DHC
Internet-Draft
Expires: November 27, 2005

R. Droms
Cisco Systems, Inc.

May 26, 2005

Authentication of DHCP Relay Agent Options Using IPsec
draft-ietf-dhc-relay-agent-ipsec-02.txt

Status of this Memo

This Internet-Draft will expire on November 27, 2005.

Copyright Notice

Abstract

The DHCP Relay Agent Information Option (RFC 3046) conveys information between a DHCP relay agent and a DHCP server. This specification defines a mechanism for securing the messages exchanged between a relay agent and a server using IPsec (RFC 2401).

1. DHCP Terminology

This document uses the terms "DHCP server" (or "server") and "DHCP client" (or "client") as defined in RFC 2131. The term "DHCP relay agent" refers to a "BOOTP relay agent" as defined in RFC 2131.

2. Introduction

DHCP (RFC 2131 [5]) provides IP addresses and configuration information for DHCP clients. It includes a relay agent capability (RFC 951 [6], RFC 1542 [7]), in which processes within the network infrastructure receive broadcast messages from clients and forward them to servers as unicast messages. In network environments like DOCSIS data-over-cable and xDSL, for example, it has proven useful for the relay agent to add information to the DHCP message before forwarding it, using the relay agent information option, RFC 3046 [1]. The kind of information that a relay agent adds is often used in the server's decision making about the addresses and configuration parameters that the client should receive. The way that the relay agent data is used in server decision-making tends to make that data very important, and highlights the importance of the trust relationship between the relay agent and the server.

The existing DHCP Authentication specification (RFC 3118) [8] only secures communication between the DHCP client and server. Because relay agent information is added after the client has signed its message, the DHCP Authentication specification explicitly excludes relay agent data from that authentication.

The goals of this specification is to define a method that a relay agent can use to:

1. protect the integrity of the data that the relay adds
2. provide replay protection for that data
3. leverage the existing IPsec mechanism

3. Deployment of Relay Agents in a DHCP Service

DHCP relay agents forward messages between DHCP clients and DHCP servers, so that the DHCP service can be provided without requiring a DHCP service on each network segment. Usually, there is a DHCP relay agent on the same network segment as the client, and the relay agent forwards messages directly between the client and DHCP server, as illustrated in Figure 1.

```
                                         ______
                  _____                 /      \
      +------+   /     \   +--------+  /        \   +------+
      | DHCP |--|Network|--| Relay |--| internet |--| DHCP |
      |client|  |Segment|  |Agent A|   \        /   |server|
      +------+   \_____/   +--------+   \______/    +------+
   .
```

Deployment of a DHCP relay agent to forward messages between a DHCP client and a DHCP server

Figure 1

In some deployments, there may be more than one relay agent between the DHCP client and server. In Figure 2, relay agent A is configured to forward DHCP messages to relay agent B. Relay agent B is configured to forward DHCP messages to relay agent C, which is, in turn, configured to forward DHCP messages to the DHCP server

In the case where multiple relay agents are deployed between the DHCP client and server, the responses from the server to the client are sent directly to the relay agent closest to the DHCP client. In Figure 2, the DHCP server will send its responses to the DHCP client directly to relay agent A.

```
                                         ______
                  _____                 /      \
      +------+   /     \   +-------+   /        \
      | DHCP |--|Network|--| Relay |--| internet |
      |client|  |Segment|  |Agent A|   \        /
      +------+   \_____/   +-------+    \______/
                                            |
                                            |
                                        +-------+
                                        | Relay |
                                        |Agent B|
                                        +-------+
                                            |
                                         ______
                                        /      \
                                       /        \
                                      | internet |
                                       \        /
                                        \______/
                                            |
                                        +-------+
                                        | Relay |
                                        |Agent C|
                                        +-------+
                                            |
                                         ______
                                        /      \
                                       /        \
                                      | internet |
                                       \        /
                                        \______/
                                            |
                                        +-------+
                                        | Relay |
                                        |Agent D|
                                        +-------+
                                            |
                                         ______
                                        /      \
                                       /        \   +------+
                                      | internet |--| DHCP |
                                       \        /   |server|
                                        \______/    +------+
```

Deployment of multiple relay agents between a DHCP client and server

Figure 2

4. Relay Agent Message Threat Model

DHCP messages are forwarded by DHCP relay agents between DHCP clients and DHCP servers. The messages exchanged between relay agents and servers, in addition to carrying the contents of the messages between the clients and server, may carry additional information in relay agent information options. The information in the relay agent information options may be used by the relay agent, for example to track the physical interface to which a DHCP client is attached, and by the server, for example to affect the selection of an IP address and other configuration information to be assigned to the client.

Because the information carried in the relay agent information option may affect the behavior of relay agents and servers, operation of a DHCP service may be disrupted through malicious attacks on DHCP messages carrying relay agent information options.

The attacks available to a malicious attacker through the relay information option include inserting new relay information options, modifying the contents of existing relay information options or deleting relay information options. There is no attack available through examining the contents of relay information options so there is no requirement for privacy of the contents of relay information options.

A malicious attacker might mount the following denial of service attacks against a DHCP client:

- Change the contents of the Agent Circuit ID sub-option or the Agent Remote ID sub-option [1], causing the relay agent to be unable to return DHCP messages from the server to the client
- Change the contents of the DOCSIS Device Class sub-option [9], causing the DHCP server to provide incorrect configuration parameters to a DOCSIS device
- Change the contents of the Link Selection sub-option [10], causing the DHCP server to assign an IP address from an incorrect subnet to the DHCP client

In some networks, hosts are assigned to different VLANs that provide different types of access to the network depending on the identity of the host or the user of that host. For example, a host might be assigned to an internal company VLAN or an isolated VLAN that provides only external Internet access depending on the identity of the host. A malicious attacker might mount the following attacks designed to gain unauthorized network access:

- Change the contents of the Link Selection sub-option to cause the DHCP client to be assigned an IP address from an inappropriate VLAN

- Change the contents of the RADIUS Attributes sub-option [11] to cause the DHCP client to be authorized to access inappropriate network resources
- Replay an earlier DHCP message that contained a valid RADIUS Attributes sub-option to cause the DHCP client to be authorized to access inappropriate network resources

5. Use of IPsec to secure DHCP messages

Relay agents and servers can use IPsec mechanisms [2] to exchange messages securely as described in this section. If there is a single relay agent between the DHCP client, there is an IPsec trust relationship established between the relay agent and the DHCP server. In Figure 1, relay agent A and the DHCP server must have an IPsec session through which DHCP messages are exchanged.

If a client message is relayed through multiple relay agents, there are independent, pairwise IPsec sessions among the relay agents. In a deployment with multiple relay agents, the relay agents are assumed to belong to a single administrative domain or otherwise have the ability to establish IPsec sessions. For example, in Figure 2, there must be an IPsec session between pairs of relay agents A and B, B and C, and C and D. There must also be be a IPsec session between relay agent D and the DHCP server. In addition, there must be an IPsec session between the DHCP server and relay agent A, for messages that will be returned from the server directly to relay agent A.

Relay agents and servers that support secure relay agent to server or relay agent to relay agent communication use IPsec under 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 that exchange DHCP messages on the DHCP UDP ports 67 and 68.

Mode: Relay agents and servers use transport mode and ESP [3]. The information in DHCP messages is not generally considered confidential, so encryption need not be used (i.e., NULL encryption can be used).

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, if replay protection is required, IKE [4] with preshared secrets must be used. IKE with public keys may be used.

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 featureful 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.

6. IANA Considerations

There are no IANA considerations for the authentication mechanisms described in this document.

7. Security Considerations

The threat model for messages exchanged between DHCP relay agents and DHCP servers is described in Section 4. In Section 5, this specification describes a mechanism that can be used to provide authentication and message integrity protection to the messages between DHCP relay agents and DHCP servers.

The use of IPsec for securing relay agent options in DHCP messages requires:

- o the existence of an IPsec implementation available to the relay agents and DHCP servers
- o that the DHCP relay agents and servers be under appropriate administrative control so that IPsec sessions can be established among the relay agents and servers
- o manual configuration of the participants, including manual distribution of key

The dhc WG has developed two documents describing authentication of DHCP relay agent options to accommodate the requirements of different deployment scenarios: this document and "The Authentication Suboption for the DHCP Relay Agent Option" [12]. In deployments where IPsec is readily available and pairwise keys can be managed efficiently, the use of IPsec as described in this document may be appropriate. If IPsec is not available or there are multiple relay agents for which multiple keys must be managed, the protocol described in "The Authentication Suboption for the DHCP Relay Agent Option" may be appropriate. As is the case whenever two alternatives are available,

local network administration can choose whichever is more appropriate. Because the relay agents and the DHCP server are all in the same administrative domain, the appropriate mechanism can be configured on all interoperating DHCP server elements.

8. Acknowledgments

The need for this specification was made clear by comments made by Thomas Narten and John Schnizlein at IETF 53.

9. References

9.1 Normative references

[1] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[2] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[4] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

9.2 Informative References

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

[6] Croft, B. and J. Gilmore, "Bootstrap Protocol", RFC 951, September 1985.

[7] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.

[8] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[9] Jones, D. and R. Woundy, "The DOCSIS (Data-Over-Cable Service Interface Specifications) Device Class DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Sub-option", RFC 3256, April 2002.

[10] Kinnear, K., Stapp, M., Johnson, R., and J. Kumarasamy, "Link Selection sub-option for the Relay Agent Information Option for DHCPv4", RFC 3527, April 2003.

[11] Droms, R. and J. Schnizlein, "RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option", draft-ietf-dhc-agentopt-radius-08 (work in progress), September 2004.

[12] Stapp, M. and T. Lemon, "The Authentication Suboption for the DHCP Relay Agent Option", draft-ietf-dhc-auth-suboption-05 (work in progress), August 2004.

Author's Address

Ralph Droms
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: +1 978.936.1674
Email: rdroms@cisco.com

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.