Internet Engineering Task Force (IETF)
Request for Comments: 5873
Category: Experimental
ISSN: 2070-1721

Y. Ohba
Toshiba
A. Yegin
Samsung

May 2010

Pre-Authentication Support for the Protocol for Carrying Authentication for Network Access (PANA)

Abstract

This document defines an extension to the Protocol for Carrying Authentication for Network Access (PANA) for proactively establishing a PANA Security Association between a PANA Client in one access network and a PANA Authentication Agent in another access network to which the PANA Client may move.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5873.

Table of Contents

1. Introduction

The Protocol for Carrying Authentication for Network Access (PANA) [RFC5191] carries Extensible Authentication Protocol (EAP) messages between a PANA Client (PaC) and a PANA Authentication Agent (PAA) in the access network. If the PaC is a mobile device and is capable of moving from one access network to another while running its applications, it is critical for the PaC to perform a handover seamlessly without degrading the performance of the applications during the handover period. When the handover requires the PaC to establish a PANA session with the PAA in the new access network, the signaling to establish the PANA session should be completed as fast as possible. See [RFC5836] for the handover latency requirements.

This document defines an extension to the PANA protocol [RFC5191] used for proactively executing EAP authentication and establishing a PANA SA (Security Association) between a PaC in an access network and a PAA in another access network to which the PaC may move. The extension to the PANA protocol is designed to realize direct pre-authentication defined in [RFC5836]. How to realize authorization and accounting with the use of the pre-authentication extension is out of the scope of this document.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

2. Terminology

The following terms are used in this document, in addition to the terms defined in [RFC5191].

Serving Network: The access network to which the host is currently attached.

Candidate Network: An access network that is a potential target of the host's handover.

Serving PAA (SPAA): A PAA that resides in the serving network and provides network access authentication for a particular PaC.

Candidate PAA (CPAA): A PAA that resides in a candidate network to which the PaC may move. A CPAA for a particular PaC may be a SPAA for another PaC.

Pre-authentication: Pre-authentication refers to EAP pre-authentication and is defined as the utilization of EAP to pre-establish EAP keying material on an authenticator prior to arrival of the peer at the access network served by that authenticator [RFC5836]. In this document, EAP pre-authentication is performed between a PaC and a CPAA.

3. Pre-Authentication Procedure

A PaC that supports pre-authentication may establish a PANA session for each CPAA.

There may be several mechanisms for a PaC to discover a CPAA. An IP address of the discovered CPAA is the output of those mechanisms. PANA pre-authentication is performed between the PaC and CPAA using the discovered IP address of the CPAA. IEEE 802.21 [802.21] Information Service MAY be used as a CPAA discovery mechanism.

There may be a number of criteria for CPAA selection, the timing to start pre-authentication, and the timing as to when the CPAA becomes the SPAA. Such criteria can be implementation-specific and thus are outside the scope of this document.

Pre-authentication is initiated by a PaC in a way similar to normal authentication. A new 'E' (prE-authentication) bit is defined in the PANA header. When pre-authentication is performed, the 'E' (prE-authentication) bit of PANA messages is set in order to indicate that this PANA run is for pre-authentication. Use of pre-authentication is negotiated as follows.

- When a PaC initiates pre-authentication, it sends a PANA-Client-Initiation (PCI) message with the 'E' (prE-authentication) bit set. The CPAA responds with a PANA-Auth-Request (PAR) message with the 'S' (Start) and 'E' (prE-authentication) bits set only if it supports pre-authentication. Otherwise, the 'E' (prE-authentication) bit of the PAR message will be cleared according to Section 6.2 of [RFC5191], which results in a negotiation failure.

- Once the PaC and CPAA have successfully negotiated on performing pre-authentication using the 'S' (Start) and 'E' (prE-authentication) bits, the subsequent PANA messages exchanged between them MUST have the 'E' (prE-authentication) bit set until the CPAA becomes the SPAA of the PaC. The PaC may conduct this exchange with more than one CPAA. If the PaC and CPAA have failed to negotiate on performing pre-authentication, the PaC or CPAA that sent a message with both the 'S' (Start) and 'E' (prE-authentication) bits set MUST discard the message received from the peer with 'S' (Start) bit set and the 'E' (prE-authentication) bit cleared, which will eventually result in PANA session termination.

If IP reconfiguration is needed in the access network associated with the CPAA, the 'I' (IP Reconfiguration) bit in PAR messages used for pre-authentication between the PaC and CPAA is also set. The 'I' (IP Reconfiguration) bit in these messages takes effect only after the CPAA becomes the SPAA.

When a CPAA of the PaC becomes the SPAA, e.g., due to movement of the PaC, the PaC informs the PAA of the change using PANA-Notification-Request (PNR) and PANA-Notification-Answer (PNA) messages with the 'P' (Ping) bit set and the 'E' (prE-authentication) bit cleared. The 'E' (prE-authentication) bit MUST be cleared in subsequent PANA messages.

A PANA SA is required for pre-authentication in order to securely associate the PNR/PNA exchange to the earlier authentication.

The PANA session between the PaC and a CPAA is deleted by entering the termination phase of the PANA protocol.

An example call flow for pre-authentication is shown in Figure 1. Note that EAP authentication is performed over PAR and PANA-Auth-Answer (PAN) exchanges, including the one with the 'C' (Complete) bit set.

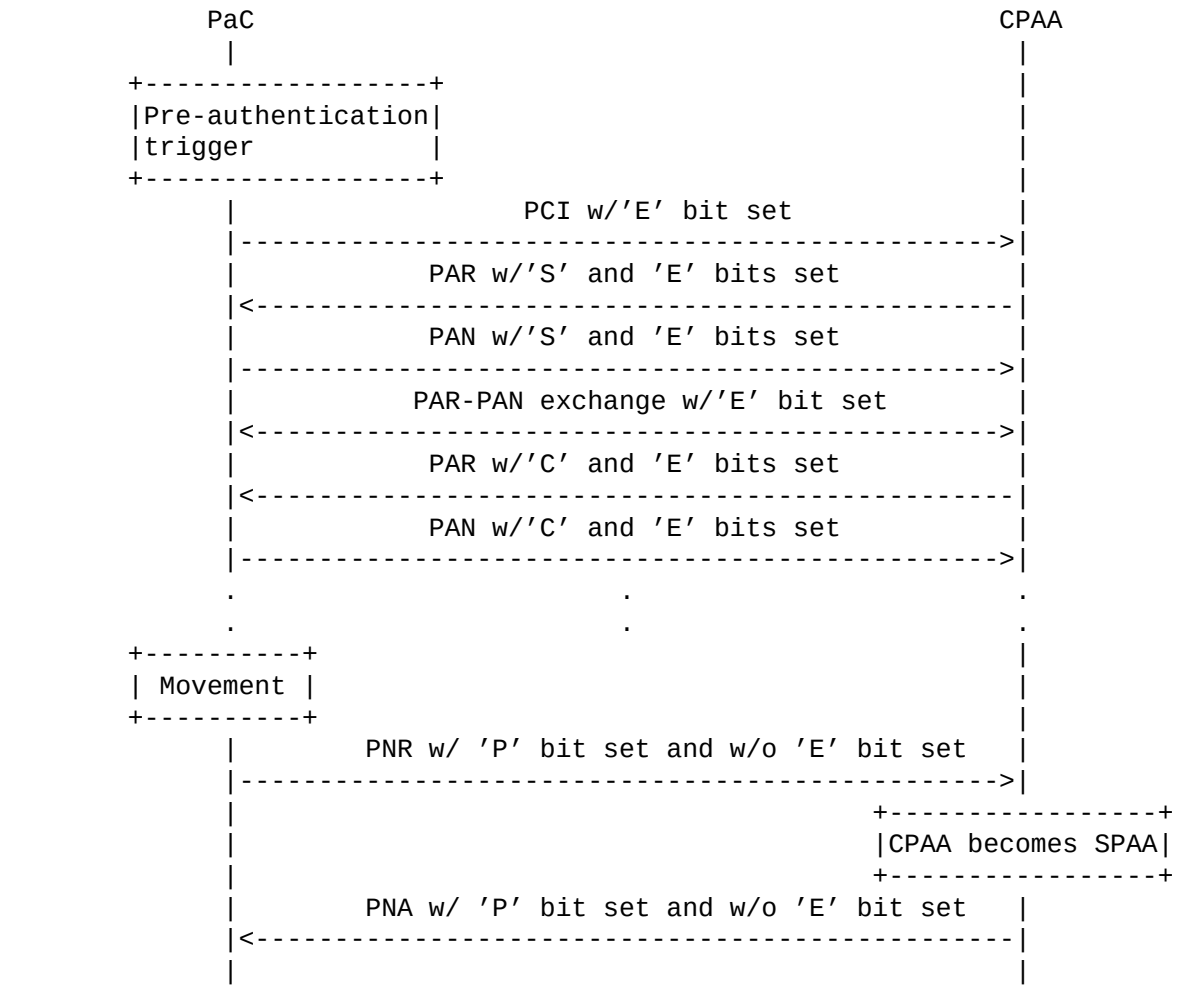

Figure 1: Pre-Authentication Call Flow

4. PANA Extensions

A new 'E' (prE-authentication) bit is defined in the Flags field of the PANA header as follows.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R S C A P I E r r r r r r r r r|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

'E' (prE-authentication) bit: When pre-authentication is performed, the 'E' (prE-authentication) bit of PANA messages is set in order to indicate whether this PANA run is for pre-authentication. The

exact usage of this bit is described in Section 3. Bit 6 has been assigned by IANA.

5. Backward Compatibility

Backward compatibility between a PANA entity that does not support the pre-authentication extension and another PANA entity that supports the pre-authentication extension is maintained as follows.

When a PaC that supports the pre-authentication extension initiates PANA pre-authentication by sending a PCI message with the 'E' (prE-authentication) bit set to a PAA that does not support the pre-authentication extension, the PAA will ignore the 'E' (prE-authentication) bit according to Section 6.2 of [RFC5191], and try to process the message as a normal authentication attempt. As a result, the PaC will receive a PAR message with the 'E' (prE-authentication) bit cleared. In this case, the negotiation on the use of pre-authentication will fail, and eventually the PANA session will be terminated as described in Section 3.

6. Security Considerations

This specification is based on the PANA protocol, and it exhibits the same security properties, except for one important difference: Pre-authenticating PaCs are not physically connected to an access network associated with the PAA, but they are connected to some other network somewhere else on the Internet. This distinction can create greater denial-of-service (DoS) vulnerability for systems using PANA pre-authentication if appropriate measures are not taken. An unprotected PAA can be forced to create state by an attacker PaC that merely sends PCI messages.

[RFC5191] describes how the PAA can stay stateless while responding to incoming PCIs. PAAs using pre-authentication SHOULD be following those guidelines (see [RFC5191], Section 4.1).

Furthermore, it is recommended that PANA pre-authentication messages be only accepted from PaCs originating from well-known IP networks (e.g., physically adjacent networks) for a given PAA. These IP networks can be used with a whitelist implemented on either the firewall protecting the perimeter around the PAA or the PAA itself. This prevention measure SHOULD be used whenever it can be practically applied to a given deployment.

7. IANA Considerations

As described in Section 4, and following the new IANA allocation policy on PANA messages [RFC5872], bit 6 of the Flags field of the PANA header has been assigned by IANA for the 'E' (prE-authentication) bit.

8. Acknowledgments

The authors would like to thank Basavaraj Patil, Ashutosh Dutta, Julien Bournelle, Sasikanth Bharadwaj, Subir Das, Rafa Marin Lopez, Lionel Morand, Victor Fajardo, Glen Zorn, Qin Wu, Jari Arkko, Pasi Eronen, and Joseph Salowey for their support and valuable feedback.

9. References

9.1. Normative References

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

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5872] Arkko, J. and A. Yegin, "IANA Rules for the Protocol for Carrying Authentication for Network Access (PANA)", RFC 5872, May 2010.

9.2. Informative References

[RFC5836] Ohba, Y., Ed., Wu, Q., Ed., and G. Zorn, Ed., "Extensible Authentication Protocol (EAP) Early Authentication Problem Statement", RFC 5836, April 2010.

[802.21] IEEE, "Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", LAN MAN Standards Committee of the IEEE Computer Society 802.21, 2008.

Authors' Addresses

Yoshihiro Ohba
Toshiba Corporate Research and Development Center
1 Komukai-Toshiba-cho
Saiwai-ku, Kawasaki, Kanagawa 212-8582
Japan

Phone: +81 44 549 2230
EMail: yoshihiro.ohba@toshiba.co.jp

Alper Yegin
Samsung
Istanbul
Turkey

EMail: alper.yegin@yegin.org