Network Working Group
Internet-Draft
Expires: December 26, 2005

J. Bournelle (Ed.)
M. Laurent-Maknavicius
GET/INT
H. Tschofenig
Siemens
Y. El Mghazli
Alcatel
G. Giaretta
TILab
R. Lopez
Univ. of Murcia
Y. Ohba
Toshiba
June 24, 2005

Use of Context Transfer Protocol (CxTP) for PANA
draft-bournelle-pana-ctp-03

Status of this Memo

Copyright Notice

Abstract

The PANA protocol offers a way to authenticate clients in IP based access networks. However, in roaming environments, IP clients might change of gateways and new EAP authentication from scratch may occur. The present document describes a solution based on the Context Transfer Protocol (CxTP) to enhance IP handover in mobile environments. This protocol can recover the previously established PANA security context from previous PANA Authentication Agent.

Table of Contents

1. Introduction 3
2. Terminology 4
3. Background 6
3.1 PANA framework 6
3.2 Performance limitations in mobile environments 6
3.3 CxTP protocol overview 7
4. The PANA Context 9
5. CxTP usage in the PANA framework 11
6. Conditions to Perform the Transfer 13
7. Security considerations 14
8. Acknowledgements 15
9. References 16
9.1 Normative References 16
9.2 Informative References 16
Authors' Addresses 16
Intellectual Property and Copyright Statements 19

1. Introduction

In IP based access network, PANA [I-D.ietf-pana-pana] may be used as a front-end to a AAA architecture in order to authenticate users before granting them access to the resources. For this purpose, it uses EAP which offers a variety of authentication methods. In a shared medium, this is typically accomplished with the help of cryptographic mechanisms. Note that this type of cryptographic mechanism prevents a malicious node from sending packet to the network and thereby authenticating each data packet. In addition, encryption is often enabled to prevent eavesdropping.

While roaming, the PANA client might change its access router. In some cases and without extensions to PANA, the PaC has to restart a new PANA protocol exchange to authenticate itself to the network. This authentication may need to execute the EAP exchange from scratch.

In this document, we analyse the interaction between the framework defined in [I-D.ietf-seamoby-ctp] and PANA. In particular, we define what should be transferred (i.e. the PANA context).

Rough consensus in the PANA working group leaded to the solution where the transfer occurs between authentication agents, according to the recommendations in [I-D.ietf-pana-mobopts].

2. Terminology

Most of the terms are defined in the PANA [I-D.ietf-pana-pana] and CxTP [I-D.ietf-seamoby-ctp] specifications:

nAR New Access Router. The router to which the PaC attaches after the handover.

pAR Previous Access Router. The router to which the PaC was attached before the handover.

CTAA Context Transfer Activate Acknowledge.

CTAR Context Transfer Activate Request.

CTD Context Transfer Data.

CxTP Context Transfer Protocol.

EP Enforcement Point. (PANA term)

FPT Feature Profile Type (CxTP term).

PaC PANA Client. A mobile node (MN) using a PANA protocol implementation to authenticate itself to the network.

PAA PANA Authentication Agent. The access network (server) side entity of the PANA protocol. A PAA is in charge of interfacing with the PaCs for authenticating and authorizing them for the network access service.

nPAA New PANA Authentication Agent. The PAA in charge of the subnet to which the PaC is attached after the handover.

pPAA Previous PANA Authentication Agent. The PaC's default PAA prior to handover.

PANA Protocol for Carrying Network Authentication for Network Access

3. Background

This section gives basic information on PANA framework and CxTP protocol. The intent here is to further explain the context being referred to and the terminology used in the remaining of the document.

3.1 PANA framework

PANA is a protocol that carries EAP over IP/UDP to authenticate users. The PANA Authentication Agent (PAA) is the endpoint of the PANA protocol at the access network. The PAA itself might not be able to authenticate the user by terminating the EAP protocol. Instead the PAA might forward the EAP payloads to the backend AAA infrastructure.

The Enforcement Point (EP) is an entity which enforces the result of the PANA protocol exchange. The EP might be co-located with the PAA or separated as a stand-alone device. In the latter case, the SNMPv3 protocol [I-D.ietf-pana-snmp] is used to communicate between PAA and EP.

A successful EAP authentication exchange results in a PANA security association (PANA SA) if the EAP method was able to derive session keys. In this case, all further PANA messages between PaC and PAA will be authenticated, replay and integrity protected thanks to the MAC AVP.

3.2 Performance limitations in mobile environments

```
              PaC ------------ pEP ---- pPAA
               |                |
               |                |
               |                +------ pAR
(IP handover)  |
               |
               v
              PaC------------ nEP ---- nPAA
                               |
                               |
                               +------ nAR
```

Figure 1: Example Scenario

Figure 1 shows an example scenario with a roaming PaC which has been previously authenticated. The PAA is at one IP hop away from PaC; this means that a specific PANA module on a PAA is in charge of one

IP network. After a PaC's IP handover, the PaC changes of IP subnet and of PAA accordingly. The new PAA (nPAA) does not share any context with the PaC. The new EP (nEP) will detect the PaC and will trigger a new PANA authentication phase from scratch. A new authentication phase involving the AAA infrastructure will then occur. Such a signaling can seriously degrade handover performance in term of latency.

For this reason, we propose to use the Context Transfer Protocol (CxTP) to transfer the PANA context established between the PaC and pPAA to the nPAA.

3.3 CxTP protocol overview

Context Transfer Protocol (CxTP) [I-D.ietf-seamoby-ctp] enables context transfers between access routers (ARs). The context transfer can be either initiated by a request from the mobile node ("mobile initiated") or at the initiative of either the new or the previous access router ("network initiated"). Furthermore it can be performed prior to handover ("predictive mode") or after the handover ("reactive mode").

In reactive mode, the MN sends a CT Activate Request (CTAR) to the new AR (nAR) (cf. Figure 2). In this message the MN includes an authorization token: this token is calculated based on a secret shared between the MN and the previous AR (pAR) and it is used in order to authorize the transfer. This means that the MN and the pAR must share a secret. The definition of this secret is out of scope of CxTP. As soon as the nAR receives a CTAR message, it generates a CT-Request message which includes the authorization token and the context to be transferred (i.e. Feature Profile Types). This message is received by the pAR that verifies the authorization token and sends a Context Transfer Data (CTD) message including the requested context.

```
      MN              nAR             pAR
      --              ---             ---
       |               |               |
       |    CTAR       |               |
       +-------------->|               |
       |               |   CT-Request  |
       |               +-------------->|
       |               |               |
       |               |      CTD      |
       |               |<--------------+
       |    CTAA       |               |
       |<--------------+               |
```

Figure 2: CxTP in reactive mode

In the predictive case, the pAR receives a CTAR message from the MN whose feature contexts are to be transferred. This message provides the IP address of the nAR and an authorization token. The pAR predictively transmits to the nAR a Context Transfer Data (CTD) that contains feature contexts. This message contains also parameters for the nAR to compute an authorization token in order to verify the MN's token. Regardless the MN sent the CTAR to the pAR, it sends another CTAR message to the nAR in order to ascertain that the context transfer reliably took place. Furthermore in this CTAR the MN includes the authorization token so that the nAR verifies it.

CxTP messages use Feature Profile Types (FPTs) to identify the way data is organized for a particular feature context. The FPTs are registered in a number space that allows a node to unambiguously determine the type of context and the context parameters present in the protocol messages.

4. The PANA Context

The PANA Context is what should be transferred between the two PAAs to avoid re-authentication from scratch. The attributes described in [I-D.ietf-pana-pana] list elements that could constitute the PANA context at PAA. However some of these data are PAA specific and as such does not need to be transferred.

Figure 3 summarizes the PANA Context.

Data	Type	Length
Session-Lifetime Elapsed	Unsigned32	Fixed
AAA-Key-int	UTF8String	Fixed (64 octets)
ISP-Identifier	Unsigned32	Fixed
ISP-Name	UTF8String	Variable
NAP/ISP Separate Authentication	Unsigned32	Fixed

Figure 3: The PANA Context

Data have the following meanings:

Session-Lifetime: The authentication phase also determines the PANA session lifetime when authorization succeeds. This value is included in Session-Lifetime AVP. In Diameter [RFC3588], this AVP (Session-Timeout) is of type Unsigned32 and contains the maximum number of seconds of service to be provided to the user before session termination. Note that the value forwarded to the new PAA needs to reflect the already 'consumed' session lifetime. This helps to avoid problems where roaming is used to reset the lifetime when re-attaching at a new PAA. It must be assured that the sum of the individual session lifetimes is never greater than the initially communicated lifetime (type: Unsigned32, length: 4)

AAA-Key-int: cf. [I-D.ietf-pana-mobopts].

ISP-Identifier: IANA assigned "SMI Network Management Private Enterprise Codes" of the provider.

ISP-Name: UTF8-encoded name of the provider.

Separate NAP/ISP authentication: This variable indicates if a separate NAP/ISP authentication has been performed at pPAA.

5. CxTP usage in the PANA framework

The transfer may occur either after or before the handover. From this standpoint, we only consider the reactive mode. This means that the PaC has already performed the handover. Predictive mode is left for further study.

The solution described here is based on [I-D.ietf-pana-mobopts]: the transfer is triggered using the PANA signalling and CTD message is used to carry the PANA context.

The CTD message is described in the following figure (ABNF notation):

```
      CTD-PANA ::= < CTD-Header>
      < Context Data Block, Ctx-Type: PANA-Context-Transfer, FPT>
         { Session-Lifetime-Elapsed }
      { AAA-Key-int }
      { ISP-Identifier }
      { ISP-Name }
      { Double Authentication NAP/ISP information }
```

Figure 4: CTD-PANA message

where FPT (Feature Profile Type) identifies the way the particular feature context is organized.

In the solution proposed by PANA [I-D.ietf-pana-mobopts], the PaC does not use CTAR message to request and activate the context. Instead, it replies to PSR message with a PSA message containing the unexpired previous PANA session identifier and a MAC AVP (cf. Figure 5). This AVP is computed using the PANA_MAC_KEY shared between the PaC and its pPAA.

```
      PaC           nPAA              pPAA
      ---           ----              ----
         PSR[PAA_Nonce]
       <------------

      PSA[oSession-ID][PaC_Nonce][MAC]
        -------------->

                        CT-Request [PSA]
                        ---------------->
                          CTD-PANA
                     <----------------
         PBR[nSession-Id][MAC]
       <--------------
          PBA [MAC]
       --------------->
```

Figure 5: The PANA approach

The nPAA receives this PSA message and it deduces that it must perform CxTP (because of the Session-Id AVP). It determines the identity of pPAA by looking at the DiameterIdentity part of the PANA session identifier. It sends a CT-Request to the pPAA containing the PSA message. The pPAA checks the validity of the PSA message and transfers the PANA context in the CTD message. Then the PANA session continues with a PANA-Bind exchange.

6. Conditions to Perform the Transfer

In this section, we list conditions and recommendations to perform a PANA context transfer between two PAAs. This list is mostly inherited from [I-D.aboba-802-context]:

- o Homogeneous PAA's device deployment within a single administrative domain.

- o This solution only consider intradomain scenario.

- o Entities engaged in the context transfer should authenticate each other. For this purpose, CxTP indicates that IPsec ESP must be used in order to provide connectionless integrity, data origin authentication and confidentiality protection. Thus pPAA and nPAA should have IPsec SAs to protect CxTP messages.

- o The nPAA should not obtain keys used to encrypt traffic between PaC and pEP. This traffic may be encrypted at layer 2 or at layer 3.

- o The new key (AAA-Key-new) derived between PaC and nPAA is based on Nonces exchanged during PANA-Start-Exchange. For this reason, the proposed solution only work with PANA Stateful Discovery mechanism.

7. Security considerations

This document deals with interaction between the Seamoby Context Transfer Protocol and PANA. Therefore, all security considerations described in [I-D.ietf-seamoby-ctp], in [I-D.ietf-pana-pana] and in [I-D.ietf-pana-mobopts] also apply here.

The approach described in this document considers only the intra-domain scenario. This means that the PAAs involved in the context transfer belong to the same administrative domain. Therefore, at this stage the inter-domain scenario is out of scope.

As described in [I-D.ietf-seamoby-ctp] IPsec ESP must be used to protect CxTP messages between PAAs. In order to avoid the introduction of additional latency due to the need for establishment of a secure channel between the context transfer peers, the two PAAs should establish such a secure channel in advance. The mechanism used by the PAAs to establish such a channel is out of the scope of this draft: for example, IKE [RFC2409] with pre-shared key authentication might be used.

8. Acknowledgements

The authors would like to thank Vijay Devarapalli, James Kempf, Rajeev Koodli, Nakhjiri Madjid-MNAKHJI, Jean-Jacques Puig, Rene Soltwitsch and Alper Yegin for their valuable comments.

9. References

9.1 Normative References

[I-D.ietf-pana-pana]
Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-08 (work in progress), May 2005.

[I-D.ietf-pana-mobopts]
Forsberg, D., "PANA Mobility Optimizations", draft-ietf-pana-mobopts-00 (work in progress), January 2005.

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

[I-D.aboba-802-context]
Aboba, B. and T. Moore, "A Model for Context Transfer in IEEE 802", draft-aboba-802-context-02 (work in progress), April 2002.

9.2 Informative References

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[I-D.ietf-pana-snmp]
Mghazli, Y., "SNMP usage for PAA-EP interface", draft-ietf-pana-snmp-03 (work in progress), February 2005.

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

Authors' Addresses

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Maryline Laurent-Maknavicius
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: maryline.maknavicius@int-evry.fr

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

Email: Hannes.Tschofenig@siemens.com

Yacine El Mghzali
Alcatel
Route de Nozay
Marcoussis 91460
France

Email: yacine.el_mghazli@alcatel.fr

Gerardo Giaretta
TILab
via G. Reiss Romoli, 274
TORINO 10148
Italy

Email: gerardo.giaretta@telecomitalia.it

Rafa Marin Lopez
University of Murcia
30071 Murcia
Spain

Email: rafa@dif.um.es

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

Phone: +1 732 699 5365
Email: yohba@tari.toshiba.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.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

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

Acknowledgment

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