A. Yegin
Samsung AIT

February 18, 2005

AAA Mobile IPv6 Application Framework
draft-yegin-mip6-aaa-fwk-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a framework for using AAA backend protocols (e.g., RADIUS, Diameter) between home agents and AAA servers for centralizing Mobile IPv6 service management. Implementation of this framework requires definition of a new AAA application on the aforementioned protocols.

Table of Contents

1. Introduction

AAA backend protocols, such as RADIUS [RFC2865] and Diameter [RFC3588], enable centralized management of authentication, authorization, and accounting (AAA) for a limited type of services (Mobile IPv4 [I-D.ietf-aaa-diameter-mobileip], network access [I-D.ietf-aaa-diameter-nasreq], SIP [I-D.ietf-aaa-diameter-sip-app]). Currently there is no standard mechanism to centralize AAA for Mobile IPv6 [RFC3775]" services.

The current Mobile IPv6 protocol design assumes pre-established static configuration between a mobile node (MN, the client) and a home agent (HA, the server) for authentication and authorization of the mobility service. Although there are no standard protocols to retrieve accounting information from a HA yet, SNMP will be useful in the near future with the development of Mobile IPv6 MIBs [I-D.ietf-mip6-mipv6-mib].

The distributed AAA management model could be sufficient in the presence of one static HA per MN, but this is not always the case. In the presence of multiple HAs on a home subnet, reliance on pre-configuration increases the network management overhead. Additionally, there may be more than one home subnet that can be used by a mobile node, in which case the number of possible HAs is further increased. A central AAA infrastructure that is in charge of authentication, authorization, and accounting for the Mobile IPv6 service between any MN and any HA in a domain would benefit deployments by preventing AAA information replication and management across the domain.

Furthermore, at times Mobile IPv6 service may have to cross operator domain boundaries. For example, an (serving) operator may wish to provide Mobile IPv6 service to another operator's customers for whom it does not have any per-MN configuration in its local servers. A scalable and secure Mobile IPv6 roaming service [I-D.ietf-mip6-bootstrap-ps] cannot be made possible by solely relying on the HA pre-configuration. The MN can only be authenticated and authorized by an entity in its home operator ÇÖs domain. The serving HA has to get in touch with the local AAA infrastructure, which in turn must contact the AAA infrastructure of the home operator. Upon successful authorization and delivery of the service, associated accounting information can be delivered from the serving operator to the home operator.

This document describes AAA Mobile IPv6 application framework that enables AAA centralization and roaming for Mobile IPv6 services. There is more than one way to use AAA technologies with Mobile IPv6. The reader should note that the framework advocated in this document

constitutes only a subset of those possibilities. See Section 5 for more on this subject.

2. Framework

The following figure depicts the interaction among various entities using AAA for Mobile IPv6.

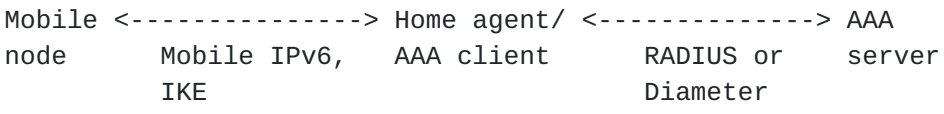

Figure 1: MIP6-AAA framework

In this framework, Mobile IPv6 protocol is executed between the MN and the HA, as it normally would. Unlike a HA that relies on the preconfigured information, the AAA-enabled HA (more precisely: AAA client on HA) communicates with a AAA server in order to authenticate and authorize the MN before starting the Mobile IPv6 service, and later for making the accounting information available.

The current Mobile IPv6 design relies on use of IPsec for authentication of protocol signaling between the MN and the HA. The associated IPsec SA is created by running IKE [RFC3776] between the two. The initial authentication and authorization of MN and HA should be performed during the IKE execution. This is where HA must consult the AAA infrastructure. The authorization at this stage is for establishing an IPsec SA for Mobile IPv6 service. Authorization parameters (e.g., max allowed lifetime) for the subsequent Mobile IPv6 binding updates may also be delivered to the HA at this stage.

Upon successful IPsec SA establishment for Mobile IPv6 service, MN can send binding updates to the HA. By the help of IPsec SA, the HA can authenticate the MN without AAA server ÇÖs help. Furthermore, the HA can also authorize the binding update if it already has the authorization parameters from its earlier interaction with the AAA server. Otherwise, the HA must contact the AAA server again to perform binding update authorization.

Figure 2 is an illustration of a Mobile IPv6 session that starts with IPsec SA establishment and includes one initial and one refreshing binding updates.

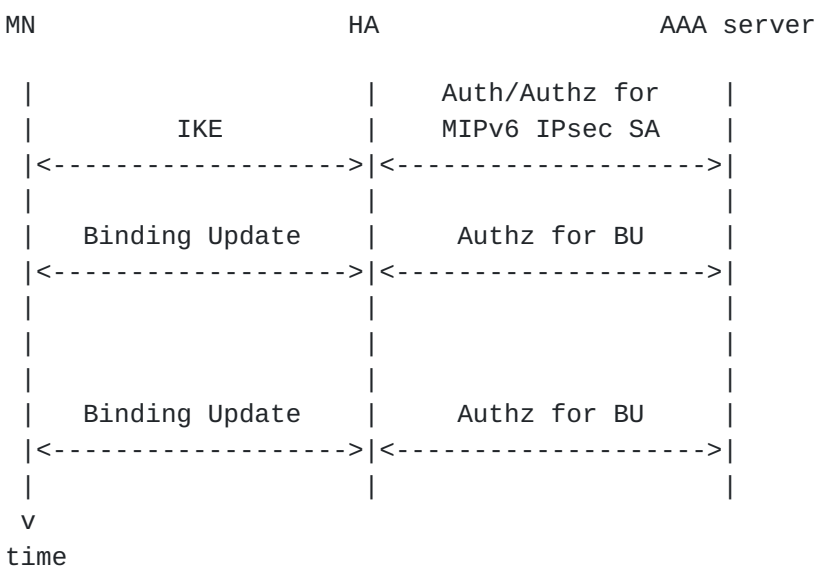

Figure 2: Message flow

Accounting-oriented HA-AAA interaction can take place any time MN is authorized for the service, and it can be piggybacked with the authentication/authorization messaging.

This framework is built upon following trust model.

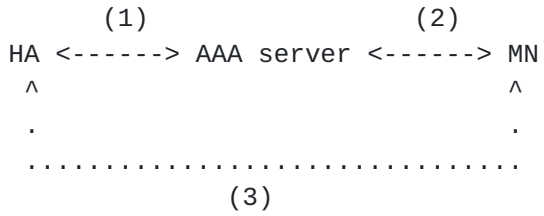

Figure 3: Trust model

It is assumed that HA-AAA (1) and MN-AAA (2) trust relations are pre-configured. HA-AAA may have an indirect trust relation, that spans multiple intermediate server and operator domains. MN-HA (3) trust relation is dynamically created as a result of the AAA interaction. MN can create trust relations with several HAs. These trust relations should not outlive neither the MN-AAA nor the HA-AAA trust relations.

An instance of this framework that relies on EAP-based authentication is depicted in Figure 4.

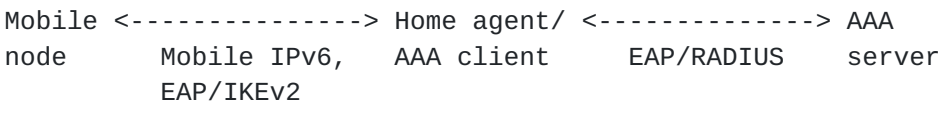

Figure 4: EAP-based IKE authentication

EAP [RFC3748] can provide end-to-end authentication between the MN and AAA server. It can be used for IPsec SA authentication and authorization by being transported on IKEv2 between the MN and HA, and by a AAA-backend protocol between the HA and AAA. EAP framework enables authentication between the peer (MN) and authentication server (AAA server) via an authenticator (HA), and produces a security association between the peer and the authenticator as a result. While the produced security association is not an IPsec SA, it can be used in building one. EAP is not used with Mobile IPv6 binding update authentication and authorization.

This framework can also be used with scenarios where other authentication methods (non-EAP-based) are used with IKE. Furthermore, future extensions to Mobile IPv6 specification may involve IPsec/IKEless operation [I-D.ietf-mip6-auth-protocol]. They should readily fit this framework as well.

[TBD: Consider using AAA with the CN as well. Now that alternatives to RR-based BU security are being considered, and MN-CN pre-shared key concept is around, leveraging AAA may come into the picture.]

3. New AAA Application

The architectural differences between Mobile IPv4 and Mobile IPv6 necessitate different AAA application framework for each.

Mobile IPv4 involves an intermediate server between the MN and the HA, namely foreign agent (FA) which can be co-located with a network access server (NAS). This impacts the end-to-end AAA flow.

The signaling authentication is built-in with the Mobile IPv4 protocol, whereas an additional protocol (IPsec) is used for Mobile IPv6. Use of IPsec requires yet another protocol (IKE) for session establishment. This nature of Mobile IPv6 leads to additional authentication and authorization exchanges between the HA and AAA server. The triggering event dictates the nature of exchange (e.g., for authentication and authorization of a Mobile IP IPsec SA creation, vs. authorization of a Mobile IPv6 binding update). In Mobile IPv4, a single interaction between the serving agent (FA or HA) and the AAA server is sufficient to accomplish authentication and authorization of a registration request (equivalent of a Mobile IPv6 binding update).

The new AAA application is required to associate a given authorization and accounting to the Mobile IPv6 service. When a AAA client contacts a AAA server, it should be able to convey that the request is for Mobile IPv6 service, as opposed to any other services (network access, SIP, etc.). Additionally, service authorization should take into account parameters like home address and binding lifetime, which are specific to a Mobile IPv6 service. Finally, accounting should support Mobile IPv6-specific MIBs [I-D.ietf-mip6-mipv6-mib].

3.1 Requirements

It is assumed that the AAA client to server interface will be a new AAA application on RADIUS and Diameter protocols. The following requirements capture specific needs of this application in addition to what is already available in the base AAA protocols.

In a typical deployment, the same node will implement both the Mobile IPv6 Home Agent and AAA client functionalities. The interface discussed in this document is the one between the AAA client and the AAA server. The interface between the HA and the AAA client is outside the scope of this document. Although it is abbreviated as HA interfacing with the AAA server, in fact there is a AAA client between the two.

The interface MUST be able to identify the service as "Mobile IPv6".

This is necessary in order to differentiate the sought/authorized service from others, such as network access, SIP, Mobile IPv4, etc. [a].

The interface MUST serve authentication, authorization, and accounting purposes [b].

The interface MUST perform authentication and authorization of MN and HA for building an IPsec SA for Mobile IPv6 service. EAP/IKEv2 is used for this step [c]. The interface MUST be able to carry EAP between the HA and the AAA server [d]. This step produces a shared secret between the MN and HA. The secret key is generated on the MN by the EAP protocol and method. On the other hand, the same secret key is generated by the AAA server and MUST be delivered to the HA via this new interface [e]. This step MAY also deliver Mobile IPv6 authorization parameters to the HA (e.g., maximum allowed lifetime) [f].

The interface MUST perform authorization of MN for creating or updating a binding cache entry on the HA for EAP/IKEv2-based deployments [g]. This step MUST take place within the lifetime of the IPsec SA produced in the previous step [h]. The interface does not deal with the authentication of the MN as this is already taken care of by the IPsec processing on the HA. The interface MUST allow the content of the Binding Update communicated from the HA to the AAA server [i]. The AAA server needs the Binding Update values in order to make an authorization decision. The authorization result returned by the AAA server MUST include the authorized lifetime and an error code if the update request is rejected [j]. The authorized lifetime cannot exceed the IPsec SA lifetime.

The interface MUST perform authentication and authorization of the MN for creating or updating a binding cache entry on the HA for IPsec/IKEless deployments [I-D.ietf-mip6-auth-protocol] [k]. There is no IPsec SA building step in these deployments. The interface MUST support delivery of Binding Update values from the HA to the AAA server, and the authorization decision along with the lifetime and error codes (if available) in return [l]. The authorized lifetime cannot exceed the MN-AAA security association lifetime. The AAA server MAY also assign a home address for the MN and deliver its value via this interface [m].

The AAA server MUST be able to learn the Mobile IPv6 accounting information maintained by the HA [n]. The accounting information includes the counts of BUs, HoTIs, HoTs, forward and reverse tunneled IP packets for a given MN.

4. Relation to Mobile IPv6 Bootstrapping

Mobile IPv6 bootstrapping mechanisms [I-D.ietf-mip6-bootstrap-ps] are potentially useful for providing three pieces of information to a MN: HA address or home subnet prefix, home address, and a security association between the MN and HA. The security association does not have to be an IPsec SA, but something that helps creation of an IPsec SA eventually.

Use of this framework assumes the MN already knows the HA address. Hence an implementation of this framework cannot help with HA discovery.

The security association between MN and HA can be created by using the HA-AAA interface (see EAP-based example).

Home address can be obtained before or after running the AAA protocol. For example, the home address may be known by the MN by the time it engages in IKE or Mobile IPv6 with the HA, or it may be dynamically assigned by the HA or the AAA server. An implementation of the framework should work with any of these options.

Overall, this framework can be used as part of a Mobile IPv6 bootstrapping operation, but not necessarily as a complete solution to that problem.

5. Other Ways to Talk About Mobile IPv6 and AAA

Talking about AAA does not make sense without specifying the associated service. There is a difference between AAA for network access and AAA for Mobile IPv6 services [8]. This distinction may be blurry in certain cases (e.g., when Mobile IPv4 authentication is used for network access as well), but otherwise they are at least logically separate services.

There are several ways to mix the keywords Ç£Mobile IPv6 Ç¥ with Ç£AAA Ç¥ in addition the one described in this document. They are listed here for the sake of identification, but not necessarily for advocating them.

(a) Using network access AAA to deliver Mobile IPv6 bootstrapping information directly to a node (MN)
[I-D.giaretta-mip6-authorization-eap]
[I-D.le-aaa-mipv6-requirements]
[I-D.ohnishi-mip6-aaa-problem-statement].

(b) Using network access AAA to deliver Mobile IPv6 bootstrapping information to the network access server (NAS)
[I-D.chowdhury-mip6-bootstrap-radius]. It is assumed that the information is delivered from NAS to the MN via some additional protocol [I-D.jang-dhc-haopt]

(c) Piggybacking Mobile IPv6 signaling with network access AAA
[I-D.le-aaa-mipv6-requirements] This approach assumes that the AAA servers for network access and Mobile IPv6 services are the same.

6. Security Considerations

The framework defined in this document is aligned with the AAA backend protocols and the existing AAA applications. Therefore there are no new security considerations stemming from the general framework.

Details of the authorization are Mobile IPv6 specific. Exact parameters, their semantics and processing details must be described in an implementation of this framework.

7. Acknowledgements

Thanks to Kent Leung and Alpesh Patel for useful feedback.

8. References

8.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2 Informative References

[I-D.chowdhury-mip6-bootstrap-radius]
Chowdhury, K. and A. Lior, "RADIUS Attributes for Mobile IPv6 bootstrapping", draft-chowdhury-mip6-bootstrap-radius-01 (work in progress), November 2004.

[I-D.giaretta-mip6-authorization-eap]
Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

[I-D.ietf-aaa-diameter-mobileip]
Calhoun, P., Johansson, T., Perkins, C. and T. Hiller, "Diameter Mobile IPv4 Application", draft-ietf-aaa-diameter-mobileip-20 (work in progress), August 2004.

[I-D.ietf-aaa-diameter-nasreq]
Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-17 (work in progress), July 2004.

[I-D.ietf-aaa-diameter-sip-app]
Garcia-Martin, M., "Diameter Session Initiation Protocol (SIP) Application", draft-ietf-aaa-diameter-sip-app-06 (work in progress), February 2005.

[I-D.ietf-mip6-auth-protocol]
Leung, K., "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-04 (work in progress), February 2005.

[I-D.ietf-mip6-bootstrap-ps]
Patel, A., "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-01 (work in progress), October 2004.

[I-D.ietf-mip6-mipv6-mib]

Keeni, G., Nagami, K., Koide, K. and S. Gundavelli, "Mobile IPv6 Management Information Base", draft-ietf-mip6-mipv6-mib-06 (work in progress), January 2005.

[I-D.jang-dhc-haopt] Yegin, A., "DHCP Option for Home Agent Discovery in MIPv6", draft-jang-dhc-haopt-00 (work in progress), June 2004.

[I-D.le-aaa-mipv6-requirements] Faccin, S., "Mobile IPv6 Authentication, Authorization, and Accounting Requirements", draft-le-aaa-mipv6-requirements-03 (work in progress), February 2004.

[I-D.ohnishi-mip6-aaa-problem-statement] Ohnishi, H., "Mobile IPv6 AAA Problem Statement", draft-ohnishi-mip6-aaa-problem-statement-00 (work in progress), February 2004.

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC3775] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3776] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

Author's Address

Alper E. Yegin
Samsung Advanced Institute of Technology
75 West Plumeria Drive
San Jose, CA 95134
USA

Phone: +1 408 544 5656
EMail: alper.yegin@samsung.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.