DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2007

L. Morand
France Telecom R&D
A. Yegin
Samsung
S. Kumar
Tech Mahindra Ltd
S. Madanapalli
Samsung

December 18, 2006

DHCP options for PANA Authentication Agents
draft-ietf-dhc-paa-option-05

Status of this Memo

Copyright Notice

Abstract

This document defines new DHCPv4 and DHCPv6 options that contain a list of IP addresses to locate one or more of PANA Authentication Agents (PAA). This is one of the methods that a PANA Client (PaC) can use to locate PANA Authentication Agents (PAA).

Table of Contents

1. Introduction

The Protocol for carrying Authentication for Network Access (PANA) [I-D.ietf-pana-pana] defines a new Extensible Authentication Protocol (EAP) [RFC3748] lower layer that uses IP between the protocol end-points.

The PANA protocol is run between a PANA Client (PaC) and a PANA Authentication Agent (PAA) in order to perform authentication and authorization for the network access service.

This document specifies DHCPv4 [RFC2131] and DHCPv6 [RFC3315] options that allow PANA client (PaC) to discover PANA Authentication Agents (PAA). This is one of the methods for locating PAAs.

The DHCP options defined in this document are used only as a PAA discovery mechanism. These DHCP options MUST NOT be used to perform any negotiation on the use of PANA between the PaC and a PAA.

2. 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].

3. Terminology

This document uses the DHCP terminology defined in [RFC2131], [RFC2132] and [RFC3315].

This document uses the PANA terminology defined in [I-D.ietf-pana-pana]. In particular, the following terms are defined:

PANA Client (PaC):

The client side of the protocol that resides in the access device (e.g., laptop, PDA, etc.). It is responsible for providing the credentials in order to prove its identity (authentication) for network access authorization.

PANA Authentication Agent (PAA):

The protocol entity in the access network whose responsibility is to verify the credentials provided by a PANA client (PaC) and authorize network access to the device associated with the client and identified by a Device Identifier (DI).

4. PANA Authentication Agent DHCPv4 Option

This section defines a DHCPv4 option that carries a list of 32-bit (binary) IPv4 addresses indicating one or more PANA Authentication Agents (PAA) available to the PANA client.

The DHCPv4 option for PANA Authentication Agent has the format shown in Fig. 1.

```
    0                   1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  option-code  | option-length |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |
   +      PAA IPv4 Address         +
   |                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             ...               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: PAA DHCPv4 option

```
option-code:        OPTION_PANA_AGENT (TBD)

option-length:      Length of the 'options' field in octets;
                    MUST be a multiple of four (4)

PAA IPv4 Address:   IPv4 address of a PAA for the client to use.
                    The PAAs are listed in the order of preference
                    for use by the client.
```

A PaC (DHCPv4 client) SHOULD request the PAA DHCPv4 Option in a Parameter Request List as described in [RFC2131] and [RFC2132].

If configured with a (list of) PAA address(es), a DHCPv4 server SHOULD send a client with the PAA DHCPv4 option, even if this option is not explicitly requested by the client.

A PaC (DHCPv4 client) receiving the PAA DHCPv4 option SHOULD use the (list of) IP address(es) to locate PAA.

The PaC (DHCPv4 client) MUST try the records in the order listed in the PAA DHCPv4 option received from the DHCPv4 server.

5. PANA Authentication Agent DHCPv6 Option

This section defines a DHCPv6 option that carries a list of 128-bit (binary) IPv6 addresses indicating one or more PANA Authentication Agents (PAA) available to the PANA client.

The DHCPv6 option for PANA Authentication Agent has the format shown in Fig. 2.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       option-code             |       option-length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         PAA IPv6 Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           ....                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: PAA DHCPv6 option

option-code: OPTION_PANA_AGENT (TBD)

option-length: Length of the 'options' field in octets;
MUST be a multiple of sixteen (16)

PAA IPv6 Address: IPv6 address of a PAA for the client to use.
The PAAs are listed in the order of preference
for use by the client.

A PaC DHCPv6 client SHOULD request the PAA DHCPv6 option in an Options Request Option (ORO) as described in the DHCPv6 specification [RFC3315].

If configured with a (list of) PAA address(es), a DHCPv6 server

SHOULD send a client with the PAA DHCPv6 option, even if this option is not explicitly requested by the client.

A PaC (DHCPv6 client) receiving the PAA DHCPv6 option SHOULD use the (list of) IP address(es) to locate PAA.

The PaC (DHCPv6 client) MUST try the records in the order listed in the PAA DHCPv6 option received from the DHCPv6 server.

6. IANA Considerations

The following DHCPv4 option code for PANA Authentication Agent option MUST be assigned by IANA:

Option Name	Value	Described in
OPTION_PANA_AGENT	TBD	Section 4

The following DHCPv6 option code for PANA Authentication Agent options MUST be assigned by IANA:

Option Name	Value	Described in
OPTION_PAA_AGENT	TBD	Section 5

7. Security Considerations

The security considerations in [RFC2131], [RFC2132] and [RFC3315] apply. If an adversary manages to modify the response from a DHCP server or insert its own response, a PANA Client could be led to contact a rogue PANA Authentication Agent, possibly one that then intercepts call requests or denies service.

In most of the networks, the DHCP exchange that delivers the options prior to network access authentication is neither integrity protected nor origin authenticated. Therefore, the options defined in this document MUST NOT be used to perform any negotiation on the use of PANA between the PANA Client and a PANA Authentication Agent. Using the presence (or absence) of these DHCP options as an indication of network mandating PANA authentication (or not) is an example such a negotiation mechanism. This negotiation would allow bidding down attacks by making the clients choose to use a lower-grade security mechanism (or even no security at all).

8. Acknowledgements

We would like to thank to Ralph Droms, Stig Venaas, Ted Lemon, Andre Kostur and Bernie Volz for their valuable comments. We would like to thank also Jari Arkko, Thomas Norten, Bernard Aboba that provided several draft reviews, as well as all members of the PANA and DHC working groups that contribute to improve this document.

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-13 (work in progress), December 2006.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

9.2. Informative References

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

Authors' Addresses

Lionel Morand
France Telecom R&D

Email: lionel.morand@orange-ft.com

Alper E. Yegin
Samsung

Email: alper01.yegin@partner.samsung.com

Suraj Kumar
Tech Mahindra Ltd

Email: surajk@techmahindra.com

Syam Madanapalli
Samsung

Email: syam@samsung.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).