            Security of Messages Exchanged between Servers and Relay Agents

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 require
   encryption. With recent concerns about pervasive monitoring and
   other attacks, it is appropriate to require securing relay-to-relay
   and relay-to-server communication for DHCPv6 and relay-to-server
   communication for DHCPv4.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc8213.

Table of Contents

1. Introduction

   The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) [RFC2131]
   and the Bootstrap Protocol [RFC1542] have 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. With
   recent concerns about pervasive monitoring [RFC7258], it is
   appropriate to require use of IPsec with encryption for relay-to-
   server communication for DHCPv4 and require use of IPsec with
   encryption for relay-to-relay and relay-to-server communication for
   DHCPv6.

   This document specifies the optional requirements for relay agent and
   server implementations to support IPsec authentication and encryption
   and recommends that operators enable this IPsec support.

2. Requirements Language and 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 BCP
   14 [RFC2119] [RFC8174] when, and only when, they appear in all
   capitals, as shown here.

   This document uses terminology from [RFC1542], [RFC2131], and
   [RFC3315].

3. Security of Messages Exchanged between Servers and Relay Agents

   For DHCPv6 [RFC3315], this specification REQUIRES relay and server
   implementations to support IPsec encryption of relay-to-relay and
   relay-to-server communication as documented below. The remainder of
   this section replaces the text in Section 21.1 of [RFC3315] when this
   specification is followed.

   For DHCPv4 [RFC2131], this specification REQUIRES relay and server
   implementations to support IPsec encryption of relay-to-server
   communication as documented below.

   This specification RECOMMENDS that operators enable IPsec for this
   communication.

   By using IPsec with encryption for this communication, potentially
   sensitive client message and relay included information, such as the
   DHCPv4 Relay Agent Information option (82) [RFC3046], vendor-specific
   information (for example, the options defined in [CableLabs-DHCP]),
   and Access-Network-Identifier option(s) [RFC7839], are protected from
   pervasive monitoring and other attacks.

   Relay agents and servers MUST be able to exchange messages using the
   IPsec mechanisms described in [RFC4301] with the conditions below.
   If a client message is relayed through multiple relay agents (relay
   chain), 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.

Relay agents and servers use IPsec with the following conditions:

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 use Encapsulating Security Payload (ESP).

Encryption and authentication algorithms
                  This document REQUIRES combined mode algorithms for
                  ESP authenticated encryption, ESP encryption
                  algorithms, and ESP authentication algorithms as per
                  Sections 2.1, 2.2, and 2.3 of [RFC7321],
                  respectively. Encryption is required as relay
                  agents may forward unencrypted client messages as
                  well as include additional sensitive information,
                  such as vendor-specific information (for example,
                  the options defined in [CableLabs-DHCP]) and the
                  Access-Network-Identifier Option defined in
                  [RFC7839].

Key management   Because both relay agents and servers tend to be
                  managed by a single organizational entity, public
                  key schemes MAY be optional. Manually configured
                  key management MAY suffice but does not provide
                  defense against replayed messages. Accordingly,
                  Internet Key Exchange Protocol Version 2 (IKEv2)
                  [RFC7296] with pre-shared secrets SHOULD be
                  supported. IKEv2 with public keys MAY be supported.
                  Additional information on manual vs. automated key
                  management and when one should be used over the
                  other can be found in [RFC4107].

Security policy   DHCP messages between relay agents and servers MUST
                  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.

Note: As using IPsec with multicast has additional complexities (see [RFC5374]), relay agents SHOULD be configured to forward DHCP messages to unicast addresses.

4. Security Considerations

The security model specified in this document is hop by hop. For DHCPv6, there could be multiple relay agents between a client and server, and each of these hops needs to be secured. For DHCPv4, there is no support for multiple relays.

As this document only mandates 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 [RFC7844] to minimize what information they expose or make use of secure DHCPv6 [SEC-DHCPv6] to secure communication between the client and server.

As mentioned in Section 14 of [RFC4552], 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 that if the requirements 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 both the systems themselves and when transferred over a network (i.e., to network attached storage for backups or to operational support systems).

Use of IPsec as described herein is also applicable to Lightweight DHCPv6 Relay Agents [RFC6221], as they have a link-local address that can be used to secure communication with their next-hop relay(s).

5. IANA Considerations

This document makes no request of IANA.

6. References

6.1. 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>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <http://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

   [CableLabs-DHCP]
              CableLabs, "CableLabs' DHCP Options Registry",
              <https://apps.cablelabs.com/specification/CL-SP-CANN-DHCP-
              Reg>.

   [RFC3046] Patrick, M., "DHCP Relay Agent Information Option",
              RFC 3046, DOI 10.17487/RFC3046, January 2001,
              <http://www.rfc-editor.org/info/rfc3046>.

   [RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic
              Key Management", BCP 107, RFC 4107, DOI 10.17487/RFC4107,
              June 2005, <http://www.rfc-editor.org/info/rfc4107>.

   [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>.

   [RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast
              Extensions to the Security Architecture for the Internet
              Protocol", RFC 5374, DOI 10.17487/RFC5374, November 2008,
              <http://www.rfc-editor.org/info/rfc5374>.

   [RFC6221] Miles, D., Ed., Ooghe, S., Dec, W., Krishnan, S., and A.
              Kavanagh, "Lightweight DHCPv6 Relay Agent", RFC 6221,
              DOI 10.17487/RFC6221, May 2011,
              <http://www.rfc-editor.org/info/rfc6221>.

   [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>.

   [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
              Kivinen, "Internet Key Exchange Protocol Version 2
              (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October
              2014, <http://www.rfc-editor.org/info/rfc7296>.

   [RFC7839] Bhandari, S., Gundavelli, S., Grayson, M., Volz, B., and
              J. Korhonen, "Access-Network-Identifier Option in DHCP",
              RFC 7839, DOI 10.17487/RFC7839, June 2016,
              <http://www.rfc-editor.org/info/rfc7839>.

   [RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity
              Profiles for DHCP Clients", RFC 7844,
              DOI 10.17487/RFC7844, May 2016,
              <http://www.rfc-editor.org/info/rfc7844>.

   [SEC-DHCPv6]
              Li, L., Jiang, S., Cui, Y., Jinmei, T., Lemon, T., and D.
              Zhang, "Secure DHCPv6", Work in Progress,
              draft-ietf-dhc-sedhcpv6-21, February 2017.

Authors' Addresses

   Bernie Volz
   Cisco Systems, Inc.
   1414 Massachusetts Ave
   Boxborough, MA 01719
   United States of America

   Email: volz@cisco.com

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

   Email: yogpal@cisco.com