

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 26, 2009

J. Brzozowski
Comcast Cable Communications
T. Lemon
Nominum
G. Hollan
Telus
March 25, 2009

DHCP Authentication Analysis
draft-brzozowski-dhcp-eap-analysis-00

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), 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 September 26, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft

DHCP Authentication Analysis

March 2009

Abstract

This document analyzes and technically evaluate the techniques proposed to support end-user authentication using extensions to DHCP.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	3
2.	Terminology	3
3.	Message and Option Definition	3
3.1.	Message and Option Parity	4
3.2.	Use of Vendor Options and Messages	4
3.3.	Message and Option Sizing	4
3.4.	RADIUS Message Requirments	5
4.	Protocol behavior	5
4.1.	DHCP Clients	5
4.2.	DHCP Relay Agents	6
5.	Compatibility	6
6.	Naming	6
7.	Acknowledgements	7
8.	IANA Considerations	7
9.	Security Considerations	7
10.	References	7
10.1.	Normative References	7
10.2.	Informative References	7
	Authors' Addresses	8

1. Introduction

This document provides an independent analysis of the proposal to support end-user authentication using extension to DHCP. While the current proposal largely focuses on Broadband Digital Subscriber Line scenarios the adhoc team that has been assembled will evaluate the proposal generally from a DHCP point of view. This analysis will also cite architectural and best practice considerations for the authors to consider as part of this work.

1.1. Requirements Language

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 [RFC 2119](#) [[RFC2119](#)].

2. Terminology

The following terms and acronyms are used in this document:

DHCPv4 - "Dynamic Host Configuration Protocol" [[RFC2131](#)]

DHCPv6 - "Dynamic Host Configuration Protocol for IPv6" [[RFC3315](#)]

DHCP - DHCPv4 and/or DHCPv6

3. Message and Option Definition

This section discusses considerations pertaining to how the DHCPEAP messages have been defined in [[I-D.pruss-dhcp-auth-dsl](#)]. This section also makes recommendations as to how messages may be defined.

The draft [[I-D.pruss-dhcp-auth-dsl](#)] specifies two new message types, DHCPEAP-REQ and DHCPEAP-RES, which are the primary DHCP messages

required to support end-user DHCP-based authentication. However, based on the desired protocol behavior and common practices we recommend that additional DHCPEAP message be specified to represent the appropriate interaction between clients, servers, and relay agent, because in some cases the DHCPEAP-REQ and DHCPEAP-RES messages are being overloaded. A four message model would be more in keeping with standard practice as exemplified by the message types defined in [\[RFC3315\]](#).

[3.1.](#) Message and Option Parity

Throughout the document [[I-D.pruss-dhcp-auth-dsl](#)] references to DHCPv4 and DHCPv6 messages and options DHCPv6 are intermingled in ways that are not valid. In some cases, message and option definitions for DHCPv4 or DHCPv6 are omitted entirely. DHCPv4 messages and options must be referenced only for IPv4, and DHCPv6 messages and options must be used only for IPv6, where applicable, to support DHCP-based end-user authentication. Definition of the DHCP Authentication Protocol Option and EAP message option must be clarified and explicitly defined for both DHCPv4 and DHCPv6. Further, the DHCPEAP-REQ and DHCPEAP-RES messages along with any additional messages must be clarified and explicitly defined for both DHCPv4 and DHCPv6.

[3.2.](#) Use of Vendor Options and Messages

Given the very specific target of the proposal-- Broadband Digital Subscriber Line networks--it seems practical for this proposal to use vendor specific options for DHCP options required by the draft, specifically the EAP message option. Furthermore, depending on the availability of support for DHCP Vendor Messages, and its standardization, the use of DHCP vendor message should also be considered as part of this specification for any messages required to support DHCP-based end-user authentication. The use of vendor messages and options should be considered for clients, servers, and relay agents to support the desired protocol behavior.

[3.3.](#) Message and Option Sizing

[I-D.pruss-dhcp-auth-dsl] introduces the EAP message option, which is specified to carry authentication information. This information is necessary to support the desired protocol behavior. However, including this data in a DHCP packet greatly increases the size of the options. [I-D.pruss-dhcp-auth-dsl] does specify how large options are to be handled. However, there are a number of remaining concerns:

The Maximum Message Size option is rarely used by DHCP clients and as such we have no real operational experience to reassure us that DHCP packets larger than 576 bytes will be carried transparently by the infrastructure.

DHCPv4 clients are not required to implement buffers larger than 576 bytes; this draft must explicitly make such a requirement for conforming DHCPv4 clients.

DHCPv4 servers are required not to send DHCP packets to clients that are larger than 576 bytes without prior negotiation with the client.

We have not studied how widespread support for DHCP packets longer than 576 bytes is among deployed DHCP relay agents. We are concerned that some DHCP relay agents will not be capable of relaying such packets, and that this may create obstacles to deploying the proposed protocol extension.

The EAP option may crowd out other options needed by the DHCP client for normal operation.

3.4. RADIUS Message Requirments

Per section 5.1 of [I-D.pruss-dhcp-auth-dsl] RADIUS attributes to support this behavior are required and not included as part of [RFC4014]. These messages do not exists and need to be specified.

4. Protocol behavior

Generally the draft [[I-D.pruss-dhcp-auth-dsl](#)] defines specific protocol behavior to support end-user DHCP-based authentication using IPv4 and IPv6; each are handled independently. [I-D.pruss-dhcp-auth-dsl] is not clear as to how clients and servers handle conflicts where both IPv4 and IPv6 are used simultaneously. The draft should specify how such conflicts are resolved when this situation arises. See section 5 of [[I-D.pruss-dhcp-auth-dsl](#)]

[4.1.](#) DHCP Clients

Packet size for DHCP clients that support end-user DHCP-based authentication remains a concern. DHCP clients MUST advertise their ability to support larger packet sizes. DHCP clients in this case include but are not limited to those included with operating systems and home networking equipment.

The behavior for home gateway (HG) as defined in [I-D.pruss-dhcp-auth-dsl] has been specified. However, specification of standalone client behavior remains absent. In order for this proposal to be complete it must specify how standalone client are to behave to support end-user authentication using DHCP.

if the NAS client indicates to the home gateway (HG) client that DHCP Authentication is supported but in fact does not support it, this will cause the HG client to attempt DHCP Authentication erroneously. The home gateway client's behavior in this case must be specified.

[4.2.](#) DHCP Relay Agents

The impact of the enlarged DHCP packets that contain the DHCP options specified in [[I-D.pruss-dhcp-auth-dsl](#)] specifically the formation and transmission of messages destined for the DHCP server(s) must be considered. DHCP relay agents that support this behavior must be able to generate the appropriate DHCP message types in addition to supporting the necessary options.

[I-D.pruss-dhcp-auth-dsl] proposes that DHCP relay agent will be required to append information to DHCP client requests to support DHCP-based end-user authentication. The current text suggests that [[RFC4014](#)] defines the appropriate attributes that would need to be appended. It is not clear that [[RFC4014](#)] explicitly specifies both the DHCPv4 and DHCPv6 attributes to support this behavior.

[5.](#) Compatibility

The compatibility of clients, servers, and relay agents that implement this behavior with legacy clients, servers, and relay agents MUST be explicitly documented. The behavior of the remaining elements that do not support this behavior while others do MUST be considered, specifically, how will legacy element handle the presence of the corresponding DHCP options when present. Consider the following scenarios, for example:

Only one element among the DHCP client, DHCP server and DHCP relay agent support authentication.

Two of these elements support authentication, one does not.

All three elements support authentication.

[6.](#) Naming

The draft is currently titled "Authentication Extensions for the Dynamic Host Configuration Protocol." This title implies that the draft is a generic authentication extension for DHCP. Despite optimistic suggestions that it might actually turn out to be such a thing, really this proposed extension is fairly sharply targeted. So we recommend choosing a title that reflects this specificity, rather than the current generic title.

[7.](#) Acknowledgements

This template was derived from an initial version written by Pekka Savola and contributed by him to the xml2rfc project.

This document is part of a plan to make xml2rfc indispensable .

8. IANA Considerations

This memo includes no request to IANA.

All drafts are required to have an IANA considerations section (see the update of [RFC 2434](#) [[I-D.narten-iana-considerations-rfc2434bis](#)] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

9. Security Considerations

This draft does not propose the use of [RFC3118](#)-style options. It is possible to use [RFC3118](#) in conjunction with the protocol described in this draft. Indeed, the draft suggests the possibility of bootstrapping the [RFC3118](#) authentication key using the DHCP/EAP protocol. The use cases for that extension are hard to evaluate, so it seems that this draft is neutral toward other DHCP security mechanisms, with one small caveat: since it increases the DHCP message size, it is competing for space in the DHCP packet with other authentication options.

10. References

10.1. Normative References

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

10.2. Informative References

[I-D.narten-iana-considerations-rfc2434bis]
Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs",
[draft-narten-iana-considerations-rfc2434bis-09](#) (work in progress), March 2008.

Pruss, R., Zorn, G., Maglione, R., and Y. Li,
"Authentication Extensions for the Dynamic Host
Configuration Protocol", May 2008.

- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol",
March 1997.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor
Extensions", March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
and M. Carney, "Dynamic Host Configuration Protocol for
IPv6 (DHCPv6)", July 2003.
- [RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the
Dynamic Host Configuration Protocol", November 2002.
- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC
Text on Security Considerations", [BCP 72](#), [RFC 3552](#),
July 2003.

Authors' Addresses

John Jason Brzozowski
Comcast Cable Communications
1360 Goshen Parkway
West Chester, PA 19473
USA

Phone: +1-609-377-6594
Email: john_brzozowski@comcast.com

Ted Lemon
Nominum
USA

Phone:
Email: mellon@nominum.com

Geoffrey Holan
Telus
Canada

Phone:

Email: geoffrey.holan@telus.com

