University of Piraeus

Piraeus - Greece

Thesis for Master Telecommunications
Department of Digital Systems
University of Piraeus

Security issues at NGN networks

By Tzouanopoulos Dionysis
February 22, 2012

Supervising Committee:
Dr. Costas Lambrinoudakis (University of Piraeus)

Contents

List of figures

List of tables

List of abbreviations

2G	Second Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
ACR	Accounting Request
AES	Advanced Encryption Algorithm
AG	Access Gateway
AH	Authentication Header
AKA	Authentication and Key Agreement
AN	Access Network
AP	Access Point
ARP	Address Resolution Protocol
AS	Application Server
AUC	Authentication Center
AV	Authentication Vector
BGCF	Breakout Gateway Control Function
BNF	Backus-Naur Form
CA	Certificate Authorities
CCMP	Counter-Mode/CBC-MAC Protocol
CDRs	Charging Data Records
CS	Circuit-Switched

CSCF	Call Session Control Function
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSL	Digital Subscriber Line
EAP-AKA	Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement
EAPOL	EAP over LAN
EAP-SIM	Extensible Authentication Protocol Method for GSM Subscriber Identity Module
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FMC	Fixed-Mobile Convergence
FSM	Finite State Machine
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Services
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
I-CSCF	Interrogating Call Session Control Function
ID	Identity
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange Version 2

IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISIM	IP Multimedia Services Identity Module
ITU-T	ITU Telecommunication Standardization Sector
MG	Media Gate
MGCF	Media Gateway Control Function
MGW	Media Gateway
MRCF	Media Resource Control Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
NAI	Network Access Identifier
NAS	Network Access Server
NGN	Next Generation Network
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
PRF	Pseudo-Random Function
PS	Packet-Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	Alleged RC4
RTP	Real-time Transport Protocol

S-CSCF	Serving Call Session Control Function
SCTP	Stream Control Transmission Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscriber Location Function
SMTP	Simple Mail Transfer Protocol
SPI	Security Parameter Index
TCP	Transmission Control Protocol
THIG	Topology Hiding Inter-working Gateway
TISPAN	Telecoms & Internet Converged Services & Protocols for Advanced Networks
TKIP	Temporal Key Integrity Protocol
TS	Traffic Selectors
TU	Transaction User
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network

WAG	Wireless Access Gateway
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

1 Introduction

The major security challenge of wireless networking and mobile communication is to protect network resources and secure end users. Additional security measures are required to cope with the interception of data on radio interfaces and illegitimate access to mobile services. The interception of user's data breaks the confidentiality of user's information and the illegitimate use of services cause masquerading and false charging the users [9].

Security in next-generation networks (NGNs) is a formidable challenge for all the involved parties (researchers, vendors, and service providers) since NGNs are based on Internet Protocol (IP) network technology, which has demonstrated the potential for significant security vulnerabilities.

The IP Multimedia Subsystem (IMS), defined by the 3rd Generation Partnership Project (3GPP) and 3rd Generation Partnership Project 2 (3GPP2) standards partnerships, is an important aspect of NGN evolution since it provides for access-independent advanced multimedia services in a distributed architecture. Its session control mechanism is based on Session Initiation Protocol (SIP) and employs many Internet Engineering Task Force (IETF)-defined protocols to provide a flexible, distributed network architecture for deployment of advanced consumer and business services. IMS security is a key enabler of large scale deployments of NGNs and must provide equivalent or better security than existing network solutions. In order to accomplish this goal, IMS security needs to be addressed in a comprehensive way to ensure that security needs are understood, standardized solutions are implemented, and security processes are in place to continually advance security as IMS evolves [5].

In this thesis we begin with a brief description of the AAA concept. Next an overview of the IMS architecture is provided to serve as a reference point for our IMS security discussion. IMS security threats and attacks through the 3G – WLAN interworking infrastructure are discussed in the next section to provide a view of the security challenges of an IMS solution. We follow with an analysis of the employed network and security architectures deployed to IMS in order to handle the aforementioned

security issues. Finally in appendices A and B the main protocols used in IMS are briefly introduced.

2 Theoretical background

In this chapter the concept of AAA is explained and other terms used in the introduction are further defined, like the IMS. In textboxes simple examples are given to illustrate the theory in this chapter.

2.1 AAA

AAA stands for Authentication, Authorization and Accounting. This section looks into the meaning of AAA, and the models used for authentication, authorization and accounting.

Authentication is the verification of the identity of the entity. An entity can be a user or the device a user has, like a computer or the SIM of his mobile phone. With authentication someone can prove that it is really the person or device he or it claims to be. This prevents from impersonations from other parties. Authentication consists of three sorts: user authentication, message authentication and device authentication [1].

> Joe wants to get some money from his bank account. He goes to the ATM machine of his bank and inserts his bankcard. The ATM machine wants to know if it is really Joe that tries to withdraw money. The ATM machine asks for the PIN code belonging to the bankcard. When Joe enters his PIN code correct, the bank has authenticated Joe as the owner of the card.

Authorization is the determination whether the requesting entity is allowed access to a particular resource. Authorization is the process of determining if the user has the right to access the network or use services, like the print server from that network.

Furthermore, authorization is needed for resource reservation and quality of service support.

Now Joe can enter the amount of money he wants to withdraw. The ATM machine checks with the bank if the amount Joe is asking for, is not more than he has on his account. If there is enough money left in his account, the ATM is authorized to hand out the requested amount to Joe.

Accounting is the collecting of information about resource usage for the purpose of capacity planning, auditing, billing or cost allocation. For example, records are kept about the duration a user surfs the Internet.

Joe's balance must be updated to process the withdrawal. The withdrawn amount is deducted from his account. *Accounting* is the registration of the withdrawal.

Re- authentication is the renewal of the authentication by the client upon request of the server. When a session lifetime has expired, or when an error has occurred in the path, re-authentication can be necessary to ensure trust.

When Joe enters a wrong PIN code, the ATM machine asks again for the PIN code of Joe. Joe is *re- authenticated* by entering this PIN code again.

2.1.1 Authentication models

As mentioned above, there are three different levels of authentication: user authentication, device authentication and message authentication. User authentication is the verification of the identity of the user; this can be done using authentication protocols like Diameter and RADIUS. Device authentication is sometimes needed when the device is from another, not trusted domain; here protocols like Kerberos can be used. Message authentication is used to authenticate messages without their context of a session. Digital signatures can be used to provide

message authentication [1].

For authentication a two-party model and a three-party model exists. The two-party model is used when two peers interact. A client and server are directly interconnected with no involvement of the middle nodes like gateways or proxies.

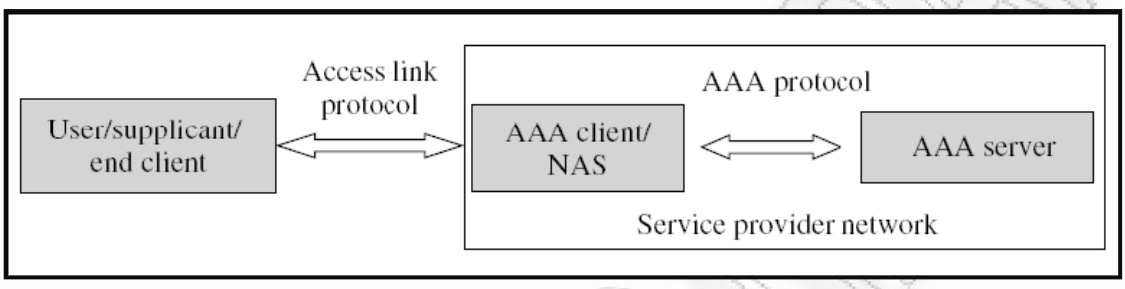

Figure 1: Three-party authentication model

A three-party authentication model is shown in Figure 1. In this example a user wants to access a network, like the network of his internet service provider. The user wants to connect to the network and connects to the first edge device, which is the Network Access Server (NAS). The NAS acts as an AAA client who connects to the AAA server to authenticate the user. The AAA server makes the decisions regarding granting access to the user.

Joe goes to the ATM machine to withdraw money. He enters his PIN code, and with that the ATM machine verifies with the bank if this is correct. Also authorization is granted by the bank to give Joe his money. In this case, Joe's contact with the bank goes through the ATM machine. The ATM fulfills the role of the *AAA client.* The bank takes the decisions about authentication and authorization and fulfills the role.

2.1.2 Authorization models

The informational RFC [2] about AAA authorization frameworks distinguishes three

different architectural models for authentication: the agent sequence, the pull sequence and the push sequence.

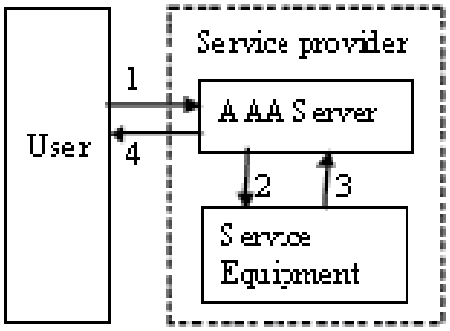

Figure 2: Agent sequence

In the scenario of the agent sequence showed in Figure 2, the user contacts the AAA entity first. The AAA server authorizes the user, and the service equipment is notified. The service equipment can set up the service and notifies the AAA server that it is ready, which notifies the user. The user and service equipment can precede the communication directly, without the AAA server functioning as an agent. An example of this situation is when a user requests Internet access. The user is first connected to the AAA server of the internet service provider. When the AAA server has authenticated the user, the proxy of the service provider is notified and the connection is established.

Before Joe can use his bank card, he has to prove to the bank that he is really Joe. He visits the bank office and shows his passport. Now he has proven he is Joe and is authorized by the bank that he can use the ATM machines. The system is updated that the ATM machines can accept Joe's card. Joe is informed that he is allowed to use the ATMs.

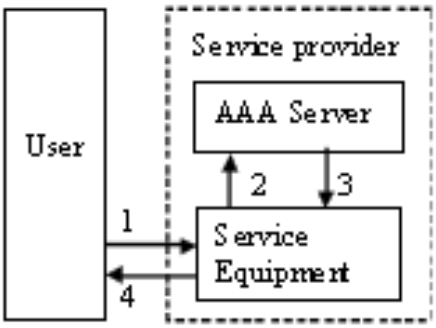

Figure 3: Pull sequence

Figure 3 shows the pull sequence. The user directly requests the service from the service equipment, which authorizes the user by placing a request at the AAA server. An example of this situation is when you pay with your credit card and the store checks with the credit card company if the card is still valid.

Joe withdraws money from his bank account. He goes to the ATM machine. The ATM machine contacts the bank and the bank authorizes that he has enough money, and can withdraw the requested amount. The ATM hands the amount to Joe.

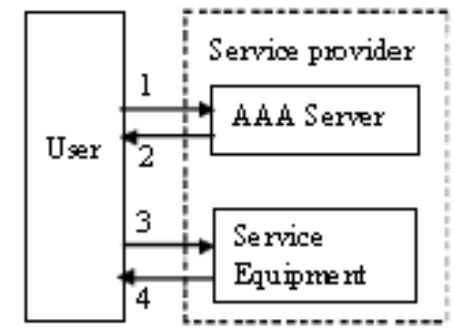

Figure 4: Push sequence

The push sequence is shown in Figure 4. The user receives a token from the AAA server with which the user can request the service and prove that it is authorized to use the service. An example of this situation is if you are going to the theater. First you buy a ticket at the box office. Before entering the auditorium the attendant

requests for your ticket, which is proof that you have paid.

> Most bankcards also have a ‘chipknip’, a kind of e-wallet. Before Joe can use his ‘chipknip’ in a store to pay for small purchases, the bank must give authorization. This authorization token is the credit that is placed on the chip of the bankcard. With this token the store knows that Joe has enough money on this ‘chipknip’ to pay for the product he wants to buy.

2.1.3 Accounting overview

The billing process describes all the sub processes needed for getting an invoice to the user for having used services. Figure 5 gives an overview of all the sub processes covered by billing, in particular accounting.

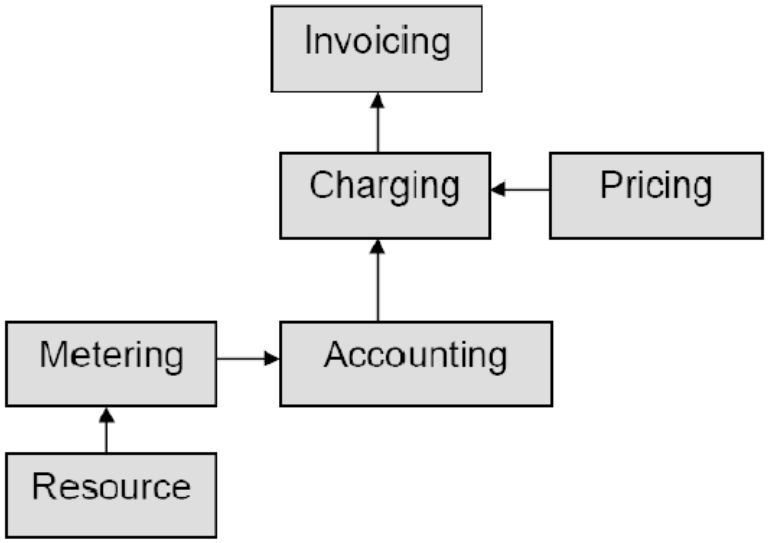

Figure 5: Accounting overview

Assume that a user consumes services generated by a resource. Then metering is the process which collects consumption statistics at a specific resource in the network. Accounting is the collection of this metering information, stored in accounting records. Charging combines the pricing information (set by pricing) and the accounting records and calculates the charging records, i.e. the amounts the user has

to pay. Finally, invoicing is the process of consolidating the charging records on a per customer basis and sending an invoice to the user [3].

AAA servers are able to collect metering information from the resource, for example from the Network Access Server about how long a user is surfing on the Internet. They order this information in accounting records, which are kept per user. This is what is meant by accounting in AAA. Note that invoicing and the handling of cash flows are never done by AAA protocols.

> If Joe is abroad and wants to withdraw cash from his bank account, it is possible that he has to pay for that transaction service. The foreign bank has a price, e.g. 2 Euro, which a withdrawal costs and calculates for Joe how much transactions he has done. The foreign bank sends an invoice to Joe's bank for the withdrawals and the transaction costs.

2.2 IMS

IMS stands for IP Multimedia Subsystem and is a standardized framework used by telecom operators to provide mobile and fixed multimedia services in an all IP environment. Its purpose is to make network management easier and to provide better interoperability, roaming between networks and enable network convergence [4].

2.2.1 IMS architecture

IMS was initially defined by the 3rd Generation Partnership Project (3GPP) and 3rd Generation Partnership Project 2 (3GPP2) wireless working groups. Its main objective was to provide a new mobile network architecture that enables convergence of data, voice and mobile network technology over an IP based infrastructure. The IP

Multimedia Subsystem was designed to fill the gap between the existing traditional telecommunications technology and Internet technology [5]. IMS has been embraced by ITU-T, European Telecommunications Standards Institute (ETSI), Telecoms & Internet Converged Services & Protocols for Advanced Networks (TISPAN), and other standards development organizations as a key part of Next Generation Networks (NGNs) [6].

Although initially developed for wireless applications, IMS was designed from the ground up to provide for access-independent services (wireless and wireline) and interworking with traditional telephone networks. Figure 6 demonstrates the different types of access-independent networks that the IMS can run on. These include Fixed Broadband, WLAN, GPRS and UMTS [7].

3GPP has decided to use a layered approach to architectural design for IMS. This means that transport and bearer services are separated from the IMS signaling network and session management services. A key benefit of this layered architecture is the use of common application layer while reusing common access and session control layers to provide multiple services to users across multiple access networks. This will allow operators to provide their subscribers with access to common applications across divergent networks [6]. The layered approach aims at a minimum dependence between layers. A benefit is that it facilitates the addition of new access networks to the system later on.

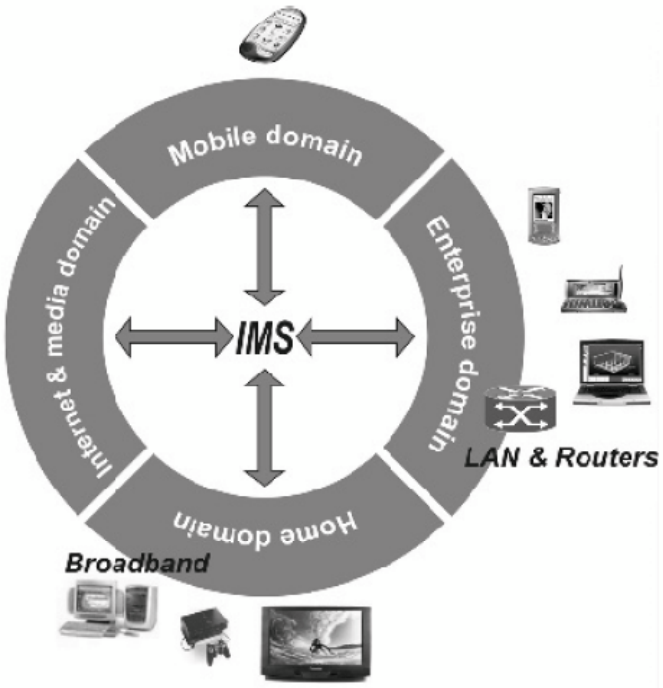

Figure 6: Access-independent IMS

Figure 7 depicts the 3GPP/3GPP2 network architecture, which can be further divided into three layers: the application layer, session control layer and the access and transport layer.

The application layer comprises application servers which provide IMS customer services such as voice messaging.

The session control layer contains the call session control function (CSCF), which provides for the registration of endpoints and routing of SIP messages to the appropriate application servers. The home subscriber server (HSS) maintains service profile information for each subscriber and is accessed by the CSCF to authenticate and authorize communication with appropriate application servers. If the CSCF determines a session is to be routed to the public switched telephone network (PSTN), the breakout gateway control function (BGCF) decides which network and media gateway control function (MGCF) or peer BGCF to route the session. The CSCF function is divided into three functions: the proxy CSCF (P-CSCF), the interrogating CSCF (I-CSCF) and the serving CSCF (S-CSCF). Common to all CSCFs is that they all play a role during registration and session establishment and

form the SIP routing machinery. The session control layer also includes the following functions: the policy decision function (PDF), which implements policy decisions for standard quality of service (QoS) mechanisms; and the media resource control function (MRCF), which controls media resources for conferencing, announcements, and tones.

Finally, the access and transport layer provides for termination of signaling to end points, and routing and control of bearer traffic. Included in this layer are: the media gateway (MGW), which provides for signaling and media between IMS and PSTN/ public land mobile network (PLMN) entities; the media resource function processor (MRFP) which provides the necessary coding, transcoding, and mixing required for payload processing; and the endpoints themselves which are contained in multiple access networks. IMS works with multiple access networks such as digital subscriber line (DSL), cable, wireless fidelity (Wi-Fi), Ethernet, and third-generation (3G) wireless providing multiple multimedia services using the same IMS service elements. Note that IMS defines basic network functions and interfaces which can be provided and partitioned in various ways in the actual implementation of network elements [5].

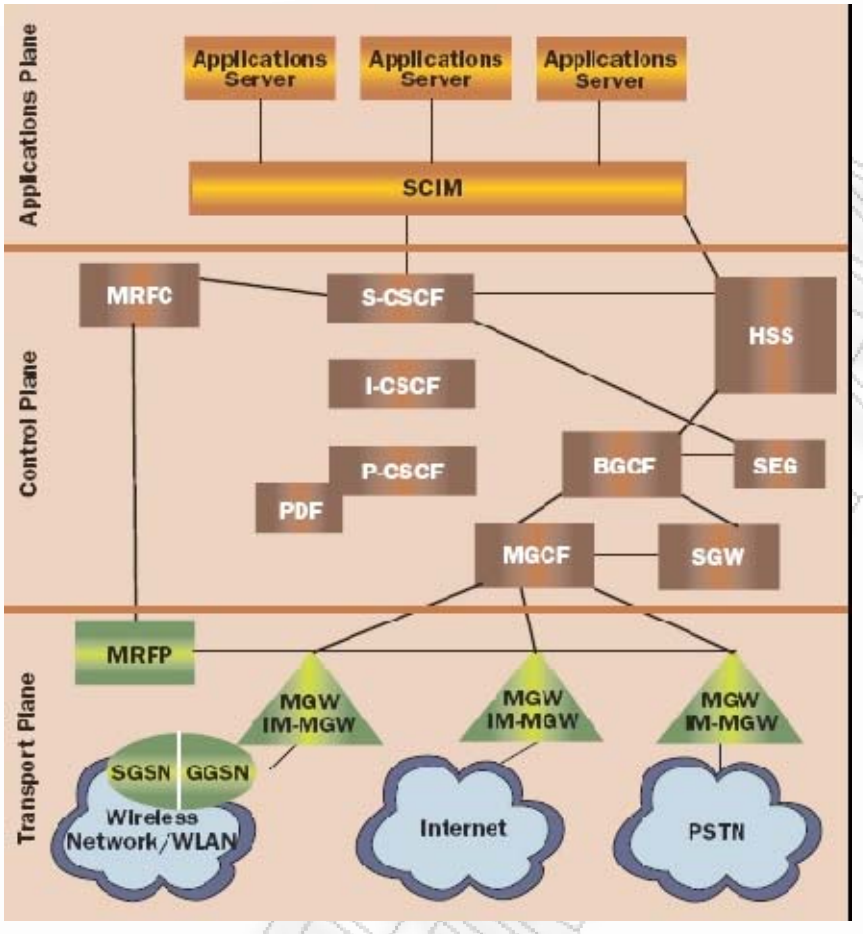

Figure 7: Layered view of IMS

2.2.2 IMS Inter – domain

The IP multimedia subsystem (IMS) is managed by one operator. If multiple operators want to communicate using IMS applications, they must interconnect their networks. It is possible that both networks are IMS networks, or only one of them. The IMS networks are interconnected using the Za interface, which is not further specified yet.

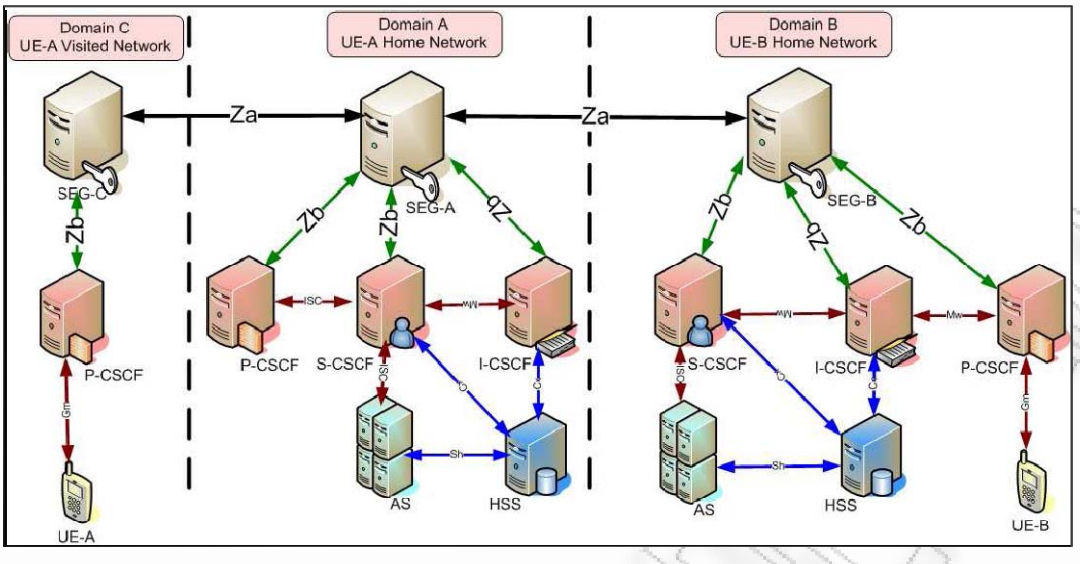

Figure 8: IMS inter-domain architecture

Networks from different security domains are interconnected through Security Gateways (SEG). The SEG's ensure that the IMS network is securely connected to other networks and protects the traffic between the networks and the IMS core.

With the architecture shown in Figure 8, not only IMS networks can be interconnected, also other IP networks can be connected to an IMS network. In this architecture the applications from the IMS domain can be used in other domains as well.

The IMS network is developed to run in a single trusted administrative domain under management of one operator. It is not possible in the current design to split the IMS network and divide it over multiple realms. The IMS network should be managed by one single party. As described above, multiple parties with their own IMS network can be interconnected, but IMS is not developed with the idea that multiple parties manage a single IMS network [4].

2.2.3 IMS Components and Entities

The IMS entities and key functionalities can be classified in six categories [7]:

- Session management and routing family (CSCFs).
- Databases (HSS, SLF).
- Services (application server, MRFC, MRFP).
- Interworking functions (BGCF, MGCF, IMS-MGW, SGW).
- Support functions (PDF, SEG, THIG).
- Charging.

Proxy CSCF (P-CSCF): It is the first contact point for a SIP endpoint (user) to gain access to IMS. Its address is discovered by UEs following Packet Data Protocol (PDP) context activation. The tasks assigned for the P-CSCF are: SIP compression, IPSec security association, interaction with Policy Decision Function (PDF), emergency session detection and generation of charging records.

Interrogating CSCF (I-CSCF): It is the contact point within a service provider's network for all sessions from another network destined to a subscriber of that service provider, or for a roaming subscriber currently located in another service provider's network. There may be multiple I-CSCFs within an operator's network. I-CSCF performs functions like obtaining the name of the next hop (either S-CSCF or application server) from the Home Subscriber Server (HSS), assigning an S-CSCF to a user performing SIP registration, charging and resource utilization (i.e. generation of Charging Data Records (CDRs)) and acting as a Topology Hiding Inter-working Gateway (THIG).

Serving CSCF (S-CSCF): It is the focal point of the IMS, the workhorse CSCF function, providing overall management of SIP sessions and coordination of sessions with other network elements. S-CSCF functions include SIP registration of endpoints, end user authentication, session and service control, and call monitoring and recording for charging.

Home Subscriber Server (HSS): The HSS is equivalent of the HLR (Home Location Register) in 2G systems; however, extended with two Diameter based reference points. It is the main data storage for all subscriber and service-related data of the IMS. The main data stored in the HSS include user identities, registration information, access parameters and service-triggering information.
In addition to functions related to IMS functionality, the HSS contains the subset of Home Location Register and Authentication Center (HLR/AUC) functionality required by the Packet-Switched (PS) domain and the Circuit-Switched (CS) domain.

Application Servers (ASs): Keeping in mind the layered design, ASs are not pure IMS entities; rather, they are functions on top of IMS. However, ASs are described as part of IMS functions because ASs are entities that provide value-added multimedia services in the IMS, such as presence and Push to talk Over Cellular. An AS resides in the user's home network or in a third-party location. The third party here means a network or a standalone AS. The main functions of the AS are the possibility to process and impact an incoming SIP session received from the IMS, the capability to originate SIP requests and the capability to send accounting information to the charging functions.

Media Processing: The Media Resource Function (MRF) can be split up into Media Resource Function Controller (MRFC) and Media Resource Function Processor (MRFP). It provides media stream processing resources like media mixing, announcements, analysis and media transcoding as well speech [7]. The other three components are Border Gateway Control Function (BGCF), Media Gate Control Function (MGCF) and Media Gate (MG) which perform the bearer interworking between RTP/IP and the bearers used in the legacy networks.

3 Vulnerabilities of IMS, Threats and Attacks through the interworking infrastructures

3.1 IMS network threats

The potential attacks and vulnerabilities suffering to IP Multimedia Subsystem (IMS) include [7]:

- *Denial of Service* - the consequence of a DOS is that the entity attacked becomes unavailable.
- *SQL Injection* – is a type of message tampering attacks and database modification or deletion.
- *Eavesdropping* - if messages are sent in clear text, any malicious user could eavesdrop and get session information to launch a variety of hijacking-style attacks.
- *Tearing down sessions* - an attacker could insert messages like a CANCEL request to stop a caller or send a BYE request to terminate the session.
- *Registration hijacking* - an attacker could register on user's behalf and could re-direct all traffic toward the attacker's machine.
- *Session hijacking* - an attacker could send an INVITE request within dialog request to modify requests en route to change session descriptions and redirect media elsewhere.
- *Impersonating a server* - someone else pretends to be the server and forges a response. The original message could be misrouted.
- *Man in the middle* - this attack is where attacker intercepts, modifies, or fabricates the flow of messages.

3.2 WLAN-3G inter-working networks threats

The security and data privacy is a big challenge especially due to integration of different networks and technologies because any single security solution is not

suitable to provide complete security. The Fixed-Mobile Convergence (FMC) based on IP Multimedia Subsystem (IMS) is considered one of the most important and open technology of this decade. This all IP based network architecture provides open and flexible interfaces to deploy innovative services. In parallel, this open IP based technology has security threats from Internet world [8].

The IMS is also vulnerable to different peer-to-peer attacks because users are always connected and online. In a typical WLAN-3G inter-working scenario the attacker can set up a rouge access point (AP) for example attempt to get free access, modify legitimate user traffic or launch denial of service attack. Most of the attacks launched at WLAN access network may have implications on 3G networks. The attacks can be deployed remotely over the Internet by setting up a radio jumper in a hotspot to the WLAN to become a legitimate user. The following are the possible attacks on 3G through WLAN access networks.

1) *Attacks at WLAN User Equipment*

The user terminals may be infected by malicious software (viruses, Trojan horses, etc). These programs operate without the knowledge of the user on his terminal to launch multiple types of attacks:

- USIM is used to store user authentication credentials and a Trojan residing in the terminal can send fake requests to the UICC and forward challenge-response results to another Mobile Station. This type of attack is launched inside the terminal and it does not involve external link between the terminal and UICC which is assumed to be physically secure.
- Trojans may monitor user keyboard or sensitive data operation activities and forward to another machine.
- Malicious software residing on different hosts can be used to launch Distributed DoS (DDoS) attacks against a target.

2) *Attacks from Attacker Equipment or Access Point*

Several types of attacks are possible if the attacker has access to equipment with WLAN interfaces or Access Point. For some WLAN technologies, layer 2 control signaling are not integrity protected and causing DoS. If they are not protected the attacker can easily eavesdrop on the traffic between a user and AP. This type of attack can cause different threats. For example:

- The attacker could modify the user traffic or divert the traffic to another network.
- The attacker could also fake a network or a commercial site to get access to credit card information.
- The attacker can act as a man-in-the-middle during the authentication to get credentials of the legitimate user. After getting credentials, attacker can access the services of legitimate user, while the legitimate user is denied to access.
- Important IP-network attacks in connection with rogue AP/networks are service spoofing attacks, where the attacker impersonates servers like DNS or DHCP.
- The attacker could use fake configuration or control messages such as ARP or ICMP messages to redirect a user's traffic. The ARP spoofing could also be used to redirect the AP's traffic, e.g. AAA messages generated by the AP.

3) *Attacks at WLAN Access Network Infrastructure*

- Attacks can be launched at WLAN access network infrastructure e.g. Access Points, LAN connecting APs, Ethernet switches etc.
- To perform any type of attacks inside the WLAN access network, the attacker needs access to the network.

- The WLAN is partially a wired network, and attacker may hook up to that part of the network. In public spaces the APs and corresponding wired connections may be physically accessible by attackers.
- For WLAN Direct IP Access if the charging is based on IP address, there exists a threat of IP address spoofing attack against WLAN access network [9].

4 NGN Network architectures

In the sequel we analyze the architectures of the WLAN - 3G interworking model that materializes next generation converged networks. Currently next generation networks (NGN) are deployed using two different access scenarios: *a) WLAN Direct Access* and *b) WLAN 3GPP IP Access*.

Each scenario incorporates a specific security architecture that aims at protecting the involved parties and the data exchanged among them. These architectures consist of various security protocols that provide mutual authentication, as well as confidentiality and integrity services to the data sent over the air interface of the deployed WLANs and specific parts of the core network.

In figure 9 the architecture for a general case of a converged network is illustrated where the WLAN is not directly connected to the user's home 3G PLMN. The network shown in figure 9 consists of a WLAN Access network (WLAN – AN), the visited 3G PLMN and the home 3G PLMN.

The WLAN-AN consist of the wireless Access Points (APs), which act like Authentication, Authorization, Accounting (AAA) clients that forward security related messages to the AAA server through AAA proxies, the Network Access Server (NAS) that provides to the mobile users access to the public internet, and the WLAN-Access Gateway (WLAN-AG) which is a gateway to 3G PLMN networks. It is assumed that WLAN is based on the IEEE 802.11 standard.

The visited 3G PLMN includes an AAA proxy that forwards AAA information to the AAA server (located in the home 3G PLMN) and a Wireless Access Gateway (WAG), which is a data gateway that routes users' data to the home 3G PLMN.

Finally the home 3G PLMN includes the AAA server that provides authentication services to the WLAN, the Packed Data Gateway (PDG) and the core network elements of the Universal Mobile Telecommunications System (UMTS), such as the Home Subscriber Service (HSS) or the Home Location Register (HLR), the Authentication Centre (AuC), the Gateway GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN). The AAA server retrieves authentication information from the HSS/HLR and validates authentication credentials provided by users. The PDG routes user data traffic between a user and an external packet data network, which is selected based on the 3G PS-services requested by the user.

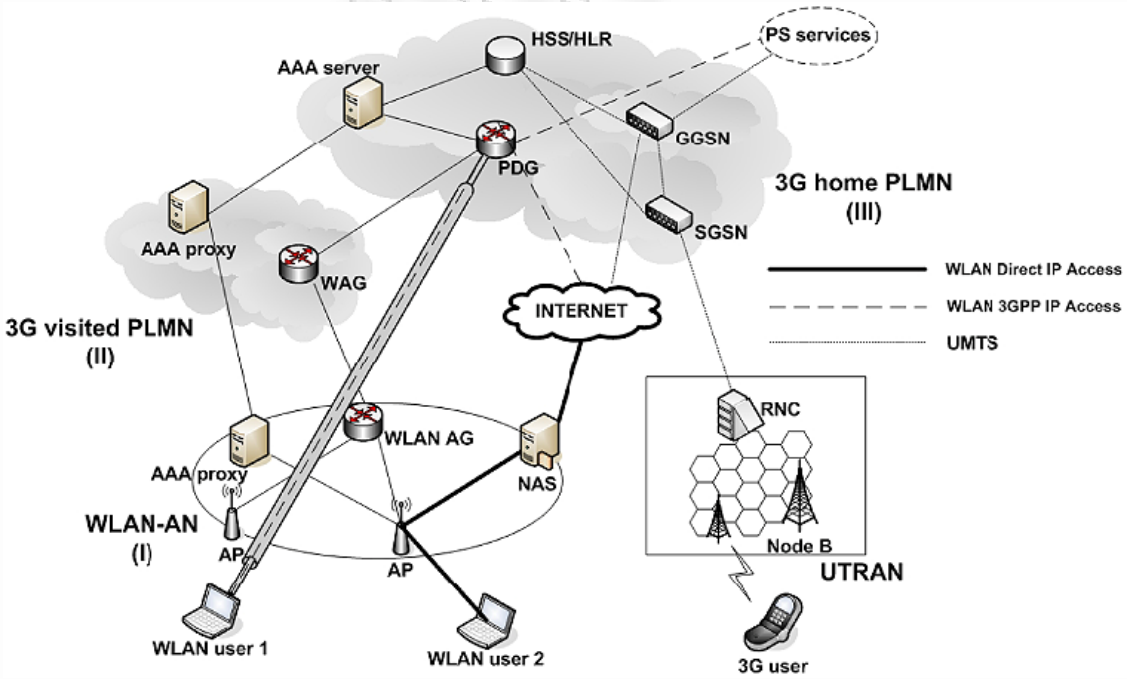

Figure 9: Converged network architecture

As mentioned previously we can distinguish between two different access scenarios *a) WLAN Direct Access* and *b) WLAN 3GPP IP Access*. In the first scenario the user acquires connection to the public Internet or an intranet via the WLAN-AN. In this scenario both the user and the network are authenticated to each other using the EAP-SIM or the EAP - AKA [11] protocol. Moreover in this scenario the confidentiality and integrity of user's data transferred over the air interface are ensured by the 802.11i security framework. In the second scenario, the WLAN 3GPP IP Access allows a user to connect to the PS services (like WAP, MMS, etc) or the public Internet through the 3G PLMN In this scenario the user is authenticated to the 3G PLMN using the EAP – SIM or alternatively the EAP-AKA protocol encapsulated within IKEv2 messages [10].

4.1 Security architectures

In the following, the security architectures and the involved security protocols which are employed in converged networks are presented.

4.1.1. WLAN Direct IP Access scenario

In the WLAN Direct IP Access scenario, both the user and the network are authenticated to each other using EAP-SIM or EAP-AKA, which are based on the 802.1X port access control. After a successful authentication, the user obtains an IP address from the WLAN-AN and then he gets access to the public Internet or an intranet, depending on the requested service. In this scenario, the confidentiality and integrity of user's data conveyed over the air interface of WLAN are ensured by the security mechanisms of 802.11i.

4. 1. 1. 1. Authentication

The specific security protocol that will be used for mutual authentication between the user and the network depends on the user's subscription. If the user possesses a UMTS Subscribers Identity Module (USIM) card, then, the EAP-AKA protocol is employed. Otherwise, EAP-SIM is used in cases that the user has a SIM-card of Global System for Mobile communications (GSM)/General Packet Radio Service (GPRS).

When the AAA server receives the user's identity, it fetches from the HSS/HLR the user's profile in order to determine the authentication protocol that will be employed (i.e., EAP-SIM or EAP-AKA). Because authentication for IMS access is based on the AKA protocol, in the following, we analyze the functionality of the EAP - AKA protocol focusing on the security services it provides.

EAP - AKA provides mutual authentication in a network environment that integrates 3G and WLANs, using the credentials included in a USIM – card and the UMTS Authentication and Key Agreement (AKA) procedure. It involves a user, an AAA client (which is actually a wireless AP), and an AAA server that obtains authentication information (i.e., authentication triplets) from the HSS/HLR of the network where the user is subscribed (see Fig. 10)

The WLAN access authentication signaling are transported over the 'Wa' reference point by standard mechanisms which are independent of the specific WLAN technology and based on standard Diameter protocol which uses IPsec for signaling security protection. If the user is roaming then the WLAN authentication signaling are transported over 'Wd' reference point between AAA Proxy and AAA Server. These signals are carried out between AAA server and Home Subscriber Server (HSS) over 'Wx' reference point.

Figure 10 shows the message exchange of EAP-AKA between the user and the AAA server. Note that the user communicates with the wireless AP via the EAP over LAN (EAPOL) protocol. First, the user associates with the wireless AP and the

latter sends an EAP-Request/Identity message to the user asking for his identity. The user responds with a message (EAP-Response/Identity) that includes his identity in the format of Network Access Identifier (NAI). This identity can be either the International Mobile Subscriber Identity (IMSI), or a temporary identity (i.e., pseudonym).

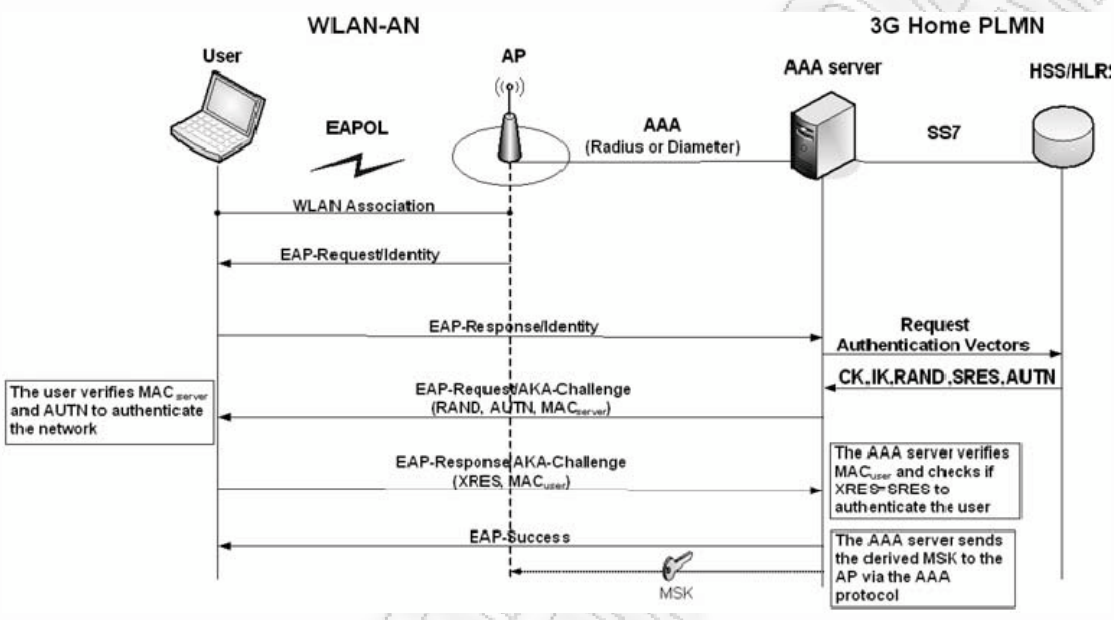

Figure 10: EAP – AKA authentication procedure and session key agreement (WLAN Direct IP Access scenario)

Figure 10 shows the message exchange of EAP-AKA between the user and the AAA server. Note that the user communicates with the wireless AP via the EAP over LAN (EAPOL) protocol. First, the user associates with the wireless AP and the latter sends an EAP-Request/Identity message to the user asking for his identity. The user responds with a message (EAP-Response/Identity) that includes his identity in the format of Network Access Identifier (NAI). This identity can be either the International Mobile Subscriber Identity (IMSI), or a temporary identity (i.e., pseudonym).

After obtaining the user's identity, the AAA server checks whether it possesses a 3G authentication vector, stored from a previous authentication with the specific user. If not, the AAA server sends the user's IMSI to the HSS/HLR. The latter generates n authentication vectors for the specific user by using the UMTS permanent secret key,

K, which is assigned to the user when he is subscribed to the network, and sends it to the AAA server. Note that an authentication vector includes a random challenge (RAND), the authentication token (AUTN), the expected response (XRES), the encryption key (CK) and the integrity key (IK). The authentication vector is calculated as:

$$AV = RAND \| XRES \| CK \| IK \| AUTN$$

In the sequel, the AAA server selects one out of the n obtained authentication vectors to proceed with the EAP-AKA authentication procedure and stores the remaining n-1 for future use. From the selected authentication vector, it uses the keys CK and IK and the identity of the user to compute the new key material which is required by EAP - AKA (*Master Key (MK), Master Session Key (MSK), K_auth & Message Authentication Code (MAC$_{server}$)* [10]). Additionally to the EAP-AKA key material some extra key material may also be generated for WLAN technology specific confidentiality and integrity protection.

The next EAP-AKA message *(EAP-Request/AKA-Challenge)* send by the AAA server to the user contains the RAND, AUTN and MAC$_{server}$ payload. The MAC$_{server}$ verifies the integrity of the sent message. After receiving this information message, the user executes the UMTS – AKA algorithms and verifies the AUTN payload. If the AUTN is correct, the network is authenticated otherwise the terminal rejects the authentication. The second verification is sequence number; if it is out of order, the terminal initiates a synchronization procedure. If AUTN is correct the USIM computes the IK and CK keys. From the computed IK and CK the user derives the additional new key material (*Master Key (MK), Master Session Key (MSK) and K_auth* [10]) to verify the received MAC$_{server}$ value. If this verification is also successful, the user computes the user's response to the challenge, noted as XRES payload, and sends an EAP-Response/ AKA-challenge message to the AAA server that includes the XRES and a new MAC$_{user}$ value, which covers the whole EAP message.

Upon receiving the EAP-Response/AKA-challenge message the AAA server verifies the received MAC_{user} value and checks if the received user's response to the challenge (XRES) matches with the response (i.e., SRES) received from the HLR/HSS. If all these checks are successful, the AAA server sends an EAP-success message along with the key MSK to the wireless AP. The latter stores the key and forwards the EAP-success message to the user. Finalizing the EAP-AKA protocol, both the user and the network have been authenticated each other, and the user and the wireless AP share the key MSK, which is used in the security framework of 802.11i for generating the session encryption keys.

4.1.1.2. Data protection (802.11i standard)

As mentioned previously, 802.11i is employed to provide confidentiality and integrity services to users' data conveyed over the radio interface of the deployed WLANs in the WLAN Direct IP Access scenario. The 802.11i standard was developed to enhance the security services provided in WLANs. Its design was motivated by the fact that the Wired Equivalent Privacy (WEP) protocol, due to its security flaws, could not adequately fulfill the security requirements of WLANs. The design goal of 802.11i is twofold:

(a) to provide session key management by specifying a four way handshake and group key handshake procedures, and (b) to enhance the confidentiality and integrity services provided to users' data by incorporating two security protocols: (i) the Counter-Mode/CBC-MAC Protocol (CCMP), which employs the Advanced Encryption Algorithm (AES), and (ii) the Temporal Key Integrity Protocol (TKIP), which uses the same encryption (RC4) with WEP. We do not proceed to the further analysis of the four-way and group key handshake procedures of 802.11i, and the functional details of the CCMP protocol because this is out of the scope of the current thesis [10].

4.1.2. WLAN 3GPP IP Access scenario

In contrast to the WLAN Direct IP Access scenario, in which a user gets access to the public Internet, directly, through the WLAN AN, the WLAN 3GPP IP Access scenario provides to the WLAN user access to the PS services or the Internet through the 3G PLMN. Before getting access to them, the user must perform the six (6) discrete steps, presented in Fig. 11 and described below:

1. Initial authentication. The user and the network are authenticated each other using either the EAP-SIM or EAP-AKA protocol. This authentication step enables the user to obtain a local IP address, called Transport IP address, which is used for access to the WLAN environment and the PDG. Note that this initial authentication can be omitted, if the PDG trusts the WLAN network and its users.

2. After the EAP-SIM or EAP-AKA execution, the four way handshake and optionally the group key handshake follow to provide the 802.11i session keys. Then, the communication between the user and the wireless AP is encrypted using the CCMP or alternatively the TKIP protocol.

3. After the completion of the initial authentication step and the 802.11i handshakes, the user communicates with the DHCP server to obtain the Transport IP address. This local address is used by the user to execute the IKEv2 in the following step 4.

4. The user retrieves the IP address of the PDG using the W-APN identity and the DNS protocol. Thus, the user and the PDG participate in a second authentication step that combines IKEv2 and EAP-SIM or EAP-AKA.

5. Second authentication. The user and the PDG execute the IKEv2 negotiation protocol, which encapsulates either EAP-SIM or EAP-AKA for authentication of the negotiating peers. After authentication completion, the user obtains a global IP address, called Remote IP address, which is used for access to the PS services and the public Internet via the

3G PLMN. In addition, the execution of IKEv2 results in the establishment of a pair of IPsec Security Associations (SAs) between the user and the PDG, which are used for the deployment of an IPsec-based Virtual Private Network (VPN).

6. The deployed IPsec based VPN protects user's data exchanged between the user and the PDG (in both directions), ensuring data origin authentication, data confidentiality and message integrity.

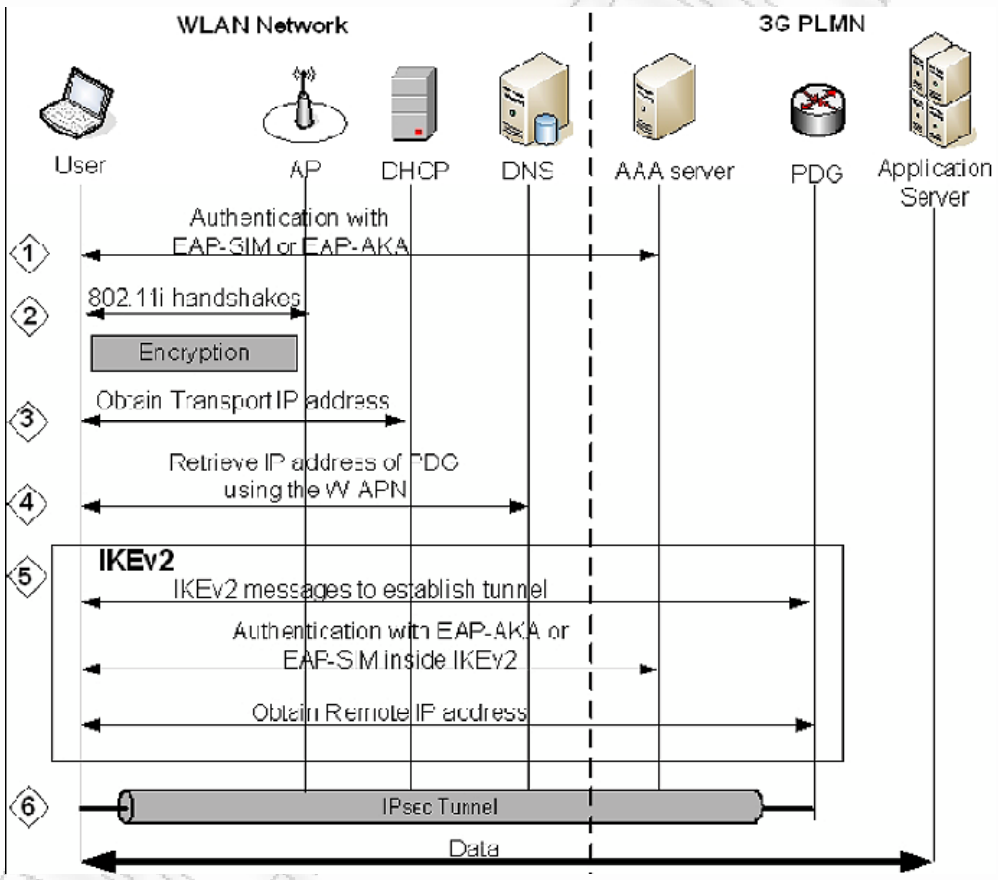

Figure 11: EAP – AKA authentication procedure and session key agreement (WLAN 3GPP IP Access scenario)

4.1.2.1. Authentication

IKEv2 is a simplified redesign of IKE that allows two peers to authenticate each other

(i.e., mutual authentication) and derive keys for secure communication with IPsec. The exchanged messages within IKEv2 are protected ensuring confidentiality and integrity, while the peers are authenticated using certificates, pre-shared keys or the EAP protocol. In the context of the WLAN 3GPP IP Access scenario, the user and the PDG execute IKEv2. The authentication of the user is based on EAP-SIM or EAP- AKA, while the authentication of the PDG is based on certificates.

Similarly to IKE, the IKEv2 protocol is executed in two sequential phases (i.e., phase 1 and phase 2). In phase 1, the user and the PDG establish two distinct SAs: (a) a bidirectional IKE_SA that protects the messages of phase 2, and (b) an one way IPsec_SA that protects user's data. During phase 2, the user and the PDG using the established IKE_SA can securely negotiate a second IPsec_SA that is employed for the establishment of a bidirectional IPsec-based VPN tunnel between them.

The EAP messages over IKEv2 will be exchanged between AAA server and WLAN client via PDG through Wm interface. The PDG extracts the EAP messages received from the user over IKEv2, and sends them to the AAA server over Diameter.

The IKEv2 phase 1 negotiation between the user and the PDG is executed in two sub- phases: (a) the IKE_SA_INIT and (b) the IKE_AUTH exchange, as shown in Fig. 12 IKE_SA_INIT exchange (noted as step 1 in Fig. 12) consists of a single request and reply messages, which negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange. In the context of this sub-phase, four cryptographic algorithms are negotiated: (a) an encryption algorithm, (b) an integrity protection algorithm, (c) a Diffie-Hellman group, and (d) a pseudo-random function (prf). The latter (prf) is employed for the construction of keying material for all of the cryptographic algorithms used.

After the execution of the IKE_SA_INIT, an IKE_SA is established that protects the IKE_AUTH exchange. The second sub-phase (i.e., IKE_AUTH) authenticates the previous messages, exchanges identities and certificates, encapsulates EAP-SIM or alternatively EAP-AKA messages, and establishes an IPsec_SA (step 2–5 in Fig. 12). All the messages of IKEv2 include a header payload (HDR), which contains a

Security Parameter Index (SPI), a version number, and security related flags. The SPI is a value chosen by the user and the PDG to identify a unique SA.

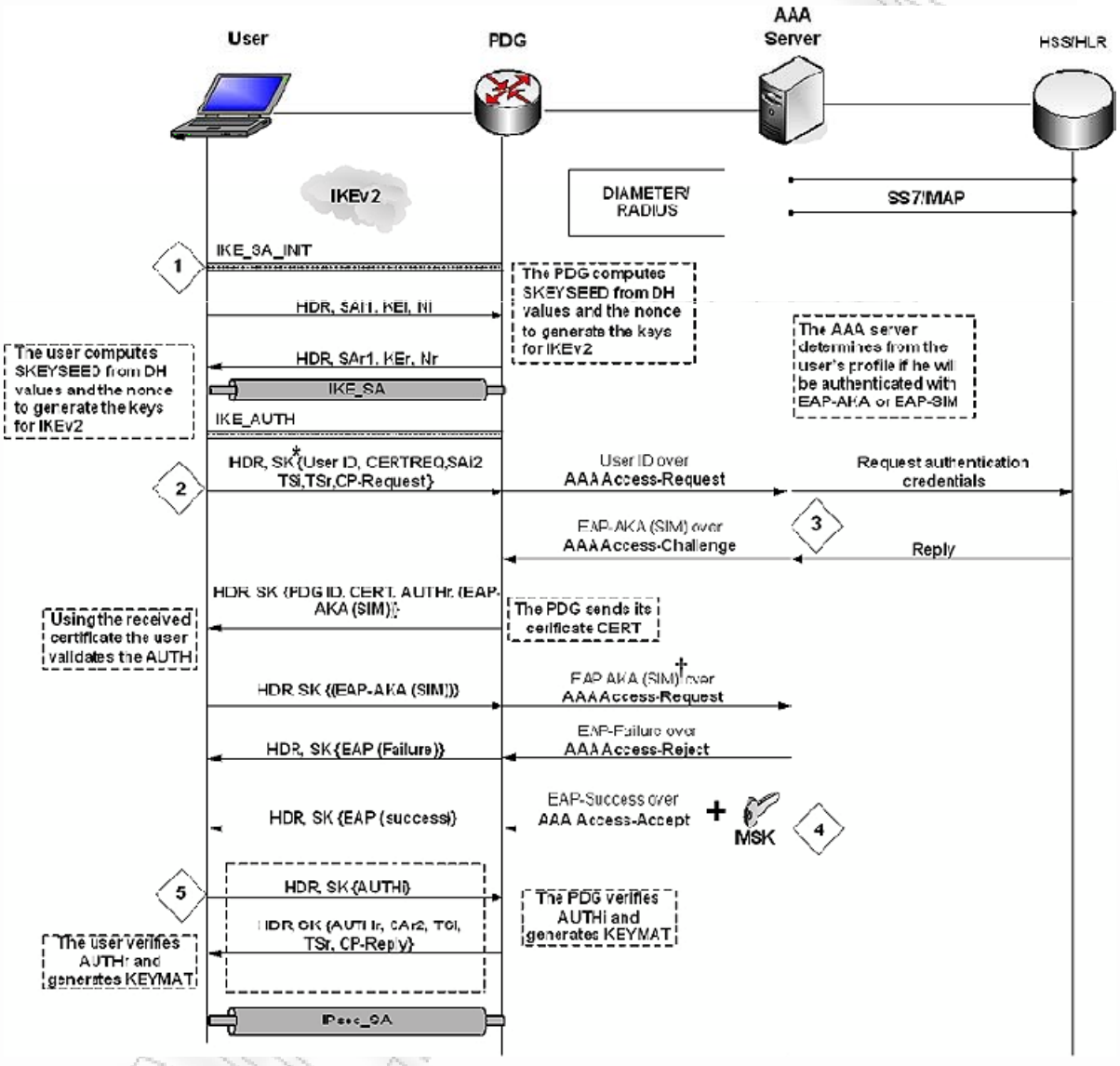

Figure 12: Execution of IKEv2 based on EAP-SIM or EAP-AKA

At the beginning of the IKEv2 negotiation (step 1 in Fig. 12), the user sends to the PDG the SAi1, which denotes the set of cryptographic algorithms for the IKE_SA that he supports, the KEi that is the Diffie-Hellman value, and a Ni value that represents the nonce. The nonce (i.e., a random number at least 128 bits) is used as input to the cryptographic functions employed by IKEv2 to ensure liveliness of the keying material and protect against replay attacks. The PDG answers with a message that contains its choice from the set of cryptographic algorithms for the IKE SA (SAr1), its value to complete the Diffie-Hellman exchange (KEr) and its nonce (Nr). Finalizing the IKE_SA_INIT exchange, the IKE_AUTH exchange can start. It is worth noting that from this point all the payloads of the following IKEv2 messages, excluding the message header (HDR payload), are encrypted and integrity protected using the IKE_SA (see step 2 in Fig. 12).

The IKE_AUTH exchange of messages starts when the user sends to the PDG a message that includes his identity (IDi), which could be in a NAI format, the CERTREQ payload (optionally), which is a list of the Certificate Authorities (CA) whose public keys the user trusts, and the traffic selectors (TSi and TSr), which allow the peers to identify the packet flows that require processing by IPsec. In addition, in the same message the user must include the Configuration Payload Request (CP- Request), which is used to obtain a Remote IP address from the PDG and get access to the 3G-PLMN.

After receiving this information, the PDG forwards to the AAA server the user identity (IDi) including a parameter, which indicates that the authentication is being performed for VPN tunnel establishment. This will facilitate the AAA server to distinguish between authentications for WLAN access and authentications for VPN setup. Upon receiving the IDi, the AAA server fetches the user's profile and authentication credentials (GSM triplets if authentication is based on EAP-SIM, or 3G authentication vectors if authentication is based on EAP-AKA) from HSS/HLR (if these are not available in the AAA server in advance). Based on the user's profile the AAA server initiates an EAP-AKA (if the user possesses a USIM card) or an EAP-SIM authentication (if the user possesses a GSM/GPRS SIM card) by sending to the PDG the first message of the related procedure (i.e., EAP-

SIM or EAP-AKA) included in a AAA protocol (i.e., Radius or Diameter) (step 3 in Fig. 12). Note that since there is no functional difference between the EAP-SIM and the EAP-AKA authentication when these protocols are encapsulated in IKEv2, we present them in a generic way. Thus, we introduce the EAP-AKA (SIM) payload notation (see Fig. 12) to indicate that this payload can be an EAP-SIM or an EAP-AKA message.

Upon receiving the first EAP-AKA (SIM) message, the PDG encapsulate it within an IKEv2 message and forwards the encapsulated message to the user. Except for the EAP-AKA (SIM) payload, this message also includes the PDG's identity, which identifies the provided 3G services (W-APN), the PDG's certificate (CERT), and the AUTHr field. The latter contains signed data used by the user to authenticate the PDG. Similarly to the previous messages, the payload of this IKEv2 message, except for the message header, is encrypted using the IKE_SA. Upon receiving the EAP-AKA (SIM) payload, the user verifies the AUTHr field by using the public key of the PDG included in the certificate field (CERT), and answers by sending an EAP-AKA (SIM) response message encapsulated again within an IKEv2 message. From this point, the IKEv2 messages contain only EAP-AKA (SIM) payloads, which are encrypted and integrity protected as described previously. The EAP-SIM or EAP-AKA exchange continues, normally, until an EAP-SUCCESS message (or an EAP-FAILURE in case of a failure) is sent from the AAA server to the PDG, which ends the EAP-AKA or the EAP-SIM dialogue. Together with the EAP- SUCCESS message, the key MSK is sent from the AAA server to the PDG via the AAA protocol, as shown in Fig. 12 (step 4).

After finishing the EAP-AKA or EAP-SIM dialogue, the last step (step 5) of IKEv2 re- authenticates the peers, in order to establish an IPsec_SA. This authentication step is necessary in order defeat man-in-the-middle attacks, which might take place because the authentication protocol (e.g.,EAP-SIM or EAP-AKA) runs inside the secure protocol (e.g., IKEv2). This combination creates a security hole since the initiator and the responder have no way to verify that their peer in the authentication procedure is the entity at the other end of the outer protocol. Thus, in order to

prevent possible attacks against IKEv2 (i.e., man in the middle attacks), both the user and the PDG have to calculate the AUTHi and the AUTHr payloads, respectively, using the MSK key that was generated from the EAP-SIM or EAP-AKA protocol. Then, both the user and the PDG send each other the AUTHi and AUTHr payloads to achieve a security binding between the inner protocol (EAP-SIM or EAP-AKA) and the outer protocol (IKEv2). Note that the PDG together with the AUTHr payload sends also its traffic selector payloads (TSi and TSr), the SAr2 payload, which contains the chosen cryptographic suit for the IPsec_SA and the assigned user's Remote IP address in the Configuration Payload Reply (CP-REPLY) payload. After the establishment of the IPsec_SA the keying material (KEYMAT) for this SA is calculated. The KEYMAT is used to extract the keys that the IPsec protocol uses for security purposes. Note that the deployed IPsec_SA protects the one way communication between the user and the PDG. For bidirectional secure communication between them, one more SA needs to be established (between the PDG and the user) by executing the IKEv2 phase 2 over the established IKE_SA [10].

4.1.2.2. Data protection

After the completion of the authentication procedure and the execution of IKEv2 between the PDG and the user, a pair of IPsec_SAs has been established between these two nodes. This pair deploys a bidirectional VPN between them that allows for secure data exchange over the underlying network path. At the same time, the user has been subscribed to the 3G PLMN network for charging and billing purposes using either the EAP-AKA or EAP-SIM protocol.

The deployed VPN runs on top of the wireless link and extends from the user's computer to the PDG, which is located in the user's home 3G PLMN (see Fig. 9). It is based on IPsec, which is a developing standard for providing security at the network layer. IPsec provides two choices of security service through two distinct security protocols: the Authentication Header (AH) protocol, and the Encapsulating Security Payload (ESP) protocol. The AH protocol provides support for

connectionless integrity, data origin authentication and protection against replays, but it does not support confidentiality. The ESP protocol supports confidentiality, connectionless integrity, anti-replay protection and optional data origin authentication. Both AH and ESP support two modes of operation: transport and tunnel. The transport mode of operation provides end-to-end protection between the communicating end-points by encrypting the IP packet payload. The tunnel mode encrypts the entire IP packet (both IP header and payload) and encapsulates the encrypted original IP packet in the payload of a new IP packet.

In the deployed VPN of the WLAN 3GPP IP Access scenario, IPsec employs the ESP protocol and is configured to operate in the tunnel mode. Thus, VPN provides confidentiality, integrity, data origin authentication, and anti-reply protection services protecting the payload and the header of the exchanged IP packets. From the two IP addresses (i.e., Transport and Remote IP address) of each authenticated user, the Remote IP address serves as the inner IP address, which is protected by IPsec, and the Transport IP address serves as the IP address of the new packets, which encapsulate the original IP packets and carry them between the user and the PDG. Thus, an adversary can not disclosure, fabricate unnoticed or perform traffic analysis to the data exchanged between the user and the PDG. Finally, IPsec can use different cryptographic algorithms (i.e., DES, 3DES, AES, etc.) depending on the level of security required by the two peers and the data that they exchange.

4.1.3 HTTP digest and 3GPP AKA

Authentication for IMS access is based on the AKA protocol. However, the AKA protocol cannot be run directly over IP; instead, it needs a vehicle to carry protocol messages between the UE and the home network. Obviously, as the entire objective of IMS access authentication is to authenticate for SIP access, SIP is a natural choice for such a vehicle.

SIP, as part of the IETF process, is based on the Hypertext Transfer Protocol (HTTP). The Hypertext Transfer Protocol (HTTP) digest is specified in [12], and how it is used with SIP is described in [13]. The IMS on the contrary is part of the Third Generation Partnership Project/Universal Mobile Telecommunications System (3GPP/UMTS) architecture, which uses the 3GPP Authentication and Key Agreement (AKA) mechanism for authentication.

In order to achieve 3GPP AKA-based authentication within the IMS, [14] defines how 3GPP AKA parameters can be mapped to HTTP digest authentication. Therefore, the signaling elements (SIP headers and parameters) used to transport 3GPP AKA information are identical to those used for the HTTP digest. Nevertheless, their meanings (i.e., their interpretation at the UE, the P-CSCF and the S-CSCF) are different.

In order to distinguish the 3GPP AKA authentication mechanism from other HTTP digest mechanisms, it was given a new algorithm value: ‘‘AKAv1-MD5’’.

4. 2. 1. 1 Authentication

Within the initial REGISTER request Tobias’s UE utilizes the HTTP Digest Authorization header to transport Tobias’s private user identity. In order to fulfill HTTP digest requirements, the UE includes the following fields in the Authorization header:

- The authentication scheme – set to the value ‘‘Digest’’, as the 3GPP AKA is mapped to the HTTP digest mechanism.
- The username field – set to Tobias’s private user identity, which will be used by the S-CSCF and the HSS to identify the user and to find the corresponding AV.
- The realm and URI fields – set to the home domain of Tobias.

- The response and nonce fields – which are left empty. These fields are mandated by the HTTP digest, but not used in the initial REGISTER request.

The REGISTER now looks like:

```
REGISTER sip: home1.fr SIP/2.0
Authorization: Digest username="tobias_private@home1.fr",
realm= "home1.fr",
nonce= "",
uri= "sip:home1.fr",
response= ""
```

As the UE and the P-CSCF did not establish any kind of mutual security mechanism at the SIP signaling level, the P-CSCF cannot guarantee that the REGISTER request really does originate from Tobias: for example, a malicious user could have constructed the request and sent it to the P-CSCF, without the P-CSCF knowing. Therefore, the P-CSCF adds the integrity-protected field with the value ‘‘no’’ to the Authorization header, before sending the request toward Tobias’s home network:

```
REGISTER sip: home1.fr SIP/2.0
Authorization: Digest username="tobias_private@home1.fr",
realm="home1.fr",
nonce= "",
uri= "sip:home1.fr",
response= "",
integrity-protected= "no"
```

The S-CSCF, after receiving the REGISTER request, identifies the user by the private user identity found in the username field and downloads the AV from the HSS. Based on the data in the AV, it returns the WWW-Authenticate header in the 401 (Unauthorized) response and populates its fields as follows:

- in the nonce field it has the RAND and AUTN parameters, both 32 bytes long and Base 64-encoded (the nonce field may include additional server-specific data);
- in the algorithm field it has the value ‘‘AKAv1-MD5’’, which identifies the 3GPP AKA mechanism; and
- in the ik and ck extension fields it has the integrity and ciphering keys. Note that these two fields are not part of the original definition of the WWW-Authenticate header, which is defined in [13].

The WWW-Authenticate fields look like:

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest realm= "home1.fr",
                  nonce= A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
                  ik= "0123456789abcdeedcba9876543210",
                  ck= "9876543210abcdeedcba0123456789"
```

After receiving the 401 (Unauthorized) response, the P-CSCF must remove and store the ik and ck fields from the WWW-Authenticate header, before sending the response toward the UE:

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest realm= "home1.fr",
                  nonce= A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5
```

From the received AUTN parameter the ISIM application in Tobias’s UE now discovers that it was really Tobias’s home operator network that sent the 401 (Unauthorized) response. It can also derive from the AUTN that the SQN (sequence number) is still in sync between the HSS and the ISIM.

The received parameters as well as the shared secret allow the ISIM to generate the values for the response and hand them over to the UE. The UE adds the Authorization header to the second REGISTER request, including (among others) the following fields:

- The username field – which includes Tobias's private user identity.
- The nonce field – which is returned with the same value as it was received in the WWW-Authenticate header of the 401 (Unauthorized) response.
- The response field – which includes the authentication challenge RES that was derived by the ISIM from the received RAND and the shared secret.

The ISIM will also calculate the IK, which is also known by the P-CSCF. Based on this key the UE and the P-CSCF establish IPsec SAs, over which the UE sends the second REGISTER request:

```
REGISTER sip: home1.fr SIP/2.0
Authorization: Digest username="user1_private@home1.fr",
realm="home1.fr",
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
uri="sip:home1.fr",
response="6629fae49393a05397450978507c4ef1"
```

The P-CSCF is now in a position to discover whether the received REGISTER request was modified on its way from the UE to the P-CSCF, as it can now check its integrity. If this check is successful, the P-CSCF adds the ''integrity-protected'' field with the value ''yes'' to the Authorization header and sends the REGISTER request toward Tobias's home network:

REGISTER sip:home1.fr SIP/2.0

Authorization: Digest username="user1_private@home1.fr",

realm="home1.fr",

nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,

uri="sip:home1.fr", response="6629fae49393a05397450978507c4ef1",

integrity-protected="yes"

The S-CSCF now compares the received RES and the XRES that was included in the AV. If these two parameters are identical, then the S-CSCF has successfully authenticated the user. Only after that, it will proceed with normal SIP registration procedures [7].

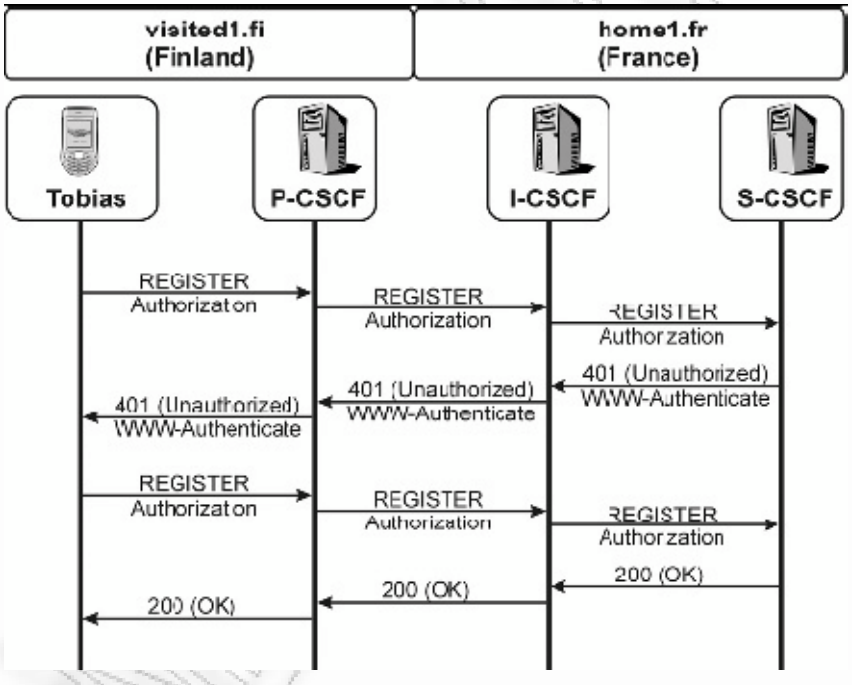

Figure 13: IMS - digest AKA authentication

Conclusions

In this thesis we have presented the employed security architectures at NGN networks materialized by the interworking model that integrates 3G and WLANs. Two different IMS access scenarios are used by the NGN networks: (a) the WLAN Direct IP Access and (b) the WLAN 3GPP IP Access. In the first scenario the user gains access to the public internet or to an intranet through the WLAN-AN. Both the user and the network are authenticated to each other using EAP-SIM or EAP-AKA depending on the user's subscription. Although EAP-AKA supports a higher level of security services compared to the EAP – SIM, both present some common security weaknesses which can be exploited by adversaries to perform attacks. In the WLAN Direct IP Access scenario the 802.11i security frame work ensures the confidentiality and integrity of users' data transferred over the air interface thus eliminating the security flaws of WEP. The second access scenario allows a user to connect to the PS services or to the public Internet through the 3G PLMN. In the WLAN 3GPP IP Access scenario, the user is authenticated to the 3G PLMN using EAP-SIM or alternatively EAP-AKA encapsulated within IKEv2 which eliminates their identified security weaknesses. The network is authenticated to the user using its certificate. Moreover, the execution of IKEv2 is used for the establishment of an IPsec-based VPN between the user and the network that provides additional confidentiality and integrity protection to the data exchanged between them. Finally since the IMS access is based on the AKA protocol a description of how the SIP protocol becomes the vehicle for this authentication procedure is mandatory to complete the purpose of this thesis.

References

[1] Thales e-security, *Advanced Authentication*, whitepaper 2006, http://www.thales-security.com/Whitepapers/documents/Advanced_Authentication.pdf

[2] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, *AAA Authorization Framework*, RFC 2904, August 2000

[3] Yoann Hinard, H. Bettahar, Y. Challal, A. Bouabdallah, *AAA based security architecture for multicast content distribution*, Compiegne University of Technology, Heudiasyc lab. France IEEE proceeding ISCN'06, June 2006

[4] Wendy Ooms, *Providing AAA with the Diameter protocol for multi-domain interacting services*, Faculty of Electrical Engineering, Mathematics and Computer Science, (DACS),University of Twente, The Netherlands, Master Thesis, June 2007

[5] Erik E. Anderlind, David W. Faucher, Eric H. Grosse, Daniel N. Heer, Andrew R. McGee, David P. Strand, Robert J. Thornberry Jr. *IMS Security*, Lucent Technologies Inc., January 2006

[6] Faruk, A.b.m. Omar, *The Role of IMS in Global Roaming for 3G Networks*, School of Information and Communication Technology The Royal Institute of technology (KTH), Sweden

[7] M. Poikselkae, G. Mayer, H. Khartabil, A. Niemi, The *IMS: IP Multimedia Concepts and Services, Second Edition* ISBN 0-470-01906-9, John Willey & Sons Ltd, 2006.

[8] Muhammad Sher, *Secure Service Provisioning (SSP) Framework for IP Multimedia Subsystem (IMS)*, Fakultät Elektrotechnik und Informatik der Technischen Universität, Berlin, Master Thesis, December 2007

[9] Muhammad Sher, Thomas Magedanz, 3G-*WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model)*, Fakultät Elektrotechnik und Informatik der Technischen Universität, Berlin, 2007

[10] C. Xenakis, C. Ntantogian, *Security architectures for B3G mobile networks*, September 2007

[11] Arkko, J., & Haverinen, H. (2006). *EAP-AKA authentication*. RFC 4187, January 2006.

[12] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P. Luotonen, A. and L. Stewart, HTTP *Authentication: Basic and Digest Access Authentication*, RFC2617, June 1999.

[13] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J.,Sparks, R., Handley, M. and E. Schooler, *SIP: Session Initiation Protocol*, RFC3261, June 2002.

[14] Niemi, A., Arkko, J. and V. Torvinen, Hypertext Transfer Protocol (HTTP) *Digest Authentication Using Authentication and Key Agreement (AKA)*, RFC3310, September 2002.

Appendix A Diameter

A.1 Introduction

Diameter is an Authentication, Authorization and Accounting (AAA) protocol developed by the Internet Engineering Task Force (IETF). Diameter is used to provide AAA services for a range of access technologies focusing on supporting access to IP networks. It was developed to resolve the issues the Remote Authentication Dial In User Service (RADIUS) protocol left open. RADIUS has previously been used to provide AAA services, at least for dial-up and terminal server access environments RADIUS. The Diameter protocol was not built from scratch; it is loosely based on the RADIUS.

The Diameter protocol consists of two parts: Diameter Base Protocol and Diameter applications (Figure 14). The base protocol is needed for delivering Diameter data units, negotiating capabilities, handling errors and providing for extensibility. The base protocol must be supported by all applications. A Diameter application defines application-specific functions and data units.

Figure 14: Diameter Framework

The Diameter Base Protocol uses both the Transmission Control Protocol (TCP) [RFC0793] and the Stream Control Transmission Protocol (SCTP) [RFC 2960] as transport.

Diameter has three different types of network nodes: clients, servers and agents.

Clients are generally the edge devices of a network that perform access control. A Diameter agent can be relay, proxy, redirect or translation agent. A Diameter server handles the AAA requests for a particular domain, or realm.

Diameter clients originate AAA requests. The Diameter sever services the client's requests within a realm, according to the used Diameter application. Diameter agents provide value-added services for clients and servers.

Typically, the Diameter client is a Network Access Server (NAS) that performs AAA services for a particular access technology. The NAS needs to authenticate the terminals that are attached to a network before allocating network resources for them.

Diameter agents can be deployed in a network to perform load balancing, distribute system administration and maintenance, concentrate requests and perform additional message processing.

Diameter relay agents are protocol-transparent, and are also agnostic about Diameter applications. They simply accept requests and route messages based on the supported realms and known peers. Relay agents are usually used to reduce the configuration load on Diameter clients and servers.

Diameter redirect agents perform realm-to-server resolution. A redirect agent instead of routing a request by itself returns a special answer message that includes the identity of the next-hop peer. The originator of the request then contacts the next-hop peer directly. Redirect agents operate in a stateless fashion thus providing scalability and centralized message routing. However, centralized message routing is always a compromise between ease of configuration and fail-over resilience.

Diameter proxy agents carry out value-added message processing on the requests and answers. They are similar to relay agents in that message routing is based on a Diameter routing table, but different in that they also modify the messages by implementing policy enforcement (e.g., resource usage enforcement, admission

control or provisioning).

Diameter translation agents perform protocol translation services between Diameter and another AAA protocol. Translation agents are used to allow legacy systems to communicate with the Diameter infrastructure.

A.2 Diameter services

The Diameter Base Protocol provides two types of services to Diameter applications: authentication and/or authorization, and accounting.

A.2.1 Authentication and Authorization

Authentication and authorization services are interlinked in Diameter. An auth request is issued by the client to invoke a service. Depending on the AVPs carried in the auth request, either authentication or authorization (or both) are performed on it.

Authentication clearly either succeeds or fails, whereas the Diameter Base Protocol provides authorization services in either stateless or statefull mode. In statefull authorization the server maintains a session state and the authorization session has a finite length. The total lifetime of a session consists of an authorization lifetime and a grace period, which together represent the maximum length of a session the server is willing to take responsibility for. The authorization session can, of course, be terminated by the client or aborted by the server and, at the end of the authorization lifetime, it can also be re-authorized. These functions are provided by the Diameter Base Protocol.

The two authorization modes of operation correspond to a statefull authorization Finite State Machine (FSM) and a stateless authorization FSM, with which all Diameter nodes that support authentication and authorization services have to comply.

A.2.2 Accounting

The Diameter Base Protocol provides accounting services to Diameter applications. A successful Accounting Request (ACR) activates an accounting session, in which the accounting records exchanged fall into two categories, based on the accounting service type:

- *Measurable length services* have clearly defined beginnings and ends. An accounting record is created when the service begins and another is sent when the service ends. Optionally, interim accounting records can be produced at certain intervals within the measurable length session.
- *One-time events* are services without a measurable service length. In a one- time event accounting record the beginning of the service and the end of the service actually coincide; therefore, a one-time event only produces a single accounting record.

The accounting server directs the client to use either measurable length service accounting or one-time event accounting. It also optionally specifies the time interval to use when generating interim accounting records.

The Diameter Accounting Protocol has built-in fault resilience to overcome small message loss and temporary network faults, as well as real-time delivery of accounting information.

In the sequel the most important Diameter application for this thesis is briefly described the Diameter Session Initiation Protocol (SIP). This application is used in the Cx, Dx, Sh and Dh interfaces.

A.3 Diameter SIP application

The Diameter SIP application defines a Diameter application that can be used by a SIP server to authenticate users and to authorize usage of different SIP resources. The Diameter SIP application is close to the 3GPP IMS Cx interface in functionality, but it is designed to be generic enough for other SIP deployment scenarios to be able to benefit from it. Table 1 illustrates a mapping between Cx interface parameters and Diameter SIP application AVPs.

The general architecture used as the basis for the Diameter SIP application is illustrated in Figure 15. Proxy A and proxy B have different roles: proxy A is configured as an edge proxy to a domain and proxy B as the home proxy of a domain. Proxy A closely resembles the Interrogating Call Session Control Function (I-CSCF) function and proxy B the Serving-CSCF (S-CSCF) function in IMS. For redundancy and fault tolerance, there may be additional Diameter Subscriber Locator (SL) nodes that either implement the Diameter relay or Diameter redirect agent functionality.

Table 1: Mapping Cx parameters to the Diameter SIP application.	
Cx parameter	Diameter SIP application AVP Name
Visited network identifier	SIP-Visited-Network-Identifier
Public user ID	SIP-AOR
Private user ID	User-Name
S-CSCF name	SIP-Server-URI
S-CSCF capabilities	SIP-Server-Capabilities SIP-Mandatory-Capability SIP-Optional-Capability
Result	Result-Code SIP-Reason-Code
User profile	SIP-User-Data SIP-User-Data-Request-Type SIP-User-Data-Already-Available
Server assignment type	SIP-Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item number	SIP-Item-Number
Authentication scheme	SIP-Authentication-Scheme
Authentication information	SIP-Method SIP-Authenticate SIP-Authentication-Context
Authorization information	SIP-Authorization SIP-Authentication-Info
Confidentiality key	SIP-Confidentiality-Key
Integrity key	SIP-Integrity-Key
Number authentication items	SIP-Number-Auth-Items
Reason for de-registration	SIP-Deregistration-Reason SIP-Reason-Info
Charging information	SIP-Accounting-Information SIP-Accounting-Server-URI SIP-Credit-Control-Server-URI
Route information	Destination-Host
Type of authorization	SIP-User-Authorization-Type

Table 1: Mapping Cx parameters to the Diameter SIP

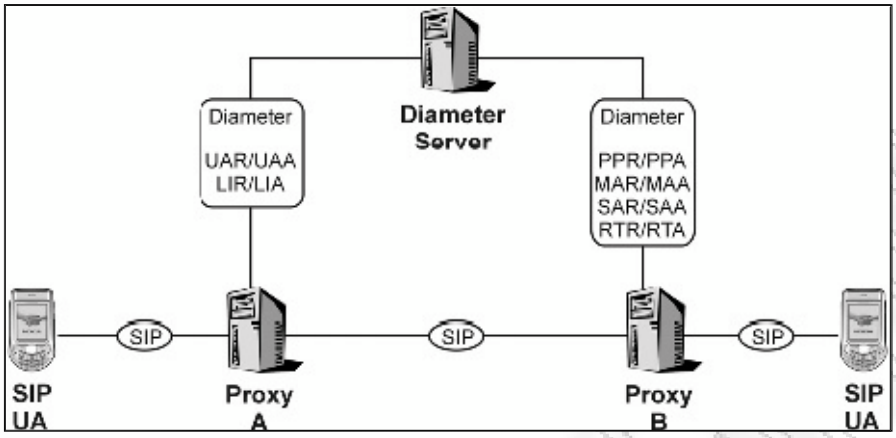

Figure 15: Diameter SIP application architecture

The Diameter SIP application defines a set of Command-Codes that are an extension to the Diameter Base Protocol (see Table 2). These Command-Codes perform the following functions:

- UAR/UAA – determine whether a user is authorized to receive a certain service and, if so, indicate the local server capable of providing that service.
- SAR/SAA – assign a specific SIP server to a particular user and deliver the user profile to it in a synchronous way.
- LIR/LIA – determine the next-hop SIP entity at an edge proxy.
- MAR/MAA – authenticate and authorize a user for a specific SIP service (e.g., SIP registration). Authentication can either be performed in the Diameter server or delegated to the SIP server.
- RTR/RTA – de-registration initiated by the Diameter server.
- PPR/PPA – asynchronously delivers the user profile to the SIP server from the Diameter server [7].

Table 2: Diameter Base Protocol Command-Code values	
Command-Name	Abbreviation
User-Authorization-Request	UAR
User-Authorization-Answer	UAA
Server-Assignment-Request	SAR
Server-Assignment-Answer	SAA
Location-Info-Request	LIR
Location-Info-Answer	LIA
Multimedia-Auth-Request	MAR
Multimedia-Auth-Answer	MAA
Registration-Termination-Request	RTR
Registration-Termination-Answer	RTA
Push-Profile-Request	PPR
Push-Profile-Answer	PPA
Credit-Control-Request	CCR
Credit-Control-Answer	CCA

Table 2: Diameter Base Protocol Command-Code values

Appendix B SIP

B.1 Introduction

SIP is an application layer protocol that is used for multimedia sessions handling in an Internet Protocol (IP) network. It was standardized by the Internet Engineering Task Force (IETF).

SIP was designed to be independent of the underlying transport layer (it can run on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Stream Control Transmission Protocol (SCTP)). It is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP).

Elements in SIP can be classified as User Agents (UAs) and intermediaries (servers).
A SIP UA can perform the role of a User Agent Client (UAC), which sends SIP requests, and the User Agent Server (UAS), which receives the requests and returns a SIP response. These roles of UAC and UAS only last for the duration of a SIP transaction.

SIP intermediaries are logical entities through which SIP messages pass on their way to their final destination. Although two SIP endpoints can communicate without any intervening SIP infrastructure, which is why the protocol is described as peer-to-peer, this approach is often impractical for a public service.

Proxy server – is an intermediary entity that acts as both a server and a client. Its purpose is to receive and forward SIP requests and its primary role is to route requests to another entity closer to the targeted end point. It can interpret or re-write certain parts of SIP messages that do not disturb the state of a request or dialog at the end points, including the body. A proxy server can also send a request to a number of locations at the same time. This entity is labeled a ‘‘forking proxy’’. Forking can be parallel or sequential.

There are three proxy server types:

- *dialog-statefull proxy* – a proxy is dialog-statefull if it retains the state for a dialog from the initiating request (INVITE request) right through to the terminating request (BYE request);
- *transaction-statefull proxy* – a proxy that maintains client and server transaction state machines during the processing of a request;
- *stateless proxy* – a proxy that forwards every request it receives downstream and every response it receives upstream.

Redirect server – maps the address of requests to new addresses. It redirects requests but does not participate in the transaction.

Location server – keeps track of the location of users.

Registrar server – a server that accepts REGISTER requests. It is used to store explicit binding between a user's address of record (SIP address) and the address of the host where the user is currently residing or wishes to receive requests.

B.2 SIP structure

SIP is a layered protocol that allows different modules within it to function independently with just a loose coupling between each layer. Figure 16 visualizes the layered approach taken.

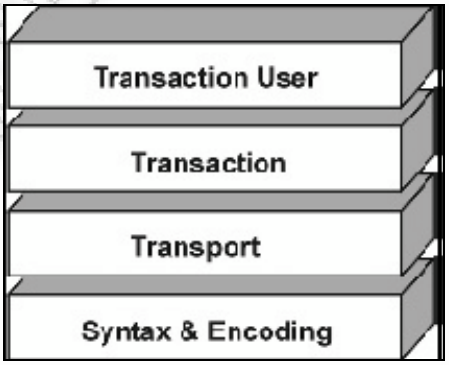

Figure 16: SIP protocol layers

The first (bottommost) layer in the protocol is the syntax and encoding layer. Encoding makes use of augmented Backus-Naur Form (BNF) grammar, the complete description of which can be found in [RFC3261].

The second layer is the transport layer. As the name indicates, this is the layer that dictates how clients send requests and receive responses and how servers receive requests and send responses. The transport layer is closely related to the sockets layer of a SIP entity.

The third layer is the transaction layer. A transaction, in SIP terms, is a request that is sent by a client to a server, along with all responses to that request sent from the server back to the client. The transaction layer handles the matching of responses to requests. Application-layer re-transmissions and application-layer transaction timeouts are also handled in this layer and are dependent on the transport protocol used. A client transaction sends requests and receives responses, while a server transaction receives requests and sends responses. The transaction layer uses the transport layer for sending and receiving requests and responses.

The fourth (topmost) layer is the Transaction User (TU) layer. This is the layer that creates client and server transactions. When a TU wishes to send a SIP request it creates a client transaction instance and sends the request along with the destination IP address, port and name of the transport protocol to use. TUs are defined to be UAC core and UAS core, or simply UAC and UAS. UACs create and send requests and receive responses using the transaction layer, while UASs receive requests and create and send responses using the transaction layer.

There are two factors that can affect TU behavior: one is the method name in the SIP message and the other is the state of the request with regard to dialogs.