Network Working Group
Internet-Draft
Expires: April 24, 2006

D. Forsberg (Ed.)
Nokia
Y. Ohba
Toshiba
B. Patil
Nokia
H. Tschofenig
Siemens
A. Yegin
Samsung

October 21, 2005

PANA Mobility Optimizations
draft-ietf-pana-mobopts-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 24, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This specification describes PANA optimizations for handling mobility. Proposed optimizations aim reducing protocol latency and signaling associated with PANA-based network access AAA.

Table of Contents

1. Introduction

A PaC using PANA [I-D.ietf-pana-pana] MUST execute full EAP/PANA upon inter-subnet (inter-PAA) movement. In case seamless mobility is desirable, having to execute full EAP authentication with a AAA server would incur undesirable latency. This document outlines the required extensions to the base PANA specification to eliminate the need to execute EAP each time the PaC performs an inter-PAA handover.

The scheme described in this document allows creation of a new PANA session with a new PAA based on an existing session with another PAA. Generation of the new PANA session does not require executing EAP-based authentication. Instead, a context-transfer-based scheme is used to bring in relevant state information from the previous PAA to the new PAA.

It should be noted that this document is limited to describing AAA optimizations on the PANA protocol. Additional optimizations aiming at EAP or specific AAA backend protocols (e.g., RADIUS, Diameter) can be defined independently. Furthermore, specification of the required context-transfer mechanism is left to other documents ([I-D.bournelle-pana-ctp]).

2. Requirements notation

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].

3. Framework

The call flow depicting mobility-optimized PANA execution is shown below.

```
            PaC                   newPAA            prePAA
             |                       |                  |
          1  |<---------- live PANA session ----------->|
             |                       |                  |
          2  x move from subnet1     |                  |
             | to subnet2            |                  |
             |                       |                  |
             |         PDI           |                  |
          3  |---------------------->|                  |
             |         PSR           |                  |
          4  |<----------------------|                  |
             |         PSA           |                  |
          5  |---------------------->|      CT-req      |
          6  |                       |----------------->|
             |                       |      CT-resp     |
          7  |         PBR           |<-----------------|
          8  |<----------------------|                  |
             |         PBA           |                  |
          9  |---------------------->|                  |
```

In this flow, the PaC is already authorized and connected to subnet1, where prePAA resides (step 1). Later, the PaC performs a handover from subnet1 to subnet2 (step 2). Following the movement, PANA discovery and handshake phases are executed (steps 3-5). In response to the parameters included in the PSA, PANA session context is transferred from the prePAA to the newPAA (steps 6,7). Finally, PANA-Bind exchange signals the successful PANA authorization (steps 8,9). In this flow, EAP authentication does not take place.

4. Protocol Details

A mobile PaC's network access authentication performance can be enhanced by deploying a context-transfer-based mechanism, where some session attributes are transferred from the previous PAA to the new one in order to avoid performing a full EAP authentication (reactive approach). Additional mechanisms that are based on the proactive AAA state establishment at one or more candidate PAAs may be developed in the future (see for example [I-D.irtf-aaaarch-handoff]'). The details of a context-transfer-based mechanism is provided in this section.

Upon changing its point of attachment, a PaC that wants to quickly resume its ongoing PANA session without running EAP MAY send its unexpired PANA session identifier in its PANA-Start-Answer message. Along with the Session-Id AVP, a MAC AVP MUST be included in this message. The MAC AVP is computed by using the PANA_MAC_KEY shared between the PaC and its previous PAA that has an unexpired PANA session with the PaC. This action signals the PaC's desire to perform the mobility optimization. In the absence of a Session-Id AVP in this message, the PANA session takes its usual course (i.e., EAP-based authentication is performed).

If a PAA receives a session identifier in the PANA-Start-Answer message, and it is configured to enable this optimization, it SHOULD retrieve the PANA session attributes from the previous PAA. The identity of the previous PAA is determined by looking at the DiameterIdentity part of the PANA session identifier. The MAC AVP can only be verified by the previous PAA, therefore a copy of the PANA message MUST be provided to the previous PAA. The mechanism required to send a copy of the PANA-Start-Answer message from current PAA to the previous PAA, and to retrieve the session attributes is outside the scope of PANA protocol. The Context Transfer Protocol [I-D.ietf-seamoby-ctp] might be useful for this purpose.

When the previous or current PAA is not configured to enable this optimization, the current PAA can not retrieve the PANA session attributes, or the PANA session has already expired (i.e., session lifetime is zero), the PAA MUST send the PANA-Auth-Request message with a new session identifier and let the PANA exchange take its usual course. As a result the PaC will engage in EAP-based authentication and create a fresh PANA session from scratch.

In case the current PAA can retrieve the on-going PANA session attributes from the previous PAA, the PANA session continues with a PANA-Bind exchange.

As part of the context transfer, an intermediate AAA-Key material is

provided by the previous PAA to the current PAA.

```
AAA-Key-int = The first N bits of
              HMAC-SHA1(AAA-Key, DiameterIdentity | Session-ID)
```

The value of N depends on the integrity protection algorithm in use, i.e., N=160 for HMAC-SHA1. DiameterIdentity is the identifier of the current (new) PAA. Session-ID is the identifier of the PaC's PANA session with the previous PAA.

The current PAA and the PaC compute the new AAA-Key by using the nonce values and the AAA-Key-int.

```
AAA-Key-new = The first N bits of
              HMAC-SHA1(AAA-Key-int, PaC_nonce | PAA_nonce)
```

New PANA_MAC_KEY is computed based on the algorithm described in [I-D.ietf-pana-pana], by using the new AAA-Key and the new Session-ID assigned by the current PAA. The MAC AVP contained in the PANA-Bind-Request and PANA-Bind-Answer messages MUST be generated and verified by using the new PANA_MAC_KEY. The Session-ID AVP MUST include a new session identifier assigned by the current PAA. A new PANA session is created upon successful completion of this exchange.

5. Deployment Considerations

Correct operation of this optimization relies on many factors, including applicability of authorization state from one network attachment to another. [I-D.ietf-eap-keying] identifies this operation as "fast handoff" and provides deployment considerations. Operators are recommended to take those guidelines into account when using this optimization in their networks.

6. Keying Considerations

Upon PaC's movement to a another PAA (new PAA) and request to perform a context transfer based optimization, the previous PAA computes a AAA-Key-int based on the AAA-Key, ID of new PAA, and the session ID. This AAA-Key-int is delivered to the new PAA, and used in the computation of the AAA-Key-new, which further takes a pair of nonce values into account. After this point on, the AAA-Key-new becomes the AAA-Key between the PaC and the new PAA.

The AAA-Key-int can be deleted as soon as AAA-Key-new is derived. The lifetime of AAA-Key-new is bounded by the lifetime of AAA-Key.

7. Security Considerations

The mobility optimization described in this document involves the previous PAA (possessing the AAA-Key) providing a AAA-Key-new to the current PAA of the PaC. There are security risks stemming from potential compromise of PAAs. Compromise of the current PAA does not yield compromise of the previous PAA, as the AAA-Key cannot be computed from a compromised AAA-Key-new. But a compromised previous PAA along with the intercepted nonce values on the current link leads to the compromise of AAA-Key-new. Operators should be aware of the potential risk of using this optimization.

An operator can reduce the risk exposure by forcing the PaC to perform an EAP-based authentication immediately after the PaC gains access to new link via the optimized PANA execution.

8. References

8.1. Normative References

[I-D.ietf-eap-keying]
Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-07 (work in progress), July 2005.

[I-D.ietf-pana-pana]
Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-10 (work in progress), July 2005.

[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.bournelle-pana-ctp]
Bournelle, J., "Use of Context Transfer Protocol (CxTP) for PANA", draft-bournelle-pana-ctp-03 (work in progress), June 2005.

[I-D.ietf-seamoby-ctp]
Loughney, J., "Context Transfer Protocol", draft-ietf-seamoby-ctp-11 (work in progress), August 2004.

[I-D.irtf-aaaarch-handoff]
Arbaugh, W. and B. Aboba, "Experimental Handoff Extension to RADIUS", draft-irtf-aaaarch-handoff-04 (work in progress), November 2003.

Authors' Addresses

Dan Forsberg
Nokia Research Center
P.O. Box 407
FIN-00045 NOKIA GROUP
Finland

Phone: +358 50 4839470
Email: dan.forsberg@nokia.com

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

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

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX 75039
USA

Phone: +1 972-894-6709
Email: Basavaraj.Patil@nokia.com

Hannes Tschofenig
Siemens Corporate Technology
Otto-Hahn-Ring 6
81739 Munich
Germany

Email: Hannes.Tschofenig@siemens.com

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

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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