

A Secure Network Access System for Mobile IPv6

Hong Zhang^{*a,b}, Man Yuan^c, Rui He^c, Luliang Jiang^d, Jian Ma^d, Hualin Qian^a

^a Computer Network Information Center, CAS; ^b Institute of Computing Technology, CAS

^c Beijing Univ. of Area. & Astro; ^d Nokia Research Center, China

Abstract

With the fast development of Internet and wireless and mobile communication technology, the Mobile Internet Age is upcoming. For those providing Mobile Internet services, especially from the view of ISP (Internet Service Provider), current mobile IP protocol is insufficient. Since the Mobile IPv6 protocol will be popular in near future, how to provide a secure mobile IPv6 service is important. A secure mobile IPv6 network access system is highly needed for mobile IPv6 deployment. Current methods and systems are still inadequate, including EAP, PANA, 802.1X, RADIUS, Diameter, etc. In this paper, we describe main security goals for a secure mobile IPv6 access system, and propose a secure network access system to achieve them. This access system consists of access router, attendant and authentication servers. The access procedure is divided into three phases, which are initial phase, authentication and registration phase and termination phase. This system has many advantages, including layer two independent, flexible and extensible, no need to modify current IPv6 address autoconfiguration protocols, binding update optimization, etc. Finally, the security of the protocol in this system is analyzed and proved with Extended BAN logic method.

Keywords: Mobile IPv6, EAP, AAA, Diameter

1. Introduction

With the fast development of Internet and wireless and mobile communication technology, the Mobile Internet Age is upcoming. When the user is roaming, the mobile node (MN) will move and may connect to different networks from time to time. Security for MN to access different networks is very important. In this paper, we proposed a secure network access system for MN using mobile IPv6, which will be a prevalent protocol in near future.

Mobile IPv6 [1] uses a home address and some care-of addresses, one of which is primary care-of address registered in home agent. When an MN enters foreign network, it will get care-of address through address autoconfiguration, without the need for foreign agent as mobile IPv4. Usually the new care-of address will be the primary care-of address, and MN will register it in the home agent through binding update message. Then IPv6 packets addressed to MN's home address are transparently routed to its care-of address via home agent.

From the view of Internet service provider (ISP), mobile IPv6 protocol alone is not enough for secure mobile Internet service. The MN should be authenticated and authorized when it requires network access, either in the foreign network or home network, and its resource consumption could be accounted. Internet service for the MN should be protected and not stolen by attackers.

In order to achieve a secure network access system for mobile IPv6, We propose several important security goals to accomplish. 1) The MN and the network attendant could authenticate each other in authentication phase, which prevents man-in-the-middle attack. 2) Inter-domain authentication/authorization must be supported, so that MN could be authenticated and authorized in foreign networks. 3) No one including AAA servers in foreign domain could forge access request of MN and

* contact: hong.zhang@ipv6.com.cn; phone 86-10-65392828-2855; Computer Network Information Center, 4 South 4th Street, Zhongguancun, Beijing, 100080, P.R.China

send it to AAA servers in home domain. 4) Transport service for the MN should be protected and prevent attacker to steal the service after MN is authenticated.

There already have some researches on network access security, but they are insufficient for a secure mobile IPv6 access system, especially on multi-access links. EAP [2][3] methods (such as EAP-MD5, PEAP, etc.) are layer two authentication on point-to-point links, not suitable for multi-access links like IEEE802.3. The IEEE802.1X [4] defines port-based network access control that is used to provide authenticated network access for Ethernet networks and it's also a link layer dependant authentication methods. PANA [5] is a new layer two agnostic network layer messaging protocol for authenticating IP hosts for network access. Its main idea is carrying EAP payload in IP layer. But it doesn't support Mobile IP. AAA protocols such as RADIUS [6] and Diameter [7] are protocols between attendant and AAA server, also insufficient for secure access support for mobile node. Other solutions such as AAA architectures for IPv6 network access proposed in [AAAv6] [8] require modification of IPv6 address autoconfiguration protocols.

In next section, this paper gives overview of the proposed secure access system for mobile IPv6. In section 3, three phases of the access procedure are described. The security of this system is proved through formal logic extended BAN in section 4. A brief introduction of system implementation is given in section 5.

2. Secure Access System Overview

The proposed mobile IPv6 access system consists of access router, attendant, local AAA server (AAAL), home AAA server (AAAH) and home agent (HA), as figure 1 shows. The access router is the first hop to MN, and it has dynamic access control list (DACL), which is configured by attendant and enforces the MN's traffic. The attendant is back end server, which may be multi-hop from MN. It deals with MN's access request and controls access routers. The MN's access request, NAI (Network Access Identifier) and identity credentials etc. are encapsulated in AAA access request messages and sent to AAA servers (AAAL and/or AAAH) by attendant. We choose Diameter as the AAA protocol in this system, because it has many advantages over RADIUS. MN also could register its binding update message in HA through AAAH. This system combines binding update procedure with AAA procedure, thus reduce the number of message round trips. After successful authentication, attendant could modify DACL in access router to let MN's packet pass, and distribute session key to build Security Association (SA) between MN and access router to protect user traffic from service theft.

This mobile IPv6 secure access system has many advance features: It is layer two independent, since it runs on IP and upper layers and does not modify current IPv6 autoconfiguration protocols. It is flexible and extensible, and could be applied on multi-access links as well as point-to-point links. User identity confidentiality in access is provided through dynamic built secure channel. This system also provides an optimization for mobile IP binding update registration.

In figure 1, a mobile node (MN) needs access to Internet being provided by foreign domain. Before MN can access the foreign network, it should be authenticated and authorized through network authentication server, and its resource usage may be accounted. The overall problem is AAA (Authentication, Authorization and Accounting). An agent in the foreign domain attends to the MN's request and provides network access service (called the attendant). Attendant is likely to require that the MN provide some credentials which can be authenticated before access the resource. The attendant is expected to consult a local authority in the same local domain (AAAL) in order to obtain proof that the MN has acceptable credentials. AAAL itself may not have enough information to verify credentials of the MN, so it may negotiate with the authority in MN's home network (AAAH).

In this system, we suppose that there already have some static security associations, such as, SA1 between AAAL and AAAH, SA2 between AAAL and attendant, SA3 between AAAH and HA, and SA4 between attendant and routers. Such assumption is feasible in practical deployment. After the MN is authenticated by the access system, dynamic SA will be built between MN and access router.

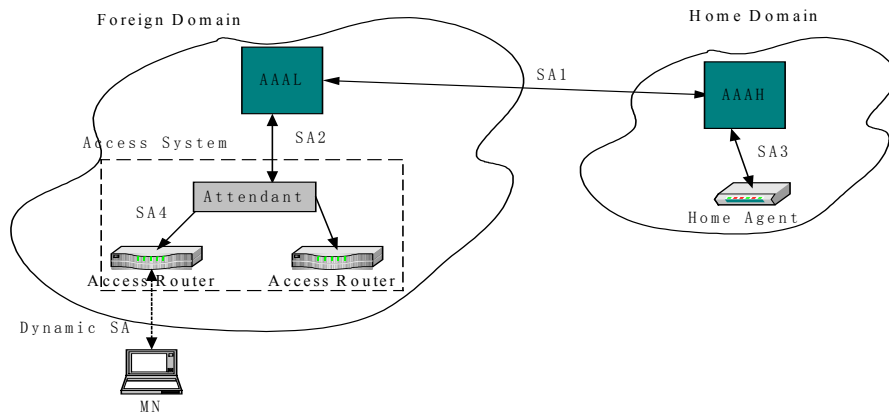


figure 1 the secure access system architecture

The secure access procedure for MN is comprised of three phases, which are, initial phase, authentication-registration phase and termination phase. The detail of these phases is described in following section.

3. Procedure in Secure Access System

3.1 Initial Phase

The first phase is initial phase. When MN first enters a foreign network, it is in this phase. The MN will get IPv6 care-of-address by either stateful or stateless address autoconfiguration. This system does not modify current IPv6 address autoconfiguration protocols. Then MN sends a server-request packet to attendants with an IPv6 site-local anycast address. The anycast mechanism ensures the nearest attendant to the MN will receive this request. The attendant receives the request and sends reply. MN will build secure channel with the attendant by a TLS-alike way. This secure channel will protect further authentication and registration messages. The messages flow is shown in figure 2.

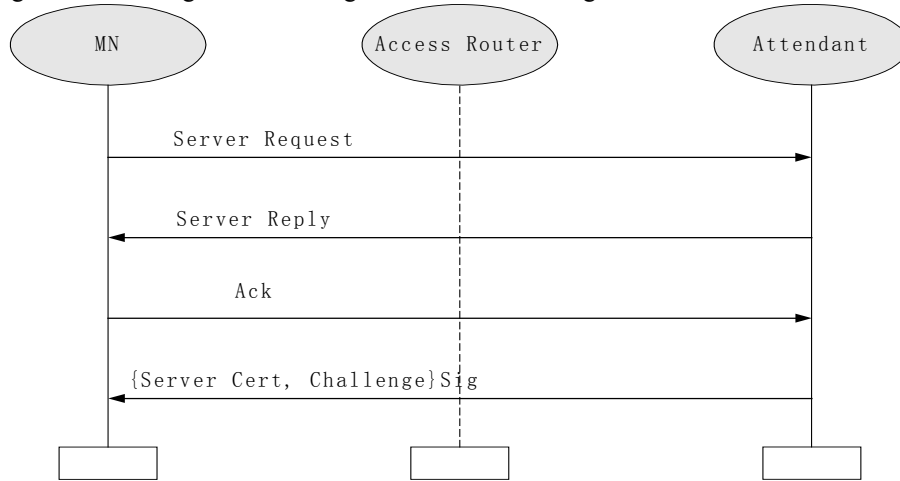


figure 2 initial phase messages flow

Message 1: Server Request := MN’s request for a attendant to deal with its access request

Message 2: Server Reply := Attendant’s reply

Message 3: Ack := MN’s acknowledge for one of the attendants.

Message 4: Server Cert, Challenge := the chosen attendant returns its certificate and a challenge, the whole message is signed by the attendant. {}Sig means message is signed by private key of the attendant, for abbr.

In Message 1, the source IPv6 address is MN’s care-of address, and the destination address is attendants’ well-known IPv6 site-local anycast address. In initial phase, router allows IP packets from unauthenticated MN with destination address of attendants’ anycast/unicast addresses to pass, and also packets from attendants to unauthenticated MN, thus only allows communication between unauthenticated MN and attendants. When the attendant receives message 1, it will response message 2 as a reply to the MN’s request and tell the MN its unicast IPv6 address.

Receiving message 2, MN will send acknowledge to it, as message 3. There may be multiple attendants in this system to improve system robustness. The routing mechanism of anycast will ensure that the nearest attendant to the MN will provide service for the MN.

Then, the attendant should return a message, including its certificate, a challenge for the MN for subsequent message. The message must be signed by the server’ private key. After receiving this message, MN could verify attendant’s certificate and its public key. Then MN could build a TLS-alike secure channel with the attendant through encrypting data with the attendant’s public key.

In initial phase, attendant won’t compute and return certificate with challenge until MN send ACK message. This could prevent attacker from doing blind DoS attack by sending lots of requests to some extent.

3.2 Authentication – Registration Phase

The second phase is authentication- registration phase. In the second phase, MN will send its NAI, identity credentials to attendant through the secure channel built in initial phase. Thus the user identity privacy is achieved by encryption. Authentication of MN may need AAAH if MN is in foreign domain, and AAAH will do binding update registration in HA for the MN. Authentication is accomplished by transferring EAP payload between MN and AAAH. We adopt EAP-MD5 as major authentication method and other EAP methods are also allowed as complement. After successful authentication, the attendant tells the router to modify DACL to allow MN’s traffic and could build SA between MN and router to protect traffic. The messages flow is shown in figure 3.

- Message 1: $E\{NAI, Cha, N\}$:= MN's NAI, Challenge (Cha) in initial phase, Nonce (N) for message freshness, the whole message is encrypted using the attendant's public key
- Message 2: AMR1 := Auth-MN-Request message, this message contains NAI. AAAL will forward this message to MN's AAAH
- Message 3: AMA1 := Auth-MN-Answer message, this message contains NAI, EAP-MD5 challenge AVP
- Message 4: $\{EAP, N\}sig$:= attendant sends the EAP-MD5 challenge to MN. Nonce guarantees the message freshness. This message is signed
- Message 5: $E\{NAI, EAP, N, BU\}$:= MN sends NAI, EAP-MD5 challenge and response, nonce and binding update (BU) request to attendant.
- Message 6: AMR2 := attendant encapsulate NAI, EAP response in AVPs, BU and sends them to AAAL through AMR message
- Message 7: BUR := Binding Update Request, AAAH sends binding update request to HA, and HA replies BUA(Binding Update Answer)
- Message 8: AMA2 := This message contains success or failure code for MN authentication request.
- Message 9: Notice := Notice the MN's acceptance or rejection

In message 1, the MN sends its NAI, challenge and nonce for freshness to attendant. This message is encrypted with the attendant's public key, so only the attendant could know the content while others can't see it. Then attendant decrypts the message 1, and get NAI of the MN. After getting the NAI of the MN, the attendant composes a Diameter MIP application message AMR that is Diameter MIP access request message and sends this message to local AAA server. AAAL couldn't authenticate the user and it forwards this message to AAAH. When AAAH receives AMR message from an AAA server from foreign domain that has roaming agreement with the home domain, it will help AAAL to authenticate the MN. AAAH replies AAAL the AMA1 message with EAP-MD5 Challenge AVP (attribute value pairs) in it. AAAL receives the AMA1 message and forwards it to the attendant. The attendant gets EAP-MD5 challenge AVP from AMA1 message, and sends the MD5 challenge and nonce to the MN. This message is signed with the attendant's private key. When the MN received the MD5 challenge from the attendant, it computes MD5 response to AAAH's challenge, and sends NAI, EAP-MD5 challenge, EAP-MD5 response and binding update request to the attendant. The attendant composes AMR2 message and puts NAI, EAP-MD5, BU into AVPs, then sends the AMR2 message to the AAAL. The AAAL forwards AMR2 to the AAAH and the AAAH authenticates the MN. If MN is authenticated, AAAH will send BUR message (binding update request) to HA. HA replies BUA message and updates the binding of MN's HoA and CoA. The AAAH sends AMA2 message to the AAAL and the AAAL forwards AMA2 to the attendant. The attendant reacts according to the result in AMA2, say, whether accepts or rejects the MN.

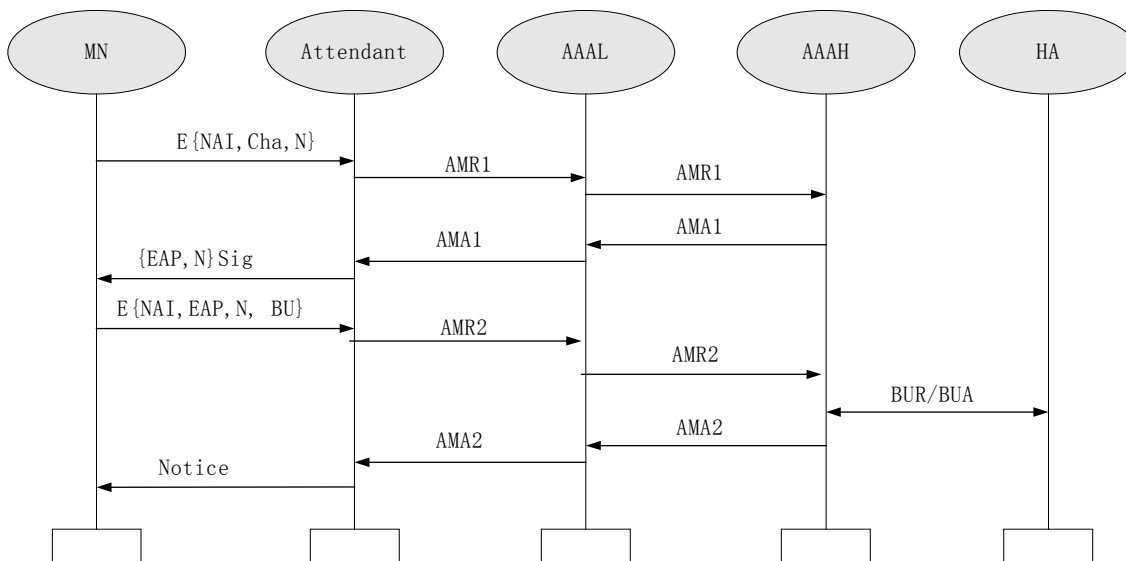


figure 3 authentication- registration phase message flow

After successful authentication, the attendant configures the router's DACL, thus allow MN's inbound/outbound traffic. In case of service theft, that is, attacker steal MN's network configuration, router could bind MN's MAC address and IP address. For more secure environment, some stricter mechanism such as IPSec could be adopted to protect traffic.

In order to build SA between the MN and the router, the attendant delivers SA to MN and router after successful authentication. The SA includes security algorithm and key. SA messages must be confidential, and messages to MN is encrypted with temp key, which is generated by Hash(NAI, EAP, N). SA message to the router is encrypted with pre-configured key.

3.3 Termination Phase

The third phase is termination phase. MN sends termination request to the attendant and the server replies. In order to detect when MN has disconnected abnormally, the attendant and access router can use layer 2 detection or heartbeat mechanism by sending probe message periodically.

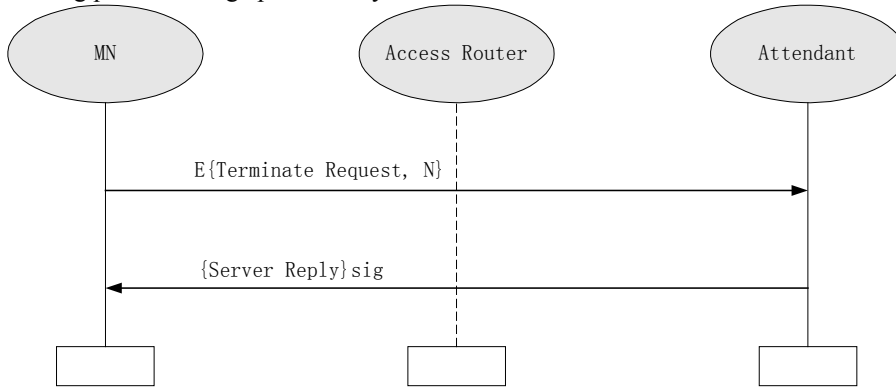


figure 4 Termination phase

Message 1: $E\{\text{Terminate Request}, N\}$:= MN's request to terminate access, this message is encrypted by XOR with a temp key. We use response of EAP-MD5 which is 128 bits length.

Message 2: $\{\text{Server Reply}\} \text{sig}$:= Attendant's reply with signature

4. Security Analysis

Formalized protocol security analysis using BAN logic [9] is provided as following. AT means Attendant.

4.1 Cryptographic Message Exchange:

1. $AT \rightarrow MN: \text{Cert}, \text{Cha}, \{\text{Cert}, \text{Cha}\} \text{Sig}$
2. $MN \rightarrow AT: \{\text{MN}, \text{Cha}, N\} \text{pk}$
3. $AT \text{ (and AAAH)} \rightarrow MN: \text{EAP-Cha}, N, \{\text{EAP-Cha}, N\} \text{sig}$
4. $MN \rightarrow AT \text{ (and AAAH)}: \{\text{EAP-Res}, \text{MN}, N\} \text{pk}$

$\text{Cert} :=$ Attendant's Cert, MN can judge it by CA's signature.

$\{\text{Message}\} \text{sig} :=$ Message signature with attendant's private key

$\{\text{Message}\} \text{pk} :=$ Message encrypted with attendant's public key.

$\text{EAP-cha} :=$ EAP-MD5 Challenge

$\text{EAP-Res} :=$ EAP-MD5 Response

4.2 Protocol Analysis

$MN \triangleleft \text{Cert}, \text{Cha}, \{\text{Cert}, \text{Cha}\} \text{Sig}$

$MN \models \text{Cert}$

$MN \models \text{PK} \mapsto AT$

$MN \models AS \sim \text{Cha}$

$AT \triangleleft \{\text{MN}, \text{Cha}, N\} \text{pk}$

$AT \models \#(\text{Cha})$

$AT \models \#(\text{MN}, N)$

$MN \triangleleft \text{EAP-Cha}, N, \{\text{EAP-Cha}, N\} \text{sig}$

$MN \models AT \sim \text{EAP-Cha}, N$

$MN \models \#(N)$

$MN \models \#(EAP-Cha)$
 $AT \triangleleft \{EAP-Res, MN, N\}pk$
 $AAA_H \triangleleft EAP-Res$
 $AAA_H \models MN's\ Identity$

4.3 Comparison With Former Goals

As to the four main security goals we mentioned in section 1. This system accomplishes all of them.

1) The attendant is authenticated by certificate it provides. The MN is authenticated later by EAP methods. 2) Inter-domain authentication/authorization is supported by AMR and AMA messages in Diameter protocol. 3) No one could forge access request of MN and send it to AAA servers in home domain. 4) Service theft attack is prevented by security association between MN and router.

5. Implementation

The system implementation architecture is shown in fig 5.

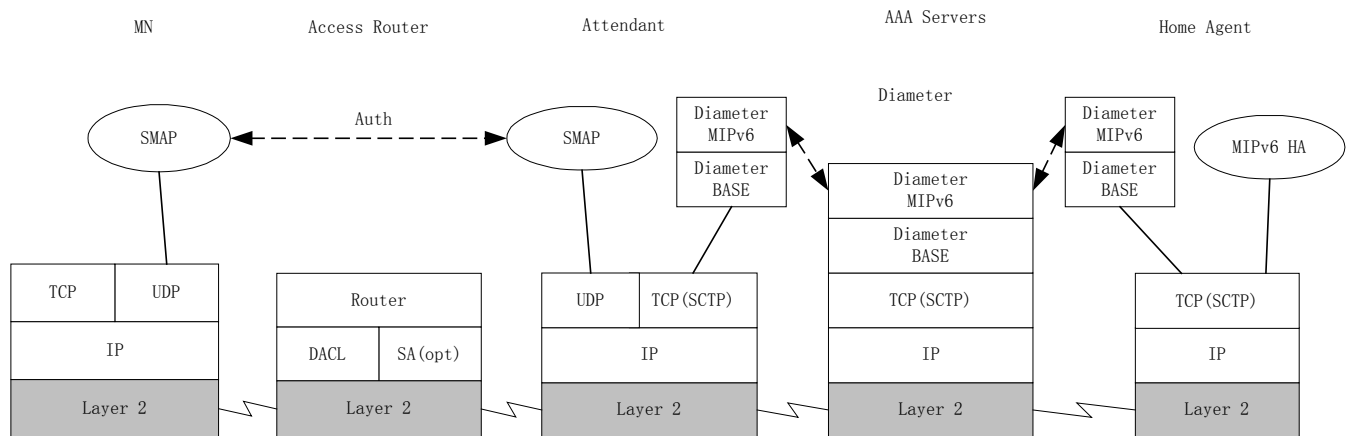


figure 5 system architecture

The protocol runs between MN and attendant in this system is called SMAP (Secure MobileIP Access Protocol). SMAP is a protocol beyond UDP and carries messages between MN and attendant. The access router has dynamic access control list to prevent unauthenticated MN from access. For stronger security requirement, it can also build security association with MN. The attendant is a key part in this system. It is a bridge between the MN and AAA servers, so it must support SMAP and diameter protocols (Diameter base and Diameter MIPv6 application). AAA servers must support diameter protocols to authenticate Mobile IPv6 nodes and home agent must also support Diameter MIPv6 application.

6. Conclusion

In this paper, we propose a secure access system for mobile IPv6. It comprises three phases and has many advance features: layer two independent, without modifying current IPv6 autoconfiguration protocols, flexible, extensible, user identity confidentiality, etc. Its security is proved by formalized logic method.

Notes: This paper is supported by National Advanced Science and Technology 863(2001AA112040, 2001AA112136): ‘Next Generation Internet Comprehensive Experiment Environment’ and 863(2001AA112052): ‘Next Generation Internet and Related Technique’

References

- 1 D. Johnson, Mobility Support in IPv6, draft-ietf-mobileip-ipv6-21.txt, February 26, 2003
- 2 L. Blunk, PPP Extensible Authentication Protocol (EAP),RFC 2284, March 1998
- 3 T. Hiller, Diameter Extensible Authentication Protocol (EAP) Application, draft-ietf-aaa-eap-00.txt, June 2002
- 4 [IEEE8021X] IEEE Standard for Local and metropolitan networks Port-Based Network Access Control, IEEE Std 802.1X-2001, June 2001
- 5 D. Forsberg, Protocol for Carrying Authentication for Network Access (PANA), draft-ietf-pana-pana-00.txt, March 2003

- 6 C. Rigney, Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000
- 7 Pat R. Calhoun, Diameter Base Protocol, draft-ietf-aaa-diameter-17.txt, December 2002
- 8 N. Asokan, AAA for IPv6 Network Access, draft-perkins-aaav6-02.txt, January 2000
- 9 M Burrows, A Logic of Authentication, 1990