Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 8, 2011

P. Duffy
Cisco
S. Chakrabarti
Unaffiliated
R. Cragie
PG&E
Y. Ohba (Ed.)
Toshiba
A. Yegin
Samsung

February 4, 2011

Protocol for Carrying Authentication for Network Access (PANA) Relay Element
draft-ohba-pana-relay-03

Abstract

This document specifies Protocol for carrying Authentication for Network Access (PANA) Relay Element functionality which enables PANA messaging between a PANA Client (PaC) and a PANA Authentication Agent (PAA) where the two nodes cannot reach each other by means of regular IP routing.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on August 8, 2011.

Table of Contents

1. Introduction

Protocol for carrying Authentication for Network Access (PANA) [RFC5191] is a UDP-based protocol to perform EAP authentication between a PANA Client (PaC) and a PANA Authentication Agent (PAA).

This document specifies PANA Relay Element (PRE) functionality which enables PANA messaging between a PaC and a PAA where the two nodes cannot reach each other by means of regular IP routing. For example, in ZigBee IP that uses 6LoWPAN [RFC4944], a joining node (PaC) can only use a link-local IPv6 address to communicate with a parent node prior to PANA authentication. The PAA typically resides in a 6LowPAN Border Router (6LBR) [I-D.ietf-6lowpan-nd] which is often multiple IP hops away from the PaC. The PRE implemented on the parent node is used for relaying PANA messages between the PaC and the PAA in this scenario.

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. PANA Relay Element

The PANA Relay Element (PRE) is a node that is located between the PaC and the PAA. It is responsible for relaying the PANA messages between the PaC and the PAA. The PRE does not need to maintain per-PaC state. From the PaC's perspective, the PRE appears as the PAA. Normal IP routing is performed between the PRE and the PAA. It is assumed that the PRE's IP address that is reachable from the PaC is known to the PaC prior to PANA authentication by some means that is not specified in this document. It is also assumed that the PAA's IP address that is reachable from the PRE is known to the PRE by some means that is not specified in this document.

The PRE and the PAA support the relay operation as follows.

When the PRE receives a PANA message from the PaC, it creates a PANA-Relay (PRY) message (see Section 4.1) containing a Relayed-Message AVP (see Section 5.2) and a PaC-Information AVP (see Section 5.1). The Relayed-Message AVP encapsulates the entire PANA Message received from the PaC. The PaC-Information AVP contains the PaC's IP address and UDP port number. The PRY message is sent to the PAA.

When the PAA receives the PRY message, it retrieves the PaC-originated PANA message from the Relayed-Message AVP and the PaC's IP address and UDP port number from the PaC-Information AVP. The PaC-originated PANA message is processed in the same way as specified in [RFC5191], with the following exceptions:

(a) The IP address and the port number contained in the PaC-Information AVP and the source IP address and UDP port number of the PRE are used to identify the PaC among multiple PANA-Client-Initiation messages sent from different PaCs through the same PRE or sent from more than one PaC with the same the IP address and the port number through different PREs.

(b) The IP address and the port number contained in the PaC-Information AVP are maintained in the PANA session attribute "IP address and UDP port number of the PaC".

(c) The IP address and UDP port number of the PRE is stored in a new PANA session attribute "IP address and UDP port number of the PRE". A PANA session is referred to as a relayed PANA session if this attribute has a non-null value.

When the PAA originates a PANA message for a relayed PANA session, it sends a PRY message to the PRE's IP address and UDP port number. The PRY message includes a Relayed-Message AVP containing the PAA-originated PANA message and also includes a PaC-Information AVP containing the PaC's IP address and UDP port number.

When the PRE receives the PRY message, it retrieves the PAA-originated PANA message from the Relayed-Message and the PaC's IP address and UDP port number from and PaC-Information AVPs. The PAA-originated PANA message is sent to the PaC's IP address and UDP port number.

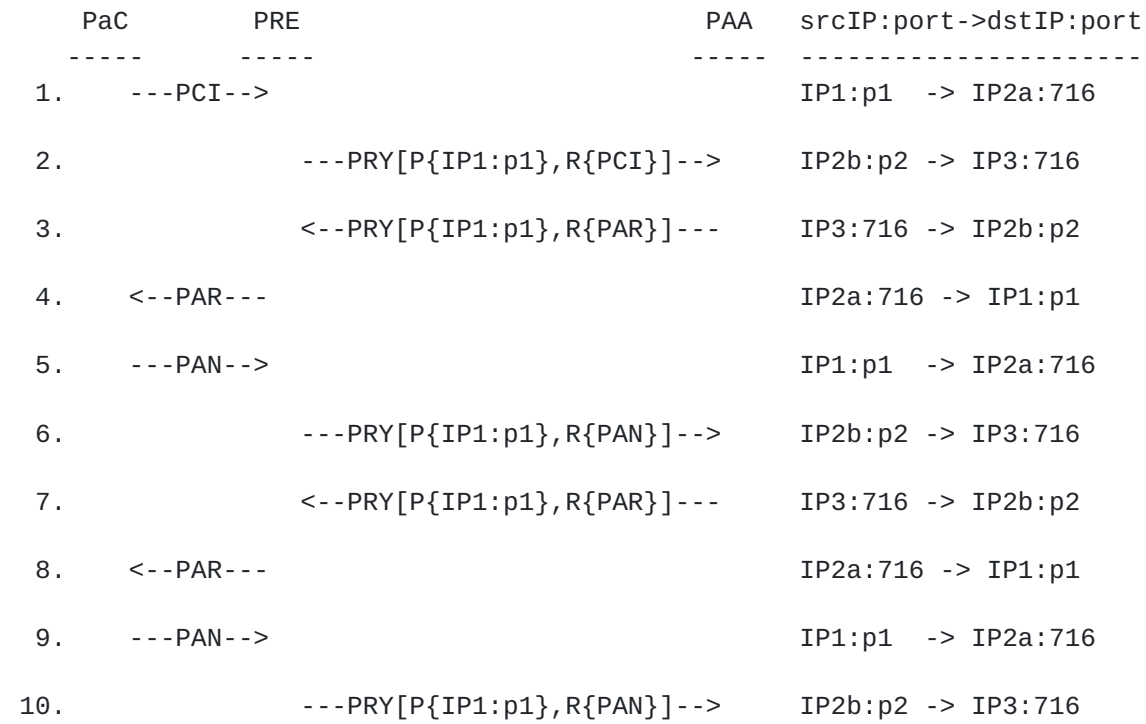
The Session Identifier and Sequence Number of a PRY message are set to zero. A PRY message is never retransmitted by the PRE or the PAA. The PRE and PAA do not advance their incoming or outgoing sequence numbers for request when transmitting or receiving a PRY message. Note that the PANA message carried in a Relayed-Message may be retransmitted by the PaC or PAA, leading to transmission of another PRY carrying the same Relayed-Message.

A PAA that supports this specification MUST be able to process PRY messages for PaC-initiated PANA sessions.

This specification assumes there is at most one PRE between the PaC and the PAA. Performing relay operation on a PANA message that is already relayed (i.e., carried inside a PRY message) is out-of scope

of this specification.

Figure 1 is an example message flow with a PRE.



IP1 is the IP address of PaC.

IP2a and IP2b are the IP addresses of PRE.
IP2a is used for communicating with PaC.
IP2b is used for communicating with PAA.
The two IP address may be the same.

IP3 is the IP address of PAA.

p1 is PaC-assigned UDP port number. p2 is PRE-assigned UDP port number.

P: PaC-Information AVP
R: Relayed-Message AVP

Figure 1: Example Call Message for PANA Relay

3. Security of Messages Sent between PRE and PAA

PREs and PAAs must exchange PRY messages securely. Please see Section 6 for a detailed threat analysis. Required security can be

achieved by using IPsec or another mechanism (e.g., via physical security, cryptographically-secured link-layers, DTLS, etc.). This section describes how IPsec [RFC4301] can be used to handle such threats.

When IPsec is used, each PRE must have an established pairwise trust relationship with a PAA. That is, if messages from a PaC will be relayed by a PRE to a PAA, the PRE and PAA must be configured to use IPsec for the messages they exchange.

PREs and PAAs that support secure PRE to PAA communication use IPsec under the following conditions:

Selectors	PREs are manually configured with the addresses of the PAAs to which PANA messages are to be forwarded. PAAs that will be using IPsec for securing PANA messages must also be configured with a list of the PREs to which messages will be returned. The selectors for the PREs and PAAs will be the pairs of addresses defining PREs and PAAs that exchange PANA messages on the PANA UDP port 716 in their source or destination port.
Mode	PREs and PAAs use transport mode and ESP. The information in PANA messages is not generally considered confidential, so encryption need not be used (i.e., NULL encryption can be used).
Key management	Because the PREs and PAAs are used within an organization, public key schemes are not necessary. Because the PREs and PAA must be manually configured, manually configured key management may suffice, but does not provide defense against replayed messages. Accordingly, IKE with preshared secrets SHOULD be supported. IKE with public keys MAY be supported.
Security policy	PANA messages between PREs and PAAs should only be accepted from PANA peers as identified in the local configuration.
Authentication	Shared keys, indexed to the source IP address of the received PANA message, are adequate in this application.

Availability	Appropriate IPsec implementations are likely to be available for PAAs and for PREs in more featureful devices used in enterprise and core ISP networks. IPsec is less likely to be available for PREs in low end devices primarily used in the home or small office markets.

4. PANA messages for Relay Operation

4.1. PANA-Relay

The PANA-Relay (PRY) message is sent by the PRE to the PAA or by the PAA to the PRE. It contains one PaC-Information AVP and one Relayed-Message AVP. The PRY message SHOULD NOT carry other AVPs.

In a PRE-originated PRY message, the PaC-Information AVP contains an IP address and the UDP port number of the PANA message that was originated by the PaC and is contained in the Relayed-Message AVP.

In a PAA-originated PRY message, the information in the PaC-Information AVP MUST be copied from the "IP address and UDP port number of the PaC" attribute of the associated PANA session [RFC5191].

The Session Identifier and Sequence Number field of any PRY message MUST be set to zero. A PRY message MUST NOT be retransmitted by the PRE or the PAA. The PRE and PAA MUST NOT advance their incoming or outgoing sequence numbers for request when transmitting or receiving a PRY message.

```
PANA-Relay ::= < PANA-Header: 5 >
               { PaC-Information }
               { Relayed-Message }
              *[ AVP ]
```

5. PANA AVPs for Relay Operation

5.1. PaC-Information AVP

The PaC-Information AVP (AVP Code 10) is of type OctetString and contains an IP address (16-octet for an IPv6 address or 4-octet for an IPv4 address) followed by a 2-octet UDP port number of the PaC, both encoded in network-byte order.

5.2. Relayed-Message AVP

The Relayed-Message (AVP Code 11) is of type OctetString and contains a relayed PANA message.

6. Security Considerations

A PRE's main objective is to assist transport of PANA messages between the PaC and the PAA. Relay operation performed between the PRE and the PAA forms an additional logical link for relaying the end-to-end PANA messages between the PaC and the PAA. In that sense, a PRE resembles a bridge or a router that sits between the PaC and the PAA when non-relayed PANA [RFC5191] is used.

A PRE can pose certain threats to the relayed PANA messages. A PRE can delay or drop PANA messages sent by the PaC or the PAA. It can also spoof or modify PANA messages sent towards the PaC or the PAA. These threats are similar to what an on-path bridge/router (i.e., a man-in-the-middle, MitM) can pose to non-relayed PANA. EAP and PANA protocols are designed to operate over unsecure links where aforementioned threats can already exist. Even though these threats cannot be leveraged to gain unauthorized network access, or compromise of cryptographic keys (e.g., MK, MSK, EMSK, etc.), other damages such as preventing authentication to complete, or denial-of service are still possible.

Even though the PRE-to-PAA relay path appears to be a separate additional logical link for transporting the PANA messages, the PRE may pose a few additional risks versus traditional on-path bridges and routers. The following explains the risks and mitigations of PRE as a relay device.

The PRE inserts PaC-Information AVP as the PaC-generated PANA packet is encapsulated in a PRY packet to the PAA. This AVP carries the IP address and the UDP port number values of the PANA packet as sent by the PAC. These values are already carried inside the IP and UDP headers with non-relayed PANA and they are not necessarily secured. EAP and PANA are designed to work in the absence of their protection. Therefore, no additional PANA-layer security is needed when these values are carried as PANA AVPs between the PRE and the PAA. If a future document defines additional payload AVPs for the PRY messages, there may be a need to define additional security for those messages.

A rogue PRE can spoof PANA messages on behalf of a victim PaC and receive the PAA response irrespective of the location of the PRE with respect to the network topology. Achieving the same threat with non-relayed PANA requires the rogue node be a MitM, otherwise the spoofed

packets may be dropped by the ingress filtering network elements, or the responses would be directly sent to the victim PaC IP address and may not be received by the rogue node. Nevertheless, such a rogue PRE cannot perform full initial authentication on behalf of the victim PaC unless it also holds the PaC's credentials (including the master key). Furthermore, any spoofed PANA messages after the initial authentication will fail the integrity checks at the PAA when a key-generating EAP method is used.

The only state that can change on the PAA upon a rogue PRE sending a spoofed PRY is the IP address and UDP port number of the PRE stored as PANA session attributes, which impacts where the PAA sends the next PANA packet (i.e., to the rogue PRE instead of the legitimate PRE). The PAA also needs to handle the PaC-Information AVP in addition to the PaC-originated PANA message carried in the Relayed-Message AVP, so use of the PRE may impose additional storage requirements on the PAA. A rogue PRE generating a valid PANA packet requires it be a MitM in order to synch up with the PANA session state and attributes on the PaC. Such a MitM can already disturb the EAP and PANA even without playing the role of a PRE.

An unauthorized node pretending as PAA can spoof the relayed PANA messages to the PRE in order to get them delivered to the PaC. While the harm caused by such spoofed packets are limited (due to the EAP and PANA design with unsecured network operation in mind), processing of bogus packets can cause processing load on the PaC.

Some of the risks stemming from the aforementioned threats are already handled by the EAP and PANA as described. The residual risks shall be mitigated using additional physical or cryptographic security in the network hosting the PREs and the PAAs. Access control lists implemented on the PRE, PAA, or intermediary firewalls supported by cryptographic or physical authentication/authorization are needed for protecting legitimate PRE and PAAs against rogue ones. Details of the cryptograhpic mechanisms using IPsec are specified in Section 3. Use of manually configured preshared keys for IPsec between PREs and PAAs does not defend against replayed PANA messages.

PREs do not need to maintain per-PaC state, therefore they are robust against resource consumption DoS (Deniable of Service) attacks.

In the relay operation, the IP address of the PAA that is seen by the PaC (i.e., an IP address of the PRE) is different from the IP address of the PAA that is seen by the authentication server. If an EAP channel binding solution uses the IP address of the PAA as part of channel binding parameters, such a solution must take this into account. Note that the same issue arises even when non-relayed PANA is used and the PAA has one IP address configured on its interface

facing the PaC and another IP address on the other interface facing the authentication server.

7. IANA Considerations

As described in Section 4 and Section 5, and following the new IANA allocation policy on PANA messages [RFC5872], one Message Type and two PANA AVP Codes need to be assigned. The following is the requested assignment.

- A Message Type of 5 for PANA-Relay (PRY) message.
- A standard AVP Code of 10 for PaC-Information AVP.
- A standard AVP Code of 11 for Relayed-Message AVP.

8. Acknowledgments

The authors would like to thank Vlad Gherghisan, Shohei Watanabe, Richard Kelsey, Rafa Marin Lopez, Margaret Wasserman and Alan DeKok for valuable comments.

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.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[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

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[I-D.ietf-6lowpan-nd]
Shelby, Z., Chakrabarti, S., and E. Nordmark, "Neighbor Discovery Optimization for Low-power and Lossy Networks", draft-ietf-6lowpan-nd-15 (work in progress), December 2010.

Authors' Addresses

Paul Duffy
Cisco Systems
200 Beaver Brook Road
Boxborough, MA 01719
USA

Email: paduffy@cisco.com

Samita Chakrabarti
Unaffiliated

Email: samitac2@gmail.com

Robert Cragie
Pacific Gas & Electric
Gridmerge Ltd., 89 Greenfield Crescent
Wakefield, WF4 4WA
UK

Email: robert.cragie@gridmerge.com

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

Phone: +81 44 549 2127
Email: yoshihiro.ohba@toshiba.co.jp

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org