

dhc
Internet-Draft
Intended status: Informational
Expires: August 8, 2010

J. Brzozowski
Comcast Cable Communications
T. Lemon
Nominum
G. Hollan
Telus
February 4, 2010

DHCP Authentication Analysis
draft-jjmb-dhc-eap-auth-analysis-02

Abstract

This document analyzes and technically evaluates a proposal by Ric Pruss, et al., to implement end-user EAP-based authentication as a part of a DHCP protocol transaction in DSL networks.

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 August 8, 2010.

Copyright Notice

Copyright (c) 2010 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

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

<u>1.</u>	<u>Introduction</u>	<u>3</u>
<u>1.1.</u>	<u>Requirements Language</u>	<u>3</u>
<u>2.</u>	<u>Terminology</u>	<u>3</u>
<u>3.</u>	<u>Message and Option Definition</u>	<u>3</u>
<u>3.1.</u>	<u>Message Type Overloading</u>	<u>3</u>
<u>3.2.</u>	<u>Differences in Message and Option Names</u>	<u>4</u>
<u>3.3.</u>	<u>Message and Option Sizing</u>	<u>4</u>
<u>3.4.</u>	<u>RADIUS Message Requirements</u>	<u>4</u>
<u>4.</u>	<u>Protocol behavior</u>	<u>4</u>
<u>4.1.</u>	<u>DHCP Clients</u>	<u>4</u>
<u>4.1.1.</u>	<u>Packet Size</u>	<u>4</u>
<u>4.1.2.</u>	<u>Standalone Client Behavior</u>	<u>5</u>
<u>4.1.3.</u>	<u>Handling of non-EAP responses</u>	<u>5</u>
<u>4.1.4.</u>	<u>Protocol State Machine is Only in Client</u>	<u>5</u>
<u>4.1.5.</u>	<u>Transaction IDs</u>	<u>6</u>
<u>4.1.6.</u>	<u>EAP Protocol Direction</u>	<u>6</u>
<u>4.1.7.</u>	<u>Reliable Delivery of EAP messages</u>	<u>7</u>
<u>4.1.8.</u>	<u>Re-Authentication</u>	<u>7</u>
<u>4.1.9.</u>	<u>Authorization lifetime versus lease time</u>	<u>7</u>
<u>4.2.</u>	<u>DHCP Servers</u>	<u>7</u>
<u>4.3.</u>	<u>DHCP Relay Agents</u>	<u>8</u>
<u>5.</u>	<u>Compatibility</u>	<u>8</u>
<u>6.</u>	<u>Dual-Stack issues</u>	<u>9</u>
<u>7.</u>	<u>Appropriateness</u>	<u>9</u>
<u>7.1.</u>	<u>Motivation</u>	<u>9</u>
<u>7.2.</u>	<u>Applicability</u>	<u>10</u>
<u>8.</u>	<u>Acknowledgements</u>	<u>10</u>
<u>9.</u>	<u>IANA Considerations</u>	<u>11</u>
<u>10.</u>	<u>Security Considerations</u>	<u>11</u>
<u>11.</u>	<u>References</u>	<u>11</u>
<u>11.1.</u>	<u>Normative References</u>	<u>11</u>
<u>11.2.</u>	<u>Informative References</u>	<u>11</u>

[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:

- o DHCPv4 - "Dynamic Host Configuration Protocol" [[RFC2131](#)] [[RFC2132](#)]
- o DHCPv6 - "Dynamic Host Configuration Protocol for IPv6" [[RFC3315](#)]
- o DHCP - DHCPv4 and/or DHCPv6

[3.](#) Message and Option Definition

In this section considerations pertaining to how the DHCPEAP messages have been defined in [[I-D.pruss-dhcp-auth-dsl](#)] are discussed. Recommendations as to how messages may be defined are also documented in this section.

[3.1.](#) Message Type Overloading

[I-D.pruss-dhcp-auth-dsl] defines a DHCP single EAP message to support end-user DHCP-based authentication. However, the DHC working group has found that using the same DHCP message type for more than one leg of a packet exchange creates confusion, and we recommend instead that a different message type be used for each leg of the transaction. In this case a four message model may better satisfy the requirements, similar, for example, to the DISCOVER/OFFER/REQUEST/ACK cycle in the standard DHCPv4 bootstrapping exchange.

[3.2.](#) Differences in Message and Option Names

[I-D.pruss-dhcp-auth-dsl] mingles DHCPv4 and DHCPv6 message types. This is not valid. DHCPv4 messages and options must be clearly defined and referenced to for IPv4. DHCPv6 messages and options must be defined and referenced for IPv6.

[3.3.](#) Message and Option Sizing

[I-D.pruss-dhcp-auth-dsl] introduces a DHCP Capability Vendor-specific Suboption for DHCPv4 and DHCPv6 which is specified to carry authentication information. This information is required to support the desired protocol behavior. However, including this data in a DHCP greatly increases the size of the DHCP option payload. While [\[I-D.pruss-dhcp-auth-dsl\]](#) specifies how large options are to be handled, this large option payload still has the potential to create problems; there is the potential for this option to squeeze out other DHCP options required for correct DHCP configuration

Additionally, the authors of [\[I-D.pruss-dhcp-auth-dsl\]](#) should mention that in practice the Maximum Message Size option is rarely used by DHCP clients and as such we have no real operational experience that tells us what percentage of relay agents will fail in the face of DHCP packets larger than 576 bytes.

[3.4.](#) RADIUS Message Requirements

[Section 5.1](#) and 5.2 of [\[I-D.pruss-dhcp-auth-dsl\]](#) mention RADIUS attributes required to support this behavior. These are not included

as part of [\[RFC4014\]](#). These messages still need to be specified.

[4.](#) Protocol behavior

[I-D.pruss-dhcp-auth-dsl] requires that end-user DHCP-based authentication must be handled independently in the case where both IPv4 and IPv6 service are present. [\[I-D.pruss-dhcp-auth-dsl\]](#) is not clear as to how clients and servers handle conflicts where both IPv4 and IPv6 are used simultaneously and further how conflicts are resolved when such scenarios arise. See the beginning of section 5 of [\[I-D.pruss-dhcp-auth-dsl\]](#).

[4.1.](#) DHCP Clients

[4.1.1.](#) Packet Size

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, however, this alone will not ensure that intermediate elements like DHCP relay agents will support the same or adversely impact exchanges between DHCP clients and servers. DHCP clients in this case include but are not limited to those include with operating systems and home networking equipment.

[4.1.2.](#) Standalone Client Behavior

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 be specified how standalone client are to behave to support end-user authentication using DHCP.

[4.1.3.](#) Handling of non-EAP responses

Section 5 of [\[I-D.pruss-dhcp-auth-dsl\]](#) also indicates that a client may receive one or more DHCP OFFER/ADVERTISE messages some of which may or may not support DHCP EAP authentication. It is unclear and unspecified how or if the client is to wait for DHCPEAP messages if it has already received a DHCP OFFER or DHCP Advertise message. An EAP-capable client could accept a DHCP OFFER or DHCP Advertise message

and consequently miss a subsequent DHCPEAP message, which would prevent it from authenticating.

This is further complicated in the case where the DHCP client is not a home gateway, and may in fact be a portable device such as a laptop computer. When the DHCP/EAP capable client is connected to a provider network supporting DHCP/EAP, the client may wait for a DHCPEAP message from the server. When the client is connected to some other network, where DHCP/EAP is not supported, it may still wait for such a message. This would create a delay in the availability of the network for the end user when not connecting to the provider network.

4.1.4. Protocol State Machine is Only in Client

[I-D.pruss-dhcp-auth-dsl] proposes that if the relay agent or server decides to do DHCP/EAP, the original DHCPDISCOVER message from the DHCP client will be cached. Once the EAP authentication has succeeded, the DHCPDISCOVER will be forwarded to the server or, in the case where the server does the EAP authentication, the server will take the cached DHCPDISCOVER and send a DHCPOFFER in response to it.

However, this proposal ignores the fact that the DHCP client, not the DHCP server, drives the DHCP protocol. The DHCP client determines when to send the DHCPDISCOVER, and the DHCP server responds. The

DHCP client determines when to send the DHCPREQUEST, and the DHCP server responds. The DHCP client determines when to renew, and so on.

Hence, we strongly recommend that the proposed protocol be changed so that, after a successful DHCP/EAP exchange, the DHCP client restarts its state machine at the INIT state and sends a new DHCPDISCOVER, with a new transaction ID. This eliminates three problems:

- the need for the DHCP server or relay to cache the DHCPDISCOVER
- the problem of how to retransmit if the DHCP server doesn't send a response to the DHCPDISCOVER cached and eventually forwarded by the relay agent

- the problem that the DHCP client state machine would have to remember the xid in the original DHCPDISCOVER packet, even though it's gone through several state transitions since the DHCPDISCOVER was sent.

Needless to say, the same suggestion applies for the DHCPv6 protocol, although the names of the packets are different and DHCPv6 doesn't name the client's states.

[4.1.5.](#) Transaction IDs

The proposed protocol extension does not document the handling of the DHCP client's transaction IDs during the processing of EAP-specific messages. We recommend that each EAP message sourced by the client have a new transaction ID, which should then be returned in the response from the server.

[4.1.6.](#) EAP Protocol Direction

The proposed protocol extension attempts to replace PPPoE/EAP with a new protocol based on DHCP. However, the DHCP protocol is client-initiated, whereas EAP is server-initiated. For example, consider PPP Extensible Authentication Protocol [[RFC3748](#)]. In this document, the authenticator initiates the packet exchange after the layer two (PPPoE) connection is established.

The proposal does not explain how this incompatibility is resolved. Either the proposal needs to turn the DHCP client state machine on its head, or it needs to turn the EAP state machine on its head. The document proposes neither solution, so we can't evaluate the impact the solution to this problem would have on the DHCP protocol.

[4.1.7.](#) Reliable Delivery of EAP messages

The proposal doesn't talk about retransmission for DHCPEAP messages. This is a particularly important omission because of the reversal of roles implicit in doing DHCP over EAP, as discussed in the previous section, "EAP Protocol Direction." Since DHCP is a UDP-based protocol with no guaranteed delivery, retransmission is not optional, and the way in which the DHCP client or EAP authenticator does

retransmission must be specified explicitly, or this proposal does not in any way guarantee interoperability.

[4.1.8.](#) Re-Authentication

The proposal doesn't cover re-authentication. Although [section 2](#), "Problem Statement," mentions user authentication and connection liveness probing, the actual protocol document never proposes a method whereby this requirement is satisfied.

We theorize that it might be possible to somehow accomplish this using DHCPFORCERENEW in DHCPv4 and DHCP Reconfigure in DHCPv6, but nowhere in the document is this solution discussed. So again, there is no way to evaluate how the solution to this problem would interact with DHCP.

[4.1.9.](#) Authorization lifetime versus lease time

The underlying authentication protocol may assign a lifetime to the authorization, after which time the authorization must be renewed. DHCP clients also have a lease interval, which might be different than the authorization interval. The proposal should specify that the lease must expire before the authorization expires, in cases where the authorization expires. The proposal should also cover re-authentication, so that a new authorization with a new expiration is acquired each time the lease is renewed.

[4.2.](#) DHCP Servers

In the DHCP protocol, the state machine is in the client, not the server. The server retains information about the client's IP address allocation, but from the perspective of the protocol, the DHCP server only sends messages in response to messages sent by the DHCP client. So [[I-D.pruss-dhcp-auth-dsl](#)] places a new requirement on DHCP servers that they retain DHCPDISCOVER messages sent by clients during the EAP authentication process. This problem would be solved by following the related recommendations in the earlier section on DHCP clients.

[4.3.](#) DHCP Relay Agents

[I-D.pruss-dhcp-auth-dsl] does not say whether or not the relay agent should append a relay agent information option to EAP-specific messages. We think that a non-EAP-aware relay agent would have to do so, but the draft should talk about this issue.

[I-D.pruss-dhcp-auth-dsl] proposes a mode in which the DHCP relay agent implements the EAP protocol itself, rather than relying on the DHCP server to do so. In order to do this, the relay agent, which in the normal DHCP protocol is completely stateless, must now retain state regarding the progress of the DHCP protocol. There are two different ways in which this protocol extension adds state to the relay agent:

- The relay agent must retain the initial DHCPDISCOVER packet sent by the client.
- Once the EAP authentication has succeeded, the relay agent must remember that the authentication has succeeded, so that if the DHCP client must retransmit its DHCPDISCOVER, the relay agent does not attempt to redo the entire EAP authentication process. This state must be retained for the entire duration of the DHCP protocol from that point on, so that the initial four-way handshake can complete, and so that any subsequent renewals, rebinds, and INIT-REBOOT renewals can complete. In order to avoid caching this state forever, the relay agent would have to retain lease timing information so that it could time out cached information as the leases associated with that information expire.

For this reason, we strongly recommend that the authors abandon the idea of implementing this protocol extension in the relay agent. Also, please note that this is true for the DHCPv6 exchange as well as the DHCPv4 exchange; we only document the DHCPv4 exchange for brevity.

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:

1. DHCP client support for authentication
2. DHCP relay agent support for authentication
3. DHCP server support for authentication
4. DHCP client, server, and relay agent support for authentication

6. Dual-Stack issues

The proposed DHCP extension performs authentication in a way that is linked with the DHCP transaction. The legacy authentication protocol may only support a single authentication per connection. In a dual-stack environment, both the DHCPv4 and DHCPv6 clients might attempt to authenticate. The underlying authentication protocol might then succeed for DHCPv4 and fail for DHCPv6, or vice versa.

The proposal should account for this issue, either specifying that in a dual-stack situation, one or the other DHCP clients should do the authentication, or specifying that this protocol does not work in a dual-stack environment, or specifying how the underlying EAP authentication works in the presence of parallel authentications.

7. Appropriateness

The proposed DHCP extension embeds the network authentication process into the network configuration process, which, it could be argued, goes against the recommendation in Principles of Internet Host Configuration [[RFC5505](#)], which states:

Network access authentication and authorization is a distinct problem from Internet host configuration. Therefore, network access authentication and authorization is best handled independently of the Internet and higher-layer configuration mechanisms.

There are two aspects to this objection. The first is that of course there are reasons why strict adherence to this provision of [RFC5505](#) was not followed. Second, does this provision actually apply?

7.1. Motivation

To address the first point, the motivation stated by the authors for embedding an authentication protocol into a configuration protocol is

essentially economic: it allows ISPs implementing the protocol to continue using network infrastructure they have already deployed and

paid for, while providing a substantial benefit by allowing them to move away from using PPPoE as, essentially, a gatekeeper protocol and toward running native (non-tunneled) IP.

A second motivation is that existing protocols for authenticating at layer two aren't applicable to the DSL environment - 802.1x, for instance, can't work, because the device doing the authentication has no connectivity to the node being authenticated until layer three (IP) configuration has occurred. And yet authentication is required before decisions can be made as to how to configure the client. The DHCPv4 and DHCPv6 protocols provide a mechanism for doing the authentication despite the lack of a layer three configuration.

[7.2.](#) Applicability

As to the question of applicability of the statement in question, it is not really the case that configuration and authentication are being done by the same protocol. Configuration is being done by DHCP. Authentication is being done by EAP. True, DHCP is being used as a transport for the EAP protocol, but it is not the case that DHCP itself is being used for authentication and authorization.

In addition, existing network access authentication protocols that work over layer three do use DHCP to configure the node prior to authentication in cases, such as this, where the authentication agent is not available on the local link.

Once the node is configured, in order to get new DHCP configuration information based on the authentication and authorization results, a second DHCP transaction must be done. In order for this to work, essentially the same mechanisms being proposed in Authentication Extensions for the Dynamic Host Configuration Protocol [[I-D.pruss-dhcp-auth-dsl](#)] are needed - the DHCP server or DHCP relay agent must have access to the results of the authentication. And the DHCP protocol itself provides no mechanism for reconfiguring subsequent to a successful layer three authentication. Hence the difference between such a protocol and the one being proposed is minor, and largely serves to make the configuration/authentication process slower and more awkward.

8. Acknowledgements

Thanks to Alper Yegin, Ric Pruss, Glen Zorn, Alan DeKok, Yoshihiro Ohba, Miles David, Alan Kavanaugh, Steinar Haug and Alfred Hoenes for the review and feedback.

Brzozowski, et al.

Expires August 8, 2010

[Page 10]

Internet-Draft

DHCP Authentication Analysis

February 2010

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

The current version of [[I-D.pruss-dhcp-auth-dsl](#)] indicates that [[RFC3118](#)] likely cannot be seamlessly integrated with existing RADIUS-based AAA infrastructure used in Broadband DSL environments. [[I-D.pruss-dhcp-auth-dsl](#)] must elaborate on how DHCP EAP can be secured if not by leveraging [[RFC3118](#)]. While 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. However, existing [[RFC3118](#)] authentication schemes use relatively short signatures and keys, so in practice this is probably not a serious concern.

11. References

11.1. Normative References

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

11.2. Informative References

[[I-D.pruss-dhcp-auth-dsl](#)]
Pruss, R. and G. Zorn, "EAP Authentication Extensions for

the Dynamic Host Configuration Protocol for Broadband",
[draft-pruss-dhcp-auth-dsl-06](#) (work in progress),
June 2009.

- [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.
- [RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP
Messages", [RFC 3118](#), June 2001.
- [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.

Brzozowski, et al.

Expires August 8, 2010

[Page 11]

Internet-Draft

DHCP Authentication Analysis

February 2010

- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.
Levkowetz, "Extensible Authentication Protocol (EAP)",
[RFC 3748](#), June 2004.
- [RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication
Dial-In User Service (RADIUS) Attributes Suboption for the
Dynamic Host Configuration Protocol (DHCP) Relay Agent
Information Option", [RFC 4014](#), February 2005.
- [RFC5505] Aboba, B., Thaler, D., Andersson, L., and S. Cheshire,
"Principles of Internet Host Configuration", [RFC 5505](#),
May 2009.

Authors' Addresses

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

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

Ted Lemon
Nominum
USA

Phone:
Email: mellon@nominum.com

Geoffrey Holan
Telus
Canada

Phone:
Email: geoffrey.holan@telus.com