MIPv6
Internet-Draft
Expires: April 18, 2005

H. Tschofenig
S. Thiruvengadam
Siemens

October 18, 2004

Bootstrapping Mobile IPv6 using PANA
draft-tschofenig-mip6-bootstrapping-pana-00.txt

Status of this Memo

Copyright Notice

Abstract

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 heavily focuses on one specific authentication and key exchange protocol. Obviously, this approach suffers from some limitations. This document investigates the usage of an EAP based bootstrapping approach using PANA.

Table of Contents

1. Introduction

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.

IKEv2 [I-D.ietf-ipsec-ikev2] supports the Extensible Authentication Protocol. Unfortuntately, IKEv2 only creates IPsec SAs since the concept of Domain of Interpretations (DoIs) was removed due to the limited usage in IKEv1. The authors think that most arguments against the IPsec protection of MIPv6 MN<->HA Binding Updates address problems caused by IPsec rather than IKEv2. It might be worth mentioning that IKEv2 is far more complex than [I-D.ietf-mip6-auth-protocol] . The extension proposed by [I-D.eronen-ipsec-ikev2-eap-auth], which tried to address some deployment aspects in certain environments, has not been considered by the IPsec working group.

Following the typical separation between

(a) Authentication and security association establishment and

(b) "Data" traffic protection

which is exercised by a number of protocols today (such as TLS, IKEv1, IKEv2) it seems to be reasonable to re-use the MIPv6 bootstrapping procedure for the former task whereas a simple integrity and replay protection mechanism is used to protect the Binding Update in a fashion similar to Mobile IPv4 [I-D.ietf-mip4-rfc3344bis] (or also similar to a modified version of the MIPv6-Auth-Protocol [I-D.ietf-mip6-auth-protocol]). Note that the "data" is, in our case, the signaling traffic.

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

o MN finding HA's address

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

With the most 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.

Protocol for Carrying Authentication for Network Access (PANA) is a lightweight protocol exchanging EAP payloads over UDP. This document suggests to consider the usage of PANA for bootstrapping of a security association between the MN and the HA.

Note that this document does not aim to replace the MIPv6-Auth-Protocol [I-D.ietf-mip6-auth-protocol].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Furthermore, we use the same terminology as in [RFC3775], [I-D.ietf-seamoby-mobility-terminology], [I-D.ietf-pana-requirements].

3. Introduction to PANA

PANA is a link layer agnostic transport for Extensible Authentication Protocol (EAP) to enable network access authentication between clients and access networks. PANA is currently being standardised at the IETF PANA working group. PANA can carry any EAP method and thereby allows user authentication and the establishment of a PANA security association between the PANA client (PaC) and PANA authentication agent (PAA) at the end of successful protocol run. The PAA indicates the results of the authentication using the PANA-Bind-Answer message.

3.1 PANA message flow

The protocol has four phases, which are explained briefly below. For detailed explanation and message formats, the reader should see [I-D.ietf-pana-pana].

Discovery phase: This is the initial handshake phase. The PaC discovers the PAA in this phase. The PaC sends a multicast discovery packet and the PAA responds to it with a PANA-start-request (PSR) message. The PaC responds with a PANA-start-answer (PSA) message. The PaC is also allowed to send a unicast discovery message if it knows the PAA in advance.

Authentication phase: A PANA-authentication-request is sent by the PAA and the PaC replies with PANA-authentication-answer. This message-pair may be repeated many times according to the EAP method in use. But finally PANA-bind-request message and PANA-bind-answer message pairs are exchanged. The PANA-bind-request would convey whether PaC is successfully authenticated or not. After the exchange of this message pair, the PAA would enforce the policy rules at the EP.

Termination phase: Either the PaC or the PAA could request termination of the PANA session. The PANA-termination-request message would initiate session termination and PANA-termination-answer would acknowledge the teardown of session.

Re-authentication phase: The PaC may have to re-authenticate periodically. For the reauthentication phase, the PAA sends the PANA-reauthentication-request message to PaC. It is acknowledged with PANA-reauthentication-answer and the PAA sends PANA-start-request message to trigger the authentication phase again.

An example message flow using the EAP-AKA [I-D.arkko-pppext-eap-aka]

is shown in Figure 1. The re-authentication and the termination phase are optional.

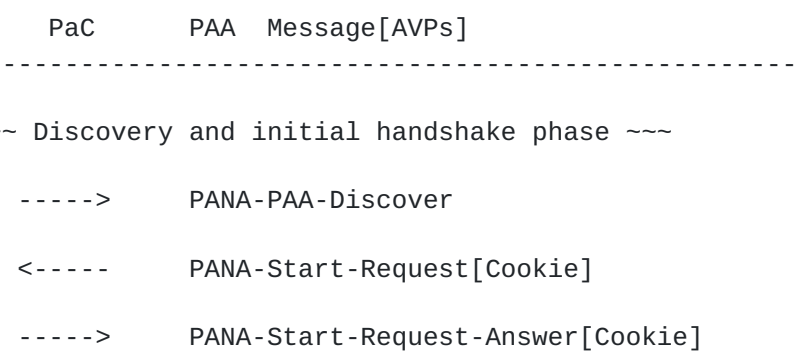

Figure 1: PANA message flow

3.2 Relaxing PANA Assumptions

PANA was designed with a focus on network access authentication. This fact is reflected in the discovery mechanism whereby a multicast address is used (see Section 8.2 of [I-D.ietf-pana-pana]) whereby it is assumed that the PAA is only one IP hop away from the PaC.

This assumption is not applicable to this environment. The PaC might address the PAA directly via a unicast message or a new discovery message needs to be added. In the former case the PAA would be co-located with the home agent.

4. 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.

4.1 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 incorporated into the PANA discovery mechanism is possible and for further investigation.

4.2 Obtaingin 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 [I-D.ietf-ipsec-nat-t-ike] 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).

4.3 MN-HA security association

As motivated in Section 1 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. Section 4.1.5 of [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). Section 4.4 of [I-D.ietf-pana-pana] 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].

5. Security Considerations

This document tries to raise some additional aspects for the MIPv6 MN <-> HA Binding Update security discussions in context of Mobile IPv6 Bootstrapping.

The security considerations of the following documents are directly applicable to this draft: PANA [I-D.ietf-pana-pana], MIPv6-Auth-Protocol [I-D.ietf-mip6-auth-protocol], MIPv4 [I-D.ietf-mip4-rfc3344bis], MIPv6 [RFC3775] and MIPv6 Boostrapping [I-D.ietf-mip6-bootstrap-ps]

A future version of this document will extract the relevant security issues from these documents in order to present them in more details once further steps have been taken within the MIPv6 working group.

6. Contributors

Many parts of this documents are the result of some discussions within the PANA WG team. In particular the authors would like to thank D. Forsberg, Y. Ohba, B. Patil and A. Yegin.

Furthermore, we would like to thank Udo Schilcher and Thomas Hambrusch for their contributions to this document.

7. References

7.1 Normative References

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

[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-05 (work in progress), July 2004.

[I-D.ietf-mip6-auth-protocol] "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-00 (work in progress), July 2004.

7.2 Informative References

[I-D.ietf-mip6-bootstrap-ps] Patel, A., "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-00 (work in progress), July 2004.

[I-D.ietf-seamoby-mobility-terminology] Manner, J. and M. Kojo, "Mobility Related Terminology", draft-ietf-seamoby-mobility-terminology-06 (work in progress), February 2004.

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

[I-D.ietf-pana-requirements] Yegin, A. and Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)Requirements", draft-ietf-pana-requirements-08 (work in progress), June 2004.

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

[I-D.eronen-ipsec-ikev2-eap-auth] Eronen, P., "Extension for EAP Authentication in IKEv2", draft-eronen-ipsec-ikev2-eap-auth-01 (work in progress), May 2004.

[I-D.ietf-ipsec-ikev2]
Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-16 (work in progress), September 2004.

[I-D.ietf-mip4-rfc3344bis]
"IP Mobility Support for IPv4, revised", draft-ietf-mip4-rfc3344bis-00 (work in progress), July 2004.

[I-D.arkko-pppext-eap-aka]
Arkko, J. and H. Haverinen, "EAP AKA Authentication", draft-arkko-pppext-eap-aka-12 (work in progress), April 2004.

[I-D.ietf-ipsec-nat-t-ike]
Kivinen, T., "Negotiation of NAT-Traversal in the IKE", draft-ietf-ipsec-nat-t-ike-08 (work in progress), February 2004.

[I-D.blanchet-v6ops-tunnelbroker-tsp]
Blanchet, M., "IPv6 Tunnel Broker with the Tunnel Setup Protocol(TSP)", draft-blanchet-v6ops-tunnelbroker-tsp-00 (work in progress), February 2004.

Authors' Addresses

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

EMail: Hannes.Tschofenig@siemens.com

Srinath Thiruvengadam
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: srinath@mytum.de

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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