Access Control Architecture for Nested Mobile Environments in IPv6

appeared in the
proceedings of the 4th Conference on Security and Network Architecture (SAR)
Batz-sur-Mer, France, 6-10 June 2005

http://www-lor.int-evry.fr/sar05/

Saber Zrelli[†] and Thierry Ernst[‡] and Julien Bournelle[§] and Guillaume Valadon[¶] and David Binet[‖]

Nautilus6 Project http://www.nautilus6.org

Access control mechanisms have been designed and implemented to limit the access, authenticate and authorize single users, either in fixed networks, or in mobile environments. With the recent advances in network mobility support in IPv6 (NEMO), access networks will soon be deployed in public transportation such as buses or trains and will in turn provide access to mobile nodes and even mobile networks. However, access control mechanisms have not been designed for users located in such nested mobile environments, that is, when the access network in which they get access to is itself mobile. An actual deployment scenario comprising a bus offering both Internet and local services to its passengers is used to illustrate the needs and the issues from a security and authentication point of view. An authentication architecture based on the latest access control mechanisms and protocols is then proposed to offer basic authentication in nested mobile environments.

Keywords: NEMO, AAA, PANA, Diameter, EAP

1 Introduction

Nomadicity of users and their needs to access foreign networks require authentication and authorization procedures in order to grant them access to resources. Mechanisms have been proposed and standardized to address such concerns. However, emerging protocols and usages are starting to challenge these mechanisms in IPv6.

In particular, NEtwork MObility (NEMO) support mechanisms have recently been specified by the IETF to allow an entire network, referred to as a *mobile network*, to migrate in the IP topology. With such network mobility support, anything can migrate in the Internet, particularly PANs (Personal Area Networks, i.e. small networks attached to people and composed of Internet appliances like PDAs, mobile phones, digital cameras, etc.), networks of sensors deployed in vehicles (aircrafts, boats, buses, trains) [EU02], and access networks deployed in public transportation (taxis, trains, aircrafts, trucks and personal cars) to provide Internet access in turn to devices carried by passengers (laptop, camera, mobile phone, and even PANs).

Network mobility does challenge the authentication mechanisms as it questions how the multiple users located in a mobile network will be granted or prevented access to the many available networks, and thus

[†]Japan Advanced Institute of Science and Technology, Japan
[‡]Keio University, Japan
[§]GET/INT Evry, France
[¶]University of Tokyo, Japan; LIP6 - UPMC, France
[‖]France Telecom R&D, France

how they would be authenticated and authorized. It is the purpose of this paper to analyze the issues and to propose an authentication architecture.

This paper is organized as follows: in section 2, we overview the existing protocols that provide mobility support and authentication. Then in section 3 we describe the case study used in the remaining parts of this paper. Based on a number of needs from a security and authentication point of view listed in section 4, we propose in 5 an access control architecture that suits the requirements of our case study. Remaining issues are listed in 6 before concluding with this paper.

2 Overview

2.1 Mobility in the Internet

According to the IPv6 address assignment rules, each node is identified by a unique IPv6 address with a prefix which identifies the location of the given node in the Internet topology. There is typically a change of this physical IPv6 address each time a mobile node changes its point of attachment and thus its reachability in the Internet topology. Such mobile nodes (MN) could either be a *mobile host* (e.g. a mobile phone or a PDA) or a *mobile router* (e.g. one providing Internet access to other nodes located in a bus). In the mobile router (MR) case, the MR and the number of nodes attached behind it are forming what is referred to as a *mobile network*, also abbreviated as a NEMO (standing for either a *NEtwork that is MObile* or *NEtwork MObility*).

The change of the physical address of the mobile node results into losing packets in transit and broken transport protocol connections if mobility is not handled by specific mechanisms, particularly in the NEMO case, where this change of address has an impact on routing to the entire mobile network. Support mechanisms are thus necessary to maintain open connections. Mobile IPv6 [JPA04] is usually sought to manage *host mobility*, i.e. mobility of a single IPv6 device, whereas NEMO Basic Support [DWPT05] would be used to manage *network mobility*, i.e. entire IPv6 networks that change their point of attachment to the Internet topology.

2.2 NEMO Basic Support

NEMO Basic Support [DWPT05] has been specified recently by the IETF community within the NEMO working group. The primary objective of this solution is to preserve session continuity between *correspondent nodes* (CNs) and nodes located behind the mobile router (called *mobile network nodes*, MNNs) while the mobile router changes its point of attachment.

In the most basic configuration, the MR has two interfaces, one *egress* and one *ingress*. The *egress interface* is attached to the access network, served by an access router (AR), initially on the *home link*, and later on a *visited link*. The *ingress interface* is attached to an *internal link* in the mobile network. All nodes (MR and MNNs) attached to a given internal link have their addresses taken from the same *mobile network prefixes* (MNPs) advertised on this link. MNNs are either fixed nodes (LFN) or visiting mobile nodes (VMN). Fixed nodes are unable to change their point of attachment while keeping their connections open, whereas mobile nodes have this ability, presumably using Mobile IPv6. If such a mobile node is indeed a MR with a number of nodes behind it, a *sub-MR* and its respective *sub-NEMO* is getting attached to a *root-NEMO* under a *root-MR*. In this case, the aggregated network is said to be *nested* and is referred to as a *nested-NEMO*.

NEMO Basic Support associates each egress interface of a mobile router with two distinct addresses, much like what is done in Mobile IPv6. The *home address* (HoA) serves as a permanent location invariant identifier whereas the *care-of address* (CoA) serves as a routing directive to the current point of attachment. The permanent HoA is obtained from the home network and has the same prefix as the home link. The temporary CoA is obtained in the visited network and formed from the prefix advertised on the visited link. MNNs behind the MR do not change their address as they do not change their physical point of attachment.

The purpose of the protocol is to establish bidirectional tunnels between the home link and the mobile network for each (HoA,CoA) pair. The MR does so by registering a binding between the MNP and the MR's CoA with a router on the home link called the Home Agent (HA). This mechanism allows nested NEMOs.

Since the concept of network mobility is relatively new to most of the readers, we suggest to read the requirements representing the consensus of the IETF community [Ern05] and the terminology defined by this working group [EL05]. The terms used in the present paper and introduced above are taken either from the NEMO terminology or from a more general terminology defined in [MK04].

2.3 AAA Mechanisms

To control access to their network, IP operators deploy an AAA infrastructure. AAA stands for Authentication, Authorization and Accounting. A basic AAA infrastructure is composed of three elements: an authentication method, an AAA protocol and an authentication protocol. The authentication protocol is used between the client's device (e.g. laptop, PDA) and the authentication agent located at the edge of the operator's network, whereas the AAA protocol is used between the authentication agent and a remote AAA server located in the access network. This AAA server contains users' profiles. The authentication method is ran between the client and the AAA server. Fig.1 presents the AAA architecture using PANA and Diameter EAP which are introduced below.

PANA PANA (Protocol for carrying Authentication Network Access) [FOP+05] is a new authentication protocol currently designed at the IETF in the PANA working group. It is link-layer agnostic and thus can be used over any access technologies (802.11, 802.16, xDSL, GPRS, 3G, etc). It permits clients to dynamically select ISPs. Any authentication method can be used as PANA carries the EAP (Extensible Authentication Protocol [ABV+04]) protocol, which is an authentication framework that supports many authentication mechanisms such as certificates or one-time passwords. The PANA protocol also introduces the *Enforcement Point* (EP), an equipment on which security policies are applied. This Enforcement Point can be configured by the authentication agent using SNMPv3 [EOB04]. The PANA protocol is used between the PANA client (PaC) and the PANA Authentication Agent (PAA) which relies on a AAA server to authenticates clients using the EAP protocol. The AAA protocol used between the PAA and the remote AAA server must be able to carry EAP packets.

Diameter Diameter is the next generation AAA protocol. It aims at replacing the well-known RADIUS protocol [RRSW00]. Diameter offers several advantages over RADIUS and is intended to provide an Authentication, Authorization & Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is composed of a Base protocol [CAG+03] extended by other mechanisms called *Diameter-applications*. Network access is an example of such a *Diameter-application*. Another *Diameter-application* is the Diameter EAP application [ETZ04] which can be used as the AAA protocol by the PAA.

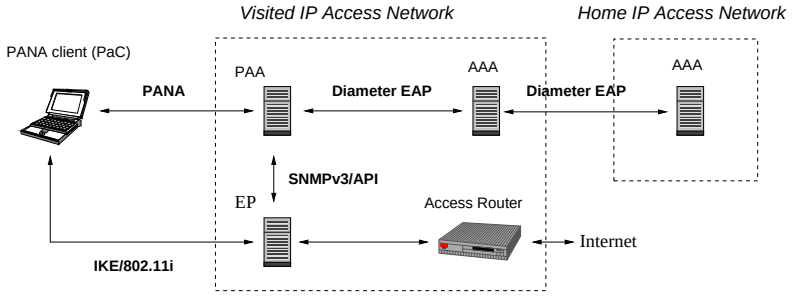

Fig. 1: Overview of AAA Mechanisms

3 Nested NEMO Case Study: PAN in a Bus

The analysis detailed in this paper is based on a nested-NEMO scenario as this configuration represents one of the most elaborated use case. It is elaborated in the sense that it introduces more complexity compared to other use cases, since we have two mobile networks, with one using the other one to access the Internet.

In our case study, we consider a PAN-like sub-NEMO located in a LAN-like root-NEMO deployed in a bus. The PAN (referred to as $NEMO_{pan}$) is a mobile network composed of several nodes ($MNNs_{pan}$, e.g. a mobile phone, a personal assistant, an MP3 player) and a mobile router (MR_{pan}). The ingress interface is a bluetooth link. The MR_{pan} and all $MNNs_{pan}$ communicate with one another through this bluetooth link. Only MR_{pan} can get a direct access to the Internet through its egress interfaces (e.g. 3G and 802.11). The bus (referred to as $NEMO_{bus}$) is an in-bus mobile network served by a mobile router (MR_{bus}) equipped with high bandwidth egress interfaces (e.g. 802.16) and an ingress link (802.11).

$NEMO_{bus}$ uses its egress interface to connect to access routers in the *Access Operator*'s (AO) infrastructure that provides Internet connectivity to the bus. $NEMO_{bus}$ in turn provides Internet access to passengers ($MNNs_{bus}$) which carry a $NEMO_{pan}$ through the 802.11 access link**. $NEMO_{bus}$ may offer some local services (e.g. video and audio on demand) and some global services (e.g. Internet connectivity) to its passengers. $MNNs_{pan}$ must be able to use local bus services and also global services, for example Internet services. This scenario is illustrated on Fig.2.

We refer to the *NEMO Operator* (NO) network as the network hosting the HA of $NEMO_{bus}$. MR_{bus} operates NEMO Basic Support to maintain connectivity to the Internet through its HA via the AO. MR_{pan} also operates NEMO Basic Support to maintain connectivity to the Internet to its own HA via $NEMO_{bus}$.

In our scenario, the in-bus network can offer Internet connectivity services as well as local services such as video or audio on demand, a local web site, network games, etc. These services may be free or not. Access to paid services must be restricted to the passengers who have paid the relevant fees.

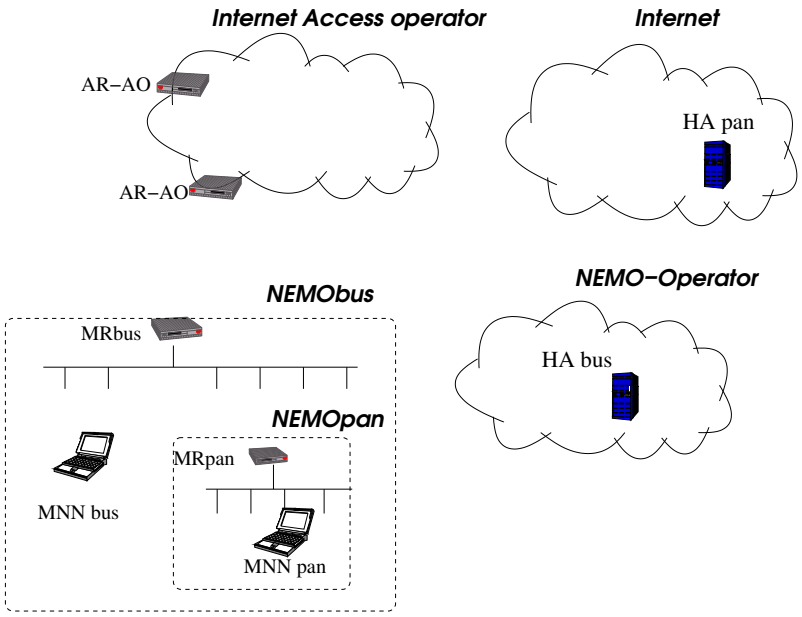

Fig. 2: Case Study Scenario: PAN in a Bus

4 Requirements

In this section, we are enumerating a number of requirements that must be met by an AAA architecture in a nested NEMO. These requirements are divided into requirements resulting from security threats, and requirements resulting from service needs.

** Note that according to the NEMO terminology defined in [EL05], MRs_{pan} are perceived as $MNNs_{bus}$ (i.e. VMN_{bus}) from the point of view of $NEMO_{bus}$

4.1 Security

Some studies have already been pursued to analyze threats introduced by NEMO Basic Support:

- [POJL04] describes various NEMO-specific threats. It divides the analysis between MR and HA signaling, forwarding information at HA and nested mobility configurations. It appears that the signaling message used between MR and HA could be used to launch attacks such as redirection of traffic. Moreover, the tunnel created between MR and HA to relay traffic from ingress network to the Internet should also be protected by AH. For this reason, use of IPsec AH [KA98a] and/or ESP [KA98b] is required to protect the communication flow.

- In [JZW+04], authors also try to determine possible attacks under the operation of NEMO Basic Support. They describe an attack called "Binding Update spoofed" by which an attacker could create false signaling packet (the *Binding Update*) in order to redirect traffic to a victim. However, the attack described is not feasible since the packet does not comply with the [ADD04] specification. Some of the others described threats are more specific to IP-in-IP encapsulation than to NEMO Basic Support.

- These two studies only deal with possible threats at the NEMO functional level whereas [NT02] deals with access control for NEMO deployment. In particular, it provides a high-level overview of the AAA architecture for various scenarios of deployment. However, it does not propose any specific solution. Such threats can be handled mainly by using access control mechanism and IPsec protocols.

Networking threats occurring in usual IP environments must also be considered when deploying NEMO Basic Support:

- **Eavesdropping** A malicious attacker could sniff every packet in a NEMO and steal a lot of data from the MNNs. To prevent such problems, messages need to be encrypted. Moreover, using node authentication and communication encryption at the same time prevent the network to be a target of replay attacks. Here, message authenticity and encryption are at the same time a NEMO and a user issue. It should not be possible to steal and replay the credentials of a MNN once this MNN is authenticated in the mobile network.

- **Spoofing** An attacker can use address spoofing to alter packets sent in the network. He can then decide to reset TCP sessions by forging fake TCP FIN packets or disrupt UDP transfers sending fake ICMP host unreachable or port messages. Under such attacks, the mobile network could be crashed if not protected. Another related problem is messages' integrity. Messages integrity can be corrupted if an attacker is able to change the contents of the packets exchanged between two entities in the mobile network. To avoid such threats, the message flows between all nodes involved in a NEMO (MNN, MR, AR, HA) should be authenticated.

As consequences of the threats identified in this section can be quite serious, security mechanisms must be deployed to secure the infrastructure. Encryption and data flow authentication are therefore required components of the NEMO infrastructure. IPsec deployment is described with the proposed AAA architecture in section 5.

4.2 Authentication and Authorization

Entities must be authenticated before they can be granted services in the NEMO infrastructure as well as in the AO's infrastructure. This is necessary for any kind of service as it would allow the service operator to apply access control and avoid any unauthorized use. Authentication of network services is also useful for the clients in order to be protected against any type of impersonation.

4.2.1 Authentication of Routers

Mobile routers are entities that can be owned by different actors. The MR embedded in the bus (MR_{bus}) is owned by the NO and aims at providing connectivity for passengers located in the bus ($MNNs_{bus}$). On the other hand, the mobile router in the PAN (MR_{pan}) is owned by an individual and used by other equipments

($MNNs_{pan}$) owned by the same individual to access the Internet. MR_{pan} would thus allow $MNNs_{pan}$ to benefit from the services offered by the NO including Internet connectivity provided by $NEMO_{bus}$ as well as the mobility service. Securing the mobile routers at every level is therefore vital for the safety of the entire nested NEMO.

When deploying nested MRs, we need to define security requirements, taking into account each use case and threats that could occur in each situation. When the MR is used by a mobile network to provide connectivity to its local nodes in a root-NEMO such as $NEMO_{bus}$, the MR must be authenticated beforehand by the AO's AAA system.

If the MRs belong to the same administrative domain as the AO, then, the MRs need to be registered in the AO's authentication back-end. Otherwise, if the MRs are not owned by the AO, the AO's authentication framework must contact the authentication servers of the institution where the MR is registered. The institution operating the MRs must have an agreement with the AO for this authentication to be successful.

When an MR owned by some individual is used to serve a $NEMO_{pan}$ to access NO services inside a root-NEMO, it becomes a sub-MR. The sub-MR needs to be authenticated by the root-NEMO as any MNN would be.

On the other hand, MNN_{bus} and MR_{pan} will use MR_{bus} as the default router. For this reason, they need means to trust this router. In particular, traffic from and to MR_{bus} should be authenticated. Similarly, MR_{bus} needs to trust the AR located in the fixed access network. ARs must thus be equipped with the necessary AAA materials to prove their identity.

4.2.2 Authentication of Nested MNNs

Under NEMO Basic Support, the traffic originating from the mobile network is always tunneled by the MR to its HA. The fact that the traffic actually comes from the ingress network is thus hidden by the MR. As a result, MR_{bus} can not differentiate traffic originated from or intended to a MR_{pan} or a MNN_{pan}. From a service point of view, this translates into $MNNs_{pan}$ using MR_{pan} as a point of attachment transparently to $NEMO_{bus}$. Indeed the PAA in $NEMO_{bus}$ can not authenticate $MNNs_{pan}$. It only sees IP traffic whose source IP address is the egress interface of the MR_{pan}, and thus can not detect $MNNs_{pan}$. $MNNs_{pan}$ may consume the bandwidth resource of $NEMO_{bus}$ although only a single host (MR_{pan}) is supposed to use the service. This side effect is a natural consequence of the characteristics and properties of the protocols involved in a nested NEMO scenario.

Three possibilities to authenticate a MNN_{pan} normally hidden by its MR_{pan} come to mind. The first is to modify the PANA protocol to allow MR_{pan} to authenticate both himself and its ingress network. This could be done if MR_{pan} provides its ingress prefix or addresses in use in its network. The second is for MR_{pan} to act as a sort of PANA relay between the PAA of $NEMO_{bus}$ and the MNN_{pan}. The third is for each MNN_{pan} to authenticate individually with the access network. This would imply that MNN_{pan} can directly contact the PAA located in MR_{bus}. The first solution is desirable since MNNs wouldn't be required to perform AAA mechanisms. The second would basically break the current AAA concept since credentials should not be shared with third parties. The third would not work for all NEMO configurations since in some cases MNNs are expected to be very simple nodes. Like for NEMO Basic Support, a generic solution must be able to meet the needs of MNNs without requiring them to support any additional mechanism.

4.2.3 Authorization for Services Offered in a NEMO

Inside a mobile network, authorization for using the services offered by $NEMO_{bus}$ must be granted only for users that the NO's authentication servers can authenticate. These users may belong to the NO or any other ISP which has an agreement with the NO. In order to process this authentication, the NO's MRs need enough local or remote resources. This authentication process must allow authentication of users if they are registered and grant them the use of the Internet connectivity service or other services if their credentials permit it.

At this point, we have to distinguish between the Internet connectivity service, and other local free and non-free services. Some user may not have paid for local non-free services, thus the local non-free services should no be available for this user. On the other hand, the free services should be available in any case.

We can conclude that we need to make a distinction between the services from an authorization point of view. The authorization for each type of service should also be independent from the others. To fulfill this requirement, the authentication system must have enough granularity in its actions.

4.2.4 Conclusion

Authorization for any kind of service must be granted after mutual authentication between the entity using the service and the entity providing the service, in order to avoid unauthorized users and ensure the identity of the service provider. The nested NEMO scheme does not require additional mechanisms than those required for mutual authentication between the MR and the MNNs in a root-NEMO. Sub-MRs are considered as usual MNNs in the root-NEMO and are authenticated the same way.

5 Proposed AAA Architecture

In this section, we propose an AAA architecture which allows the authentication of participating entities in a NEMO deployment scenario. This architecture permits to authenticate $NEMO_{bus}$ to the Internet Access Operator, and to authenticate MNN_{bus} and MR_{pan} in the $NEMO_{bus}$. Note that, currently, without any optimization, $MNNs_{pan}$ can not be authenticated. Our AAA architecture is a collection of processes and information distributed among the different entities, used in collaboration to fulfill the authentication and authorization requirements.

In addition to the requirements identified in earlier sections, we are targeting an AAA architecture that offers minimal resources consumption, scalability and automatic bootstrapping capability of the authentication process, as well as simplicity of deployment, management and use. Our AAA architecture detailed below is limited to authentication operations in a nested NEMO environment.

5.1 Design of the AAA Architecture

As mentioned in section 4, we need to authenticate users for local services as well as for Internet connectivity services. The local services should be available even if $NEMO_{bus}$ does not have connectivity. We could have separated authentication systems, one for local services and one for Internet connectivity services. However, this approach would require allocation of more resources in an embedded environment. The other disadvantage of separate authentication systems is that their maintenance and management costs will be more expensive. For this reason, the authentication for local services and the authentication for Internet connectivity services will be provided by the same system. Only one credential material (e.g. certificate, login and password) will be needed for each entity to authenticate itself and gain access to a specific set of services.

One part of the authentication framework is the authentication system that allows the AO's infrastructure to authenticate MRs. This authentication system will involve entities in the AO's infrastructure as well as entities in the NO's infrastructure.

5.2 Description of the AAA Architecture

Our design choices are illustrated using the case study described in section 3 but could apply to any nested NEMO scenario. Fig.3 shows the overall AAA architecture. Four networks are involved: $NEMO_{pan}$, $NEMO_{bus}$, the AO's network and the NO's network. Arrows show the use of authentication protocols (PANA and Diameter) between entities involved in the authentication process.

PANA is used between MR_{bus} and $MNNs_{bus}$ (i.e. between MR_{bus} and MR_{pan} or VMN_{bus}), as well as between Internet service routers (MR_{bus} and the AR in the AO's network). In the back-end of the authentication system, the Diameter EAP application of the Diameter base protocol is used in the communication between the service front-end entities and the back-end authentication servers. The Diameter EAP application is also used between the AO's AAA servers and the NEMO operator's AAA servers for inter-domain authentication of MR_{bus}. The AAA architecture is explained in details in the following paragraphs.

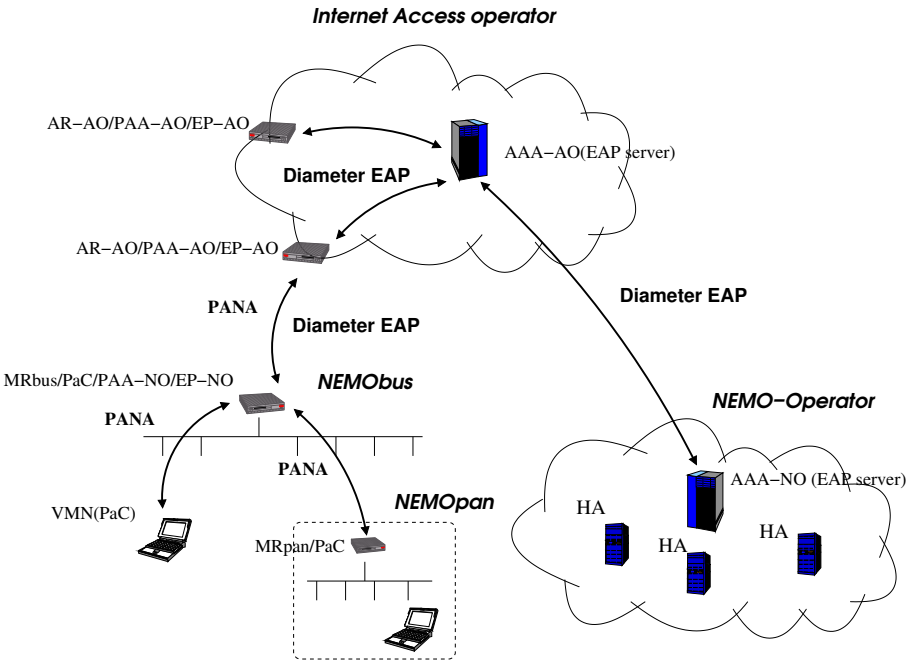

Fig. 3: Global AAA architecture in a nested NEMO

5.3 Authentication in NEMO

In this section we describe the authentication mechanisms used inside $NEMO_{bus}$ to authenticate its clients (MR_{pan} or MNN_{bus}) before they can access bus' services (as described in section 4.2.2, $NEMO_{bus}$ can not authenticate $MNNs_{pan}$). For the practical deployment of this authentication system, we suggest the use of PANA. The PANA Authentication Agents will authenticate the user and set the access rights accordingly in the Enforcement Points (EP). For simplicity, we assume here that MR_{bus}, PAA and EP functions are co-located. The use of PANA will permit to bootstrap IPsec between the PANA client and its access router thus providing a trust relationship between clients and the AR.

Services offered by a NEMO network may be free or not free. For accessing non free services such as Internet access, authentication must be performed. The requirements and assumptions for this authentication system were identified in section 4.2.3. During this authentication process, the AAA server can provide filtering rules to be applied at the Enforcement Point and thus it implicitly authorizes some services. The actual AAA architecture thus allows only static configuration for services.

5.3.1 AAA Architecture in the Access Network

To authenticate classic IP clients and mobile networks such as $NEMO_{bus}$, the Access Operator uses PANA and Diameter EAP. The PANA protocol is ran between IP clients (MR_{bus} in Fig.3) and an authentication agent (PAA-AO) which are located around the access router. The authentication agent (PAA-AO) contacts a remote AAA server (AAA-AO) to authenticate users. This AAA server is in fact an EAP server since PANA carries EAP packets. If users belong to another administrative domain, the AAA server will contact the corresponding AAA server. In our scenario, the Access Operator's AAA server can contact the NEMO Operator's AAA (AAA-NO) server to authenticate $NEMO_{bus}$.

Thus, from the Access Operator point of view, the mobile network is an IP client and it is assimilated to a PANA client (PaC) for the access network. It implies that the NEMO operator needs to have some agreements with the Access Operator.

The use of PANA in the access network allows us to bootstrap IPsec between $NEMO_{bus}$ and the AR of the Internet Access Operator. This results in a trust relationship between $NEMO_{bus}$and its AR.

Signaling messages			
MR_{bus}	$<->$	HA_{bus}	AH and ESP
MR_{pan}	$<->$	HA_{pan}	AH and ESP
Tunneling			
MR_{bus}	$<->$	HA_{bus}	AH
MR_{pan}	$<->$	HA_{pan}	AH
Data traffic			
MR_{bus}	$<->$	AR	AH
MR_{pan}	$<->$	MR_{bus}	AH
MNN_{bus}	$<->$	MR_{bus}	AH

Tab. 1: IPsec deployment

5.4 IPsec Usage in NEMO

In order to provide IP security in a deployed NEMO, IPsec should be used. We can divide IP traffic in three categories. For each category, we propose a specific IPsec usage :

1. **MR and HA signaling:** the signaling messages between MR and HA (*Binding Update* and *Binding Acknowledgment*) must be protected by using AH and ESP (cf. [POJL04]). This concerns signaling messages exchanged between MR_{bus} and HA_{bus} and also between MR_{pan} and HA_{pan}.

2. **MR and HA tunneling to relay traffic between IP clients and their correspondents:** this traffic should be at least protected by AH.

3. **Data traffic between IP client and Access Router:** this traffic concerned MR_{bus} to AR of the access operator but also traffic from MNN_{bus} or MR_{pan} to MR_{bus}. Use of AH will permit to the IP client to authenticate the access router. For this reason we recommend to use at least AH to protect this traffic, however security at the layer 2 may be sufficient. Note that the PANA protocol allows the bootstrapping of IPsec.

Tab.1 presents the necessary IPsec deployment in a NEMO infrastructure.

6 Open Issues and Future Work

In our future work, we will consider the open issues listed in the forthcoming paragraphs and we will try to extend the AAA architecture in order to fulfill all the AAA requirements.

Loss of connectivity The nature of mobile environments forces us to take into account the problem of IP connectivity outage. The bus may loose IP connectivity in situations when no access networks are reachable. If we rely on a remote AAA server, the authentication process would be interrupted during the loss of connectivity. The interruption of the authentication process would have no impact as long as the only service offered inside the bus is the Internet connectivity. On the other hand, if the bus offers local services as well, such as video and audio on demand, no authentication can be done during the loss of connectivity as long as the authentication of user inside the bus relies on a remote AAA service. To avoid total service outage during loss of connectivity to the Internet, the AAA framework must rely on local means. A simple solution is to put all the required AAA resources inside the bus.

Multiple logins and credential abuse We can not rely on a remote entity to detect multiple logins using the same credentials since a NEMO may loose its connectivity. As it is a problem for ISPs and their deployment of NEMO, the answer can be found according to different business models. In the $NEMO_{bus}$ scenario for example, a potential solution is to deliver credentials to clients on trip basis. They would be linked to the bus ticket and couldn't be used in another bus at the same time.

Dynamic service authorization The AAA architecture described in this paper can offer authorization services. The authorization data can be transported by the Diameter-EAP protocol. The protocol however does not define how, neither where to get the authorization data. This is left to the implementer and the operator's decision. Nevertheless, this AAA architecture does not provide dynamic authorization. It has a different scheme than the authorization capabilities provided by the proposed AAA architecture. When dynamic authorization is used, the client is authenticated at first. After that, when a request for a service is issued, the client's privileges are checked by the AAA architecture before the network decides to grant the service or not. The advantage of dynamic authorization is that changes on user's privileges can be identified. Moreover, this scheme allows a better separation between the authentication and the authorization processes.

Distinction between IP NEMO client and IP classic hosts The Access Operator might need to know if a client is a mobile network that may require more bandwidth than a single host. One possible approach is to use the full features of the AAA architecture to add more information about the clients and the services. This information should then allow the access operator to distinguish between the different categories of clients.

7 Conclusion

The protocol to manage the mobility of entire networks, i.e. NEMO Basic Support is surely a better approach than Mobile IPv6 because it allows to bring an unlimited number of usual IPv6 devices behind a mobile router and to manage the mobility of the entire network transparently to the nodes located in it. However, this challenges the existing AAA mechanisms used to authenticate and authorize users to access resources in foreign access networks, particularly when mobile networks become nested. We proposed a comprehensive AAA architecture adapted to nested-NEMO configurations which solve some issues and risks towards communication security. As demonstrated in this paper, the combination of NEMO Basic Support and AAA mechanisms causes new issues. Further work will be necessary to achieve an architecture that fulfill the requirements and thoroughly suppress threats specifically targeting NEMO networks.

Acknowledgments

This paper is the output of discussions between members of the Nautilus6 project[††], which spans several laboratories working on IPv6 mobility in both Japan and France.

References

[ABV+04] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). Technical report, IETF, June 2004.

[ADD04] Jari Arkko, Vijay Devaparalli, and Francis Dupont. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. Request For Comments 3776, IETF, June 2004.

[CAG+03] P. Calhoun, J. Arrko, E. Guttman, G. Zorn, and J. Loughney. Diameter Base Protocol. Technical report, IETF, September 2003.

[DWPT05] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. Network Mobility (NEMO) Basic Support Protocol. Request For Comments 3963, IETF, January 2005.

[EL05] Thierry Ernst and Hong-Yon Lach. Network Mobility Support Terminology. Internet Draft draft-ietf-nemo-terminology-03.txt, IETF, February 2005. Work in progress.

[EOB04] Y. El Mghazli, Y. Ohba, and J. Bournelle. PANA: SNMP usage for PAA-2-EP interface. Internet draft, IETF, October 2004. Work in progress.

[††] Nautilus6: http//www.nautilus6.org

[Ern05] Thierry Ernst. Network Mobility Support Requirements. Internet Draft draft-ietf-nemo-requirements-04.txt, IETF, February 2005. Work in progress.

[ETZ04] P. Eronen, T.Hiller, and G. Zorn. Diameter Extensible Authentication Protocol (EAP) Application. Internet draft, IETF, November 2004. Work in progress.

[EU02] Thierry Ernst and Keisuke Uehara. Connecting Automobiles to the Internet. In *ITST: 3rd International Workshop on ITS Telecommunications*, Seoul, South Korea, November 2002.

[FOP+05] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for Carrying Authentication for Network Access. Internet draft, IETF, January 2005. Work in progress.

[JPA04] David B. Johnson, C. Perkins, and Jari Arkko. Mobility Support in IPv6. Request For Comments 3775, IETF, June 2004.

[JZW+04] Souhwan Jung, Fan Zhao, S. Felix Wu, HyunGon Kim, and SungWon Sohn. Threat Analysis on NEMO Basic Operations. Internet Draft draft-jung-nemo-threat-analysis-02.txt, IETF, February 2004. Expired.

[KA98a] Stephen Kent and Randall Atkinson. IP Authentication Header. Request For Comments 2402, IETF, November 1998.

[KA98b] Stephen Kent and Randall Atkinson. IP Encapsulating Security Payload. Request For Comments 2406, IETF, November 1998.

[MK04] J. Manner and M. Kojo. Mobility Related Terminology. Request For Comments 3753, IETF, June 2004.

[NT02] Chan-Wah Ng and Takeshi Tanaka. Usage Scenario and Requirements for AAA in Network Mobility Support. Internet Draft draft-ng-nemo-aaa-use-00.txt, IETF, October 2002. Work in progress.

[POJL04] A. Petrescu, A. Olivereau, C. Jeanneteau, and H.-Y. Lach. Threats for Basic Network Mobility Support (NEMO threats). Internet Draft draft-petrescu-nemo-threats-01.txt, IETF, January 2004. Expired.

[RRSW00] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service. Technical report, IETF, June 2000.