Aalto University
School of Science
Degree Programme in Security and Mobile Computing

Bhanu Teja Kotte

Analysis and Experimental Verification of Diameter Attacks in Long Term Evolution Networks

Master's Thesis
Espoo, June 30, 2016

Supervisors:	Prof. Tuomas Aura, Aalto University
	Prof. Markus Hidell, KTH Royal Institute of Technology
Advisor:	Dr. Silke Holtmanns, Nokia Bell Labs

Aalto University
School of Science
Degree Programme in Security and Mobile Computing

ABSTRACT OF
MASTER'S THESIS

Author:	Bhanu Teja Kotte		
Title: Analysis and Experimental Verification of Diameter Attacks in Long Term Evolution Networks			
Date:	June 30, 2016	**Pages:**	69
Major:	Security and Mobile Computing	**Code:**	T-110
Supervisors:	Prof. Tuomas Aura, Aalto University Prof. Markus Hidell, KTH Royal Institute of Technology		
Advisor:	Dr. Silke Holtmanns, Nokia Bell Labs		

In cellular networks, the roaming interconnection was designed when there were only a few trusted parties and security was not a major concern or design criteria. Most of the roaming interconnections today are still based on the decades-old SS7 and the lack of security is being blamed for several vulnerabilities. Recent research indicates that the roaming interconnection has been widely misused for gaining access to the core network. Several attacks have been demonstrated by malicious attackers and other unauthorized entities such as intelligence agencies by exploiting the SS7 signaling protocol. Some operators moved to the more modern LTE (Long Term Evolution) and Diameter Signaling for high-speed data roaming and enhanced security. While LTE offers very high quality and resilience over the air security, it still requires special security capabilities and features to secure the core network against attacks targeting the roaming interconnection.

This thesis analyses and identifies attacks that exploit the roaming interconnection and Diameter signaling used in LTE networks. The attacks are analyzed in accordance with the mobile network protocol standards and signaling scenarios. The attacks are also implemented in a test LTE network of a global operator. This thesis also focuses on potential countermeasures to mitigate the identified attacks.

Keywords:	LTE, Diameter Signaling, Roaming Interconnection, Security
Language:	English

Acknowledgements

This thesis work was carried at Nokia Bell Labs, Finland under the supervision of Dr. Silke Holtmanns (Nokia Bell Labs), Dr. Tuomas Aura (Aalto University) and Dr. Markus Hidell (KTH Royal Institute of Technology) as part of the Erasmus Mundus NordSecMob program. This work was supported in part by TEKES as part of the Cyber Trust program of DIGILE (the Finnish Strategic Center for Science, Technology and Innovation in the field of ICT and digital business).

I would like to express my sincere thanks to my supervisors Dr. Tuomas and Dr. Silke, who were always available for my questions and consistently steered me in the right direction. I would like to thank Dr. Markus Hidell for his co-supervision and remote support.

I would also like to thank the experts from Vodafone Labs, UK who readily helped me with the testing and support: Mr. Michael Dugdale and Mr. Nick Edwards. The experiments could not have been successfully conducted without them.

I would also like to acknowledge my friends Shubham and Rakesh for proofreading the thesis, and I am grateful for their valuable comments.

I express my very profound gratitude to my parents and my brother for their unfailing support and continuous encouragement throughout my life. This accomplishment would not have been possible without them.

Espoo, June 30, 2016

Bhanu Teja Kotte

Abbreviations and Acronyms

2G/3G/4G/5G	2nd/3rd/4th/5th Generation (wireless telephone technology)
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
AIA	Authentication Information Answer
AIR	Authentication Information Request
APN	Access Point Name
AuC	Authentication Center
BSS	Base Station Subsystems
BTS	Base Transceiver Station
CHAP	Challenge Handshake Authentication Protocol
CLA	Cancel Location Answer
CLR	Cancel Location Request
CSG	Closed Subscriber group
DEA	Diameter Edge Agent
DoS	Denial of Service
DRA	Diameter Routing Agent
DSA	Delete Subscriber Data Request
DSR	Delete Subscriber Data Answer
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EAP	Extensible Authentication Protocol
EAP-GSM	Extensible Authentication Protocol for Global System for Mobile Communications
EAP-SIM	Extensible Authentication Protocol for Subscriber Identity Modules
EIR	Equipment Identity Register
eNB	evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
GPRS	General Packet Radio Service

GRX	GPRS Roaming Exchange
GSM	Global System for Mobile communication
GT	Global Title
GTP-C	GPRS Tunnelling Protocol for Control plane
GTT	Global Title Translation
H-PCRF	Home PCRF
HeNodeB	Home evolved Node B
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IDA	Insert Subscriber Data Answer
IDR	Insert Subscriber Data Request
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPX	IP Packet Exchange
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LTE	Long Term Evolution
MAC	Media Access Control
MAP	Message Application Part
MAP PRN	MAP Provide Roaming Number
MAP SRI	MAP Send Routing Information
MCC	Mobile Country Code
MiTM	Man in The Middle
MME	Mobility Management Entity
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number
MSRN	Mobile Station Roaming Number
MTP	Message Transfer Part
NAI	Network Access Identifier
NDC	National Destination Code
NDS	Network Domain Security
NOA	Notification Answer
NOR	Notification Request
NSS	Network Switching Subsystem
OSI	Open Systems Interconnection
P-GW	Packet data network Gateway
PAP	Password Authentication Protocol

PCEF	Policy Control Enforcement Function
PCRF	Policy Control and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Protocol Data Packet
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
PUA	Purge Answer
PUR	Purge Request
QoS	Quality of Service
RAN	Radio Access Network
RLC	Radio Link Control
RRC	Radio Resource Control
RSA	Reset Request
RSR	Reset Answer
S-GW	Serving Gateway
SAE	System Architecture Evolution
SCCP	Signaling Connection Control Part
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Center
SRR	Send Routing Info for SM Request
SRVLOC	Service Location Protocol
SS7	Signaling System No. 7
SSN	Sub System Numbers
TCAP	Transaction Capabilities Application Part
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
ULA	Update Location Answer
ULR	Update Location Request
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
V-PCRF	Visited PCRF
VLR	Visitor Location Register
VPLMN	Visited Public Land Mobile Network

Contents

Chapter 1

Introduction

Over the last two decades, mobile network coverage grew significantly and has become an important part of today's communication infrastructure. The extent of the populace covered by a cellular network grew from 58% in 2001 to 95% in 2015 [1]. The near-ubiquitous network coverage coupled with affordable mobile devices and smart phones has led to the vast increase in the number of mobile users. By the end of 2015, there were more than 7 billion mobile cellular subscriptions [1]. The number of 4G subscriptions was nearly one billion and predicted to reach 3.1 billion by 2019 [2]. Considering all these facts, it is not surprising that mobile networks have become more attractive targets also for the darker sides of life.

The security of cellular networks has evolved considerably over the last three decades. Due to the emerging threats and various limitations found in the analog systems, some security functions where introduced in the Global System for Mobile communication (GSM) systems during its standardization three decades ago. Firstly, eavesdropping on conversations by using simple radio receivers in the earlier systems led to the specification of encryption on the radio interface. Secondly, tamper-resistant SIM cards were introduced to address the risk of fraud attacks on billing. This provided strong subscriber authentication and robust charging. Finally, to address the issues of subscriber privacy, randomized temporary identities were introduced to make it difficult to track subscribers. Many vulnerabilities in GSM security have been discovered in the last decade. Even then the GSM security goals were met because it was past the economic lifetime for which GSM was initially designed. To overcome these challenges in 3G systems, further security improvements were made. The most important ones are mutual authentication to identify false base stations, stronger encryption algorithms and moving the encryption deeper into the network. When the 4G Long Term Evolution (LTE) standard was set, the user data encryption is moved back to the base station and enhanced key management was introduced to prevent physical tampering of base stations. Overall, the LTE air interface security is very similar to that of the 3G networks. This paragraph has been adapted from [3].

Contemplating on the thinking behind 2G to 4G security, it can be said that security measures were instigated to protect voice and packet data services to safeguard the charging mechanism and also to protect the subscriber's privacy [3]. Besides protecting subscriber privacy and the confidentiality and integrity of their communication, the protection of the network itself against any form of attack is of paramount importance. In the past years, many open-source implementations of radio base-band stacks have become available which resulted in a number of "proof of concept" attacks exploiting vulnerabilities in the implementation or configuration of mobile network nodes. In spite of the strong security measures, 3G and 4G systems are still prone to attacks because of the practicality of implementing these measures, misconfiguration of network elements and negligence of some telecom operators.

As per the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), "interconnect" is defined as
"The commercial and technical arrangements under which service providers connect their equipment, networks and services to enable customers to have access to the customers, services and networks of other service providers." [4].

Interconnects are highly important in telecommunication networks as they help the network operators to provide services consistently to their subscribers, even in the regions where the operators do not operate. Three decades ago when Signaling System No. 7 (SS7) protocol was designed, there were only a few state owned operators and the interconnection network was a private network built upon trust. Today the situation has completely changed due to the market liberalization and there are more operators than they could have ever anticipated when SS7 was standardized. The confluence of decades old SS7 with the IP-based LTE networks has given rise to a need for additional security enforcement. While the air interface security got quite some attention and substantial improvement to keep abreast with the latest attack vectors, the interconnection security has not received the same amount of improvement or attention.

Research problem: The goal of this thesis is to thoroughly analyze the signaling on LTE roaming interconnection and to identify various threats. We aim to achieve the following:

1. Identify the existing and possibly new attacks on the LTE roaming interconnection.
2. Provide proof-of-concept for the discovered attacks.
3. Analyze the attacks and suggest potential countermeasures.

Research methods: We first theoretically analyze the signaling protocol on a roaming interface to find loopholes and then attempt to discover possible ways to cause privacy breach, fraud and service denial. Subsequently, the attacks will be verified in a test network of an operator that reflects the realistic key features of a LTE network to prove that they actually work. Finally, the network data packets are captured and analyzed.

Impact and sustainable development: As only about 50% of the commercial network operators have deployed LTE, identifying and evaluating threats in LTE networks can foster its adoption and ensure the security of the future LTE deployments. LTE networks have two main advantages, first, it will increase the efficiency of the entire network thereby resulting in substantial energy savings. Second, it will make network operations easier to manage and results in cost savings.

Our research brings in ethical impacts to the society since it identifies the various security threats leading to service denial, privacy invasion and fraud, that may be exploited by criminals and foreign governments. We hope that through this research, the communities and the network operators can see the importance of these threats and spend a considerable amount of time and incorporate countermeasures to mitigate them.

1.1 Structure of the Thesis

The rest of this thesis is structured as follows. Chapter 2 presents an overview of LTE networks. Chapter 3 provides a brief survey about the existing research in 4G security. Chapter 4 presents an overview of the interconnection network, signaling protocols and their vulnerabilities. Chapter 5 discusses the threat model and attacks on the 2G and 3G signaling and the newly identified attacks in LTE signaling. Chapter 6 presents the results of the experiments conducted to verify the attacks. Chapter 7 presents the potential countermeasures and mitigation strategies. Finally, chapter 8 concludes the thesis.

Chapter 2

Long Term Evolution (LTE) Networks

Mobile networks are gradually transforming into data networks and shifting towards an open and flat architecture which is inherently more vulnerable to security threats. This transition is being driven by the increase of smartphones and moving to Internet Protocol (IP) [5] based architecture in 4G LTE networks. So, LTE networks have a possibility of inheriting vulnerabilities that exist in other IP networks, such as the Internet. Furthermore, the exponential growth in traffic makes it more difficult for operators to protect their networks [6].

The 4G networks are an evolution of the third generation Universal Mobile Telecommunications System (UMTS). The evolution of the radio access through Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) is termed the Long Term Evolution (LTE). The evolution of the non-radio aspects is termed System Architecture Evolution (SAE), which includes the Evolved Packet Core (EPC) network. LTE and SAE together are called the Evolved Packet System (EPS). Unlike the earlier generation cellular systems which provide circuit-switched services, the EPS has been designed to support primarily packet-switched services. EPC, EPS and SAE are Third Generation Partnership Project (3GPP) standard terms for the 4G cellular technologies but the marketing branches of telecom operators and manufacturers decided to label the whole 4G technology as LTE and market it under that name. Hereafter in the thesis, the term LTE refers to EPS. The structure of this chapter is adapted from [7].

2.1 Network Architecture

From a high level point of view, LTE has three main components: the user equipment (UE), the E-UTRAN and the EPC. The communication with other IP networks, such as the IP multimedia subsystem (IMS), and the Internet is carried out through the EPC. The high level architecture of LTE is shown in Figure 2.1. The following sections will give a brief overview of the main components and their interfaces.

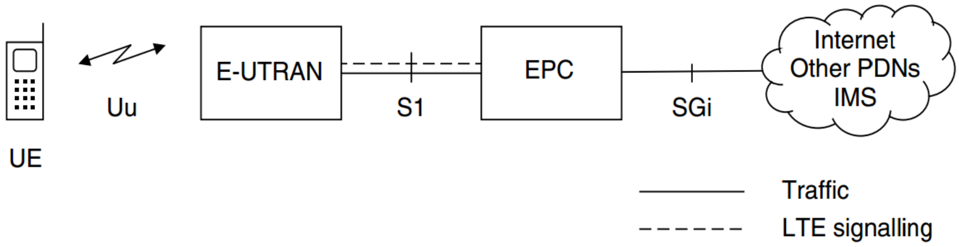


Figure 2.1: High Level Architecture of LTE [7]

2.1.1 User Equipment

The UE is a mobile device or a smartphone with an integrated Universal Integrated Circuit Card (UICC). The UE has two main functions. Firstly, it handles all the communication between the E-UTRAN and the mobile device. Secondly, it terminates the data streams received from the E-UTRAN. The UICC is a smart card that replaces the 2G Subscriber Identity Module (SIM) card. Universal Subscriber Identity Module (USIM) [8] is an application that runs on the UICC, which stores the user's network access credentials and home network identity. Certain operators provide device management servers from which the USIM can download the required data. The primary use of USIM is to carry out security related operations such as authentication and key exchange between the subscriber and the network.

The radio interface between the radio access network and the UE is the Uu interface. It includes the user and control planes and allows data transfer between the eNodeB and the UE. The Radio Resource Control (RRC) signaling is part of the control plane whereas the Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and Media Access Control (MAC) layers are part of the user plane protocols [9].

2.1.2 Evolved UMTS Terrestrial Radio Access Network

The architecture of E-UTRAN is shown in the Figure 2.2. The E-UTRAN has just one component called the evolved Node B (eNodeB). The radio communications between the EPC and the UE are handled by the E-UTRAN. In wireless telephony, a cell is the geographical area covered by a cellular transmission facility. Each eNodeB is a base transmitter station (or simply called a base station) which controls the mobile devices in a single cell or multiple cells. The eNodeB sends and receives radio transmissions from its mobile devices using the analogue and digital signal processing functions of the LTE air interface. The eNodeB also sends signaling messages, such as handover commands that relate to those radio transmissions [7].

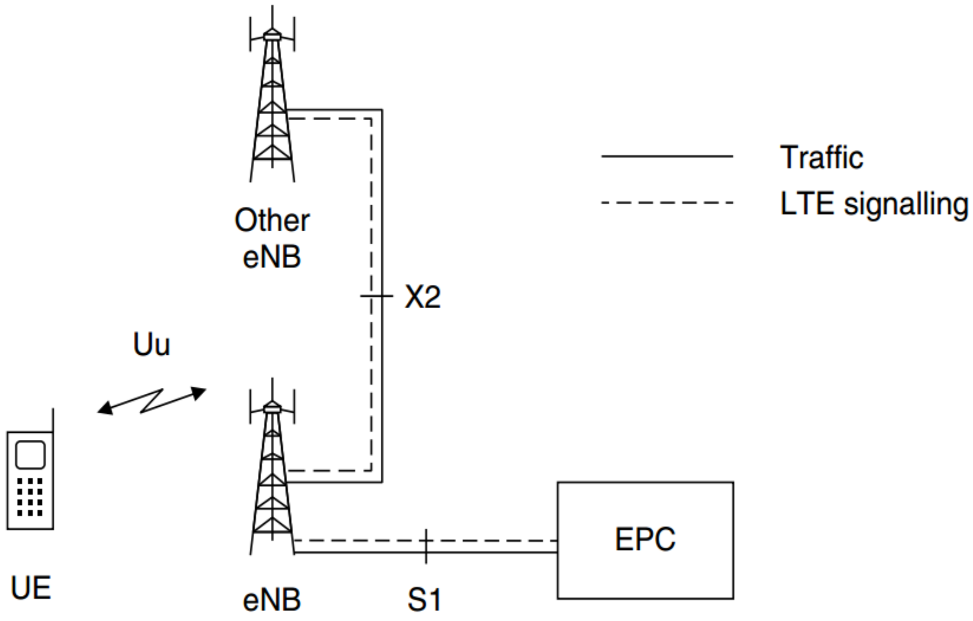


Figure 2.2: Architecture of E-UTRAN [7]

The S1 [10] interface connects the eNodeBs to the EPC. An eNodeB is connected to a nearby eNodeB by the X2 [11] interface. The X2 user plane provides forwarding of buffered packet data when the UE moves between different eNodeBs. The X2 control plane provides various functions and procedures between eNodeBs that are related to handover and management of load-balancing [9]. The X2 and S1 interfaces are just logical connections and the data is routed through an underlying IP transport system.

Operators increase the capacity of their networks through smaller base stations called Home eNodeB (HeNodeB) [12], which provide femtocell coverage within the subscriber's home. HeNodeBs provide better coverage and higher data rates compared to eNodeBs. The S1 communications for a HeNodeB are secured more carefully than normal as the HeNodeB connects to the EPC through the subscriber's ISP.

2.1.3 Evolved Packet Core

The core network is called EPC. The architecture of the EPC is shown in Figure 2.3. It is responsible for the overall control of the UE and establishment of the bearers [13]. The main components of EPC are described below:

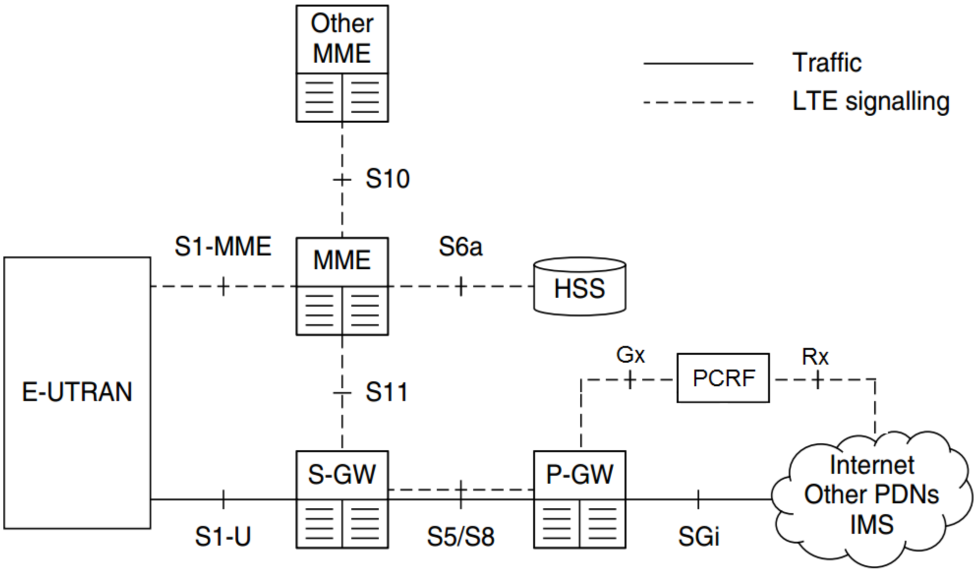


Figure 2.3: Architecture of EPC (Non-Roaming Scenario) [7]

1. Mobility Management Entity (MME) controls the high-level operations of the control plane such as subscriber and session management. The MME sends signaling messages to a mobile device about issues such as security, terminal-to-network session handling and location management. Each mobile device is associated with a single MME which may change with the mobility of the user. The associated MME is called its serving MME.

2. Home Subscriber Server (HSS) is the heart of the EPC. It is a central database that stores information about all the subscribers of the network. It holds subscription data which includes user identification and addressing, access restrictions, Quality of Service (QoS) profile, default PDN configuration and the identity of the serving MME. The HSS is generally integrated with the Authentication Center (AUC), which generates the security keys and authentication vectors.

3. Packet data network Gateway (P-GW) is the point of interconnect between the EPC and the external IP networks. The P-GW routes packets to and from the PDNs. The P-GW also performs various functions such as IP address and IP prefix allocation, policy control and charging [14].

4. Serving Gateway (S-GW) transports the IP data traffic between the UE and the external networks. It is the point of interconnect between the radio-side and the EPC and serves the UE by routing the incoming and outgoing IP packets. It is logically connected to the P-GW [14].

5. The Policy Control and Charging Rules Function (PCRF) is primarily responsible for policy making and control decisions. It also supports QoS authorization (QoS class identifier and bit rates), flow-based charging and service data flow detection [15].

LTE has many interfaces and reference points. The detailed information about the interfaces is beyond the scope of this thesis. Some of the interfaces in EPC are briefly discussed below:

1. The S1 interface is defined between the E-UTRAN to the EPC. The S1-MME interface connects the eNodeB and MME. It is responsible for reliable and guaranteed delivery of user data between the eNodeB and the MME. The S1-U connects the eNodeB and MME. It provides non-guaranteed data delivery of LTE user plane Protocol Data Units (PDUs) between the eNodeB and the S-GW [9].

2. The S5 and S8 interfaces [16] provide user plane tunneling and tunnel management between S-GW and P-GW. S8 is the inter PLMN variant of S5.

3. The S6a interface is an Authentication-Authorization-Accounting (AAA) interface that lies between the HSS and MME. This interface is discussed in detail in section 4.2.4.

4. The S11 interface [17] sits between the S-GW and MME. It is based on GPRS Tunnelling Protocol for Control plane (GTP-C) with additional functions for mobility and paging coordination [18].

5. The SGi interface [19] is the gateway between the EPC network and the connected PDN. This interface specifies the end of the EPC network as the connected PDN generally belongs to a different network operator [20].

6. The Gx interface [21] lies between the PCRF and the Policy Control Enforcement Function (PCEF). It enables the PCRF to have dynamic control over the policy and charging control behavior at the PCEF.

7. The Rx interface [22] lies between the operator-provided service and PCRF. This interface provides the transport of application-level session information [23].

2.2 Roaming Architecture of LTE

Roaming allows a subscriber to move outside their home network operator's coverage area and access the services through another operator's network. For a roaming subscriber, the HSS will always be in the home network whereas the UE, E-UTRAN, MME and S-GW are always in the visited network. IP Exchange (IPX) and GPRS Roaming Exchange (GRX) are the two GSMA standard interconnection models used for roaming [24]. Depending on the location of the PDN gateway, the roaming architecture is categorized into either home routing or local breakout.

2.2.1 Home Routing

The home routing architecture is shown in Figure 2.4. In this architecture, the PDN gateway lies in the home PLMN of the subscriber. By using home routing, all the traffic from the visited PLMN is routed to the subscriber's home PLMN and the home network operator can charge for it directly. Communications with the the Internet generally use home routing.

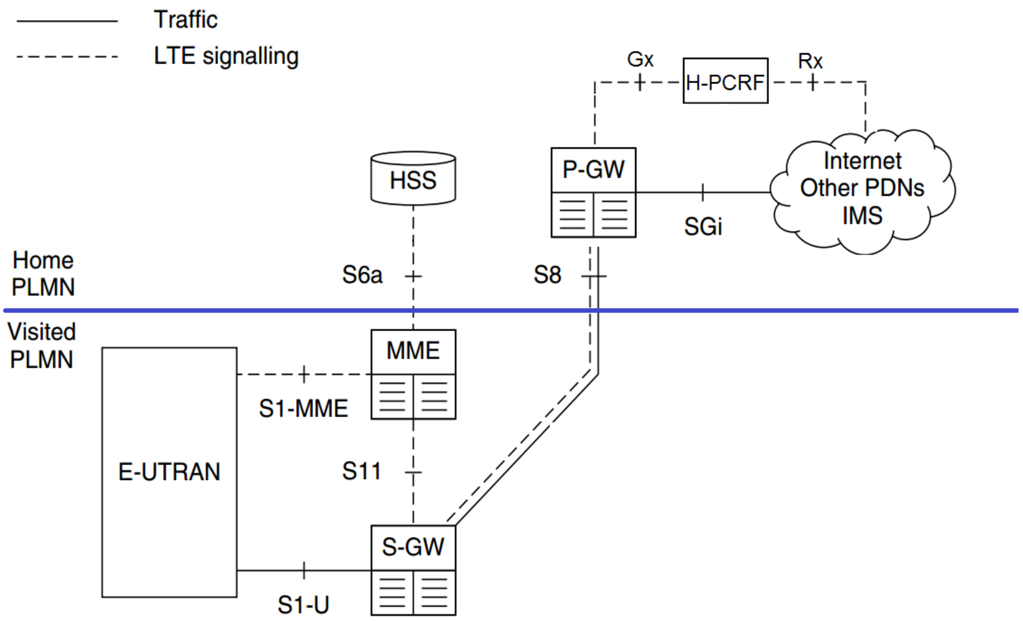


Figure 2.4: Roaming Architecture with Home Routing [7]

2.2.2 Local Breakout

The local breakout architecture is shown in Figure 2.5. In this architecture, the PDN gateway lies in the visited PLMN. The Visited PCRF (V-PCRF) and the Home PCRF (H-PCRF) are connected through the S9 interface. The S9 interface provides transfer of charging control information and QoS policies between the H-PCRF and the V-PCRF [25].

This architecture has two important benefits for voice communications. Firstly, a user can make a local call or send a message without the traffic getting routed back to the home network. Secondly, the local emergency services can handle the emergency calls. Communications with the IP multimedia subsystem generally use local breakout [7].

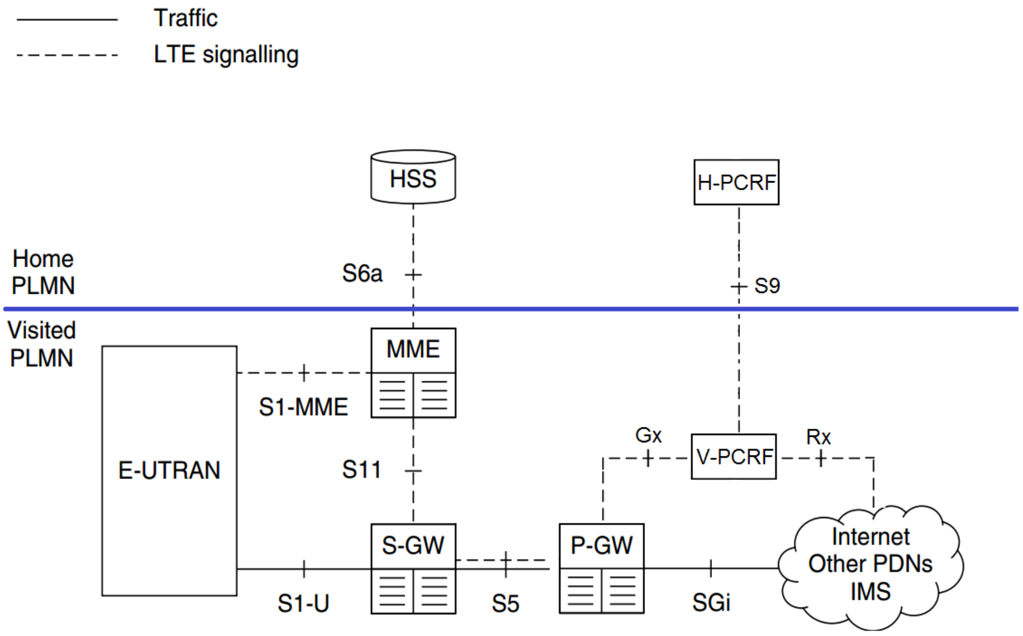


Figure 2.5: Roaming Architecture with Local Breakout [7]

Chapter 3

Related Research

After the standardization of 4G networks, many research results on 4G security have been published. In this chapter we give a brief overview of the research related to security of LTE and 4G networks.

The research in [26] gave a generic overview of security threats in 4G networks and also proposed a tool to analyze the security vulnerabilities of 4G networks. It presented various vulnerabilities in WiFi and WiMAX technologies, which could be inherited by 4G networks. Furthermore, it also indicated that 4G systems might inherit most of the IP-specific security vulnerabilities and threats because of their IP based architecture. In [27] the security architecture of LTE has been analysed with respect to Medium Access Control (MAC) layer security issues. This study discussed about various threats in LTE networks by exploiting the vulnerabilities in MAC layer. Some of these threats include denial of service attacks, replay attacks, eavesdropping attacks and data integrity attacks. The research in [28] dealt with the security of 4G networks with respect to application layer. It also dealt with the security issues of IPv6 wireless networks in 4G systems. Additionally, it also proposed some countermeasures and strategies to defend against the identified security issues.

The research in [29] dealt with network access security in 4G systems. It analysed EPS architecture and discussed EPS security threats and requirements. The research in [30] analyzed the privacy and security threats on the LTE radio interface and identified several new threats which include active attack and location tracking attack. The research in [31] investigated the security of 3GPP Authentication and Key Exchange (AKA) protocol and identified certain threats, such as false base station attack, redirection attack and impersonation attack. Furthermore, it proposed an enhancement to the AKA protocol to mitigate these threats. The research in [32] dealt with security issues in 3GPP roaming architecture, such as man-in-the-middle

(MiTM) attacks and practical problems with the security algorithms used in AKA protocol. Additionally, it also proposed solutions to these issues with two different architectures. The research in [33] dealt with the relationship between performance and security in the 4G signaling plane. It also analysed the performance overhead caused due to the security in signaling plane.

As evident from the above information, most research in the field of 4G security is focused on air interface security and security architecture whereas the research on interconnection security and signaling protocols is minimal. In this thesis, we concentrate on interconnection security and aim to go one step forward towards a sound telecom security architecture.

Chapter 4

Roaming Interconnection and Signaling

As per the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), "signaling" is defined as
"The exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls, and network management, in automatic telecommunications operations" [34].

SS7 is the most widely used signaling protocol on the interconnection network in both 2G and 3G cellular systems. It is gradually being replaced by Diameter protocol [35] in the 4G systems. This chapter briefly discusses the roaming interconnection and its signaling protocols.

4.1 SS7 Signaling

Signaling System No. 7 (SS7) is a ITU-T standard signaling protocol for exchanging information between different telecom network nodes over a digital signaling network. It is used in mobile networks and fixed-line networks for establishment and tearing down of calls, routing, information exchange and billing. The following sections briefly discuss the 2G core network architecture for better understanding of the SS7 interconnection.

4.1.1 2G Core Network Architecture

The 2G core network architecture is shown in Figure 4.1. The Home Public Land Mobile Network (HPLMN) is the network to which the mobile user is subscribed. All the other networks to which a mobile user can connect are called Visited Public Land Mobile Networks (VPLMNs). During roaming the VPLMN will fetch the subscriber data (such as subscription information, profile, service restrictions) from the HPLMN. The core network entities are briefly discussed below:

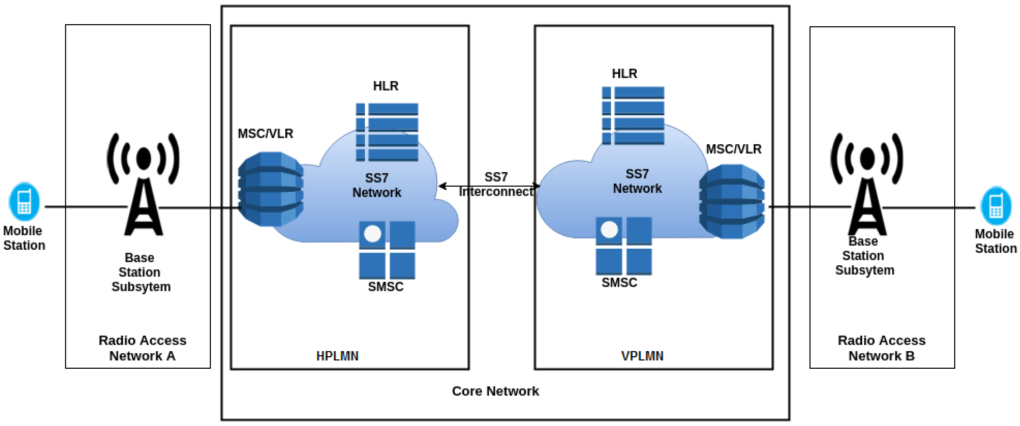


Figure 4.1: 2G Core Network Architecture [36]

1. Mobile Station (MS) is the mobile device with a 2G SIM card. It has the same functionality as the UE in LTE.

2. Base Transceiver Station (BTS) is a radio equipment that facilitates radio communication between the MS and a network. BTS is the predecessor of eNodeB.

3. Home Location Register (HLR) is a centralized database that stores information about all the subscribers of the network [37]. HLR is the predecessor of HSS.

4. Visitor Location Register (VLR) is a server that ensures mobility management and call-handling functions of the subscriber, who is roaming in the VLR's network. VLR obtains the subscription information from the subscriber's HLR and maintains a temporary record while the subscriber is roaming.

5. Mobile Switching Center (MSC) controls the Network Switching Subsystem (NSS) and performs various operations, such as communication switching (call setup, routing and tear down), interface management and billing. The VLR functionality is often combined with the MSC. The Gateway Mobile Switching Centre (GMSC) is an edge MSC that is used to route calls to and from the other mobile networks. MME in LTE is the successor of the combined MSC/VLR.

6. Short Message Service Center (SMSC) handles Short Message Service (SMS) operations such as routing, forwarding, storing and delivering messages [38].

4.1.2 SS7 Protocol Stack

SS7 has different possible protocol stack combinations based on the types of services that are being offered. A traditional SS7 protocol stack includes Message Transfer Parts (MTP 1, 2, and 3), Signaling Connection Control Part (SCCP), Transaction Capabilities Application Part (TCAP), Telephony User Part (TUP), ISDN User Part (ISUP) and Message Application Part (MAP). These protocols are categorized into functional abstractions called levels based on their functionality. SS7 uses a four level protocol stack with reference to the Open System Interconnection (OSI) seven layer model [39]. A comparison between SS7 protocol stack and the OSI layered model in shown in Figure 4.2.

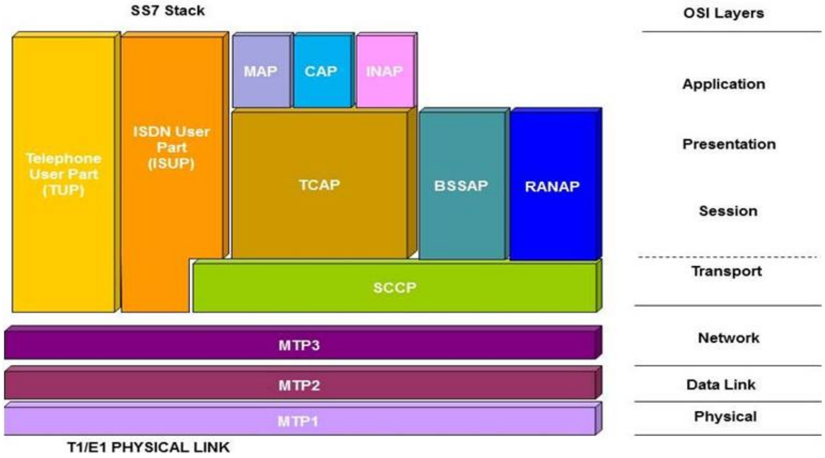


Figure 4.2: SS7 Protocol Stack vs OSI Layered Model [40]

MAP protocol is one of the most important protocols in the SS7 stack. It provides an application layer for various network nodes in 2G and 3G networks. It also allows communication between the nodes of NSS and enables them to provides various services, such as subscriber authentication, location management, subscription management, and fault recovery. In the latest 3GPP specifications, MAP supports about 81 different services [41]. These services are categorized into mobility services, location management services, operation and maintenance, supplementary services, and Protocol

Data Packet (PDP) context services [42]. MTP, SCCP, and TCAP are used to encapsulate and transport MAP.

4.2 Diameter Signaling in LTE

Diameter protocol defined in RFC 3588 [35] is the next generation Authentication-Authorization-Accounting (AAA) protocol. It is an application layer peer-to-peer (P2P) protocol that evolved from the RADIUS [43] protocol. Diameter runs on top of TCP/IP and also supports SCTP [44], which is a widely used transport protocol in telecom networks. Diameter is a message based request-answer protocol. The data units in a Diameter message are called Attribute Value Pairs (AVPs). A comprehensive tutorial about Diameter base protocol can be found in [45].

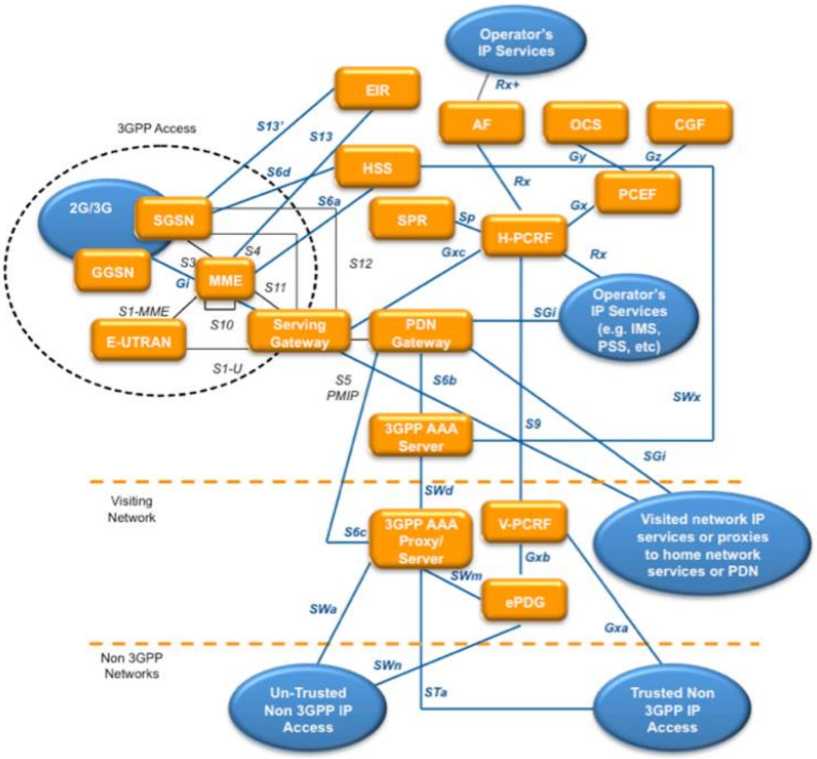


Figure 4.3: Diameter Interfaces in LTE [23]

Mobile networks require secure and efficient provision of AAA services, so Diameter was chosen by 3GPP for signaling and AAA provisioning in 4G and all next generation mobile networks. Figure 4.3 shows the Diameter based interfaces in a LTE network.

4.2.1 Diameter Signaling Stack

The comparison between Diameter and SS7 signaling stacks is illustrated in Figure 4.4. The network and transport layer protocols of SS7 such as MTP2 and MTP3 are replaced by SCTP/IP in Diameter. The session, presentation and application layer protocols such as SCCP, TCAP and MAP are replaced with Diameter protocol.

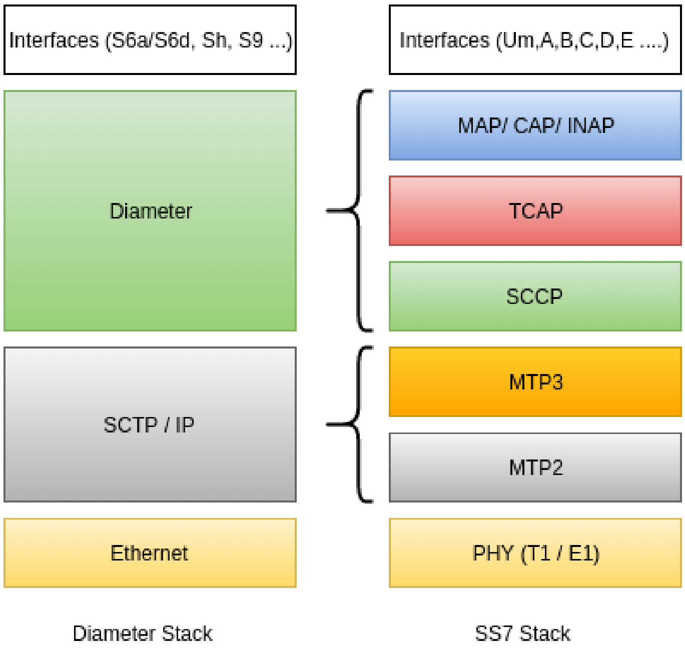


Figure 4.4: Diameter vs SS7 stack

4.2.2 Security Considerations in Diameter

Due to the increased security concerns in the communication protocols built on top of IP networks, Diameter has been designed to provide several security features. In spite of the security features being provided by Diameter, the actual security offered will completely rely on factors such as complete and correct implementation of Diameter. 3GPP standards assume that nodes on either sides of the interconnection can be trusted as these nodes reside within the domain of trusted operator network, or the communication between the nodes beyond interconnection is secured individually as per Network Domain Security NDS/IP Security [46] using TLS or IPsec by the operators. In practice this proves to be a business challenge as the operators often do not connect their nodes directly with their partners over interconnection, instead they utilize roaming hubs in order to provide their customers with a large base of roaming partners. The implementation of security features over the roaming hubs raises reliability concerns as the communication between Diameter nodes connected by the roaming hubs may not be using NDS/IP Security.

Inbuilt Global Title Translation (GTT): One of the main reasons for the attacks that abuse the SS7 interconnection is the exposure of critical nodes of the core network nodes to the partner or attackers from outside the home network. In this realm, the Global Title Translation functionality provides protection to the core network nodes by reducing the need for explicitly disclosing the GTs of the nodes of entire network in the routing tables of a communication message. GTT hides the topology of critical infrastructure, such as HSS and EIR, by provisioning internal routing tables within the nodes rather than the communication message. The concept of GTT is implemented by default in Diameter suite, particularly in HSS. Along with mutual node authentication, GTT protects the core network against port scanning and impersonation attacks. On the other hand, operators tend to use and assign ranges of global titles to their nodes. Therefore, an attacker who has knowledge of one valid global title e.g. SMSC can start from there a brute force probing attack to discover other core network nodes.

Dynamic peer discovery: Diameter is capable of dynamic peer discovery methods using which a Diameter client can discover the next hop node to forward Diameter messages. In a nutshell, a Diameter node broadcasts the application and security level that they support, so that the neighboring nodes can dynamically discover the appropriate peers using either SRVLOC (Service Location Protocol) [47] or DNS Service Protocol [48]. Upon discovering a new peer, the relevant information about the peer location (realm name and IP address) and routing configurations along with the application and service that the peers support will be stored in peer tables and peer routing tables respectively. In terms of local storage of application specific routing information, the dynamic peer discovery feature adds another level of security as an attacker cannot learn the routing paths or IP addresses of critical nodes. Dynamic peer discovery makes the configuration of networks much easier since the sender does not need to be aware of the internal IP addresses. However, an attacker can easily misuse such automatic mechanism to exploit the vulnerabilities without detailed knowledge of the network topology.

Inbuilt security: Contrary to SS7 which offers no inbuilt security to the communication between the core network nodes, Diameter provides cryptographic protection in several ways [35]. It offers session-based (end-to-end) and connection-based (hop to-hop) security through IP Security (IPsec) and Transport Layer Security (TLS) [49]. Diameter protocols suggests using TLS between diameter nodes. Additionally, it also supports other authentication protocols, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Network Access Identifier (NAI) and Extensible Authentication Protocol (EAP) to enhance the security of authentication procedures.

4.2.3 Shortcomings of Diameter Security

With the strong support for AAA and other security considerations as we discussed above, Diameter appears to provide more security to the core network nodes and enhance the end-user privacy compared to SS7. Due to this, there is the perception that "Diameter provides security by default". However, in reality several business and interoperability factors decides the actual implementation and hence the level of security in LTE networks. In addition to the generic security issues discussed in [27] (which are related to air interface vulnerabilities), we will now discuss some of the shortcomings which enable an attacker to impersonate network nodes.

Gap between standardization and implementation: The 3GPP standard for Diameter base protocol [35] strongly recommends the use of IPsec for intra-operator communication and TLS for inter-operator communication. Even though the IPsec and TLS have been standardized in Diameter based communication, using them is not obligatory. Furthermore, the nodes in a Diameter based network may have no means to verify the use of IPsec and TLS [50] while communicating with their peers because there is no standard procedure for it. In practice, it can be seen that many operators do not secure their home LTE network to reduce the overhead of implementing the non-mandatory functionality and this definitely shows their ignorance to recognize the threats from the interconnection. It should be noted that while we focus mostly on the attacks coming over the interconnection interface, the same attacks can also be launched from a compromised core network node directly. Sometime the core network nodes (that run telnet or ftp protocol) are visible on the Internet, and the attackers may try to compromise them to further launch their attacks.

Reachability is decided by the applications: As Diameter is an application layer protocol, the communication messages (data packets) that a

Diameter node sends are dependent on the application rather than on the network configuration. An attacker can impersonate at the application layer and penetrate deeper into the network as the application decides the reachability [50]. The application driven penetration capabilities make Diameter vulnerable to spoofing or impersonation attacks, particularly if an attacker succeeds to intercept the interconnection traffic.

Imposed overhead due to encryption: Diameter relies on the use of Public Key Infrastructure (PKI) and X.509 certificates for authentication. The management issues with PKI, such as the key distribution, certificate management and revocation continue to create the administration overhead for mobile networks. Additionally, the piggybacking of acknowledgement messages in the transport layer (via TCP or SCTP) induces more encrypted traffic in the upper layers, which requires more bandwidth. As the interconnection network is a global network, the financial overhead of certificate distribution, maintenance of certificate revocation lists, and management of the central PKI system poses serious problems. For the same reasons, operators with less capital to spend often fail to safeguard their nodes with PKI.

Problems due to fail-over algorithms: The Diameter base protocol [35] has provisions for various fail-over [51] and error-handling algorithms to provide descriptive feedback in case of system or network failures. These algorithms are initiated by the client when it has not received any answers for a certain amount of time [52]. An attacker can impersonate a Diameter client to flood the peers by sending bogus traffic of the fail-over algorithms. Even though the receiving peers can recognize the traffic as bogus or faulty (if the peer filters them), the fail-over algorithms attempt to process the traffic to provide useful feedback, which eventually results in a denial of service (DoS) attack. Therefore, we can argue that the Diameter protocol is vulnerable to DoS attacks.

Support for legacy systems at the interconnection: The upgradation from 2G and 3G networks to LTE is a slow and gradual process. Due to this, the current interconnection network contains nodes that support either SS7 or Diameter or both, making it an inhomogeneous setup. This inhomogeneous setup enables an attacker to pose as a roaming partner with SS7 network and and downgrade the LTE network to use less secure legacy communication messages. For interoperability with other operators, the network edge nodes often support translation between Diameter and SS7 protocols, which is done using Interworking Functions (IWF) [53] [54]. Additionally, the IWF provides an easy means of porting the SS7-based attacks to Diameter-based LTE networks. The attacks exploiting lack of security measures in the interconnection due to interoperability can be found in detail in [36].

4.2.4 Diameter S6a Interface

The S6a interface lies between the HSS and the MME. This is one of the most important interfaces because the signaling messages related to authentication and authorization are communicated over the S6a interface. This interface is used for subscriber authentication, subscription updates, location updates from MME etc. Unlike some local interfaces such as Sh, the S6a interface cannot be disabled. It must always be open to roaming partners and hubs. The following are the Diameter messages that are sent on the S6a interface:

1. Authentication-Information-Request/Answer(AIR/AIA) — MME fetches authentication data from HSS to authenticate the subscriber.

2. Update-Location-Request/Answer (ULR/ULA) — MME stores its own identity at HSS and fetches subscription data from HSS.

3. Notification-Request/Answer (NOR/NOA) — MME stores PDN address and other attachment information at HSS.

4. Purge Request/Answer (PUR/PUA) — MME informs the HSS that UE has been inactive for a long period and, thus, MME has deleted from its end the subscription data received in the most recent ULR/ULA.

5. Insert-Subscriber-Data-Request/Answer (IDR/IDA) — Invoked by HSS when the subscriber is attached and there is an update in the subscriber profile at the HSS end so that the changes are reflected in subscriber profile at the MME.

6. Delete-Subscriber-Data-Request/Answer (DSR/DSA) — Invoked by HSS when the subscriber is attached and some data is deleted in the subscriber profile at the HSS end so that the changes are reflected in the subscriber profile at the MME.

7. Cancel-Location-Request/Answer (CLR/CLA) — Invoked by HSS to detach the subscriber.

8. Reset-Request/Answer (RSR/RSA) — Invoked by HSS to inform the MME about HSS failure or planned HSS outage. The MME should subsequently sync the data and send fresh location/PDN information to the HSS.

Chapter 5

Attacks on Roaming Interconnection

This chapter discusses the vulnerabilities in the global interconnection network and the attacks on the interconnection network. Some SS7 attacks from the literature are briefly discussed in the initial section. Inspired by them, in the later sections we then propose seven potential attacks that target Diameter signaling on the interconnection.

5.1 Interconnection Vulnerabilities

The roaming interconnection is often considered one of the weak points in a telecommunication network, as the access is opened to many other telecom operators and ISPs. There are multiple ways in which an attacker can gain easy access to the roaming interconnection network. Some of the potential methods are mentioned below

- The GSM IR.21 database is a confidential database with all information related to International Roaming between various telecom providers. It contains the hostnames and IP addresses of various core network elements such as the HSS, MME and the DEA. The database is accessible only to the members of the GSM association but many operators made them available on the Internet. For e.g. Claro Americas, which serves clients in most South American countries, has their IR.21 database information accessible on the Internet along with sensitive information such as login credentials [55]. Even Vivo telecom, the largest telecommunications company in Brazil has the IR.21 database accessible on the Internet [56]. The incident has been reported to both Claro Americas and Vivo telecom.

- The roaming interconnection is global and spreads across countries and regions where exploiting subscriber data is legal or privacy regulation is not strictly enforced.

- Most operators lease out infrastructure and SS7 access to third parties and various service providers. In fact, the European Union requires operators to provide such access in order to encourage competition in the mobile services market. The legal framework and the monitoring of the actual behavior of the third party varies widely.

- Governments may mandate access or even take control of a network operator in order to have unrestricted entry to the network.

- Misconfigured network nodes that are visible over the Internet (e.g. through www.shodan.io), could be compromised and act as an entry point for hackers.

- Insider attacks such as social engineering and bribing.

5.2 Important Identifiers

International Mobile Subscriber Identity (IMSI) is a globally unique identifier for a cellular subscriber and are stored in the HSS. The IMSI can be upto 15 digits long. It contains a 3-digit Mobile Country Code (MCC), a 2-digit Mobile Network Code (MNC) and upto 10 digits Mobile Station Identification Number (MSIN). The MCC and MNC together uniquely identify the country and home operator of the subscriber. The MSIN is used within the scope of the home operator [57]. To protect subscriber privacy, frequent use of the IMSI is reduced by temporary identifiers called Temporary Mobile Subscriber Identity (TMSI). TMSIs are locally significant to the network to which a subscriber is connected and therefore stored only in the VLR.

Mobile Station International Subscriber Directory Number (MSISDN) is the phone number (i.e. the number normally dialed to make a voice call) assigned to a cellular subscriber. It contains a 3-digit Country Code (CC), 2-3 digits National Destination Code (NDC) and a 10 digit Subscriber Number (SN). When a subscriber is roaming in a different network, the Mobile Station Roaming Number (MSRN) is used instead of MSISDN. The MSRN has the same format as that of MSISDN but all the codes refer to the visited network instead of the home network.

Global Title (GT) is an address used in the SCCP protocol for routing signaling messages in telecommunications networks. GT is unique and serves as an alias for a destination address. It is usually translated into a network address or a signaling point code within the SS7 network [41].

5.3 SS7 Attacks with Interconnection Access

As discussed before SS7 does not have inbuilt security. There are no mechanisms to ensure source node authentication and cryptographic protection for communications. The only security mechanisms currently available are related to traffic analysis, such as monitoring and screening traffic to identify unusual activity [39]. Over the last decade many vulnerabilities have been discovered and exploited in the SS7 MAP protocol, resulting in various attacks. These attacks include denial of service against subscribers and network, privacy leaks, network exposure, eavesdropping, SMS interception, fraud and credential threat [58]. In the following sections we discuss two SS7 attacks from [42] that are relevant to this thesis. Both the attacks result in stealing of the IMSI and tracking the location of a subscriber.

5.3.1 Location Tracking with Call Setup Messages

The MS location is saved in the HLR as part of mobility management. Whenever a MS moves into a new MSC area the location has to be updated at the HLR. The location information is used to route the calls and short messages to the intended MS. The general message flow when a subscriber makes a call to another subscriber is as follows:

1. The caller's GMSC sends the MAP Send Routing Information (MAP SRI) message to the receiver's HLR.
2. To get the location of the receiver's MS, the HLR sends the MAP Provide Roaming Number (MAP PRN) message to the VLR.
3. The VLR responds with the MAP PRN ack message, which contains the MSRN, IMSI and the GT of the MSC serving the receiver's MS.
4. The receiver's HLR sends the MAP SRI Ack message containing the MSRN, IMSI and MSC GT to the caller's GMSC.
5. The caller's GMSC has all the necessary information to establish a call.

Attack An attacker with SS7 access can impersonate a GMSC and track the location of the subscriber using call setup messages. The attacker sends a MAP SRI message to the HLR. As SS7 lacks source node authentication,

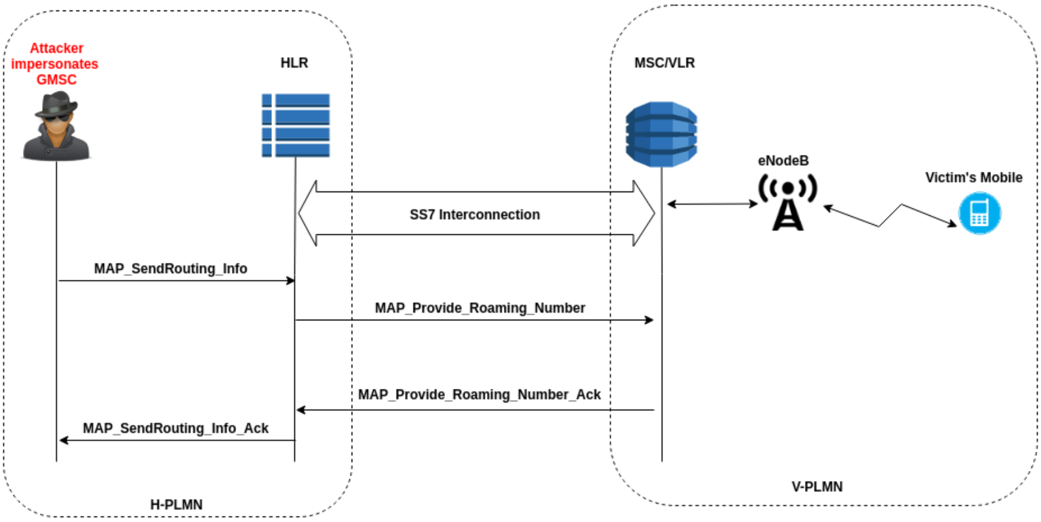


Figure 5.1: Location Tracking with SRI

the HLR is tricked into thinking that a call is being established and responds with MAP SRI Ack as described above. A successful attack [59] would reveal the IMSI and MSC GT to the attacker, which can be used to identify the subscriber's geo-location approximately. Figure 5.1 shows the attack sequence.

5.3.2 Location Tracking with SMS Protocol Messages

Short Message Service (SMS) is a text messaging service that allows mobile phone devices to exchange messages up to 140 bytes. End to end SMS delivery comprises of two parts. First, the Mobile Originating (MO) part where the Short Message (SM) is submitted by the sender to the SMSC. Second, the Mobile Terminating (MT) part where the SMSC delivers the SM to the recipient. The basic message flow is as follows:

1. MO part
   - The SM along with the SMSC address (usually stored in the SIM) are transmitted to the sender's serving MSC.
   - Sender's MSC sends the MO ForwardSM message to the received SMSC address.
   - The SMSC acknowledges the MSC with the MO ForwardSM Ack message after a successful delivery of the SM.

2. MT part

    - The sender's SMSC requires the IMSI, and the GT of the serving MSC to deliver the SM to the recipient's MS.
    - The sender's SMSC sends the MAP Send Routing Info For SM (MAP SRISM) message to the recipient's HLR.
    - The recipient's HLR responds with the MAP SRISM Ack message containing the IMSI and the MSC GT.
    - The sender's SMSC routes the SM to the recipient's MSC for further delivery

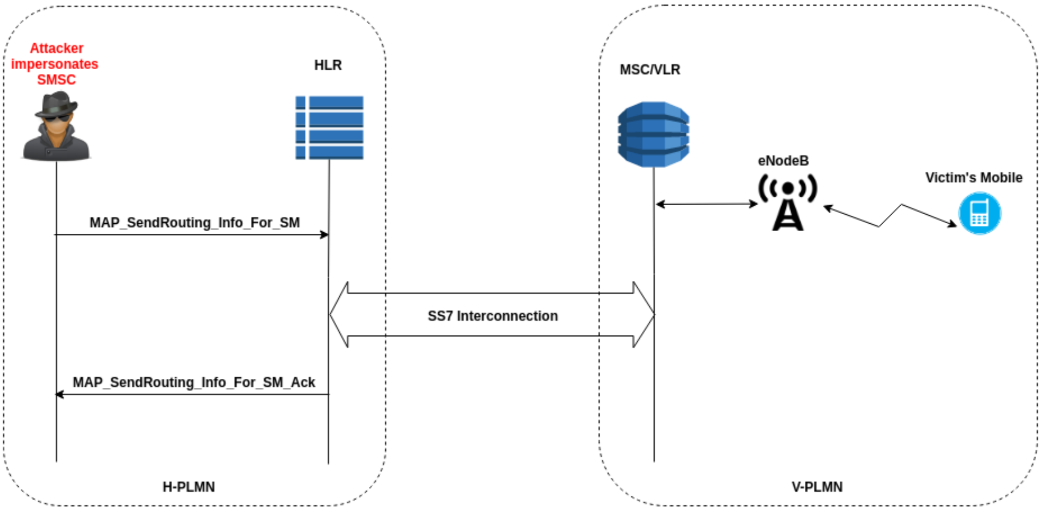

Attacker impersonates SMSC
HLR
MSC/VLR
eNodeB
Victim's Mobile
MAP_SendRouting_Info_For_SM
SS7 Interconnection
MAP_SendRouting_Info_For_SM_Ack
H-PLMN
V-PLMN

Figure 5.2: Location Tracking with SRISM

Attack An attacker with SS7 access can impersonate a SMSC and track location of the subscriber using the MT-SMS protocol messages. The attacker sends a MAP SRISM message to the HLR. As SS7 lacks source node authentication, the HLR is tricked into thinking that a SM is being sent and responds with MAP SRISM Ack as described above. A successful attack would reveal the IMSI and MSC GT to the attacker, which can be used to identify the subscriber's geo-location approximately. Figure 5.2 shows the attack sequence.

5.4 Diameter Attacks in LTE

As part of the thesis we analysed the Diameter signaling on the LTE interconnection and identified seven potential attacks. Due to time constraints we could implement only three of them in a test LTE network and the implementation of the rest is part of our future research. All the attacks are done in two phases. The first phase is the information collection phase, which collects information needed to perform the attack in the second phase. The following sections discuss the practical assumptions and the two phases.

5.4.1 Practical Considerations

If an attacker can gain access to the interconnection network, then he can start sending messages worldwide to operators that are connected either directly or through roaming hubs.

In the standard TS 33.201[46] the 3GPP has specified IPsec based security mechanisms for Diameter. Even TLS can be used but the industry is converging towards IPsec [60]. A key issue with the Diameter base protocol specifications is that IPsec and TLS are recommended but not mandatory on many interfaces [35]. Also, there are no procedures for the higher protocol layers to verify whether IPsec or TLS has been implemented by a Diameter node [50]. Exchanging public-key certificates between large telecom networks with thousands of nodes of different operators is quite a challenge and a costly process. Moreover, even if the certificates could be verified, the roaming interconnection like the Internet is already so vast and open that it is not possible to keep all malicious entities out of it. Therefore, the proposed attacks work under the following assumptions, which correspond to the reality in many deployed networks [36]:

1. IPsec is not used.

2. No layer matching is done i.e. no comparison and checking of sender address and return address between different protocol layers.

3. No holistic checks are made by the receiving node e.g. checking if the user is really in the given location.

If roaming hubs are utilized, then the tracking of the real sender becomes even greater challenge. Due to the hop-by-hop routing and use of the hop indicator of Diameter messages, the answers to the requests are routed to the original requester even if the data fields on the request contain the wrong identity. This makes it possible to spoof the requester identity and nevertheless receive answers to requests.

5.5 Diameter Attacks: Phase 1

In this phase, the attacker knows the phone number (MSISDN) of the mobile subscriber and tries to learn the IMSI and HSS address. The HSS address can be obtained by brute forcing on the IP address range of the operator. Since some operator's IR.21 database is available on the Internet the HSS details can be extracted from it. On the other hand, IMSI is not exactly a well-kept secret: it is printed so some SIM and UICC cards, and can also be accessed from the mobile device's user interface. More information on IMSI and MSISDN can be found in Section 5.2. There are other ways to learn an IMSI without having physical access to the phone. Some approaches are described below.

5.5.1 IMSI Catchers

IMSI catchers impersonate a network operator's base station and attract nearby mobile devices to register to it. For an LTE network, IMSI catchers basically work by jamming the LTE radio signal and downgrading a mobile device to use the less secure GSM and thereby circumvent the mutual authentication procedure in LTE. IMSI catchers can be distinguished into two main operating modes [61] discussed below.

Identification Mode When a mobile device gets connected to the fake base station, the IMSI is retrieved by the IMSI catcher and the connection is sent back to the original network by denying its original *Location Update Request* with a *Location Update Reject* message.

Camping Mode When a mobile device is in the cell of the fake base station, the IMSI catcher collects data and then forwards the traffic to the genuine network. To avoid such passive snooping attacks A5/3 and A5/4 ciphers are introduced into 2G networks to replace the broken A5/1 and A5/2 ciphers. IMSI catchers can still operate in this mode by downgrading the network to GSM and its less secure ciphers.

5.5.2 Fake WLAN Access Points in 3G-WLAN Interworking

Wireless Local Area Network (WLAN) is a complementary technology to the 3GPP system. The term 3G-WLAN interworking refers to extending the 3GPP services and functionality to the WLAN access environment [62]. The 3G-WLAN interworking is built on a key technology called Extensible Authentication Protocol (EAP) [63] which is an authentication framework that supports multiple authentication methods called EAP methods. Extensible Authentication Protocol for SIM (EAP-SIM) [64] is an EAP method that allows using the SIM and GSM authentication vectors and cryptographic functions within the EAP framework. Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA) [65] is an EAP method that allows the USIM and UMTS authentication vectors and cryptographic functions within the EAP framework [30]. A WLAN UE should support either of these EAP methods to access the 3GPP services. The overview of the EAP based authentication in 3G-WLAN interworking is shown in Figure 5.3. After successful WLAN registration, the UE's identity is requested by the AAA server. The UE responds with the IMSI in the EAP-Response message. The detailed information of the messages can be found in 3GPP TS 33.234 [66].

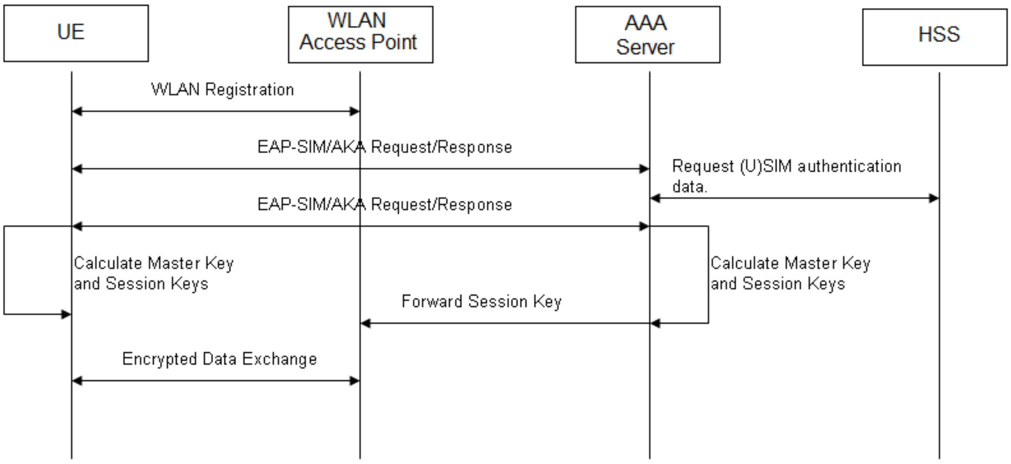

UE
WLAN Access Point
AAA Server
HSS
WLAN Registration
EAP-SIM/AKA Request/Response
Request (U)SIM authentication data.
EAP-SIM/AKA Request/Response
Calculate Master Key and Session Keys
Calculate Master Key and Session Keys
Forward Session Key
Encrypted Data Exchange

Figure 5.3: 3G-WLAN Interworking Using EAP-SIM/EAP-AKA

Attack An attacker can setup a fake WLAN access point and can trick (for e.g. by jamming other signals) the UE to register itself. After registration the attacker can send an EAP-Request/Identity message to the UE and the UE responds with the IMSI in EAP-Response/Identity message. Thereby an attacker can steal the IMSI.

5.5.3 Diameter Send Routing Info for SM Procedure

The *Send-Routing-Info-for-SM-Request* (SRR) on the S6c [67] interface is sent by the SMSC to the HSS in order to retrieve the routing information needed for routing a short message to the serving MME of the recipient. It is the equivalent of MAP SRISM in the LTE network and Diameter. The working and functionality is the same as described in Section 5.3.2. Figure 5.4 illustrates the workflow of the SMS MT part in LTE.

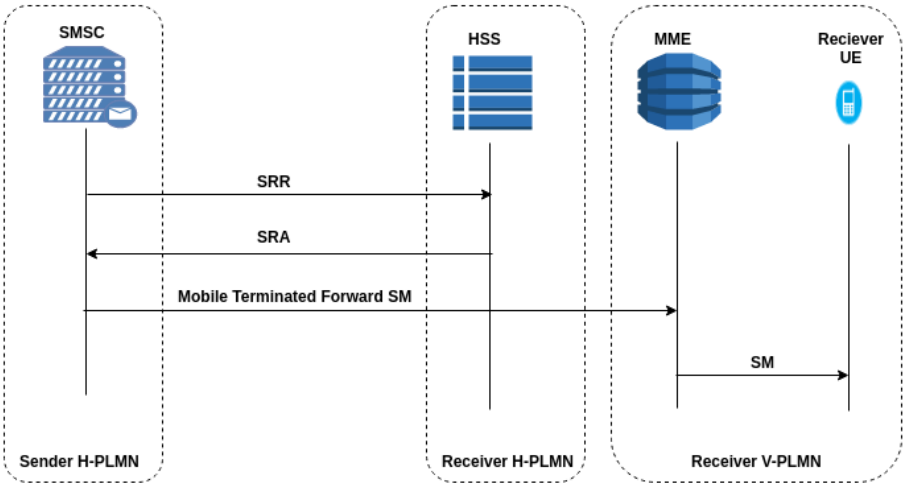


Figure 5.4: SMS MT Part Workflow

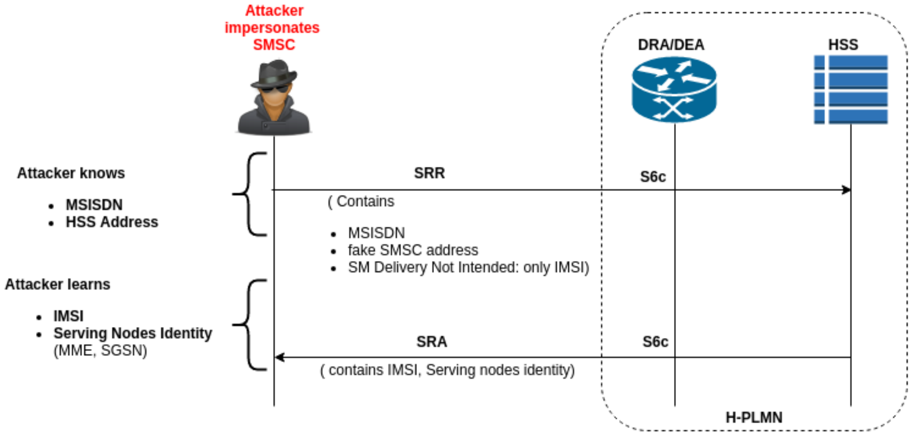

Attacker impersonates SMSC
DRA/DEA
HSS
Attacker knows
• MSISDN
• HSS Address
SRR
S6c
(Contains
• MSISDN
• fake SMSC address
• SM Delivery Not Intended: only IMSI)
Attacker learns
• IMSI
• Serving Nodes Identity (MME, SGSN)
SRA
S6c
(contains IMSI, Serving nodes identity)
H-PLMN

Figure 5.5: Obtaining IMSI with SRR

Attack An attacker with an interconnection access can misuse the above protocol to identify the IMSI and identity of the subscriber's serving MME. The SRR request must contain a mandatory *SC-Address* AVP whose value is the SMSC address in the E.164 format [68]. The request must also contain the *MSISDN* AVP to identify the subscriber. After a successful attack, the attacker will receive a SRA message with the *Serving-Node* AVP which in turn contains the Diameter identity and the Diameter realm of the MME and SGSN (if present). If the home network uses SMS home routing (Section 7.2) then the *MT-SMS Correlation ID* is sent in the SRA instead of IMSI. If a SMS home router is deployed, then the SRR message can also be used to explicitly request the IMSI of a subscriber. To do this, the SRR message should contain the *SM-Delivery Not Intended* AVP with the value *only IMSI* along with the SC-Address and MSISDN AVPs. This indicates that the IMSI is requested and delivery of a short message is not intended. The attack sequence is shown in Figure 5.5.

5.6 Diameter Attacks: Phase 2

In the first phase of the attacks, the identity of the serving MME and IMSI are discovered, as described above. In the second phase, the attacker impersonates a HSS towards the MME or as MME towards the HSS, according to the 3GPP TS 29.272 [69] and performs the attack over the S6a interface. The attacks are described in the following sections.

5.6.1 DoS Attack with CLR

The *Cancel-Location-Request* (CLR) message is sent by the HSS to the MME. This message informs the MME about an initial attach procedure, or about an ongoing change in the serving MME, or about subscription withdrawal of a subscriber.

Bit	Name	Description
0	S6a/S6d Indicator	When set, indicates that the CLR message is sent on the S6a interface; when cleared, indicates the S6d interface
1	Reattach-Required	When set, indicates that the MME should request the UE to initiate an immediate reattach procedure

Table 5.1: Bitmask description of CLR-Flags AVP [69]

The CLR message must contain two mandatory AVPs. First, the *User-Name* AVP whose value is the IMSI of the subscriber. Second, the *Cancellation-Type* AVP which is an enumeration. When it is set to the enum value *Subscription_Withdrawal (2)*, the MME deletes the subscription data and de-

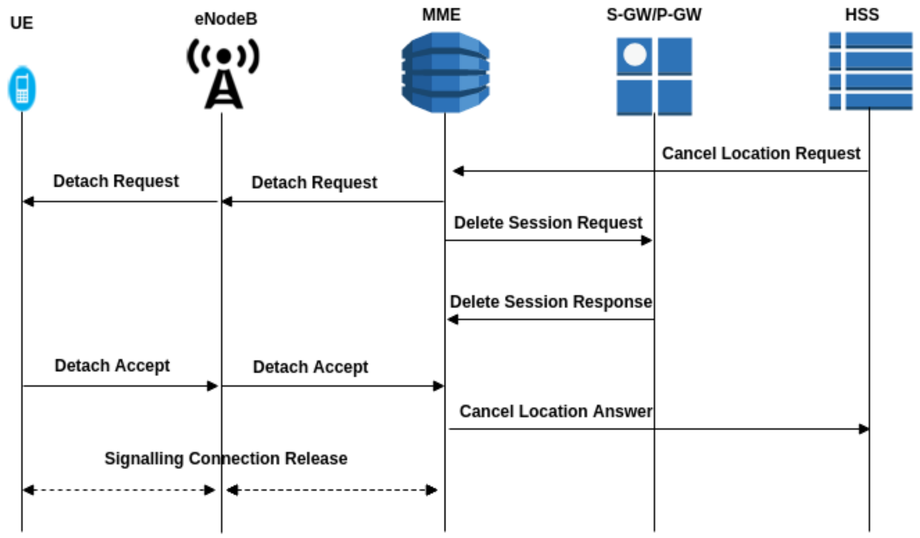


Figure 5.6: HSS Initiated Detach Procedure

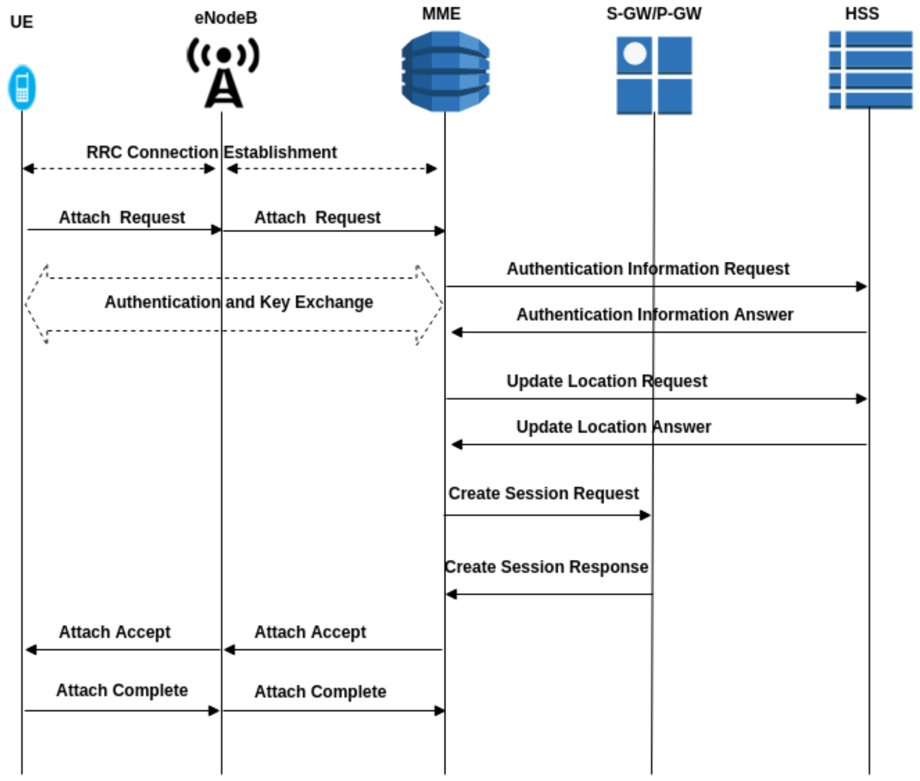


Figure 5.7: UE Attach Procedure

taches the UE. An overview of the HSS initiated detach procedure is shown in Figure 5.6 and the detailed procedure can be found in 3GPP TS 23.272 [70]. Furthermore, the HSS can also specify additional actions, such as requesting the UE to re-attach to the network immediately after the detach. This is achieved through the *CLR-Flags* AVP whose value is a bitmask. The bits relevant to the attack are described in Table 5.1, and the detailed description of all the bits can be found in Section 7.3.152 of [69]. An overview of the UE attach procedure can be seen in Figure 5.7, and the detailed procedure can be found in 3GPP TS 24.301 [71].

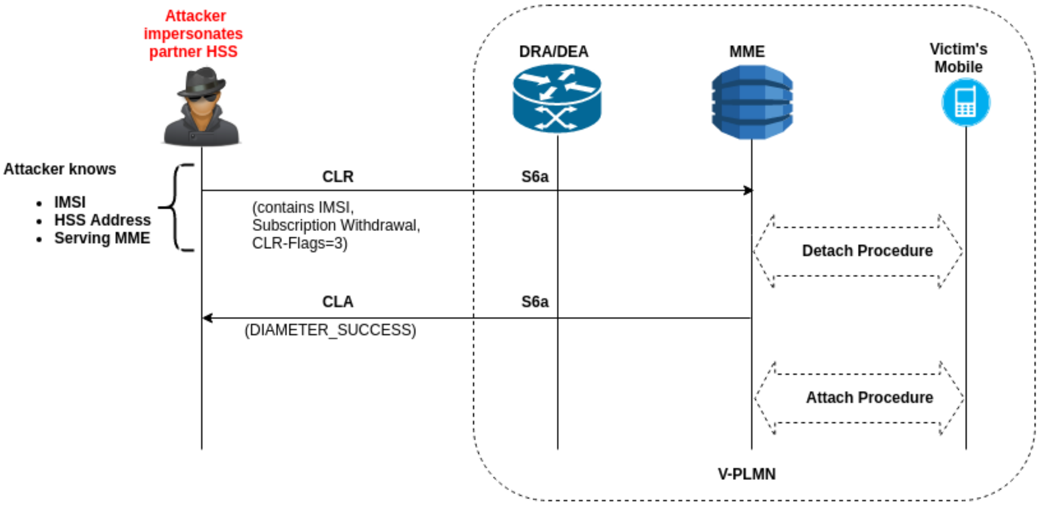


Figure 5.8: DoS with CLR

Attack An attacker with interconnection access can impersonate the HSS of the subscriber's home network and send a CLR to the serving MME to cause a DoS attack against the subscriber. Figure 5.8 shows the attack sequence. The CLR should contain the AVPs described above and is expressed as XML in Snippet 5.1. A serving MME receiving this CLR message will detach the subscriber from the network, thereby resulting in a denial of service. Furthermore, a DoS attack is possible on both the serving MME and the actual HSS of the home network. If the *Reattach-Required* bit is set in the *CLR-Flags* AVP, the UE initiates the attach procedure. The attach procedure involves a lot of signaling messages and performing this attack continuously can create signaling storms in the core network. In this way, the MME and the HSS can be overloaded with signaling messages which could ultimately lead to performance degradation or even their failure. This attack might also cause a battery drain in the UE. The attack is implemented in a test network and the results are presented in Section 6.2.1.

```
<command name="Cancel-Location-Request" code="317">
 <avp name="User-Name" value="XXXXXXXXXXX4001" />
 <avp name="Cancellation-Type" value="2" />
 <avp name="CLR-Flags" value="3"/>
</command>
```

Snippet 5.1: CLR Message for DoS Attack

5.6.2 DoS Attack with ULR

The *Update-Location-Request* (ULR) message is sent by the MME to the HSS. This message informs the HSS about the identity of the MME currently serving the subscriber, and optionally provides other subscriber data such as the Radio Access Terminal (RAT) information.

Bit	**Name**	**Description**
1	S6a/S6d Indicator	When set, indicates that the ULR message is sent on the S6a interface; when cleared, indicates the S6d interface
5	Initial-Attach-Indicator	When set, indicates that the HSS should send a CLR with Cancellation-Type of *MME_Update_Procedure* to the serving MME (if any registered for the IMSI in context)

Table 5.2: Bitmask description of ULR-Flags AVP [69]

The ULR must contain the following mandatory AVPs. First, the *User-Name* AVP whose value is the IMSI of the subscriber. Second, *Visited-PLMNId* whose value is the concatenation of the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Third, the *RAT-Type* whose value is the RAT information the UE is using. Fourth, the *ULR-Flags* AVP whose value is a bitmask. The bits relevant to the attack are described in Table 5.2, and the detailed description of all the bits can be found in Section 7.3.7 of [69]. When the HSS receives an ULR, it replaces the stored MME identity with the value received in the ULR's *Origin-Host* AVP.

Attack An attacker with interconnection access can impersonate a MME of a roaming partner and send an ULR to the HSS of the subscriber's home network, to cause a DoS attack against the subscriber. Figure 5.9 shows the attack sequence. The ULR should contain the AVPs described above and is

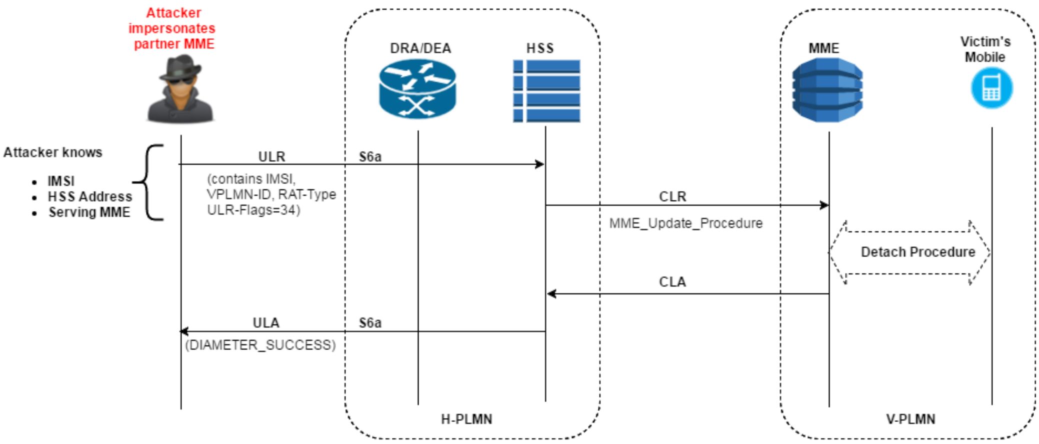


Figure 5.9: DoS Attack with ULR

expressed as XML in Snippet 5.2. A HSS receiving this ULR message will send a CLR to the subscriber's serving MME, and therefore the subscriber gets detached from the network, resulting in a denial of service. The MCC and MNC codes are available on many websites, such as mcc-mnc.com, mcclist.com etc., and so the Visited-PLMNId can be easily obtained to carry out the attack. The attack is implemented in a test network and the results are presented in Section 6.2.2.

```
<command name="Update-Location-Request" code="316">
 <avp name="User-Name" value="XXXXXXXXXXX4001" />
 <avp name="Visited-PLMNId" value="XXXX3"/>
 <avp name="RAT-Type" value="1004"/>
 <avp name="ULR-Flags" value="34"/>
</command>
```

Snippet 5.2: ULR Message for DoS Attack

5.6.3 DoS and Fraud Attacks with IDR

The *Insert-Subscriber-Data-Request* (IDR) message is sent by the HSS to the MME. This message is invoked due to administrative changes, such as adding or updating the subscription information at the MME, requesting certain subscriber data from the MME, and applying or removing Operator Determined Barring (ODB) [72] for a subscriber. ODB allows the home network operator to regulate access to the services availed by a subscriber.

Bit	Description
0	All Packet Oriented Services Barred
1	Roamer Access HPLMN-AP Barred
2	Roamer Access to VPLMN-AP Barred
3	Barring of all outgoing calls
4	Barring of all outgoing international calls
5	Barring of all outgoing international calls except those directed to the home PLMN country
6	Barring of all outgoing inter-zonal calls
7	Barring of all outgoing inter-zonal calls except those directed to the home PLMN country
8	Barring of all outgoing international calls except those directed to the home PLMN country and Barring of all outgoing inter-zonal calls

Table 5.3: Bitmask description of Operator-Determined-Barring AVP [69]

The IDR must contain two mandatory AVPs. First, the *User-Name* AVP whose value is the IMSI of the subscriber. Second, the *Subscription-Data* AVP which contains the part of the subscription profile that either is to be added or updated in the subscription profile stored in the MME. To apply or remove ODB the *Subscription-Data* AVP can contain two child AVPs. First, the *Subscriber-Status* AVP, an enumeration that specifies if a service is granted or barred. It informs the MME that certain services are barred for the subscriber when set to the enum value 1. Second, the *Operator_Determined_Barring*, is a bitmask that indicates the barred services. The meaning of the bits is defined in Table 5.3 and the detailed description can be found in Section 7.3.30 of [69]. ODB can be removed by setting the *Subscriber-Status* AVP to the value 0.

Attack An attacker with interconnection access can impersonate the HSS of the subscriber's home network and send an IDR to the subscriber's serving MME in order to bar the services of a subscriber. The message should contain the above described AVPs and is expressed as XML in Snippet 5.3. A MME receiving this IDR message will bar the services of a subscriber, thereby resulting in a denial of service attack. The attacker can also misuse the IDR message to unbar the barred services of a subscriber and thereby resulting in a fraud attack. This impacts the revenue flow of the operator rather than the data flow and does not break any underlying technology. The attack sequence is shown in Figure 5.10. The attack is implemented in a test network and the results are presented in Section 6.2.2.

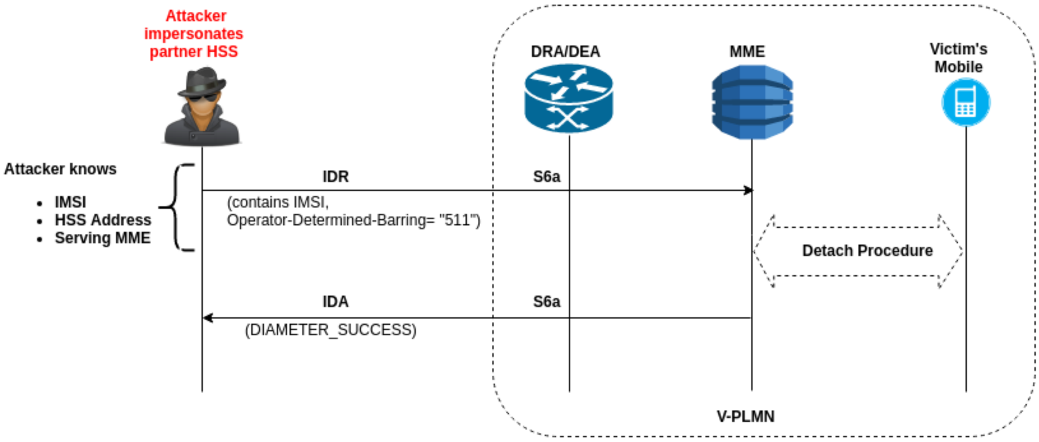


Figure 5.10: DoS Attack with IDR

```
<command name="Insert-Subscriber-Data-Request" code="319">
  <avp name="User-Name" value="XXXXXXXXXXX4001" />
  <avp name="Subscription-Data">
   <avp name="Subscriber-Status" value="1" />
   <avp name="Operator-Determined-Barring" value="511" />
  </avp>
</command>
```

Snippet 5.3: IDR Message for DoS Attack

5.6.4 Location Tracking with IDR

The HSS can send the IDR message to a MME to request the location information of a subscriber. Along with the *User-Name* and *Subscriber-Data* AVPs, the IDR must also contain a *IDR-Flags* AVP, whose value is a bitmask. The bits relevant to the attacks are described in Table 5.4, and the detailed description of all the bits can be found in Section 7.3.103 of [69]. A MME receiving the *IDR-Flags* with the *EPS Location Information Request* bit set, responds with the *EPS-Location-Information* AVP. This AVP in turn contains three more AVPs: *Cell-Global-Identity*, *Location-Area-Identity*, *Service-Area-Identity*. If the *Current Location Request* bit is set along with *EPS Location Information* bit and the UE is in idle mode, then the MME will page the UE to return the most up-to-date location of the subscriber.

Attack An attacker with interconnection access can impersonate the HSS of the subscriber's home network and send an IDR to the subscriber's serv-

Bit	Name	Description
0	UE Reachability Request	When set, informs the MME that the HSS is awaiting a notification of UE reachability. (This bit is used in the attack described in Section 5.6.6)
3	EPS Location Information Request	When set, informs the MME that the HSS is requesting the subscriber's location information.
4	Current Location Request	When set, informs the MME to provide the most current location information by paging the UE (if in idle mode). This bit can be used only in conjunction with bit 3.
5	Local Time Zone Request	When set, informs the MME that the HSS is requesting the time zone of the location in the visited network where the UE is attached.

Table 5.4: Bitmask description of IDR-Flags AVP [69]

ing MME to track the location of the subscriber. The IDR must contain the above described AVPs and is expressed as XML in Snippet 5.4. Figure 5.11 shows the attack sequence. The MME receiving this message responds with the location information and the time zone which can be used to identify the approximate location of the subscriber. The implementation of this attack is part of our future research.

```
<command name="Insert-Subscriber-Data-Request" code="319">
  <avp name="User-Name" value="XXXXXXXXXXX4001" />
  <avp name="Subscription-Data"> </avp>
  <avp name="IDR-Flags" value="56" />
</command>
```

Snippet 5.4: IDR Message for Location Tracking Attack

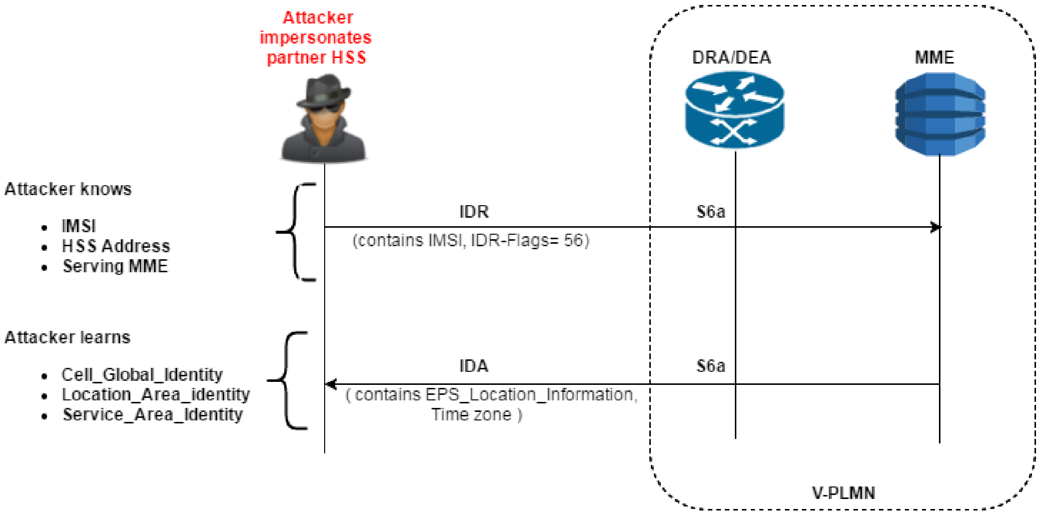


Figure 5.11: Location Tracking Attack with IDR

5.6.5 DoS Attack with NOR

The *Notify Request* (NOR) is sent by the MME to the HSS. It is used to notify the HSS about various events, such as an update of UE terminal information, UE reachability, and removal of MME registration for SMS. For the removal of MME registration for SMS, the NOR message must contain two AVPs. First, the *User-Name* AVP whose value is the IMSI of the subscriber. Second, the *NOR-Flags* AVP whose value is a bitmask. The bits relevant to the attack are described in Table 5.5, and the detailed description of all the bits can be found in Section 7.3.49 of [69]. Bit 9 is *Removal of MME Registration for SMS* which, when set, indicates that the MME requests to remove its registration for SMS. The detailed procedure for removal of SMS registration can be found in 3GPP TS 23.272 [70].

Bit	**Name**	**Description**
8	S6a/S6d Indicator	When set, indicates that the NOR message is sent on the S6a interface; when cleared, indicates the S6d interface
9	Removal of MME Registration for SMS	When set, indicates that the MME requests to remove its registration for SMS from the HSS

Table 5.5: Bitmask description of NOR-Flags AVP [69]

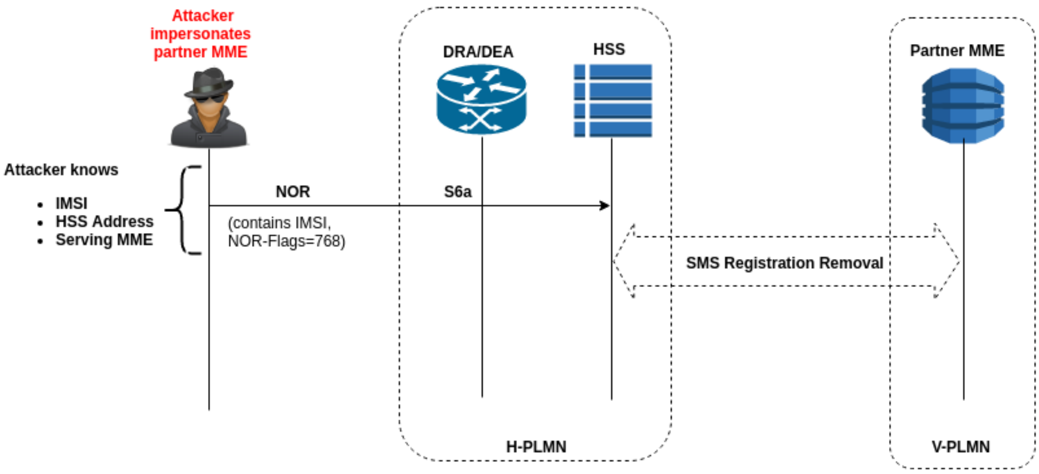


Figure 5.12: SMS DoS Attack with NOR

Attack An attacker with interconnection access can impersonate a MME of a roaming partner and send a NOR to the HSS of the subscriber's home network, to cause a SMS DoS attack. The message should contain the above described AVPs and is expressed as XML in Snippet 5.5. The HSS receiving this NOR message will remove SMS registration for the MME, and thereby resulting in SMS denial of service for some subscribers (associated with the HSS) attached to the MME. Figure 5.12 shows the attack sequence. The implementation of this attack is part of our future research.

```
<command name="Notify-Request" code="323">
 <avp name="User-Name" value="XXXXXXXXXXX4001" />
 <avp name="NOR-Flags" value="768"/>
</command>
```

Snippet 5.5: NOR Message for SMS DoS Attack

5.6.6 DoS Attack with IDR and NOR Combined

The IDR can be used to inform the MME that the HSS is awaiting a notification of UE reachability. This is done by setting bit 0 in the *IDR-Flags* AVP. The bit description can be seen in Table 5.4. When there is an authenticated radio contact from the UE, the MME sends a NOR to the HSS to inform about the UE reachability. If the MME receives a Notification Answer (NOA) message from the HSS with the result code *DIAME-*

TER_ERROR_USER_UNKNOWN, the MME will detach the UE and remove the subscriber from its database.

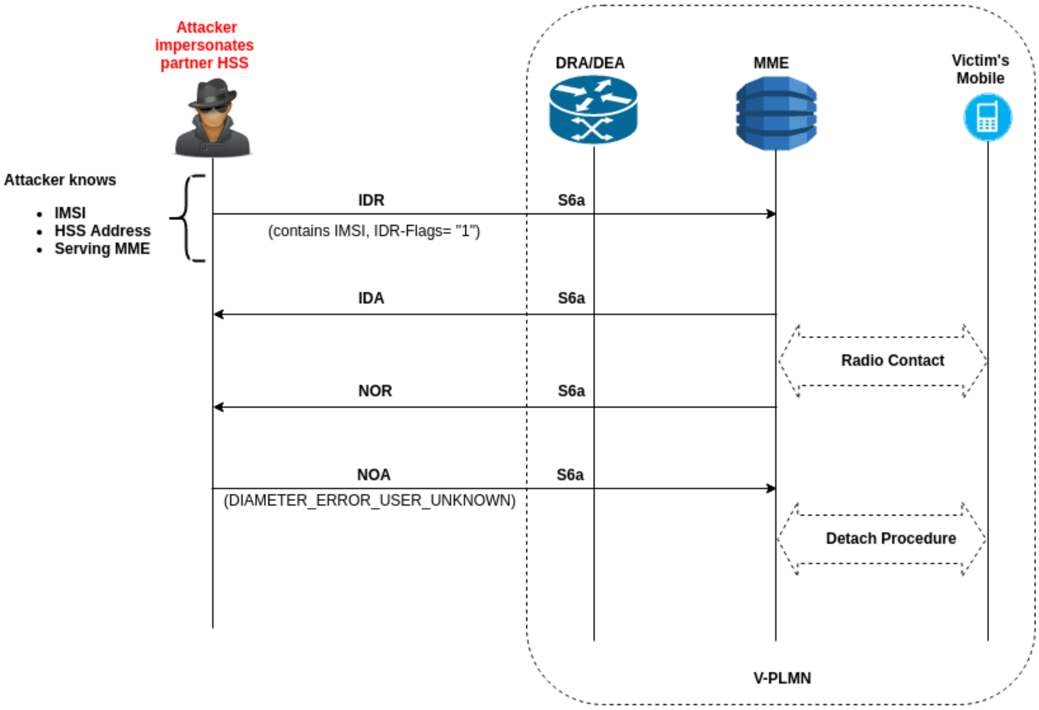


Figure 5.13: DoS Attack with IDR and NOR Combined

Attack An attacker with interconnection access can impersonate the HSS of the subscriber's home network and send an IDR to the subscriber's serving MME with bit 0 set in the *IDR-Flags* AVP. The MME responds with a NOR when there is a radio contact from the UE. The attacker receiving the NOR, sends a NOA with the result code *DIAMETER_ERROR_USER_UNKNOWN*. The MME receiving this NOA will detach the subscriber from the network, and thereby resulting in a denial of service. Figure 5.12 shows the attack sequence. The message format is the same as described in the previous sections. The implementation of this attack is part of our future research.

5.6.7 DoS Attack with RSR

The *Reset-Request* is sent by the HSS to the MME to inform about a previous HSS failure or about maintenance operations for e.g. to allow planned HSS outage without service interruption. The RSR message contains a *User-Id*

AVP whose value is a list of User-Ids. A User-Id contains the leading digits of an IMSI (i.e. MCC, MNC, leading digits of MSIN) which identifies the set of subscribers whose IMSIs start with the User-Id. The MME receiving a RSR triggers restoration procedures [73] for all the subscribers associated with the received User-Ids. The MME sends an ULR to the HSS as part of the restoration procedure.

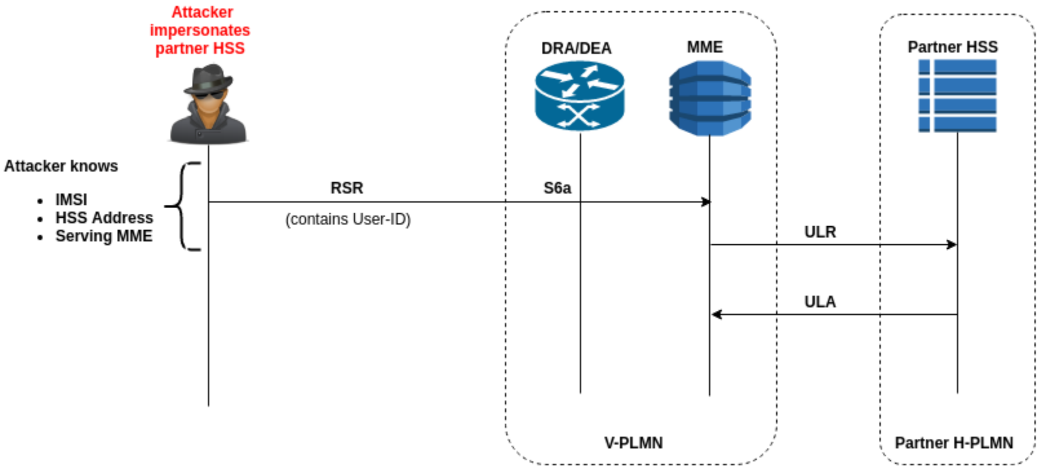


Figure 5.14: DoS Attack with RSR

Attack An attacker with interconnection access can impersonate the HSS of the subscriber's home network and send a RSR to the subscriber's serving MME to cause a DoS attack against the actual HSS. The message should contain *User-Id* AVP with the value *MCC+MNC* and is expressed as XML in Snippet 5.6. The MME will start restoration procedures for all the subscribers whose IMSI match with the User-Id. An ULR is sent to the HSS for each matching subscriber. Performing this attack continuously can create signaling storms in the core network. The MME and the HSS can be overloaded with signaling messages and might ultimately lead to performance degradation or even their failure. The attack sequence is shown in Figure 5.14. The implementation of this attack is part of our future research.

```
<command name="Reset-Request" code="322">
 <avp name="User-ID" value="XXXX3" />
</command>
```

Snippet 5.6: RSR Message for DoS Attack

Chapter 6

Experiments

Experiments were conducted to verify the attacks in a test network of a global operator which corresponds to an actual deployed network. Due to the privacy and security legislation in the country of residence of the author, the attacks could not be performed in practice against real subscribers in deployed networks.

6.1 Testbed Setup

The test network setup is illustrated in Figure 6.1. The UE is roaming in the test network and has Internet access. It is connected to the network through a HeNodeB. The DEA is the network entry and exit point for the roaming interconnection and acts as a Diameter routing agent. The DEA does not have any filtering mechanism. The attacker is a laptop computer with two network interfaces which have access to the interconnection network. The interface with IP xx.xx.34.14 is used impersonate the HSS of the HPLMN. The interface with IP xx.xx.34.10 is used to impersonate the MME of the VPLMN. The attacker laptop computer is also configured with a custom Diameter traffic generator which we developed based on the RestComm jDiameter [74] open-source library.

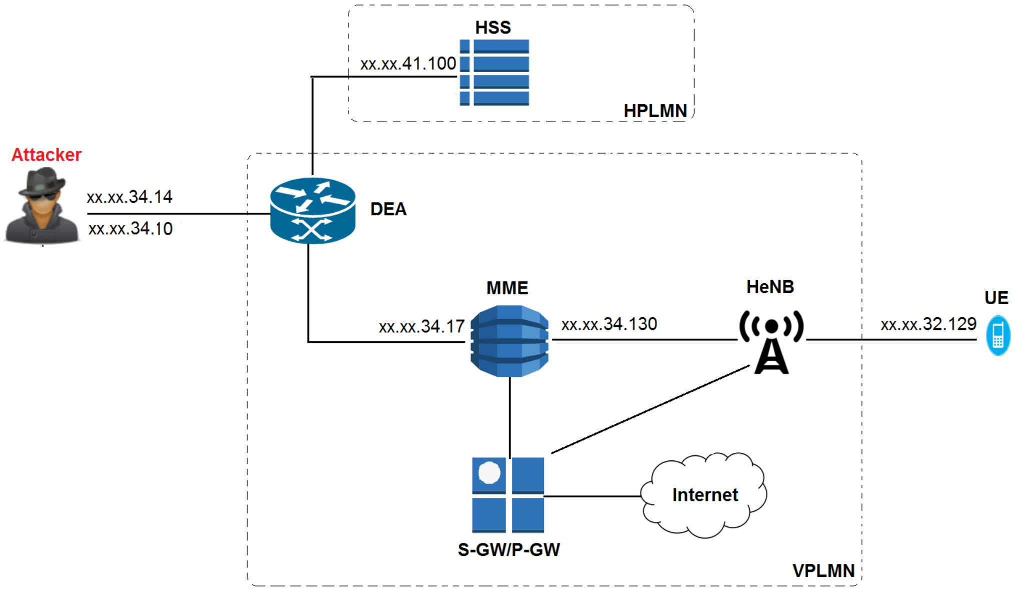


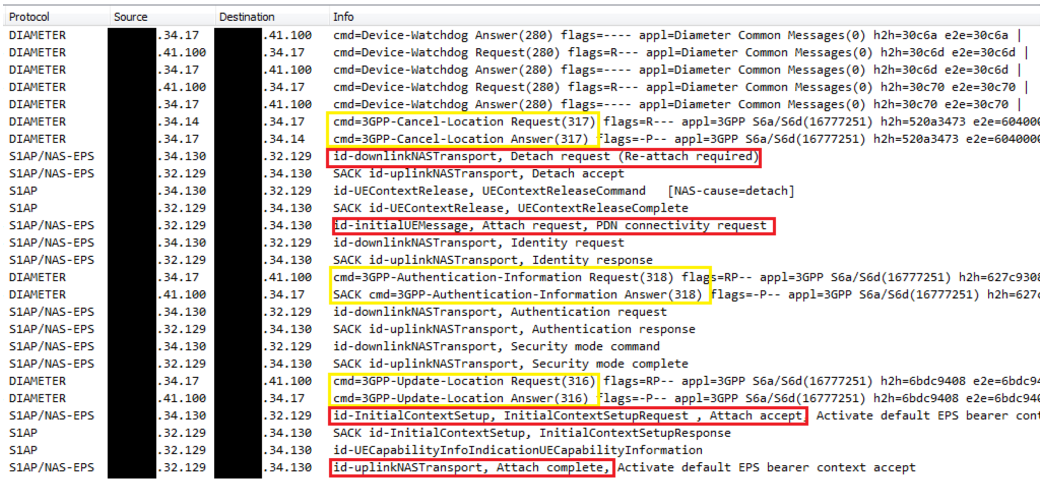
Figure 6.1: Test Network Setup

6.2 Results

The results shown in the following sections are network captures (using Wireshark [75] tool) on the interfaces of MME and HSS in the test network. All the confidential information, such as IP addresses, IMSIs, host names and realm names have been blacked out in the images.

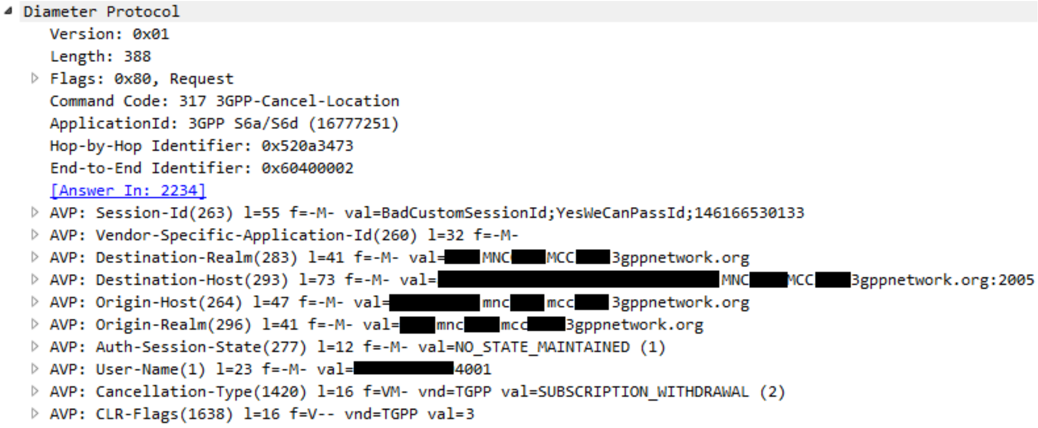
6.2.1 DoS Attack with CLR

Figure 6.2 illustrates a successful DoS attack on the subscriber with CLR. The attacker impersonated the HSS and sent a CLR message to the MME. The MME detached the UE from the network and also requested the UE to re-attach. After the detach, the UE initiated the attach procedure which included the AIR/AIA and ULR/ULA along with other signaling messages. The highlighted portions show the sequence of messages. Figure 6.3 shows the contents of the CLR message sent.



```
Protocol      Source             Destination        Info
DIAMETER      [redacted].34.17   [redacted].41.100  cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=30c6a e2e=30c6a |
DIAMETER      [redacted].41.100  [redacted].34.17   cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=30c6d e2e=30c6d |
DIAMETER      [redacted].34.17   [redacted].41.100  cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=30c6d e2e=30c6d |
DIAMETER      [redacted].41.100  [redacted].34.17   cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=30c70 e2e=30c70 |
DIAMETER      [redacted].34.17   [redacted].41.100  cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=30c70 e2e=30c70 |
DIAMETER      [redacted].34.14   [redacted].34.17   cmd=3GPP-Cancel-Location Request(317) flags=R--- appl=3GPP S6a/S6d(16777251) h2h=520a3473 e2e=60400
DIAMETER      [redacted].34.17   [redacted].34.14   cmd=3GPP-Cancel-Location Answer(317) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=520a3473 e2e=604000
S1AP/NAS-EPS  [redacted].34.130  [redacted].32.129  id-downlinkNASTransport, Detach request (Re-attach required)
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  SACK id-uplinkNASTransport, Detach accept
S1AP          [redacted].34.130  [redacted].32.129  id-UEContextRelease, UEContextReleaseCommand   [NAS-cause=detach]
S1AP          [redacted].32.129  [redacted].34.130  SACK id-UEContextRelease, UEContextReleaseComplete
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  id-initialUEMessage, Attach request, PDN connectivity request
S1AP/NAS-EPS  [redacted].34.130  [redacted].32.129  id-downlinkNASTransport, Identity request
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  SACK id-uplinkNASTransport, Identity response
DIAMETER      [redacted].34.17   [redacted].41.100  cmd=3GPP-Authentication-Information Request(318) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=627c930
DIAMETER      [redacted].41.100  [redacted].34.17   SACK cmd=3GPP-Authentication-Information Answer(318) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=627
S1AP/NAS-EPS  [redacted].34.130  [redacted].32.129  id-downlinkNASTransport, Authentication request
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  SACK id-uplinkNASTransport, Authentication response
S1AP/NAS-EPS  [redacted].34.130  [redacted].32.129  id-downlinkNASTransport, Security mode command
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  SACK id-uplinkNASTransport, Security mode complete
DIAMETER      [redacted].34.17   [redacted].41.100  cmd=3GPP-Update-Location Request(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=6bdc9408 e2e=6bdc9
DIAMETER      [redacted].41.100  [redacted].34.17   cmd=3GPP-Update-Location Answer(316) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=6bdc9408 e2e=6bdc94
S1AP/NAS-EPS  [redacted].34.130  [redacted].32.129  id-InitialContextSetup, InitialContextSetupRequest , Attach accept, Activate default EPS bearer con
S1AP          [redacted].32.129  [redacted].34.130  SACK id-InitialContextSetup, InitialContextSetupResponse
S1AP          [redacted].32.129  [redacted].34.130  id-UECapabilityInfoIndicationUECapabilityInformation
S1AP/NAS-EPS  [redacted].32.129  [redacted].34.130  id-uplinkNASTransport, Attach complete, Activate default EPS bearer context accept
```

Figure 6.2: CLR DoS: Wireshark Overview

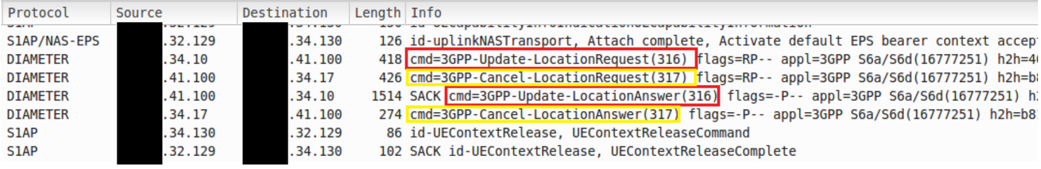


```
◢ Diameter Protocol
    Version: 0x01
    Length: 388
  ▷ Flags: 0x80, Request
    Command Code: 317 3GPP-Cancel-Location
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x520a3473
    End-to-End Identifier: 0x60400002
    [Answer In: 2234]
  ▷ AVP: Session-Id(263) l=55 f=-M- val=BadCustomSessionId;YesWeCanPassId;146166530133
  ▷ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  ▷ AVP: Destination-Realm(283) l=41 f=-M- val=[redacted]MNC[redacted]MCC[redacted]3gppnetwork.org
  ▷ AVP: Destination-Host(293) l=73 f=-M- val=[redacted]MNC[redacted]MCC[redacted]3gppnetwork.org:2005
  ▷ AVP: Origin-Host(264) l=47 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▷ AVP: Origin-Realm(296) l=41 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▷ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ▷ AVP: User-Name(1) l=23 f=-M- val=[redacted]4001
  ▷ AVP: Cancellation-Type(1420) l=16 f=VM- vnd=TGPP val=SUBSCRIPTION_WITHDRAWAL (2)
  ▷ AVP: CLR-Flags(1638) l=16 f=V-- vnd=TGPP val=3
```

Figure 6.3: CLR DoS: CLR Message Contents

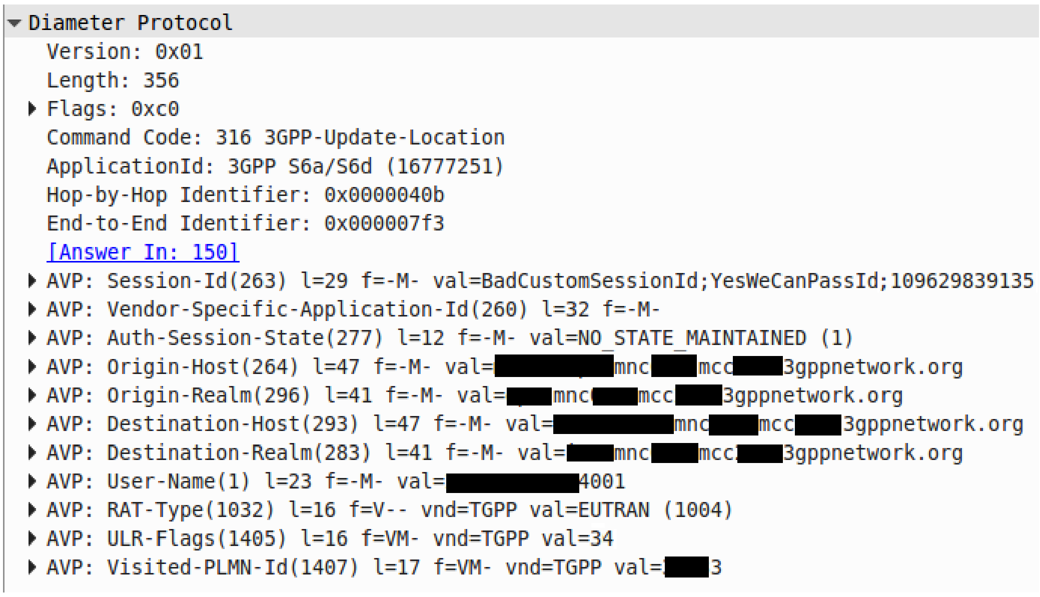
6.2.2 DoS Attack with ULR

Figure 6.4 illustrates a successful DoS attack on the subscriber with ULR message. The attacker impersonated a partner MME and sent an ULR message to the HSS. The HSS triggered a CLR and sent it to the serving MME which detaches the UE from the network. The highlighted portions show the sequence of messages. Figure 6.5 shows the contents of the ULR message. Figure 6.6 shows the contents of the CLR message triggered due to the ULR.



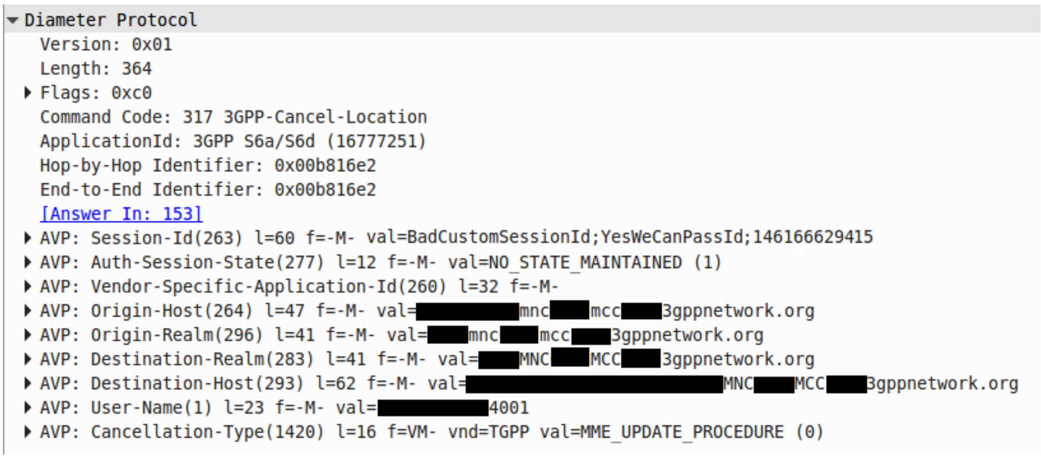
```
Protocol     Source             Destination        Length Info
S1AP/NAS-EPS [redacted].32.129  [redacted].34.130     126 id-uplinkNASTransport, Attach complete, Activate default EPS bearer context accep
DIAMETER     [redacted].34.10   [redacted].41.100     418 cmd=3GPP-Update-LocationRequest(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=4
DIAMETER     [redacted].41.100  [redacted].34.17      426 cmd=3GPP-Cancel-LocationRequest(317) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=b
DIAMETER     [redacted].41.100  [redacted].34.10     1514 SACK cmd=3GPP-Update-LocationAnswer(316) flags=-P-- appl=3GPP S6a/S6d(16777251) h
DIAMETER     [redacted].34.17   [redacted].41.100     274 cmd=3GPP-Cancel-LocationAnswer(317) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=b8
S1AP         [redacted].34.130  [redacted].32.129      86 id-UEContextRelease, UEContextReleaseCommand
S1AP         [redacted].32.129  [redacted].34.130     102 SACK id-UEContextRelease, UEContextReleaseComplete
```

Figure 6.4: ULR DoS: Wireshark Overview



```
▾ Diameter Protocol
    Version: 0x01
    Length: 356
  ▸ Flags: 0xc0
    Command Code: 316 3GPP-Update-Location
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x0000040b
    End-to-End Identifier: 0x000007f3
    [Answer In: 150]
  ▸ AVP: Session-Id(263) l=29 f=-M- val=BadCustomSessionId;YesWeCanPassId;109629839135
  ▸ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  ▸ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ▸ AVP: Origin-Host(264) l=47 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Origin-Realm(296) l=41 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Destination-Host(293) l=47 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Destination-Realm(283) l=41 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: User-Name(1) l=23 f=-M- val=[redacted]4001
  ▸ AVP: RAT-Type(1032) l=16 f=V-- vnd=TGPP val=EUTRAN (1004)
  ▸ AVP: ULR-Flags(1405) l=16 f=VM- vnd=TGPP val=34
  ▸ AVP: Visited-PLMN-Id(1407) l=17 f=VM- vnd=TGPP val=[redacted]3
```

Figure 6.5: ULR DoS: ULR Message Contents

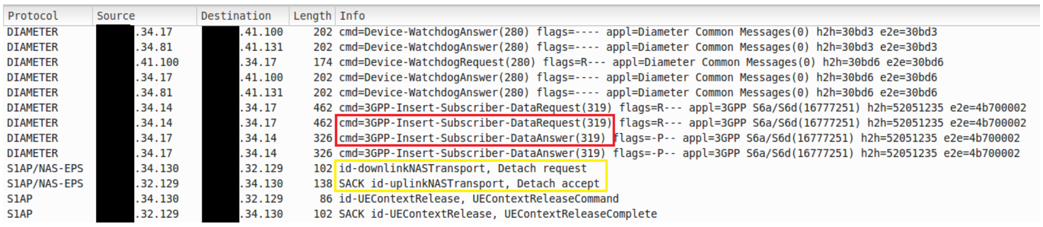


```
▾ Diameter Protocol
    Version: 0x01
    Length: 364
  ▸ Flags: 0xc0
    Command Code: 317 3GPP-Cancel-Location
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x00b816e2
    End-to-End Identifier: 0x00b816e2
    [Answer In: 153]
  ▸ AVP: Session-Id(263) l=60 f=-M- val=BadCustomSessionId;YesWeCanPassId;146166629415
  ▸ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ▸ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  ▸ AVP: Origin-Host(264) l=47 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Origin-Realm(296) l=41 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Destination-Realm(283) l=41 f=-M- val=[redacted]MNC[redacted]MCC[redacted]3gppnetwork.org
  ▸ AVP: Destination-Host(293) l=62 f=-M- val=[redacted]MNC[redacted]MCC[redacted]3gppnetwork.org
  ▸ AVP: User-Name(1) l=23 f=-M- val=[redacted]4001
  ▸ AVP: Cancellation-Type(1420) l=16 f=VM- vnd=TGPP val=MME_UPDATE_PROCEDURE (0)
```

Figure 6.6: ULR DoS: CLR Message Contents

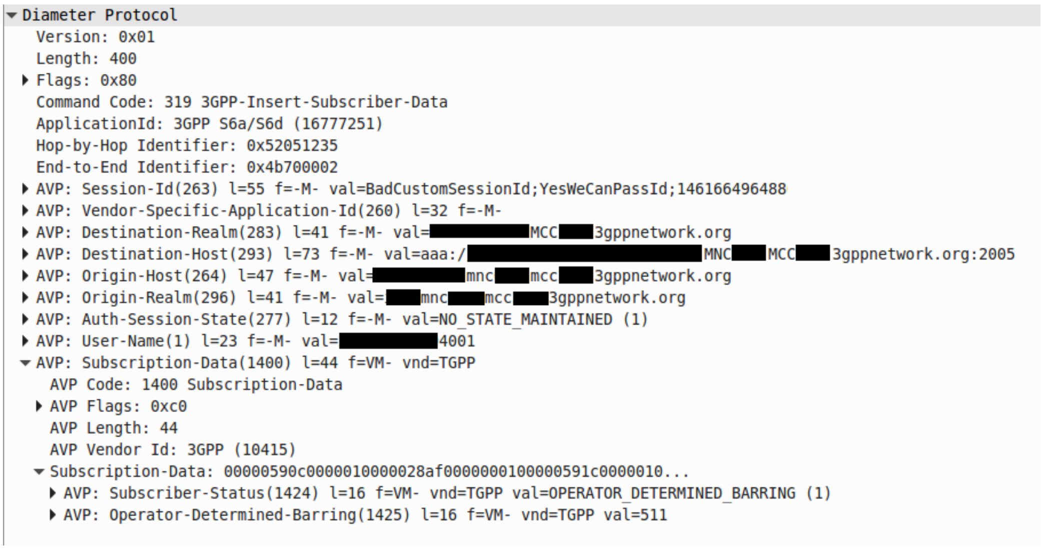
6.2.3 DoS Attack with IDR

Figure 6.7 illustrates a successful DoS attack on the subscriber with IDR message. The attacker impersonated the HSS and sent an IDR to the MME. The MME barred the services for the subscriber and detached the UE from the network. The highlighted portions show the sequence of messages. Figure 6.8 shows the contents of the IDR message. The change of subscription data could not be captured in wireshark as it is an MME internal operation. The fraud attack sequence is the same as the DoS attack except for the changes in IDR content.



```
Protocol      Source              Destination         Length Info
DIAMETER      [redacted].34.17    [redacted].41.100   202 cmd=Device-WatchdogAnswer(280) flags=---- appl=Diameter Common Messages(0) h2h=30bd3 e2e=30bd3
DIAMETER      [redacted].34.81    [redacted].41.131   202 cmd=Device-WatchdogAnswer(280) flags=---- appl=Diameter Common Messages(0) h2h=30bd3 e2e=30bd3
DIAMETER      [redacted].41.100   [redacted].34.17    174 cmd=Device-WatchdogRequest(280) flags=R--- appl=Diameter Common Messages(0) h2h=30bd6 e2e=30bd6
DIAMETER      [redacted].34.17    [redacted].41.100   202 cmd=Device-WatchdogAnswer(280) flags=---- appl=Diameter Common Messages(0) h2h=30bd6 e2e=30bd6
DIAMETER      [redacted].34.81    [redacted].41.131   202 cmd=Device-WatchdogAnswer(280) flags=---- appl=Diameter Common Messages(0) h2h=30bd6 e2e=30bd6
DIAMETER      [redacted].34.14    [redacted].34.17    462 cmd=3GPP-Insert-Subscriber-DataRequest(319) flags=R--- appl=3GPP S6a/S6d(16777251) h2h=52051235 e2e=4b700002
DIAMETER      [redacted].34.14    [redacted].34.17    462 cmd=3GPP-Insert-Subscriber-DataRequest(319) flags=R--- appl=3GPP S6a/S6d(16777251) h2h=52051235 e2e=4b700002
DIAMETER      [redacted].34.17    [redacted].34.14    326 cmd=3GPP-Insert-Subscriber-DataAnswer(319) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=52051235 e2e=4b700002
DIAMETER      [redacted].34.17    [redacted].34.14    326 cmd=3GPP-Insert-Subscriber-DataAnswer(319) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=52051235 e2e=4b700002
S1AP/NAS-EPS  [redacted].34.130   [redacted].32.129   102 id-downlinkNASTransport, Detach request
S1AP/NAS-EPS  [redacted].32.129   [redacted].34.130   138 SACK id-uplinkNASTransport, Detach accept
S1AP          [redacted].34.130   [redacted].32.129    86 id-UEContextRelease, UEContextReleaseCommand
S1AP          [redacted].32.129   [redacted].34.130   102 SACK id-UEContextRelease, UEContextReleaseComplete
```

Figure 6.7: IDR DoS: Wireshark Overview



```
▾ Diameter Protocol
    Version: 0x01
    Length: 400
  ▸ Flags: 0x80
    Command Code: 319 3GPP-Insert-Subscriber-Data
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x52051235
    End-to-End Identifier: 0x4b700002
  ▸ AVP: Session-Id(263) l=55 f=-M- val=BadCustomSessionId;YesWeCanPassId;146166496488
  ▸ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  ▸ AVP: Destination-Realm(283) l=41 f=-M- val=[redacted]MCC[redacted]3gppnetwork.org
  ▸ AVP: Destination-Host(293) l=73 f=-M- val=aaa:/[redacted]MNC[redacted]MCC[redacted]3gppnetwork.org:2005
  ▸ AVP: Origin-Host(264) l=47 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Origin-Realm(296) l=41 f=-M- val=[redacted]mnc[redacted]mcc[redacted]3gppnetwork.org
  ▸ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ▸ AVP: User-Name(1) l=23 f=-M- val=[redacted]4001
  ▾ AVP: Subscription-Data(1400) l=44 f=VM- vnd=TGPP
      AVP Code: 1400 Subscription-Data
    ▸ AVP Flags: 0xc0
      AVP Length: 44
      AVP Vendor Id: 3GPP (10415)
    ▾ Subscription-Data: 00000590c0000010000028af0000000100000591c0000010...
      ▸ AVP: Subscriber-Status(1424) l=16 f=VM- vnd=TGPP val=OPERATOR_DETERMINED_BARRING (1)
      ▸ AVP: Operator-Determined-Barring(1425) l=16 f=VM- vnd=TGPP val=511
```

Figure 6.8: IDR DoS: IDR Message Contents

Chapter 7

Countermeasures

In this chapter we discuss potential countermeasures and mitigation strategies to counteract the attacks we identified. We also discuss the challenges and trade-offs for these countermeasures.

7.1 Using IPsec

IPsec protection following 3GPP TS 33.210 is one of the foremost protection measures that can be deployed. IPsec ensures that the both ends of a tunnel know the identity of each other. But it is helpful only if the other end could be trusted. The trust issue becomes challenging, in particular, when hop-by-hop security is deployed, for example, in roaming hubs because each hop would need its own IPsec tunnel. In such a hop-by-hop security approach, the duty of checking the next leg of the communication and ensuring that the communication is secure within the roaming hub server falls on the roaming hub provider. In SS7, there was no need for certificate management, therefore the roaming hub providers did not have any related costs. When it comes to Diameter, extra costs are to be incurred by the roaming hub providers. So changes to business practices would be needed. Another major challenge is that, if a partner operator rents out access to less trustworthy entities, it might potentially lead to the misuse of the trusted certificates of the partner operator. Also governments and spy agencies can misuse the operators in their own country, for e.g. to track the location of people.

7.2 SMS Home Routing

SMS protocol is one of the most commonly exploited protocols by the attackers to sniff operator network topology and to obtain subscriber information such as IMSI. As per 3GPP TS 29.338 [67], for SMS routing, the SMSC of the subscriber contacts the HSS of the home network to identify the location of the recipient's UE. Normally all outbound and cross-network SMS messages pass through the sender's home network. Since SMS was initially designed for voice-message notification and not as a person-to-person messaging system, the inbound messages generated on other networks can be directly sent to the target subscribers that are under the control of the sending network. The MT-SMS protocol is discussed in Section 5.5.3.

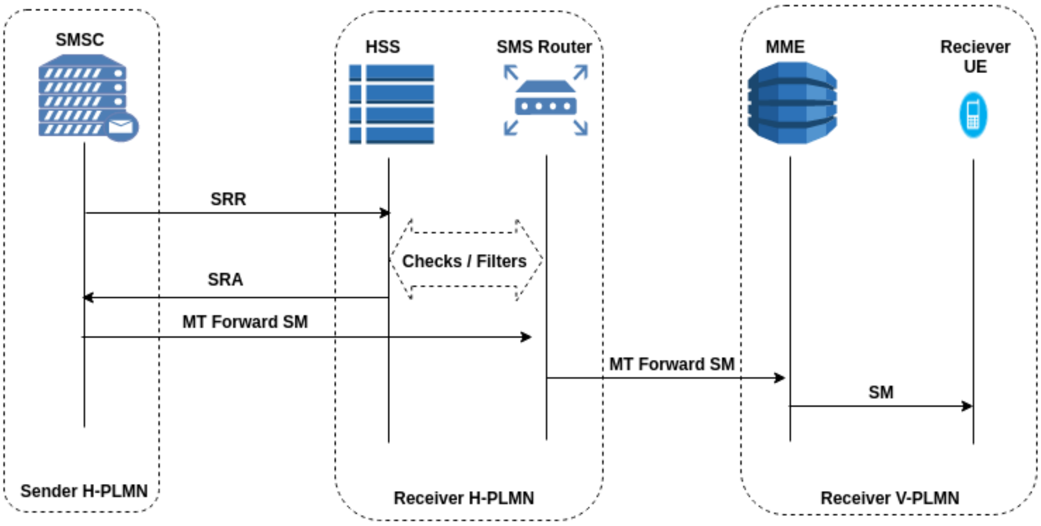


Figure 7.1: SMS Home Routing

The 3GPP TR 23.840 [76], defines Mobile Terminated SMS home routing where the inbound short messages are routed through a MT service platform (commonly called SMS router), in the recipient's home network. Figure 7.1 illustrates the working of SMS home routing. The SMS router safeguards the IMSI of a subscriber by using a 15 digit MT-SMS Correlation ID, which is unique and mapped to the IMSI and MSISDN of a subscriber. In a SRA message the Correlation-ID is sent instead of the IMSI, thereby hiding the IMSI from the sender's SMSC. The Correlation-ID consists of a 3-digit MCC, a 3-digit MNC and a 9-digit Sender ID. The structure of MT-SMS Correlation ID is shown in Figure 7.2. The MCC and MNC are the codes of receiver's HPLM, whereas the Sender ID is a random number unique for its lifetime. The Sender ID maps the inbound MT Forward SM message to a previous SRR.

SMS home routing relieves the VPLMN from requesting the IMSI and location of the receiving UE, and thereby defends the network against privacy

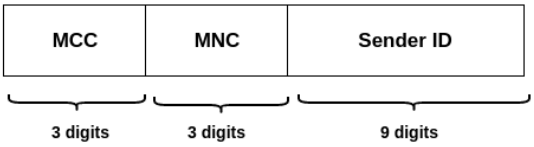


Figure 7.2: MT-SMS Correlation ID

breaches and fraud. The SMS router can also implement other protection mechanisms, such as anti-spam and filtering to defend against spam, phishing and malware. SMS home routing is not mandatory and the implementation of the protection mechanisms is up to the operator. However, the possible implementation flaw with *SM-Delivery Not Intended* AVP discussed in Section 5.5.3 should be take care of when implementing SMS home routing.

7.3 Enhancements in DEA/DRA

Diameter Edge Agents and Diameter Routing Agents are the entry and exit points of any roaming interconnection. So securing the DEA/DRA can help in preventing many attacks. Since some of the messages used for the attacks that we described are part of regular communication, directly blocking those messages would interrupt the cellular services. The first approach is, that the nodes residing on the edge have proper interface separation i.e. they know if a message is for the Sh or S6a interface. For example, only some interfaces are open on the roaming interconnection such as S6a/S6d, S8, S9, and all other interface connections should be rejected on the interconnection.

Efficient filtering mechanisms based on the smart combination of cross-layer verification, IP address based blocking, origin host and realm checking, AVP verification and advance access control methods are recommended the LTE networks against the location privacy breach attacks. Firstly, the operators should white-list their partners based on the protocols, IP address of the nodes, or origin host and realm and support for requested applications and required permissions. Such white-listing is highly recommended due to the increased risk for the support for interoperability with lower generation networks of partner operators. Secondly, the operators should thoroughly monitor their network traffic in real time. They should include robust statistical traffic analysis methods to detect any unusual or abnormal behavior of the network nodes. Furthermore, the traffic from suspected nodes should be directed to honey-pots for further investigation to finally block the nodes. One of the key advantages of using strong access control policies in the nodes—

particularly in DEA/DRA — is that, even if the attacker bypasses sender origin filtering, the node would not respond beyond its configured functionality. On the other hand, the cross-layer verification in the hop-by-hop routes of Diameter helps to verify the origin of a message such that the operators can automatically block the messages originated from illicit nodes. However, telecom networks have a large number of requests every second and filtering every message might have a significant effect on the node performance. So, there is a security vs performance trade-off. The above mentioned filtering mechanisms might be available in the firewalls available in the market and it is very important to configure the firewall policies to effectively defend the LTE network against the attacks that are discussed in this thesis.

Chapter 8

Conclusion

Diameter is gradually replacing the SS7 signaling protocol in the next generation telecommunication networks. In this thesis, we provided a comprehensive review of security considerations of Diameter protocol. We discussed the possible exploits in Diameter signaling for an LTE network, which enables an attacker to deny services to targeted subscribers and illegitimately track the location of the mobile users. Though the advantages of Diameter signaling are many, the default security provided by Diameter is not sufficient to make LTE an attack-resistant network. While the roaming interconnections ensures cost-efficient way to provide cellular services on a global scale, it is important to deploy additional measures in the interconnection network to protect the users from privacy breaches and denial of service.

We described the various internal components of the core network, the roaming architecture to provide an insight into the working of 4G networks. Furthermore, we gave a detailed background on the interconnection network and the signaling protocols used. We explained how an attacker can gain access to the interconnection network and exploit the diameter signaling messages. We described in detail the various attacks ranging from denial of service to location tracking. We demonstrated the practical relevance of these attacks by implementing some of them in a test network and discussed their results in detail. We also articulated some potential countermeasures and explained the security mechanisms that can be used to identify attackers and block malicious messages at the Diameter Edge Agents (DEA) without affecting the normal functioning of other core network nodes.

The findings in this thesis are very useful to ensure interconnection security in the existing LTE deployments and the ones that are to be deployed. The standardization of fifth generation mobile networks has gained a lot of momentum recently and we argue that, without appropriate countermeasures and mitigation techniques in place, the threats discussed in this thesis might be carried onto the next generation networks. With this thesis, we go one step further in the direction towards a sound telecom security architecture. The future work includes implementation of unverified attacks and finding appropriate mitigation strategies.

Bibliography

[1] B. Sanou, "The World in 2015: ICT facts and figures," *International Telecommunications Union*, 2015.

[2] Statistia, "Number of LTE subscriptions worldwide from 2015 to 2020." `http://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-LTE-subscriptions-up-to-2014/`. [Accessed 30-June-2016], 2012.

[3] "White Paper: 5G Security," tech. rep., Ericsson AB, 2015.

[4] E. Noam, "Interconnection practices," *Handbook of telecommunications economics*, vol. 1, pp. 385–421, 2002.

[5] J. Postel, "Internet Protocol," RFC 791, The Internet Engineering Task Force, September 1981.

[6] M. Paolini, "White Paper: Wireless security in LTE networks," tech. rep., Senza Fili Consulting, 2012. [Accessed 30-June-2016].

[7] C. Cox, *An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications.* John Wiley & Sons, 2012.

[8] S. Sesia, I. Toufik, and M. Baker, *LTE: the UMTS long term evolution.* Wiley Online Library, 2nd ed., 2011.

[9] A. A. Atayero, M. K. Luka, M. K. Orya, and J. O. Iruemi, "3GPP long term evolution: Architecture, protocols and interfaces," *International Journal of Information and Communication Technology Research*, vol. 1, no. 7, pp. 306–310, 2011.

[10] 3GPP, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 layer 1 general aspects and principles," TS 36.410; Release 12, 3rd Generation Partnership Project (3GPP).

[11] 3GPP, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP)," TS 36.423; Release 12, 3rd Generation Partnership Project (3GPP).

[12] M. Anas, C. Rosa, F. D. Calabrese, P.-H. Michaelsen, K. I. Pedersen, and P. E. Mogensen, "QoS-aware single cell admission control for UTRAN LTE uplink," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pp. 2487–2491, IEEE, 2008.

[13] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios," TR 36.942; Release 12, 3rd Generation Partnership Project (3GPP).

[14] F. Firmin, "The Evolved Packet Core," `http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core` [Accessed 30-June-2016].

[15] "The LTE network Architecture—A comprehensive tutorial," tech. rep., Alcatel Lucent, 2009.

[16] 3GPP, "Architecture enhancements for non-3GPP accesses," TS 23.402; Release 12, 3rd Generation Partnership Project (3GPP).

[17] 3GPP, "General Packet Radio Service (GPRS); Evolved GPRS Tunnelling Protocol (eGTP) for EPS," TS 29.274; Release 12, 3rd Generation Partnership Project (3GPP).

[18] B. Dhindsa, A. Kaur, and S. Ahuja, "LTE interfaces and protocols," in *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*, pp. 870–874, IEEE, 2015.

[19] 3GPP, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)," TS 29.061; Release 12, 3rd Generation Partnership Project (3GPP).

[20] G. Sanders, L. Thorens, M. Reisky, O. Rulik, and S. Deylitz, *GPRS networks.* John Wiley & Sons, 2004.

[21] 3GPP, "Policy and charging control over Gx reference point," TS 29.212; Release 12, 3rd Generation Partnership Project (3GPP).

[22] 3GPP, "Policy and charging control over Rx reference point," TS 29.214; Release 12, 3rd Generation Partnership Project (3GPP).

[23] N. Kottapalli, “Diameter and LTE Evolved Packet System: Radisys White Paper,” tech. rep., Radisys, 2011.

[24] M. Hata, “Empirical formula for propagation loss in land mobile radio services,” *Vehicular Technology, IEEE Transactions on*, vol. 29, no. 3, pp. 317–325, 1980.

[25] 3GPP, “Policy and Charging Control (PCC) over S9 reference point,” TS 29.215; Release 12, 3rd Generation Partnership Project (3GPP).

[26] Y. Park and T. Park, “A survey of security threats on 4G networks,” in *2007 IEEE Globecom Workshops*, pp. 1–6, IEEE, 2007.

[27] N. Seddigh, B. Nandy, R. Makkar, and J.-F. Beaumont, “Security advances and challenges in 4G wireless networks,” in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pp. 62–71, IEEE, 2010.

[28] J. Zheng, “Research on the Security of 4G Mobile System in the IPv6 Network,” in *Recent Advances in Computer Science and Information Engineering*, pp. 829–834, Springer, 2012.

[29] C. Sankaran, “Network access security in next-generation 3GPP systems: A tutorial,” *IEEE Communications Magazine*, vol. 47, no. 2, pp. 84–91, 2009.

[30] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanara, “Enhancing security and privacy in 3GPP E-UTRAN radio interface,” in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, IEEE, 2007.

[31] M. Zhang and Y. Fang, “Security analysis and enhancements of 3GPP authentication and key agreement protocol,” *IEEE Transactions on wireless communications*, vol. 4, no. 2, pp. 734–742, 2005.

[32] B. Ravishankar and M. Harishankar, “Roaming issues in 3GPP security architecture and solution using UMM architecture,” in *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM’08. The Second International Conference on*, pp. 457–462, IEEE, 2008.

[33] D. S. Tonesi, L. Salgarelli, and A. Tortelli, “Securing the signaling plane in beyond 3G networks: analysis of performance overheads,” *Security and Communication Networks*, vol. 3, no. 2-3, pp. 217–232, 2010.

[34] "General Recommendations on Telephone Switching and Signalling-Vocabulary of switching and signalling terms," tech. rep., ITU-Telecommunication Standardization sector, 1993.

[35] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter base protocol," RFC 3588, The Internet Engineering Task Force, September 2003.

[36] S. Holtmanns, S. P. Rao, and I. Oliver, "User Location Tracking Attacks for LTE Networks Using the Interworking Functionality," in *IFIP Networking Conference (IFIP Networking)*, IEEE, 2016.

[37] B. Gabelgaard, "The (GSM) HLR-advantages and challenges," in *Universal Personal Communications, 1994. Record., 1994 Third Annual International Conference on*, pp. 335–339, IEEE, 1994.

[38] 3GPP, "Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)," TR 23.039; Release 12, 3rd Generation Partnership Project (3GPP).

[39] L. Dryburgh and J. Hewett, *Signaling System No. 7 (SS7/C7): protocol, architecture, and services.* Cisco press, 2005.

[40] T. Moore, T. Kosloff, J. Keller, G. Manes, and S. Shenoi, "Signaling System 7 (SS7) network security," in *Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on*, vol. 3, pp. III–496, IEEE, 2002.

[41] 3GPP, "Mobile Application Part (MAP) specification," TS 29.002; Release 12, 3rd Generation Partnership Project (3GPP).

[42] S. Rao, "Analysis and Mitigation of Recent Attacks on Mobile Communication Backend," Master's thesis, Aalto University School of Science and Technology, Espoo, Finland, 2015.

[43] C. Rigney, A. Rubens, W. Simpson, and S. Willens, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, The Internet Engineering Task Force, June 2000.

[44] R. Stewart, "Stream Control Transmission Protocol," RFC 4960, The Internet Engineering Task Force, September 2007.

[45] J. Liu, S. Jiang, and H. Lin, "Introduction to Diameter." `https://www.ibm.com/developerworks/library/wi-diameter/`. [Accessed 30-June-2016].

[46] 3GPP, “3G security; Network Domain Security (NDS); IP network layer security,” TS 33.210; Release 12, 3rd Generation Partnership Project (3GPP).

[47] E. Guttman, C. Perkins, and J. Kempf, “Service Templates and Service: Schemes,” RFC 2609, Internet Engineering Task Force, June 1999.

[48] S. Cheshire and M. Krochmal, “DNS-Based Service Discovery,” RFC 6763, Internet Engineering Task Force, Feb. 2013.

[49] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol,” RFC 5246, The Internet Engineering Task Force, August 2008.

[50] P. Langlois, “Diameter vs SS7 from a security perspective,” 2013. `http://labs.p1sec.com/2013/07/28/346/` [Accessed 30-June-2016].

[51] S. K. Yoo, H. G. Kim, and S. W. Sohn, “Enhancement of failover using application layer watchdog and SCTP heartbeat in diameter,” in *Mobile Communications*, pp. 239–246, Springer, 2003.

[52] A. Hosia, “Comparison between RADIUS and Diameter.” `http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf`, May 2003.

[53] 3GPP, “InterWorking Function (IWF) between MAP based and Diameter based interfaces,” TS 29.305; Release 12, 3rd Generation Partnership Project (3GPP).

[54] 3GPP, “InterWorking Function (IWF) between MAP based and Diameter based interfaces,” TR 29.805; Release 12, 3rd Generation Partnership Project (3GPP).

[55] “Claro Americas IR.21 Data.” `http://www.claro.com.br/sites/files/contratos/arquivos/orpa_roam_claro_001-2015_-_anexo_4-apend_a-roaming_nacional_-_ir_21_0.pdf`. [Accessed 30-June-2016].

[56] “Vivo Brazil IR.21 Data.” `https://www.vivo.com.br/portalweb/ShowPropertyServlet?nodeId=/UCMRepository/CONTRIB_093689`. [Accessed 30-June-2016].

[57] 3GPP, “Numbering, addressing and identification,” TS 23.003; Release 12, 3rd Generation Partnership Project (3GPP).

[58] L. Ghigonis, “SS7map: SS7 country risk ratings,” 2014. `http://labs.p1sec.com/2014/12/28/ss7map-country-risk-ratings/` [Accessed 30-June-2016].

[59] T. Engel, "Locating mobile phones using signalling system 7," in *25th Chaos communication congress*, 2008.

[60] GSMA, "IR.77 Inter-Operator IP Backbone requirements for service providers and Inter-Operator Ip backbone providers," Tech. Rep. 3.0, GSM Association (GSMA), 2015. (Internal document).

[61] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th annual computer security applications Conference*, pp. 246–255, ACM, 2014.

[62] 3GPP, "Feasibility study on 3GPP system to Wireles Local Area Network (WLAN) interworking," TR 22.934; Release 12, 3rd Generation Partnership Project (3GPP).

[63] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, The Internet Engineering Task Force, June 2004.

[64] H. Haverinen and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)," RFC 4186, The Internet Engineering Task Force, January 2006.

[65] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187, The Internet Engineering Task Force, January 2006.

[66] 3GPP, "3G security; Wireless Local Area Network (WLAN) interworking security," TS 33.234; Release 12, 3rd Generation Partnership Project (3GPP).

[67] 3GPP, "Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)," TS 29.338; Release 12, 3rd Generation Partnership Project (3GPP).

[68] ITU-T, "E 164: The international public telecommunication numbering plan," *International Telecommunications Union (ITU)*, 2010.

[69] 3GPP, "MME Related Interfaces Based on Diameter Protocol," TS 29.272; Release 12, 3rd Generation Partnership Project (3GPP).

[70] 3GPP, "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2," TS 23.272; Release 12, 3rd Generation Partnership Project (3GPP).

[71] 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," TS 24.301; Release 12, 3rd Generation Partnership Project (3GPP), Sept. 2008.

[72] 3GPP, "Technical realization of Operator Determined Barring (ODB)," TS 23.015; Release 12, 3rd Generation Partnership Project (3GPP).

[73] 3GPP, "Mobility Management Entity (MME) - Visitor Location Register (VLR) SGs interface specification," TS 29.118; release 12, 3rd Generation Partnership Project (3GPP).

[74] "RestComm JDiameter." `https://github.com/RestComm/jdiameter/`. [Accessed 30-June-2016].

[75] "Wireshark." `https://www.wireshark.org/`. [Accessed 30-June-2016].

[76] 3GPP, "Study into routing of MT-SMS via the HPLMN," TR 23.840; Release 7, 3rd Generation Partnership Project (3GPP).