Signaling Security in LTE Roaming

Isha Singh

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo Sunday 7th April, 2019

Supervisor

Prof. Raimo Kantola

Advisor

Dr. Silke Holtmanns

Aalto University
School of Electrical
Engineering

Aalto University
School of Electrical
Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author Isha Singh

Title Signaling Security in LTE Roaming

Degree programme Computer, Communication and Information Science

Major Communications Engineering **Code of major** ELEC3029

Supervisor Prof. Raimo Kantola

Advisor Dr. Silke Holtmanns

Date Sunday 7th April, 2019 **Number of pages** 67+3 **Language** English

Abstract

LTE (Long Term Evolution) also known as 4G, is highly in demand for its incomparable levels of experience like high data rates, low latency, good Quality of Services (QoS) and roaming features. LTE uses Diameter protocol, which makes LTE an all IP network, connecting multiple network providers, providing flexibility in adding nodes and flexible mobility management while roaming. Which in turn makes LTE network more vulnerable to malicious actors. Diameter protocol architecture includes many nodes and the communication between the nodes is done through request and answer messages. Diameter manages the control session. Control session includes the signaling traffic which consists of messages to manage the user session. Roaming signaling traffic arises due to subscribers movement out of the geographical range of their home network to any other network. This signaling traffic moves over the roaming interconnection called S9 roaming interface.

This thesis project aims to interfere and manipulate traffic from both user-to-network and network-to-network interfaces in order to identify possible security vulnerabilities in LTE roaming. A fake base-station is installed to establish a connection to a subscriber through the air interface. The IMSI (International Mobile Subscription Identity) is captured using this fake station. To explore the network-to-network communication an emulator based LTE testbed is used. The author has investigated how Diameter messages can be manipulated over the S9 interface to perform a fraud or DoS attack using the IMSI number. The consequences of such attacks are discussed and the countermeasures that can be considered by the MNOs (Mobile Network Operators) and Standardization Committees.

Keywords LTE, Diameter, EPC, Diameter Roaming, PCC, IPX, S9, RAR, RAA

Preface

I express my sincere gratitude to everyone whose contribution brought me to the position and ability to write this thesis.

This Masters Thesis is a research for Aalto University, Department of Communications and Networking, undertaken, funded and completed at Nokia Bell Labs. I thankfully acknowledge **Aalto University** and **all my faculty members** for the knowledge I gained as the masters student.

I sincerely thank to **Nokia Bell Labs**, Security Team members **Gabriel Waller, Leo Hippelainen, Ian Oliver, Silke Holtmanns, Yoan Miche, Aapo Kalliola** for providing me the opportunity to work, learn and grow throughout this research. Their consistent support, understanding and patience motivated me throughout the research period.

I am grateful and deeply thankful to my supervisor, **Prof. Raimo Kantola, Aalto University** and my instructor, **Dr. Silke Holtmanns, Nokia Bell Labs**. Their consistent guidance and help at every stage of the research has driven me to its successful completion. It is my greatest honor and fortune to work with them.

Friends can never be forgotten and my friendly gratitude goes to all my friends around the world. I'm grateful to have **Asta Kumar, Erja Tuunanen, Mayank Khandelwal, Bhavya Omkarappa, Kiran Vangapattu, Juha-Matti Tilli** in my life, for they are always there for me. My special gratitude to **Gabriela Limonta** and **Borger Vigmostad** for helping and guiding me at various stages of the project.

The endless love and patience of my family, especially my loving children **Adwitiya and Aarna**, support of my in-laws **Bhagirath Mal Verma** and **Shakuntala Verma**, motivation of my parents **Dr. I. P. S. Punia** and **Sushma Punia**, and love of my spouse **Vikas Singh** has helped me in becoming what I am today. Their belief and support cannot be expressed merely by words.

Above all I thank to **The Universe** for blessing me with all my accomplishments, family and friends.

Otaniemi, Sunday 7th April, 2019

Isha Singh

Contents

List of Figures

List of Tables

Symbols and Abbreviations

Abbreviations

(1-5)G	(First-Fifth) Generation of Mobile Systems
3GPP	Third Generation Partnership Project
5G PPP	The 5G Public Private Partnership
AF	Application Function
AMPS	Advanced Mobile Phone System
AN-Gateway	Access Network Gateway
API	Application Programming Interface
APN	Access Point Name
ARIB	Association of Radio Industry and Businesses
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute-Value Pair
BBERF	Bearer Binding and Event Reporting Function
BTS	Base Transceiver Station
CCA	Credit Control Answer
CCR	Credit Control Request
CCSA	China Communications Standards Association
CN	Core Network
CDR	Charging Data Record
CVOPS	C based Virtual Operating System
DEA	Diameter Edge Agent
DNS	Domain Name Server
DoS	Denial-of-Service
DPA	Disconnection-Peer-Answer
DPR	Disconnection-Peer-Request
DRA	Diameter Routing Agent
DTLS	Datagram Transport Layer Security
DWA	Device-Watchdog-Answer
DWR	Device-Watchdog-Request
EDGE	Enhanced Data rate for GSM Evolution
EIR	Equipment Identity Register
eNB	evolved Node Base-station

EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
ETSI	European Standards Institute
FBC	Flow Based Charging
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GRX	GPRS roaming exchange service
GSM	Global System for Mobile Communications
GSMA	GSM Association
H-AF	Home AF
HLR	Home Location Register
H-PCRF	Home PCRF
HPLMN	Home PLMN
HR	Home-Routed
HSS	Home Subscriber Server
ICCID	Integrated Circuit Card Identifier
IDA	Inter Subscribers Data Answer
IDR	Inter Subscribers Data Request
IETF	Internet Engineering Task Force
IoT	Internet of Things
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPI	IP Interconnecting
IPSec	Internet Protocol Security
IPX	IP Packet Exchange
ISP	Internet Service Provider
ITU	International Telecommunications Union
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Message Authentication Code
MAP	Mobile Application Part

MitM	Man-in-the-Middle
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSC	Mobile Switching Center
NAI	Network Access Identifier
NAS	Network Access Server
NRTRDE	Near Real Time Roaming Data Exchange
OAI	Open Air Interface
OCS	On-line Charging System
OFCS	Off-line Charging system
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rule Function
PDN	Packet Data Network
PGW	PDN Gateway
PLMN	Public Land Mobile Network
PPID	Payload Protocol Identifier
QoE	Quality of Experience
QoS	Quality of Service
RAA	Re- Authentication Answer
RADIUS	Remote Authentication Dial In User Service
R&D	Research and Development
RAR	Re-Authentication Request
SAE	System Architecture Evolution
SBLP	Service Based Local Policy
SCTP	Stream Control Transmission Protocol
SDF	Service Data Flow
SDN	Software Defined Network
SDR	Software Defined Radio
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscriber Location Function

SMQ	SIP Message Queue
SON	Self Organizing Network
SS7	Signaling System No.7
STP	Signaling Transfer Point
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSDSI	Telecommunications Standards Development Society
TSG	Technical Specification Groups
TTA	Telecommunication Technology Association
TTC	Telecommunication Technology Committee
UE	User Equipment
UDP	User Data Protocol
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USRP	Universal Software Radio Peripheral
VLR	Visitor Location Register
V-AF	Visited AF
VoIP	Voice over Internet Protocol
V-PCRF	Visited PCRF
VPLMN	Visited PLMN

1 Introduction

Figure 1 shows the statistics by International Telecommunication Union's (ITU - T)[1] standardization sector, estimating the number of mobile subscribers, which has grown to more than the number of people on the planet [60]. It is debatable if all subscribers consider how they are able to make calls or use data at any point of time and at any location on the globe. When a subscriber moves out of the coverage area of its subscribed network and enters to other network its state is called roaming state. The User Equipment (UE) stays connected to a network available at any point of time without the subscriber having any awareness of background processing. The visited network knows the subscriber as a visitor and communicates with the network where subscriber is subscribed. The subscribed network is called the home network and all other networks are the visited networks. The visited network communicates with the home network either directly or with the help of a private network called IPX[2] (IP Packet eXchange). All the network operators around the world exchange roaming traffic with each other through the IPX network [43] to provide its subscribers uninterrupted, secure and high quality of services (QoS) anywhere around the globe.

Long Term Evolution (LTE), is designed as per the 3GPP[3] specification for cellular

[1] www.itu.int
[2] http://www.whatisipx.com/
[3] www.3gpp.org

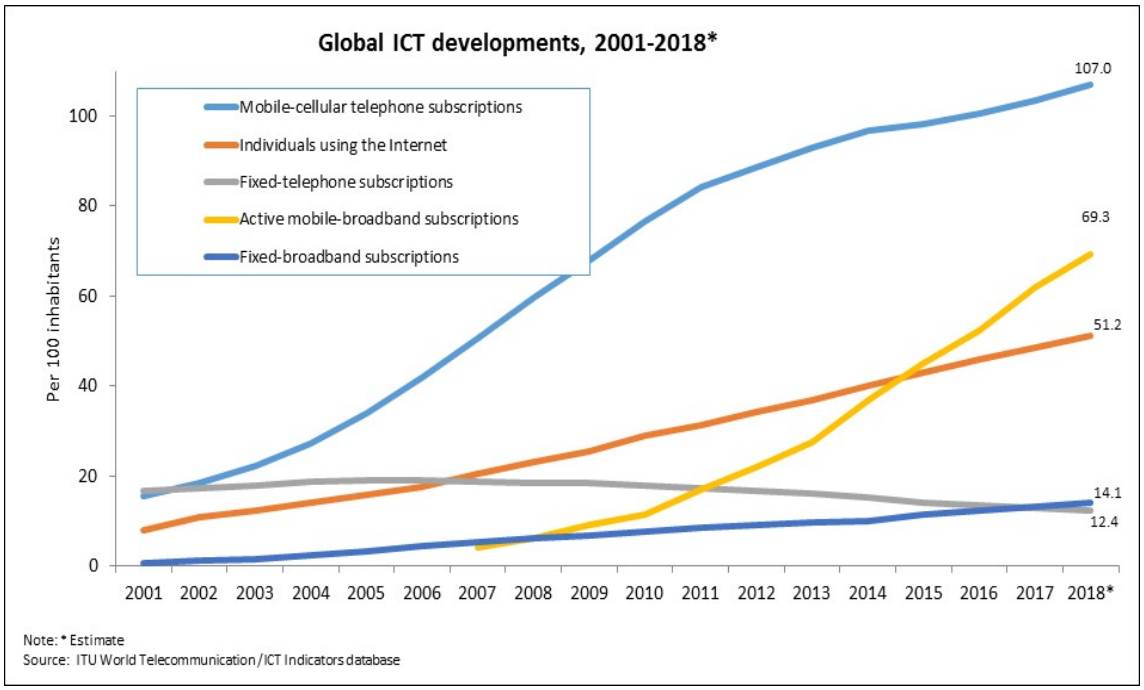

Figure 1: ICT Statistics on Global Information and Communication Technologies Development (Adapted from [60])

network, which uses the Diameter Protocol for signaling and charging control. Before Diameter, SS7, its IP version, SIGTRAN and RADIUS were used. SS7 was used for user voice and data session and online charging was done with the support of another protocol and Radius was used for authorization and authentication. The number of protocols used tells us that the telecommunication infrastructure is very complex and difficult to manage. The researchers in [7, 19, 20, 38, 50], have figured out many flaws in the legacy telecommunication infrastructure including eavesdropping, fraud attacks on billing, subscriber privacy, location tracking and DoS attacks. Therefore the telecom networks migrated to the Diameter protocol, which is a single substitute to several legacy protocols.

In this thesis, we demonstrate a roaming vulnerability in the LTE networks for a specific network configuration. In this chapter we introduce the research and motivation to choose and work on the topic. Then, we document the goals and question of this research. The procedure to obtain the results is covered under the methodology, and, finally the structure of the thesis is introduced.

1.1 Motivation

The rate of increase in global subscribers of LTE in comparison to other technologies is exponential and the growth is expected to carry on in the coming years. The OVUM [4] analytically compared different mobile network technologies and the increase in subscribers around the world yearly, as shown in Figure 2. From the Figure 2 it is clear that LTE has the maximum number of subscribers compared to the 2G and 3G network [40]. This exponential growth of subscriber traffic has made LTE network management and protection challenging for the operators [13].

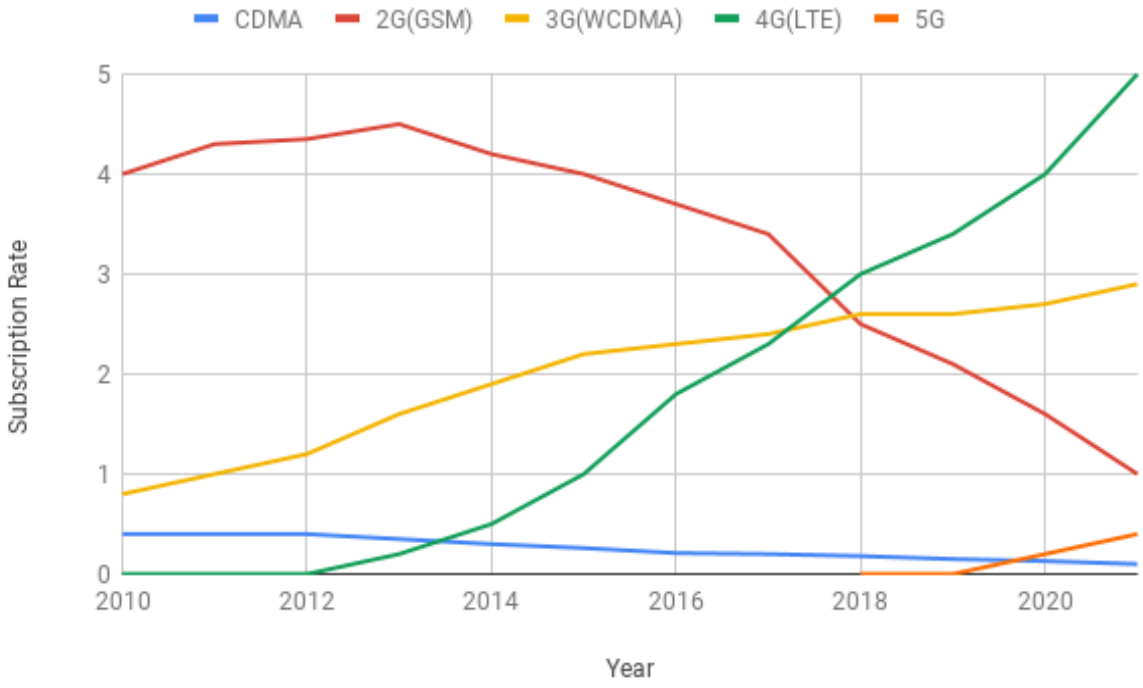

Figure 2: Global subscription evolution for different Cellular Technologies (Adapted from[40])

Due to the high growth rate of LTE subscribers worldwide, mobile network service providers aim to provide high data rate and best QoS to mobile consumers. The users expect to experience the high quality data, voice and multimedia services not only in their home mobile network, but also while roaming into the network of a different operator. For this reason, operators need to implement international

[4] ovum.informa.com

roaming services. To provide best services Diameter is a suitable choice [21]. It provides flexibility in addition of applications over the Diameter Base Protocol. It is interoperable with the legacy protocol RADIUS [37].

Industrial professionals and researchers reveal that the Diameter roaming traffic and the amount of LTE subscribers will continue to increase [41], along with new Internet of Things (IoT) subscribers, therefore better services and high security is in demand. This growth is equally visible in the roaming signaling traffic.

To manage roaming traffic and services a third party interconnection network IPX is involved to connect all the continents introduction the new roaming interface "S9" which communicates the policy and charging related signaling traffic over the IPX network. It is important to study how the signalling traffic between two operators across different continents is communicated over Diameter protocol through third party networks.

The possibilities can be seen in making a Man-in-the-Middle (MitM) intrusion scenario by creating a fake Diameter node in the IPX network or in the core network. Vulnerability tests for Diameter roaming interface S6a and S6d are done in master thesis research [36]. In this master thesis the researcher has demonstrated the attack on the S6a interface by pretending itself as a partner node and exchanging messages with the home MNO. This research further explains the possibilities to access the interconnection network.

Similar to S6a and S6d interfaces S9 interface also passes through interconnection network. Subscription and billing related messages are communicated over the S9 interface. If an attacker manages to get access to these messages it is possible to make fraud or DoS attacks.
Weather the roaming subscribers are paying for what they are subscribed for, makes Diameter S9 interface and LTE roaming an attractive point of research.

1.2 Goals and Research question

This research aims to study the 3GPP specifications for LTE network design and discover the real time implementation vulnerabilities in LTE roaming. The work includes the analysis of recently discovered vulnerabilities and attacks made on LTE network interfaces and the methodology used. The background literature reviews the LTE design, Diameter message details and roaming architecture of LTE.

Therefore, the primary goal of the thesis is to understand LTE, Diameter, IPX and Policy and Charging Control (PCC) rules as per 3GPP specifications. Understanding the types of attacks on different LTE interfaces based on Diameter protocol gives us an idea to discover new attacks.

The LTE roaming interface "S9" is the target interface of this research. The PCC (Policy Control and Charging) rules are communicated during roaming over S9 interface between Home-PCRF (Policy and Charging Rule Function) and Visited-PCRF. Similarly the Gx interface is used to communicate PCC rules between PCRF and PCEF (Policy and Charging Enforcement Function) within the home network. Figure 3 highlights the S9 interface between the home and visited PLMNs(Public Land Mobile Networks), while the Gx interface is within the home PLMN in the LTE architecture. HPCRF and VPCRF communicate signaling messages through S9 roaming interface with the help of IPX network.

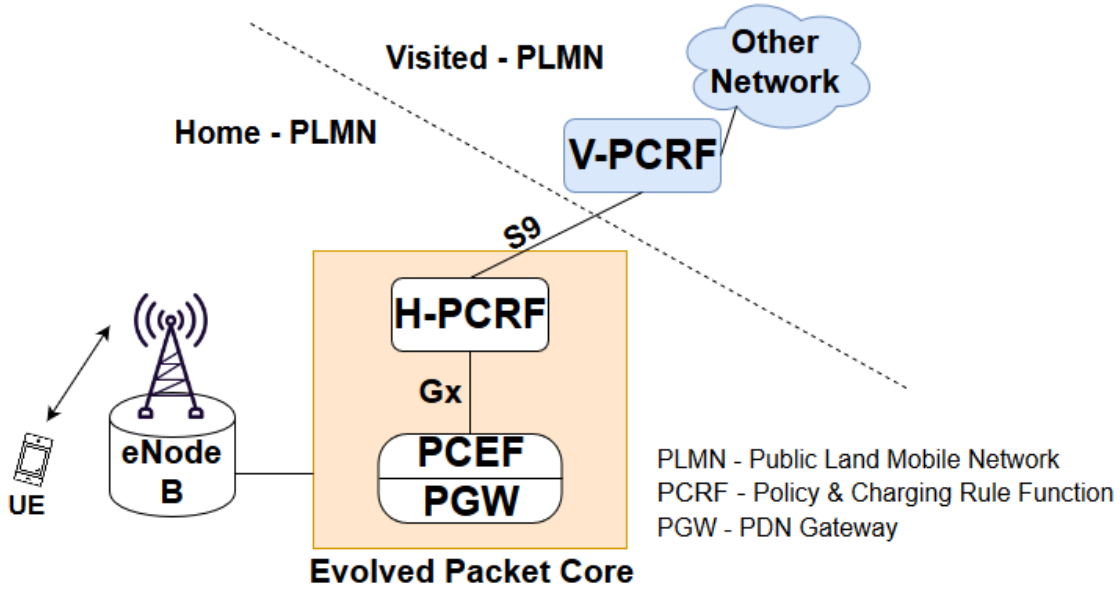

Figure 3: Gx and S9 interfaces in LTE architecture

In brief IPX is necessary tool to exchange LTE, IP based traffic and other services including, ISP via IP based network-to-network interface. To maintain the same quality of service around the world the IPX network provides communication between the two MNO's. It also solves the problem of interoperability.

The research question is pointed out here as "**How secure is the LTE roaming and how a fraudulent attempt can be made to manipulate Diameter messages over S9 interface?**". The fraud attempt is made by collecting the International Mobile Subscriber Identity (IMSI) over user-to-network interface and manipulating the PCC rules carried in Diameter message AVP's. A test bench is set up for (IMSI) catcher and to manipulate Diameter messages first the S9 and Gx interface messages are compared and which are almost same and then with the help of the LTE emulator the message manipulation task is accomplished. The manipulated messages can be seen through the Wireshark captured Diameter packets. This test gives an insight to frame a real time scenario for a MitM attack attempting fraud and DoS (Denial of Services).

1.3 Related work

In the evolution of LTE and the signaling protocol advancement from SS7 to Diameter, the challenges are consistently faced by the users, operators or service providers. A survey on security of LTE networks [47] shows a number of threats that may cause unexpected service and information intrusions. Diameter protocol and LTE networks security are highlighted here in context of different researches.

Diameter poor configurations spotted inside LTE networks are mentioned to be unique for each network [64] and are broadly classified in five kinds of attacks: User data leaking (identity theft), Network traffic interference and manipulation, User traffic interception, Fraud attempts, DoS.

To target a subscriber, we need to access the radio interface and collect the information using radio sniffing devices. This is similar to the research [55] which demonstrates three different attacks on the LTE network, two of which are passive, subscriber information and traffic interception. The third attack, however, is active, which aims to mislead the subscriber by performing a website fingerprinting attack. The passive attacks in [55] are carried out using a device called "IMSI Catcher" or "Stingray". Similarly we have also built an IMSI catcher for subscriber

information retrieval.

According to the researcher, in [55] the active attack is Domain Name System (DNS) spoofing, and this attack is possible due to a data layer weakness. Despite being encrypted, the packets are not integrity protected.

Various kinds of attacks have been made through different interfaces of LTE networks and Diameter protocol. Table 1 represents the LTE interfaces and the possible attacks made through these interfaces.

Interface	Objective	Attack name
Sh	Capturing IMSI by making user data retrieve	Man-in-the-Middle[13, 31]
S6a	Authentication message manipulation	DoS [32]
S6a	Location tracking cancellation	DoS [33]
S6a	New location update	DoS [33, 62]
S6a	Delete subscriber data in repository	DoS[51]
S6a	Cancelling user request	DoS [33, 34]
Sh	Location tracking	Spoofing [13, 33, 52]

Table 1: Diameter interfaces and the known attacks

Current state of the research can be understood studying the newly published results on Diameter roaming interconnection vulnerabilities.

The research [30] explains which 4G network configurations can be attacked and by collecting subscribers information, how the access point configuration can be changed in different core network nodes. Exploiting this, the attacker can create a Man-in-the-Middle (MitM) attack on the data traffic of the subscriber.

The research [62] describes the DoS attack on DNS in the international roaming LTE network. The Open Air Interface (OAI) software is used to perform a DoS attack a on DNS server. Another research work on Self Organizing Network (SON) LTE [57] attempts a DoS attack on the end user, by implanting malicious information in the respective system. Paging the LTE messages of targeted subscriber is discussed in research [13]. It discusses identity theft and location tracking of an LTE subscriber using publicly available tools.

1.4 Methodology

To answer the research question a qualitative approach is used. A quantitative method was not chosen, mainly due to the fact that setting up an LTE roaming architecture model was not feasible.

All the essential background knowledge, LTE emulator testbed, is covered from Third Generation Partnership Project (3GPP) specifications [1] and GSMA[5] documentation. We use the analytical approach to analyze and evaluate existing research literature. Active attacks were made for IMSI collection making sure it did not interfere with the normal users.

LTE interface vulnerabilities have been passively tested on the LTE emulator for the proof of concept. Finally, the research concludes with the publication of results and further insights on the topic.

1.5 Structure of the Thesis

The thesis consists of six chapters and rest of it is structured as follows.

In Chapter 2, the background and theory of the concept useful for this research work is covered. The subsections of this chapter will highlight the 3GPP Specifications used in this research work, LTE Architecture, LTE Emulator design, Diameter Architecture and its interfaces, working of LTE Roaming, IPX Architecture and the PCC Architecture. It is worth understanding the basic architecture and working, in order to understand the attacks, which are made at the roaming interface.

Chapter 3 details about the possibilities of the attacks at the air interface and network to network interface. Here, we have defined methods to make successful attacks at these interfaces. This helps in knowing the available vulnerabilities and loop holes in the network.

Chapter 4 defines the steps we have adopted to make a fraud and DoS attack. It includes the air interface attack and roaming interface attack and how both of these lead to a successful fraud attack.

[5] www.gsma.com

Chapter 5 explains the man in the middle attack, with an example, explaining the attack scenario and its consequences.

This thesis is concluded with brief discussion on results and future work opportunities in Chapter 6.

Appendix A is the table mentioning all the nodes of the emulator used for LTE core network and their functioning.

2 Background

This chapter provides the basic technical background of the technologies and methodologies used in this project. The objective is to create a resource which is helpful to the readers to understand this research and take advantage of the thesis.

In the next section, we describe details about the 4G network architecture, also called Long Term Evolution (LTE) or Evolved Packet System (EPS). EPS is a combination of Evolved Packet Core and the LTE radio access network called E- UTRAN. In this thesis we will term it as LTE network. The LTE emulator used to prove the concept is explained in continuation, as its design is similar to the real LTE system. LTE uses the Diameter protocol, which is responsible for Authentication, Authorization and Accounting.

LTE roaming is discussed, which is useful to understand the working of mobile network, when the subscriber is in home network and when it is in the visited (roaming) network. IPX, which is the targeted part of the research and key role player in roaming scenarios is discusses next. The last section covers the Policy Control and Charging (PCC) rules architecture.

2.1 LTE architecture

The mobile network architecture, including all network elements, their interfaces and protocols used, are defined through standardization. The network used for

communications has also evolved far from circuit switched, to upcoming Software Defined Network (SDN). To come up to this definition, mobile communication technologies have undergone through a number of generation advancements.

In research [53] the author describes how wireless transmission has reached the all-IP based network communication.

The basic mobile communication architecture for LTE can be seen in Figure 4 which consists of four main blocks: User Equipment (UE) can be any electronic device capable of accessing the network. It includes, laptops, Mobile, tablets, IoT devices. Evolved Universal Mobile Telecommunication Systems(UMTS) Terrestrial Radio Access Network (E-UTRAN) is known as Access Network. Evolved Packet Core (EPC) is also referred as System Architecture Evolution (SAE) or core network. External Network includes IP Multimedia Subsystem (IMS)/PDN (Packet Data Network), the Internet.
These four blocks communicate with each other through specific interfaces, with unique names, as shown in Figure 4.

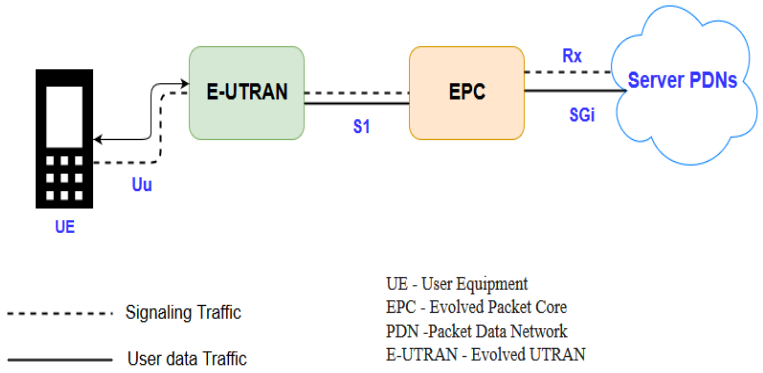

Figure 4: Basic EPS architecture with E-UTRAN access [Adapted from [45]]

Figure 4 also depicts the user and control plane communications between E-UTRAN and EPC. The dash line shows the control signals, while the solid line represents the user traffic. Therefore there are two planes in LTE architecture: Control Plane and User Plane.

EPC block shown in Figure 4 represents the core network of LTE. It consists of

multiple nodes, as shown in Figure 5. Figure 5 also shows the E-UTRAN and UE (User Equipment), which are connected by the air interface. Here we discuss each block in detail, also shown in Figure 5 which shows the E-UTRAN and EPC block of the LTE architecture.

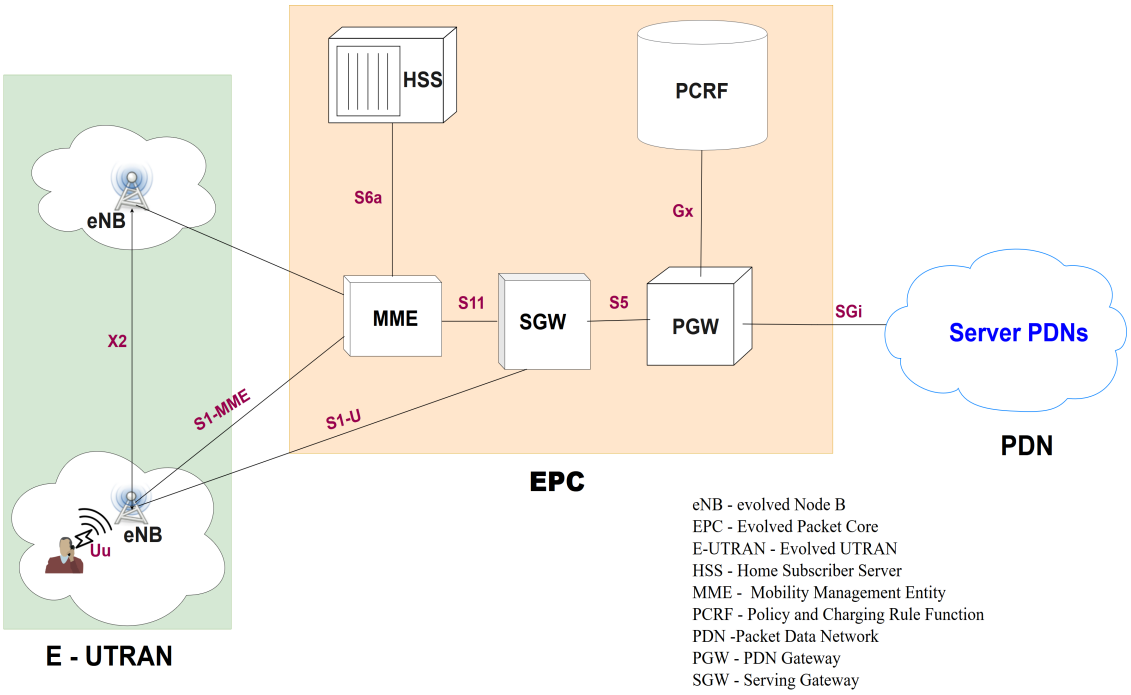

Figure 5: EPS architecture

User Equipment (UE)

Electronic devices which have the capability to connect to the LTE network, are termed as UE. It can be a mobile handset, laptop, tablet or any IoT device. The key component of an UE is a Universal Integrated Circuit Card (UICC). It is a microprocessor based smart card and an evolution to SIM (Subscriber Identification Module) card used in GSM networks [4]. The UICC holds the network specific information used to establish communication between the subscriber and the network. The main keys a SIM card stores, include ICCID (Integrated Circuit Card Identifier, a unique serial number), IMSI (International Mobile Subscription Identity) and the Authentication key.

E-UTRAN

Evolved Universal Terrestrial Radio Access Network (E-UTRAN), consists of evolved Node B (eNB), establishes the air interface with the UEs by mutual authentication.

UE communicates with just one base station (eNB) at a time. It controls up-link and down-link frequencies and multiplexing techniques. Key features of an eNB [2] are :
Establishing, maintaining and releasing the radio transmissions to all the UEs through the LTE air interface during the user session. Controlling and performing the handover procedures. Transferring the signaling messages to authenticate UEs and establishing the user session between a UE and EPC by supporting SCTP (Stream Control Transmission Protocol) [61].

Evolved Packet Core (EPC)

A simplified EPC architecture is illustrated in Figure 5. Its not practical to include all nodes of the complex EPC architecture. The main purpose is to understand the functioning of the nodes.

An EPC network is a packet switched all-IP network, where voice services are handled using IP Multimedia Subsystem (IMS) network [43].

The EPC architecture in Figure 5 includes the nodes that are the main focus of this research.

HSS (Home Subscriber Server): This is the main database of the EPC. It includes of HLR (Home Location Register) and AuC (Authentication Center). HLR is responsible for storing and updating subscriber location and subscription information. AuC is responsible for secure authentication key generation.

P-GW (Packet Data Network Gateway): This node is responsible for communicating with PDN(Packet Data Network). It also supports policy enforcement functions.

S-GW (Serving Gateway): This is the mobility anchor of the EPC and is responsible for switching between different wireless mobile technologies. It also routes data

traffic between P-GW and eNB.

MME (Mobility Management Entity): This entity controls and manages authentication, authorization and mobility of the UE in control plane.

PCRF (Policy Control and Charging Rules Function): This entity manages service policies and QoS for each user. It communicates with the PCEF (Policy and Charging Enforcement Function) in the P-GW and updates the PCC (Policy and Charging Rules) rules.

The EPC performs functions fundamental to the delivery of mobile data services and provides connectivity to the internet and the services environment of the carrier. These attributes make the packet core influential to innovation of services and a cornerstone to operator monetizing strategies.

Release 8 of 3GPP defines EPC and is newly developed technology to support LTE; but along with new services is has the features to incorporate with 2G, 3G, and non-3GPP access as well. Key functions of the mobile packet core, which are common in all the generations, include:

Mobility Management The ability to track users as they move between cell sites (across routing areas or tracking areas) and route traffic accordingly is the key function of core network. In EPC this functionality, potentially, also applies to non-cellular access, such as WiFi.

Session Management Establishing bearer setups and managing the information flow of a particular service or application is the basic function of the packet core. This "session layer" is critical to delivering differentiated service quality.

Security and Privacy Authentication, encryption, and user privacy are primary functions of the core network. Insofar as the operator positions itself as a trusted provider, these are commercially valuable service attributes, above and beyond their primary functions.

Policy and Charging The mobile packet core has always had a role in charging for usage and content. This is extended significantly in LTE, with sophisticated policy management, inherent to the architecture, the policy is tightly linked to session management.

EPC elements interact with each other according to the policy architecture, which makes decisions about how to allocate network resources. The policy architecture manages information provided by the lower-layer packet core nodes and acts on it according to operator preferences. It is fundamental to network management and is an important tool to help operators evolve their service portfolios.

The introduction of LTE has moved the wireless communication market from its traditional voice environment to a data environment.

LTE introduces new approaches to charging, policy control and policy enforcement functions as well as new network elements. This creates a need for multiple fraud protection and network security system integration points [22].

2.2 LTE emulator

LTE emulator is a (Linux based) SW reference implementation of a certain 3GPP/LTE network elements and the terminal. It is functionally a 3GPP standard based Nokia product, which is similar to any real time LTE network, capable of communicating with respective network elements. The whole emulator family covers all parts, end-to-end, i.e. from terminal to core network elements. LTE air interface (layer 1) is out of the scope of the main emulator.

Emulators are typically used in all sorts of R&D demos, concepts and trial developments. They are also used in product testing phases, for example, they provide tested, executable protocol software family and real-time emulators based on 3GPP specifications.

LTE emulators have a long history. The story goes back to early 1990's, when GPRS (General Packet Radio Service) emulators were developed. Later they were extended by EDGE (Enhanced Data rates for Global Evolution) and 3G support. A new configuration parameter set was taken into use for the LTE emulator 2011 release. LTE emulator elements are tabulated in Appendix A and provide a better understanding of it.

LTE Emulator setup

Figure 6 represents the emulator nodes used in this research.

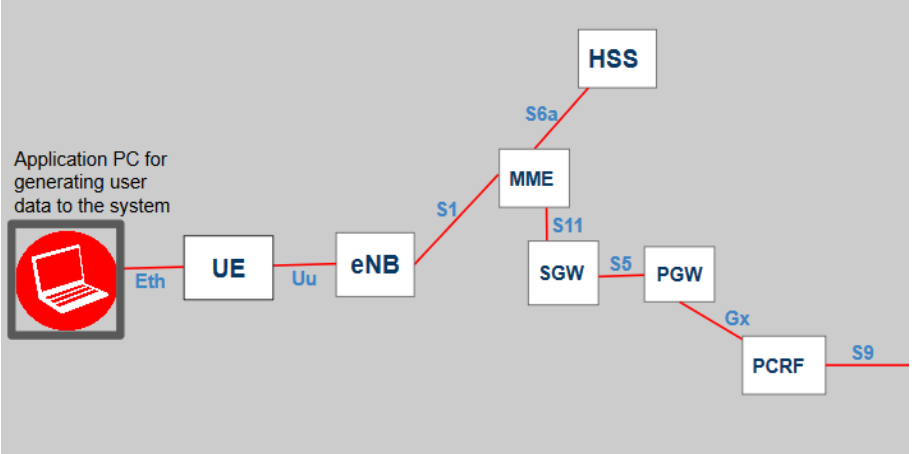

Figure 6: Logical structure of LTE Emulator

Operation

The prerequisite for starting an emulator is that an emulator has to be installed and configured.

The LTE emulator system is typically managed by issuing commands to LTE emulator elements and entities which are under execution. If they are started in foreground or window mode, then commands are entered into character based xterm–windows. If they were started in background mode, the only option is to use the user interface run-time environment.

In this project, we are using emulator in foreground and windows mode as shown in Figure 7. All the emulator windows are opened on the host computer screen and we can write the commands directly on the xterm-windows. Commands are basically macros, i.e. a set of CVOPS (C- based Virtual Operating Systems) signals, and possible parameter values to them. CVOPS is a protocol development framework. The highlighted text in Figure 7 represents the IMSI number, mentioining the communication between the nodes is done using IMSI number of the subscriber.

Figure 7: LTE emulator windows

2.3 Diameter architecture

For 2G/3G, the SS7 (Signaling System 7) and RADIUS (Remote Authentication Dial In User Service) protocols were used for authentication, authorization, accounting [59]. The need to design new protocols arose by the introduction of IP networks, roaming and security [21]. The variation in user equipment utilized to access the network became multidimensional; for example, 3G, LTE, Ethernet and WiFi. As specified in the IETF [9] documentation the reasons of Diameter introduction also include fail over, security and audit ability.

Diameter is referred to as Authentication, Authorization and Accounting AAA Pro-

tocol [6] and is defined as a base protocol by IETF in document 3588 [63] and 6733 [46]. Diameter applications are used in all mobile environments including Evolved Packet System (EPS), IP Multimedia Subsystem (IMS), Policy and Charging Control (PCC), Generic Authentication Architecture Generic Bootstrapping Architecture (GAA/GBA) and Machine-to-Machine (M2M).

Key features of the Diameter base protocol include: message delivery (between the nodes) in the form of AVPs, switching to different protocols, error and fault notification, expansion (addition of new nodes), managing both user sessions and accounting.

This section covers the basic architecture of the Diameter protocol and highlights the LTE network interfaces that are using Diameter. Later, Diameter message structure, AVP and session establishment are discussed.

Diameter Base Protocol Architecture

Diameter Architecture is a combination of entities which include:

Diameter Peer: Every Diameter Node directly connected to other Diameter Node is a Diameter Peer.
Diameter Client: Diameter clients control the access to the network. It includes MME, PCEF and PCRF.
Diameter Server: Diameter server deals with the authorization and authentication of a subscriber and its accounting details. Diameter servers are HSS and PCRF.
Diameter Agent: They provide services, such as relay, proxy, redirect and translation. The agents are defined according to the services.
Diameter Relay Agent: Diameter relay agents manages the routing of the messages, on the basis of destination information. No application level processing is performed by a relay agent. Only routing information is modified. It does not manage the session state, but manages the transaction state.
Diameter Proxy Agent: Proxy agent also routes the Diameter messages based on the Diameter routing table. It can modify the messages, manages the transaction state and implement the policy enforcement function. It may also manage

[6] https://tools.ietf.org

the session state. Understanding of services provided is necessary for policy enforcement, therefore, the proxy agent only advertises the Diameter Applications it support. An example of Diameter Proxy Agent in LTE is Diameter Routing Agent.
Diameter Translation Agent: It translates between two protocols; for example, one which translates S6 Diameter Interface into Cx MAP interface.
Diameter Redirect Agent: It only returns answers with important information for direct communication with the destination. No session state or transition state is managed. Redirect Agent performs no application level processing, it only provides relaying services for all Diameter applications. One example is the SLF (Subscriber Locator Function) in IMS.
Figure 8 represents the block diagram of LTE, in which Diameter interfaces are highlighted in green color. The Diameter based interfaces between the Diameter Nodes and their functions are summarized in Table 2.

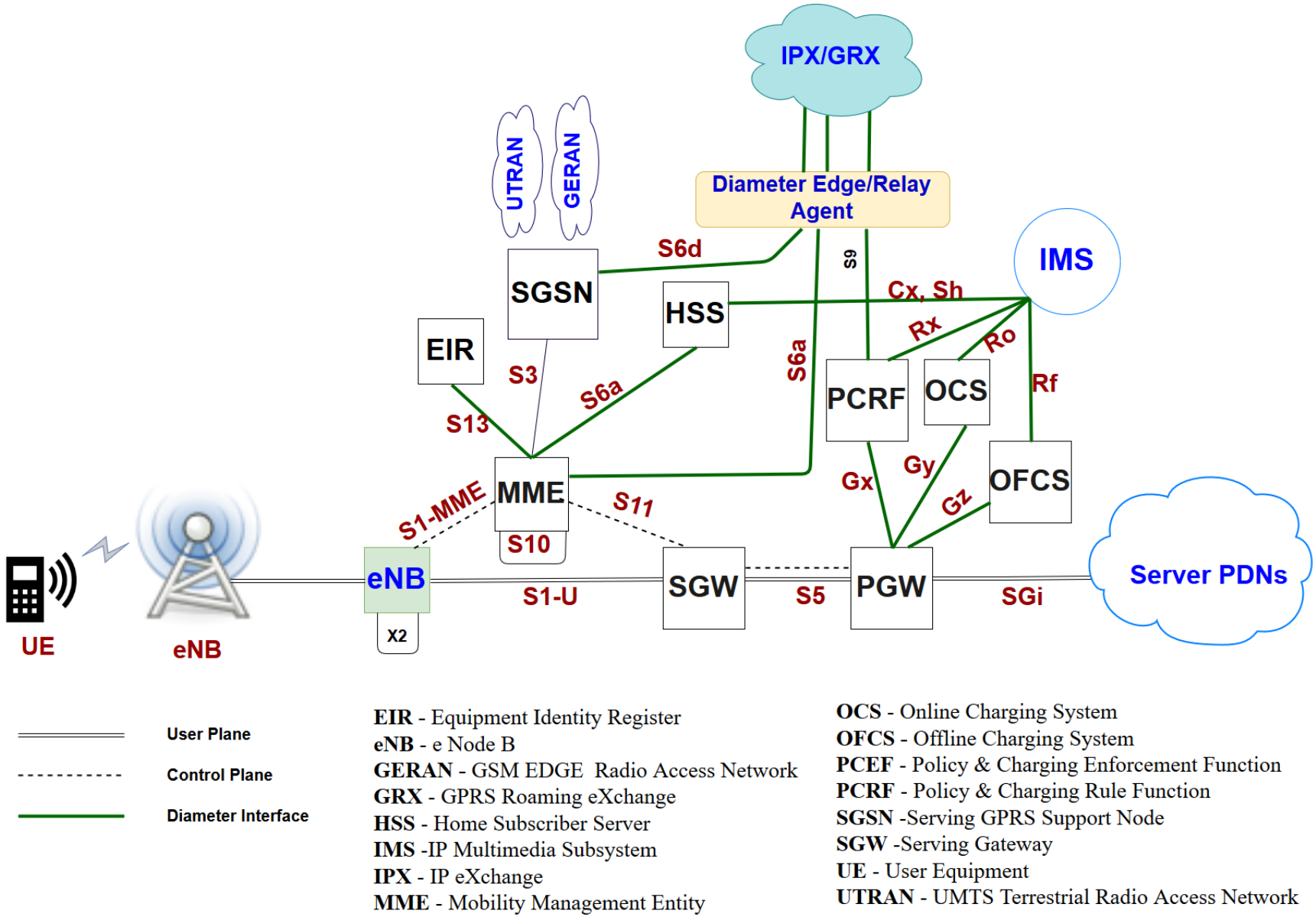

Figure 8: LTE Architecture with Diameter Interfaces

Interface	Nodes	Function
S6	MME - HSS	Enables transfer of subscriptionand authenticationdata for authenticating/authorizing user access to the LTE network.
S13	MME - EIR	Used for IMEI (International Mobile Equipment Identity) check which is stored in Equipment Identity Register.
Gx	PCEF - PCRF	Is used to communicate PCC rules.
Gy	PCEF - OCS	Is the online charging interface.
Gz	PCEF - OFCS	Is the offline charging interface.
S9	HPCRF - VPCRF	It is used when the PGW stsrts or terminates the bearers of the visiting user.
Rx	IMS - PCRF	It enables IMS to request dedicated bearer to guarantee the quality of service of the IMS sessions.
Cx	IMS(call server) - HSS	It is used to authenticate,authorize and locate the user.
Sh	IMS(application server) - HSS	This interface is used to obtainservice data required for service execution.
Rf	IMS(entities) - OFCS	Used for offline charging of IMS sessions and services.
Ro	IMS(entities) - OCS	Used for online charging of IMS sessions and services.

Table 2: Diameter interfaces, their position and functionality

Diameter Message Structure

Diameter Protocol is message based and includes two types of messages: request and answer messages. The message structure is shown in Figure 9, and the fields included in the message are explained in Table 3

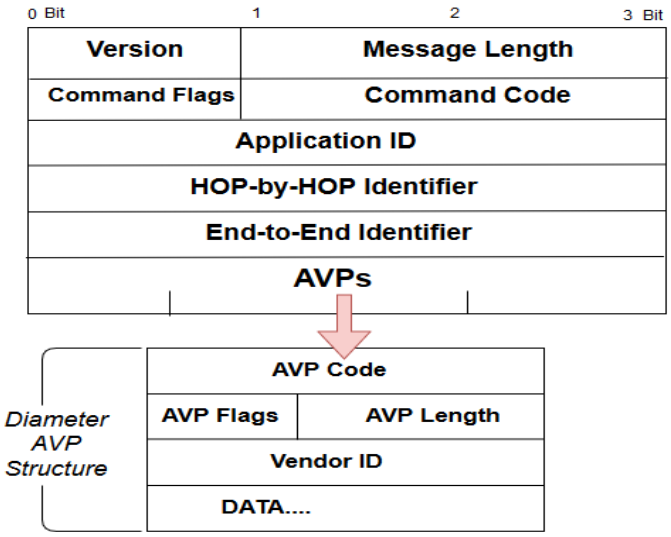

Figure 9: Diameter message and AVP structure

Fields	values
Version	The used version of the Diameter Protocol.
Message Length	Total length of the Message Header and AVP.
Command Flag	Eight bits [0-7] length representing [R P E T r r r r] respectively. R - For set -> Request message else an answer message. P- Message is either proxy, relay or redirected. E - If set -> Error message. T - if set -> potentially re-transmitted message and r stand for reserved , to be used as per the requirement.
Command Code	This field is three octets. It is uniquely assigned for each message request. For RAR/RAA messages, Command Code value is 258, for CCR/CCA it is 272.
Application ID	To identify the Diameter applications. It is four octets. eg, application ID for S9 interface is 16777267.
Hop-by-Hop Identifier	It is unique 32 bit integer for per connection per defined time. The request and answer messages have same Hop-by-Hop identifier values.
End-to-End Identifier	Detects duplicate messages.

Table 3: Diameter Message Structure Fields [8]

Diameter AVP Structure

Data exchange in the Diameter Protocol is in the form of AVP (Attribute Value Pair). It is a basic part of the Diameter message. The AVP message format is depicted in Figure 9 and the fields are discussed in Table 4.

Fields	Functions
AVP Code	AVP Code and Vendor-ID are used together to identify the unique attribute.
AVP Flags	To inform the receiver about handling each attribute.
AVP Length	Total number bits used in all fields of the message.
Vendor-ID	This field contains individual vendor identification number assigned by the IANA[7]. Vendor can add their own specific Vendor -ID to this ID.
Data	It contains the information.

Table 4: Diameter AVP Structure Fields [8]

AVPs are the fundamental data representation in many applications.To explain AVP structure we consider Figure 10. Figure 10 shows the Diameter packets captured over Gx interface and the details of RAA (Re -Authentication Answer) packet. The packet consist of multiple AVPs which are differentiated by their AVP code: Session-Id, Origin-Host, Origin-Realm, Result-Code, Origin-State, IP-Can-Type and Charging-Rule-Report.

In Figure 10 the Charging-Rule-Report AVP details:AVP code, AVP Flags, AVP Length, AVP Vendor Id and Charging-Rule-Name.

The Charging-Rule-Name AVP details about the PCC rule, which we target to manipulate in this research.

Figure 10: Wireshark captured Diameter packet showing AVPs

Diameter Stack

Figure 11 demonstrates the Diameter stack flow. Diameter messages can be streamed over both transport protocols, Stream Control Transmission Protocol(SCTP) and Transmission Control Protocol (TCP) [67]. Transport security protocols are optional. Transport Layer Security can be applied between two Diameter peers. The request initiating node represents the TLS Client and the receiver is the TLS Server. The TLS client is requested for the authentication certificate by TLS server for mutual authentication. Independent security options are also available with Diameter, such as IPSec. It is dependent on the user to have secure peer to peer communication. The diameter existing applications which are implemented using AVPs can be extended by adding new AVPs. Different 3GPP interfaces have their own defined application AVPs.

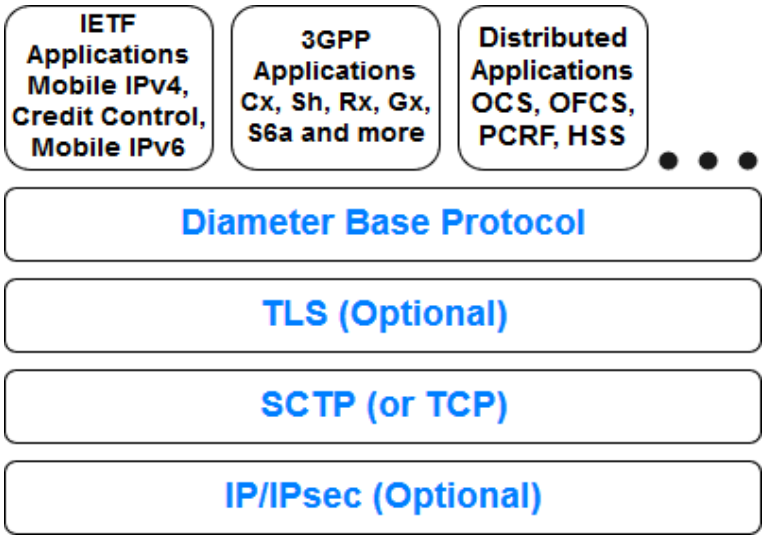

Figure 11: Diameter protocol stack (Adapted from [67])

2.4 LTE roaming

Roaming is the state of the subscriber or UE, when it is out of the geographical coverage area of its home subscribed network operator. When a subscriber is out of the network range, the mobile phone tries to communicate using an available network (visiting networks) and gets connect access from the network which has legal agreements with the home network operator. These agreements among different MNOs (Mobile Network Operators)are handled by GSMA [8] (GSM Association) GSMA addresses and supports the mobile operators across the world. The main support areas of GSMA include international roaming, interconnect agreements and solutions.

The LTE roaming includes the availability of services to a user, by the visited network. Mode of connection services, both in user plane and control plane depend on the type of roaming scenarios.

2.4.1 Roaming scenarios

The methods by which the roaming services are accessed, define the roaming scenarios. The services can be provided in many ways to a mobile user, depending on the type of services available at the home network operator and the visited network

[8] https://www.gsma.com

operator. For this research we consider both home network operator and visited network operator support and implement LTE services. By this we can come up with two roaming scenarios as mentioned in GSMA IR.88 [6].

Home routing roaming In this scenario the UE is connected to the network by PDN gateway (PGW) but the services are used from the Home network. **Local breakout roaming** In this scenario the services are used from the visited network and the status of the services is updated with the home PCRF (HPCRF).

A detailed explanation of the roaming scenarios is shown in Figure 12.

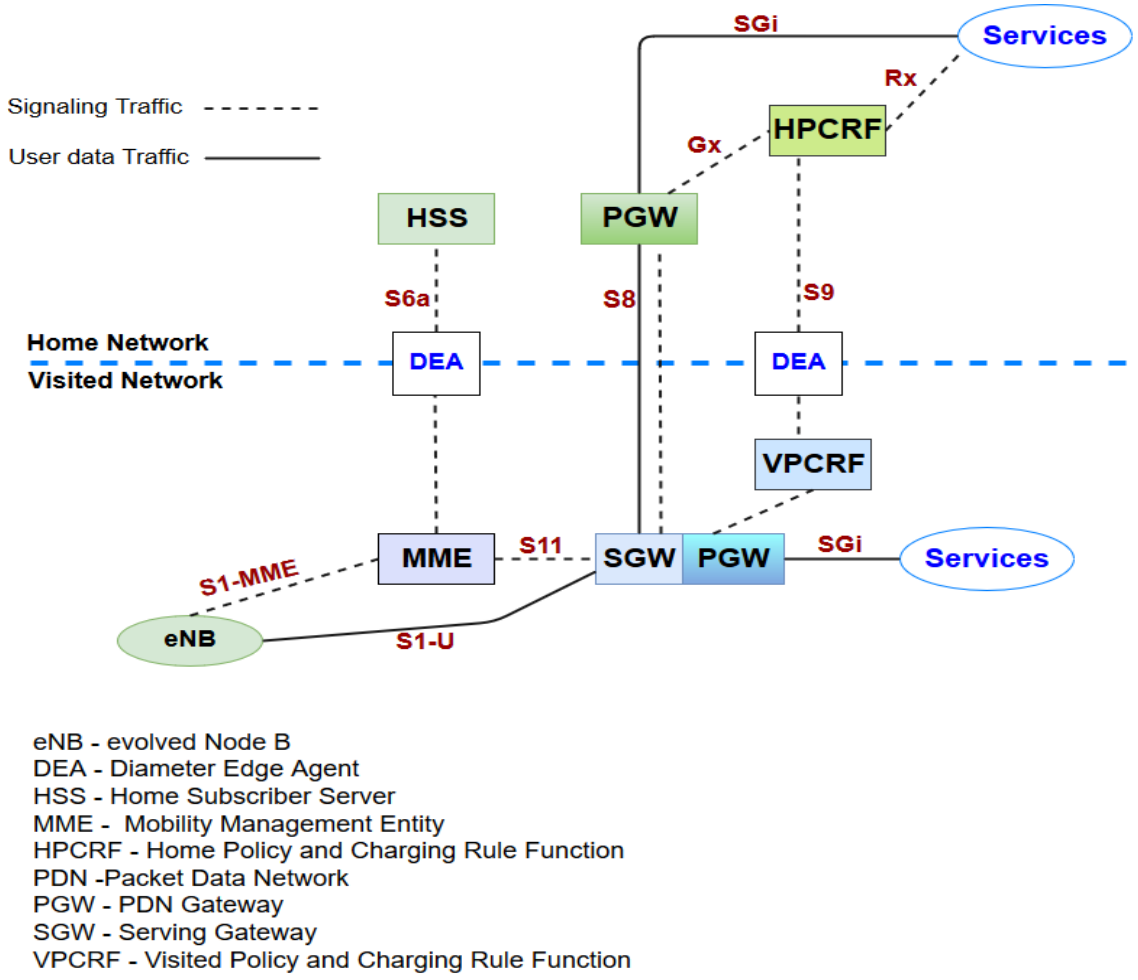

Figure 12: Roaming architecture

2.4.2 Roaming interface protocol stack

Figure 13 shows the roaming interface S9 between the Home PCRF and the Visited PCRF. The interface is used in Local Breakout Roaming scenario to commu-

nicate policy and Charging Control (PCC) rules.

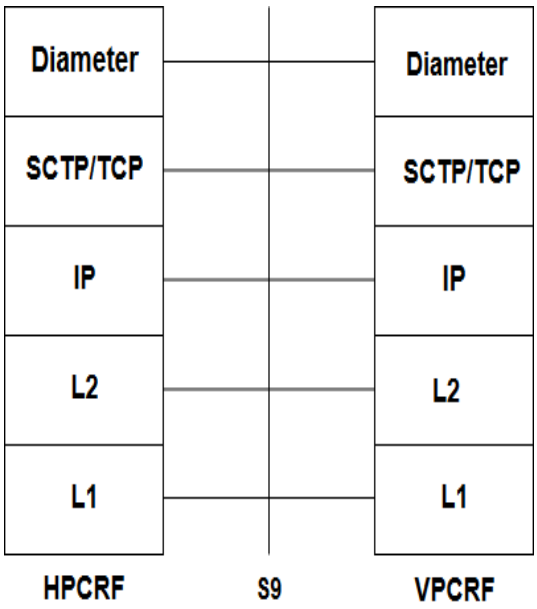

Figure 13: S9 interface protocol stack (Adapted from [10])

2.4.3 Roaming charging

The roaming charging depends on the type of roaming scenario used.

In the case of home routed roaming the charging is done by the home network of the roaming subscriber.
While in the case of the local breakout roaming, since all the controls are in the visited network, charging is also done by the visited network for the roaming subscriber, and is communicated to the home network over the S9 interface through the third party network service provider IPX [24].

2.4.4 Roaming security and issues

The biggest challenge with LTE roaming, is the agreements among the operators needed to support IP signalling. This requires to overcome interoperability challenges, as not all operators support all existing operational technologies. Quality of services varies from network to network which remains an issue to the roaming subscribers. Since third party network is introduced for routing, security has become a key issue with LTE roaming [26].

2.5 IPX architecture

IPX (IP eXchange) is an interconnection network defined by GSMA [9]. It was introduced to provide global roaming facilities to the MNO's subscribers. IPX services include Voice over IP (VoIP), IP Multimedia Subsystem (IMS) interworking, LTE roaming [39].

To provide roaming services to its subscribers MNOs need to spend on infrastructure and have to manage many agreements between different MNOs across the world. IPX is the solution to these problems and provide same network services overseas as a subscriber uses in it home network.

IPX manages multilateral interconnection agreements among the operators and the operator has to manage only one agreement contract. Also the infrastructure cost to have interconnection with other MNOs is reduced.

Interoperability is another issue with roaming. Interoperability is defined as a degradation from LTE network to 2G or 3G while roaming. Its not always necessary that LTE network is deployed in the visiting network. There are different cellular network technologies and a visitor subscriber has to switch to some other technology. IPX is a solution to this and supports local breakout and home routed roaming, providing large coverage area while maintaining QoS.

There are also some issues with IPX network providers. To provide full coverage and maximum connectivity the IPX service provider across the world have to be interconnected and this is called peering among the IPX providers.

World wide peering of IPX network providers helps in flexibly routing of signaling traffic between different MNOs across the world.

Here comes the loophole in handling the signaling traffic of a roaming subscriber. The MNO has an agreement with one IPX network provider and it is the IPX network provider who routes the signaling traffic. Therefore the introduction of the third party service provider may make roaming insecure. Figure 14 shows the connection between two MNOs by S9 interface through IPX network and the Diameter agents (DRA, DEA).

[9] www.gsma.com

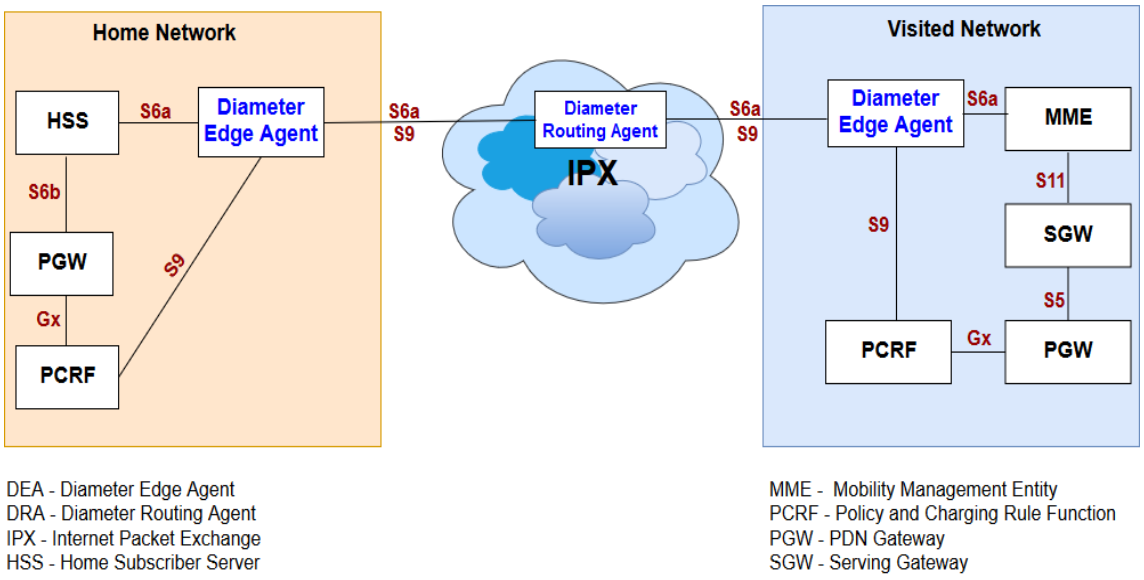

Figure 14: IPX connecting home and visited network providers around the world

2.6 PCC architecture

The 3GPP Policy Control and Charging rule specifications [5] define the functionality of PCC rules.

A subscriber purchases subscription plan, to access the network services. As per the subscription plan the MNO provides services to the subscribers. At the starting of a new or modified EPS (Evolved Packet System) or IP-CAN session the PCC rules are decided for that session. This decision is made as per the subscription plan and are applied to the EPS session by PCEF (Policy and Charging Enforcement Function). This subscription plan is communicated over the Gx interface in case of Home Routed Roaming and is communicated over S9 interface in case of Local Breakout Roaming. PCC rules define everything about the subscription including data plan type, data rate, prepaid or postpaid, QoS.

PGW (PDN Gateway) establishes the Service Data Flow (SDF) and implements the PCC rules for the specific user. PCC rules also define the establishment of new session, its termination and modification.

When a session is established, the PCEF sends Credit Control Request (CCR) message to the PCRF requesting the applicable rules for that session. PCRF answers with the Credit Control Answer. This procedure is called pull procedure.

The other procedure is push procedure in which the PCRF pushes the PCC rules through the Re-Authentication Request (RAR) message. PCEF authenticates with the Re-Authentication Answer (RAA) message.

3 Mobile network security breaching

The most common mobile security breaches include [18]: Lost or stolen mobile device, Mobile app vulnerabilities, Web services attack and MitM attacks

Mobile networks have been breached through several interfaces [13, 31–34, 51, 52]. In the latest research [35] 36 new flaws have been spotted in LTE network design and implementation scenario along with different carriers and device vendors. The vulnerability attacks include DoS, phishing, eavesdropping and manipulating data traffic. To get into the system, an attacker needs at least one legitimate authentication message request. Different methods are used depending on the generations of mobile technologies [66].

In case of the LTE and Diameter Protocol, we have opted for a man in the middle attack, by capturing the policy decision messages over the S9 interface. To have a targeted attack and least probability to get access denial message, attacker need to have an IMSI number which then opens doors for many possible attack methods.

In this section, we discuss the methods to breach the mobile network through the air interface (to collect the IMSI) and network-to-network interface (MitM attack).

3.1 Fake base station

A fake base stations is virtual base trans-receiver station utilized in mobile communications. The most common one is the GSM base station, which works for 2G mobile technology. Since there is no dual authentication requirement, it is easier to target GSM subscribers[27]. The fake base station is mostly used for intercepting mobile call traffic and performing MitM attacks. Despite having mutual authentication, LTE fake base stations are also designed and used [14]. Researchers are coming up with new methods for protecting 5G from fake base stations [44].

3.2 IMSI Catcher

The IMSI (International Mobile Subscriber Identity) is used for the identification of any subscriber and is stored in the SIM (Subscriber Identity module) card [3].

An IMSI catcher is a setup designed to operaate as a base trans-receiver station in order to trick the mobile phones to connect to a fast and strongest signal strength available network. Designing of cell phones focus on connecting to all compatible towers. This feature is used by the IMSI catcher to represent itself to cell phones as a tower from the mobile network services provider. This vulnerability allows the attacker to view all the data to and from the mobile device [42].

Experimental Setup

To build the fake base station, we used two tools: OpenBTS[10] software and Universal Software Radio Peripheral (USRP[11]) as Software Defined Radio (SDR)

Open BTS replaces the GSM tower by software implementation [12]. Figure 15 shows the basic blocks of Open BTS.

[10] www.openbts.org
[11] www.ettus.com

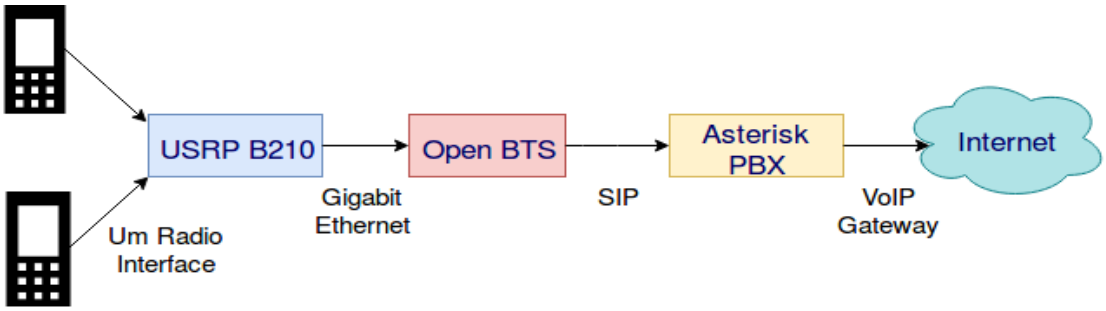

Figure 15: Open BTS blocks

Network air interface is implemented by software defined radio (SDR) which is an electronic device commonly called USRP, and is designed to work on various frequency bands.

The core management functions are executed by the Open BTS software, which directs the calls to the Asterisk instead of MSC (Mobile Switching Center) as in GSM.

Astrisk[12] is an open source VoIP service, used to handle all voice traffic to and from the OpenBTS cell tower. It communicates and handle SIP (Session Initiation Protocol) requests.

Figure 16 shows the block view of the OpenBTS Software structure.

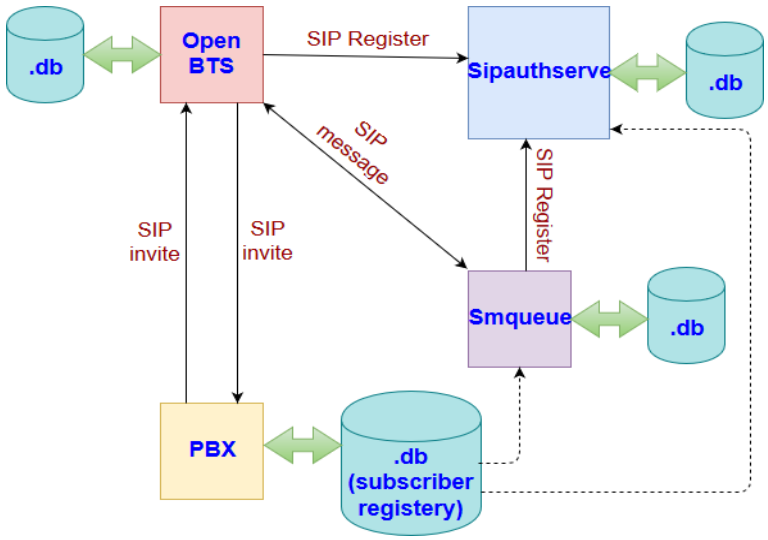

Figure 16: Software Architecture of Open BTS (Adapted from [11])

[12] www.astrisk.org

A brief explanation of the building blocks of this fake base station are as follows.

SIPAuthServe signifies (SIP Authentication Server) and is used for all types of authentications in OpenBTS. It processes the SIP Register request every time a mobile handset agrees to connect to the OpenBTS network. Once the connection is established. The IP address of the OpenBTS is updated by the SIPAuthServe at the subscriber registry database, which enables other subscribers to communicate.

SMQueue (SIP Message Queue) processes the SIP message requests. The SIP message requests are made by OpenBTS to let the handset send SMS, which can also be stored and forwarded at any scheduled time in the SMQueue register.

Subscriber Registry It is similar to the HLR responsible to save and authenticates the subscriber identity. It helps Asterisk to communicate using text messages and voice calls among different subscribers.

3.3 Uses of IMSI

International Mobile Subscriber Identity (IMSI) is necessary to communicate, to access services from the subscribed network to the UE. A Mobile Network Operator (MNO) identifies UE with its subscribers IMSI number and provides services according to the subscription [3]. The IMSI retrieved have many applications within or outside the MNO's network.

Uses of IMSI Catcher

A fake base station has both positive and negative uses.

Advantages include the use of IMSI catcher by law enforcement personnel (Secret Services, national Guards, Police) to point out and locate the major or minor criminals [29]. It can be used for Searching and locating someone at emergency sites. Establishing emergency cellular network in case of disaster [28]. It can be used to detect the Presence of targeted person or someone suspicious.

Contrary to this IMSI catcher uses have some drawbacks including, spy on law enforcement personnel or businesses activities, intercepting calls, invading privacy of anyone in range, data usage, messages and denial of services in case of emergency.

3.4 Possible IMSI catching methods and countermeasures

Other ways to get the IMSI:

WiFi Access point (WiFi Pinapple) - A wireless router can be used to spy and track people just by small modifications in the software.[54]

IPX access and SMS delivery trick [65]

Device virus can also be one of the option to hack a device. By providing system update message one can implant malicious software and control the device.

There are countermeasures to catch the IMSI catchers[16]. An efficient way to catch the IMSI catcher are apps. These software apps communicate to the UE baseband chip to detect strange handovers and other network anomalies which point to a potential fake base station activity. Few example apps are AIMSICD, Snoopsnitch, Darshak [15] and Pwnie Express [17, 49].

3.5 Network-to-network breaching methods

The Network to network interconnection consist of a connection between the home network and networks in rest of the world . These networks may not always be directly connected which is next to impossible. Vulnerability in network to network interconnection exist when the user in the VPLMN (Visited Public Land Mobile Networks) is in roaming scenario. An example attack on roaming interconnection is made through S6a interface (an interface between HSS and MME) [48]. Such attacks are used to identify the subscriber profile over S6a interface from MME using IDR (Insert Subscriber Data Request) or IDA (Insert Subscriber Data Answer) messages. Here the attacker represent itself as HSS.

In this thesis project we are discussing S9 interface vulnerabilities where we aim to modify the billing parameters, called the PCC (Policy and Charging Rules) rules during the communication between VPCRF (Visited Policy and Charging Rule Function) and HPCRF (Home Policy and Charging Rule Function). An interconnection security procedure is discussed by GSMA FS.19 [25], defining filtering in the signaling messages on DEA(Diameter Edge Agent) or DRA (Diameter Routing Agent), demonstrated in Figure 17. This filtering Architecture in Diameter is unable to distinguish between the fake and real messages . We use this drawback of

Diameter to successfully manipulates the RAR (Re Authentication Request) and RAA (Re Authentication Answer) messages over S9 interface.

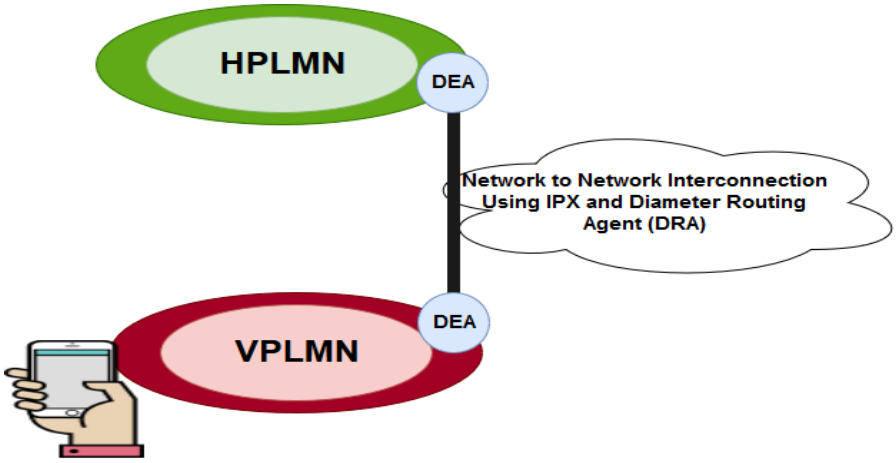

Figure 17: Roaming Interconnection defined by GSMA

4 Steps Leading to Fraud or DoS Attack

It is always challenging to prove the real time complex network results on an experimental platform. This section demonstrates the steps followed to successfully implement the denial of services and fraud attack on LTE subscriber, through roaming interconnection S9. The test setup may vary for different environments and may differ from the real implementation. A standard implementation process is used to perform all the tests. The steps includes: IMSI catching, Fake PCRF pretending to be HPCRF or VPCRF, Capturing PCC rules from RAA messages Manipulating the PCC rules.

4.1 IMSI Catchers

The IMSI capture designed for this project is using Ettu's USRP. The whole setup is similar to the one explained in section 3.2. The image shows the laboratory setup for an IMSI catcher and image has the captured IMSI's.

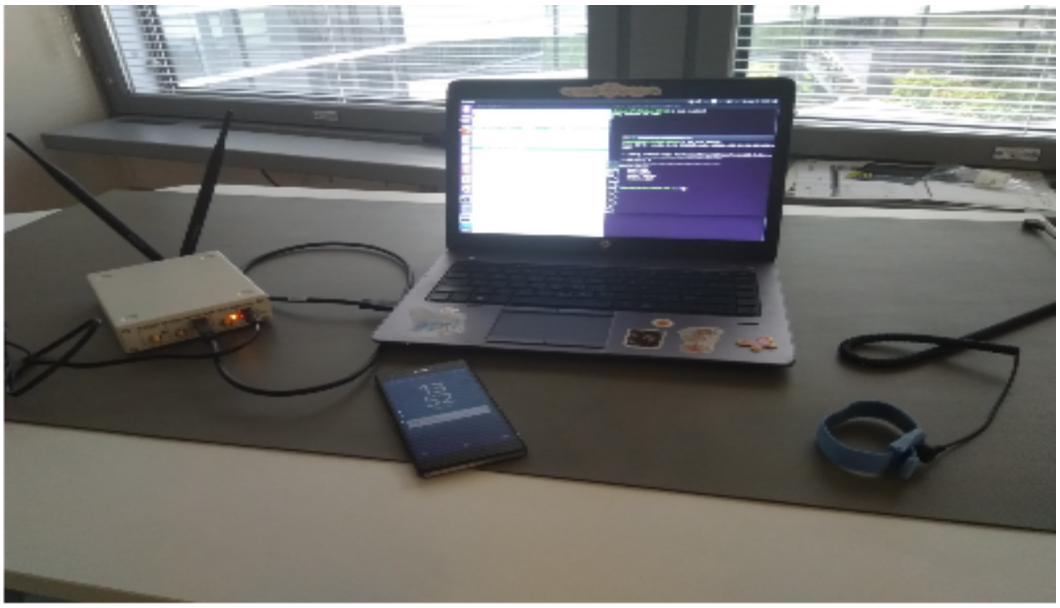

Figure 18: Designed IMSI Catcher setup

```
OpenBTS> tmsis
IMSI TMSI IMEI AUTH CREATED ACCESSED TMSI_ASSIGNED


OpenBTS> tmsis
IMSI            TMSI IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
244054104821808 -    353393091029920 2    15s     15s      0


OpenBTS> tmsis
IMSI            TMSI IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
244054104821808 -    353393091029920 2    28s     28s      0


OpenBTS> tmsis
IMSI            TMSI IMEI            AUTH CREATED ACCESSED TMSI_ASSIGNED
244123100083365 -    358571072674620 2    135s    135s     0
244070103900373 -    354187076122880 2    95m     95m      0
244054104821808 -    353393091029920 2    106m    106m     0
```

Figure 19: Snapshot of the captured IMSIs

4.2 Fake PCRF (HPCRF or VPCRF)

After the IMSI is collected, a fake PCRF can be used to communicate to the MNO's PCRF pretending it to be a visited PCRF. It can communicate and trigger the Credit Control Request (CCR) to the HPCRF. HPCRF in response sends

the Credit Control Answer (CCA).

The PCRF used to pretend as a Home PCRF or Visited PCRF, is from the LTE emulator. In LTE emulator the PCRF is assigned a node IP address, since we have tested them on the same machine, the PCRF and PGW, work on the same kernel. The VPCRF can trigger the message to the HPCRF if the IP address of the host node is known, which our case is same on both ends. The communication between the HPCRF and VPCRF is as shown in the Figure 20.

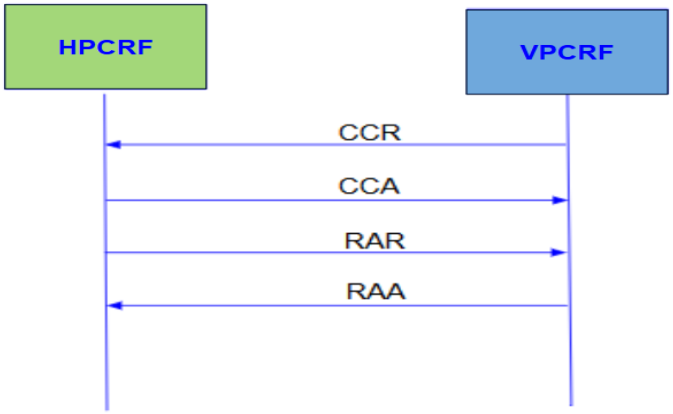

Figure 20: Communication between the two PCRF nodes

The messages shown in Figure 20 are CCA, CCR, RAR and RRA. The Credit Control Request (CCR) is send by the VPCRF to HPCRF in order to request PCC and QoS rule. Credit Control Answer (CCA) is send by the HPCRF to VPCRF in reply of the CCR message. This procedure initiates the event. Re-Authentication Request (RAR) is sent by the HPCRF to the VPCRF providing QoS and PCC rules for that event. Re-Authentication Answer (RAA) is send by the VPCRF to the HPCRF in reply of the RAR message.

4.3 Capturing Diameter messages

The Diameter message packets can be captured through wireshark. Wireshark is a helpful open source packet analyzer tool. The network traffic can be captured and analyzed.

DIAMETER uses TCP or SCTP as its transport protocol and the default port number is 3868. By setting the port number and diameter filter on the wireshark

we captured the Diameter packets.

The captured packet is used to check the Policy Control and Charging Rules for the specific IMSI number.

The Diameter Gx interface packets were captured twice. Once before changing the PCC rules, as shown in Figure 21 and second, after changing the PCC rules, shown in Figure 22.

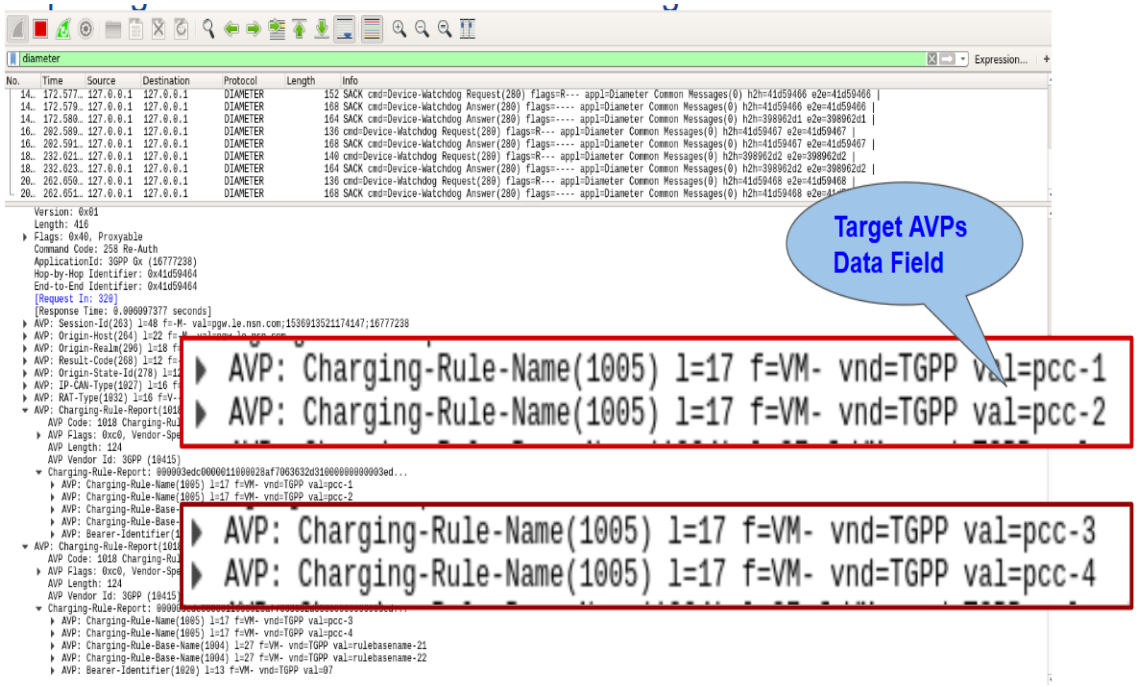

Figure 21: PCC rules before any change in the captured packet

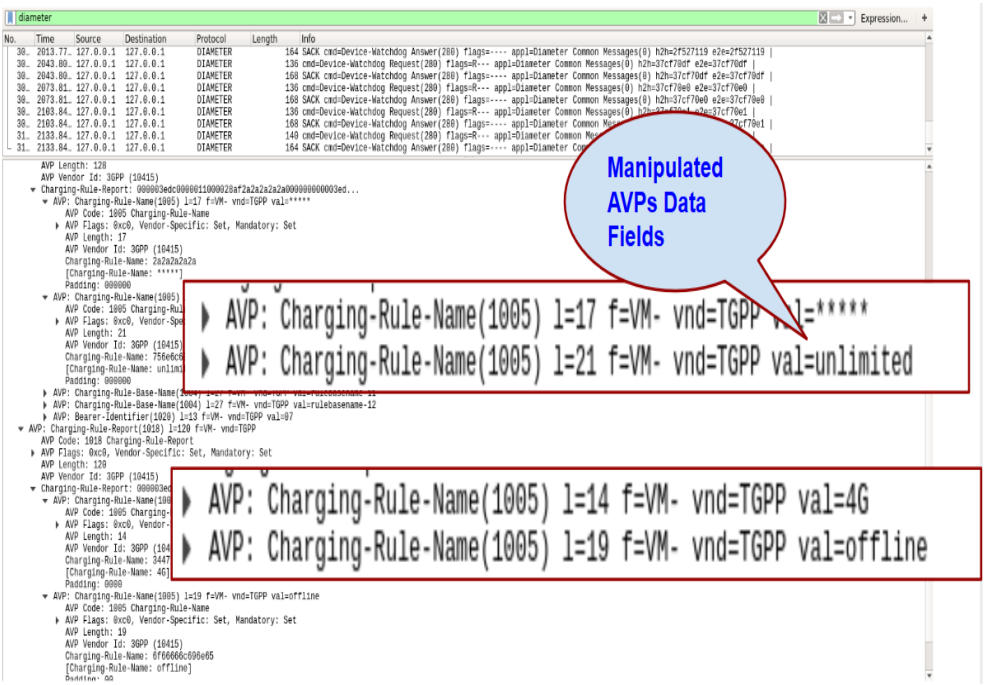

Figure 22: PCC rules after the change has been made in the name field AVP

4.4 Manipulating the PCC Rules

The Denial of Service (DoS) or fraud attempt can be interpreted as a man in the middle attack. The attacker posing as a HPCRF and VPCRF is the man in the middle and can also be a part of the IPX or outside its network. Snapshot represents the concept how the PCRF emulator can be used to talk to the HPCRF or VPCRF over Diameter Edge Agent.

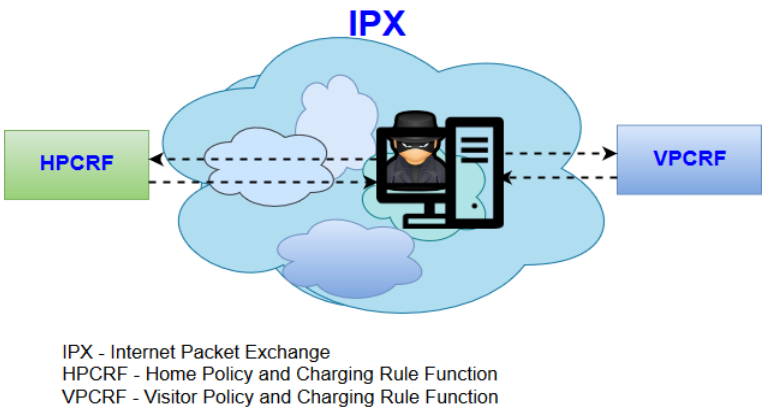

Figure 23: Attacker posing to be the Home PCRF and Visited PCRF

5 Attack scenarios

We consider an example to frame the attack scenarios and understand the concept of fraud or denial of service for a roaming LTE subscriber. We consider LTE subscriber from USA with home subscription of ABC operator. The IMSI captured is 310150123456789. The IMSI is described in the Figure 24. The operator ABC may have multiple plans for its customers. A subscription plan is as mentioned in Figure 25 which our example subscriber is registered to.

IMSI: 310150123456789

MCC	**310**	**USA**
MNC	**150**	**ABC**
MSIN	**123456789**	

Discription of IMSI number

Figure 24: IMSI details

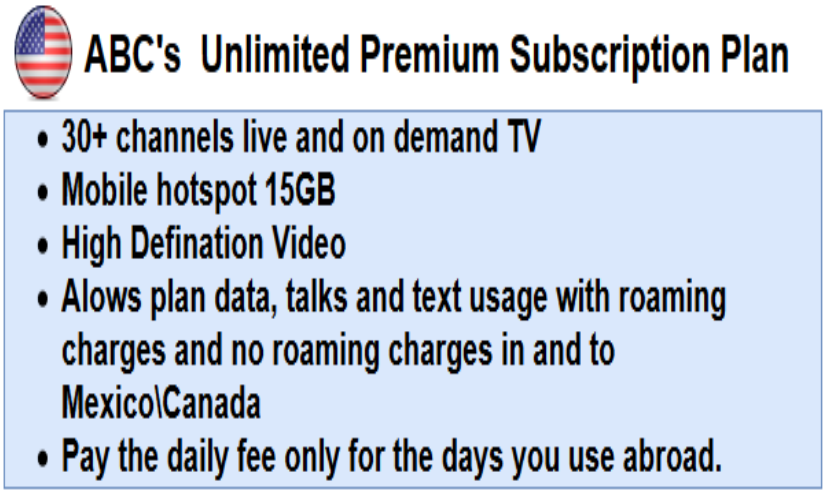

Figure 25: USA operator ABC's Subscription plan

The subscriber happens to visit Finland and is supposed to have network available to access. The operators in Finland will provide services to this visitor but which operator?

The operator XYZ from Finland that already has roaming agreement signed with ABC, USA is supposed to provide network services to the visitor. Through the IMSI communication between the UE and the network it can be identified who is responsible to provide the services. The UE can have the roaming services as per its subscription plan, which are requested by XYZ (VPCRF) to the ABC (HPCRF). The communication is done on S9 interface through the CCR, CCA, RAR and RAA messages. The message communication is depicted in the Figure 26.

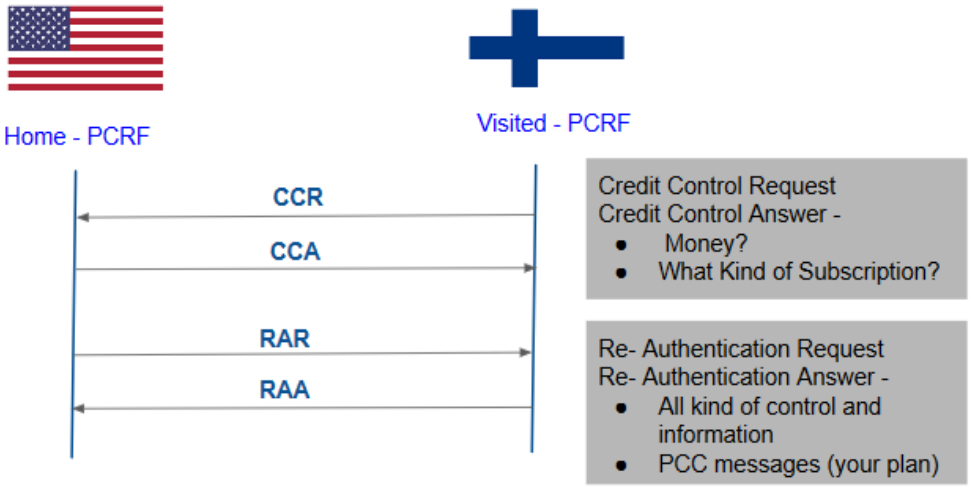

Figure 26: Message flow over S9 between operator ABC(USA) and XYZ(Finland)

The change in the subscription plan can be made during this communication between the HPCRF and VPCRF. The Figure 27 shows the steps included to make a successful fraud attempt.

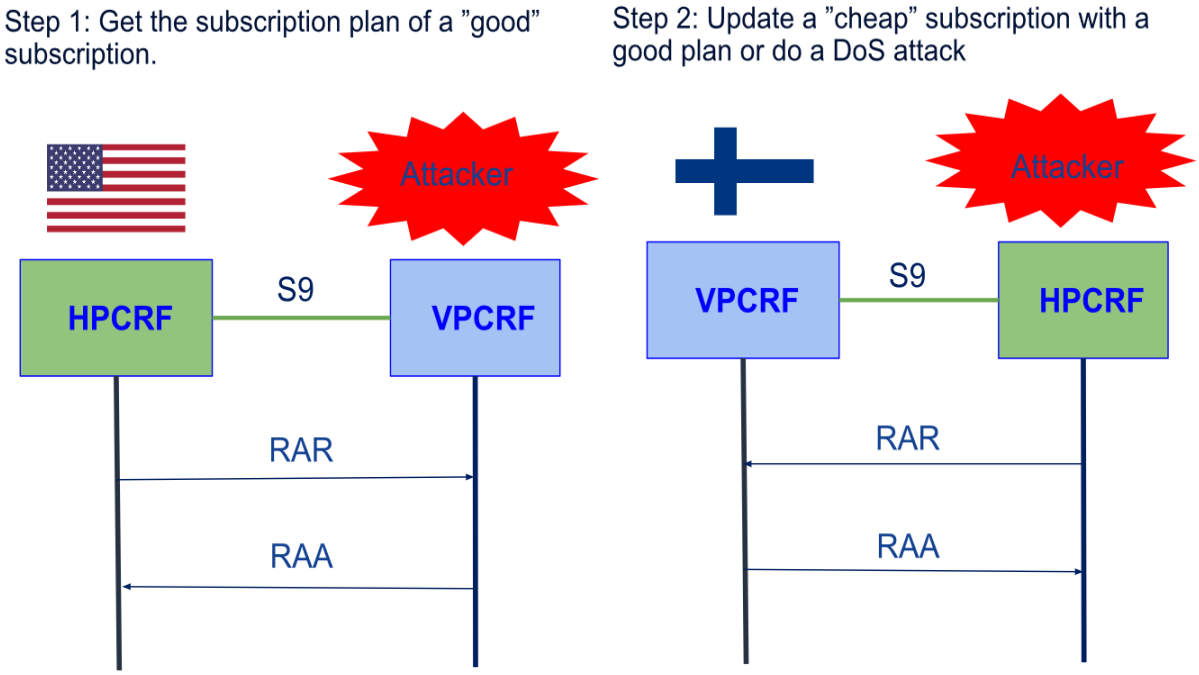

Figure 27: Attack steps

In our experiment on LTE emulator we captured the Diameter packets through the Wire-shark and checked the AVP field containing PCC rules. With the help of PCRF, which can act as a home or visited PCRF a trigger request is made to transmit the PCC rules over RAA messages.

It is manageable to manipulate them and the manipulation is visible on the recaptured packets.

Consequences of the attacks

We have demonstrated a successful procedure to change the Attribute Value Pairs (AVPs) field in the Re Authentication Answer (RAA) messages. These changes results in MitM and DoS attacks which may affect not only subscriber but also MNOs.

The attacker may be benefited to have better services if he is using the attack for his own benefit by changing the cheap subscription to a good subscription.
The attacker can also play by exchanging the subscriptions this may cause shifting in the costs and letting the phone bills in others name. Re-selling is also an opportunity with the attacker to get money out of the attack.

The subscriber may receive a bill for the services he has not used. It is also possible the subscriber is not able to receive services for what he is paying. In both the cases company subscriptions are at risk.

The MNOs may end up in disputes. The consequences are loss of corporate customers. MNOs may be in debt for the costs they cannot charge the subscribers. The carrier cost to the service providers have to be cleared.

6 Conclusion

The question of this research was to identify the vulnerabilities in LTE roaming. In this research we are able to figure out possible attacks on LTE roaming interface, highlighting the gap between the standards and the real implementation. Roaming in LTE is leading towards complex interconnected MNOs. The security and management of the growing roaming traffic need to be framed systematically. Successful IMSI catcher is implemented to capture IMSI. LTE emulator is used to check the Diameter traffic. The MitM attack is made possible using fake PCRF. The manipulated RAA messages can lead to fraud or DoS attack.

6.1 Countermeasures

The real networks may different from the tested network, resulting in failure of attack scenario. But since the opposite case is also possible the author has come up with considerable countermeasures. For every roaming signaling message exchange filters can be introduced with the sending node confirmation as a partner node. Along with this before authenticating the UE the location of the UE and the travel time for the change in location can be compared to avoid illegal authentication. It is also possible that the attacker sends the attach request pretending itself to be HPCRF, this can be avoided by checking messages coming from the own domain address. It is also possible to separate the traffic based on visited subscribers and own roaming subscribers. Another option is to use realm based communication

instead of IMSI.

Using the machine learning tools and algorithms the author suggests a solution of scaling the authentication requests. A bad request can be scaled as negative rank and a true request can be scaled as positive rank. The rank grow stronger or weaker as per the number of true or false attempts. If the false request attempts exceeds certain limit the IMSI is blocked or in red alert zone. Similarly if the true attempts exceeds certain limit the IMSI is in green or safe zone. Green zone user will have more priorities to access the network.Targeting towards intelligent mobile roaming network.

Stronger roaming agreements by GSMA are introduced under Near Real Time Roaming Data Exchange (NRTRDE) [23]. Again it is up to the MNOs how strongly they follow and implement the specifications.

6.2 Limitations

The most challenging part of this thesis is implementing the attack on a real network. Not all deployment possibilities are considered in this thesis which may result in different test cases. The flaws in Diameter protocol figured out in this study may be holed up by other layer protocols.

6.3 Presented work

This thesis work is also presented at security conference (DEF CON 26)[13]under title "4G - Who is paying your cellular phone bill? " where Silke Holtmanns presented the vulnerabilities in LTE roaming interface which leads to fraud attack and DoS attack. The experimental tests were video recorded by Isha Singh and were included in the presentation [56]. Also the work is published with title "Roaming Interface Signaling Security for LTE Networks" in Springer LNCS volume 11359 from year 2018 and presented at 11th International Conference, SECITC 2018 [58].

6.4 Discussion and Future work reflections

The research question for this thesis came up with the discussion on roaming issues with the network operators and subscribers implementing LTE. The research

[13]https://media.defcon.org/DEF

aimed to highlight flaws in Diameter protocol and LTE roaming interfaces. Since LTE roaming is in its early stages across the world and practical setup for the proof of concept is out of the scope of the research therefore no real time test were performed. The tests done in the thesis are done keeping the ethical limits in mind and have not interrupted any user and services.

It is clear from the results that Diameter roaming interfaces are exposed to attacks and threats, therefore the correct configuration of Diameter Signaling control and intelligent routing with firewall is the need of the hour. It is always useful to implement and test in the real time network scenarios, which can be the first thing to advance in this research. Secondly similar vulnerabilities can be looked in the upcoming 5G and IoT network technologies. A suggested solution for IMSI catcher in 5G network technology by implementing a pseudonym between the user equipment and the gNB (5G Base Station) [44].

References

[1] 3GPP. The interconnection of Next Generation Corporate Network . Technical Specification (TS) 32.299, 3rd Generation Partnership Project (3GPP). Version 15.3.0.

[2] 3GPP. Evolved Universal Terrestrial Radio Access Network. Technical Specification (TS) 36.300, 3rd Generation Partnership Project (3GPP), 2010. version 9.4.0 Release 9.

[3] 3GPP. Numbering, addressing and identification. Technical Specification (TS) 23.003, 3rd Generation Partnership Project (3GPP), 2012. Version 3.14.0.

[4] 3GPP. Characteristics of the Universal Subscriber Identity Module (USIM) application. Technical Specification (TS) 31.102, 3rd Generation Partnership Project (3GPP), 2014. version 12.5.0 Release 12.

[5] 3GPP. Policy and Charging Control and Reference Points. Technical Specification (TS) 29.212, 3rd Generation Partnership Project (3GPP), 04 2018. Version 15.3.0.

[6] Association, G. *LTE and EPC Roaming Guidelines*. GSMA, 2017. IR.88.

[7] Aussel, J.-D. Smart cards and digital security. In *Computer Network Security* (Berlin, Heidelberg, 2007), V. Gorodetsky, I. Kotenko, and V. A. Skormin, Eds., Springer Berlin Heidelberg, pp. 42–56.

[8] B. Aboba, J. W. *Authentication, Authorization and Accounting (AAA) Transport Profile*. IETF, 2003. RFC3539.

[9] B. Aboba, T. Hiller, P. M. H. S. P. W. *Criteria for Evaluating AAA Protocols for Network Access*. IETF, 2000. RFC2989.

[10] Balbás, J.-J. P., Rommer, S., and Stenfelt, J. Policy and charging control in the evolved packet system. *IEEE Communications Magazine 47*, 2 (2009), 68–74.

[11] Baldini, G., Sturman, T., Dalode, A., Kropp, A., and Sacchi, C. An emergency communication system based on software-defined radio. *EURASIP Journal on Wireless Communications and Networking 2014*, 1 (Oct 2014), 169.

[12] Behan, L., Orcik, L., Rezac, F., Baronak, I., and Lin, J. C. W. Prepaid voice services based on openbts platform. In *Proceedings of the 3rd Czech-China Scientific Conference 2017* (2017), IntechOpen.

[13] Bikos, A. N., and Sklavos, N. Lte/sae security issues on 4g wireless networks. *IEEE Security & Privacy 11*, 2 (2013), 55–62.

[14] Borgaonkar, R., Shaik, A., Asokan, N., Niemi, V., and Seifert, J.-P. Lte and imsi catcher myths. *BlackHat Europe 2015* (2015).

[15] Borgaonkar, R., and Udar, S. Understanding imsi privacy. In *Vortrag auf der Konferenz Black Hat* (2014).

[16] Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., and Weippl, E. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference* (New York, NY, USA, 2014), ACSAC '14, ACM, pp. 246–255.

[17] De Vries, J. P. Fcc: Friend or foe: Sdr: Trick or treat. *Colo. Tech. LJ 15* (2016), 257.

[18] Delac, G., Silic, M., and Krolo, J. Emerging security threats for mobile platforms. In *2011 Proceedings of the 34th International Convention MIPRO* (May 2011), pp. 1468–1473.

[19] Engel, T. Locating mobile phones using signalling system 7. In *25th Chaos communication congress* (2008).

[20] Engel, T. Ss7: Locate. track. manipulate. In *FTP: http://events. ccc. de/congress/2014/Fahrplan/system/attachments/2553/or iginal/31c3-ss7-locate-track-manipulate. pdf* (2014).

[21] Ewert, J., Norell, L., and Yamen, S. Diameter signaling controller in next-generation signaling networks. *Ericsson Review 284* (2012), 23–31761.

[22] Forsberg, D., Horn, G., Moeller, W.-D., and Niemi, V. *LTE security*. John Wiley & Sons, 2012.

[23] Gillot, D., and Jiang, J. Y. J. Method and system for exchanging nrtrde files between a visited network and a home network in real time, Nov. 12 2013. US Patent 8,583,109.

[24] GSM Association. International roaming explained. White Paper.

[25] GSMA. Guidelines for Independent Remote Interconnect Security Testing. Official Document FS.26, GSM Association, 2017. Version 1.0.

[26] Gunawan, D., and Budiono, K. Comparative analysis on some possible partnership schemes of global ip exchange providers. *arXiv preprint arXiv:1404.2989* (2014).

[27] Hadžialić, M., Škrbić, M., Huseinović, K., Kočan, I., Mušović, J., Hebibović, A., and Kasumagić, L. An approach to analyze security of gsm network. In *2014 22nd Telecommunications Forum Telfor (TELFOR)* (Nov 2014), pp. 99–102.

[28] Hatorangan, E., and Juhana, T. Mobile phone auto registration to openbts-based cellular network in disaster situation. In *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)* (Oct 2014), pp. 1–3.

[29] Heath, B. Police secretly track cellphones to solve routine crimes. *USA Today* (2015).

[30] Holtmanns, S., Ekman, J., and McDaid, C. Mobile data interception in 4g via diameter interconnection. In *Safety and Reliability–Safe Societies in a Changing World*. CRC Press, 2018, pp. 2985–2992.

[31] Holtmanns, S., Miche, Y., and Oliver, I. Subscriber Profile Extraction and Modification via Diameter Interconnection. In *Network and System Security* (Cham, 2017), Z. Yan, R. Molva, W. Mazurczyk, and R. Kantola, Eds., Springer International Publishing, pp. 585–594.

[32] Holtmanns, S., and Oliver, I. Sms and one-time-password interception in lte networks. In *2017 IEEE International Conference on Communications (ICC)* (May 2017), pp. 1–6.

[33] Holtmanns, S., Rao, S. P., and Oliver, I. User location tracking attacks for lte networks using the interworking functionality. In *2016 IFIP Networking Conference (IFIP Networking) and Workshops* (May 2016), pp. 315–322.

[34] Jinwen, D., Chen, F., Hou, Z., Huang, S., and Shiyong, T. Method, system and device for implementing security control, Dec. 10 2009. US Patent App. 12/543,971.

[35] Kim, H., Lee, J., Lee, E., and Kim, Y. Touching the untouchables: Dynamic security analysis of the lte control plane. In *Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane* (2018), IEEE, p. 0.

[36] Kotte, B. T. *Analysis and Experimental Verification of Diameter Attacks in Long Term Evolution Networks*. Master's thesis, Aalto University, 2016.

[37] L. Morand, Ed., F. N. *Diameter Applications Design Guidelines*. IETF, 2014. RFC7423.

[38] Lee, S., and Kim, S. Hacking, surveilling and deceiving victims on smart tv. *Blackhat USA* (2013).

[39] Marques, V., Aguiar, R. L., Garcia, C., Moreno, J. I., Beaujean, C., Melin, E., and Liebsch, M. An ip-based qos architecture for 4g operator scenarios. *IEEE Wireless Communications 10*, 3 (June 2003), 54–62.

[40] Matti Keskinen, U. o. O. Mobile Network Evolution. http://www.oulu.fi/sites/default/files/content/Keskinen-5Glecture_0.pdf, 2017.

[41] Metz, C. AAA protocols: authentication, authorization, and accounting for the Internet. *IEEE Internet Computing 3*, 6 (Nov. 1999), 75–79. 00150.

[42] Meyer, U., and Wetzel, S. A man-in-the-middle attack on umts. In *Proceedings of the 3rd ACM Workshop on Wireless Security* (New York, NY, USA, 2004), WiSe '04, ACM, pp. 90–97.

[43] Moriya, T. Survey of ipx (ip exchange) as an emerging international interconnection between telecommunication networks. *IEICE transactions on Communications 96*, 4 (2013), 927–938.

[44] Norrman, K., Näslund, M., and Dubrova, E. Protecting imsi and user privacy in 5g networks. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications* (ICST, Brussels, Belgium, Belgium, 2016), MobiMedia '16, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 159–166.

[45] Otsu, T., Okajima, I., Umeda, N., and Yamao, Y. Network architecture for mobile communications systems beyond imt-2000. *IEEE Personal Communications 8*, 5 (Oct 2001), 31–37.

[46] P. Calhoun, J. Loughney, E. G. G. Z. J. A. *Diameter Base Protocol*. IETF, 2003. RFC3588.

[47] Park, Y., and Park, T. A survey of security threats on 4g networks. In *2007 IEEE Globecom Workshops* (Nov 2007), pp. 1–6.

[48] Positive Technologies. Diameter Vulnerabilities Exposure Report. https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Diameter-2018-eng.pdf.

[49] Powell, M. B. Method for preventing cellular telephone fraud, Nov. 23 1999. US Patent 5,991,617.

[50] Puzankov, S. Stealthy ss7 attacks. *Journal of ICT Standardization 5*, 1 (2017), 39–52.

[51] Rao, S. P., Holtmanns, S., Oliver, I., and Aura, T. Unblocking stolen mobile devices using ss7-map vulnerabilities: Exploiting the relationship between imei and imsi for eir access. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Aug 2015), vol. 1, pp. 1171–1176.

[52] Rao, S. P., Oliver, I., Holtmanns, S., and Aura, T. We know where you are! In *2016 8th International Conference on Cyber Conflict (CyCon)* (May 2016), pp. 277–293.

[53] Raychaudhuri, D., and Mandayam, N. B. Frontiers of Wireless and Mobile Communications. *Proceedings of the IEEE 100*, 4 (Apr. 2012), 824–840. 00182.

[54] Rouveyrol, P., Raveneau, P., and Cunche, M. Large Scale Wi-Fi tracking using a Botnet of Wireless Routers. In *SAT 2015 - Workshop on Surveillance & Technology* (Philadelphia, United States, June 2015).

[55] Rupprecht, D., Kohls, K., Holz, T., and PÃ¶pper, C. Breaking lte on layer two. In *2019 2019 IEEE Symposium on Security and Privacy (SP)* (Los Alamitos, CA, USA, may 2019), IEEE Computer Society.

[56] S. Holtmanns, I. S. 4G Who is Paying Your Cellular Phone Bill. Presented at DEF CON 26.

[57] Shaik, A., Borgaonkar, R., Park, S., and Seifert, J.-P. On the impact of rogue base stations in 4g/lte self organizing networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (New York, NY, USA, 2018), WiSec '18, ACM, pp. 75–86.

[58] Singh, I., Holtmanns, S., and Kantola, R. Roaming interface signaling security for lte networks. In *International Conference on Security for Information Technology and Communications* (2018), Springer, pp. 204–217.

[59] Stanke, M., and Sikic, M. Comparison of the radius and diameter protocols. In *ITI 2008 - 30th International Conference on Information Technology Interfaces* (June 2008), pp. 893–898.

[60] Statistics, I. *World Telecommunication/ICT Indicators Database 2018*. ITU, 2018. 22nd Edition.

[61] Stewart, R. Stream Control Transmission Protocol. Technical specification (ts), IETF, 2007. RFC4960.

[62] Tian, Y., Zhou, W., Liu, W., Wang, G., Atiquzzaman, M., Yan, Z., and Choo, K.-K. R. Security review and study of dos attack on dns

in the international roaming epc_lte network. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (Cham, 2017), Springer International Publishing, pp. 64–73.

[63] V. Fajardo, J. Arkko, J. Loughney, G. Zorn. *Diameter Base Protocol*. IETF, 2012. RFC 6733.

[64] Wang, D. An xml-based testing strategy for probing security vulnerabilities in the diameter protocol. *Bell Labs Technical Journal 12*, 3 (2007), 79–93.

[65] Wanka, J. T. Remote controlled tracking transmitter and tracking support system, June 24 1986. US Patent 4,596,988.

[66] Xenakis, C., and Ntantogian, C. An advanced persistent threat in 3g networks: Attacking the home network from roaming networks. *Computers and Security 40* (02 2014), 84–94.

[67] Yamen, S. Diameter signaling controller in next-generation signaling networks.

A LTE Emulator Elements

Element	Description
UE	This element corresponds to the User Equipment (terminal) of the LTE network defined by 3GPP specifications.
ENB	This element corresponds to the LTE base station (eNodeB) of the LTE network defined by 3GPP specifications.
HSS	This element corresponds to the Home Subscriber Server of the LTE network defined by 3GPP specifications. Optionally HSS emulator may also contain EIR-functionality.
EIR	This element corresponds to the Equipment Identity Register of the LTE network defined by 3GPP specifications. Optionally EIR-functionality may be included in HSS emulator and then separate EIR emulator is not needed.
MME	This element corresponds to the Mobility Management Entity of the LTE network defined by 3GPP specifications.
SGW	This element corresponds to the Serving Gateway of the LTE network defined by 3GPP specifications.
PGW	This element corresponds to the PDN GW of the LTE network defined by 3GPP specifications.
PCRF	This element corresponds to the Policy and Charging Rules Function of the LTE network defined by 3GPP specifications.
SGSN	This element corresponds to the Serving GPRS Support Node of the 3G network defined by 3GPP specifications. Although this element is not a part of LTE architecture this is supported as a standalone tester.
MSC	This element corresponds to the Mobile Switching Center of the 3G network defined by 3GPP specifications. As such this element is not supported but needed due to indirect parameter references.

VLR	This element corresponds to the Visitor Location Register of the 3G network defined by 3GPP specifications. Although this element is not a part of LTE architecture this is supported as a standalone tester.
AAA	This element corresponds to the Authentication, Authorization and Accounting server of the LTE network defined by 3GPP specifications.
S2GW	This element corresponds to the S2a and S2b interface Mobility Access Gateway defined by 3GPP specifications. Element contains S2 Trusted functionality.
GMLC	This element corresponds to the Gateway Mobile Location Center of the core network defined by 3GPP specifications.
ESMLC	This element corresponds to the Evolved Serving Mobile Location Center of the core network defined by 3GPP specifications.
CBC	This element corresponds to the Cell Broadcast Center of the core network defined by 3GPP specifications.
MBMSGW	This element corresponds to the Multimedia Broadcast Multicast Service Gateway of the core network defined by 3GPP specifications.
IMS	This element corresponds to the Internet Protocol (IP) Multimedia Subsystem defined by 3GPP specifications.

Table A1: Explanation for the supported emulator elements