Integrating Mobile IPv4 and IPsec authentication

Lauri Helenius
Helsinki University of Technology
Laboratory of telecommunications software and multimedia
lheleniu@cc.hut.fi

Abstract

This paper deals with IPsec authentication on mobile IP. As a mobile IP I mean mobility that is defined in RFC3344 (mobility in IPv4, MIPv4)[1]. Authenticating requests sent by a mobile node that tries to access a corporate intranet have been causing difficulties in MIPv4 model. IETF have been dealing with this situation for couple of years and RFC for AAA (Authentication, Authorization, and Accounting) has been released to solve difficulties. AAA is a good standard but it presumes too much. Not every foreign network has a fully operating FA and AAAF server in their network systems. This paper first presents the basic technologies behind authentication and after that go through the AAA model and how it could be altered to be more compatible.

KEYWORDS: IPsec Authentication, Mobile IPv4, MIPv4 IKE, AAA, RADIUS, Diameter

1 Introduction

New trends in wireless network area show huge growth in the mobile net browsing sector. Use of PDAs (personal data assistant) and laptops combined to WLANs (Wireless Local Area Network) is becoming more and more common [17]. Mobility is not yet true mobility. Crossing the borders of two separate WLAN sectors will present true challenges to IP protocols.

What is the actual need for IPsec authentication in MIPv4? Perhaps corporate customers present the greatest need for authentication. Companies have been traditionally needed authentication devices for authenticating incoming connections. After the connection is authenticated it can be easily transferred into secure line [5].

IPv4 has an IPsec extension that has three main properties. It can be used in authorization clients, produce authorization headers AH and encrypting the message with encapsulating security payload ESP. These properties combined to each other offer a secure way to change information through untrusted network, which is exactly something that corporate users need and want. Unfortunately MIPv4 and IPsec are not very compatible.

To figure out the problems the existing protocols have to be studied. Mobility of IPv4 is defined in RFC3344 [1]. The IPsec in regular IP is defined quite well in RFCs 2402 and 2406 [11, 10]. Few solutions of solving the problems of mobile authentication have been made and perhaps AAA structure [9] is most interesting out of them. AAA could be very good solution and AAA servers such as RADIUS and Diameter [3, 2, 14] have to be taken under consideration.

The Structure of this paper is following. First we take a brief look to MIPv4 and solutions used to implement it. Then we go through regular IPsec and problems that occur when it is made mobile. After that there are chapters about protocols AAA, RADIUS and Diameter that are used for authenticating mobile clients. Chapter five contains also a solution to few problems. After that there is a short conclusion of the content of this paper that tries to summarize the main points founded in IPsec authentication scenarios in MIPv4 situations.

2 Mobility on IPv4

IPv4 was not originally designed for mobility. The place of the receiving node is decided on its IP address. The IP address dictates where datagrams are delivered and that is the biggest question mark when designing protocols that make mobility available to IP. The other option to forward the datagrams to their rightful target would be adding routing information about the location of the node to the datagrams. This solution is good but the overhead that is created is usually too much. The security issues act also as a major part in mobility. How to authenticate mobile node and what routers do we trust [1].

2.1 Mobility solutions using foreign agent (FA)

The main solution to these problems is based on home agent (HA) foreign agent (FA) model. In this model every mobile node has a home agent that is responsible of delivering datagrams to the right foreign network that node is visiting in. When entering the visiting network mobile node gets a temporary address from FA. When Mobile node wants to contact somebody FA delivers the message and sets the source IP address as mobile nodes home IP address. When contacted host sends in reply it sends it to HA who then tunnels it to FA. FA delivers the incoming package to mobile node. When tunnel is created all the messages send to HA are delivered to straight to FA. Foreign agent works as a primary router for mobile node. The routing schema is explained in figure Fig. 1 [1]

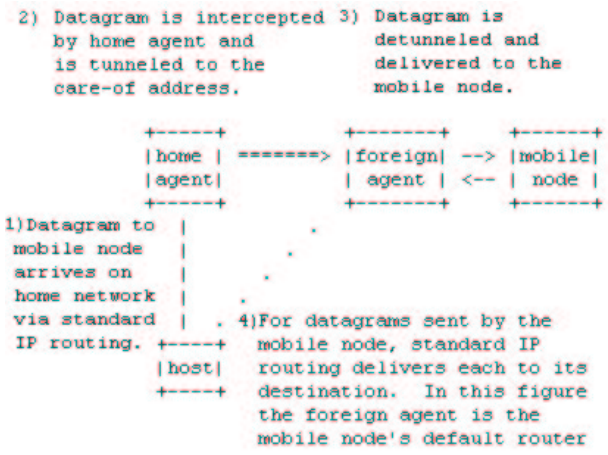

Figure 1: Discovering mobile node

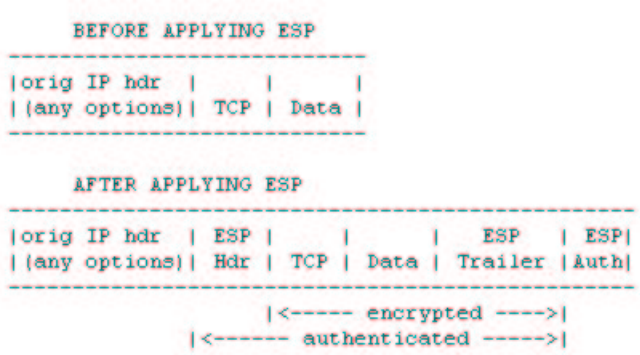

Figure 2: ESP on IPv4 packet, transport mode

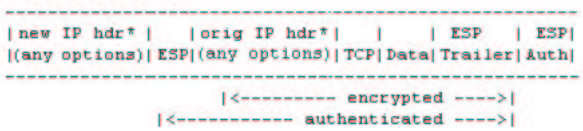

Figure 3: ESP on IPv4 packet, tunnelling mode

2.2 Mobility solutions without foreign agent (FA)

The solutions that do not have foreign agent are also very common. Especially in business world they are numerous solutions where foreign agents do not exists. If FA doesn't exist mobile node has to grant an IP address that it can use while visiting the foreign network. IP address can be given by DHCP or something else similar to it. After the mobile node gets temporary IP address it can start communicating. The positive side of this solution is that no FA is needed. The negative side of this solution is that a pool of IP addresses needs to be reserved for every possible mobile node visiting the network and as we can see later this presents challenges to IPsec authenticating protocols that are based on AAA such as Diameter and RADIUS [1].

3 IPsec

IPsec is union of two well known protocols authorization headers AH and encapsulating security payload ESP. IPsec is also used in authorization of client.

IPsec is designed to provide security to IP traffic. SAs (security association) are big part of IPsec. SAs hold all the information needed to IPsec including keys used in symmetric encryption of ESP packet payload. When SAs are constructed IPsec needs a pair of keys that are used to create SAs. IPsec does not really care where it gets necessary keys used needed in symmetric encryption but usually IKE protocol is used to provide these keys to IPsec [18].

3.1 IPsec Authentication

Part of IPsec is authentication that is done in the beginning of IPsec session. Authenticating is usually done with IKE and it is based on either shared secret or public key infrastructure. Shared secret is based on something that both parties are aware of before hand and public key infrastructure is based on the fact the parties own signature is encrypted with his private key and only the public key of the subject can decrypt the signature [2].

3.2 Authorization Headers (AH)

The purpose of AH is to provide connectionless integrity and data origin authentication for IP datagrams. This is done by special AH header that is attached to IP datagram [11]. Most important fields that AH header has are SPI (Security Parameters Index) and authentication data. AH was originally inserted to IPsec because some countries do not allow strong encryption in IP traffic. ESP protocol can perform also this function and when ESP is used AH practically becomes obsolete.

3.3 Encapsulating Security Payload (ESP)

ESP in a tunnelling mode is a protocol that is use to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service sequence and limited traffic flow confidentiality. ESP protocol builds a separate packet in the top of original IP packet. This new packet acts a self to the original IP packet and the whole original packet is located as a encrypted payload of this new packet. ESP can also be used in transport mode and the differences between transport and tunnelling mode can be found out from figures Fig. 2 Fig. 3 [10]

3.4 Combining MIPv4 and IPsec

One solution that is trying to solve problems with making IPsec available to mobility by suggesting that another layer is needed between IPsec and mobility. This layer would hide mobility from IPsec and consider it to be in regular network. This solution would solve problems with ESP part. In this solution authorization is still a problem. Authenticating structures that need keys (shared secret or public/private key) would work but the security issues of keeping these keys secure especially in client end will cause problems. Smart cards or something else like that could be a solution. RADIUS and SecurID are offered as solutions to these problems [23, 22, 5].

There is also other solution [25] that is based on IETFs drafts and RFCs. AAA (Authentication, Authorization, and Accounting) is a framework that defines requirements for safe authentication in MIPv4. AAA servers are designed to be solution to problems with combining MIPv4 and IPsec. AAA servers such as Diameter and RADIUS are designed in a way that can handle both situations local and roaming use [9, 4].

3.5 Problems with making IPsec mobile

There are numerous problems with making IPsec mobile. There is usually no strong authentication of the visiting user in foreign node. Sometimes there are no FAs in foreign network or FAs are configured differently from what is needed. AAA is designed in a way that it needs FAs [25]. Usually there is a RADIUS server in a network but the configuration is not suitable for mobile node.

Also PKI end-user authenticating causes problems because of key distribution. Mobile host are not often very well protected to hold secret keys in a way that they are not compromised. Also if secret keys could be preserved enough safely the number of keys is a problem when thinking the administration. Should only one key be used between all the different users? What then when somebody decides to change company. All the mobile workstations need a new key. If everybody will have their own key, how are the keys managed. Is their after all a need for AAA server [16, 7, 12].

4 Internet Key Exchange, IKE

Internet key exchange is a framework that defines protocol used to change security keys between two parties of communication via Internet. IKE supports also client mode that means it can work between two connection points although they are not end points. Attributes that are necessary are encryption algorithm, hash algorithm and authentication method. SA (security association) has a close connection to IKE. It is a set of policy and keys used to protect information. Used SAs are decided in handshake stage of IKE protocol [2].

4.1 How IKE works

IKE has two main modes to work there is a normal mode and aggressive mode (there is also third mode named quick-mode but it is only used to refresh SAs). IKE uses UDP packets and the normal mode needs six messages. Below is shortly described the content of each IKE message used in building the SAs. Two communicating parties are named client and server because of the clarity of example although IKE is defined to work between two clients. Fig. 4[21, 2]

- 1. Client: IKE SA proposal of supported authentication methods, Diffie-Hellman groups, encryption and hash algorithms, SA lifetime
- 2. Server: IKE SA response of authentication to attributes asked in message 1.
- 3. Client: Diffie-Hellman secret + random value

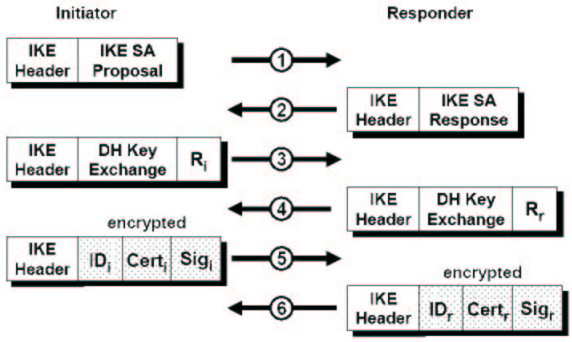

Figure 4: IKE in normal mode

- 4. Server: Diffie-Hellman secret + random value. Now symmetric session key can be produced and rest of the messages can be encrypted with it
- 5. Client: Identity and possible certificate/public key
- 6. Server: Same message back to client

4.2 IKEv2

IKE is defined in three different RFCs 2407, 2408 and 2409. IKEv2 draft was published in January 2004 and the new document should cover all these three old ones and have some improvements to IKEv1.

The interesting part in the IKEv2 is the scenario where it is used to provide endpoint to security gateway transport. This scenario is designed in a way that endpoint is a portable computer on a foreign network. IKEv2 is used to build up SAs that enable creation of an IPsec tunnel between endpoint and home network. The other interesting fact is that endpoint computer has an option that it can request an IP that belongs to security gateway and use it during the duration of its SA. Basically there are two addresses used in this scenario. Because endpoint computer gets an IP address that belongs to gateway its packet are forwarded straight to there and the gateway tunnels them to the actual location of the endpoint.

Because IKEv2 packets uses port numbers as their identifiers, LANs with NAT on shouldn't cause too big problems. Also firewalls can be configured to let IKE UDP packets pass freely to the host machines [8].

4.3 Other solutions to IKE

There are also other authentication possibilities: X.509 certificates, naming trusted certifiers, user name password combinations, SecurID or other challenge response cards and of course Windows authentication system Kerberos [23, 15].

5 AAA

AAA is an Authentication, Authorization, and Accounting is more like a framework than a protocol. In RFC3127 is defined the possible protocols that meet the criteria of becoming a protocol that fulfils the requirements set in AAA. The most suitable of them are RADIUS [3] and Diameter

[14]. AAA is also considered to be a solution to MIPv4 authenticating problems. AAA servers are designed in a way that mobile clients should not cause any problems to them. Although AAA solution model requires that foreign network that mobile node is visiting in needs a FA to routing purposes. LetŠs first take a brief look to RADIUS and Diameter and then go on how AAA can offer authentication in situations that require mobility [13].

5.1 RADIUS

RADIUS is an authenticating protocol that verifies if client has access rights to resource it trying to use. RADIUS works with UDP packets and it is designed for client-server model. The basic model of RADIUS is that it receives a request from the client and checks with the server that the request is directed to if it is ok to grant access to the client. If access is granted the client is given access rights to resource [3].

RADIUS messages are defined in RFCs 2865, 2866, 2867, 2868 and 2869. The message passing between RADIUS client and server is described below. Fig. 5[3, 19, 22]

- 1. Network Access Server gets username/password combination from the client that requests access. NAS sends this message encrypted to the RADIUS Server. This is an authentication phase.
- 2. If authentication data is real, RADIUS server replies to network access server with accept message. This message can have extra content like IP-addresses that are allowed. This is an authorization phase.
- 3. NAS sends an Accounting-request that indicates that the remote user is logged onto the network. This is an accounting phase.
- 4. The RADIUS Server responds with an Accounting-response when it has stored the relevant information.
- 5. When user logs out NAS sends an Accounting-request that indicates that the remote user has logged out.
- 6. RADIUS Server sends an Accounting-response when it stored the relevant information about user leaving the system.

5.2 Diameter Base Protocol

Diameter is a protocol that defines AAA framework for applications that require network access or mobility. Diameter is designed for both local and roaming situations. This means that it would probably be able to solve problems with Authentication if it can be implemented efficiently to MIPv4. The need for Diameter was realized when new ways of connecting the Internet surfaced (wireless, DSL, MIPv4 and Ethernet) and complexity of these new connection types were lot higher than in the older models(dial-up PPPs)[14].

Diameter works almost as same as the RADIUS when authorizating and authenticating the client. The protocol uses message format defined in RFC 2924 when sending requests between server and client [20, 14].

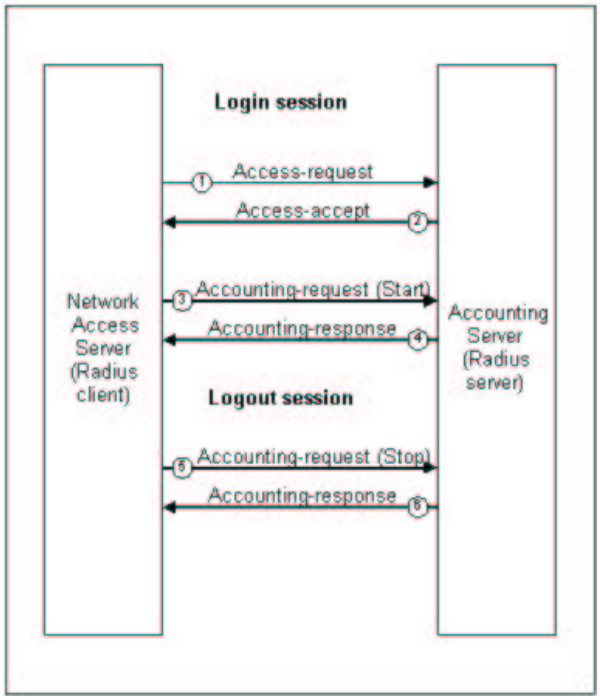

Figure 5: RADIUS message passing flow

5.3 AAA in authentication of mobile node

AAA is a one way of identificating of mobile node in foreign domain. The typical way of doing this is passing request to authenticate from foreign domain to home domain. The information is passed via local authority (AAAL) and home authority (AAAH). Fig. 6 [9]

5.4 Different phases of AAA

AAA can be divided into twelve different steps. The next list of phases in authentication should clear the picture of what happens in AAAA and important parts of AAA can be easily detected from it.

5.4.1 Phase one

Fig. 7 represents phase one. This the initial message passing sequence from mobile node to HA. [25]

- Nro. Message
- 0: Foreign agent (FA) advertises challenge
- 1: Mobile node (MN) adds NAI, Challenge Response etc., to Mobile IP registration request
- 2: FA invokes AAA protocol with its local AAA server (AAAF)
- 3: AAAF (proxy) parses NAI, sends MN's home server address (AAAH)
- 4: AAAF invokes AAA protocol and awaits approval by AAAH
- 5: AAAH checks MN credentials and may allocate a home address for the mobile node

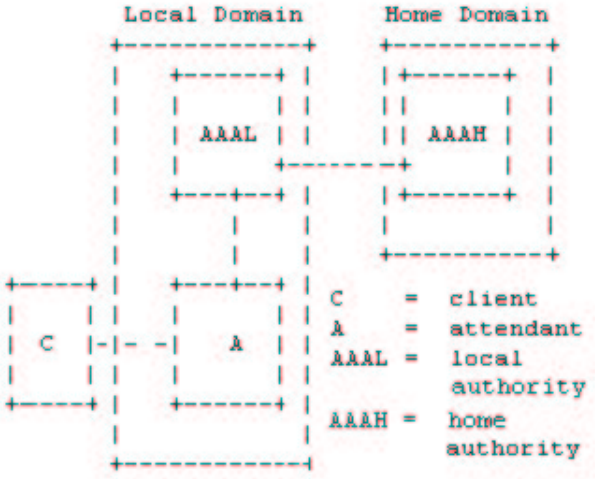

Figure 6: AAA in foreign network

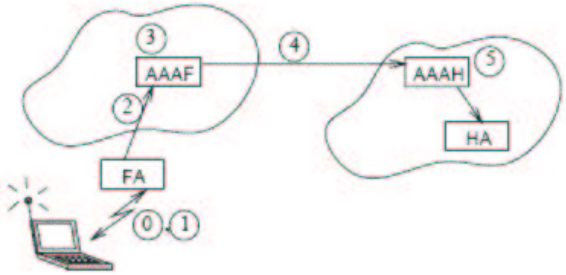

Figure 7: AAA phase 1

5.4.2 Phase two

Fig. 8 represents phase two. This phase describes the key generation and SAs between communicating parties. This is step six in AAA [25].

AAAH generates:

- K1: MN FA
- K2: MN HA
- K3: FA HA

AAAH encrypts:

- K1 and K2 using SA1 ! MN
- K1 and K3 using SA3 ! FA
- K2 and K3 using SA2 ! HA

5.4.3 Phase three

Fig. 9 represents phase three. In phase three the keys are passed to rightful owners and MN is authenticated [25].

- 7: AAAH relays Mobile IP information to HA with K2, K3
- 8: HA creates registration reply using K2, and K3 for FA.

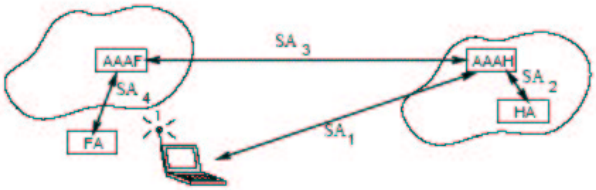

Figure 8: AAA phase two

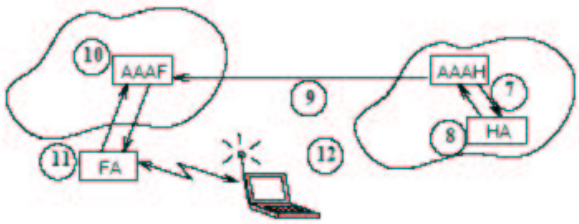

Figure 9: AAA phase three

- 9: HA sends results to AAAH, which proxies request to AAAF
- 10: AAAF decrypts K1 and K3 using SA3, re-encrypts using SA4
- 11: FA decrypts K1 and K3 using SA4, checks registration reply and FA HA authentication, adds MN FA using K1
- 12: MN decrypts K1 and K2 using SA1, checks registration reply, and MN FA authentication

5.5 Modifications

RADIUS and Diameter are AAA servers that are used to provide security services in local and roaming situations. Because MIPv4 requires strong authentication between mobile node and its home agent some kind of mobile security association is needed and perhaps AAA can be modified to solve this problem. Solutions of these modifications have been made and they can be found from IETF drafts "AAA Keys for Mobile IPv4" and "Mobile IPv4 Extension for carrying Network Access Identifiers" which can be found from IETF's web pages [7, 6].

The other big question mark is the role of FA. As mentioned earlier in text AAA servers aren't the only best option to MIPv4 authentication 3.4. Company WLANs without FA are common and as pointed out AAA can not work without FA. Even with FA already existing RADIUS servers are sometimes very difficult to be configured to handle requirements of AAA or FA will not co-operate with AAA servers.

5.5.1 Proposal of eliminating foreign FAs

How could be problems with AAA model to be solved? One pretty straight forward solution is to move FA from foreign network to home network. The overhead problems would be bigger but the compatibility problems that MN and FA could have would be solved. The list of comments presented below

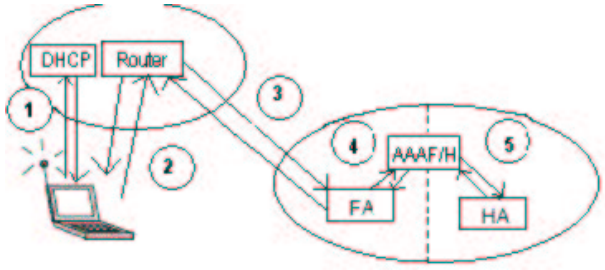

Figure 10: AAA proposal - Foreign agent inside companyŠs LAN

should clear the picture what is needed and how this solution would solve the problems.

- Corporate networks already have usually two different sectors inside them. The other one is intranet and the other one is outside intranet. This outside network usually provides services to other persons than employees of the corporation (good example would be web servers). The FA could be part of this outside network.
- When contacting the FA, which is open to everyone, MN could use SecurID authentication method described in reference [23] to prove itself and establish symmetric encoded tunnel between MN and FA. The time stamp based secret is widely used in corporate world and perhaps SecurID is the one of the most used one. SecurID is based on two facts something that you know and something that you have. The thing that you know is a password that can be used multiple times and the thing that you have is RSA based code generator that creates a random code in every sixty seconds. If code creators are properly synchronized in both end points of communication this code should prove that the same code at the same time and authentication should not be problem. The code creator could be integrated to MN and it could only be activated with the password provided to end user [23].
- After the tunnel is operating FA could send the authentication data to AAAF/H which is combined in this scenario and they could proceed with the AAA protocol. AAAF/H would be a gateway between public and private corporate network (AAAF part would be interface to public side and AAAH part to private side). AAAF/H would perform all the same phases then in regular AAA [9].
- The tricky part has been how to send the MN-HA shared secret to MN. The problem can be seen in Fig. 8 if the FA is part of the home network. This problem is solved if the tunnel is established as described in second argument of this list.
- Because FA belongs to company itself, the FA can be configured as wanted. The problems with miss configured FAs are solved.
- The picture Fig. 10 should clear the picture.
  - Nro. 1 The mobile node gets IP address from DHCP in foreign network.
  - Nro. 2 The MN communicates with outside network trough router located at foreign network. The packets payload can be encrypted with symmetric encoding based on time stamp secrets.
  - Nro. 3 Router in foreign network sends the data into FA located in home network.
  - Nro. 4 FA decrypts the packets and begins the AAA procedure with AAAF/H. In this stage the border between public and private corporate network is crossed.
  - Nro. 5 HA does not know that anything is different from original AAA.

5.6 Corporate vendor view

Some companies like Cisco are taking the angle of AAA when combining the MIPv4 and IPsec authentication. They are providing equipment to this sector such as RADIUS and Diameter servers [24].

The basic point of favouring this angle is that AAA servers can be used to other things also as authenticating PPP connections over PSTN. That is the reason why lot of companies already have a RADIUS server and selling them a new one does not take as much effort as selling them a totally new product. CISCO offers only modified RADIUS servers but they are getting ready to switch to Diameter protocol based servers. The possible demands presented by mobility are taken under consideration in Cisco's web pages [24].

6 Conclusion

Let's start this conclusion by summarizing the problem and then going into what have been done and what could be done to solve the problems mobility causes to regular IPsec.

Mobility has been one the key questions in IP protocols and IPv4 offers basically two options to offer mobility. The first one is agent model with home agent (HA) and foreign agent (FA). In that model mobile node actually has its own IP address and agents are responsible of routing the packets. Other mode is one without FA and this scenario mobile node gets a new IP address for the time it visits the foreign network.

The problem that is relevant to this paper is authentication. Authentication in regular network is usually done with IKE and certificates are used to provide authentication data. In the case of MIPv4 there is lot of other parties involved in transferring the data and that causes problems.

One solution to solve authentication problems is AAA servers such as RADIUS and Diameter. When the need for authenticating mobile node in home network came obvious and IETF researched different options. AAA standard was released and old RADIUS servers were found suitable for the job. The planning for Diameter was also started than and it is designed to be replacement for RADIUS. AAA structure is based on the fact that corporations have AAA servers that authenticate requests coming from mobile nodes that are

visiting foreign networks. These messages are delivered by a FA of the foreign network. The main problem in this scenario is that what if foreign network does not have FA or that FAs in foreign networks are not compatible with mobile node.

Solution to this problem that I suggest is to have own FA inside the home network. This would definitely solve the problems with FA section. Of course there is still problem with how to transfer the MN-HA secret key to MN node. This problem could be solved by using symmetric encoding between MN and FA that is based on time stamp secrets for example such as SecurID. Products that enable this are already in wide use and technology is easily accessible. Although some extra overhead is created by this solution I could argue that security gained by this solution is worth the overhead.

As a summary to the end I could claim that the need for IPsec authentication in MIPv4 is real but the security issues considering it depend much on what is planned use of MNs. It could be easily agreed that everybody who offers MIPv4 should have FA in their network but the things aren't always that simple. Sometimes even no authentication at all can be good enough solution for some users. If extra security is needed it can be provided with already existing tools.

References

[1] C. Perkins, Nokia IP Mobility Support for IPv4 (RFC 3344) *http://www.ietf.org/rfc/rfc3344.txt*

[2] D. Harkins, D. Carrel, Cisco Systems The Internet Key Exchange (IKE, RFC 2409) *http://www.ietf.org/rfc/rfc2409.txt*

[3] C. Rigney Livingston, A. Rubens Merit, W. Simpson Daydreamer, S. Willens Livingston Remote Authentication Dial In User Service (RADIUS, RFC 2138) *http://www.ietf.org/rfc/rfc2138.txt*

[4] Eva Gustafsson, Annika Jonsson Ericsson, Charles E. Perkins Nokia Research Center MIPv4v4 Regional Registration, draft-ietf-mobileip-reg-tunnel-08 *http://www.ietf.org/internet-drafts/draft-ietf-mobileip - reg-tunnel-08.txt*

[5] S. Vaarala MIPv4v4 Traversal Across IPsec-based VPN Gateways draft-ietf-mobileip-vpn-problem-solution03 *http://www.ietf.org/internet-drafts/draft-ietf-mobileip-vpn- problem-solution-03.txt*

[6] F. Johansson, T. Johansson Bytemobile MIPv4 Extension for carrying Network Access Identifiers, draft-ietf-mip4-aaa-nai-02 *http://www.ietf.org/internet-drafts/draft-ietf-mip4-aaa-nai-02.txt*

[7] C. Perkins Nokia, Pat R. Calhoun Airespace AAA Keys for MIPv4, draft-ietf-mip4-aaa-key-03 *http://www.ietf.org/internet-drafts/draft-ietf-mip4-aaa-key-03.txt*

[8] Charlie Kaufman Internet Key Exchange (IKEv2) Protocol *http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-12.txt*

[9] S. Glass Sun Microsystems, T. Hiller Lucent Technologies, S. Jacobs GTE Laboratories, C. Perkins Nokia Research Center MIPv4 Authentication, Authorization, and Accounting Requirements (RFC 2977) *http://www.ietf.org/rfc/rfc2977.txt*

[10] S. Kent BBN Corp, R. Atkinson @Home IP Encapsulating Security Payload (RFC2406) *http://www.ietf.org/rfc/rfc2406.txt*

[11] S. Kent BBN Corp, R. Atkinson @Home IP Authentication Header (RFC2402) *http://www.ietf.org/rfc/rfc2402.txt*

[12] S. Kelly Airespace, S. Ramamoorthi Juniper Networks Requirements for IPsec Remote Access Scenarios (RFC3457) *http://www.ietf.org/rfc/rfc3457.txt*

[13] D. Mitton Nortel Networks, M. St.Johns Rainmaker Technologies, S. Barkley UUNET, D. Nelson Enterasys Networks, B. Patil Nokia, M. Stevens Ellacoya Networks, B. Wolff Databus Inc. Authentication, Authorization, and Accounting: Protocol Evaluation (RFC3127) *http://www.ietf.org/rfc/rfc3127.txt*

[14] P. Calhoun Airespace, Inc., J. Loughney Nokia,E. Guttman Sun Microsystems, Inc., G. Zorn Cisco Systems, Inc., J. Arkko Ericsson Diameter Base Protocol (RFC3588) *http://www.ietf.org/rfc/rfc3588.txt*

[15] Stephen Kent, Tim Polk Public-Key Infrastructure (X.509) (pkix) *http://www.ietf.org/html.charters/pkix-charter.html*

[16] Prof. Dr. T. Braun Secured MIPv4 - How should MIPv4 and IPsec work together? *http://www.iam.unibe.ch/ rvs/teaching/WS00/seminar /mobileVPN.PDF*

[17] Sellen, Abigail, Murphy, Rachel The Future of the Mobile Internet: Lessons from Looking at Web Use *http://www.hpl.hp.com/techreports/2002/HPL-2002-230.pdf*

[18] Charlie Kaufman Introduction to IPsec *http://www.acm.org/sigs/sigsac/SLIDES/ccs03-2.pdf*

[19] B. Aboba Microsoft, G. Zorn Cisco Systems, D. Mitton Circular Logic UnLtd. RADIUS and IPv6 *http://www.ietf.org/rfc/rfc3162.txt*

[20] N. Brownlee The University of Auckland, A. Blount MetraTech Corp. Accounting Attributes and Record Formats *http://www.ietf.org/rfc/rfc2924.txt*

[21] Dr. Andreas Steffen Secure Network Communication *http://www.strongsec.com/zhw/KSy_IPsec.pdf*

[22] Joseph Davies, Microsoft Corporation RADIUS Protocol Security and Best Practices *http://www.microsoft.com/windows2000/techinfo/ administration/RADIUS.asp*

[23] RSA Security Inc. RSA SecurID *http://www.rsasecurity.com/products/securid/*

[24] Cisco Systems, Inc. Cisco's Overview Authentication, Authorization, and Accounting *http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/aaans_ov.htm*

[25] Gopal Dommety Cisco Systems, Steve Glass Sun Microsystems, Stuart Jacobs GTE Laboratories, Basavaraj Patil Nortelnetworks, Charles E. Perkins Nokia Research Center AAA Requirements from Mobile IP *http://www.ietf.org/proceedings/99nov/slides/mobileip-aaa.pdf*