



Tampere University of Technology
Department of Information Technology

Ilkka Vesa

Secure Network Access with IPSec Tunnels

Master of Science Thesis

Subject approved by the department council on 16.10.2002

Supervisors: Prof. Jarmo Harju

MSc. Rami Lehtonen

Foreword

This Master of Science thesis was done as part of the ICEFIN project at Tampere University of Technology, Telecommunications Laboratory during the fall 2002 and the winter 2002-2003. The thesis was a part of the research of the authentication and AAA protocols in the current and future Internet networks.

I would like to thank Prof. Jarmo Harju and especially MSc. Rami Lehtonen for guidance, my co-worker Teemu Alakoski for the proofreading and his counseling in the security related issues, Juha Laine for providing the \LaTeX class file and MSc. Jussi Lemponen, thanks to him I originally lost my way to the amazing world of the telecommunications.

Tampere, March 4, 2003

Ilkka Vesa

Tarjanteenkatu 7 A 1

33720 Tampere

Finland

`ilkka.vesa@iki.fi`

Abstract

TAMPERE UNIVERSITY OF TECHNOLOGY

Department of Information Technology

Institute of Communications Engineering

Ilkka Vesa: Secure Network Access with IPSec Tunnels

Master of Science thesis: 67 pages

Supervisors: Prof Jarmo Harju and MSc. Rami Lehtonen

March 2003

During the last ten years, the Internet has extended rapidly and developed technically. New access technologies and especially wireless networks have given Internet service providers an opportunity to offer customers the possibility to access Internet in different places and with various technologies. To manage and to charge from the usage of the constructed networks and services, Internet service providers need effective tools to handle authentication, authorization and accounting (AAA).

This Master of Science thesis examines the usage possibilities of the authentication and network access on the Internet protocol. These operations have normally been implemented on the link layer, but the universality and the inclusiveness of the Internet protocol makes a link layer independent network access system a tempting alternative.

In this thesis the functional and security requirements of a generic network access protocol are derived from the most important usage scenarios. Based on those requirements one possible implementation of the authentication and the network access on the Internet protocol is developed. The emphasis in the implementation is on the security aspects, since their importance in the Internet communications is constantly increasing.

Tiivistelmä

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

Tietoliikennetekniikan laitos

Ilkka Vesa: Secure Network Access with IPSec Tunnels

Diplomityö: 67 sivua

Tarkastajat: Prof. Jarmo Harju ja DI Rami Lehtonen

Maaliskuu 2003

Viimeisen kymmenen vuoden aikana Internet on laajentunut nopeasti ja kehittynyt teknisesti. Uudet verkkoon sisäänpääsyteknologiat ja etenkin langattomat verkot ovat antaneet Internet-palveluntarjoajille mahdollisuuden tarjota asiakkailleen Internet-yhteyksiä eri ympäristöissä ja erilaisia tekniikoita käyttäen. Voidakseen hallita rakentamiensa verkkoja ja palveluita ja laskuttaakseen niiden käytöstä Internet palveluntarjoajat tarvitsevat tehokkaita työkaluja hoitamaan asiakkaiden tunnistamista, valtuuttamista ja laskutusta (AAA).

Tässä diplomityössä tutkitaan Internet-protokollan päällä tapahtuvan tunnistamisen ja verkkoon sisäänpääsyn käyttömahdollisuuksia. Nämä toiminnot on normaalisti toteutettu linkkikerroksella, mutta IP:n yleisyys ja kaikenkattavuus tekee linkkikerroksesta riippumattomasta verkkoon sisäänpääsyjärjestelmästä houkuttelevan vaihtoehdon.

Tässä työssä on johdettu yleiskäyttöisen tunnistamis- ja verkkoon sisäänpääsyprotokollan toiminnallisuus- ja turvallisuusvaatimukset tärkeimpien käyttöympäristöjen pohjalta. Määriteltyjen vaatimusten pohjalta on kehitetty yksi mahdollinen IP:ta käyttävä tunnistamisen ja verkkoon sisäänpääsyn toteutus. Pääpaino toteutuksessa on turvallisuusnäkökohdilla, koska niiden merkitys Internetin käytössä kasvaa jatkuvasti.

Table of Contents

Foreword	i
Abstract	ii
Tiivistelmä	iii
Table of Contents	iv
List of Acronyms	vi
1 Introduction	1
2 Network Access	3
2.1 Authentication and Network Access	3
2.2 Network Elements	4
2.3 Network Access Protocol Layer	5
2.4 Network Access Usage Scenarios	6
3 AAA Protocols	8
3.1 AAA Architecture	8
3.2 Remote Authentication Dial In User Service	10
3.3 Diameter	11
4 EAP Authentication Protocols	13
4.1 Operation	13
4.2 Message Formats	15
4.3 EAP Security Deficiencies	16
4.4 Authentication and Key Agreement over EAP	17
5 Internet Protocol Security	21
5.1 General Operation	22
5.1.1 Authentication Header	22
5.1.2 Encapsulated Security Payload	23
5.2 Security Associations	23
5.3 Security Policies	26
5.4 IP Traffic Processing	27
5.5 Internet Key Exchange	28
5.6 Authentication and Encryption Algorithms	29
6 Functional Requirements of Network Access	31
6.1 General Requirements	31
6.1.1 Operational Environment	31
6.1.2 Bandwidth Consumption	32
6.1.3 Response Times	33
6.1.4 Scalability	34
6.2 Access Control	35
6.2.1 Access Control List Rules	35

6.2.2	Administration of Access Control List	36
6.2.3	Authorization Requests	37
7	Network Access Security	38
7.1	Assumptions	38
7.2	Active Attacks	40
7.2.1	Man-in-the-Middle Attacks	40
7.2.2	Replay Attacks	42
7.2.3	Service Theft	42
7.2.4	Breaking the Encryption	44
7.2.5	Denial of Service Attacks	44
7.3	Passive Attacks	46
7.3.1	Eavesdropping	47
7.3.2	Traffic Analysis	47
7.3.3	Identity Collection and Tracing	48
8	Secure Network Access Operation	50
8.1	Mutual Authentication	50
8.1.1	Initiation of Authentication	50
8.1.2	EAP-AKA over Internet Protocol	52
8.2	Creation of IPSec Tunnels	54
8.2.1	Pre-negotiated Parameters	55
8.2.2	Security Association Creation with IKE	56
8.3	Secure Accessing to the Network	57
8.3.1	Structure of the Network Elements	57
8.3.2	Packet Processing in the Network Access Server	59
8.3.3	Re-authentication	62
8.3.4	Termination of Connection	64
8.3.5	Co-operation with Cellular Networks	64
9	Conclusions	66
	References	68

List of Acronyms

3GPP	3G Partnership Project
AAA	Authentication, Authorization and Accounting
AAAB	Broker AAA server
AAAH	Home AAA server
AAAL	Local AAA server
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
AKA	Authentication and Key Agreement
ARP	Address Resolution Protocol
AS	Autonomous System
AuC	Authentication Centre
AVP	Attribute Value Pair
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
CBC	Cipher Block Chaining
CHAP	Challenge Handshake Authentication Protocol
CK	Cipher Key
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol

DOI	Domain of Interpretation
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ESP	Encapsulated Security Payload
GSM	Global System for Mobile communication
HLR	Home Location Register
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IMSI	International Mobile Subscriber Identity
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JFK	Just Fast Keying
LAN	Local Area Network
MAC	Medium Access Control
MAC	Message Authentication Code
MD5	Message Digest 5
MSC	Mobile Switching Centre

MTU	Maximum Transfer Unit
NAC	Network Access Client
NAI	Network Access Identifier
NAS	Network Access Server
NIST	National Institute of Standards and Technology
PANA	Protocol for carrying Authentication for Network Access
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RNC	Radio Network Controller
SA	Security Association
SADB	Security Association Database
SHA-1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module
SPD	Security Policy Database
SPI	Security Parameter Index
SSH	Secure Shell
TMSI	Temporary Mobile Subscriber Identity
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Service
USIM	UMTS Subscriber Identity Module
VLR	Visitor Location Register
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1 Introduction

The rapid technical development of the Internet has given the Internet users new possibilities to take advantage of network services in different places and with various technologies. In addition to the traditional Internet usage at home or at office, the Internet can be accessed in the WLAN hot-spots in the public places like hotels and airports and in the near future the mobility of the Internet users is going to increase even more. For the Internet service providers this offers new business opportunities, but also a challenge how to manage and charge from the usage of the constructed networks and services. In other words, they need tools to handle the Authentication, Authorization and Accounting (AAA). The Internet Engineering Task Force (IETF) Working Groups are working to specify protocols and procedures to solve this problem.

In many existing authentication solutions the authentication is performed on the link layer, like 802.1x in the IEEE 802 links. The different access technologies use dissimilar link layers and thus many different protocols must be developed to perform the same task. To simplify the variety of the network access mechanisms the IETF Protocol for carrying Authentication for Network Access (PANA) Working Group is specifying a multi-purpose protocol to be carried over the Internet Protocol (IP). Unlike the different link layer protocols, the IP is employed in all the different network access environments and one general-purpose protocol can be used for the authentication.

In this Master of Science thesis one possible solution to secure the network access is developed. The theory is largely based on the PANA's specifications and requirements, but

it includes also some different proposals and solutions. The goal of the study was to develop a secure workable system, which employs existing proof-to-work security protocols and mechanisms. As a result of the comparison of the different solutions, the core of the authentication procedure was chosen to be built on the basis of the UMTS Authentication and Key Agreement (AKA). The AKA messages are encapsulated inside the Extensible Authentication Protocol (EAP) messages and carried over the IP layer. After a successful authentication the Internet Protocol Security (IPSec) is used to secure the actual communication to the Internet.

The thesis was done as a part of the research of the authentication and AAA protocols in the ICEFIN project at Tampere University of Technology, Institute of Communications Engineering.

The structure of this thesis is as follows. An introduction to the network access systems and usage scenarios are presented in Chapter 2. Chapters 3 to 5 introduce the most important elements used in this particular network access system: In Chapter 3 the Authentication, Authorization and Accounting protocols and architecture, in Chapter 4 the Extensible Authentication Protocol and in Chapter 5 the Internet Protocol Security. In Chapters 6 and 7 the requirements of the network access system are derived: Chapter 6 concentrates on the functional requirements and Chapter 7 on the security requirements. After the introduction of the selected protocol elements and the specification of the system requirements, Chapter 8 describes the actual operation of the developed network access system. Finally, Chapter 9 summarizes the thesis.

2 Network Access

This chapter introduces the concept of network access, the different network elements that participate in the network access, the advantages and disadvantages of network access implementations on different protocol layers and the different network access usage scenarios.

2.1 Authentication and Network Access

The network access consists of achieving a right or a permission to access some networks and network services and of the actual usage of those desired services. In the Internet networks the usage of network services basically means sending and receiving Internet Protocol (IP) packets and thus in practice, the controlling of the network access is actually controlling of the right to communicate with the IP packets.

The admittance to the desired networks and services often requires authentication. The authentication procedure verifies that the person trying to access the network really is who he or she claims to be and that he or she can be authorized to get the access. In the network access the authentication is usually based on something that only the authenticating parties know, a shared secret. With the shared secret they can proof their true identities to the opposite parties. In the network access the authentication can be either one-sided or mutual. In the one-sided authentication only the user authenticates itself to the serving network and cannot be sure about the identity of the network. In the mutual authentication both parties authenticate themselves to each other and thus the total security is better.

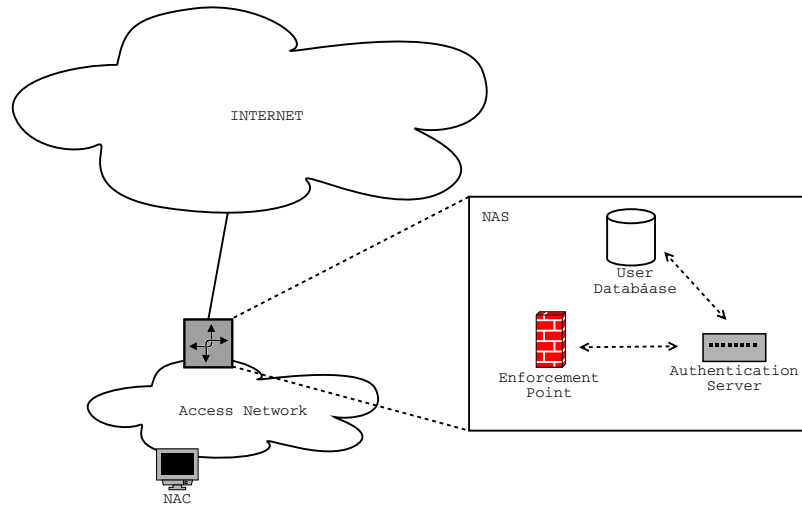


Figure 2.1: A basic network access scenario

2.2 Network Elements

The most important element of a network access system is naturally the user, a person who wants to use some networks or services, and for whom the entire access network is constructed. The user takes part in the operation of the network access system through a software installed into his or her network device. This software which is responsible for the network access is called a Network Access Client (NAC). The operation of the NAC is rather transparent to the user and as the user turns his or her network device on or arrives to a new network, the NAC can operate automatically without any involvement from the user.

The element with which the NAC communicates directly in the network access system is a Network Access Server (NAS). The NAS consists of an authentication server, an enforcement point and an optional local user database as shown in Figure 2.1. The authentication server is responsible for either authenticating the NACs or acting as an intermediary to a back-end authentication architecture. It is the part of the NAS which participates in the message exchanges with the NACs. The enforcement point is the function which actually controls the network access. It separates the traffic of the legitimate NACs and lets it continue and discards everything else.

If the network access system is not just one access network with a single NAS, there is usually a back-end architecture to manage and control the network access. The back-end architecture can contain a common user database of the Internet service provider and some

control tools, or it can consist of many such operators with co-operation agreements with each other.

2.3 Network Access Protocol Layer

Traditionally the authentication for the network access has been performed on the link layer, like 802.1x [1] in the IEEE 802 links. One disadvantage of the link layer authentication is that the different network access environments have dissimilar link layer protocols with different characteristics. This leads to development of many different protocols to perform the same assignment. To simplify the variety of the network access mechanisms the IETF Protocol for carrying Authentication for Network Access (PANA) Working Group [2] has begun to specify a more multi-purpose protocol to be carried over the IP. Unlike the different link layer protocols, the IP is employed in all the different network access environments and one general-purpose protocol can be used for the authentication in both multi-access and point-to-point links.

Another advantage of implementing the authentication and the network access over the IP is that the used protocol has better possibilities to co-operate with other Internet protocols. The security of the network can be provided by the Internet Protocol Security (IPSec) [3] with the keying material delivered at the authentication. In the Mobile IP [4] [5] the mobile node needs authentication services that can be combined with the network access authentication.

If the authentication is performed on the link layer, the location of the NAS is restricted to the same link with the NAC. The IP layer authentication does not have this limitation and the NAS can locate farther in the network. This makes it possible to build more complicated and scalable access networks. The Internet Service Provider (ISP) can allow the NACs to use some parts of the networks without authentication and initiate the network access only if a NAC desires to use also other services. By managing the IP traffic filtering rules in the NAS, those free networks can locate also behind the NAS.

2.4 Network Access Usage Scenarios

The network access controlling is useful in many different scenarios. If an ISP wants to control the usage of the Internet and perhaps bill for the provided services, it needs to restrict network access to only its customers. To be able to do this, ISP can place a NAS functionality in the access router as in Figure 2.1. The NAS controls the Access Control List (ACL) of the access router so that only authenticated and authorized clients are allowed to send and receive traffic from the Internet. The ISP may also want to offer its customers services and access to some networks free of charge and without authentication. An example of such situation could be a hotel offering network access to its clients. The clients can use hotel's or its partners' commercial web-servers for free, but before accessing to the Internet, they have to authenticate themselves to the service provider.

It is profitable for an ISP to implement the network access control for the traditional Internet clients who access the Internet from their homes e.g. by modems or digital subscriber lines. New, especially wireless, access technologies are increasing the demand for access controlling. The number of Wireless Local Area Network (WLAN) hot-spots is increasing and new access networks are contracted to the airports, hotels and other public spaces. Also the companies can increase the security by implementing network access control in their company networks. If the company provides wireless access to the network, the controlling is essential.

In the future Internet networks, the Mobile IP [5] will play an important role in the network access. In the Mobile IP the clients can roam from access network to another without cutting the connections to the Internet. As the clients can access to the Internet also outside their home domain, the network access system requires a workable authentication back-end architecture to enable the authentication within different location. A mobile node accessing to the Internet outside its home domain is presented in Figure 2.2. The figure demonstrates also the connections between different ISPs in the back-end architecture.

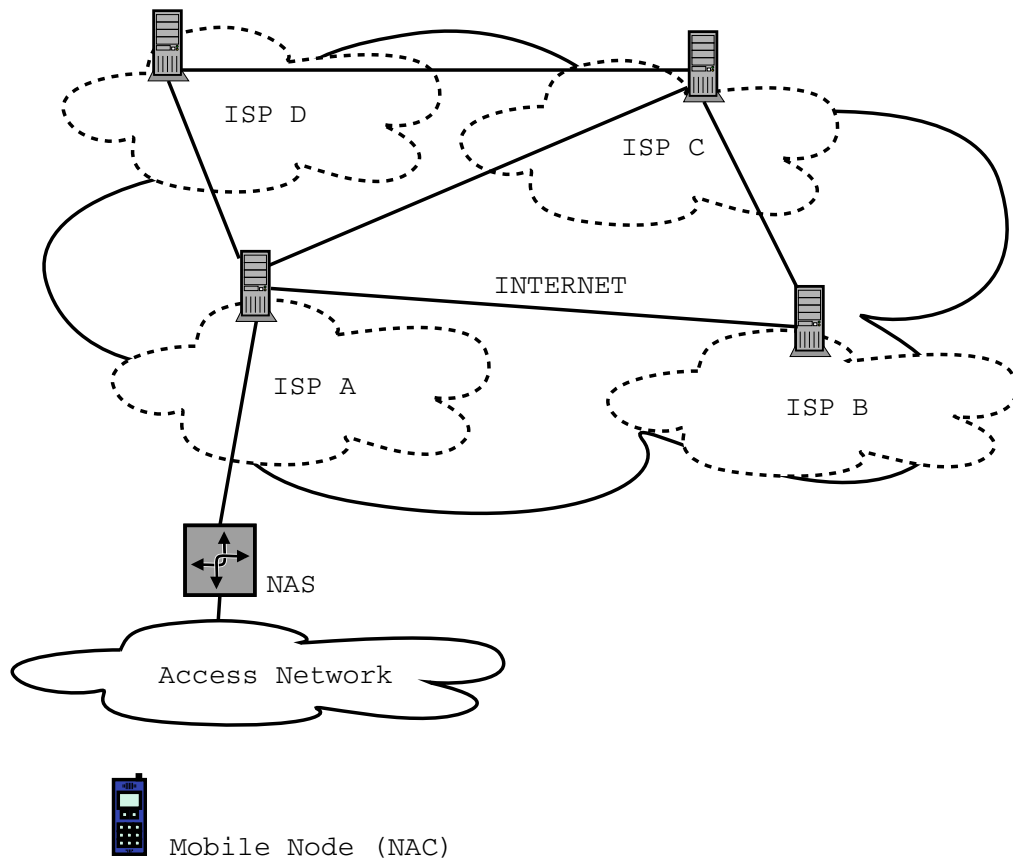


Figure 2.2: Mobile device roams from an autonomous system to another.

3 AAA Protocols

The widespread employment of the Internet, the variety of the different access technologies and the increasing number of the mobile clients have created a demand for powerful tools to manage the Authentication, Authorization and Accounting (AAA) among the Internet Service Providers. The IETF's AAA working group [7] is focused on the development of the requirements for the AAA as applied to the network access. This chapter provides the working knowledge on the AAA architecture and the AAA protocols, that are needed to understand the following chapters.

3.1 AAA Architecture

The AAA architecture [8] consists of three elements: Authentication, Authorization and Accounting.

Authentication is an act of verifying a claimed identity. In the network access it basically means the verification of the identities of the NAC and the serving network, before the NAC gets a right to access to the desired networks. The authentication methods are based on unambiguous pieces of information, like an username-password combination or a secret shared key. An authenticator compares these data elements against its own information and if they match, the authentication succeed.

Authorization is an act of determining if a particular right, such as access to some resource,

can be granted to the presenter of a particular credential. The authorization and the authentication are usually performed together in the AAA architecture, but the authorization does not need to be based on the authentication.

Accounting is an act of collecting information on the resource usage for the purpose of trend analysis, auditing, billing or cost allocation. The accounting is especially vital part of the AAA architecture for the commercial Internet service providers, who need it to be able to make their services profitable.

The requirements for the network access AAA protocol are defined in the IETF RFC 2989 [9]. The common requirements are:

- scalability to support a huge number of clients and network elements
- fail-over recovery mechanism in case one server fails
- mutual authentication between different AAA servers
- transmission level security by the confidentiality and the integrity protection
- data object confidentiality and integrity
- ability to transfer certificates
- reliable AAA transport mechanism
- support for both the IPv4 and the IPv6
- support for the proxy and the routing broker AAA servers (AAAB)
- auditability of the whole AAA protocol message
- ability to carry service-specific attributes.

In addition to the common requirements, the RFC defines also special requirements for authentication, authorization and accounting. For the authentication is required e.g. the support for the use of the Network Access Identifier (NAI) [10], which is used to link the clients to the right AAA servers, and the support to carry Extensible Authentication Protocol (EAP) [11] packets as the payload of the AAA messages. The authorization specific requirements demand e.g. that the AAA protocol must be capable to carry network access filter rules and thereby administer dynamically configurable packet filters, which are an essential part of the Network Access Servers.

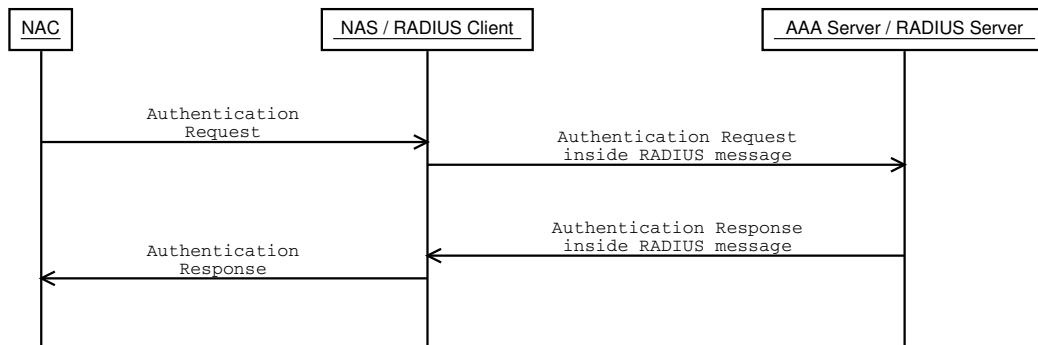


Figure 3.1: RADIUS Client-Server model

3.2 Remote Authentication Dial In User Service

The Remote Authentication Dial In User Service (RADIUS) protocol is defined in the IETF RFC 2865 [12]. The RADIUS is a protocol for carrying authentication, authorization and accounting information between a Network Access Server (NAS) and an AAA server. It was developed to handle the authentication in the dial-in services, in which it is still widely used. The later defined RADIUS extensions [13], such as the support for the Extensible Authentication Protocol (EAP) and operation with the IPv6 [14] have made the RADIUS more versatile AAA protocol.

The RADIUS is a client-server protocol. Figure 3.1 demonstrates the RADIUS client-server model in the network access. The messages between the NAC and the NAS are carried over a network access protocol, such as the 802.1x [1] implemented in many WLANs. The NAS operates as a RADIUS client and is responsible for acting as an intermediary between the NAC and the RADIUS AAA server. It receives authentication requests from the NAC and forwards them inside RADIUS messages to the RADIUS server. The RADIUS server authenticates the received connection requests and returns the authentication responses with necessary configuration information inside a RADIUS message. The NAS receives the responses and forwards them to the NACs.

The RADIUS server can also act as a proxy client to other RADIUS servers or other kind of authentication servers. This kind of functionality is required when the operator has a large and complicated network of AAA servers or when the operator's AAA infrastructure is connected to other operators.

All the connections between the RADIUS clients and the RADIUS servers and between the RADIUS servers are authenticated through the use of shared secrets, which are never sent over the network. In addition, all the credentials, like the user passwords, are sent encrypted. In consideration of these security functions and the fact that the RADIUS connections and servers are usually administrated by a single Internet operator, the AAA infrastructures based on the RADIUS can be considered safe, at least in the Internet's scale.

3.3 Diameter

Although the RADIUS is widely in use, it has restricting deficiencies. It is not very scalable and not easily expandable. To solve these problems, the IETF AAA Working Group is defining a new AAA protocol, Diameter. The Diameter protocol consists of the Diameter base protocol [15] and of the different Diameter applications. The Diameter base protocol provides only the minimum requirements required for a AAA protocol. The base protocol can be used by itself for accounting purposes only, or it may be used with a Diameter application, like the Mobile IPv4 [16], the network access [17], or the EAP support [18].

The Diameter itself does not define the parameters for the authentication, the authorization and the accounting. It specifies only the formats of the messages and the way data is transmitted. All the data delivered by the Diameter is in the form of an Attribute Value Pairs (AVP). Some of the AVP values are used by the Diameter protocol itself, while others are used to deliver data associated with the particular applications employing the Diameter.

The Diameter defines three different network elements: a client, an agent and a server. The Diameter agent acts similarly to the RADIUS client, generating Diameter messages to request authentication, authorization, and accounting services for the NAC. The Diameter agent is a node that does not authenticate or authorize messages locally. It can act as a proxy and redirect or relay the messages to the Diameter servers, which perform the authentication and the authorization of the NACs. A Diameter node may also act as an agent for certain requests while acting as a server for others.

The approach to the protocol operation in Diameter is different to RADIUS's client-server model. Any node can send a request and initiate a connection. In that sense, the Diameter is

a peer-to-peer protocol. The Diameter protocol structure with a common base under different application protocols, the AVP data model and the Diameter agents make it possible to build complicated but still configurable and scalable AAA networks to serve many different kind of clients.

4 EAP Authentication Protocols

Extensible Authentication Protocol (EAP) is a general protocol for authentication. It was originally developed to be an extension for Point-to-Point Protocol (PPP) [19] so that different authentication mechanisms could be used.

EAP was originally defined in RFC 2284 [11] and was meant to operate only over PPP, but today EAP has also been implemented with switches and access points using IEEE 802 protocols. In a new IETF Internet-Draft [20] these new purposes of use are considered and EAP is changed to be more compatible with other protocols and environments.

4.1 Operation

The EAP conversation takes place between the Network Access Client (NAC) and the AAA server as depicted in Figure 4.1. One of the benefits of using EAP is that new authentica-

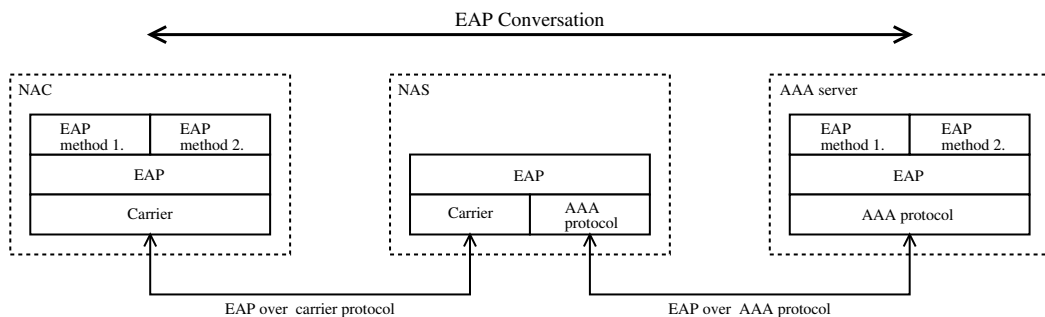


Figure 4.1: EAP operation

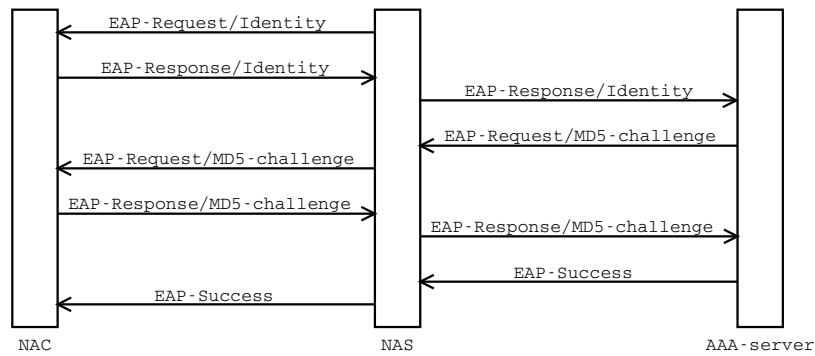


Figure 4.2: An example of the EAP authentication procedure

tion methods can be developed without modifying the code in the Network Access Server (NAS). This way, the NAS acts only as a “pass-through” and delivers the EAP information between the NAC and AAA server. EAP authentication methods are implemented only in the end points of the EAP conversation and the structure of the NAS can be simpler and more stable.

The EAP messages are carried over different carrier protocols in the different parts of the EAP conversation path. Between the NAC and the NAS EAP messages are usually transported over the link layer protocol, like in the 802.1x [1] and in the Point to Point Protocol over Ethernet (PPPoE) [21]. Another possibility is to use the advantages of the widespread Internet Protocol, and use protocols such as ICMP [22] or UDP [23] to carry the EAP messages. The path between the NAS and the AAA server and inside the AAA infrastructure the EAP messages are transported encapsulated into the AAA protocol messages. It is also possible that the NAS and the AAA server are located in the same network element and the EAP messages use only one carrier. This solution is not very scalable, because every client network would need a separate user database.

The EAP is a client-server protocol and the EAP conversation consist of request-response -pairs between the NAC and the AAA server. Figure 4.2 demonstrates the actual use of the EAP with MD5 -challenges, a procedure that is similar to the PPP Challenge Handshake Authentication Protocol (CHAP) [24]. The NAS initiates the EAP conversation by asking the NAC to identify itself by sending an EAP-Request/Identity -message. The NAC replies with an EAP-Response/Identity, which includes the NAC’s identity, e.g. username. The NAS forward the response in an AAA message to the AAA server, which recognizes the NAC as one of its clients. The AAA server challenges the NAC to authenticate itself by

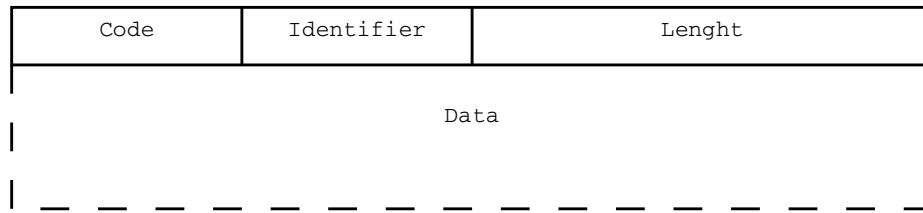


Figure 4.3: EAP packet format

sending an EAP-Request/MD5-Challenge -message. The NAC uses the challenge and the shared secret and calculates a checksum, which it sends back to the AAA server in an EAP-Response/MD5-Challenge -message. The AAA server verifies the checksum and if the authentication succeeded, replies with an EAP-Success -message. Otherwise the AAA server sends an EAP-Failure -message and the NAC doesn't get access to the network.

The EAP can support multiple authentication methods. The AAA server decides which method to use with each client based on the NAC's identity and their pre-negotiated agreements. The AAA server can in fact require more than one method from the NAC before accepting the authentication. Still, usually only one method is used since the authentication procedure should be as fast and light as possible.

4.2 Message Formats

The format of the EAP packets is illustrated in Figure 4.3. All EAP packet headers begin with four octets header. First eight bits indicate the code of the message. The EAP defines four different message codes: Request(1), Response(2), Success(3) and Failure(4). The next eight bits are the Identifier which helps in matching Responses with Requests. The AAA server selects an unique number to each Request and the NAC copies that value to its responses. The rest 16 bits describe the Length of the EAP packet in octets including the header. This is also the format of the EAP-Success and the EAP-Failure messages, which have no data to be carried.

The format of the EAP-Request and the EAP-Response messages is shown in Figure 4.4. After the common EAP header is a 8-bit value Type, which defines the type of the Request or the Response. Normally the Type of the Response is the same as the Type of the Request it is replying. The Type-Data field carries the actual payload of the Request or the Response

Code	Identifier	Lenght
Type	Type-Data	

Figure 4.4: EAP-Request and EAP-Response message format

and its length and contents depend on the Type of the particular message.

All EAP implementation must support four Request or Response Types, which are defined in the EAP specification. The Types are Identity (1), Notification (2), Nak (3) and MD5-Challenge (4). The Identity Type is used to query the identity of the client as in the example above. The Notification Type is optionally used to convey a displayable information from the AAA server to the NAC and the NAC should display this message to the user. The Nak Type is used only in the Response messages to inform the AAA server that the requested authentication method is not supported by the NAC. The Response can then contain authentication methods that the NAC would be able to use.

The authentication methods are Types 4 and above. At the moment the EAP implementation must support only authentication with MD5-Challenges, but also some other methods are defined or under development. An example of such is the UMTS Authentication and Key Agreement carried over EAP which is described in Section 4.4.

4.3 EAP Security Deficiencies

The EAP itself does not provide built-in support for per-packet data origin authentication, replay or integrity protection. As a result, using the EAP without additional security mechanism is very vulnerable to many different kind of security attacks, like modification of the packets or the Denial of Service attack. The risk is especially critical in the wireless environments.

The EAP conversation can be secured by creating a protected channel between the NAC and the AAA server at the beginning of the EAP conversation. This can be done e.g. by Protected EAP Protocol (PEAP) [25].

4.4 Authentication and Key Agreement over EAP

In the Universal Mobile Subscriber System (UMTS) the mutual authentication between the client and the serving network and the key distribution is implemented using the Authentication and Key Agreement (AKA) protocol [26]. The AKA is based on the challenge-response mechanisms and on a shared secret between the client and its home environment. In the 3G mobile networks, the AKA is used both for the radio network authentication and the IP multimedia service authentication. The AKA runs typically in an UMTS Subscriber Identity Module (USIM), a smart card like device, but can also be implemented in the host software.

The use of the AKA in the IP environment is specified in the IETF Internet-Draft EAP AKA Authentication [27]. The idea is to encapsulate the AKA messages inside the EAP, so that the AKA could be used to the authentication and the key distribution wherever the EAP is available. This allows several new applications for the AKA. The EAP AKA can be employed as a secure PPP authentication method in the every-day Internet usage and it can offer additional security and session key distribution possibilities to the WLAN environments. If an operator provides both mobile phone and Internet services, the usage of the same authentication mechanisms and algorithms with all the clients would simplify its client database and control, since the Internet clients could rely on the existing mobile phone infrastructure. In the near future, some mobile phone or multimedia terminals can access both the cellular mobile networks and the wireless Internet networks like the Wireless Local Area Networks (WLAN). If the client device can use the same authentication protocols, algorithms and service agreements in both network environments, it simplifies the implementation and saves the scarce resources.

The EAP AKA also provides additional security to the EAP, so that it can protect against the known security vulnerabilities [20] [27].

The AKA is based on symmetric cryptography and it requires a pre-negotiated service agreement between the NAC and the NAC's home AAA server. The cornerstone of the mechanism is a permanent 128-bit master key K , that is shared between the NAC and the AAAH.

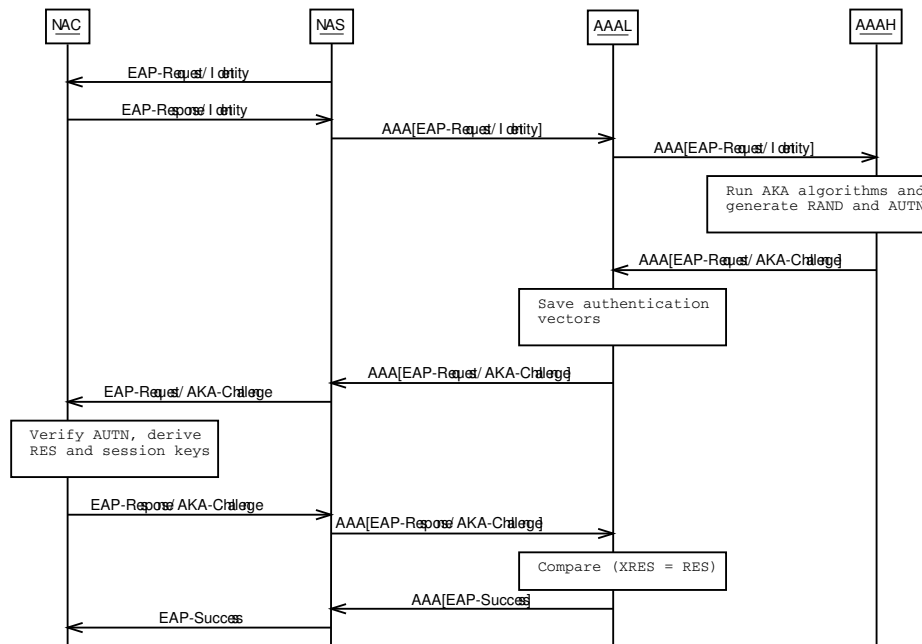


Figure 4.5: EAP AKA message flow

The message exchange between the different network elements is illustrated in Figure 4.5. The operation initiates like in any EAP conversation with a normal EAP-Request/Identity -message from the NAS to the NAC. The NAC becomes aware that the authentication is required and replies with an EAP-Response/Identity -message. The response contains the NAC's Network Access Identifier (NAI) [10], by which the NAC's home AAA server can be reasoned. These messages are no different to any other EAP messages, so at this stage the EAP-AKA is not exactly yet started, although the NAC is an EAP-AKA client.

The NAS encapsulates the EAP message inside an AAA protocol message and forwards it to the local AAA server (AAAL). If the NAC is accessing to the network inside its own home domain, the AAAL handles the response by itself. Otherwise the AAAL forwards the response to the NAC's home AAA server (AAAH) according to the NAI's realm part. The AAA server where the response finally ends up acts as an EAP server and is the other end of the EAP conversation. The AAAH recognizes that the NAC is one of its EAP-AKA clients and initiates the actual EAP-AKA protocol.

The AAAH generates the AKA authentication vectors, based on the shared key K and a sequence number used by the AKA. An AKA authentication vector consists of 128-bit random number RAND, an 128-bit authenticator part AUTN used for authenticating the

Code	Identifier	Length
Type	Subtype	Reserved
AT_RANDOM	Length	Reserved
RAND		
AT_AUTN	Length	Reserved
AUTN		
AT_MAC	Length	Reserved
MAC		

Figure 4.6: EAP-Response/AKA-Challenge message format

network to the NAC, an 128-bit expected result from the NAC XRES and 128-bit session keys, the Integrity Key (IK) for the integrity check and the Cipher Key (CK) for the encryption [28].

After the generation of the authentication vectors, the AAAH constructs an EAP-Request/AKA-Challenge by which it initiates the mutual authentication. The format of the EAP-Request/AKA-Challenge message is shown in Figure 4.6. The EAP message carries the RAND and the AUTN of the first authentication vector to the NAC. The message is integrity protected by the message authentication code MAC. The MACs are keyed with the message authentication key K_{aut} , which is derived from the IK and the CK. The derivation of the keys is described in the EAP AKA Authentication Internet Draft [27].

The actual authenticator in the EAP-AKA procedure is the local AAA server. So if the AAAL and the AAAH are not the same, as it often is e.g. in the Mobile IP, the AAAH has to deliver the AKA authentication vectors to the AAAL. The AAAH sends the authentication vectors and the EAP-Request in an AAA message to the AAAL, which stores the vectors for the later use and forwards the EAP-Request to the NAC via the NAS.

The NAC receives the EAP-Request/AKA-Challenge message and verifies that the AAAH is who it claims to be by checking the AUTN value. If the authentication succeeds, the NAC derives the session keys IK and CK, calculates its own authentication result RES and sends it to the NAS in an EAP-Response/AKA-Challenge message. The format of the

Code	Identifier	Length
Type	Subtype	Reserved
AT_RES	Length	Reserved
RES		
AT_MAC	Length	Reserved
MAC		

Figure 4.7: EAP-Response/AKA-Challenge message format

Response is shown in Figure 4.7. The EAP-Response/AKA-Challenge consist of the 128-bit RES and the authentication code. The NAS forwards the Response to the AAAL in an AAA message and the AAAL compares the expected authentication result XRES with the NAC's result RES. If the results are equal, the mutual authentication is succeeded and the AAAL informs the NAC with a regular EAP-Success message. Along with it, the AAAL delivers the derived keying material, the IK and the CK to the NAS to be used to protect the further communication.

The EAP-AKA provides identity management to both identify the NACs and to protect the NACs' true identities against the identity collection and tracing security attacks. When the NAC initiates the authentication for the first time, in all the cases it has to use its real identity in the EAP-Identity Response message. However, the EAP-AKA includes optional identity privacy support, which makes it possible to hide the clear-text permanent identity and to make the NAC's connections unlinkable to eavesdroppers. The identity privacy is based on the temporary identities, which are pseudonyms that both the NAC and the AAA server can link to the real identity. At the initial authentication, the NAC can register a new temporary identity to the AAA server. When the NAC re-authenticates itself to the same AAA server, it uses the temporary identity to identify itself instead of its real identity. Of course, if the NAC roams and tries to access the network in a different domain, it has to use its real identity again to identify itself to the new AAA server.

5 Internet Protocol Security

The Internet Engineering Task Force (IETF) [6] has a working group called IP Security (IPSec) [29], which is responsible for defining standards and protocols relating to the Internet security.

The set of security services that IPSec can provide includes access control, packet integrity, data origin authentication, rejection of replayed packets, confidentiality and limited traffic flow confidentiality [3]. These services are provided at the IP layer, therefore they can be used by any higher level protocol, e.g. TCP, UDP, ICMP, etc.

IPSec uses two protocols to provide traffic security: Authentication Header (AH) [39] [30] and Encapsulating Security Payload (ESP) [31]. The Authentication Header provides connectionless integrity, data origin authentication and anti-replay protection. The Encapsulating Security Payload provides the same features as the AH in addition to optional data confidentiality and limited traffic flow confidentiality [3]. From the two IPSec traffic security protocols, in this thesis the main attention is on the ESP, because it provides wider range of security features. In addition to the traffic security protocols, the IPSec defines an Internet Key Exchange (IKE) [32], a key exchange protocol to be used to create keying materials and to negotiate session protocol parameters for the IPSec connection.

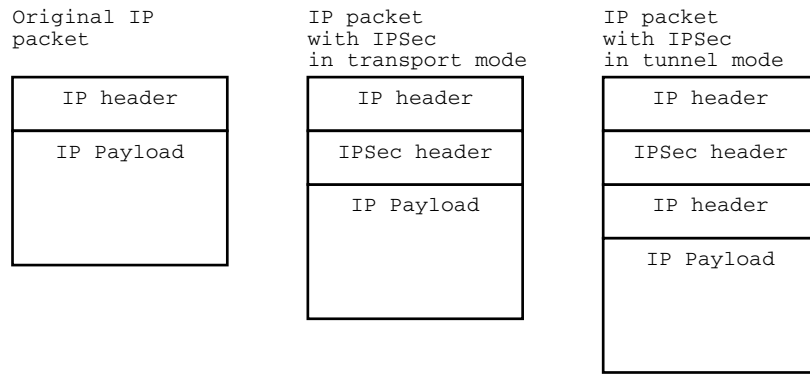


Figure 5.1: IP packets protected by IPSec in transport and tunnel mode.

5.1 General Operation

The IPSec traffic security protocols, both AH and ESP, can be used to protect either the entire IP packet or the upper layer protocols which the IP packet is carrying in the payload. This distinction is handled by considering two different modes of using IPSec: the transport mode which protects the upper-layer protocols and the tunnel mode, which protects the entire IP datagram. The difference between these two modes is illustrated in Figure 5.1. In the transport mode, the IPSec header is added between the IP header and the IP payload. In the tunnel mode, the entire IP packet is protected by encapsulating it inside a new IP packet and the IPSec header is inserted between the outer and inner IP headers. Both IPSec protocols, AH and ESP, can operate in either transport and tunnel mode.

5.1.1 Authentication Header

The AH provides packet integrity, data origin authentication and anti-replay protection. The AH provides authentication for as much of the whole IP packet as possible, only some IP header fields of which values at receiver's end can not be predicted, are left outside the authentication. These fields deal with quality of service, like the flow label in IPv6, and routing like time to live in IPv4, and are not critical in the authenticity of the actual IP payload. At calculation of the Authentication Data to the AH, these fields are set zero.

The AH adds a new header to the packet between the IP header and the data to be protected. The format of the AH in the transport mode is described in Figure 5.2. The header format in the tunnel mode is similar with the exception that a new IP header with the AH is

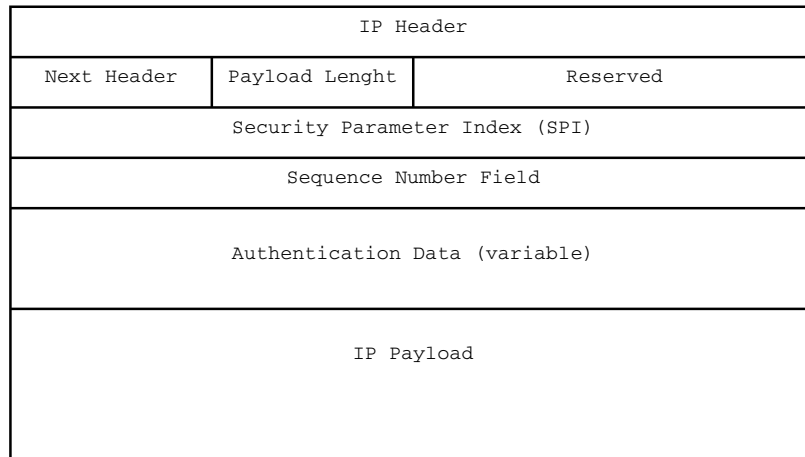


Figure 5.2: AH header format in the transport mode

constructed in front of the original IP packet, which is capsuled to the AH's payload.

5.1.2 Encapsulated Security Payload

The ESP provides all that the AH provides in addition to optional data confidentiality and limited traffic flow confidentiality [3]. The ESP header is inserted after the IP header and before the payload to be secured. In the transport mode the payload is an upper layer protocol data and in the tunnel mode, a whole IP packet, which is described in Figure 5.3.

The ESP in tunnel mode is especially useful, since it captures and encrypts the whole IP packet to its payload. This makes it possible to build Virtual Private Networks (VPN) between the security gateways or between a host and a security gateway. A VPN tunnel e.g. enables a secure connection of two secure networks through insecure network like the Internet. Such an arrangement is illustrated in Figure 5.4. All the traffic between the hosts x and y is encapsulated and encrypted between the two security gateways while it goes through the Internet.

5.2 Security Associations

Authentication and encryption requires that the sender and the receiver agree on a key, on an authentication or encryption algorithm and a set of necessary parameters such as the lifetime

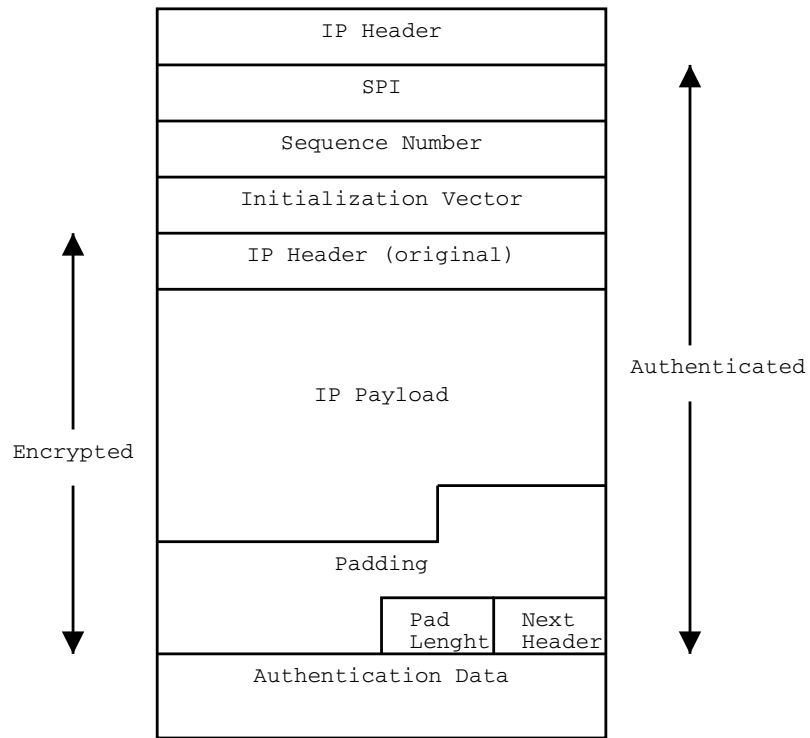


Figure 5.3: ESP header format in the tunnel mode

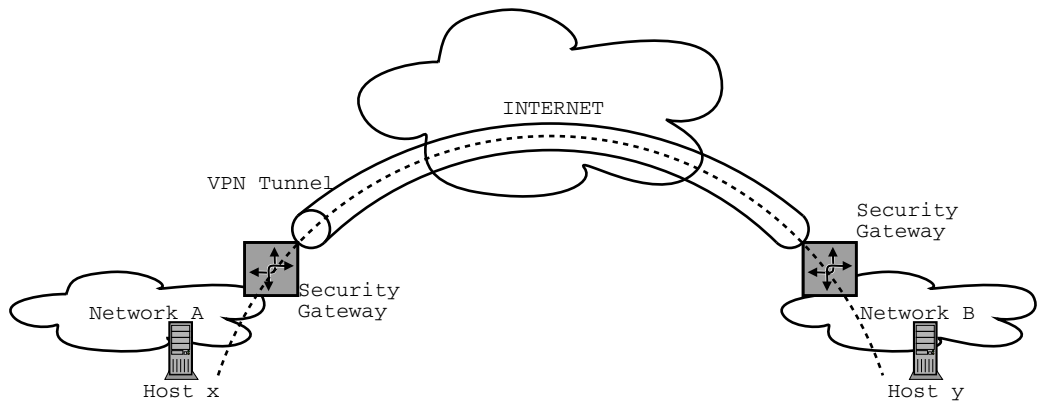


Figure 5.4: A VPN tunnel connects securely two separated networks through an insecure network.

of the keys or the details of the algorithm's utilization. This set of agreements constitutes a Security Association (SA). When a packet is received, it can be verified or decrypted only if the receiver can link it with the context of a right SA. An IPSec Security Association is an unidirectional construct, that defines an association between the security services and the traffic to be protected. The IPSec SAs are identified by a Security Parameter Index (SPI), an IP destination address and a security protocol, either AH or ESP. From these parameters the receiver can identify the SA to which an incoming packet is bound. The SPI is an arbitrary 32-bit value and it is normally selected by the destination system upon establishment of the SA.

In the IPSec implementation the SAs are stored in the Security Association Database (SADB), in which each entry defines the parameters associated with one SA. The IPSec requires the following parameters: a 32-bit SPI, a 32-bit sequence number counter and a sequence number overflow flag, a 32-bit replay protection window, the ESP or AH authentication and encryption algorithms and keys, whether the IPSec protocol is in the tunnel mode or in the transport mode, the path Maximum Transfer Unit (MTU) and a lifetime for the SA. The implementation should maintain two different lifetimes: a soft lifetime and a hard lifetime. The soft lifetime warns the implementation beforehand to initiate an action to replace the SA with a fresh one before it is destroyed at the hard lifetime. The lifetime can be based either on a time interval or on a amount of bytes sent with the particular SA.

One SA secures traffic to one direction with one specified security settings. To secure a typical, bi-directional communication between two hosts or security gateways, two SAs are needed, one in each direction. If the communicating parties want to use different kind of security services to different types of traffic, they need a new SA for each of them. So in fact, there can be several SAs between two hosts to both directions to satisfy different security level requirements.

An example of an SA is in Figure 5.5. It defines an IPSec ESP tunnel to an IPv4 host 130.230.52.73 and uses AES [33] protocol in CBC mode for the encryption and HMAC-MD5-96 [34] for the authentication. It uses periods of time in seconds for the lifetime control.

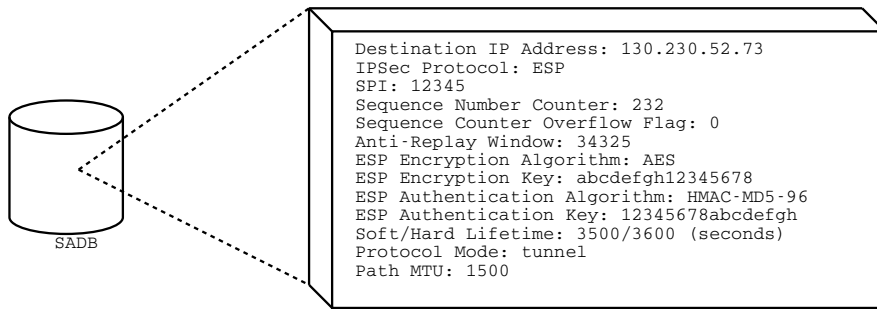


Figure 5.5: An example of an SA defining ESP tunnel to an IPv4 host 130.230.52.73

5.3 Security Policies

The user or the system administrator controls how the IPsec is applied to the traffic transmitted or received by host by the security policies. The security policies are stored in the Security Policy Database (SPD), which uses the SAs to enforce the security policies in the IPsec environment.

The SPD specifies what services are offered to IP datagrams and in what fashion. It must be consulted during the processing of all the traffic, both inbound and outbound, including all non-IPsec traffic. The SPD separates the traffic that is afforded IPsec processing and the traffic that is allowed to bypass the IPsec. The processing choices are discard, bypass IPsec or apply IPsec to the datagram. The first choice drops all packets that are not allowed to be sent or received at all. The second refers to traffic that is allowed to continue without any IPsec processing and the third requires applying IPsec to the packet. For such traffic the SPD must specify the security services to be provided, protocols to be employed and the algorithms to be used.

The SPD sorts out the traffic by selectors, which are fields in the IP packet like the destination IP address or the upper layer protocol. Based on these selectors the SPD decides what kind of processing the packet needs. If the selected policy requires IPsec processing, the SPD has a link to a proper SA in the SADB which should be used. If the link is missing, the particular SA is not yet created and the SPD must initiate a procedure to create a new SA.

The security policies are inserted to the SPD by the user or the system administrator. A simple example, where a host connects to a network from an insecure link, could require

only two security policies in the SPD: one to manage the outbound and one to inbound IPsec processing of the traffic. If the both policies required all traffic to be protected by an ESP tunnel to the specified security gateway, all communication in and out from the particular host in the insecure link would be either secured or discarded.

5.4 IP Traffic Processing

The processing of the IP traffic is concerned extensively in the IETF RFC 2401 Security Architecture for the Internet Protocol [3].

The outbound processing of the IP traffic is rather simple. The IPsec implementation compares each outgoing packet against the SPD and decides accordingly what processing is required for the particular packet. Also all packets that will not need IPsec have to be checked because otherwise the implementation is not able to know how to deal with them. If no policy is found in the SPD that matches the packet, it must be discarded and audited. If the packet doesn't need IPsec processing, it bypasses the IPsec and continues like in a normal IP stack. If the IPsec processing is required, the packet is mapped to an existing Security Association in the SAPD, or a new SA is created. The selected SA will then direct what kind of IPsec protocols will be used with the particular IP packet.

The inbound processing of the IP traffic is slightly more complicated, since the implementation must carefully link the incoming packet to existing Security Associations and Security Policies. Like in the outbound processing, every incoming IP packet must be inspected and compared against the SPD.

When a new IP packet arrives, the IPsec implementation identifies the requirement of the IPsec processing from the IP Next Protocol in the IPv4 and of AH or ESP as an extension header in the IPv6 context. If no IPsec processing is required and the packet matches that kind of policy in the SPD, it will continue in the IP stack normally. If the SPD denies all the traffic without the IPsec, the packet will be discarded and audited. If the incoming packet requires IPsec processing, it must be mapped to a proper Security Association in the SADB. The SAs are identified by the SPI, IP packets destination address and the IPsec protocol. If the SA lookup fails, the packet must get dropped and an error log written. The

found SA is used to do the IPSec processing, e.g. authenticating and decrypting the packet and checking the packet's selector values, such as the destination address in the inner header of a tunneled packet.

After the IPSec processing, the IPSec implementation tries to find an incoming policy in the SPD that matches the packet. If the SA found based on the packet's selectors matches the kind and order of the SAs required by the policy, the resulting packet is passed to the transport layer or to be forwarded. Any conflict or error in the linkage of the Security Associations and Policies causes the dropping of the packet.

5.5 Internet Key Exchange

The IPSec Security Associations can be created either manually or automatically by a specific method, Internet Key Exchange (IKE). If there are only few hosts using IPSec and thereby only some SAs are required, the manual method can be used. When a SA is created manually, the system administrator configures each communicating system with the keying material, adds the needed parameters to the SADB and the new SA is ready to use. The manually created SAs are static and so they don't have lifetime values. The administrator have to refresh them regularly with new keying material. The manual techniques can be practical and useful in the small, static environments but they don't scale well. Widespread deployment and use of the IPSec requires an Internet-standard, scalable and automated SA management protocol.

The automated key management protocol with the IPSec is defined in three IETF RFCs: RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP (DOI) [35], RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP) [36] and RFC 2409 The Internet Key Exchange (IKE) [32]. The ISAKMP defines the common framework and the packet formats, the IKE defines the key exchange procedures and the DOI describes how the IKE and the ISAKMP are used in the negotiation of the Security Associations for the IPSec.

The IKE operates in two phases. In the first phase it performs mutual authentication and establishes an IKE security association that can be used to efficiently establish SAs for

the IPSec traffic security protocols. The IKE parties authenticate each other by using a shared secret, public keys or digital signatures. The two latter methods require trust on both parties' public keys, which requires the existence and employment of the Public Key Infrastructure (PKI). In the second the IKE performs the actual negotiation of the IPSec SAs. The negotiating parties agree on the encryption and the authentication algorithms, on the keying material and on the lifetime of the new SA.

IKE has a number of deficiencies from which the three major are the high number of rounds, its vulnerability to the Denial of Service attacks and the complexity of its specification. Especially this complexity has led to interoperability problems between different implementations. These disadvantages in the IKE have led to developing new key exchange protocols specifically for Internet security applications. At the moment there are two proposals to replace the IKE: a new version of the IKE, IKEv2 [37] and a totally new protocol called Just Fast Keying JFK [38].

The IKEv2 is based on the IKE, but the protocol is lighter and simpler. The number of messages and available options is decreased to ease the implementation and the interoperability. In the IKEv2 more attention is focused on the protocol's robustness and security against the DoS attacks. The JFK has a slightly different approach to the key exchange problem than the IKE versions, although the result, the IPSec SAs, is the same. The JFK intends to be fast and effective without unnecessary negotiation options, still without compromising the security.

5.6 Authentication and Encryption Algorithms

The IPSec uses symmetric algorithms to provide security by the AH and the ESP. The compulsory sets of algorithms, which all IPSec implementations should fully implement are defined in the AH and the ESP RFCs [39] [31]. All IPSec ESP implementations should support encryption with the DES in CBC mode [40] and with the NULL algorithm [41]. The required algorithms for the AH are HMAC with MD5 [34] and SHA-1 [42].

As the calculation power of the new computers increases all the time, the strength of the old authentication and encryption algorithms is weakening. The IETF IPSec WG is up-

dating the IPSec protocol specifications and at the same time gives new recommendations for the security algorithms. In the new ESP Internet Draft [43] the compulsory to implement encryption algorithm is the Advanced Encryption Standard (AES) [33] with 128-bit keys in CBC mode [44], which is defined by the National Institute of Standards and Technology (NIST) [45]. The AES provides increased security with computational efficiency, flexibility, simplicity and ease of implementation to the IPSec ESP.

6 Functional Requirements of Network Access

A general network access system needs to have many different features and it has to manage to operate in many different environments. Still it should remain simple, efficient and rather unnoticeable to the end users. In this chapter is derived the functional requirements of the network access protocol to fulfill these needs.

6.1 General Requirements

The general requirements of a network access system cover the operational environment, the support and co-operation with different link layers and network protocols and the technical requirements, such as the bandwidth consumption and the response times.

6.1.1 Operational Environment

The Internet Protocol (IP) can be carried over various link layers. If the authentication and the network access operation are implemented over the IP, they must not rely on some link layer specific characteristics. The access network links can be divided into broadcast and non-broadcast links. The lack of broadcasting possibility in some access technologies implies that a generic network access system can not be based on delivering broadcast

messages.

A Network Access Client (NAC) needs a functional IP address to be able to perform the authentication and the network access over the IP. The access network has to provide IP addresses dynamically, if the NACs do not have predetermined IP addresses. In the IPv4 [46] this can be done with the Dynamic Host Configuration Protocol (DHCP) [47] and in the IPv6 [48] with either stateless address autoconfiguration [49] or with the IPv6 version of the DHCP [50]. The network access system can either co-operate with the address configuration of the NACs, or simply wait for it to be accomplished and then initiate the authentication procedure.

The network access and the authentication are especially important in the Mobile IP [4] [5], where the mobile clients can roam and access the Internet in different locations. The network access system must not interfere or prevent the operation of the Mobile IP. Instead, it can either co-operate with the Mobile IP, for example in the authentication procedure, or simply carry out the network access and the Mobile IP separately.

The authenticating of the NACs requires a user database, which contains information of the NAC's identity, something to authenticate the NAC, like a shared secret, and some network access and usage agreement parameters. If the network access system is small-sized and consists of only one or two access networks, the user databases can be located in the Network Access Servers (NAS). But if the system is larger and more complicated, the management and the configuration of different databases in every access network would be awkward and laborious. In such scenarios the Network Access Servers can use a shared user database, which is located in an AAA server in the AAA back-end AAA infrastructure. The network access system must support both possibilities.

6.1.2 Bandwidth Consumption

In the wireless environments the bandwidth is often limited and it is important to avoid unnecessary consumption of its capacity. The network access protocol packets are not useful traffic so their size and sending frequency should be minimized, especially when the bandwidth is low and there are a lot of clients in the same wireless link.

In practice this means two things. First, the network access protocol should work with minimum amount of message exchanges. And secondly, the protocol should try to transmit all the necessary information between the NAC and the NAS with minimum number of parameters.

6.1.3 Response Times

The authentication procedure and the connection establishment to the sought-after networks and services should be fast and unnoticeable to the client, especially when the NAC either arrives to or starts up in a new link and begins to communicate.

The total delay in the authentication consist mainly of three components: the message exchange between the NAC and the NAS, the message exchange between the NAS and the AAA infrastructure and the completion of the cryptographic operations in the different elements.

Since the NAC and the NAS are usually located in the same link or at least near each other, the delay between them is considerably small. The response times can still be minimized by keeping the amount of round trips between the NAC and the NAS as low as possible.

If the network access system has no back-end AAA infrastructure and the user database is co-located in the NAS, the second component of the total delay doesn't naturally exist. Otherwise its influence to response times and to the smoothness of the system may be crucial.

When the NAC is attached to the Internet within the same Internet service provider it has made an agreement about network access, the delay is probably very reasonable. The authenticating AAA server is located within the same autonomous system as the NAC and the connection between the NAC and AAA server runs only in the AS's internal networks and usually only over few hops. Still, the network access protocol should try to minimize the amount of round trips between the NAS and even the local AAA server to smoothen the operation.

The roaming enables the mobile clients to attach to the Internet not only within their own ISP, but also to visit in other networks. The authenticating home AAA server (AAAH) may

locate physically far away from the NAC's attachment point and may also be behind slow and tortuous connections. In these circumstances the delay between the local AAA server (AAAL) and the AAAH may become disturbing. Thereby it is important to minimize the amount of the round trips between the AAAL and the AAAH. In the initial authentication in a foreign domain it is usually mandatory to authenticate the NAC with the AAAH, because the AAAL has no information on the NAC's true identity. But after that, when the NAC moves from a network to another in the AAAL's domain or needs a re-authentication, the AAAL should be able to authenticate the NAC for a specific period of time without help from the AAAH. Of course, when the agreed time is up or the NAC moves to a new foreign domain, the authentication must be done with the AAAH.

The delay of the completion of the cryptographic operations in a network access system depends on the calculation power of the network elements and the complexity of the cryptographic algorithms. The calculation power of the NAC, especially if it is a mobile host, can be limited, and the network access implementation should be planned to minimize the calculation requirements of the NAC. The selection of the cryptographic algorithms is also important, since they have to compromise between the minimum amount of calculation and the required level of security. The modular design of the network elements makes it possible to replace the algorithms easily with new more effective ones if required.

6.1.4 Scalability

When the network access protocol operates over the Internet Protocol, it can be utilized where the IP is used. Since there are many different kinds of link layers, the network access protocol must not depend on any particular feature of one link layer type. This restricts especially the usage of the broadcast, multicast and anycast messages.

At the moment the Internet uses IPv4, but for the network access protocol to be usable also in the near future, it is important that it supports also IPv6. This is not a significant complication, since the basic communication between the parties does not need any IPv4 or IPv6 specific features. In practice, the support for both versions would mean a dual-stack in the NAC and in the NAS and either a dual-stack or two concurrent AAA servers in the AAA infrastructure.

Rule	Direction	Source	Destination	Action
A	Outgoing	130.230.52.73	Any	Permit
B	Incoming	Any	130.230.52.73	Permit
C	Either	Any	Any	Deny

Table 6.1: An example of a simple access control list

The calculation power of the modern computers increases all the time. The algorithms which are secure today may be easily cracked in the future by more powerful computers or by found new weaknesses. Therefore it is important to a network access protocol to be able to update its authentication methods. This can be done for example by negotiating the authentication method at the beginning of initial authentication and by encapsulating the algorithms so that they can be easily changed or updated.

6.2 Access Control

One of the most important tasks of the Network Access Server is the access control. When the network access protocol operates over IP, the access control is executed by a packet filter, which decides whether to forward or drop a packet based on the data in their IP-headers. The packet filter is administered by the NAS, so it can be thought as a dynamically configured firewall [51].

6.2.1 Access Control List Rules

When a packet arrives into the packet filter, it is treated by rules in the Access Control List. The ACL consists of practices which tell what to do with the certain IP packets. The possible actions are Permit when an ACL rule allows to forward the particular packet and Deny when the forwarding is not allowed.

Table 6.1 lists an example of an ACL when one client has authenticated successfully. The client has an IP address 130.230.52.73 and locates in a local network 130.230.52.0/24. The rule A allows the NAC to send IP packets from the local network to any other networks and the rule B allows the NAC to receive IP packets from the Internet. The rule C is a default

Rule	Direction	Source	Destination	Action
A	Outgoing	Any	130.230.53.0/24	Permit
B	Incoming	130.230.53.0/24	Any	Permit
C	Either	Any	Any	Deny

Table 6.2: An example of the ACL with freely available networks

rule and is applied if all else fails. It blocks all other clients' incoming and outgoing traffic from the local network.

Table 6.2 lists an example of an ACL in a situation, where the ISP wants to offer access to some parts of the Internet free of charge and without authentication. Whichever of the clients in the local network can send and receive IP traffic from the network 130.230.53.0/24 without communication with the NAS or the AAA infrastructure.

Of course, the filtering does not have to be based only on IP addresses. The ISP may want to let the clients use only some specific protocols and destination ports. For instance the roaming clients in a WLAN hot-spot could be allowed to use only Hypertext Transfer Protocol (HTTP) [52] for web surfing or Secure Shell (SSH) [53] for connecting to other hosts.

6.2.2 Administration of Access Control List

The NAS adds new ACL rules after the NAC has succeeded in its authentication. The details of the new rule sets are controlled by the policies that the service provider has decided. The policies tell, what kind of access rights the NAC will have and how long they will be valid without re-authentication. The ISP may simply want to give all its clients the same access rights with a specific lifetime or to use classification according to the contracts with the clients. For instance all clients could use the Internet but some certain customer group could also get an access to the service providers private networks or services, a client willing to pay more could get more facilities, like a right to set up a web or FTP [54] server.

The ACL rule policies are located in the client database. If there is no back-end AAA infrastructure, the ACL rule policies have to co-locate in the NAS. But usually when the network access system is more complicated than just a single NAS controlling one subnet

and the client database is updated frequently, the service provider has at least a simple AAA infrastructure. In that case the ACL rule policies are located in the ISP's client registers. When the AAA infrastructure authenticates the NAC, it sends to the NAS the ACL rules related to the NAC in question in the response message. The rules are equipped with a lifetime which they will be valid in the NAS unless removed or modified by new messages from the AAA server.

6.2.3 Authorization Requests

A client may want to ask authorization to access specific networks or to use some specific protocols, which are not available after the basic authentication process. This could be possible for example when the basic authentication enables the clients to use only HTTP for web surfing and the client wants to use some other protocols, e.g. SSH [53] or FTP [54].

If the ISP's AAA infrastructure provides a possibility for the clients to request and get additional services, the decisions whether the clients' requests are accepted or not are done in the AAA infrastructure's client registers. After an approval of a request the NAS updates the ACL rules and notifies the accounting centre about the new conditions.

7 Network Access Security

The importance of a secure connection to the Internet is increasing all the time when new services are added on-line and new access technologies are introduced. Especially the wireless environments and the Mobile IP challenges the security of the network access systems. This chapter describes the network access specific security threats and methods to prevent them.

7.1 Assumptions

The network security in a network access system is composed of three different parts: the security between the NAC and the NAS, the security between the NAS and the AAA architecture and the security within the AAA architecture. This is demonstrated in Figure 7.1. The paths between the NAS and the AAA architecture and between the different AAA servers can be considered secure, because the communication takes place over a secure AAA protocol, such as RADIUS [12] or Diameter [15]. The AAA protocols also operate only inside one Autonomous System (AS) or between ASs who have agreed on a trust relationship. As a result, the most security critical path in the network access system is the path between the NAC and the NAS. Prior to the mutual authentication the NAC and the NAS cannot trust to each other and especially in shared links, the launching of security attacks is rather simple. Most of the attacks presented in this section take place precisely in this insecure path.

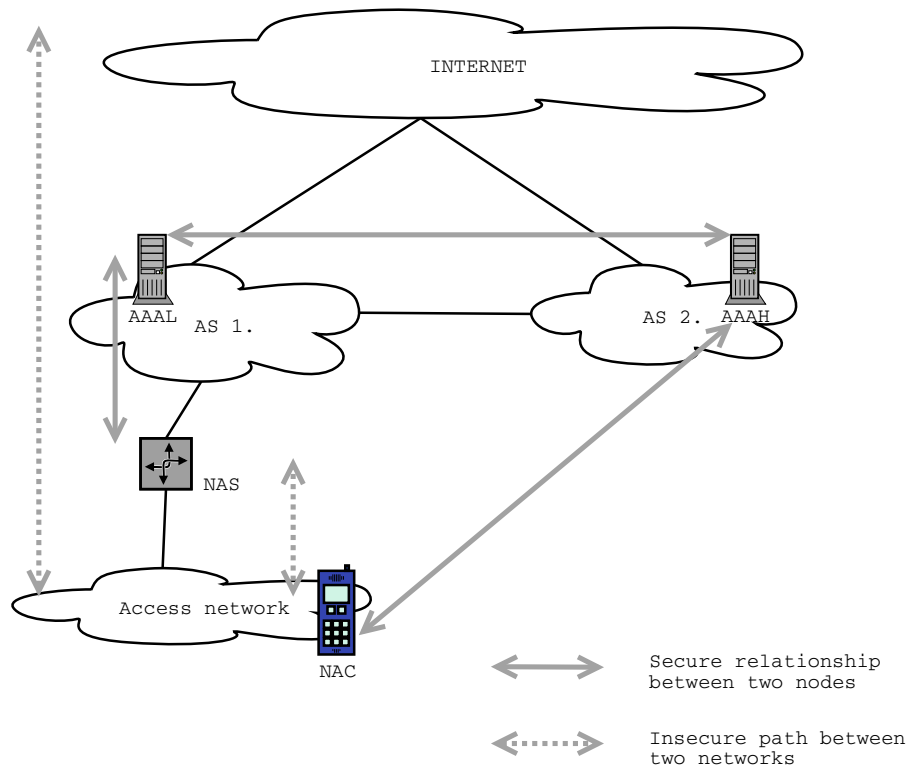


Figure 7.1: Assumptions about Security Relations

The path from the NAC to the Internet is as insecure as any other connection in the Internet without additional security mechanisms added. Therefore if the NAC needs higher level of security, it has to use IPsec [3] or some upper layer security protocols such as SSH [53] or S-HTTP [55] to secure its connections.

Before the NAC can initiate the authentication, it has to have some kind of prearranged contract with the Internet Service Provider. The establishment of the contract requires that the client has to authenticate itself to the ISP reliably. It usually means authentication in person with some official identity card or equivalent. This way the contract can be made binding in law, which is important to both parties in a case of a conflict situation.

The contract specifies all the necessary conditions and details to enable clients' network access and the use of the Internet. The client needs an individual identifier, which can be formed for example from the client's username and the ISP's name like in a Network Access Identifier (NAI) [10]. An example of such identifier could be *ilkka.vesa@tut.fi*, where "ilkka.vesa" is the username in a domain "tut.fi". It is important that the identifier maps the username to its home domain so that the AAA servers from other ISPs can attain

the client's authentication information if the client is roaming away from its home ISP.

The AAA server and the NAC need to have a shared secret to be able to authenticate each other. This secret can be in the form of a password, which the client gives to the network access application in his or her network device, or it can be a permanent key in a Subscriber Identity Module (SIM) or in a UMTS Subscriber Identity Module (USIM). Anyhow, the shared secret has to be given in advance to the NAC and to the client authentication database of the ISP. The secret has to be kept in secret and must not be sent in clear text to the network in any part of the network access system.

7.2 Active Attacks

Active attacks involve some modification of the original data packets or creation of new false packets. The active attacks that are critical in the network access on the network layer are the man-in-the-middle attacks, the replay attacks, the service theft, breaking of the possible encryption and the Denial of Service (DoS) attacks.

7.2.1 Man-in-the-Middle Attacks

A man-in-the-middle attack usually means a situation where a malicious third party hijacks the communication between the original parties. All the communication goes through the man-in-the-middle while both parties think they are communicating directly to each other. The man-in-the-middle can access to all the information sent between the original parties and if he or she likes, change the contents of the communication. It can also send false configuration information and notifications. [56]

In the network access systems the threat of a man-in-the-middle attacks lies between the NAC and the NAS. As the assumptions stated, the path between the NAS and the AAA infrastructure can be considered secure, but the path between the NAS and the NAC is insecure especially in wireless environments. It may not be possible to protect the initiation of the authentication process because the security association between the NAC and the NAS does not exist prior to the authentication and hence there is no way of protecting the

beginning of the communication.

In the man-in-the-middle attack a malicious third party can claim to be the NAS to the real NAC and to be the NAC to the real NAS [57]. This way the NAC is fooled to think that it is communicating with a real NAS and the NAS is fooled to think that it is communicating with a real NAC. The man-in-the-middle can now control the connection between the NAC and the NAS and easily operate other types of attacks against the original parties. This can happen for example in the situation where the NAC only authenticates itself to the AAA infrastructure via the NAS. The attacker can capture the authentication requests from the NAS, prevent the NAC from receiving them and then send the modified versions of them to the NAC. The NAC authenticates itself without suspecting anything to the attacker, which resends the authentication replies to the NAS. The authentication can succeed and the NAC can begin to use the Internet while the attacker can monitor or modify all its traffic, or the attacker can prevent the NAC's access to the network by modifying the credentials the NAC sent to the NAS, or simply by not re-sending the NAC's authentication requests.

The way to prevent the man-in-the-middle attacks in the initial authentication is to use mutual authentication [57]. This way also the AAA infrastructure authenticates itself to the NAC and it can be sure that the NAS really represents the AAA infrastructure and is not a malicious attacker. The mutual authentication is based on the shared secret between the NAC and the NAC's home ISP's authentication server.

If the authentication of the AAA infrastructure fails, the NAC may ask it to re-authenticate itself. But if also the re-authentication fails, the NAC must assume that there is a possibility that a man-in-the-middle attack has taken a place and not try to communicate to the Internet even though it would be possible.

Even if the mutual authentication has succeeded, the malicious attacker can launch a man-in-the-middle attack against the NAC and the NAS, if the communication between them takes place without any additional security. For example in IEEE 802 links an attacker may be able to forward traffic destined to a particular IP address to another by convincing the NAS of a new link layer address. This kind of man-in-the-middle attacks can be avoided by using per-packet authentication [57] like IPSec [3] Authentication Header (AH) [39]. Even though an attacker could redirect the traffic from both original parties to its IP address, the

attack would be recognized because the AH protects also the integrity of both the sender's and the receiver's IP addresses.

7.2.2 Replay Attacks

A replay attack involves a passive capture of a packet sent between communicating parties and re-sending it once or multiple times on a suitable time [56]. This can cause confusion or malfunction in the receiving end or even complete initiation or closing of a communication session.

In the network access systems the replay attacks can occur between the NAC and the NAS. A malicious attacker can for example re-send the messages that caused the authentication failure or success at a later time and create a false failure or success [57]. The attacker can capture old authentication messages and try to get access to the network by reusing them. Or the attacker can re-send old authentication failure messages to the new NACs and so prevent their access to the Internet.

The per-packet authentication does not solely prevent the replay attacks. The attacker can re-send the old messages and the receiver may not recognize the cheating if the authentication does not include a replay protection. The replay protection can be implemented by adding timestamps, synchronized challenges or sequence numbers into the authentication mechanism. In practice, this could be done by using IPSec [3] AH [39], which provides replay protection by monotonically increasing sequence numbers in every packet [58].

7.2.3 Service Theft

A service theft attack means basically stealing the service that was intended for someone else [56]. In the network access systems this usually means that the attacker pretends to be a different NAC to gain unauthorized access to the network [57].

Once the NAC has successfully authenticated, the NAS updates its filters so that the NAC's traffic is allowed to pass through. If the filtering is based only on the IP addresses, the attack can easily fool the NAS to believe that the NAC's MAC address have changed and packets sent to the NAC's IP address are routed to the attacker. In a same way, by using the NAC's

IP address as the source address the attacker can send packets to the Internet. In IPv4 [46] this can be done by Address Resolution Protocol (ARP) [59] and in IPv6 [48] by a Neighbor Advertisement [60] message with the new link-layer address option and the override flag set.

If the filter is based on both the IP and the MAC address, it binds the MAC address to the NAC's IP address at the initial authentication and requires a re-authentication if the either one of the addresses change during the session. The attacker can still use the NAC's connection by using the NAC's MAC address.

When the NAC leaves the network it has to inform the NAS properly so that the resources used by the NAC can be released and accounted properly. If the NAS don't get the notification of the NACs leaving, it keeps assuming that the NAC is present and allow traffic from the earlier IP address and MAC address pair. In this situation a malicious node can pretend to be the NAC by taking its IP and MAC address. The NAS doesn't notice anything and the attacker can use the Internet while the NAC is still charged.

If the disconnect messages are not authenticated and acknowledged by the receiving party, the attacker can use them to launch service theft attacks. The attacker can pretend to be the NAS and send a disconnect message to the NAC. If the NAC accepts the message and stops communication, the attacker can do the same kind of attack as when the NAC was leaving the network.

This kind of service theft attacks can be prevented by the frequent re-authentication or the per-packet authentication. In the frequent re-authentication either the NAC or the NAS initiates a new authentication procedure regularly. The period of time between authentications have to be enough short so that both parties can be sure that no one can steal the connection. The frequent re-authentication has still some weaknesses. If done too often, it produces extra traffic to the network and extra work to the communicating parties. But if the time period between consecutive authentications is long, the risk of service theft attacks increases. The frequent re-authentication also consumes valuable keying material, which complicates the operation and may open some security vulnerabilities related to encryption.

Because already the protecting from the man-in-the-middle attacks demands per-packet authentication, it is also the better way to prevent the service theft attacks. Since every

packet sent between the NAC and the NAS is authenticated, both parties can rely on the origin of the packets and all the un-authenticated packets can be dropped. The disconnect messages must also be authenticated and acknowledged. Without the acknowledgement message the sender of the disconnect message cannot be convinced that the other party received the indication.

7.2.4 Breaking the Encryption

Breaking the encryption means translating the encrypted message back to the original form without knowing the secret decrypting key. There are two general approaches to attacking a conventional encryption methods, the cryptanalysis and the brute-force attack. The cryptanalytic attacks rely on the nature of the algorithm in addition to some knowledge on the general characteristics of the algorithm to attempt to deduce a specific plain-text or to deduce the key being used. If the attack succeeds in finding out the key, the attacker can decrypt all future and past messages encrypted with that key. In the brute-force attack every possible key is tried on a piece of ciphertext until an intelligible translation into plaintext is obtained.

As the calculation power of the new computers increases all the time, the strength of the authentication and encryption algorithms is weakening. To protect against the known attack types, the used algorithms must be tested and evaluated regularly and new more effective encryption methods researched and if necessary, take in use.

7.2.5 Denial of Service Attacks

A Denial of Service (DoS) attack prevents or inhibits the normal use or management of the communications facilities [56]. The flooding is the simplest and most common way to carry out DoS attacks, but a cleverer attacker can also disable services, reroute them, or replace them with false ones [51].

The effect of the attacks can be made even more effective by using Distributed Denial of Service (DDoS) attacks where many nodes are harnessed to launch the attack concurrently.

In the network access systems a DoS attack usually means that a malicious node tries to

prevent the communication between the NAC and the NAS [57]. The attack can be targeted both to the authentication procedure and to the usage of the connection to the Internet. At the initial authentication the attacker can pretend to be the NAS and ask the NAC to authenticate itself. When the NAC sends the authentication messages, the attacker receives them but does not send any replies. The NAC still believes it is communicating with the real NAS and waits for the responses. The attack can be detected at the end, but even the mutual authentication can't prevent this kind of DoS attacks.

The attacker can also disturb the operation of the NAS by bombarding it with the authentication requests. This can lead to a DoS attack, if the resources needed for discarding the request are more than what is needed for authenticating the real NAC [57]. The NAS should not allocate resources to the NACs before the authentication is completed. If the NAS is too busy serving false authentication request, it may not have time for the real NACs, who will be left without service.

After the NAC has successfully authenticated and began to communicate to the Internet, the attacker can launch the ordinary DoS attacks. The attacks can be targeted to both the NAS and the NAC. The attacker can launch attacks against the NAC also from outside of the local network, because after a successful authentication the NAS forwards all the traffic to the NAC. Of course, the NAS's filtering rules can be implemented so that they make the attacks from the outside more difficult.

If the NAC and the NAS use encryption in the connection between them, either the per-packet authentication or the per-packet encryption, the cryptography provides security against many other kind of attacks, but is itself vulnerable to the DoS attacks. The calculation of the modular exponentiation or the product of two very large prime numbers, even the decrypting and the verifying the integrity of the incoming packets, takes both wall clock time and CPU time [58]. The attacker could send bogus packets that look like they were coming from the original communicating parties, but instead of calculating the integrity value or doing the encryption, the attacker would build up packets from junk. The attacker would have almost no work at all, but the receiver would have to a lot calculation decrypting or verifying the integrity of the packets. These kind of DoS attacks against the cryptographic systems are very difficult to prevent totally.

If the communication and the network access messages between the NAC and the NAS are sent without the per-packet authentication or stronger cryptography, the attacker can easily launch a DoS attack by sending false disconnect messages. If the NAS receives and approves a false disconnect message, it believes that the NAC is moving to some other NAS's network or shutting down. The NAS updates the packet filter and removes authorization of the NAC's traffic and the NAC's connections to the Internet get suspended. If the NAC wants to keep on using the Internet, it has to re-authenticate itself. Equally, the attacker can fool the NAC with false disconnect messages and block it from using the services it has authenticated to. Of course the NAC can still carry on communicating or try to re-authenticate itself, but it is also possible that the NAC comes to a conclusion that its access to the Internet is really blocked for some reason. Naturally the attack can be detected at the end, but the attacker may have already achieved his or her goals by preventing the NAC's access to the Internet for a period of time.

The protection against the DoS attacks is especially difficult in wireless environments. Anyone in the receiving area can monitor the traffic in the network and if he or she wants, send own messages. Even if the messages were just junk, they still consume the limited bandwidth and slow down the communication rate from the legitimate users. In fact, the attacker can shut down the whole network by flooding messages constantly. Of course, this kind of blocking attack is possible in any kind of shared links, but easy access to the media makes it easier in the wireless links.

Many of these Denial of Service attacks are not only network access specific, but equally noticeable risk in all communication. The network access protocol must still do its own part in trying to prevent DoS attacks. In practice this means, in addition to requirements stated by other threats, concentration on how the protocol's resource delegation and cryptographic calculation is implemented.

7.3 Passive Attacks

The passive attacks are in the nature of eavesdropping on or monitoring of the communication. The goal of the attacker is to obtain information that is being transmitted [56]. In the network access systems there are three kind of passive attacks that should be concerned:

the reveal of the message contents, the traffic analysis and the collection and tracing of the NAC's identity.

7.3.1 Eavesdropping

If the contents of the messages between the NAC and the NAS are sent without any kind of encryption, they are easily readable to anyone who is able to access them. This is especially easy in the wireless links, where all packets are accessible to anyone in the coverage area.

The eavesdropping can be prevented or at least made very difficult by using encryption to create confidentiality. When the payload of the message is encrypted with a properly used efficient security protocol, the attacker's chances in finding out the content are very low. This can be done for example by using the IPsec [3] Encapsulated Security Payload (ESP) [31] in the transport mode.

7.3.2 Traffic Analysis

In the traffic analysis attacks the attacker listens to the communication and collects statistical data of it. The attacker may be interested in who is communicating with whom, what upper-layer protocols they use or how big their traffic flows are to specific destinations. This way the attacker can get personal or even private information about the users of the network.

The encryption of the packet payloads in the IP layer is not enough to prevent some traffic analysis attacks. The IP header of the packet still reveals the sender's and receiver's IP addresses and thereby it is possible to monitor to where and how frequently each client is communicating. In practice, this means that the traffic between the NAC and the NAS must be protected with a tunnel, which encapsulates the whole IP packet so that also the original IP header is encrypted. This can be done e.g. by using IPsec [3] (ESP) [31] in the tunnel mode. Now the attacker can only see the NAC's and the NAS's IP addresses as the sender and the receiver, regardless of with whom the NAC is communicating. The attacker can still calculate the amount and the size of the packets the NAC sends and receives, but a paranoid client can confuse such calculations by sending some false packets of different

sizes sporadically.

7.3.3 Identity Collection and Tracing

At the beginning of the authentication the NAC must identify itself to the AAA architecture by some kind of identifier, in order for the local AAA server to be able individualize the NAC and re-route the request to the its home AAA server when necessary. In the Internet services the identifier can be e.g. a Network Access Identifier (NAI) [10] or the mobile node's home IPv6 address in the Mobile IPv6 [5] and in the GSM [61] and UMTS [28] networks it can be an International Mobile Subscriber Identity (IMSI) [61] or a Temporary Mobile Subscriber Identity (TMSI) [28].

At the initial authentication the NAC and the NAS have not been in contact with each other earlier and thereby they are not able to create any security relationships prior to the authentication. So the NAC has to send its identity to the NAS in a clear-text without encryption [28]. If an attacker is able to listen to the traffic in the network, he or she can collect the information who is trying to get the access to the network [57]. If the NAC is a mobile client and roams from a network to another, the attacker with a capability to listen to all the networks can trace the path the NAC is using. In practice this means, that a skillful attacker can precisely point where and when a certain person have used his or her computer or mobile phone.

The identity collection and tracing can be prevented by using either the temporary identities [27] or by encrypting the identities. Naturally these both methods are available only after the initial authentication in the re-authentications. Therefore they don't guarantee 100 % protection but it offers a relatively good protection level [28]. When the NAC and the NAS have authenticated each other and have set up a security association, they can agree a new temporary identity for the NAC which is used in the future authentication procedure. Since the negotiation of the new identity is encrypted, the attacker cannot link the temporary identity with the original at the next authentication. The encryption of the identity can be used in the re-authentication, if the NAC and the NAS use the existing security association.

If the NAC is a mobile node and roams to another AAA server's domain, it has to initiate the authentication with the real identity. This gives a possibility to trace the user's movement

in a larger scale, but it may be difficult to carry out, since the attacker should be able to monitor a large number of networks in different domains. In the real life there are a lot of easier ways to track someone's location.

8 Secure Network Access Operation

This chapter introduces a secure network access system, which qualifies the issued operational and security requirements. The operation can be seen happening in three separate phases: first the mutual authentication, secondly the creation of the IPsec Security Associations and thirdly the actual secure accessing to the network.

8.1 Mutual Authentication

The secure network access process begins with the mutual authentication of the NAC and the network the NAC is accessing. This is done with the UMTS Authentication and Key Agreement protocol carried inside the Extensible Authentication Protocol messages.

8.1.1 Initiation of Authentication

When the NAC arrives to a new network link or is switched on, it has to first configure a new working IP address to be able to communicate with other IP hosts. In IPv4 this would usually mean using the Dynamic Host Configuration Protocol (DHCP) [47], especially in roaming environments, where the delivery and the configuration of the static IP addresses would be cumbersome. If the NAC employs IPv6, it can derive an IP address by the stateless [49] or the stateful autoconfiguration (DHCPv6) [50] depending on the network's configuration. After the NAC has successfully configured a valid IP address to itself,

it can begin to communicate with other hosts.

The NAS can detect the presence of a new NAC by two methods: either relaying on its Access Control List (ACL) or acting actively. As the NAS is located in the access router to the Internet, it can compare all packets, tried to send through it, to its rules in the ACL. If there are some freely available networks or servers provided, the NAC may use them without authentication and doesn't even notice the existence of the NAS. For example the NAS may allow connections to a local web server by using HTTP [52]. But when the NAC tries to send an IP packet to the restricted areas of the Internet through the NAS, the ACL notices it, drops the packet and stores the NAC's IP address.

If the NAS acts actively, it listens to the network and tries to perceive the NACs before they even begin to try to access the Internet. When the NAC performs its address configuration, it has to communicate with a DHCP server or inform its presence like in stateless autoconfiguration in IPv6. Especially in a shared media, the NAS can capture these packets and conclude the NAC's new IP address. Even if the NAS acts actively, it still has to implement the ACL functionality.

Sometimes, e.g. when NAC enters to a foreign wireless network and is intending to use some security critical services like Internet banking, it may not want to use the network services at all, if it can't get the network to authenticate itself properly to the NAC. If the NAS doesn't initiate the authentication on behalf of the back-end network, the NAC can try to do it by sending some IP packets to the NAS to inform about its presence. If the NAC and the NAS are located on the same link, this could be done by multicasting or broadcasting to a specific address, but the case where they are in different links is more problematic. In IPv6 network access servers could have their own site-local anycast address, but it would complicate the system and make it more difficult to implement. After all, if the NAS is present and working properly, it should detect new clients and initiate the authentication.

If the NAC can't find the NAS, it can either begin to use the network connection and try to achieve the needed level of security by some higher layer protocols or simply try to use another network.

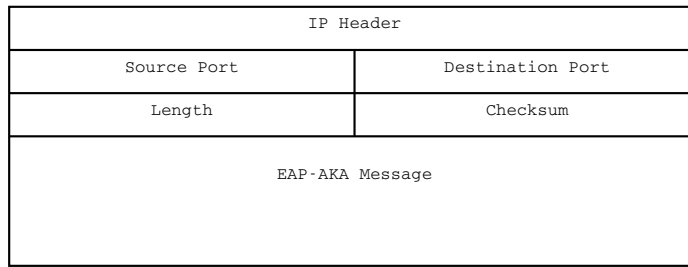


Figure 8.1: An EAP message encapsulated in an UDP over IP packet.

8.1.2 EAP-AKA over Internet Protocol

To transport the EAP messages over the Internet Protocol, a lightweight solution is needed. In the IETF PANA Working Group, two possible transport protocols have been presented: the User Datagram Protocol (UDP) [23] and the Internet Control Message Protocol (ICMP) [22] [62]. Both protocols provide a connectionless carrier to transfer the EAP messages over the IP, but the UDP is a better choice since it provides more scalability and versatility and is not as connected to the IP layer as the ICMP. The ICMP messages are identified by the 8-bit Type field, and thus the number of different ICMP messages is rather limited.

After the NAS has noticed that there is a new NAC active in its network, it initiates the authentication by sending to the NAC a normal EAP-Request/Identity, which advises to perform authentication to get access to wanted services. The EAP-AKA is carried over the Internet Protocol encapsulated in the UDP messages. The format of such a packet is presented in Figure 8.1. The UDP header is placed between the IP header and EAP-AKA message. It consists of four 16-bit fields: the source and the destination port, the length of the UDP header and its payload and the checksum of the whole IP packet.

The EAP-AKA conversation over the UDP/IP continues similarly to the normal EAP-AKA described in Section 4.4. The result is either a successful mutual authentication between the NAC and the serving access network, or the authentication fails. In the case of the failure, the access to the network is denied and the NAC has to try again, try to access to a different network or contact the system administrator to find out what is wrong. The AAA server may also inform the NAC about the reasons of the authentication failure with either an EAP-Request/Notifications [11] or an EAP-Request/AKA-Notification [27]. The EAP-Request/AKA-Notifications are specially defined for the purposes of the EAP-

AKA, but they can be only used after the AAAH has recognized the NAC as one of its EAP-AKA clients and generated the authentication vectors and the necessary keying material. If the AAAH cannot identify the NAC's identity, it can only use the regular EAP-Request/Notification to deliver additional information to the NAC.

If the EAP-AKA succeeds, the both parties, the NAC and the serving network can be sure that each other really is who they claim to be and they can rely on that they can continue communicating with the opposite party. In the EAP-AKA the NAC generates the encryption and the integrity key from the shared secret and the random number received from the AAAH. The AAAH has distributed the same pair of keys to the AAAL which delivers them to the NAS after the successful authentication. The EAP-AKA is concluded resulting the secure relationship and the shared secret between the NAC and the NAS.

The re-authentication with the EAP-AKA operates similarly to the initial authentication with a couple of exceptions. If the NAC is roaming outside its AAAH's domain and the AAAH has delivered more than one authentication vector to the AAAL at the initial authentication, the re-authentication procedure does not have to involve the AAAH and the authentication can be performed between the NAC and the AAAL. Of course, this is possible only if the NAC is re-authenticating inside the same domain where there initial authentication was performed.

When the network access system employs IPSec tunnels in the accessing to the network as will be defined in Section 8.3, all the traffic between the NAC and the NAS is encrypted. If the NAC does not roam and locates still in the same access network, the re-authentication is initiated before the existing security relations expire. This way the re-authentication procedure is carried inside the existing IPSec tunnel and the contents of all the EAP messages are confidentiality protected. As the identity of the NAC is sent encrypted in the EAP-Identity message, the identity protection with temporary identities is not necessary and the implementation can be simplified.

The EAP-AKA fulfills the functional and security requirements issued for the authentication in Sections 6 and 7. It does not use unnecessary messages to consume the limited bandwidth or increase delay by multiple round-trips to the home AAA server and it is scalable to be used in various environments and with many different access technologies.

The EAP-AKA also provides mutual authentication of the NAC and the serving network, key delivery for the IPSec tunnels, identity protection for the NAC, integrity protection for the EAP messages and strong cryptographic algorithms to secure from the brute-force attacks [27] [28].

8.2 Creation of IPSec Tunnels

After the NAC and the network have authenticated themselves to each other successfully and the NAC and the NAS have derived the keying material, it is time to create the IPSec tunnels to protect the traffic. The functionality of a one-way IPSec tunnel is defined by an IPSec Security Association, so in order to enable security to both directions, two different SAs are needed.

There are at least two different methods to create the required SAs between the NAC and the NAS. First, a simple method, where the client and the ISP have pre-negotiated parameters and protocols to be used like in the cellular phones. Secondly the NAC and the NAS may use the Internet Key Exchange (IKE) [32] based on the shared secret they know to negotiate and build the necessary SAs.

In addition to the Security Associations, the new IPSec tunnels requires new IPSec Policies to the Security Policy Database (SPD). Before the creation of the IPSec SAs the NAC has two possible sets of policies in the SPD: it can either allow all the inbound and outbound traffic continue without IPSec processing or to limit the incoming traffic to the necessary address configuration information, like the DHCP [47] or IPv6 Neighbor Discovery [60] messages, and to the network access EAP messages. The first choice is suitable in the situations where the authentication is not completely necessary, for example when the NAC can use free networks or services for free. On the other hand the second choice is more secure since it takes the EAP-AKA as a default function in a new network and requires the mutual authentication and the secure connection before accepting any regular IP traffic from the Internet.

After the creation of the SAs the IPSec tunnel is set up and the NAC has to automatically update its Security Policies. The new set of policies must control that all inbound and

outbound IP traffic must be protected with an ESP tunnel defined by the new SAs. This way the NAC accepts only tunneled encrypted integrity protected packets forwarded from the NAS. Only the address configuration and neighbor discovery packets from the same access network are exceptions. When either the NAC or the AAAH initiates a re-authentication procedure, also the new EAP messages will be transported inside the tunnel and thus be secure the identity of the NAC.

The NAS has little bit different sets of Security Policies. If the Internet service provider offers some parts of the network, some services or protocols for free, the NAS has to be configured to allow this traffic bypass without IPSec processing. Also it has to allow the EAP, the address configuration and the neighbor discovery messages from the access network and the AAA protocol messages from the operator's network to be received and transmitted without the IPSec. From the access network the NAS denies all other traffic, excluding traffic from the successfully authenticated NACs. The NAS has an entry for each of them in the SPD. The entries define usage of the same IPSec tunnel as ones at the NAC's end. They are added when the authentication succeeds and are removed when the authentication expires and no re-authentication has been performed.

8.2.1 Pre-negotiated Parameters

A simple, fast and straightforward method to create the necessary Security Associations to build the IPSec tunnels is to use existing pre-negotiated parameters. At the same time the Internet Service Provider and a client make an agreement of using the network services and create the needed identity and the shared secret for the client, they can also agree on the necessary parameters and protocols needed for setting up the IPSec Security Associations. This kind of practice is already commonly in use in cellular networks.

To set up the required two Security Associations the NAC and the NAS need to have two shared secrets, one key for encryption and another for integrity protection, knowledge on which IPSec protocol and algorithms to use, one Security Parameter Index for both SAs and the IP addresses of the opposite party. The Authentication and Key Agreement (AKA) procedure has already delivered keys for encryption and integrity protection, the security requirements specified the usage of IPSec ESP in tunnel mode essential and both the NAC

and the NAS have found out the each other's IP address right at the beginning of the authentication process. Therefore the pre-negotiated parameters are the used authentication and encryption algorithms and the two SPIs.

The updated version of the IPsec ESP is defined in the IETF Internet Draft IP Encapsulating Security Payload (ESP) [43]. According to it the default encryption algorithm for the IPsec ESP is the Advanced Encryption Standard (AES) [33] and the default message authentication algorithms are the Message Digest 5 (MD5) [63] and the Secure Hash Algorithm 1 (SHA-1) [64]. So the negotiation of the used algorithms is rather simple, the encryption algorithm is the AES and the authentication algorithm can be either MD5 or the SHA-1.

The agreement on the proper Security Parameter Indexes is slightly more complicated, since there exists no solution or recommendation. But since the SPI is an arbitrary number which only links the IP packet to a proper Security Association, many different methods can be implemented. The SA can have the same value in both SAs between the NAC and the NAS, so one possible solution is to derive the common SPI from the NAC's IP address. This way the NAS would have a different SPI linked with each NAC. Since the SPI is a 32-bit number, in the IPv4 it would be the whole IP address of the NAC and in the IPv6, the last 32 bits of the IP address, which are very likely to be different in every address.

8.2.2 Security Association Creation with IKE

The Internet Key Exchange (IKE) or its replacing versions can be used to negotiate the required parameters and to create the Security Associations for the IPsec tunnels. The IKE can operate with shared secrets and so it is suitable to be used with this kind of network access system.

The mutual authentication with the AKA delivers two 128-bit keys to the NAC and the NAS, and thereby creates a shared secret between them. This secret can be used as a keying material for the IKE. When the AKA is finished, the NAC and the NAS can either use the default Security Associations created by the pre-negotiated parameters, or initiate the IKE, if another one of them is dissatisfied with the default SAs. The IKE offers a wide set of selectable options and with IKE the parties can negotiate the desired parameters to their new SAs.

Both methods have advantages of their own. The pre-negotiated parameters is a simple solution and faster in action, but it also have disadvantages. The pre-negotiated parameters method may be useful in strictly controlled environment, where all networks elements are aware of the parameter agreements and how to use them. The usage of the IKE is more generic solution and allows the NAC and the NAS to negotiate individualized parameters for their SAs. It scales better in the changing environments with different kind of requirements with different NACs. A drawback of the IKE is that it is complicated and difficult to implement. It also increases the delay in the network access and adds extra traffic to the access network.

8.3 Secure Accessing to the Network

After the creation of the IPSec tunnels, the NAC can begin to communicate to the Internet through the NAS. The first and in many environments the most insecure hop from the NAC to the NAS is now secured.

8.3.1 Structure of the Network Elements

The protocol layer structure of the Network Access Client (NAC) is presented in Figure 8.2. The Internet Protocol (IP) layer with the Internet Protocol Security (IPSec) is on top of the link layer. Since all the control information is carried over the IP layer, the implementation of the link layer can vary in the different environments without a need to change the upper layer protocols. The most important components of the IPSec implemented in the IP layer are the Security Policy Database (SPD), the Security Association Database (SADB) and the Internet Key Exchange (IKE), whose interrelations are marked out in Figure 8.2. On top of the IP layer, the network access system employs the User Datagram Protocol (UDP) in the transport layer, which transports the Extensible Authentication Protocol (EAP) messages. The EAP implementation offers the basic functionality to handle the authentication requests and responses, but the actual authentication protocol is implemented on top of the EAP in the EAP methods. This network access system employs UMTS Authentication and Key Agreement (AKA) as the EAP method to perform the mutual authentication.

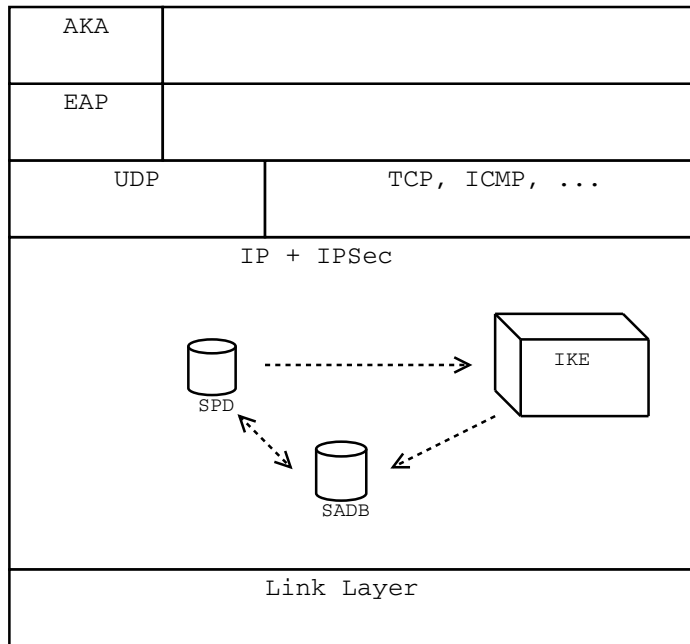


Figure 8.2: The Network Access Client (NAC) protocol stack.

The protocol layer structure and the necessary components of the Network Access Server (NAS) are presented in Figure 8.3. Unlike the NAC, the NAS has at least two network interfaces: one to the access network and one up to the operator's network, via which the NACs can access the Internet and the NAS the back-end AAA infrastructure. The IPSec is implemented in the IP layer and contains the same elements as in the NAC: the SPD, the SADB and the IKE. In addition to these in the IP layer of the NAS the forwarding of the incoming IP packets is controlled by the Access Control List (ACL), which essentially is a dynamically configurable firewall. The ACL controls that only legitimate packets are forwarded and the rest are dropped. On top of the IP layer the NAS has the EAP layer. The EAP messages are carried in the UDP messages between the NAS and the NAC and in the AAA protocol messages between the NAS and the local AAA server (AAAL). Therefore between the IP layer and the EAP layer the NAS has both the UDP and the AAA protocol. The AAA protocol messages are carried in either the UDP, the TCP [65] or the SCTP [66] over the IP.

The network access system can also be implemented without the AAA infrastructure. In such case the NAS is the other endpoint of the EAP conversation and acts as the home AAA server (AAAH). The NAS needs to implement the EAP authentication methods instead of only forwarding the messages. In practice this means that the NAS also has a local user

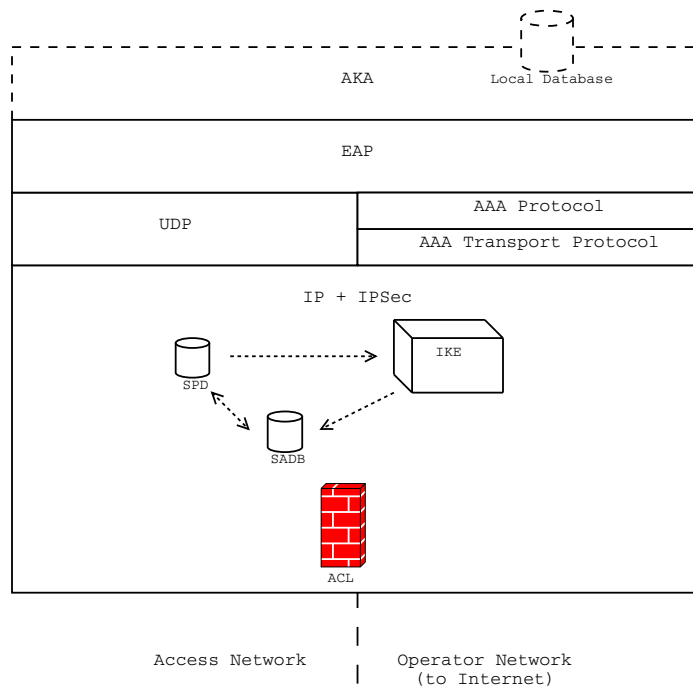


Figure 8.3: The Network Access Server (NAS) protocol stack.

database, where the information of the clients is stored.

8.3.2 Packet Processing in the Network Access Server

When an IP packet arrives to the Network Access Server (NAS), the NAS has to decide how to handle it. The different situations can be divided into two categories: the IP packets that are destined to the NAS itself and the IP packets that are intended to be forwarded by the NAS to somewhere else. If the arriving IP packet is destined to the NAS itself, it is either an IPSec tunneled packet from the NAC or an EAP message encapsulated in the UDP message or in the AAA protocol message. If the arriving IP packet is not destined to the NAS, it is either an IP packet from or to the free networks or a new NAC trying to access the network without a proper authentication.

Sometimes an Internet Service Provider (ISP) admits all clients to use some networks and services for free without authentication. Figure 8.4 shows the processing of such IP traffic inside the NAS. At the beginning, an IP packet destined to a free network arrives to the NAS from a host in the access network. Before the NAS forwards it, at stage 1 it consults the SPD to find out what kind of IPSec processing is needed for the IP packet. The policies

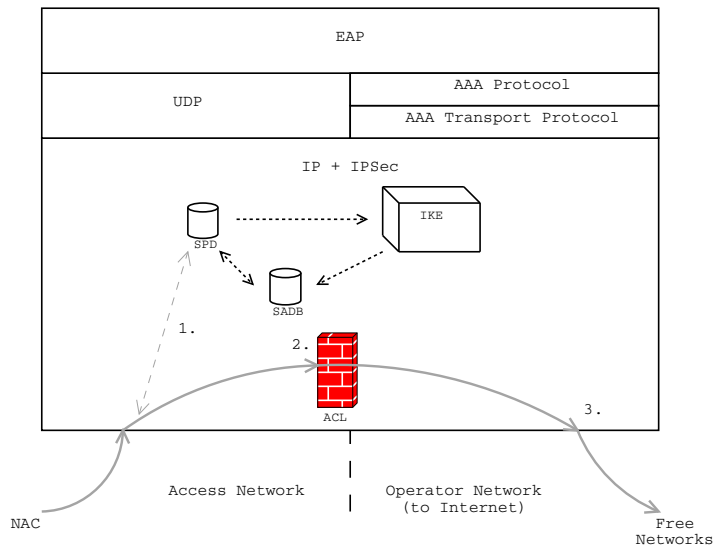


Figure 8.4: The NAC communicates through the NAS to the free networks.

in the SPD direct that the packet can continue without any IPsec processing. At the stage 2 the ACL accepts the packet to pass through the packet filter, since it is also configured to allow traffic from and to the free networks. At the stage 3 the IP packet is forwarded to the operator's network for further processing. The processing of the IP packet to the opposite direction from the free networks to the hosts in the access network operates equally.

The actual operation of the network access system initiates when a NAC in the access network tries to send traffic to the restricted parts of the Internet through the NAS. The processing of such an event is shown in Figure 8.5. At Stage 1 an IP packet destined to some non-free IP address arrives from the NAC to the NAS. Again, before forwarding it any further, the SPD is consulted what to do with such an IP packet at Stage 2. The policies in the SPD define not to allow the packet to be forwarded since the NAC has not yet authenticated itself. The packet is discarded, but the IP address of the NAC is handed to the EAP layer at Stage 3 to trigger the authentication process of the new NAC. The NAS initiates the authentication by sending an EAP-Identity/Request to the NAC at Stage 4.

The processing of the EAP messages inside the NAS is shown in Figure 8.6. When an IP packet containing an EAP message arrives to the NAS, it is first compared to the policies in the SPD at Stage 1. The policies allow it to continue without any IPsec processing and the EAP message part of the packet is handed to the EAP layer. The EAP forwards the EAP message to the AAA protocol implementation and updates its own EAP state machine [67]

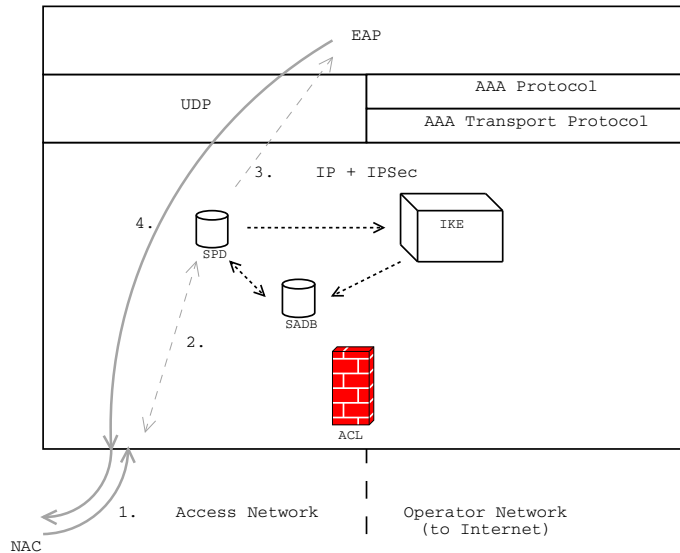


Figure 8.5: The NAS initiates the authentication when a new NAC begins to communicate.

at Stage 2. At the AAA protocol layer the EAP-message is encapsulated into an AAA protocol message which is forwarded to the AAAL at Stage 3.

After the mutual authentication of the NAC and the serving network is successfully performed and the required Security Associations have been created between the NAC and the NAS, the NAC can begin to communicate to the Internet through the NAS with the IPsec tunnels. The processing of the IP packets tunneled from the NAC to the NAS is shown in Figure 8.7. An IP packet arrives from the NAC to the NAS in an IPsec ESP tunnel at Stage

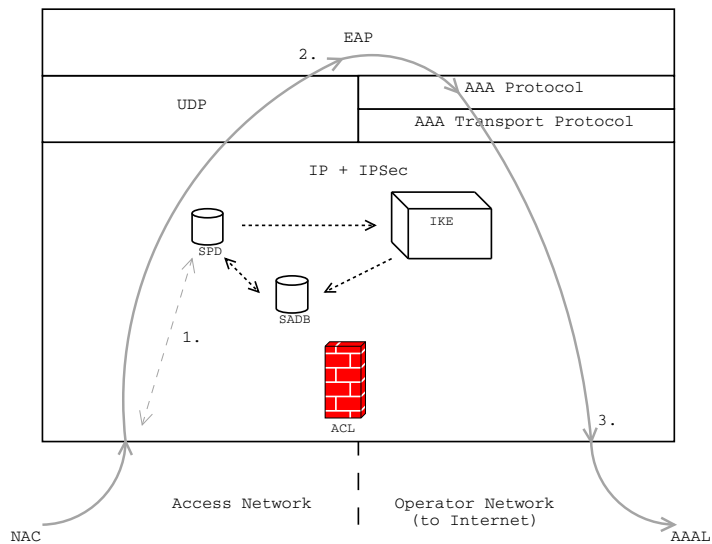


Figure 8.6: The EAP messages in the NAS.

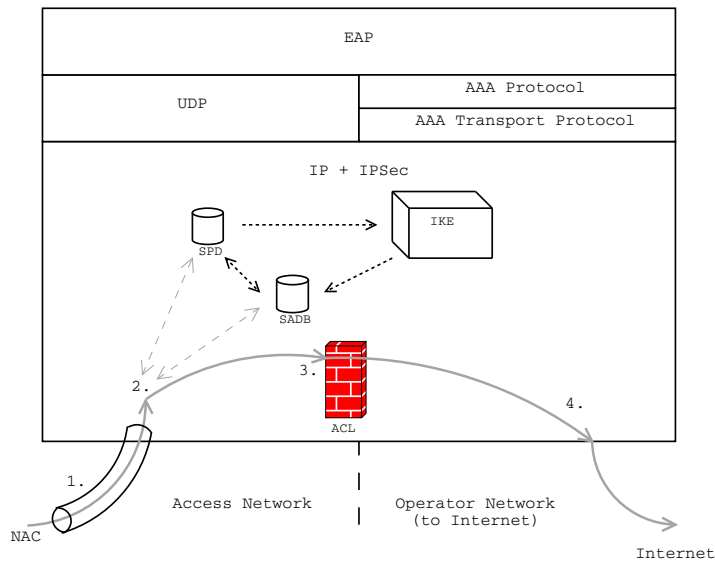


Figure 8.7: The NAC communicates to the Internet through the NAS with IPsec tunnel.

1. At Stage 2 the IPsec implementation picks out the right SA from the SADB based on the Security Parameter Index (SPI), the IPsec protocol and the destination IP address of the packet. With the parameters of the SA the IPsec implementation decrypts the tunneled packet and compares the resulting IP packet to the policies in the SPD. If the SA found based on the packet's selectors matches the kind and order of the SAs required by the policy, the packet is passed to be forwarded. At the Stage 3 the ACL allows the resulting IP packet to go through the firewall, since it is configured to pass the traffic from and to the properly authenticated NACs. At Stage 4 the IP packet is forwarded normally towards its destination.

8.3.3 Re-authentication

The results of an authentication process cannot be everlasting. The security of the cryptographic algorithms declines all the time when the same keys are used. In the network access systems this means that the IPsec SAs used between the NAC and the NAS must be replaced regularly. If the SAs are created with the Internet Key Exchange (IKE), it can be used again to negotiate a new set of SAs. But if the SAs are created based on some pre-negotiated parameters, the regeneration of them requires new fresh keying material which is attained by the re-authentication procedure.

Also the trusting relationship between the NAC and the serving network requires refreshing at regular intervals. It is important not only for the access security, but also for the accounting and auditing information. Every security relation between the serving network and the NACs accessing to the Internet through it have a lifetime, which tells when the authentication expires. If the relation is not refreshed the NAS removes that particular NAC from its client databases, shuts down the IPSec tunnels and updates the packet filters to deny the forwarding of the NAC's traffic. To keep the connection alive, the NAC or the AAA server has to initiate a re-authentication before the lifetime expires. This way the re-authentication process can be performed within the current security relations and the lifetime updated without breaks in the service.

The basic operation of the re-authentication with the EAP-AKA carried over the IP is quite similar to the normal authentication process, apart from few differences. First of all, when the re-authentication is initiated while the existing authentication is still valid, all traffic between the NAC and the NAS is sent encrypted in an IPSec tunnel. When all the EAP-messages of the re-authentication are tunneled, the total security of the system increases. The identity collection and tracing becomes even more difficult for the attackers, since all identities are transported encrypted. In fact, an eavesdropper can not even detect when a new re-authentication is processed.

If the NAC is accessing the network outside its home domain, the re-authentication can be performed without contacting the NAC's home AAA server (AAAH). At the initial authentication, the AAAH delivers a set of authentication vectors to the local AAA server (AAAL) which continues and finalizes the authentication process. The rest of the authentication vectors are stored in the AAAL and can be used in the re-authentication like they were just delivered from the AAAH.

The re-authentication can be initiated by either the NAS or the NAC. The NAS can initiate it by sending an EAP-Request/Identity message, to which the NAC replies with an EAP-Response/Identity. If the NAC wants to begin the re-authentication, it can do it simply by sending the response to the NAS. Both ways, the NAS sends the response to the AAAL, but unlike at the initial authentication, the AAAL acts as the AAAH with the authentication vectors it has for that particular NAC. The AAAL challenges the NAC with an EAP-Request/AKA-Challenge message and the re-authentication continues similarly to

the initial authentication. When the re-authentication is successfully finished, the lifetime of the security relationship between the NAC and the serving network is refreshed and the NAC and the NAS replaces the SAs between them with the new ones.

8.3.4 Termination of Connection

The network access connection terminates when its lifetime expires and neither one of the parties has initiated a re-authentication. If either the NAC or the AAA server wants to close the connection earlier, it can be done by an EAP-Failure message [27]. The EAP-Failure message itself has no integrity protection, but as it is sent through the IPsec tunnel, the Denial of Service attacks with false EAP-Failure messages are impossible to launch. When the connection is closed, the NAS removes the NAC's IP address from the ACL and shuts down the IPsec tunnels. If the NAC wishes to continue accessing the network, it has to initiate the authentication procedure from the beginning.

8.3.5 Co-operation with Cellular Networks

In the near future, some mobile phone or multimedia terminals can access both the cellular mobile networks and the wireless Internet networks like the Wireless Local Area Networks (WLAN). If the NAC can use the same authentication protocols, algorithms and service agreements in both network environments, it simplifies the implementation and saves the scarce resources. Likewise, if an operator provides both mobile phone and Internet services, it could use the same authentication mechanisms and algorithms with all the clients. It simplifies the operator's network since it can manage its all clients with a single user database and authentication service centre in stead of providing separated databases and services for different kind of clients.

The EAP-AKA is applied from the cellular networks to the Internet networks. The AKA is already in use in the GSM networks [61] and will be the authentication protocol in the future UMTS networks [26]. The usage of the EAP-AKA in the IP networks enables the defined co-operation of the IP and cellular networks. The architecture of such solution is presented in Figure 8.8 which shows the similarities of the different networks. The NAC can access the GSM networks via the Base Transceiver Station (BTS), to UMTS networks

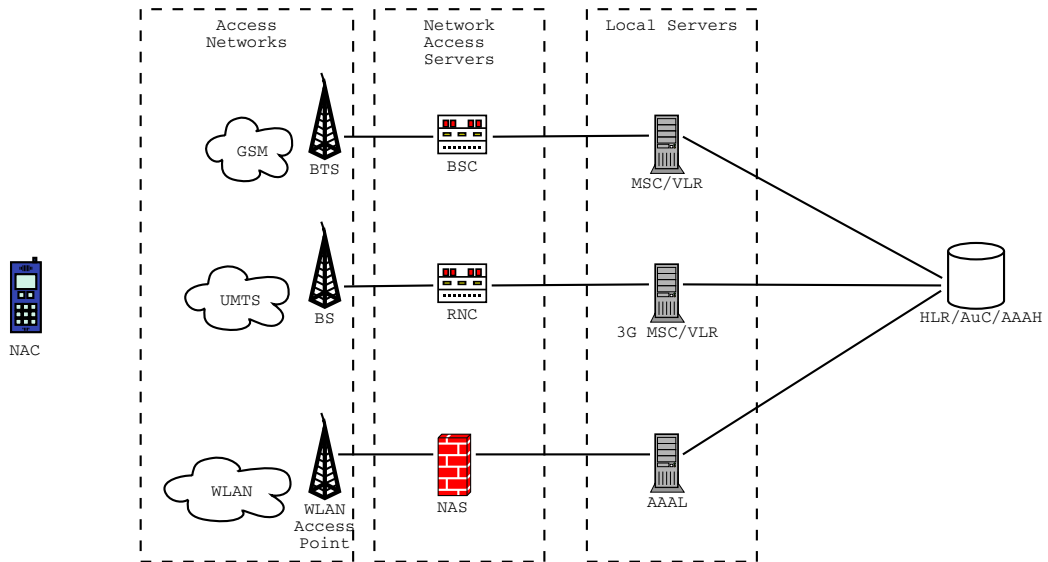


Figure 8.8:

via the Base Station (BS) and the IP networks via the WLAN Access Point. In all different networks there are network access servers to control the access of the NACs. In the GSM it is the Base Station Controller (BSC), in the UMTS the Radio Network Controller (RNC) and in the IP network the NAS.

The authentication architecture is similar in both the cellular and the IP networks with Mobile IP functionality. A local server controls the authentication in its own domain and acts as an intermediary to the NACs' home servers. The same operations as the AAAL does in the IP networks, the Mobile Subscriber Controller does with Visitor Location Register (MSC/VLR) in the GSM and UMTS networks. If the operator wants use the benefits of the one common client database, it can combine the AAAH from the IP networks with the Home Location Register (HLR) and the Authentication Centre (AuC) of the cellular network. This one authentication server could then authenticate and control the operator's all clients heedless of which access technology they are currently using.

9 Conclusions

This thesis examined the usage possibilities of the authentication and the network access on the Internet Protocol and derived their functional and security requirements. The goal of the thesis was to develop a network access system that fulfills the derived requirements and is suitable to the specified usage scenarios. A particular emphasis was put on the security aspects. An implementation approach was to employ existing, widely used and proof-to-work protocols, algorithms and network elements.

The authentication in the network access is traditionally implemented in the link layer, therefore the most relevant question was, why to use the IP layer instead. The thesis deals with the advantages and the disadvantages of the different implementation layers. The Internet Protocol is widely used and offers many benefits to the network access systems. One of them is the natural co-operation with the IPSec, which provides powerful tools to implemented strong security. On the other hand, the authentication and network access on the link layer are already implemented and widely in use. This naturally makes the introduction of a new different solution more difficult.

The biggest problems during the evaluation of different implementation possibilities were caused by the oversupply of the various authentication and network access systems. The network security in the Internet and the network access are highly topical issues and many research groups around the world develop different methods. In this thesis the core of the authentication procedure was built on the basis of the UMTS Authentication and Key Agreement encapsulated inside the EAP messages carried over the IP layer. It provides a

secure and scalable mechanisms, that is already in use and supported in the mobile phone networks.

A rather generic network access system like this can be used in many different scenarios. Perhaps the most demanding are the mobile clients, such as the laptops and the multimedia terminals, in the wireless environments. Thus the functional requirements of the network access derived in this thesis paid special attention on the requirements of the wireless links, like the limited bandwidth and the scarce calculation resources.

The security of the network access is especially important in the wireless environments and in the mobile use of the Internet. Therefore this thesis aimed at identifying the possible security threats and deriving the corresponding security requirements to protect against them. Based on the requirements it was obvious that the connection between the network access client and the access point must use an encrypted tunnel. Such a functionality can be easily achieved by employing the IPSec ESP in the tunnel mode.

The developed network access system fulfills the derived functional and security requirements and thus is suitable to the specified usage scenarios. Some problems may still arise at the implementation phase, especially in the creation of the IPSec Security Associations. The usage of pre-negotiated parameters is not a very scalable solution and the co-operation of the existing IKE implementations is rather poor. On the other hand, the Diameter AAA protocol which is quite essential in the larger scale AAA infrastructures is not yet functional either. So the obstacles before the wider use of any network access system are still bigger than just minor details in the client-side implementation.

References

- [1] IEEE 802.1 Working Group. *Port-Based Network Access Control*, IEEE Std 802.1X-2001 June 2001.
- [2] *The IETF's Protocol for carrying Authentication for Network Access (PANA) Working Group Charter*, <http://www.ietf.org/html.charters/pana-charter.html>, March 2003.
- [3] RFC 2401; S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*, November 1998.
- [4] RFC 3344; C. Perkins. *IP Mobility Support for IPv4*, August 2002.
- [5] D. B. Johnson, C. E. Perkins and J. Arkko. *Mobility Support in IPv6*, draft-ietf-mobileip-ipv6-19.txt, October 2002.
- [6] *The Internet Engineering Task Force*, <http://www.ietf.org>, December 2002.
- [7] *The IETF's Authentication, Authorization and Accounting (AAA) Working Group Charter*, <http://www.ietf.org/html.charters/aaa-charter.html>, February 2003.
- [8] RFC 2903; C. de Laat, G. Gross, L. Gommans, J. Vollbrecht and D. Spence. *Generic AAA Architecture*, August 2000.
- [9] RFC 2989; B. Aboba, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, P. Walsh, G. Zorn, G. Dommety, C. Perkins, B. Patil, D. Mitton, S. Manning, M. Beadles, X. Chen, S. Sivalingham, A. Hameed, M. Munson, S. Jacobs, B. Lim, B. Hirschman, R. Hsu, H. Koo, M. Lipford, E. Campbell, Y. Xu, S. Baba and E. Jaques. *Criteria for Evaluating AAA Protocols for Network Access*, November 2000.
- [10] RFC 2486; B. Aboba and M. Beadles. *The Network Access Identifier*, January 1999.
- [11] RFC 2284; L. Blunk and J. Vollbrecht. *PPP Extensible Authentication Protocol (EAP)*, March 1998.
- [12] RFC 2865; C. Rigney, S. Willens, A. Rubens and W. Simpson. *Remote Authentication Dial In User Service (RADIUS)*, June 2000.
- [13] RFC 2869; C. Rigney, W. Willats and P. Calhoun. *RADIUS Extensions*, June 2000.
- [14] RFC 3162; B. Aboba, G. Zorn and D. Mitton. *RADIUS and IPv6*, August 2001.

- [15] P. R. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko. *Diameter Base Protocol*, draft-ietf-aaa-diameter-14.txt, October 2002.
- [16] P. R. Calhoun, T. Johansson and C. E. Perkins. *Diameter Mobile IPv4 Application*, draft-ietf-aaa-diameter-mobileip-13.txt, October 2002.
- [17] P. R. Calhoun, G. Zorn, D. Spence and D. Mitton. *Diameter NASREQ Application*, draft-ietf-aaa-diameter-nasreq-10.txt, November 2002.
- [18] T. Hiller and G. Zorn. *Diameter Extensible Authentication Protocol (EAP) Application*, draft-ietf-aaa-eap-00.txt, June 2002.
- [19] RFC 1661; W. Simpson. *The Point-to-Point Protocol (PPP)*, July 1994.
- [20] L. Blunk, J. Vollbrecht and B. Aboba. *Extensible Authentication Protocol (EAP)*, draft-ietf-pppext-rfc2284bis-06.txt, September 2002.
- [21] RFC 2516; L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone and R. Wheeler. *A Method for Transmitting PPP Over Ethernet (PPPoE)*, February 1999.
- [22] STD 5, RFC 792; J. Postel. *Internet Control Message Protocol*, September 1981.
- [23] STD 6, RFC 768; J. Postel. *User Datagram Protocol*, August 1980.
- [24] RFC 1994; W. Simpson. *PPP Challenge Handshake Authentication Protocol (CHAP)*, August 1996.
- [25] H. Andersson, S. Josefsson, G. Zorn, D. Simon and A. Palekar. *Protected EAP Protocol (PEAP)*, draft-josefsson-pppext-tls-eap-02.txt, February 2002.
- [26] 3GPP Technical Specification 3GPP TS 33.102 V3.6.0: *Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)*, 3rd Generation Partnership Project, November 2000.
- [27] J. Arkko and H. Haverinen. *EAP AKA Authentication*, draft-arkko-pppext-eap-aka-09.txt, February 2003.
- [28] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian and V. Niemi. *UMTS Networks: Architecture, Mobility and Services*, John Wiley & Sons, Ltd, 2001.
- [29] *The IETF's IP Security Protocol (IPSec) Working Group Charter*, <http://www.ietf.org/html.charters/ipsec-charter.html>, December 2002.
- [30] S. Kent. *IP Authentication Header*, draft-ietf-ipsec-rfc2402bis-01.txt, July 2002.
- [31] RFC 2406; S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP)*, November 1998.

- [32] RFC 2409; D. Harkins and D. Carrel. *The Internet Key Exchange (IKE)*, November 1998.
- [33] NIST, FIBS PUB 197: *The Advanced Encryption Standard (AES)*, November 2001.
- [34] RFC 2403; C. Madson and R. Glenn. *The Use of HMAC-MD5-96 within ESP and AH*, November 1998.
- [35] RFC 2407; D. Piper. *The Internet IP Security Domain of Interpretation for ISAKMP*, November 1998.
- [36] RFC 2408; D. Maughan, M. Schertler, M. Schneider and J. Turner. *Internet Security Association and Key Management Protocol (ISAKMP)*, November 1998.
- [37] C. Kaufman, editor. *Internet Key Exchange (IKEv2) Protocol*, draft-ietf-ipsec-ikev2-04.txt, January 2003.
- [38] W. Aiello, S.M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A.D. Keromytis and O. Reingold. *Just Fast Keying (JFK)*, draft-ietf-ipsec-jfk-04.txt, March 2002.
- [39] RFC 2402; S. Kent and R. Atkinson. *IP Authentication Header*, November 1998.
- [40] RFC 2405; C. Madson and N. Doraswamy. *The ESP DES-CBC Cipher Algorithm With Explicit IV*, November 1998.
- [41] RFC 2410; R. Glenn and S. Kent. *The NULL Encryption Algorithm and Its Use With IPsec*, November 1998.
- [42] RFC 2404; C. Madson and R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*, November 1998.
- [43] S. Kent. *IP Encapsulating Security Payload (ESP)*, draft-ietf-ipsec-esp-v3-03.txt, July 2002.
- [44] S. Frankel, S. Kelly and R. Glenn. *The AES Cipher Algorithm and Its Use With IPsec*, draft-ietf-ipsec-ciph-aes-cbc-04.txt, June 2002.
- [45] *National Institute of Standards and Technology*, <http://www.nist.gov>, March 2003.
- [46] STD 5, RFC 791; J. Postel. *Internet Protocol*, September 1981.
- [47] RFC 2131; R. Droms. *Dynamic Host Configuration Protocol*, March 1997.
- [48] RFC 2460; S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*, December 1998.

- [49] RFC 2462; S. Thomson and T. Narten. *IPv6 Stateless Address Autoconfiguration*, December 1998.
- [50] R. Droms (ed.), Bernie Volz, Ted Lemon, C. Perkins and M. Carney. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, draft-ietf-dhc-dhcpv6-28.txt, November 2002.
- [51] E.D. Zwicky, S. Cooper and D.B. Chapman. *Building Internet Firewalls, Second Edition*, O'Reilly, June 2000.
- [52] RFC 2616; R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.1*, June 1999.
- [53] T. Ylönen, T. Kivinen, M. Saarinen, T. Rinne and S. Lehtinen. *SSH Transport Layer Protocol*, draft-ietf-secsh-transport-15.txt, September 2002.
- [54] RFC 959; J. Postel and J. Reynolds. *File Transfer Protocol (FTP)*, October 1985.
- [55] RFC 2660; E. Rescorla and A. Schiffman. *The Secure HyperText Transfer Protocol*, August 1999.
- [56] W. Stallings. *Data & Computer Communications, Sixth Edition*, Prentice Hall International, Inc., 2000.
- [57] M. Parthasarathy. *PANA Threat Analysis and Security Requirements*, draft-ietf-pana-threats-eval-00.txt, October 2002.
- [58] N. Doraswamy and D. Harkins. *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Prentice Hall PTR, 1999.
- [59] STD 37, RFC 826; D. Plummer. *An Ethernet Address Resolution Protocol*, November 1982.
- [60] RFC 2461; T. Narten, E. Nordmark and W. Simpson. *Neighbor Discovery for IP Version 6 (IPv6)*, December 1998.
- [61] GSM Technical Specification GSM 03.03 (ETS 300 523): *Digital cellular telecommunication system (Phase 2); Numbering, addressing and identification*, European Telecommunications Standards Institute, April 1997. .
- [62] RFC 2463; A. Conta and S. Deering. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, December 1998.
- [63] RFC 2403; C. Madson and R. Glenn. *The Use of HMAC-MD5-96 within ESP and AH*, November 1998.
- [64] RFC 2404; C. Madson and R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*, November 1998.

- [65] STD 7, RFC 793; J. Postel. *Transmission Control Protocol*, September 1981.
- [66] RFC 2960; R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. *Stream Control Transmission Protocol*, October 2000.
- [67] J. Vollbrecht and D. Spence. *State Machines for EAP Peer and Authenticators*, draft-vollbrecht-eap-state-00.txt, December 2002.