of the SSH closed session can be found in Figure 17.

7 CONCLUSION

Being under pressure from the technology developing requirements and the risks from the cybercriminal, every network component would be perceptive to hackers if the security is not configured properly. Therefore, the habit of applying the security rules to strengthen the server's security is encouraged to reduce the possibilities of threats. The updates in hardware and software somewhat enhance the system security but do not completely and are cost-effective. Implementing security standards is currently a trend over the world with a variety trustworthy third-parties such as National Institute of Standards and Technology (NIST), International Telecommunication Union (ITU), International Organization for Standardization (ISO) supporting the security in a way that software and hardware cannot produce. Based on different systems, the need of applying security methods will be considered differently, however, the more effort is put in investigating the security, the more security applications can be applied.

In the Evolved Packet Core network, MME is the most sensitive node, which has been the ideal target for hackers to attack in the Telecommunication Network. Providing well-designed protection on this node would prevent most of the critical threats that appear inside EPC, minimizing the loss of operators' money as well as the privacy and the sensitive data of customers. In order to implement these security Standards appropriately into the node's configuration, the security and the existed threats of the node must be analyzed. Therefore, three research questions regarding the MME's necessity and security as well as choosing the proper Standards to pursue were established.

Regarding the first question: ”Why do we need to secure Mobility Management Entity?”, the research showed the importance of Mobility Management Entity not only in the Evolved Packet Core but also in the whole Telecommunication Network. The node with the main function is the mobility management which is working as the controller of the 4G/LTE network, managing traffic inside the Evolved Packet System and also supporting the system to roam with other wireless technologies. Moreover, this is the bridge between eNodeB and the network database (HSS), providing authentication and applying appropriate subscribers' profiles to initiate users into the network. Despite its importance, the security of the node has not been protecting it properly, resulting in a gigantic number of threats existing and exploited.

The purpose of the second research question was to investigate the ITU-T X.805 and NIST800-53 Security Recommendations which have been developed by well-known security Unions. The ITU-T X.805 gives the overview of security separated by dimensions, layers and planes which can be applied to secure any end-to-end systems. On the other hand, the NIST800-53 provides the Control families, including the details of Security Controls and their effects that are recommended to comply with based on the node’s requirement.

The last objective of the thesis was to convert the lessons learnt into the practical configuration into the node. Thanks to the baseline security requirement of the MME and the security infrastructure of these defined Standards, the author was able to represent some sets of security Controls to secure the virtualized server. However, due to the complexity of the security in the real environments and the huge amount of controls defined in these Standards, the requirement for further studies as well as a much larger and well-organized group to deploy is necessary to maximize the security levels of MME.

REFERENCES

Chinavasion, 2008. 1G, 2G, 3G, 4G - The Evolution of Wireless Generations. [Online]

Available at: https://support.chinavasion.com/index.php?/Knowledgebase/Article/View/284/42/1g-2g-3g-4g---the-evolution-of-wireless-generations [Accessed 16 Mar 2020]

Ericsson, 2009. World's first 4G/LTE network goes live today in Stockholm. [Online]

Available at: https://www.ericsson.com/en/press-releases/2009/12/worlds-first-4glte-network-goes-live-today-in-stockholm [Accessed 22 Mar 2020]

Europol. Telecommunication Fraud. [Online]

Available at: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/telecommunications-fraud [Accessed 12 Apr 2020]

Firmin, F.. The Evolved Packet Core. [Online]

Available at: https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core [Accessed 28 Mar 2020]

GSMA Intelligence, 2017. Number of Mobile Subscribers Worldwide Hits 5 Billion. [Online]

Available at: https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/ [Accessed 17 Mar 2020]

IEEE, 2011. Codebook Based Interference Mitigation with Base Station Cooperation in Multi-Cell Cellular Network. [image]

Available at: https://www.semanticscholar.org/paper/Codebook-Based-Interference-Mitigation-with-Base-in-Charoen-Ohtsuki/63cb9a0ac9b238837b8df683ee43fd8276ce025c [Accessed 15 Mar 2020]

ITU-T, 2003. Series X: Data Networks and open system communications: Security architecture for systems providing end-to-end communications. [document]

Available at: https://www.itu.int/rec/T-REC-X.805-200310-I/en

Kakadia, D., Yang, J. & Gilgur, A., 2007. Network Performance and Fault Analytics for LTE Wireless Service Providers. s.l.: Springer Pvt. Ltd..

Lucian, C., 2016. Hackers can abuse LTE protocols to knock phones off networks. [Online]

Available at: https://www.computerworld.com/article/3139329/hackers-can-abuse-lte-protocols-to-knock-phones-off-networks.html [Accessed 11 Apr 2020]

Mahjabeen, D., Sayem, A., Ahmed, A., Rafique, S., 2010. Interoperability of Wireless Networks with 4G Based on Layer Modification. Int. J. Communications, Network and System Sciences, 2010, 3, 472-476. Available at: https://www.researchgate.net/publication/220099160_Interoperability_of_Wireless_Networks_with_4G_Based_on_Layer_Modification [Accessed 18 Mar 2020]

Merej, M., Kumar, S., 2015. Evolution of Mobile Wireless Technology from 0G to 5G. International Journal of Computer Science and Information Technologies, Vol. 6(3), 2015, 2545-2551

Mishra, A., 2007. Advanced Cellular Network Planning and Optimisation. s.l.: John Wiley & Sons, Ltd..

Nate Lord, 2018. What is NIST SP 800-53? Defination and Tips for NIST SP 800-53 Compliance. [Online]

Available at: https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance [Access 12 Apr 2020]

NIST, 2020. CVE-2019-16026 Detail. [Online]

Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-16026 [Accessed 11 Apr 2020]

NIST. National Vulnerability Database. [Online]

Available at: https://nvd.nist.gov/800-53/Rev4 [Accessed 02 Apr 2020]

O'Hanlon, P.. ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications. [image]

Available at: https://www.researchgate.net/figure/ITU-T-X805-Security-Architecture-for-Systems-Providing-End-to-End-Communications_fig15_317036464 [Access 01 Apr 2020]

Obaidat, M., Nicopolitidis, P. & Zarai, F., 2015. Modeling and Simulation of Computer Networks and Systems. s.l.: Elsevier Inc..

OCCRP, 2019. Report: US$32.7 Billion Lost in Telecom Fraud Annually. [Online]

Available at: https://www.occrp.org/en/daily/9436-report-us-32-7-billion-lost-in-telecom-fraud-annually [Access 10 Apr 2020]

OECD, 2004. Development of Third-Generation Mobile Services in the OECD. OECD Digital Economy Papers, No. 85, OECD Publishing, Paris. [Online] Available at: https://www.oecd-ilibrary.org/docserver/232562017400.pdf?expires=1587151652&id=id&accname=guest&checksum=C8B204AF743A47A8009E2FBFFCFE1442 [Accessed 16 Mar 2020]

Olsson, M., Sultana, S., Rommer, S., Frid, L., Mulligan, C., 2009. SAE and the Evolved Packet Core - Driving The Mobile Broadband Revolution. First Edition. s.l.: Elsevier Ltd..

Positive Technologies. 2017. Next-Generation networks, next-level Cybersecurity Problems. [Online]

Available at: https://www.gsma.com/membership/wp-content/uploads/2017/08/Diameter-Research.pdf [Accessed 04 Apr 2020]

Positive Technologies.2018.SS7 Vulnerabilities and attack exposure report. [Online] Available at:https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf [Accessed 02 Apr 2020]

RCRWireless, 2014. LTE MMEA Core Connector for LTE. [Online]

Available at: https://www.rcrwireless.com/20140509/diameter-signaling-controller-dsc/lte-mme-epc [Accessed 8 Apr 2020]

Sheridan, K., 2016. 4G Cellular Networks At Risks of DoS attacks. [Online]

Available at: https://www.darkreading.com/mobile/4g-cellular-networks-at-risk-of-dos-attacks/d/d-id/1327422 [Accessed 07 Apr 2020]

Statista, 2020. Number of LTE subscriptions worldwide from 2018 to 2023 (in billions). [Online] Available at: https://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-lte-subscriptions-up-to-2014/ [Accessed 25 Mar 2020]

Techopedia, Cellular Network. [Online]

Available at https://www.techopedia.com/definition/24962/cellular-network [Accessed 15 Mar 2020]

Wikipedia. NIST Special Publication 800-53. [Online]

Available at: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53 [Accessed 11 Apr 2020]

Wikipedia. Signalling System No. 7. [Online]

Available at: https://en.wikipedia.org/wiki/Signalling_System_No._7 [accessed 10 Apr 2020]

Wikipedia. System Architecture Evolution. [Online]

Available at: https://en.wikipedia.org/wiki/System_Architecture_Evolution [Accessed 28 Mar 2020]

Zhong, S., Zhong, H., Huang, X., Yang, P., Shi, J., Xie, L., Wang, K., 2019. Security and Privacy for Next-Generation Wireless Networks. [ebook]

Available at: https://books.google.fi/books?id=R4F7DwAAQBAJ&pg=PA17&lpg=PA17&dq=mme+security&source=bl&ots=uSw1s-k8ux&sig=ACfU3U2Bf74QPUHPcSmoNppszKG-yPajSw&hl=en&sa=X&ved=2ahUKEwijkpfpjOHoAhUOwcQBHXurDVw4ChDoATABegQICRAv#v=onepage&q&f=false [Accessed 11 Apr 2020]