

Network Working Group
Internet-Draft
Updates: [1542](#), [3315](#) (if approved)
Intended status: Standards Track
Expires: October 22, 2016

B. Volz
Cisco Systems
Y. Pal
Cisco Systems, Inc.
April 20, 2016

Security of Messages Exchanged Between Servers and Relay Agents
draft-volz-dhc-relay-server-security-00.txt

Abstract

The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) has no guidance for how to secure messages exchanged between servers and relay agents. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) states that IPsec should be used to secure messages exchanged between servers and relay agents, but does not recommend encryption. And, with recent concerns about pervasive monitoring it is appropriate to provide recommendations for DHCPv4 and also improve the recommendations for DHCPv6. This document updates [RFC1542](#) and [RFC3315](#).

Status of This Memo

This Internet-Draft is submitted 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 October 22, 2016.

Copyright Notice

Copyright (c) 2016 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 Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	Security of Messages Exchanged Between Servers and Relay Agents	3
4.	Security Considerations	4
5.	IANA Considerations	5
6.	Acknowledgments	5
7.	References	5
7.1.	Normative References	5
7.2.	Informative References	6
	Authors' Addresses	6

[1.](#) Introduction

The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) [[RFC2131](#)] and [[RFC1542](#)] has no guidance for how to secure messages exchanged between servers and relay agents. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [[RFC3315](#)] states that IPsec should be used to secure messages exchanged between servers and relay agents, but does not recommend encryption. And, with recent concerns about pervasive monitoring [[RFC7258](#)], it is appropriate to provide recommendations for DHCPv4 and also improve the recommendations for DHCPv6.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

This document uses terminology from [\[RFC1542\]](#), [\[RFC2131\]](#), and [\[RFC3315\]](#).

3. Security of Messages Exchanged Between Servers and Relay Agents

The following text replaces the text in [RFC3315 section 21.1](#) and also applies to DHCPv4 ([RFC1542](#)). This revised text essentially adds encryption. While IPsec is not mandated for relay to relay, relay to server, and server to relay communication, is it highly recommended unless some other security mechanisms are already in place (such as VPN tunnels) that protect this potentially sensitive traffic from pervasive monitoring.

Relay agents and servers that exchange messages securely use the IPsec mechanisms for IPv6 [\[RFC4301\]](#). If a client message is relayed through multiple relay agents, each of the relay agents must have established independent, pairwise trust relationships. That is, if messages from client C will be relayed by relay agent A to relay agent B and then to the server, relay agents A and B must be configured to use IPsec for the messages they exchange, and relay agent B and the server must be configured to use IPsec for the messages they exchange.

Selectors	Relay agents are manually configured with the addresses of the relay agent or server to which DHCP messages are to be forwarded. Each relay agent and server that will be using IPsec for securing DHCP messages must also be configured with a list of the relay agents to which messages will be returned. The selectors for the relay agents and servers will be the pairs of addresses defining relay agents and servers and the direction of DHCP message exchange on DHCPv4 UDP port 67 or DHCPv6 UDP port 547.
-----------	---

Mode	Relay agents and servers MUST use IPsec in transport mode and Encapsulating Security Payload (ESP).
------	---

Encryption and authentication algorithms

This document recommends combined mode algorithms for ESP authenticated encryption, ESP encryption algorithms, ESP authentication algorithms as per [section 2.1](#), 2.2, 2.3 of [\[RFC7321\]](#) respectively for data encryption and authentication.

Key management	Because the relay agents and servers are used within an organization, public key schemes are not necessary. Because the relay agents and servers 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	DHCP messages between relay agents and servers should only be accepted from DHCP peers as identified in the local configuration.
Authentication	Shared keys, indexed to the source IP address of the received DHCP message, are adequate in this application.
Availability	Appropriate IPsec implementations are likely to be available for servers and for relay agents in more full featured devices used in enterprise and core ISP networks. IPsec is less likely to be available for relay agents in low end devices primarily used in the home or small office markets.

4. Security Considerations

This entire document is about security considerations and thus there is little else to add in this particular section.

As this document addresses securing messages exchanged between relay agents and servers, the message exchanges between clients and the first hop relay agent or server are not secured. Clients may follow the recommendations in [\[I-D.ietf-dhc-anonymity-profile\]](#) to minimize what information they expose or make use of [\[I-D.ietf-dhc-sedhcpv6\]](#) to secure communication between the client and server.

As mentioned in [\[RFC4552\] section 14](#), the following are known limitations of the usage of manual keys:

- o As the sequence numbers cannot be negotiated, replay protection cannot be provided. This leaves DHCP insecure against all the attacks that can be performed by replaying DHCP packets.
- o Manual keys are usually long lived (changing them often is a tedious task). This gives an attacker enough time to discover the keys.

It should be noted if the recommendations in this document are followed, while the DHCP traffic on the wire between relays and servers is encrypted, the unencrypted data may still be available through other attacks on the DHCP servers, relays, and related systems. Securing these systems and the data in databases and logs also needs to be considered - on the systems themselves and if transferred over a network (i.e., to network attached storage, for backups, or to operational support systems).

5. IANA Considerations

This document has no requests of the fantastic IANA team.

6. Acknowledgments

The motivation for this document was several IESG discusses on recent DHCP relay agent options.

Thanks to Kim Kinnear for reviewing early drafts and helping to improve the document. And, thanks to the authors of [[RFC3315](#)] for the original [Section 21.1](#) text.

7. References

7.1. Normative References

- [RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", [RFC 1542](#), DOI 10.17487/RFC1542, October 1993, <<http://www.rfc-editor.org/info/rfc1542>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), DOI 10.17487/RFC2131, March 1997, <<http://www.rfc-editor.org/info/rfc2131>>.

- [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), DOI 10.17487/RFC3315, July 2003, <<http://www.rfc-editor.org/info/rfc3315>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.
- [RFC7321] McGrew, D. and P. Hoffman, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", [RFC 7321](#), DOI 10.17487/RFC7321, August 2014, <<http://www.rfc-editor.org/info/rfc7321>>.

7.2. Informative References

- [I-D.ietf-dhc-anonymity-profile]
Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity profile for DHCP clients", [draft-ietf-dhc-anonymity-profile-08](#) (work in progress), February 2016.
- [I-D.ietf-dhc-sedhcpv6]
Jiang, S., Li, L., Cui, Y., Jinmei, T., Lemon, T., and D. Zhang, "Secure DHCPv6", [draft-ietf-dhc-sedhcpv6-11](#) (work in progress), March 2016.
- [RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", [RFC 4552](#), DOI 10.17487/RFC4552, June 2006, <<http://www.rfc-editor.org/info/rfc4552>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), DOI 10.17487/RFC7258, May 2014, <<http://www.rfc-editor.org/info/rfc7258>>.

Authors' Addresses

Bernie Volz
Cisco Systems, Inc.
1414 Massachusetts Ave
Boxborough, MA 01719
USA

Email: volz@cisco.com

Yogendra Pal
Cisco Systems, Inc.
Cessna Business Park,
Varthur Hobli, Outer Ring Road,
Bangalore, Karnataka 560103
India

Email: yogpal@cisco.com