CHALMERS

Investigation IMS architecture

According to Security and QoS context

Master of Science Thesis [Network and distributed system]

AJMAL MUHAMMAD
RAJA MUHAMMAD SHAMAYEL ULLAH

Investigating NGN-IMS architecture accordingly security and QoS context

AJMAL MUHAMMAD
RAJA MUHAMMAD SHAMAYEL ULLAH
Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, March 2014

Examiner: ARNE LINDE

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden March 2014

Abstract

Next Generation Network moved towards full IP- based network. In NGN, various types of services are provided by CSCF – Control Service Control Function called as IMS- IP Multimedia Subsystem. IMS is located in service layer of NGN architecture. IMS network provides services to several terminals as wire and wireless independently of access network. Hence, NGN – IMS has common service control architecture. Networks are based on data and components. These are open and regulated. Security rises in this scenario when an unauthorized access is being accomplishing. As a collectively it is considered as network security. Security requirements and mechanisms are based on various techniques. Security polices and protocols are set by standardized bodies and security experts as well. Security solutions are implemented by investigation of their architectural framework.

In IMS network, security architecture is under further researched. International bodies as UMTS and 3GPP provides framework to best analyzed in security requirement. UMTS AKA authentication and key agreement implements on user and operator level. KMS based security solution is a proposed model to secure both entities of IMS network i.e. Operator and User level security. Separation of these entities invokes security concern to network operator and user as well. Mechanism is a different approach. This will be done by implementing security procedure in terms of enhanced authentication, attacks detection and cryptographic analysis. Analysis and results are evaluated on the basis of foresaid protocols and mechanisms.

Satisfaction of success is to delivery of contents with no interception and delay in reception. This comes under a separate service i.e. Quality of Service – QoS. Achievement of good quality in service delivery is done by policy based management. Solution is to set policy on appropriate entities within a network.

List of abbreviation

Lists of abbreviations of subject-specific terminolgy.

2G	2G Second Generation Telecom System
3.5G	3.5G 3.5 Generation Telecom System
3DES	3DES Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project (http://www.3gpp.org).
AAA	Authentication, Authorization, and Accounting
AES	AES Advance Encryption Standards
AH	AH Authentication Header
AKA	AKA Authentication and Key Agreement
AS	AS Application Server 72
BGCF	Breakout Gateway Control Function
CAMEL	CAMEL Customized Applications for Mobile network Enhanced Logic 73
CDMA	Code Division Multiple Access
CDR	Charging Data Records
CDR	CDR Charging Data Records
CN	CN Core Network
CS	CS Domain Circuit Switched Domain
CSCF	Call Session Control Function
DES	DES Data Encryption Standard
DNS	DNS Domain Name Service
ESP	ESP Encapsulated Security Payload
FQDN	FQDN Fully Qualified Domain Name
GGSN	GGSN Gateway GPRS Support Node
GPS	Geographical Positioning System
GSM	Global System for Mobile Communication
HSS	Home Subscriber Server
I-CSCF	Interrogating-Call Session Control Function
IETF	Internet Engineering Task Force
IKE	IKE Internet Key Exchange
IKE v2	IKEv2 Internet Key Exchange version 2
IKE v1	IKEv1 Internet Key Exchange version 1
IMN	IM Network IMS Network
IMS	IP Multimedia Subsystem
IM-SSF	IP Multimedia Service Switching Function
IP Telephony	Internet Protocol Telephony
ISAKM	ISAKM Internet Security Association Key Management
ISC	IMS Service Control
ISUP:	Integrated Service Digital Network User Part
MD5	MD5 Message Digest Algorithm
MGCF	Media Gateway Control Function

MGW	Media Gateway
MPLS	Multi-Protocol Label Switching
MRFC	MRFC Multimedia Resource Function Controller
MRFP	MRFP Media Resource Function Processor
MTP	MTP Message Transfer Part
NAT	Network Address Tranlation
NDS	Network Domain Security
NDS-IP	NDS/IP Network Domain Security/Internet Protocol
NE	NE Network Entity
NGN	Next generation Network
NIST	NIST National Institute of Standards and Technology
OSA-SCS	OSA-SCS Open Service Access-Service Capability Server
PCRF	PCRF Policy and Charging Rules Function
P-CSCF	Proxy-Call Session Control Function
PDF	PDF Policy Decision Function
PLMN	Public Land Line Mobile Network
PS	PS Domain Packet Switched Domain
PSTN	Public Switched Telephone Network
QoS	Quality of Services
SA	SA Security Association
SAD	SAD Security Association Database
S-CSCF	Serving-Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDES	Security Description
SEG	Security Gateway
SGW	Signaling Gateway
SHA	SHA Secure Hash Algorithm 74
SIP	Session Initiation protocol
SIP-AS	SIP-AS Session Initiation Protocol-Application Server
SLF	Subscriber Location Function
SPD	SPD Security Policy Database
SPI	SPI Security Parameter Index
SPQM	SIP based Proxy Quality of Service Modules
TCAP	Transaction Capability Application Part
THIG	Topology Hiding Inter-Network Gateway
TLS	Transport layer Security
UE	UE User Equipment
UMTS	Universal Mobile Telecommunication Systems
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network

1 Contents

Master of Science Thesis [Network and distributed system] 1
AJMAL MUHAMMAD 1
RAJA SHAMYAEL ULLAH 1
List of abbreviation 4
1. Introduction 9
1.1 Project description 9
1.2 Project objective 9
2 Background 10
3 NGN-IMS Architecture 11
3.1 IMS Vision 11
3.2 IMS architecture 12
3.3 SIP signaling 13
3.4 Service enabler 14
3.5 Presence 15
3.6 Group List Management 15
3.7 Secure service access 15
3.8 Quality of Service 15
4 Case study – IMS in Ericsson 16
4.1 Vision 16
4.2 Ericsson – NGN IMS Solutions 16
4.3 IMS Application Enabler 17
4.3.1 IMS Databases 17
4.4 Call Session Control Function CSCF 18
4.5 Main values 18
4.6 Multimedia Telephony Application Server MTAS 18
4.7 Product introduction 18
4.8 Create new services 19
4.9 Web communication gateway 19
4.9.1 Benefits 19
4.10 Session Border Gateway SBG 19

5 IMS Security Architecture 21
5.1 Access Security 21
5.2 Network Security 21
5.2.1 Network Domain Security 22
5.2.2 Security Policy Database 23
5.2.3 Security Association Database 23
5.3 Security in IMS 23
5.3.1 Types of Threats 23
5.4 Security architecture overview 24
5.5 UMTS Authentication and Key Agreement 25
5.6 Ticket-Based System 27
5.7 Security Description (SDES) 28
5.8 MIKEY – IBAKE solution 28
5.9 DTLS-SRTP 28
5.10 IMS Security mechanism 28
5.10.1 Enhanced Authentication mechanism 28
5.10.2 Enhanced One-Pass Authentication 31
5.10.3 Authentication Procedures 31
5.11 IMS Authentication using Public Key Techniques 33
5.11.1 Security objective 33
5.11.2 Security mechanisms - TS. 33.203. (Viviana Rodriguez) 35
5.11.3 Security analysis 35
5.11.4 Proposed techniques 36
5.11.5 Security mechanism 38
5.11.6 SIM – Session Initiation message flow 39
5.11.7 Analysis 42
6 IMS Security concern 42
6.1 IMS security concern to Network 42
6.1.1 Toll fraud 42
6.1.2 NAT and IPSec 43
6.1.3 Denial of service 44
6.1.4 Network topology 44

6.1.5 Gateway Attacks 44
6.2 IMS Security concern to user 44
6.2.1 Denial of Service 45
6.2.2 User agent application 45
6.2.3 Presence and identification 45
6.2.4 Personal data privacy 45
6.3 Analysis and result 46
6.4 Results 46
6.4.1 Enhanced authentication by using AKA procedure 47
6.5 Security protocol model 47
6.5.1 KMS based security solutions. 47
7 Quality of Service 47
7.1 Introduction 47
7.2 Background 48
7.3 QoS management framework in IMS 48
7.4 SIP based QoS architecture 49
7.5 SIP-Based Proxy QoS Modules (SPQMs) 49
7.6 SPQM Architecture 50
7.6.1 SIP based Quality of Service Monitoring Function 50
7.6.2 SIP-based Quality of Service Control Function: 51
8 Conclusion 53
9 Discussion 54
10 Future Work 56
11 List of figures and Tables 57
12 References 58

1. Introduction

This project is detailed in depth study about future network infrastructure. It is Internet Protocol Multimedia Subsystem under Next Generation Network architecture. In short, it is written as NGN-IMS network. IP Multimedia Subsystem – IMS is a Next Generation Network architecture developed on 3GPP implementation of Session Initiation Protocol- SIP. IMS network is an emerging way of delivering multimedia contents through IP core network as a backbone. In worth, IMS manages multimedia services in form of voice, data, and images. All these services are provisioned through IP core network and Packet Switched Network PSN into a single transmission link. In technical specification, IMS converges and integrates into different types of network, not only internet but also mobile and fixed network. IMS network lies on IP network and primarily supports Session Initiation Protocol - SIP as a signaling system protocol. (Joseph)

1.1 Project description

IP Multimedia Subsystem – IMS is a new and emerging framework architecture for mobile applications developed for multimedia contents. In this Project, we will deal with issues related to Security and Quality of Services in IMS Architecture. In the Security, we will investigate security issues in both user and service provider level with more emphasis on IMS security architecture. Later we will focus on Quality of Service issues in detail.

1.2 Project objective

This project investigates IP Multimedia Subsystem based network in order to study and analyze the security and Quality of Service issues. In IMS security, we will analyze security threats concern to network operator and user. In connection with security, security model will be proposed by using KMS based solution and UMTS authentication key agreement. In practice, security mechanism will be implemented basis on enhanced authentication, flood register attack and authentication by using public key techniques. QoS will be discussed in brief on policy based and service based policy in IMS network. We will wrap up this project with results and discussion on the basis of analysis.

2 *Background*

IP Multimedia Subsystem is an architectural framework uses to deliver multimedia contents. It was primary designed by 3rd generation Partnership Project – 3GPP. IP Multimedia Subsystem is based on SIP by 3GPP and IP protocols by IETF. IMS provides control and charge for services which are being delivered by network operator and service provider. Users can get services through roaming network or home network. 4G LTE- Long Term Evolution standards support packet switching to interconnection with IP ore network. As far as concern with LTE, certain applications are running to support IMS based network. VoLTE is Voice over LTE. CSFB is Circuit Switched Fallback and SVLTE- Simultaneous Voice and LTE. All these approaches are able to provide call setup and data services as well.

3GPP release 6 provisioned internetworking with WLAN to support IMS for IP based network. This support includes in the form of routing identities and registration services.
In 3GPP release 7, supports wire line network in collaboration with TISPAN release R1.1.In this release, AGCP- Access Gateway Control Function and PES- PSTN Emulation service are introduces to fix network to get same services as provided in PSTN. AGCP is bridge network between IMS network and Megaco/H.248 network. AGCP is a SIP user agent to support control functions i.e. P-CSCF. Enhancement to IMS emergency sessions were introduced in 3GPP release 10. Furthermore, in release 11, added simulation services in order to get location information in IMS network. (Project, 2006)

3 *NGN-IMS Architecture*

3.1 IMS Vision

Next Generation Network IP Multimedia Subsystem – NGN / IMS is an international standard. IMS is a framework and support as fixed to mobile convergence. It is migration of circuit switched domain network to IP Packet switched domain network. Hence it is considered as all-IP network. IMS network enables open platforms and open network interfaces for both operators and users. (Group, 2010)

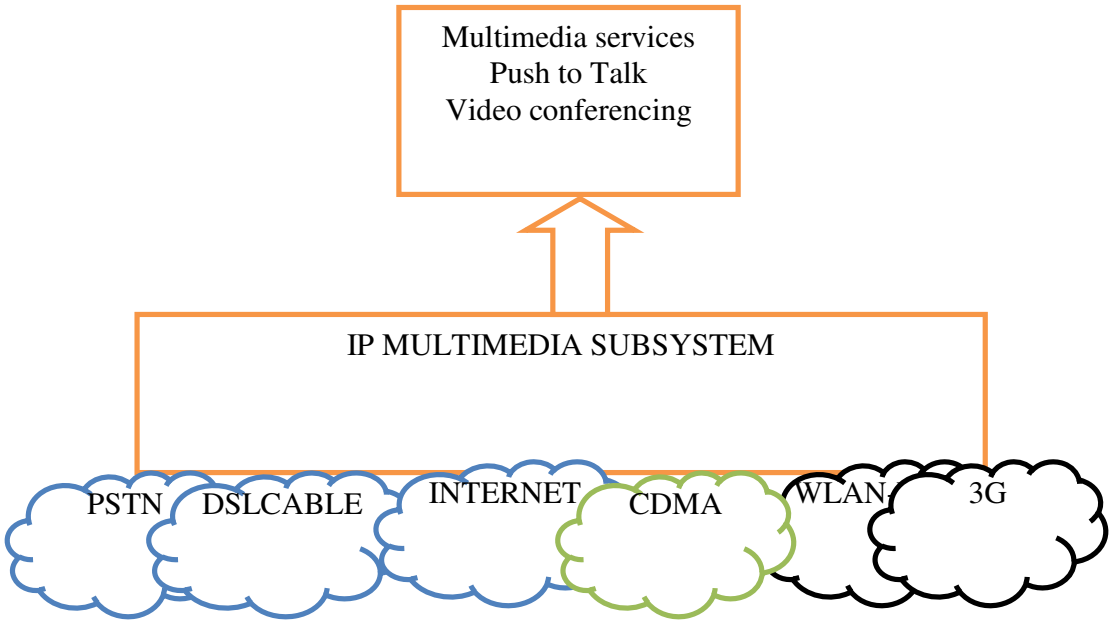

Figure 3-1 IP Multimedia Subsystem – A general overview

IMS provides open network interface and platform. IMS enables functionality to Network operator. This functionality comes under layered architecture with use of service enabler, interoperability, roaming function, billing and security. IMS for user, provides user-to-user and user-to-content communication for multimedia contents as voice and video. In figure 3.1, IMS delivers seamless experience and freedom of access. User is more likely to trade in new terminal and subscribes new services without any restriction of type of service and location specific. IMS provides service enabler for field force automation. It means that services and data can be handled either in the same location or from remote location.

3.2 IMS architecture

Implementation of an IMS network is based on three layered architecture. (Francis, 2010)

1. Connectivity layer

Connectivity layer is composed of routers and switches. It connects access network and backbone infrastructure. In this layer, IP network can use MPLS protocol to allow interoperation in different types of network as PSTN.

2. Control layer

Control layer controls specific control functions. This is responsible for session and call setup mechanism, modification, reconnection and release throughout control functions. Hence, this layer contains CSCF- call session control function. CSCF also knows as SIP server or proxies. With due to SIP protocol, IMS is called a SIP platform. SIP server is responsible for delivering SIP functions and operations in order to establishing, describing and terminating of sessions. Control layer contains modules that offer operations and management. It helps in interoperation with different network and access type by using border gateways. It supports authentication and sign-in mechanism.

There are three main types of CSCF- Call Setup Control Function in IMS.

1) P-CSCF

Proxy-CSCF is point for SIP signaling. SIP signaling in proxy service is to compress and decompress SIP messages. It secures SIP messages and offers accuracy in SIP messages. Proxy servers use DHCP protocol which determines location and identity of proxy.

2) S-CSCF

Serving- CSCF operates SIP session for user. These functions are consisting of one or more in a domain. Serving control function exists in home domain and operating as SIP registrar.

3) I-CSCF

Interrogating function operates as inter-domain SIP signaling. Like S-CSCF , exists one or more functions in a domain. In case of more than one S-CSCF control function available then I-CSCF determines which S-CSCF will work as a user.

3. Servcie layer

Third layer in IMS architecture is Application layer or Service layer. This layer serves as server platform to provide value-added service to user. It provides services as VoIP , Presence as SIP application servers.

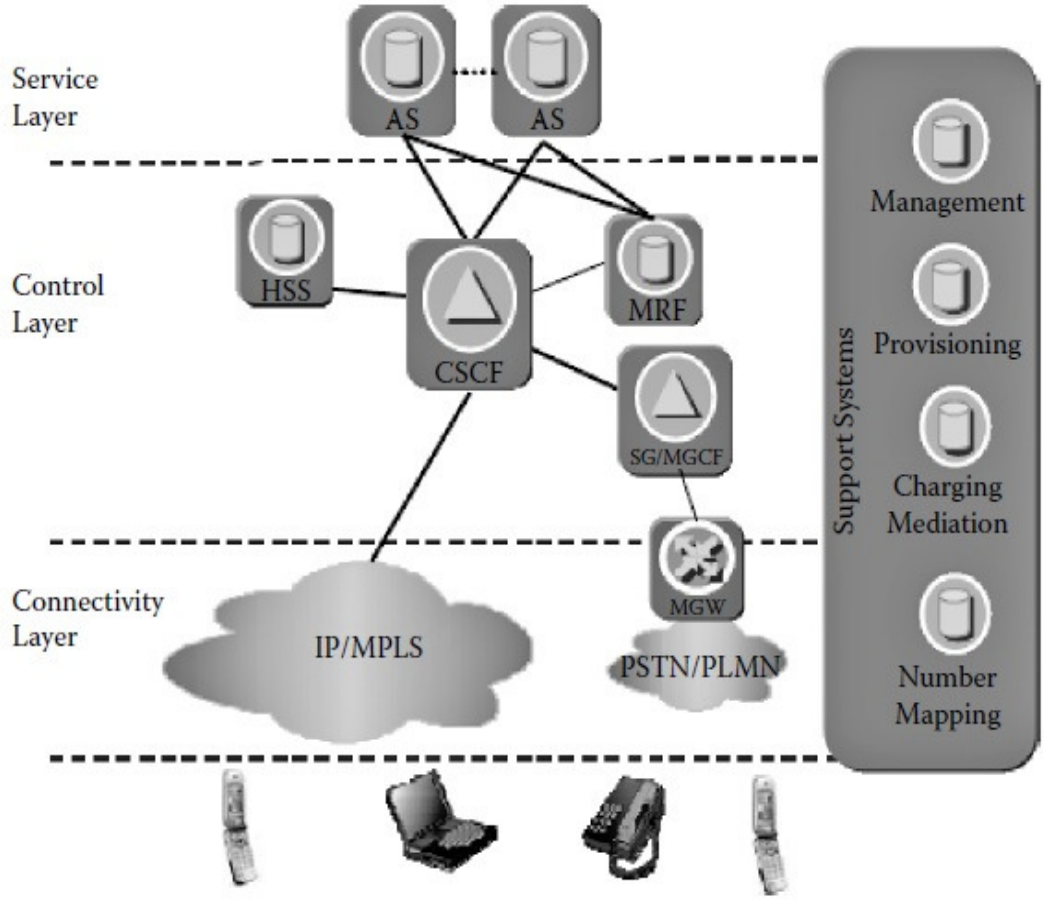

Figure 3-2 NGN IMS Architecture (Francis, 2010)

3.3 SIP signaling

In the IMS, it defines that how services are comprised, routed, requested billing and protocol implementation. It means that application server will support multiple services. These services include as Instant messaging, presence and VoIP application. Software and services can be shared and reuse. (Francis, 2010)

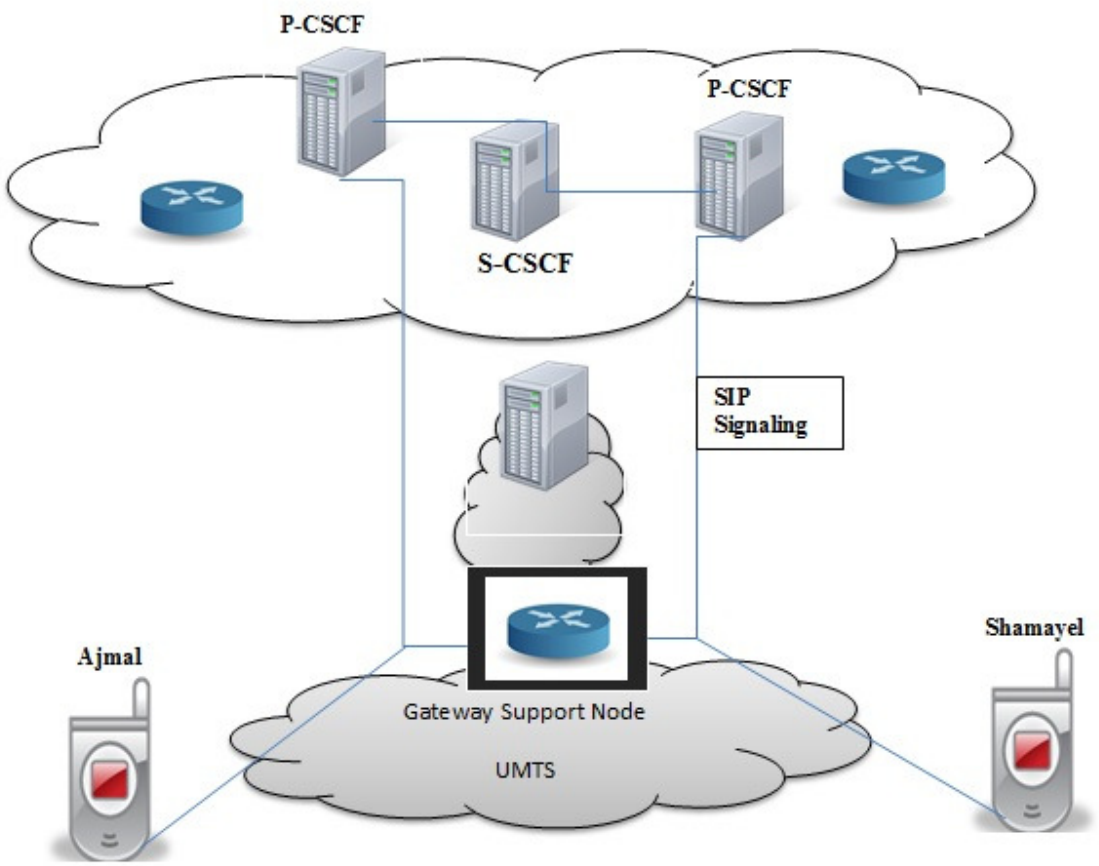

Figure 3-3 SIP signaling

IMS services reduce estimated cost and make more efficient quality-of-service throughout business policy and plan in any type of service provider and operator. To accommodate with increasing number of users, IMS provides combination of different types of services to meet specific user demands. Hence, IMS architecture designed to scale independently of different types of contents and services. In this way, CSCF functions are set in best proportion to match user requirement. The same way, application servers are set up in that proportion to get highest rate of quality in services is used to. Moreover, VoIP services will grow in internetworking capacity while introduce and utilize SIP services.

3.4 Service enabler

IP Multimedia Subsystem is a multiple service enabler or multiple services supporter. Service enabler is all-purpose reusable components for service design and implementation. It means

these are designed at once and then reuse to them many times as per required. There is certain service enabler in IMS network but we will explain to most important ones.

3.5 Presence

Presence is service enabler to provide awareness of availability and communication resource with one and other group members. Hence, users are able to see when a user is active (connected/online) or inactive (disconnected/offline). In addition, users can get alert or notification of when user is online or available. This service enabler is most dominant in social networking media or in IM. This service can set rules that permit to user who can see their presence. Certain modes in difference services are online, offline, away, not available, do not disturb, invisible or set option.

3.6 Group List Management

In group list management service enabler, allows user to create and manage group identification. Group identification facilitates to deploy network services with more feasibly. In group management example includes as personal buddy list, access control list, and public/private groups. Rules are set under personal lists either in group or in contact list.

3.7 Secure service access

IMS applies the sign-in and authentication process to both user and operator to securely access network resources. Authentication is controlled by CSCF functions. Once a user authenticated, user can get all resources at the same time in IMS services for which service a user is subscribed to access. Receiving service request, SIP based application servers –AS is verify to user that user is authenticated.

3.8 Quality of Service

Quality of service infrastructure is relied on policy – based architecture. It consists on service concern policy control to support dynamic QoS control. This guarantees QoS IP transformation in the following indicators as bandwidth, time delay jitter, bit error rate, end to end delay, and data rate.

4 *Case study – IMS in Ericsson*

Ericsson – IMS implementation and operation

4.1 Vision

World wants enhanced mobile experiences to any type of media and devices. In Ericsson, IP Multimedia Subsystem technology, network operators are used to its platform to provide cost effective and enhance experiences to gain profit.

4.2 Ericsson – NGN IMS Solutions

Ericsson provides an implemented solution for NGN IMS network operations. IMS model is based on MGCF – media gateway and SGF are co-linked by a single physical node. Proxy control function P-CSCF is implemented in IMS core node. This node operates in proxy function for request. In access network, this proxy functions are set on separate single physical node on access layer edge. (Amirhassan Darvishan, 2010)

Quality of service – QoS is implemented on access network in BRAS physical node to provide broadband services to user. To promote efficient and freedom of selection services, OSA / parlay nodes are introduce in model to support service creation by third party operators.

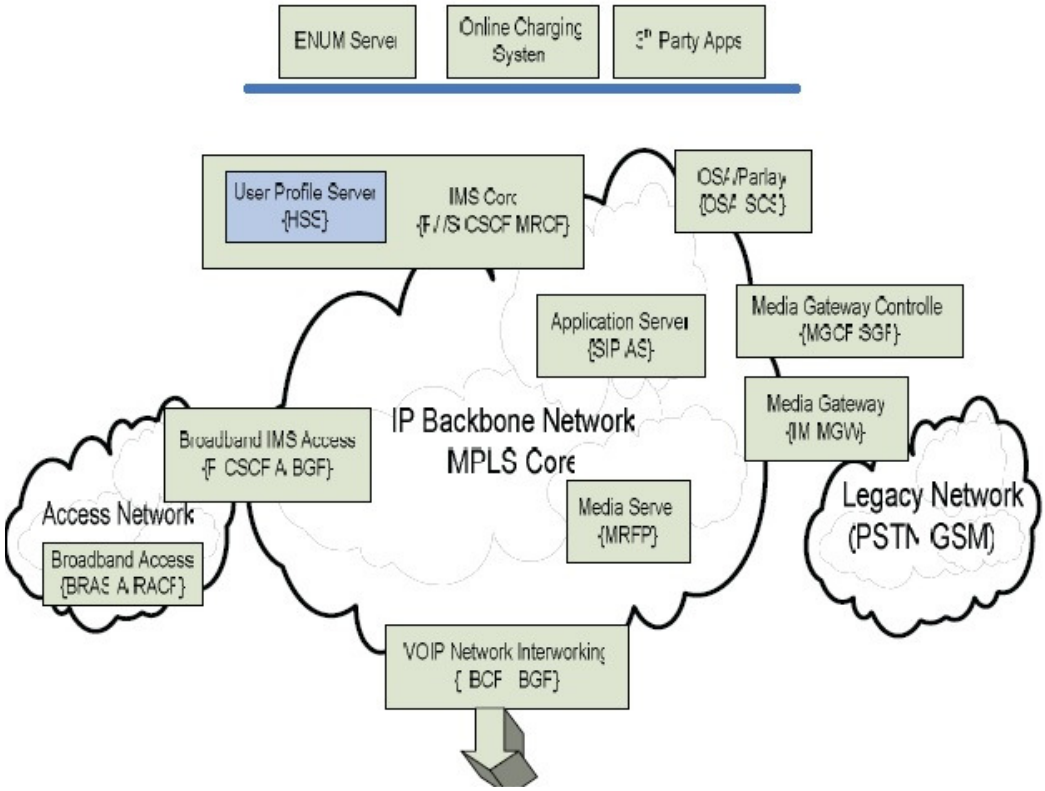

Figure 4-1 NGN / IMS model and solution in Ericsson (Amirhassan Darvishan, 2010)

4.3 IMS Application Enabler

4.3.1 IMS Databases

4.3.1.1 Ericsson HSS

Ericsson Home Subscriber Server is used to manage all the subscription services to the end users. HSS provides authentication as well as authorization functionalities in Ericsson Evolved Packet Core and GAN networks. HSS is based on 3GPP specifications and hence supports the Network control layer with subscription services and handling of sessions. There are various services which HSS provides:

- Authorization of the service
- Authorization of access
- Handling of user identity
- Security of the user
- Profile of the service
- Mobile management

Ericsson Home Subscriber Server is a blade server which is responsible of providing reliability, high availability feature and NEBS level 3 compliance. (Ericsson's "IMS Innovation Platform" for Web Real Time Communications turns any device with a web connection into an open communications device, 2013)

4.3.1.2 Evolving the network

HSS is very flexible, as it can evolve various networks and can manage the finest combination of the packet switched technologies. In general HSS can be easily evolved into the current network while working with home location register nodes. This helps operators to define new services, business and access network types without disturbing their current ongoing business. HSS supports LTE networks as well as IMS networks.

4.3.1.3 Ericsson IPWorks

Ericsson IPWorks provides a centralized placement, arrangement and control of services. It supports various forms of applications and manages Domain name server and dynamic host control protocol services centrally. It can be used in many networks such as mobile and fixed networks in addition to IMS networks. Ericsson IPWorks provides scalability feature in terms of effortlessly expansion of nodes and enhanced network topology. Ericsson IPWorks provides availability and reliability in terms of availability of services.

4.4 Call Session Control Function CSCF

Call Session Control function is the main component in IP Multimedia Subsystem's architecture. This function controls the signals generated from the end users to various networks and services. The service providers use various devices with the ability of VoLTE and RCS to form and provide different services. The operators face tough competition in the market by the new entries, so they have to introduce efficient services in terms of cost and combine mobile and fixed networks. (IMS, 2013)

4.5 Main values

Call Session Control Function is responsible of managing both types of IP Multimedia Subsystems (Fixed, Mobile) while heading towards totally joined telecommunications network. It contains functionalities needed to control the signals and communication generated from the end users with the various networks.
Call Session Control Function has various offerings described below:
Smooth transition from circuit switched network to IMS networks and can work in both domains like wired and wireless.

- It is flexible enough to support various IMS services and network situations.
- Presents a wide range of security authentication methods.
- Supports and facilitates with various features such as scalability, availability and HSS geographic redundancy.
- Provides reasonable charging options in order to meet various business prototypes based on prepaid, postpaid, quantity etc.

4.6 Multimedia Telephony Application Server MTAS

Multimedia telephony Application Server and Session initiation protocol application server fulfill all the needs and requirements for the telephony in the huge networks. MTAS is developed to provide voice over LTE with the enhanced feature of multimedia services and joined with Public Switched Telephone Networks. (IMS, 2013)

4.7 Product introduction

The use of the smart phones is increasing day by day due to the provision of enhanced multimedia applications. The mobile and fixed networks have to be joined in order to provide blend of services. Multimedia telephony Application Server and Session initiation protocol application server fulfill all the needs and requirements for the telephony in the huge networks.

MTAS is developed to provide voice over LTE with the enhanced feature of multimedia services and joined with Public Switched Telephone Networks

4.8 Create new services

Multimedia telephony Application Server is a fundamental entity which is used in the process of transition from circuit switched networks to IP based IMS networks for Voice over LTE and access networks. It creates services that meet telecommunication's needs like redundancy in network, up gradation of the applications without any effect on the traffic. MTAS is the Session Initiation protocol server, specially designed for the converged networks. It can be deployed efficiently in terms of safety and speed. It provides various services that fits to any type of media without any need of recreating the services by the vendors. It provides high capacity and meets the standards of IP Multimedia Subsystem MMTel.

4.9 Web communication gateway

Web Communication gateway has an unmatchable design, present with the Session Border Controller and provides protected connections and endwise interworking for the various devices besides Network Address Translation (NAT).
Web communication gateway differs from the session border controller in a way that it permits the devices based on the browser to use the contents and services in the network in a protected

4.9.1 Benefits

- The telecommunication contents and services can be accessed by any device with the basic internet facility.

- The worth of the service provider's network is shown by the provision of the contents and services through internet.

- Application Designer can develop the services with the combination of internet Apps and telecommunication contents. Services are enhanced and are available to the market in a very short time.

- The telecommunication network is responsible of providing maximum security, redundancy feature, charging facility and the contents will be implemented in the cloud network.

- High revenue will be generated by combining Internet Applications and telecommunication service in a secure manner.

4.10 Session Border Gateway SBG

- Session Border gateway is responsible of generating signals and manages media for the telephony, High definition video, voice and RCS contents.

- Session Border gateway is an important component of the Voice over LTE and the similar node is responsible for each and every kind of access with an inclusion of Wi-Fi.

- Session Border Gateway guarantees security in the network, QoS, Network Address Port Translation (NAPT), transcoding and important functionalities for real time communication.

- Encoded media is used such as RTP and MSRP for the access networks which are unsecure. The example of an unsecure Access network is Wi-Fi.

- It is responsible of enabling web communication for the web clients, which are present besides network Address Translation.

- Session Border Gateway can be positioned at the borders of the IMS network.

5 IMS Security Architecture

Security architecture is still in depth investigation that governs at protecting the data , users and underlying networks. In this architecture, users have to pass multi-pass authentication and Key Agreement procedure to gain IMS services. Security is the main concern for all the systems to be under design and implementation. This is considered at a very high priority to design the system enabling security detection and counter measures. In terms of communication system of any form, security threats and attacks have been disrupting the infrastructure and running business at a very high margin for many decades. In NGN- IMS communication system, all security is related to IP based security threats. Briefly, it is the convergence of IP network and Mobile network system. IMS security architecture is categorically divided into two parts, Access security and Network Security. In the access security, associate with the signaling and provides the security among different type of network and UE responsible for the user authentication and authorization mechanism. On the other hand, Network security (Domain) involves protecting the data flow between IMS user terminals and core network part both in inter-domain and intra-domain communication. (A.K.M. Nazmus Sakib)

5.1 Access Security

Access security process authenticates and authorizes the user to getting the IMS network services and components. Sets the policy that concern user is able to get the IMS resources. It begins with the authentication and then to authorize the user, then the next level is to establish the signaling process. It is set up by the UE and P-CSCF that generates the SIP signals. To secure the SIP signal, IPsec is associated at both sides by UE and P-CSCF. On the S-CSCF, it is care taker of authentication and authorization process when it comes to contact with HSS for user specific profile. It is include the authentication, user services, charging and security profile. (33.102, 2011)

5.2 Network Security

Network security is responsible for the rest of communication in terms of secure data traffic in IMS network. It specifies in the domain level, either same or different. Policies and rules are set by the operator or administrator as per requirements. Security measurement and process is implemented by operator or administrator. (V10.0.0, 2011)

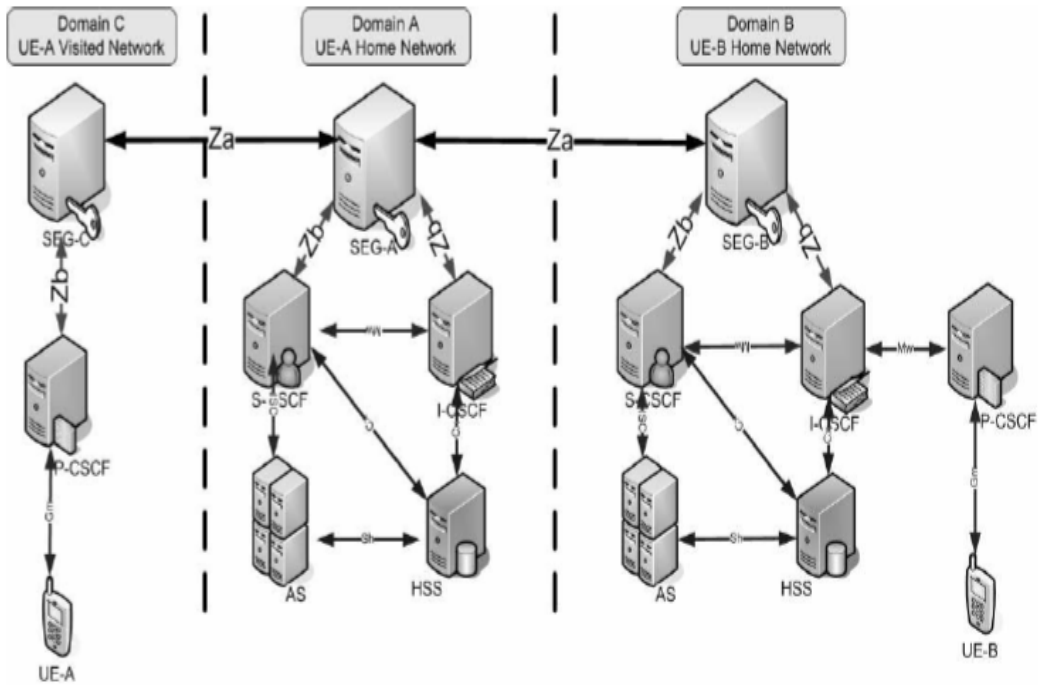

Figure 5-1 Security architecture (3GPP T. 3., 2011)

5.2.1 Network Domain Security

The NDS interfaces are the interfaces which are used for two different purposes. The two interfaces used are denoted by Za and Zb. Za interface configures security among secure domains by following AAA and integrity. (3GPP T. 3., 2011)

On the other hand, Zb interface is used to authenticate the link between the entities within the security domain. The data which passes through a link should not be modified and in this way data integrity is made sure. Cryptographic encryption, data integrity and authentication are implemented between the two security domains in Security Gateway (SEG), and IKE-Internet Key Exchange. When we take Za interface into account it shows that Network Manager is responsible of implementing the security policies within the specific network domain.

IMS also implements and based on the home and visited network architecture. There are two cases in which UE connects to the IMS core. In the first case if the UE is at the home network and in the second case UE is at the foreign or visited network. The location of the UE is denoted by P-CSCF whether it's at the home or foreign network. If the P-CSCF is at the home network it is then UE connected to home network and if it's at the foreign network then UE has to send the registration request to home network, in order to connect to the home network. IMS provides hop-by-hop security according to chained-tunnel model or hub-and-spoke model mentioned in. (3GPP, 2011)

5.2.2 Security Policy Database

Security policy database is the repository which keeps and maintains the policies that differentiates between the traffic coming inside the network or going outside the network, so that only the traffic is transferred to the SEG which has established a pair with the sender SEG and agreed on the specific security parameters. The decision of forwarding a packet is based on the security policies maintained by SPD. The Security policies can be following

- Assign the IPsec services to the packet
- Drop the packet
- Allow the packet to bypass the IPsec services.

5.2.3 Security Association Database

Security association database establishes in between security routers and host-server connected to routers. Data is secured by implementing tunneled links by following security policies in security policy database-SPD. There are specific rules set by security associations to transmit data in the network. These rules are agreed upon all communicating device in order to have secure communication.

5.3 Security in IMS

IP Multimedia Subsystem serves in different form of applications over IP network. Security in IMS based on access and network security. It includes authentication and authorization process. In addition, data protects in between terminals and nodes. As a signaling protocol, SIP is used to transfer and implement IMS services. It means that subscriber and network both will be secure with reference to SIP security. In this order, AKA- Authentication and Key Agreement is used to authenticate subscriber. AKA is an authentication process to be implemented in between subscriber and home network by using subscriber private identity. Main objective of IMS security framework is to provide secure data to all access network with point to point security and subscriber as well. (Christoforos Ntantogian)

5.3.1 Types of Threats

Convergence of internet (IP) with Mobile and Telecommunication network will inherent security issues for IP network. These issues will have a negative impact on SIP based network.
Eavesdropping – Attacker listens or steals SIP messages. Encryption is prevention.
Registration loop hole – Attacker sends Reg message along with stolen ID of subscriber.
Proxy server attack – When fake server gets control all traffic from subscriber.
Message tampering – SIP sends plain messages. This message is not secure and can be accessed.
Denial of Service – Send false request to network which may causes the services temporarily or permanently unreachable or unavailable.

Intensification – With more coverage and sends more false request that is resulting the services disable. This attack is same as DoS but with covering more coverage over network.

5.4 Security architecture overview

In the IMS network, security is implemented to protect SIP signaling by following authorization and authentication mechanisms. In the figure, IMS security architecture explains protection procedure in order to secure associations and links in IMS connected components and devices.

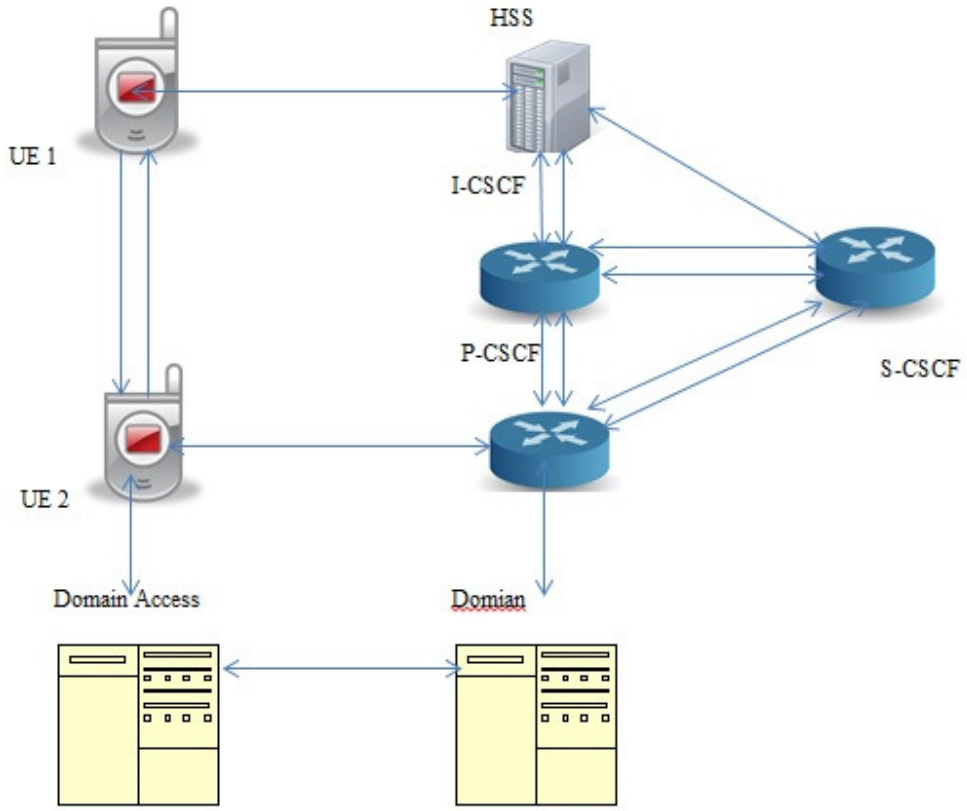

Figure 5-2 IMS secuirty architecture - Overview

According to the figure,

1. User equipment-UE with IMS network both are mutually authenticates. S-CSCF control function in a SIP server will alert by HSS in order to obtain keys.

2. Indeed, as UE is connected via P-CSCF. Both will require securing their association links.

3. HSS and CSCF control functions are connected through Cx. These links will be secured.

4. In the roaming mode, UE needs to create secure link with visited network.

5. Security will implement in between P-CSCF and UE while both are existed in home network.

5.5 UMTS Authentication and Key Agreement

UMTS AKA is an authentication and key agreement is a security system protocol. Security is implemented in terms of authentication and key agreement mechanism among UE and IMS.

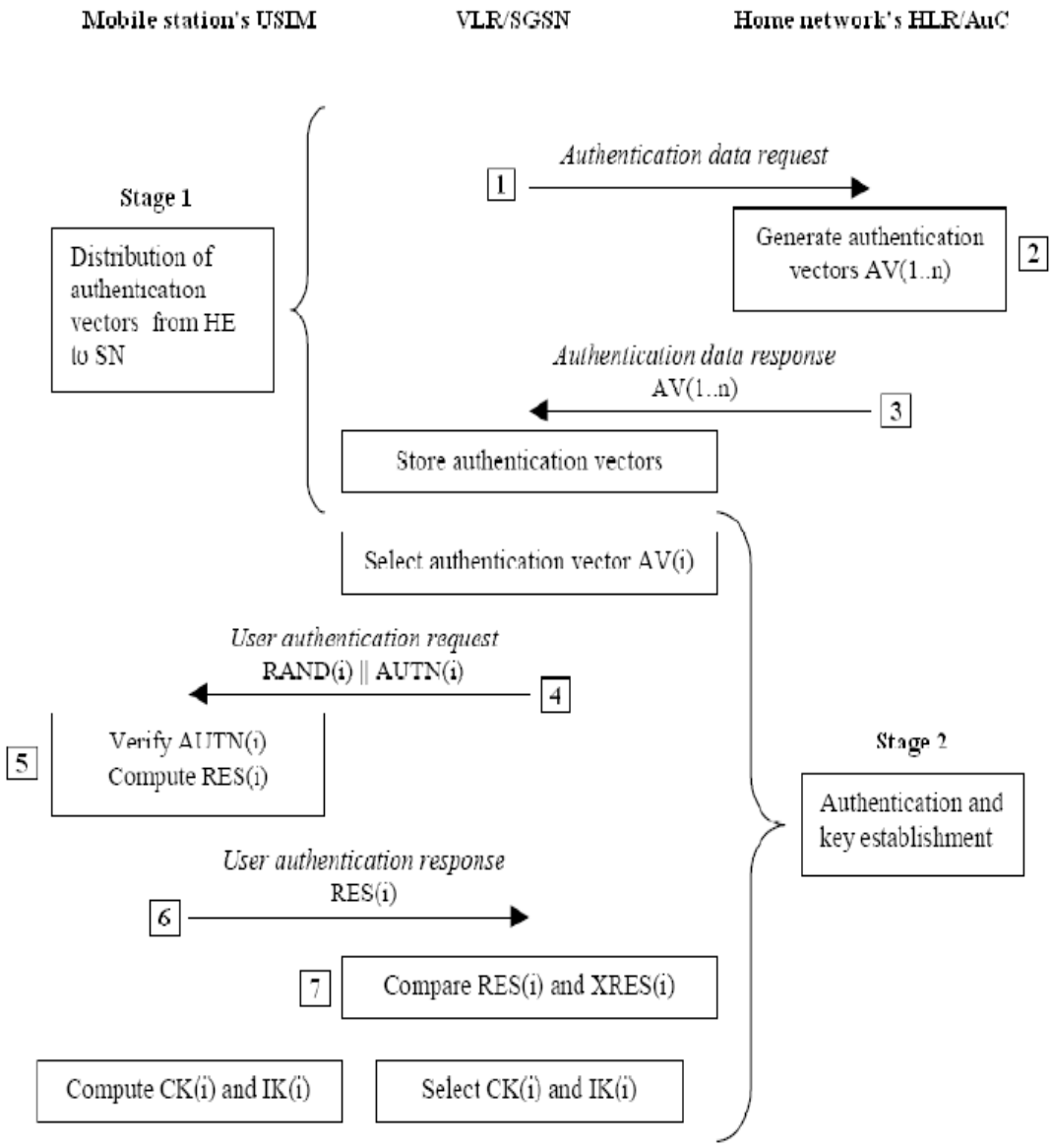

Figure 5-3 UMTS Authentication security system (Chung-Ming, 2007)

Figure as it is mentioned here explains procedure of authentication by following UMTS AKA.

According to procedure, visited network sends authentication data request to home network. Home network sends a set of Authentication Vector (AV) to visited network. Home network then computes an array of AV by using secret key K. Secret key K is located in home network and UE.

Home network responds and send (n) authentication vector to Visited network. AV arrives to visited network, it selects one (1) and sends challenge request by sending back RAND and AUTN fields. UE computes value AUTN by using secret key (K). In the last, UE generates RES and send to visited network and to compare XRES response from UE.

In this scenario, attacker cannot steal secret key while listening the transmission. Reason is that, the secret key is not transmitted. (33.102, 2011)

5.6 Ticket-Based System

Ticket based system is standardized by IETF similar to the Kerberos security system. Scope of TBS is to deliver and identify keys (secret) in IMS network. MIKEY is an exchange protocol uses to deliver ticket. TBS security system provides scalable solutions to counter measure several security concern issues. In the MIKEY modes, KMS supports security to protected and unprotected tickets in IMS network. Key Management Service is based on peer negotiation.

In KMS, key information is associated with communication media and ticket. This service stores record of all keys are implemented to protect media. The key management server needs to allow secure communication between user and KMS. This is done by mutual authentication. Here is a brief scenario explains how TBS works with KMS.

1. Ajmal´s UE initiates a connection with KMS based protocol.
2. Ajmal´s UE requests a ticket and key.
3. KMS responses and generate ticket and key.
4. Shamayel´s UE receives INVITE that includes ticket from Ajmal´s UE.
5. IMS network (components) detects INVITE message and classifies if this message is authorize then send it to KMS. Here it will receive a key in a plain text.
6. Shamayel´s UE is associates with KMS with help of MIKEY exchange protocol. Hence, KMS will authenticate user.
7. Ticket receives from Shamayel´s UE includes master key.
8. Here KMS will certify that Shamayel is authorized. This data enclosed in ticket where master key exists.
9. Shamayel will receive master key and data from KMS.
10. In the last, invitation request will be accepted for Shamayel.

5.7 Security Description (SDES)

Session Description Protocol – SDP is security protocol under cryptographic functions and mechanisms for media. SDP explains cryptographic functions (Key) and parameters to secure data streaming. SDP protocol implements on SIP signaling. In IMs network, SDES implies parallel with other security measurements in SIP. SDES guarantees to secure SIP transport layer. In SDES security solutions, keys are enclosed in SIP message. In SDES, users are communicated as briefly explain here in. Ajmal and Shamayel establish a SIP session. This session starts with using SRTP protocol with mutual sharing of crypto keys. Ajmal will envelop crypto key in SIP message for securing media. Hence, Shamayel will also enclose a key in message to secure media on both ends.

5.8 MIKEY – IBAKE solution

MIKEY Identity based Authentication Key Agreement – IBAKE is a security solution protocol proposed by 3GPP in TS 3GPP 33.828. This involves in plain media security. Security implementation is based on crypto keys as identity encryption. Mechanism is based on three-way crypto key exchange in media to get mutual authentication. In MIKEY – IBAKE, KMS involves generating and sharing the key.

5.9 DTLS-SRTP

This protocol set up parameters and algorithms to implement SRTP protocol. This protocol provides point-to-point security. This follows same patter in which users and components will mutually authenticate in that case if trusted peers can establish a connection. Instead of known peers, it provides secure communication between unknown peers with usage of certificate. This includes fingerprint of certificate in SIP message to avoid Man-in-the-Middle attack.

5.10 IMS Security mechanism

5.10.1 Enhanced Authentication mechanism

Next generation network is responsible of delivering many fresh contents and services through various access networks and therefore enhances the security problems. The data has to be protected which passes through the various access networks. A novel security mechanism is going to be developed which will provide the safety to the mobile users and the data being transferred from one network to another. The security mechanism under study makes the user of the Wireless LAN to go through the multi-pass authentication to be successful in gaining the access to IMS services. The security mechanism is composed of the three major steps of the

authentication process. Firstly user has to perform the Extensible Authentication Protocol (EAP-AKA) to register himself on the domain of the Wireless LAN. Secondly the user has to perform the Internet key Exchange Version 2(IKEv2) protocol to encapsulate EAP-AKA and then the user automatically registers on the domain of mobile network. Thirdly user uses session initiation protocol and performs IMS-AKA procedure to register him on the IMS domain. We can notice the two times usage of the EAP-AKA and the introduction of the overhead of authentication by performing IMS-AKA procedure. (Ntantogian, 2007)

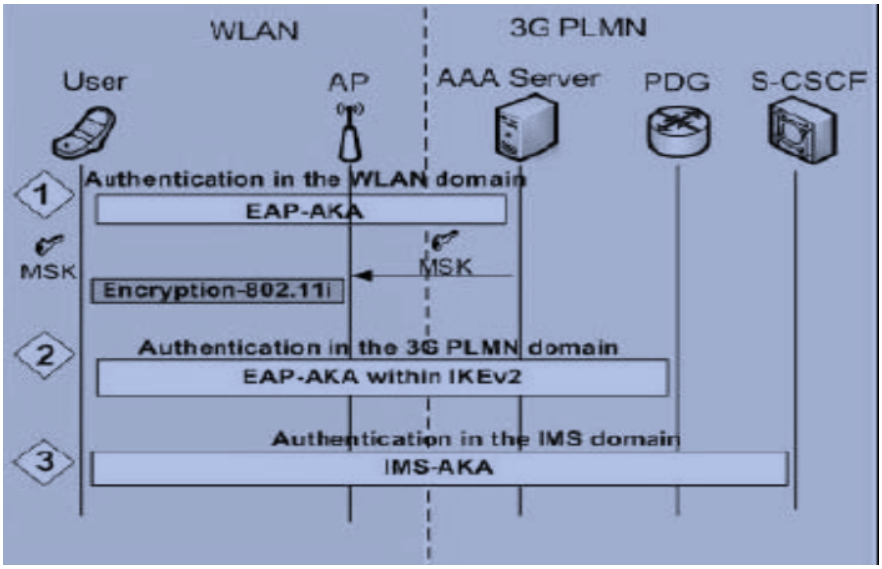

Figure 5-4 Multi pass AKA in IMS (Ntantogian, 2007)

The multi pass authentication procedure presents an overhead of authentication through dual implementation of IP Multimedia Subsystem-AKA and Extensible Authentication Protocol-AKA. An overhead is linked to various things:

- The user's authentication procedure is interrupted due to the interchange of messages. This mostly happens in the scenario where users are situated far from the home network and use the resources concerned with radio.

- The limited power and computational resources of the mobile nodes is used by the computational processing and the provision of Quality of Service to the users may be effected by using Multi-Pass authentication procedure which worsens system level performance largely.

Preliminary Authentication for Registration in the Wireless LAN Domain:

- Extensible Authentication Protocol-AKA is a user authentication protocol. Many entities are involved in this step of authentication like Access Point (AAA Wireless Client) and (Authentication, Authorization, Accounting) server which is situated at the network of service.

- AAA server gets the authentication data from the Home Subscriber Server/Authentication Center based in third generation PLMN. The user's subscription is done at the HSS/AUC according to the user's IMSI (International Mobile Subscriber Identity).

- Extensible Authentication protocol-AKA MK (Master key) is shared among the user and AAA (Authentication, Authorization, Accounting) server after the implementation of an Extensible Authentication Protocol-AKA. The EAP-AKA and Master-Key (MK) is the implementation of EAP-AKA procedure for the fast reauthentication and creates security keys.

- The Master key (MK) is used by user and AAA Server to produce the Master Session Key denoted as MSK. The Master Session Key is transferred to the Wireless Access Point. Wireless LAN session keys are produced by the user and Wireless Access Point using Master Session Key. Wireless LAN session keys are responsible of providing security features and services.

- When the Extensible Authentication protocol-AKA is implemented successfully, then the user gets a local IP Address to implement IKEV2 protocol.

Second level of an authentication for registration in the 3G mobile domain:
In the second level of an Authentication IKEV2 protocol is implemented by the user and PDG (Packet Data Gateway). Packet Data Gateway is situated at the Third Generation mobile netowrk. IKEV2 protocol is used for encapsulating EAP-AKA protocol to successfully authenticate the user and the Third Generation PLMN. The Packet gateway forwards the IP Multimedia Contents requests by the user to the network responsible for the user's requests. There are two phases in which IKEV2 protocol is implemented:

- In the phase one two way IKE-SA(IKE Security Association) is created by the user and the Packet data Gateway. The two way IKE-SA is responsible for the safety of all the following IKE messages.

- In the phase two IKEV2 messages encapsulates Extensible Authentication Protocol-AKA for the joint authentication, which is implemented by the user and AAA server.

- The Diameter protocol is used by the Packet data gateway to transfer Extensible Authentication Protocol-AKA data to AAA server and Packet data Gateway authenticates to the user on the basis of its certificate.

- Remote IP Address is obtained by the user from the Packet Data Gateway to enter IP Multimedia Subsystem.

Third level of an authentication for registering IMS domain:
In the third level of an authentication, IP Multimedia Subsystem-AKA protocol is used for authenticating the user and IP Multimedia Subsystem to each other. Session Initiation protocol is used in IP Multimedia Subsystem network. IMS consists of three kinds of CSCF's:

- Proxy-CSCF function is placed in the foreign network and forwards the users Session Initiation protocol data to their specific home networks.

- Serving-CSCS function is situated at the user's home network and talks with HSS and AUC center related to the reception of the IP Multimedia Subsystem Subscriber data, authentication data and contacts various servers to attain value added contents.

- Interrogating-CSCF function picks a serving-CSCF for the specific user.

The authentication overhead means:

- The interchange of the messages between the users when they are away from their home network delays the user's authentication.
- The limitation in the available energy and the computational resources in the mobiles will be consumed by the computational processing. In this case, quality of service and performance of the system is compromised by multi-pass AKA protocol.

5.10.2 Enhanced One-Pass Authentication

Authentication of user and wireless LAN is performed by implementing EAP-AKA protocol. The MK key is being produced and saved by the user and AAA server. Encryption algorithm is chosen by PDG when receives MK key from AAA server. In the next step the user authenticates himself on the third generation PLMN by performing IKEv2. IKEv2 ignores EAP-AKA encapsulation. MK key authenticates the two end points. S-CSCF verifies the IMPI and IMSI being received by the PDG and then authenticates to user. The third step of authentication is not required. The user has to produce a local IP address before the EAP-AKA procedure finishes in first step of authentication. The PDG must be responsible of modifying the Session Initiation protocol messages and keeping the user's MK key within the life time. IPsec tunnel is created beforehand between the PDG, AAA server and between the PDG, S-CSCF.

5.10.3 Authentication Procedures

As we have seen that in the initial first step, EAP-AKA protocol is performed to authenticate user and wireless LAN. The user produces a local IP address before the first step of the authentication fully completes. Therefore, initial steps of the authentication are combined, as the first phase of the second step of authentication is performed by user and the PDG. The user has to provide its identity (EAP) which involves the fixed and temporary IMSI identity to the AAA server when the wireless access point requests for the user's identity. Then AAA server verifies

whether the identity contains the 3G Authentication vector, which is saved form the earlier authentication with the specified user. If the AAA server doesn't find third generation authentication vector then it forwards the user's IMSI to the HSS/AUC and gets 3G authentication vectors. The third generation authentication vector is composed of the Random challenge-(rand), Authentication Token-(AUTN) , Integrity Key-(IK) and Key of encryption (CK). The MK key is being computed by the AAA server. Encryption key, integrity key and the user's identity are used by the AAA server. Message Authentication Code value (MAC) and (MACserver) are calculated by the AAA server, in order to check the integrity of the next message regarding EAP-AKA (Request of EAP/challenge of AKA). The AAA server is responsible of sending the (Request of EAP/challenge of AKA), which is composed of RAND, AUTN and (MACserver). AUTN payload is checked by the user by performing the UMTS-AKA algorithm. The MSK key is generated when the user produces the integrity and encryption keys and calculates the MK key. The user is successful in generating a response to challenge denoted as SRES, when the MACserver value is verified. The DHCP server is responsible for the provision of the basic IP configurations to the MT in the form of a default outbound proxy (P-CSCF). AAA server receives the message (EAP/challenge of AKA) from user which contains SRES, Id of the user, SAil, Kei1, Ni and MACuser. Sai1 is the combination of the cryptographic algorithms for the IKESA, which is supported by the user. Kei is the value of the Diffie-Hellman. Ni is the representation of the nonce. The nonce helps in the protection against the replay attacks. The MACuser value is being verified by AAA server and AAA server again ensures the received user's response to the challenge (SRES) equals with the response from the third generation authentication vector. There is an entry of the IKEv2 here. If the verification by the AAA server is successful then the AAA server uses a previously created IPsec tunnel to forward the identity of the user along with the MK key accompanied by SAi1, Kei1 and Ni towards the PDG. In the response, PDG sends the chosen encryption algorithm SAr1, Ker1 and Nr to the AAA server. The AAA server gives response to the user by sending an EAP success message with SAr1, Ker1 and Nr and on the other hand send MSK key to the wireless access point. Fast re-authentication is performed by the user and AAA server by keeping the MK key. The user and the wireless access point have a common MSK key. The merge concept has minimized denial of service attacks because PDG accepts the data only from the users who are connected with PDG through the IKE_SA tunnel. IKE_SA is responsible of providing protection to the all shared messages between the user and PDG.

The user and the PLMN are authenticated by performing IKEv2 in the second step of authentication. The combination of the first and the second steps of authentication create a VPN tunnel. PDG executes the third step of authentication and receives the IMPI and identity of user from the user. In this way the second step of authentication and the third step of authentication are combined. The user sends a message to the PDG which includes user's identity, SAi2 payload, traffic selectors (TSi,TSr) and configuration payload request(cp-request). The PDG in response authenticates the user, by recovering the MK key for user identification and validates the AUTHi payload in order to user authentication. If the verification of the AUTHi payload is successful then the PDG recovers the IMSI of the user by contacting the security policy data of the IPsec protocol. The recovered IMSI of the user is included in the session initiation protocol registrar message and forwarded to the S-CSCF. S-CSCF is already composed of the saved identities of the users and when it receives the Sip registrar message, S-CSCF forwards the message to the HSS/AuC. The HSs/Auc recovers the IMSI user's identity and is denoted as

IMSIHSS. The HSS/AuC is responsible of sending the IMSIHSS to the S-CSCF and then S-CSCF verifies that IMSIHSS=IMSI and sends the message saying OK to the PDG. If IMSIHSS is not equal to the IMSI then user is not able to register to the IMS. The PDG creates the AUTHr payload by calculating MAC over the second message of the IKEV2 and send a message to user, which is composed of identity of the PDG, traffic selectors, SAr2 payload, Remote IP address in the response of the CP and an Ok of the IP Multimedia Subsystem network. User in response authenticates PDG by following MK key. The user authenticates to third generation PLMN and the IMS network.

The level of the security is maintained by decreasing the authenticating messages. Decreasing the authentication messages means an automatic decrease in the authentication cost and time. The enhanced one-pass authentication protects against the denial of service attacks on the Next Generation Network.

5.11 IMS Authentication using Public Key Techniques

In the previous chapter we discussed Key Agreement standards. Here we will describe in detail structure of IMS AKA mechanism.

5.11.1 Security objective

In the IMS architecture, a solution for authentication and access exists. This is technically drafted in 3GPP TS 33.203. There are five security requirements to secure IMS network. (Viviana Rodriguez)

1. Secure link in between UE and P-CSCF control functions.
2. Mutual authentication
3. Ensures security to HSS.
4. Secure P-CSCF with outside network.
5. Secure CSCF.

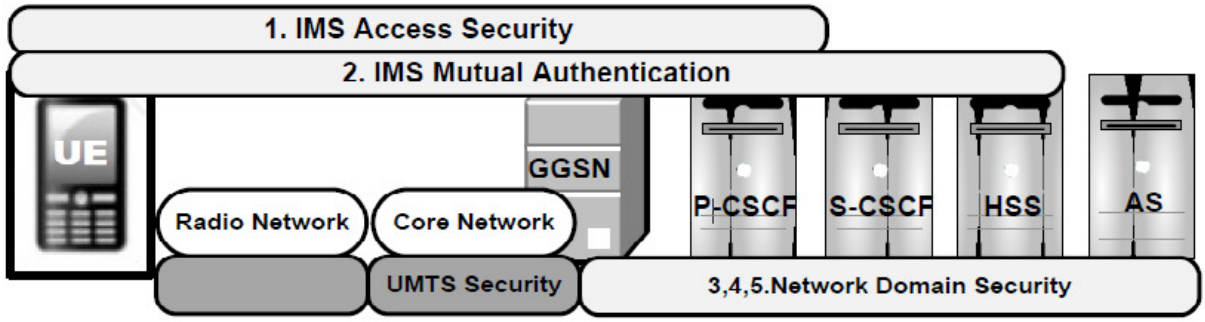

Figure 5-5 IMS Security

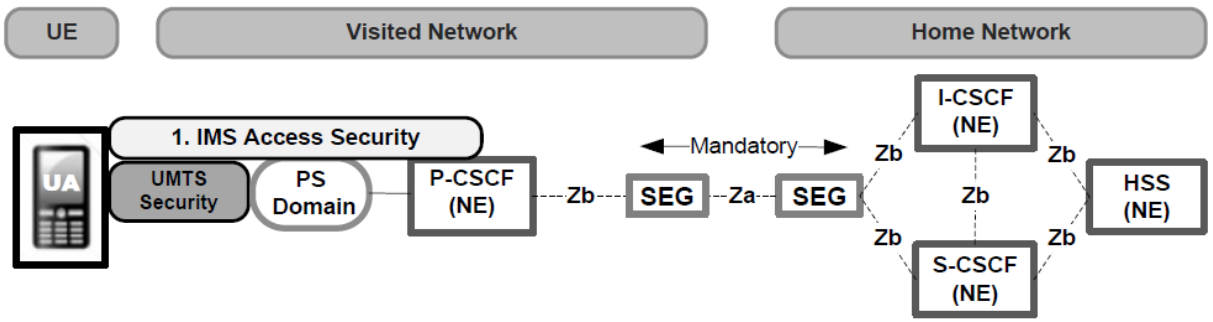

Figure 5-6 Network Domain Security (Viviana Rodriguez)

5.11.2 Security mechanisms - TS. 33.203. (Viviana Rodriguez)

Security mecanisms	AKA-authentication	IPsec ESP	IPsec IKE	SIP	TLS	SIP TLS
IMSA MA	YES	-	NO	YNA	NO	YNA
IMS AS	NO	YES	YNA	-	YNA	YNA
NDS	NO	YES	YES	-	YES	-
AUTC	NO	YES	YES	NO	YES	YES
AUTI	NO	YES	YES	-	YES	YES
PSK	YES	YES	YES	YES	YES	YES
PKI	NO	NO	YES	NO	YES	YES

IMSA MA – IMS Mutual Authentication
IMS AS – IMS Access Security
NDS – Network Security
AUTI – All User Traffic Integrity
AUTC – All User Traffic Confidentiality
PSK – Pre Shared Key
PKI – Public Key Infrastructure
YNA – YES , but not access 3GPP network

Table 5-1 Security Mechanism (Viviana Rodriguez)

5.11.3 Security analysis

There are three security vulnerabilities found in IMS AKA schema. (Viviana Rodriguez)

5.11.3.1 Denial of service DoS

Denial of service attack intrudes if an attacker sends fake de-synchronizing messages. This process confuses network and increase times of AV vectors.

5.11.3.2 Data manipulation

This attack is done when initial message is shared between UE and IMS network is not transport securely. In this situation, attacker modifies data.

5.11.3.3 Eavesdropping

Attacker gets information and analyzes data during session initialization. Attacker can get user information, requesting services and user location.

5.11.4 Proposed techniques

Techniques are proposed schemes to support security objectives and mechanism. This will help to determine flaws in IMS security specification. In addition, analysis of authentication process will be explained that security mechanism ensures security requirement.

5.11.4.1 Analysis and identification

In order to obtain secure methods, it is a basic requirement to ensure information sharing in IMS network. This can be done by defining which assets are making part of this process. This analysis explains on assets are being used in authentication process.

5.11.4.2 Assets of authentication functions

There are two assets exist in authentication functions.

1. **Technology assets**

Applications

- ISIM application used in UE
- HSS application
- Application on P-CSCF and S-CSCF servers

Servers

- HSS
- P/S/I – CSCF functions

Communication channel
Uses to transport / transmit information asset.

2. **Information assets**

In authentication process, data is the most important asset. This information asset can be managed by implementing 3GPP TS 21.133 technical specification.

Data signaling
These are Identity, address, location.

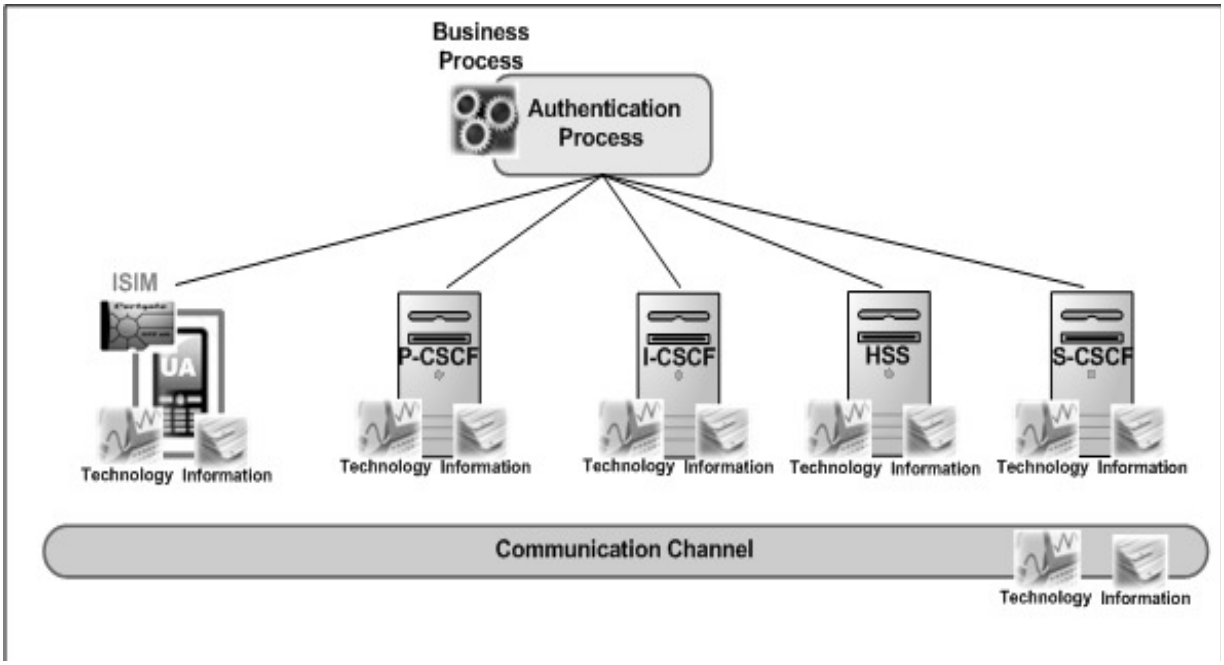

Figure 5-7 Assets from the authentication process

Data control
These are service profile, data for call control, and routing information.

User data
Any type of data is being generating by user in IMS network.

5.11.4.3 Classification of information

Classification of data is based on these three levels.
Public – data is known by entities of internal and external in IMS network.
Internal use – information is known by entities within IMS network.
Secret – Sensitive data. Only is known by authorized entities in network. (Viviana Rodriguez)

RULE	SENSITIVITY
Identity + Security management	Secret
Identity + User profile	Secret
Location + Additional data	Internal use
Public identity + Public identity	Public

Table 5-2 Classification of sensitive data

5.11.5 Security mechanism

5.11.5.1 Cryptographic analysis

Security is based on cryptographic standards. In order to ensure authentication, these are security requirement that will be identified in authentication process. (ETSI, 2009)

1. Mutual authentication.
2. Secret (confidential data) must be accessed by only authorize assets.
3. Assets must be signed in authentication process.
4. End of authentication process, IMS network must provide a secure channel to user.

Cryptographic standards

On the basis of specified security requirement, cryptographic standard supports authentication process in a very good manner.

1. Mutual authentication

Public- key techniques, digital signature, hash functions.

2. Access control

PKI supports confidentiality and integrity. This technique protects message that can only accessed by the authorized entities.

3. Secret process

This is a sensitive process. Digital signature with time stamp is implemented.

4. Secure channel

PKI solution will secure the usage of CK and IK in HSS. Because , HSS depends on cryptographic functions to get random number process.

Technique	Standard
Hash functions	MD5/SHA
Asymmetrical algorithm	RSA
Symmetrical algorithm	AES/3DES
Digital certificates	X.509
PKCS	CMS/ PKCS #7/ PKCS #5
Markup language	XML

Table 5-3 PKI Techniques-Cryptographic standards. (ETSI, 2009)

5.11.6 SIM – Session Initiation message flow

This is a XML scheme to transfer sensitive information. This information is encapsulated. Information is encrypted by the PGP techniques. (Chung-Ming, 2007)

Flow of SIM can be explained in the following steps.

1. User Equipment -UE sends a SIP REGISTER message to P-CSCF. In the parameters, secret data is in XMLSECURE. This data can be seen by HSS.

2. P/I-CSCF deliver message to HSS. Adds digital signature in message.

3. HSS certifies I-CSCF identity and decrypt data as it was sent by UE.

4. HSS sends server name to I-CSCF where it adds digital signature in the message.

5. Then, I-CSCF sends message (as in 2) to S-CSCF by adding S-CSCF name and signature.

6. S-CSCF requests CK and IK generation to HSS to validate IMPI against IMPU sent.

7. HSS sends a secure authentication XML to S-CSCF that has CK and IK. HSS then sends the saved IMPI of HSS to S-CSCF. S-CSCF will verify IMPI and after verification it will send a message.

8. Changing the status of registered user.

9. S-CSCF sends XMLSECUREAUTH to P-CSCF.

10. P-CSCF sends message to UE. This will validate the authenticity of IMS network. If it corrects then it will obtain CK and IK to establish secure channel with P-CSCF.

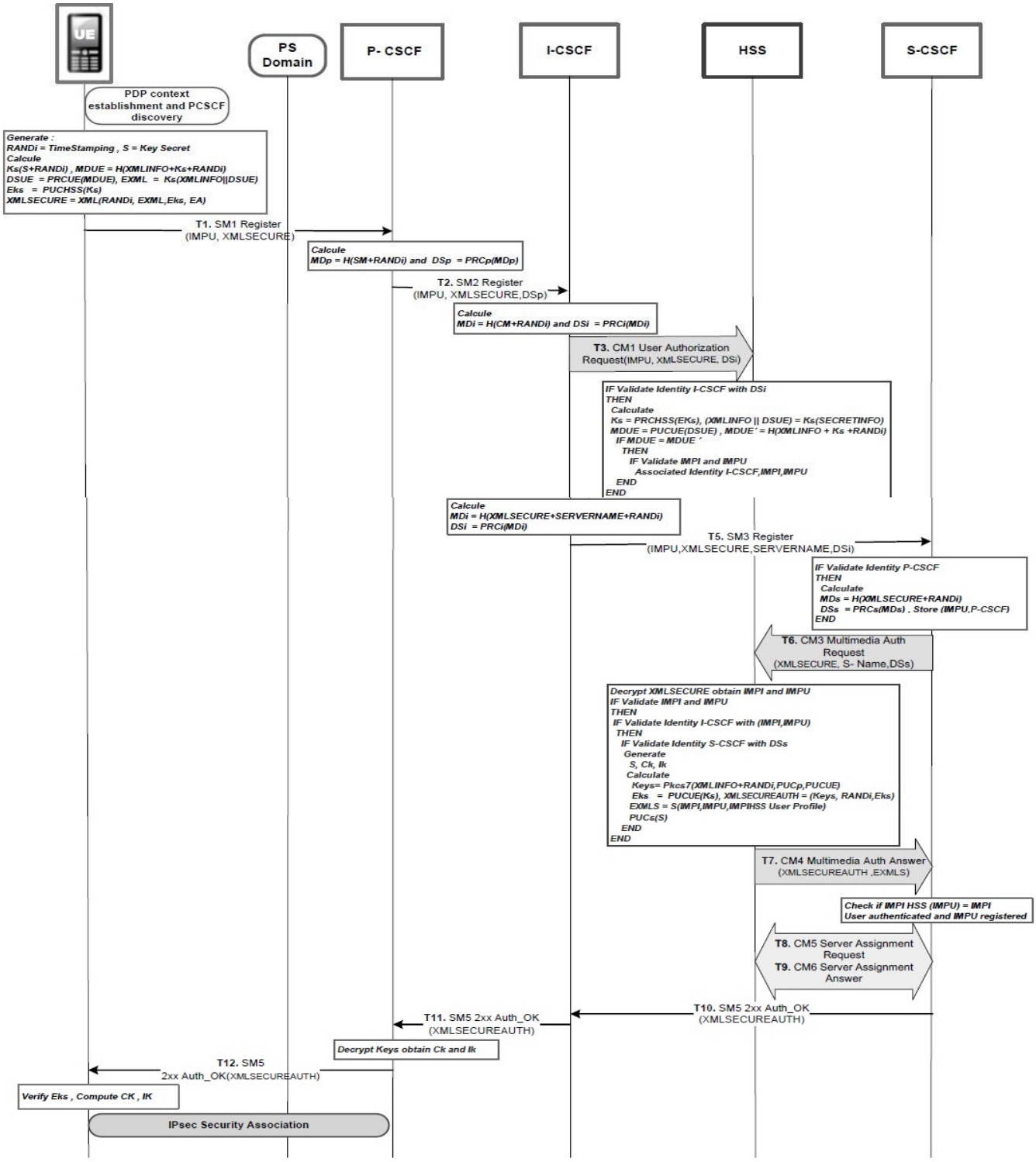

Figure 5-8 Message flow for new security mechanism (Chung-Ming, 2007)

5.11.7 Analysis

IMS services are required to identify entities or components during deployment. These entities are critical assets. Data traffic is passed through these assets. Different types of crypto protocol are implemented to detect vulnerabilities.

Before developing any IMS service or feature, it is important to identify critical entities that are involved, known as critical assets. It is important to verify information that is stored in each one of the assets. We compare below the new protocol, which take into account such aspects, to the vulnerabilities found on the different mechanisms on this paper.

Considering the results of the security analysis the authors identified that current specifications do not take into account security from the operation's transversal point of view, since the proposed requirements and mechanisms are guaranteed independently but not in an integrated way; this becomes obvious in IMS AKA and IPSec. Considering each of these mechanisms separately, one can conclude that they achieve their security requirements. However, security issues are easily found if the whole system is taken into account.

6 IMS Security concern

In this chapter, we will analyze IP Multimedia Subsystem in order to security concern. In IMS network, security is concerned to Network operator and User.

6.1 IMS security concern to Network

Network level security is under threat by applying certain types of attacks. These attacks can be intercept traffic over media and captured private data over network.

6.1.1 Toll fraud

IP Multimedia Subsystem is based on SIP and IP. This provides different mode of signaling paths as with common channel of signaling in SS7. This framework has many benefits. One of them is to allow network carriers to check and modify User Agent (UA) report procedure is in progress. In this type of service, user may intentionally or unintentionally interacts in order to utilize illegal services lead to toll fraud. (Hunter, 2007)

In the meantime, User Agent is developed by third parties instead of a network carrier. In this situation, carrier cannot validate or implement proper security while UA is allowed to access the network as it is required. Cellular mode of communication is based on connection resources as set up by carrier. These resources are signal propagating devices as Antenna or BTS. Carrier verifies data flow and audits to data as per requirement. Loophole starts in IMS. When dual mode phone or devices are allowed to access, traffic is routed through facilities where carrier cannot control it properly.

In case, if UA is connected to internet. User may communicate by using peer-to-peer. In the IMS, HSS (Home Subscriber Services) supports to map UA`s IP address and identify user with the help of SIP REGISTER mechanism. In the call set up phase, caller IP address is assigned to caller to establish data channel. UA acquires an IP address of caller UA and send a CANCEL request to network. Then again establish connection to caller directly by using same voice and data as it was in paid service.

In SIP proxy server (control functions) may also uses to establish a toll fraud. Even though, SIP proxy is used validly in a form of PBX system. Yet so, this can be exploited to share same account proceeding to fraudulent. It is done due to lack of physical location. Proxy server uses SIP redirect response (3xx) to direct data traffic toward UA. UA becomes a proxy server and registers in IMS network. Users share the same account and billing information associate with UA.

Toll fraud attacks may effect on landline and cellular phone as well in many ways. In the landline, VoIP services have different cost and package. In an example, there are unlimited calls to selected countries. Attackers use same method to set up call with having same cost but to those geographical locations where cost or package was not included to call. Toll fraud attacks can make it fake of usage of minutes or holds the constant time.

6.1.2 NAT and IPSec

Network Address translation and Network Port Translation are a mandatory services in field of internetwork communication. NAT supports a level of secure access to centralize and distributes systems. NAT follows the policy that is running in a server or management clients. It limits direct access to host that is behind of NAT and allows internal host (same network) to set up connection with external hosts (different network). In addition, NAT provides management tool to monitor network on the basis from where data is exchanged between LAN connected host and internet. NAT also supports deployment of UA with no authorization of an ARIN address assignment. (Kuhn, 2005)

Authentication Header-AH and Encapsulated Security Payload -(ESP) are used to implement IPsec. These two protocols are applied in two modes as transport and tunnel mode. In transport mode, it secures upper layer protocol in term of only IP header of an IP packet. In tunnel mode, it secures not only link (logical connection) but also to secure full IP datagram. Host and servers are supported by both modes but gateways are securely linked by only implementing tunnel mode on each link and border.

ESP – Encryption Security Payload is an IPsec security solution implement to achieve source authentication, integrity and encryption in IMS network. Security parameters are set in policy database that are depends on security associations.

.

6.1.3 Denial of service

IMS network in many cases are under Denial of service attack by many sources. This type of Denial of Service threat has a very huge exposure in any other type of network infrastructure. One of the threats is to pretend in connection with internet. There is certain way to lessen DoS threats over internet. Reason of high intensity of such a type of threat is that attacker can disrupt the internet-connected host connection or service unavailable with having a sufficient resource. In this situation, attacker can degrade the IMS capable services. On the other hand, one of the main reasons is a full enabled service and configurable UA. This UA opens a door in order to compromise. In an example, user is viewed malicious or infected contented and in further when they are simultaneously compromise may resulting UA`s flooding in IMS with request flooding and service become unavailable or denied for non-compromised user. In a very worst scenario, If compromise UA is an IMS application then it may exploit vector. This situation is even worst case scenario than a Denial of Service attack. (Kuhn, 2005)

6.1.4 Network topology

Network carriers have a very strong concern with their network infrastructure and proficiencies of different services in order to keep them secure, confidential and registered. In security point of view, analysis examines that information in the data or packets can be investigated. In an example, there are in certain numbers of CSCF control function of SIP proxy servers. Packet (voice and video data) is routed through network. Chunk of information can be extracted while investigates their way through route, record-route and pathways header in a SIP packet or signal. In this scenario, it is to do a mandatory step to secure information that is under observation through topology. In order to conceal network topology of IMS network, headers should be encrypted unless or until sends or receives data in IMS gateway.

6.1.5 Gateway Attacks

In the IMS network, gateway or border gateways are perhaps most vulnerable hosts or devices. Reason is due to their existence to public and the role when they are abide to compromise. In more technically , Media Gateway Control Function (MGCF) , Signaling Gateway (SGW) , media Gateway (MGW) are all require certain level of conversion in contents. These contents require to legal manipulation. (Hunter, 2007)

Data is converted to different media. Integrity checks are placed in to verify to these.

- Contents are same content as it as before in different format.
- Resulting data should be considered non-threatening.

6.2 IMS Security concern to user

6.2.1 Denial of Service

Denial of service is a potential attack, which can abandon the service facilities to the legitimate user. IP Multimedia Subsystem provides a collection of conditions which may be helpful in preventing a legitimate user from denial of service attack, but few of the conditions can be countered by the potential attacker.
IMS ensures that user don't fall prey to denial of service attack, buy providing quality of service while delivering the content to the legitimate user. IMS is not concerned with the layer 1 issues for example radio frequency interference or immediate loss of signals, but it ensures that the bandwidth available is provided to the authenticated user. Denial of service attack can take place if the available bandwidth is attacked by an attacker and in this way a legitimate user is refrained from having the available bandwidth. IMS must ensure the safety of the available bandwidth that it only reaches a legitimate user instead of becoming a prey to an attacker.

6.2.2 User agent application

IP Multimedia Subsystem has an important role of providing safe services and application to the legitimate users. IMS deals with the variety of applications, so there is a greater chance of a possible attack on user's and their assets while providing the services to the users. IP Multimedia Subsystem has an objective to open carriers for providing the third party services or applications to the users, as the rewards for providing the third party services are very high. The provisioning of the third party applications opens a door for an attacker, as there may be unsafe content coming from some of the dishonest service provider's.

6.2.3 Presence and identification

The major concern to the user is regarding the safety of his/her data. The variety of applications which IMS provides creates a major concern regarding the successful provision of the services to the legitimate user, as it poses a threat on user's asset and data as well which passes through the user's system. IP Multimedia Subsystem also enables the services which enforces social networking concept on the architectural level i.e. IMS creates the different groups like friends, family etc. that can have an access to the presence or available data and notifies these groups regarding the attributes of the legitimate user. The attributes of the legitimate user include various information regarding the user's location, status and availability. The groups are not created on the per user basis, but maintained by the IMS, so that user may think that these groups are working while being assigned to any of the user. (Rosenberg, 2004)

6.2.4 Personal data privacy

As we know that users are sharing their data on the internet. The data reaches from one country to another and is not location limited. The diverse location of the data brings many challenges regarding the safety of the data. The research is going on related to the concerns regarding the privacy of the location data. There is a group called GEOPRIV in the IETF which is doing research on the standards for the privacy of the location specific data. Most of the users have employed the global positioning system, in order to share the location. Apart from the users, the carrier also employs the location service which is the core enabler of an IP Multimedia

Subsystem. The implementation of the location service by the carriers is bt slow, as carriers are concerned with the right mix of the contents with respect to the demand and availability. The IP Multimedia Subsystem ensures privacy by distributing the standardized data between the services providers and users. IMS also allows the third party services to use the standardized data and make sure that the preferences of the users are kept in mind.
The other concern to the user is related to the encryption (Voice, data) of the data. The encryption of the voice and data becomes very complex due to the mismatched regulations. Many complex schemes of encryption have come in the recent era that implement encryption by using the Voice over IP architecture for the exchange of a key and allows the users to encrypt the transmissions of their data. On the other hand, the user has limited CPU and battery power to manage the encryption of the voice and even if it is successful then it can fall into the wiretapping while implementing the malicious regulatory requirements. IMS should manage the encryption of the data performed by the user and ensure that it is not the malicious user trying to copy the legitimate user. With Carriers must also compete with the malicious user trying to change the original data. Their party services developers may encrypt their data between the legitimate users and their services without giving access to the carrier for example medical data and social security numbers.

6.3 Analysis and result

In this project, we have a deep analysis basis on IP multimedia Subsystem architecture- IMS in terms of network and data traffic security. Threats are concerned to network operator and user as well. We have shown that how IMS based network enables selection procedure for different types of network during registration and call control.
It is always a very important to detect critical entities while to deploying a network service in an IMS network. These critical entities are investigated in 3GPP security requirement support to IMS network architecture. KMS based security solutions enable developer to develop more security in services for network and user as well in the same manner. Negative aspect of KMS is expensive to implement. In the other side, SDES and DTLS- SRTP are more flexible to apply the security in running IMS network. Developers can add services by modifying or reuse the module at the same cost.
Security in IMS network deals with authentication mechanism while it is used in registration process. We presented different techniques to overcome issues related to authentication. In one-pass AKA authentication, enhanced one-pass reduces DoS attack. This is done by merging mechanism of authentication by reducing authentication message.
Detection process against DoS attacks in an IMS network is based on adaptive algorithm. This is CUSUM z-score. CUSUM detects performance against flood attacks. It detects false alarm rates, detection delay and detection time.

6.4 Results

Results are carried out on the basis of analysis and investigation of authentication process and threats in IMS security architecture. We proposed a security model. This will have a deep impact on security requirement and implementation.

6.4.1 Enhanced authentication by using AKA procedure

It is achieved that authentication signaling and associated overhead can be reduce by using mulit-pass AKA and one-pass AKA procedure. User registration in IMS under multi-pass AKA involves in the sharing of four SIP message among user and p-CSCF and two messages between P-CSCF and HSS. Hence, multi-pass AKA requires total of six messages to user registration process. In the same manner, one-pass AKA involves in sharing of two SIP message between P-CSCF and user and two messages among P-CSCF and HSS. Hence, one-pass AKA requires two or four message for user registration in IMS network.
Reducing to authentication overhead reduces processing time, and energy cost. It reduces network resources as well. In this scenario, one-pass AKA uses less authentication vector as compared to multi-pass AKA.

6.5 Security protocol model

6.5.1 KMS based security solutions.

MIKEY-IBAKE, Otway-Ress and TBS are in minor differences but are considered as KMS based solutions for security. All are scalable security solution that is implemented on IMs plane media. All have the ability to handle complex security environment. Keys are unique, hence not possible to replace them with fake one. In KMS based security, network establishes mutual authentication connections. It permits as per user policy by holding secure connection and key control. All three types of attack can be prevented by using these security solutions.

7 Quality of Service

7.1 Introduction

In the recent era, technology has advanced in a fast pace. The demands of people regarding communication are increasing day by day. Nowadays preferences of people have changed and they not only want to communicate through text or voice call, but also add multimedia contents in their communication. These preferences of people are met by IMS (IP Multimedia Subsystem), by providing the blend of voice, data and multimedia communication.

Large number of packets is exchanged continuously on the internet and each user demands reliability and Quality of Service in communication. The IP Packet Switching network is based on reliable and efficient delivery mechanism, but it is very difficult to implement Quality of Service mechanism on it.

Many standard organizations like 3GPP (3^{rd} Generation Partnership project), IETF (International Engineering Task Force) and more have developed policy based Quality of Service for IP based

Packet Switching Networks to counter communication problems, service providers facing while operating Next Generation Networks. (Bo Yu, 2010)

7.2 Background

The policy based Quality of service refers to the policy which is defined by various service providers to control and manage the quality of the service delivery in an application layer. The policy is defined according to the type of the business, but it is not mandatory for the service providers to be familiar with the detailed description of the network.

In IMS, Quality of Service is guaranteed by implementing policy based quality of service and is accustomed to provide Dynamic Quality of service. (3GPP, 2009)

The policy based Quality of service architecture allows service providers to provide reliable and best service in terms of quality according to the factors i.e. (bandwidth, data rate, jitter etc.).
IMS session layer interacts with the IP layer to control the quality of service of data.

7.3 QoS management framework in IMS

IMS networks are the converged networks combining multimedia contents to enhance quality of service in the next generation mechanism. IMS has a unique quality of service framework in terms of providing quality of service for the multimedia contents. The QoS management framework is described as follows:

i. The QoS management framework in IMS employs DiffServ and MPLS techniques to provide assured quality of service while delivering multimedia contents.

ii. MPLS and DiffServ has two different roles:

iii. MPLS plays a role of providing different routing methods and improved network resources to ensure quality of service in delivering multimedia services.

iv. DiffServ is responsible of providing systemized quality of service methods to ensure quality of service from one end to another.

v. The quality of service mechanism also provides quality of service for the users who roam around from one network to another.

Various models have been developed in order to authorize the above mentioned approach of providing quality of service while delivering multimedia services. This approach helps and enhances the performance in delivering IP Multimedia contents and services over various access networks. (Umber Iqbal, 2010)

7.4 SIP based QoS architecture

IMS enforces SIP based 3GPP QoS architecture, which is used to provide quality of service over various IP networks. There is no mapping tool used by the SIP based quality of service architecture to interchange service level agreements between various networks. The unavailability of the mapping tool leads to the downfall of the network and disturbs the time. (Shaleeza sohail, 2010)

The SIP based quality of service mechanism can be viewed in the mentioned figure:

i. The IP connectivity is very essential for the IMS user to attain the IP Multimedia Subsystem contents.

ii. IMS core network is contacted by the UE through Session Initiation protocol and session description protocol while establishing the session.

iii. SIP proxy components are used to provide the anticipated user services in the access networks.

iv. The communication is initiated by SPQMs with transport networks and IP Multimedia Subsystem networks, in order to provide guaranteed quality of service from one end to another.

v. The SIP proxy modules deal with the SIP data attained from the IP Multimedia Subsystem Core network or from another Sip proxy module and transfers the received SIP data to the further present IMS network or SIP proxy module.

vi. SPQMs involve various MPLS and DiffServ routing techniques and both of them can work together if the packets obtain the correct quality of service at every LSR in the network.

vii. LDP is modified in order to maintain quality of service in MPLS and DiffServ networks.

7.5 SIP-Based Proxy QoS Modules (SPQMs)

i. SPQMs ensure quality of service while providing IMS multimedia contents over various access networks.

ii. SPQM is responsible of tracing the facts and figures of the present resource for the ongoing session and attains the Session initiation protocol data over the access networks from IP Multimedia Subsystem network.

iii. SPQMs and the access networks collaborate with each other and establish certain level of an agreement to provide quality of service from one end to another.

iv. MPLS and DiffServ routing techniques guarantee quality of service in delivering multimedia contents.

7.6 SPQM Architecture

The architecture of SPQM contains couple of quality of service functions described below:

7.6.1 SIP based Quality of Service Monitoring Function

i. SIP based Quality of Service Monitoring function monitors IP Multimedia Subsystem SIP data over the access networks by using update link state information.

ii. This function also manages the parameters used for the routing in the MPLS aware DiffServ network.

iii. This function observes the congestion in the network by keeping the data concerned with the parameters for the routing method, existing bandwidth and transmission delay.

iv. SIP based QoS Monitoring Function performs trouble shooting of the network, if the network degrades. (Umber Iqbal, 2010)

7.6.2 SIP-based Quality of Service Control Function:

The table shows the routing method used in providing quality of service over the access networks. There are couples of routing techniques used to ensure quality of service in SPQMs. One of them is Differentiated Services and the other one is Multi-Protocol label switching.

7.6.2.1 Differentiated Services:

i. The service disparity must be considered while providing multimedia contents in order to meet the expectations of the user.

ii. DiffServ routing technique provides the special dealing with the packets in order to meet the user expectations listed in the service level agreements.

iii. The packets are categorized into different classes of the data traffic by the edge routers. The classes are divided into various levels of priority and service type.

iv. The Differentiated services mechanism also provides various levels of the services delivered for the different data traffic.

v. Different functions are collected to forward data packets from one router to another according to the packet classes.

vi. The differentiated services domain categorizes the packets according to their linked service level agreements after receiving the packet from the edge routers.

vii. The data packet changes its shape and can be dropped when it is send again and again.

viii. The packet is denoted with DSCP if it is not dropped. DSCP helps in determining the router to router activity. The routers are used to save and forward the data packet to the core routers according to its priority and scheduling. There are number of forwarding techniques used i.e. best effort delivery, assured and expedited delivery/forwarding. (IETF, 2008)

7.6.2.2 Multi- Protocol Label Switching:

i. As the name suggests, unique labels are assigned to each packet at the entry point to the network. The unique labels are used for the identification of the data flow.

ii. In Multi-protocol Label Switching the path of the packet is determined by the first router.

iii. MPLS gives high importance to the traffic engineering. It helps in eliminating the concern of having high traffic on only one specific router. The data is transferred to the edge routers, in order to have an efficient network.

iv. The labels are located in the label stack. The edge routers are responsible of labeling the packets and the interior routers are used to look for the labels in the table and swap the labels.

v. Only those packets identified with Forward equivalence class can be forwarded through the edge routers. FEC refers to the order in which packets are going to be forwarded.

vi. On receiving the packet, label switching router looks in the table for the assigned label to that packet and swaps it with the label concerned with that Forwarding Equivalence class.

vii. The procedure of label look-up and swapping continues till the last router receives the packet, removes the label and forwards the packet to the final destination. The final destination of the packet is identified by the la router through the IP header of that packet.

7.6.2.3 MPLS and Traffic Engineering:

The congestion control in the traditional IP networks is very complex because each router selects the shortest path to forward the packet. Multi-Protocol Label Switching performs traffic engineering by allowing the first router to define the path. To make efficient network, high traffic data is shifted from one router to the edge routers. In this way data traffic is balanced on different routers and congestion is controlled. (Umber Iqbal, 2010)

8 Conclusion

Thoroughly researched and investigated NGN-IMS security architecture explains vulnerabilities in network at very high level. Security mechanisms govern certain rules to be followed to secure network entities. Entities have a high security concern to Network operator and User as well.. In our investigation, strong impact is on attacks and counter measures. We investigated different types of attack and on each attack we proposed a security proposal and model to secure system and user. We intensively study authentication procedure and security protocols. We proposed a security solution to best implementation when a high level of security is required. This solution is based on KMS based security. MIKEY-IBAKE, Otway-Ress and Ticket Based security are come under KMS security solution. These protocols can handle high level of security. These are implemented by unique key mechanism and mutual authentication. In mutual authentication procedure, there are two type of AKA procedure i.e. Multi-pass and One-pass. Authentication procedures take much processing time and cost. Here, One-pass AKA procedure is best solution of authentication. This reduces authentication overhead to reduce both cost and processing time as well. In QoS, SIP based and policy based quality of service is discussed. Policy based QoS refers to agree certain rules which are defined by various service providers to control and manage QoS delivery in IMS network. This may lead to determine the location of entities where to configure policy to prevent interception and delay in delivery contents. QoS management framework explains different types of protocols to be selected for assuring QoS. DiffServ and MPLS employ technique to set policy. DiffServ ensure QoS from one services to anther throughout network. MPLS is responsible for routing technique to best utilization of network resources.

9 *Discussion*

This project investigates Next Generation Network – IP Multimedia Subsystem framework in terms of data security and quality of service. IMS delivers multimedia contents through IP core network and PSTN network into a single transmission link. SIP protocol is the main signaling protocol responsible for transporting data into an IMS network via IP and PSTN network. IMS is an ALL-IP based network that exposed serious security threats concern to Network Operator and User as well. This project proposes a security model by using KMS based security solution and UMTS authentication key agreement mechanism. These mechanisms implement enhanced authentication with the help of public key techniques.

In IMS based network, security threats are concerned to IP network. IMS security architecture has been developed with further extension into two modules i.e. Access Security and Network Security. Access security sets a policy for UE to gain access to IMS services by implementing authentication and authorization mechanisms. Network security secures the data traffic in IMS network. This module of security governs policies and rules that are set by network operators as per requirement. SIP protocol is a backbone to transfer and implement IMS services. If SIP is secured then it means that UE and IMS network are both secured. In order to secure SIP, We proposed a procedure calls Authentication Key Agreement is implemented in between UE and IMS network for authentication. According to procedure, visited network sends authentication data request to home network. Home network sends a set of Authentication Vector (AV) to visited network. Home network then computes an array of AV by using secret key K. Secret key K is located in home network and UE. Home network responds and send (n) authentication vector to Visited network. AV arrives to visited network, it selects one (1) and sends challenge request by sending back RAND and AUTN fields. UE computes value AUTN by using secret key (K). In the last, UE generates RES and send to visited network and to compare XRES response from UE. In this scenario, we approved that attacker cannot steal secret key while listening the transmission. Reason is that, the secret key is not transmitted. We discussed that Session Description Protocol – SDP implements Crypto function and parameters to protect data steaming. This protocol is implemented on SIP signaling. We suggested that SIP session on both ends start with mutual sharing of crypto keys by using SRTP protocol. We strongly recommend SRTP to provide security for unknown peer by using certificate. This includes fingerprint of certificate in SIP message to avoid Man-in-the-Middle attack. Authentication process in IMS network maintains level of security. This level of security can be maintained by lowering the authenticating messages. It means that an automatic decrease in authentication cost and time as well. In this case, we finally proposed One-Pass authentication procedure to protects the network resources against denial of service attacks and can be improves the efficiency of authentication procedures. We have been discussed in detailed to ensure authentication.

We proposed a technique by using Public Key technique in authentication process. This process is based on security requirement as follows as mutual authentication,

1. Mutual authentication – Public-Key technique , Digital signature , Hash function
2. Access control -Secret (confidential data) protected by secret messages
3. Assets must be signed in authentication process. Digital signature with time stamp.

4. End of authentication process, IMS network must provide a secure channel to user.

PKI solution will secure the usage of CK and IK in HSS. Because, HSS depends on cryptographic functions to get random number process. In order to identify vulnerabilities in the IMS network, we discussed security concerns related to Network operator and User in detail. In network level, we studied different types of threats which have the ability to intercept traffic and capture confidential data through media to network as whole. One of them is toll fraud that affects VoIP services by means of fake usage of minutes, fake billing and holds the constant time of established call. In the IP core network, the data resides in the form of IP packets. IP packets are always under the severe threats. Data integrity is always compromised by the attackers by intercepting IP and extracting the actual data from the IP header. In this scenario, we suggested that IP can be secured by implementing IPSec protocol in Security gateways on network borders. Another serious threat is Denial of Service attack. DoS attack disrupts the network services and then as a result the services are unavailable to the both server and client. DoS attack occurs due to unnecessary services that opens a door to vulnerabilities. In this case we studied that the network operator should shut down unnecessary services and ports. An important component is security gateway. These security gateways are logically linked to inbound and outbound traffic. Data contents are converted in various forms and the format of these contents is further verified. If the format of the contents is different, then the contents of the data are compromised. In this situation we recommended that integrity of contents can be secured if the format of the contents remains same. Resulting data will be considered more secure.

In the last part of the security concerns, we discussed security concerns at the user level. Herein, several types of threats related to services and data are investigated. Our analysis started with Denial of Service attack that affects the legitimate user. This attack is a very serious threat that abandons the services. We proposed a method to countermeasure this threat by securing the bandwidth available to the legitimate user. User applications provide several services to user. IMS network support variety of applications which can breach the security on user assets. In this phase, we set a policy to user and an operator that only allow the authorized and legal applications. This means that no third party applications are allowed to be used because they are an easy target by the attackers. Presence and identification

The major concern to the user is regarding the safety of his/her data. The variety of applications which IMS provides creates a major concern regarding the successful provision of the services to the legitimate user, as it poses a threat not only on the user's asset but also on the data which passes through the user's system. IP Multimedia Subsystem also enables the services which enforces social networking concept on the architectural level i.e. IMS creates the different groups like friends, family etc. that can have an access to the presence or available data and notifies these groups regarding the attributes of the legitimate user. The attributes of the legitimate user include various information regarding the user's location, status and availability. The groups are not created on the per user basis, but maintained by the IMS, so that user may think that these groups are working while being assigned to any of the user. (Rosenberg, 2004)

10 Future Work

We have investigated Next Generation Networks according to security, and quality of service, but in future more research is required on the following points.

Currently, IPv4 is still widely range used in the Internet, but IPv6 protocol is required in IMS. Here, application level and IP level internetworking is an important aspect to pay full attention and has to be solved. NAT could be used to solve IP level internetworking. Applications Level Gateway can be used to resolve the application level address translation.

Intrusion detection system(IDS) could be useful to investigate in order to overcome security threats in IMS core.

11 List of figures and Tables

Figure 3-1 IP Multimedia Subsystem – A general overview 11
Figure 3-2 NGN IMS Architecture (Francis, 2010) 13
Figure 3-3 SIP signaling 14
Figure 4-1 NGN / IMS model and solution in Ericsson (Amirhassan Darvishan, 2010) 16
Figure 5-1 Security architecture 22
Figure 5-2 IMS secuirty architecture - Overview 24
Figure 5-3 UMTS Authentication security system 26
Figure 5-4 Multi pass AKA in IMS (Ntantogian, 2007) 29
Figure 5-5 IMS Security 34
Figure 5-6 Network Domain Security 34
Figure 5-7 Assets from the authentication process 37
Figure 5-8 Message flow for new security mechanism (Chung-Ming, 2007) 41

12 References

1. *Ericsson's "IMS Innovation Platform" for Web Real Time Communications turns any device with a web connection into an open communications device*. (2013, January 8). Retrieved from Ericssion: http://www.ericsson.com/news/1669129

2. *IMS*. (2013). Retrieved from Ericssion: http://www.ericsson.com/ourportfolio/telecom-operators/ims

3. 33.102, 3. T. (2011, May). *Universal Mobile Telecommunications System (UMTS).* Retrieved from ETSI TS 133 102 V10.0.0: http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/10.00.00_60/ts_133102v100000p.pdf

4. 3GPP. (2009). Quality of Service concept and architecture. *3GPP TS 23 .107*.

5. 3GPP, T. 3. (2011, October). *3G Security, Network domain security, IP network layer security.* Retrieved from Technical Specification Group Service and System Aspects: http://www.3gpp.org/ftp/Specs/archive/33_series/33.210/

6. A.K.M. Nazmus Sakib, F. J. (n.d.). Security Improvement of IEEE 802.11i (WiFi Protected Access2). *International Journal of Engineering Science and Technology.*

7. Amardeep Singh, G. M. (n.d.). QoS and Traffic Engineering MPLS, DiffServ and Constraint Based.

8. Amirhassan Darvishan, K. B. (2010). A Practical NGN Model By Evaluation of Various NGN Solutions and its. *IEEE*.

9. Bo Yu, D. Y. (2010). A Review of the Policy-Based QoS Architecture in IMS. *2010 First International Conference on Pervasive Computing, Signal Processing and Applications*.

10. Christoforos Ntantogian, C. X. (n.d.). Efficient Authentication for Users Autonomy in Next Generation All-IP Networks. *FET Program of the European Commission and the 03ED910 research project*.

11. Chung-Ming. (2007). One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem. *IEEE*.

12. ETSI. (2009). Cryptographic algorithm requirements. *3GPP TS 33.105*.

13. Francis, T. a. (2010). IMS Architecture. In *IP Communications and Services for NGN* (p. 250). LLC.

14. Group, T. a. (2010). IMS : IP Multimedia Subsystem. In *IP Communications and Services for NGN* (p. 248). LLC.

15. Hunter, M. T. (2007). Security Issues with the IP Multimedia Subsystem (IMS) version 1.0. *Georgia Institute of Technology*.

16. IETF. (2008). Definition of the Differentiated Services fields. *RFC2474*.

17. Joseph, J.-P. (n.d.). PSTN Services Migration to IMS. 6.

18. Kuhn, D. (2005). Security considerations for voice over IP systems.

19. Ntantogian, C. (2007). Efficient Authentication for Users Autonomy in Next Generation All-IP Networks. *Bionetics*, 1.

20. Poikselka, M. (n.d.). THE IMS IP Multimedia Concepts and services. *Nokia , Finland*.

21. Project, 3. G. (2006). IP Multimedia Subsystem (IMS), Stage 2, TS 23.228,. *Technical Specification Group Services and System Aspects*.

22. Rosenberg, J. (2004). A presence event package for the session initiation protocol. *RFC 3856*.

23. Shaleeza sohail, Y. j. (2010). SIP based QoS Management Architecture for IMS. *ICCNSS*.

24. Umber Iqbal, Y. J. (2010). SIP-Based QoS Management Framework for IMS Multimedia. *IJCSNS International Journal of Computer Science and Network Security*.

25. V10.0.0, E. T. (2011, May). *Security architecture (3GPP TS 33.102 version 10.0.0 Release 10).* Retrieved from ETSI TS 133 102: http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/10.00.00_60/ts_133102v100000p.pdf

26. Viviana Rodriguez, Y. D. (n.d.). Security Mechanism for IMS Authentication, Using Public Key Techniques. *Universidad de los Andes*, 1-2.