Network Working Group
Internet-Draft
Expires: August 13, 2005

G. Giaretta
TILab
R. Lopez
Univ. of Murcia
Y. Ohba (Ed.)
TARI
S. Thomson
Cisco
H. Tschofenig
Siemens

February 12, 2005

Usage Scenarios and Requirements for Multi-hop EAP Lower Layer draft-ohba-multihop-eap-00

Status of this Memo

Copyright Notice

Abstract

All EAP lower layers that have been defined for network access authentication have the requirement that an EAP peer and an EAP authenticator are in the same IP subnet. This draft describes some scenarios where relaxing this requirement so that the EAP peer and the EAP authenticator are multiple IP hops away from each other could be useful or necessary. The draft also extracts a set of requirements for the design of such a multi-hop EAP lower layer based on the scenarios.

Table of Contents

1. Introduction

The Extensible Authentication Protocol (EAP) [RFC3748] was designed to enable extensible authentication for network access in situations in which the IP protocol is not available. Originally developed for use with PPP [RFC1661], it has also been applied to IEEE 802 wireless networks [IEEE8021X]. Moreover, PANA [I-D.ietf-pana-pana] defines a new EAP lower layer that uses IP between the protocol end points; with PANA, therefore, EAP authentication framework can also be used on any link that can carry IP.

All EAP lower layers defined for network access authentication so far have the requirement that an EAP peer and an EAP authenticator are in the same IP subnet: this is obvious for layer-2 EAP lower layers (e.g. IEEE802.1X), but it is the case also of PANA, which explicitly requires that the PaC (PANA Client) and the PAA (PANA Authentication Agent) are one IP hop away.

However, recently there has been some interest to relax this requirement and to design an EAP lower layer in order to enable new scenarios and applications where EAP framework can be used. These scenarios are quite different from each others: some of them are still related to network access authentication, whereas others imply that EAP is used as the authentication protocol for a purpose different from the network access (e.g. for bootstrapping a service). On the other hand, all those scenarios are identified with a specific EAP lower layer functionality to carry EAP messages between the EAP peer and the EAP authenticator over multiple IP hops. An EAP lower layer that has such a functionality is referred to as a "multi-hop EAP lower layer".

The purpose of this draft is to describe some scenarios where a multi-hop EAP lower layer could be useful or necessary and, based on them, to list a set of requirements for the design of such a multi-hop EAP lower layer.

2. Multi-hop EAP Scenarios

2.1 Network access control protocol

The Network Access Control Protocol (NACP) [I-D.thomson-nacp] has been designed to carry EAP payloads [RFC3748] over a UDP transport between a peer and authenticator for the purposes of enforcing access control at a particular device in the network.

To date, NACP has been targeted at enterprise deployment scenarios, where it cannot be assumed that the peer and authenticator are one L3 hop way from each other. While first hop deployment scenarios may be common and may need to be optimized for, the protocol must be flexible enough to accommodate deployments where the peer and authenticator are more than one hop away from one another. Examples of multi-hop deployment scenarios include the following:

1. Network access control may be enforced at the boundaries between network domains e.g. at the border between a less trusted/ managed branch office and main campus, at the border between main campus and gateway to the Internet, at the border between extranet and intranet, and on access to protected servers in a data center.

2. While first hop deployments may be highly desirable, it may not be possible in all cases. The first-hop router may not support authenticator functionality e.g. in SOHO deployment scenarios, or there may be a transition period in a customer deployment before all first-hop devices have been upgraded to support the new functionality.

3. There may be multiple authenticators in a network, each responsible for making different kinds of checks on a host and potentially making different authorization decisions. An authenticator may be present at the first L3 hop to enforce a minimal level of compliance with security policy, while another authenticator at a different point in the network may be responsible for enforcing a stricter level of compliance where more restrictive access is needed.

PANA [I-D.ietf-pana-pana] is a protocol that also encapsulates EAP over a UDP transport. One of the remaining differences in requirements between NACP and PANA is the need to allow for multi-hop operation. In particular, PANA enforces single hop operation by requiring that the TTL field in the IP packet be set appropriately. Such a requirement would need to be relaxed to support multi-hop scenarios.

2.2 Media-independent pre-authentication

Media-independent Pre-Authentication (MPA) is a mobile-assisted, secure mobility optimization scheme that works over any link-layer and with any mobility management protocol and supports not only inter-subnet handovers but also and inter-administrative-domain handovers [MPA]. With MPA, a mobile node is not only able to securely obtain an IP address and other configuration parameters from a candidate target network where the mobile may move in the near future, but also able to send and receive IP packets using the obtained IP address and other configuration parameters through its currently attached network before it attaches to the candidate target network. This makes it possible for the mobile node to complete the binding update of any mobility management protocol and use the new care-of address before performing a handover at link-layer.

It is essential for MPA in terms of security that authentication is taken place between the mobile node in the current network and the candidate target network, before the mobile node obtains an IP address and other configuration parameters from the candidate target network. In MPA, the authentication is performed between the mobile node and an authentication agent in the candidate target network using an authentication protocol. The authentication protocol MUST be able to derive a key between the mobile node and the authentication agent and SHOULD be able to provide mutual authentication. The authentication protocol SHOULD be able to interact with a AAA protocol such as RADIUS and Diameter to carry authentication credentials to an appropriate authentication server in the AAA infrastructure. An authentication protocol that carries EAP naturally would satisfy those requirements. On the other hand, such an EAP-capable authentication protocol MUST work over IP layer and over multiple IP hops, since the candidate target network is different from the current network of the mobile node.

IKEv2 [I-D.ietf-ipsec-ikev2] is able to carry EAP and work over multiple IP hops. On the other hand, using IKEv2 as the authentication protocol for MPA might be a burden for the following reason. Since IKEv2 requires Diffie-Hellman key exchange, the mobile node would need to perform Diffie-Hellman key exchange with each of the candidate target networks even if it does not finally make a decision to move to the candidate target networks.

PANA [I-D.ietf-pana-pana] is another existing protocol that carries EAP and works over IP layer, but the PANA protocol needs to be extended to work over multiple IP hops. On the other hand, considering that PANA does not require Diffie-Hellman key exchange (this is the case when an EAP authentication method which does not use Diffie-Hellman to derive an EAP Master Session Key), it might be

worth considering some extension of the PANA protocol to work over multiple IP hops for MPA than using IKEv2.

2.3 MIPv6 bootstrapping by running PANA

The MIPv6 bootstrapping problem as described in [I-D.ietf-mip6-bootstrap-ps] involves bootstrapping of the following parameters:

- MN finding HA's address
- MN obtaining HoA
- Setting an IPsec security association (SA) between the MN and the HA

Recently the MIP6 working group has expressed a fair amount of interest in developing another Mobile Node <--> Home Agent Binding Update security solution. The currently proposed solution [I-D.ietf-mip6-auth-protocol] (referred as MIP6-Auth-Protocol) heavily focuses on one specific authentication and key exchange protocol. This protocol requires that the entire message exchange is finished in a single roundtrip with the mobile node initiating the exchange. Obviously, this approach suffers from some limitations. This document investigates the usage of an Extensible Authentication Protocol (EAP) [RFC3748] based approach which offers more flexibility. As in other areas there is the 'one size does not fit all' problem.

With these recent developments in the MIP6 working group with a possible usage of the bootstrapping protocol for authentication and security association establishment it seems to be resonable to modify the goal of the MIPv6 bootstrapping in the sense that a security association has to be established between the mobile node and the home agent for protection of the MN <--> HA Binding Update to enable the usage of [I-D.ietf-mip6-auth-protocol] in addition to the establishment of IPsec SAs.

2.3.1 Relaxing PANA Assumptions

PANA was designed with a focus on network access authentication. This fact is reflected in the discovery mechanism whereby a link-local multicast address is used [I-D.ietf-pana-pana]. It is assumed that the PAA is only one IP hop away from the PaC. This assumption is based on today's network access protocols and the observation that in many networks the administrative boundaries can be draw between the end host and the access network.

This assumption is not applicable to this environment. The PaC might address the PAA directly via a unicast message over multiple IP hops or a new discovery message needs to be added. In the former case the PAA would be co-located with the home agent. From a protocol design point of view it seems to be reasonable to communicate only between nodes that are effected in the protocol rather than arbitrary nodes and thereby imposing artifical deployment constraints.

2.3.2 Bootstrapping Issues

We assume that the MN will act as a PaC and some agent in the network will act as the PAA, most likely the home agent itself. After mutual authentication, a security association will be established between PaC and the HA, which is comparable to an enforcement point (EP). Note, the PAA and the EP may be co-located as well.

2.3.2.1 Home Agent Discovery

Finding the address of the HA will be regarded as out of scope of this document. The MN could learn about the HA either by manual configuration, DNS or some other mechanism (such as the MIPv6 anycast mechanism). Even a discovery mechanism using a Router Alert Option alike mechanisms, which is added to PANA, might be possible. This aspect is for further investigation.

2.3.2.2 Obtaining HoA

The payload of any PANA message consists of zero or more Attribute Value Pairs (AVP). [I-D.ietf-pana-pana] describes a number of AVPs for different purposes. This draft proposes a new AVP for carrying the HoA of the MN.

HoA AVP: Contains the MIPv6 home address of the mobile node that wishes to setup a security association with the corresponding home agent. The HoA AVP is integrity protected by PANA and either randomly selected or selected based on user authentication.

To deal with UDP encapsulation in case of NAT traversal or even with IPv4/IPv6 transition the same procedure as suggested with an extension for IKEv1 [RFC3947] and in IKEv2 [I-D.ietf-ipsec-ikev2] can be applied. Support for this functionality requires the introduction of a new AVP in PANA. In context of IPv4/IPv6 transition scenario this proposal provides an alternative solution for a tunnel broker (see also [I-D.blanchet-v6ops-tunnelbroker-tsp] for a different approach using SASL).

2.3.2.3 MN-HA security association

As motivated in [I-D.ietf-mip6-bootstrap-ps] a security association

is required for subsequent protection of Mobile IPv6 Binding Update messages sent between the MN and the HA. We refer to this security association as the MIPv6 SA. Since the details of the MIPv6-Auth-Protocol [I-D.ietf-mip6-auth-protocol] are subject to change we assume that the following parameters have to be established as part of the bootstrapping procedure:

- Security Parameter Index (SPI) - possibly for both directions
- Replay Protection Parameter (such as a timestamp or a sequence number)
- Algorithms (if a negotiation procedure is desired)

Finally, a session key needs to be derived. Since a PANA SA needs to be established based on the EAP method provided session key it is also useful to apply the same procedure for deriving a session key for the MIPv6 SA. The PANA protocol [I-D.ietf-pana-pana] describes the session key derivation for the PANA SA.

It might be worth noting that the PANA protocol also allows rekeying of the security association (both the PANA SA and the MIPv6 SA). The PANA protocol discusses this aspect in the context of re-authentication.

The lifetime of the MIPv6 SA can either be negotiated or indicated by the MN's home network. As another alternative the periodic retransmission of "refresh" messages is benefial to deal with NATs, stateful packet filtering firewalls and orphan state at the HA. PANA provides such a refresh message as described in Section 4.5 of [I-D.ietf-pana-pana]. Furthermore, a Session-Lifetime AVP is offered by PANA as described in Section 4.10 of [I-D.ietf-pana-pana].

Since PANA is an extensible protocol it is possible to use a single protocol for bootstrapping IPsec SAs (as described in [I-D.ietf-pana-ipsec]) and a security association for [I-D.ietf-mip6-auth-protocol].

2.4 Service Authorization and Bootstrapping

EAP [RFC3748] was designed and used so far for network access authentication and authorization. With IEEE 802.1X and IEEE 802.11i EAP and the corresponding EAP methods are used to "bootstrap" keying material for link layer security. In IKEv2, EAP is used although the EAP method provided keying material is not feed into the generation of keying material for IPsec SA establishment. The Diffie Hellman keying material is used instead. Using PANA the MSK/AAA-Key provided

by EAP methods is used to derive keying material that might be used for bootstrapping link layer or even network layer security associations.

Due to several advantages brought by EAP framework, in a similar way it could be advantageous to use EAP for service authorization and bootstrapping. Actually several services need to be bootstrapped setting up a security association between the node providing the service and the node using it. For example, see [I-D.ietf-mip6-bootstrap-ps] for the problem statement for Mobile IPv6 bootstrapping. Unfortunately, since the involved entities (i.e. bootstrapping and bootstrapped nodes) are usually more than one IP hop away, using EAP for authorization and bootstrapping purposes implies that EAP packets must be carried in a multi-hop environment.

A possible approach could be the usage of IKEv2 since, as mentioned before, it already supports EAP authentication; nonetheless IKEv2 only creates IPsec SAs since the concept of Domain of Interpretations (DoIs) was removed due to the limited usage in IKEv1. An alternative approach is the usage of PANA which has been designed with extensibility in mind. There is, however, the need to relax the requirement that the PaC and the PAA must be one IP hop away, as suggested in [I-D.tschofenig-mip6-bootstrapping-pana]. This was mainly motivated by the usage of network access authentication protocol found today.

This section briefly describes a framework for service authorization and bootstrapping that would be advantageous as soon as a multi-hop EAP lower layer is designed. Figure 1 depicts the framework architecture; the nodes involved are:

- the bootstrapped node (BN) which is the node triggering the service bootstrapping;
- the Service Provider Node (SPN) which is the node providing the service (e.g. the Home Agent in Mobile IPv6). This node acts as an EAP authenticator and it may handle the authentication locally or it may act as a pass-through to a backend authentication server;
- the backend authentication server (AAA server in Figure 1) which verifies the BN's credentials and authorizes the user for a particular service.

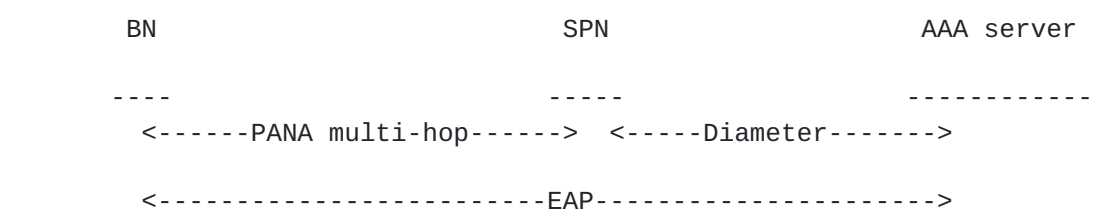

Figure 1: Service Authorization and Bootstrapping through EAP

If a backend authentication server is needed, the bootstrapping procedure consists of two phases:

- Discovery Phase: the BN discovers through an out-of-band mechanism (e.g. pre-configuration, DNS, anycast addresses) a SPN for the particular service it wants to activate;

- Authorization and Configuration Phase: during this phase an EAP exchange occurs between the BN and the AAA server, the SPN acting as a pass-through EAP authenticator. This exchange is needed to verify the credentials of the BN in order to authorize the service. Moreover during this phase, depending on the service configuration peculiarities, an exchange of configuration and authorization parameters between the BN and the AAA server or the SPN could be necessary: this can be accomplished through EAP lower layers and AAA protocol AVPs (e.g. PANA and Diameter AVPs).

- The approach depicted in Figure 1 could be generalized as shown in Figure 2 in order to bootstrap several services through a single EAP exchange. For this purposes a new node, the Service Authorization Anchor Point (SAAP) has been introduced. The BN starts an EAP exchange with the SAAP and asks for a set of services; the SAAP may act as a pass-through EAP authenticator or it may locally authenticate and authorize the users. Finally the SAAP gets in touch with the involved SPNs and sends them the authorization result and the necessary configuration parameters.

As shown in Figure 2, PANA can be used as a protocol for interacting with a that allows bootstrapping of credentials. One example of such credentials that can be dynamically created based on an EAP authentication and authorization protocol run was shown in [I-D.tschofenig-pana-bootstrap-kerberos]. Kerberos [RFC1510] is a well-known security protocol which provides authentication, authorization and key distribution. It is used to secure a number of protocols. By combining the flexibility of the EAP framework with the wide deployment of Kerberos in universitites and corporate networks it is possible to bootstrap a Kerberos Ticket Granting Ticket. This Kerberos Ticket Granting Ticket can then be used to retrieve service tickets for usage with a variety of protocols. This

approach of bootstrapping Kerberos ticket with the help of an EAP protocol interaction is described in [I-D.tschofenig-pana-bootstrap-kerberos].

Another approach to combine EAP and Kerberos is to integrate an EAP-based pre-authentication mechanism into Kerberos. However, using a generic protocol for bootstrapping credentials can also be used for bootstrapping symmetric keys for usage Mobile IP (as discussed as part of the MIPv6 bootstrapping work [I-D.ietf-mip6-bootstrap-ps]) or also to bootstrap public/private keys. Therefore, it would be necessary to confidentiality protect the delivery of an ephemeral public and private key pair to the end host. This key pair would have a short lifetime, possibly without the need for revocation mechanisms, and could be used in all security protocols utilizing public key based mechanisms (including IKEv2 or TLS). A big advantage is the avoided public key infrastructure since authentication protocols based on symmetric cryptography can still be used within EAP.

As part of the bootstrapping activity it might be necessary to exchange parameters and authorization information between the Bootstrapped Node and the Service Authorization Anchor Point (SAAP) for later communication between the Bootstrapped Node and a Service Provider Node. This information might again require confidentiality protection as, for example, illustrated in [I-D.tschofenig-enroll-bootstrapping-saml].

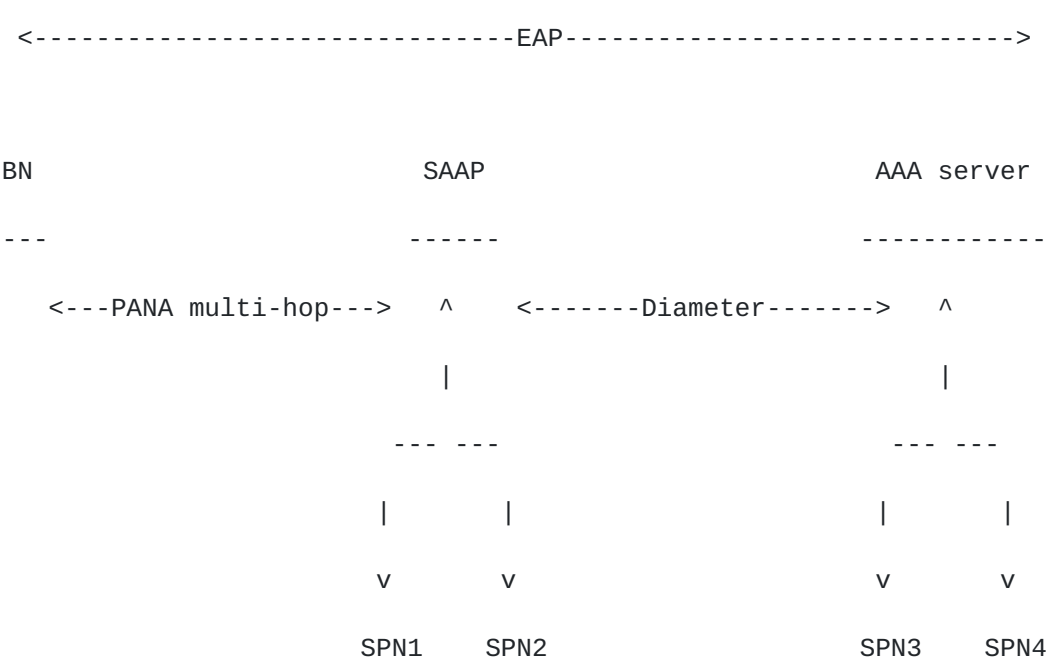

Figure 2: Service Authorization Anchor Point

2.5 Mobile ad-hoc networks (MANET) and infrastructure authentication

Mobile Ad-Hoc Networks (MANET) are envisioned to have dynamic, sometimes rapidly-changing, random, multi-hop topologies which are likely composed of relatively bandwidth-constrained wireless links.

One of the challenges which are being dealt with within the MANET community is the Internet connectivity for ad-hoc networks. Supporting global Internet connectivity for mobile ad-hoc networks is also useful because ad-hoc nodes inside a manet may want to communicate with nodes outside the MANET which are located somewhere in Internet. Some alternatives describe how to obtain a globally router address and Internet-gateway (GW) operation [I-D.wakikawa-manet-globalv6], [I-D.jelger-manet-gateway-autoconf-v6], [I-D.perkins-manet-aodvbis], [I-D.cha-manet-extended-support-globalv6], [I-D.ruiz-manet-mcast-gw-reqs] both for IPv4 and IPv6 connectivity.

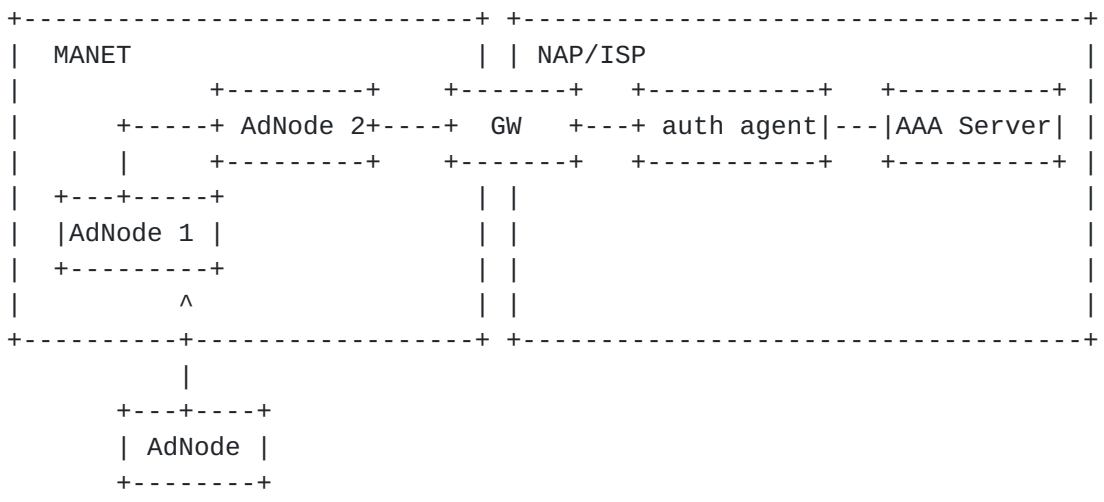

Figure 3: MANET + Infrastructure user authentication

The objective is to allow sending and/or receiving data traffic from Infrastructure side to any ad-hoc node attached to MANET. It is achieved through a gateway (GW) that is acting as another ad-hoc node in the MANET side and that belongs to the Infrastructure in the other side. In some scenarios, it MAY be required that only authenticated and authorized ad-hoc nodes can send data traffic to Internet. In order to achieve that, a mutual authentication process MUST be executed between a mobile ad-hoc node and authentication agent (AA). This authentication agent could be co-located or not in the GW depending on network management policies. Additionally authentication agent could need to interact with a backend AAA server.

EAP provides a flexible way to authenticate to entities (in particular ad-hoc nodes) because supports multiple authentication methods. EAP key management framework defines interactions between EAP peers (ad-hoc nodes in this scenario) authentication agents and AAA server. Following [I-D.ietf-eap-keying], on the one hand AAA protocols such as RADIUS or Diameter can be used to transport EAP between authentication agent and AAA server. On the other hand, EAP lower layer should be able to work over IP layer and multiple IP hop where each ac-hoc node and GW define a new hop.

Note that, in some cases, ad-hoc network MAY be considered as an un-secure link and a security association between ad-hoc node and GW MAY be needed for data traffic sent/received to/from the Internet. IPsec MAY be a choice.

Initially several alternatives are being considered (but not limited to):

- IKEv2 [I-D.ietf-ipsec-ikev2] that is able to transport EAP packets could be used between ad-hoc node and GW between multiple hops. IKEv2 is worth to be used when:
  - IPSec SA needs to be established between ad-hoc node and GW for data addressed to Internet and
  - Authentication Agent is co-located on GW
- PANA is also another protocol that is able to carry EAP and works over IP layer though currently it is not working in multi-hop scenarios. However, it is worth to make some modifications that allow to PANA works in multiple IP hop for several reasons:
  - It would allow Authentication Agent is not co-located in the GW
  - It would avoid to ad-hoc node (in general with limited computational resources) always performs Diffie-Hellman key exchange

Additionally note that several methods providing a prefix to ad-hoc nodes to allow them to configure IP global address can be find in references (i.e. [I-D.wakikawa-manet-globalv6], [I-D.jelger-manet-gateway-autoconf-v6]).It would be interesting for the sake of flexibility that multi hop-EAP lower layer will inform about what method must be used with a particular GW. For example, PANA provides that by using Post-PANA-Address-Configuration (PPAC) AVP.

Nevertheless further study must be done in order to determine that option could be considered more suitable taking into account special MANET features.

3. Mutihop EAP Requirements

This section describes requirements for a multi-hop EAP lower layer. In addition to the EAP lower layer requirements described in the EAP specification [RFC3748], a multi-hop EAP lower layer needs to satisfy the following requirements.

- A multi-hop EAP lower-layer MUST be able to establish an SA to subsequently provide integrity protection and replay protection for its later message exchange. It MUST be able to use EAP methods to establish keys from the EAP key hierarchy to create the SA.

- A multi-hop EAP lower-layer MUST be able to bootstrap SAs used for securing services that are not limited to simple network access services. The SAs MUST include not only IKE and IPsec SAs but also other types of SAs.

- A multi-hop EAP lower-layer MUST be able to carry service authorization parameters.

- A multi-hop EAP lower-layer SHOULD be specified with some out-of-band mechanism for an EAP peer to find its communicating EAP authenticator.

- A multi-hop EAP lower-layer MUST have a mechanism for NAT traversal.

4. Security Considerations

This document describes usage scenarios and requirements for running EAP over multiple IP hops between an EAP peer and an EAP authenticator. All security threats discussed in [I-D.ietf-pana-threats-eval] for the case where an EAP peer and an EAP authenticator are one IP hop away from each other and EAP is used for network access authentication apply to the usage scenarios and requirements described in this document. In the case of multi-hop EAP environments, the PANA requirement of binding the authenticated session to the device identifier of the client to mitigate service theft [I-D.ietf-pana-threats-eval] can make a denial of servcie (DoS) attack of preventing a legitimate client from binding its device identifier to the authenticated session easier because the device identifier of the client may not appear in the encapsulating header of the EAP lower layer messages. For example, when PANA is used as the multi-hop EAP lower layer and MAC address is used as the device identifier, an attacker PaC can put some other PaC's device identifier in a PANA Device-Id AVP while using its own MAC address in the encapsulating MAC header the PANA message. Since the PAA that is more than one IP hop away from the attacker is not able to see the original MAC header of the PANA message, a simple comparison of the Device-Id AVP against the device identifier contained in the MAC header does not work. This may require a cryptographic binding between the authenticated session and the device identifier of the client to be created outside the PANA protocol.

There is another type of security threats that are not addressed in [I-D.ietf-pana-threats-eval] and are related to the usage where an EAP lower layer is used for carrying authorization parameters. Eavesdropping of the authorization parameters is an issue if the authorization parameters contain privacy information without encryption. Theft of the authorization parameters is another issue if the authorization parameters are carried without encryption and there is no mechanism for cryptographically limiting the use of the authorization parameters to the authorized client only. If the authorization parameters are carried without integrity protection, a DoS attack based on by altering the authorization parameters is possible.

5. Acknowledgments

- General acknowledgments: The authors would like to thank Joseph Salowey for his valuable comments on the draft.

- Acknowledgments on Section 2.3: Section 2.3 is a byproduct of the Ambient Networks Project, partially funded by the European Commission under its Sixth Framework Programme. Section 2.3 is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained in Section 2.3 are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

- Acknowledgments on Section 2.5: The authors thank to Antonio F.Gomez Skarmeta and Pedro M.Ruiz for valuable comments for Section 2.5.

6. References

6.1 Normative References

[I-D.ietf-pana-pana]
Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-07 (work in progress), December 2004.

[I-D.ietf-pana-threats-eval]
Parthasarathy, M., "Protocol for Carrying Authentication and Network Access Threat Analysis and Security Requirements", draft-ietf-pana-threats-eval-07 (work in progress), August 2004.

[I-D.ietf-ipsec-ikev2]
Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

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

[I-D.ietf-eap-keying]
Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-04 (work in progress), November 2004.

[I-D.ietf-pana-ipsec]
Parthasarathy, M., "PANA enabling IPsec based Access Control", draft-ietf-pana-ipsec-05 (work in progress), December 2004.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A. and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

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

[I-D.tschofenig-mip6-bootstrapping-pana]
Tschofenig, H., Bournelle, J. and S. Thiruvengadam, "Bootstrapping Mobile IPv6 using PANA", draft-tschofenig-mip6-bootstrapping-pana-00 (work in progress), October 2004.

[I-D.wakikawa-manet-globalv6]
Wakikawa, R., "Global Connectivity for IPv6 Mobile Ad Hoc Networks", draft-wakikawa-manet-globalv6-03 (work in progress), October 2003.

[I-D.perkins-manet-aodvbis]
Perkins, C., "Ad hoc On-Demand Distance Vector (AODV) Routing", draft-perkins-manet-aodvbis-01 (work in progress), February 2004.

[I-D.jelger-manet-gateway-autoconf-v6]
Jelger, C., "Gateway and address autoconfiguration for IPv6 adhoc networks", draft-jelger-manet-gateway-autoconf-v6-02 (work in progress), April 2004.

[I-D.cha-manet-extended-support-globalv6]
Cha, H., Park, J. and H. Kim, "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks", draft-cha-manet-extended-support-globalv6-00 (work in progress), October 2003.

[I-D.thomson-nacp]
Thomson, S., "Network Access Control Protocol (NACP)", draft-thomson-nacp-00 (work in progress), October 2004.

[MPA] Anjum, F., Das, S., Dutta, A., Fajardo, V., Madhani, S., Ohba, Y., Taniuchi, K., Yaqub, R. and T. Zhang, "A proposal for MIH function and Information Service", January 2005.

6.2 Normative References

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[I-D.blanchet-v6ops-tunnelbroker-tsp]
Parent, F. and M. Blanchet, "IPv6 Tunnel Broker with the Tunnel Setup Protocol(TSP)", draft-blanchet-v6ops-tunnelbroker-tsp-01 (work in progress), June 2004.

[I-D.ruiz-manet-mcast-gw-reqs]
Ruiz, P., "Requirements for MANET Interworking with Wired Multicast Networks", draft-ruiz-manet-mcast-gw-reqs-00 (work in progress), February 2004.

[IEEE8021X]
"Port-Based Network Access Control", IEEE Standard for Local and Metropolitan Area Networks IEEE Std 802.1X-2004.

[RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[I-D.tschofenig-pana-bootstrap-kerberos]
Tschofenig, H., "Bootstrapping Kerberos", draft-tschofenig-pana-bootstrap-kerberos-00 (work in progress), July 2004.

[I-D.tschofenig-enroll-bootstrapping-saml]
Tschofenig, H., Giaretta, G. and A. Gomez-Skarmeta, "Enriching Bootstrapping with Authorization Information", draft-tschofenig-enroll-bootstrapping-saml-00.txt (work in progress), February 2005.

Authors' Addresses

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Phone: +39 011 2286904
EMail: gerardo.giaretta@tilab.com

Rafael Marin Lopez
University of Murcia
30071 Murcia
Spain

EMail: rafa@dif.um.es

Yoshihiro Ohba
Toshiba America Research, Inc.
1 Telcordia Drive
Piscataway, NJ 08854
USA

Phone: +1 732 699 5305
EMail: yohba@tari.toshiba.com

Susan Thomson
Cisco Systems
499 Thornall St, floor 8
Edison, NJ 08837
USA

EMail: sethomso@cisco.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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