DHC Working Group M. Stapp
Internet-Draft Cisco Systems, Inc.
Expires: December 22, 2002 T. Lemon
Nominum, Inc.
June 23, 2002

The Authentication Suboption for the DHCP Relay Agent Option
<draft-ietf-dhc-auth-suboption-00.txt>

Status of this Memo

Copyright Notice

Abstract

The DHCP Relay Agent Information Option RFC3046[1] conveys information between a DHCP Relay Agent and a DHCP server. This specification defines a new authentication suboption for that option which supports source entity authentication and data integrity for that option. The authentication suboption contains a payload derived from the option used in DHCP Authentication RFC3118[2].

Table of Contents

1. Terminology

1.1 Requirements Terminology

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[3].

1.2 DHCP Terminology

DISCUSSION:
Is there anything that should go here, or do we think that readers will be sufficiently familiar with DHCP?

2. Introduction

DHCP (RFC2131[4]) provides IP addresses and configuration information for IPv4 clients. It includes a relay-agent capability, 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 DSL, it has proven useful for the relay agent to add information to the DHCP message before forwarding it, using the relay-agent information option, RFC3046[1]. The kind of information that relays add 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[2] specification only covers communication between the DHCP client and server. Because relay-agent information is added after the client has signed its message, the DHCP Authentication specification explictly excludes relay-agent data from that authentication.

The goals of this specification are:

1. to define a method that a relay-agent can use to protect the integrity of the data that the relay adds
2. to provide replay protection for that data
3. to leverage the mechanisms that DHCP Authentication specifies in order to leverage the security review and implementation code-base of that specification.

In order to meet these goals, we specify a new relay-agent suboption, the Authentication suboption. The format of this suboption is very similar to the DHCP Authentication option's format, and the specification of the cryptographic methods and

signature computation for the suboption are inherited from that option.

The Authentication suboption is included by relay agents who wish to ensure the integrity of the data they include in the Relay Agent option. These relay agents are configured with the parameters necessary to generate cryptographically strong signatures of the data in the DHCP messages which they forward to DHCP servers. A DHCP server configured to process the Authentication suboption uses the information in the suboption to validate the signature in the suboption, and continues processing the packet only if the signature is valid. If the DHCP server sends a response, it includes an Authentication suboption in its response message, signing the data in its message. Relay agents check the signatures in DHCP server responses and decide whether to forward the responses based on the signatures' validity.

3. Suboption Format

The format of the Authentication suboption is inherited from the DHCP Authentication option.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |    Length     |   Algorithm   |  MBZ  |  RDM  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
    |  Replay Detection (64 bits)                                   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Replay Detection cont.                                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    |                                                               |
    |                  Authentication Information                   |
    |                                                               |
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The code for the suboption is TBD. The length field includes the lengths of the algorithm, RDM, and all subsequent suboption fields in octets.

The Algorithm field defines the algorithm used to generate the authentication information.

The Replay Detection Method (RDM) field defines the method used to generate the Replay Detection Data.

The Reply Detection field contains a value used to detect replays, interpreted according to the RDM.

The Authentication Information field contains the data required to communicate algorithm-specific parameters, as well as the signature. The signature is usually a digest of the data in the DHCP packet computed using the method specified by the Algorithm field.

4. Replay Detection

The replay-detection mechanism is based on the notion that a receiver can determine whether or not a message has a valid replay token value. The default RDM, with value 1, specifies that the Replay Detection field contains an increasing counter value. The receiver associates a replay counter with each sender, and rejects any message containing an authentication suboption with a Replay Detection counter value less than the last valid value. DHCP servers MAY identify relays by giaddr value or by other data in the message (e.g. data in other relay-agent suboptions). Relays identify DHCP servers by source IP address. If the message's replay detection value is valid, and the signature is also valid, the receiver updates the its notion of the last valid replay counter value associated with the sender.

All implementations MUST support the default RDM. Additional methods may be defined in the future, following the process described in Section 10.

Receivers SHOULD perform the replay-detection check before validating the signature. The authentication hash calculation is likely to be much more expensive than the replay-detection value check.

DISCUSSION:
This places a burden on the receiver to maintain some run-time state (the most-recent valid counter value) for each sender, but the number of members in a DHCP agent-server system is unlikely to be unmanageably large.

5. Computing Authentication Information

The Authentication Information field contains a computed signature, generated by the sender. All algorithms are defined to process the data in the DHCP messages in the same way. The sender and receiver compute the signature across a buffer containing all of the bytes in the DHCP message, including the fixed DHCP message header, the DHCP options, and the relay-agent suboption, with the following exceptions. The value of the 'hops' field MUST be set to zero, because its value may be changed in transmission. The value of the

'giaddr' field MUST also be set to all-zeroes because it may be modified in networks where one relay agent adds the relay-agent option but another relay sets 'giaddr' (see RFC3046[1], section 2.1). In addition, because the relay-agent option itself is included in the computation, the 'signature' part of the 'authentication information' field in the Authentication suboption is set to all zeroes. The relay-agent option length, the Authentication suboption length and other Authentication suboption fields are all included in the computation.

All implementations MUST support Algorithm 1, the HMAC-MD5 algorithm. Additional algorithms may be defined in the future, following the process described in Section 10.

5.1 The HMAC-MD5 Algorithm

Algorithm 1 is assigned to the HMAC[5] protocol, using the MD5[6] hash function. This algorithm requires that a shared secret key be configured at the relay agent and the DHCP server. A 32-bit Key Identifier is associated with each shared key, and this identifier is carried in the first 4 bytes of the Authentication Information field of the Authentication suboption. The HMAC-MD5 computation generates a 16-byte signature, which is placed in the Authentication Information field after the Key ID.

The format of the Authentication suboption when Algorithm 1 is used is:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |       34      |0 0 0 0 0 0 0 1|  MBZ  |  RDM  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Replay Detection (64 bits)                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Replay Detection cont.                                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Key ID (32 bits)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                      HMAC-MD5 (128 bits)                      |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The suboption length is 34, the RDM and Replay Detection fields are as specified in Section 4, the Key ID is set by the sender to the ID

of the key used in computing the signature, as an integer value in network byte-order. The HMAC signature follows the Key ID.

The Key ID exists only to allow the sender and receiver to specify a shared secret in cases where more than one secret is in use among a network's relays and DHCP servers. The Key ID values are entirely a matter of local configuration; they only need to be locally unique.

This specification does not define any semantics or impose any requirements on this algorithm's Key ID values.

DISCUSSION:
We specify a four-byte Key ID, following the example of the DHCP Authentication RFC. Other authentication protocols, like DNS TSIG[7], use a key name. A key name is more flexible and potentially more human-readable than a key id. DHCP servers may well be configured to use key names for DNS updates using TSIG, so it might simplify DHCP server configuration if some of the key-management for both protocols could be shared. Should we specify a variable-length Key Name instead of a fixed-length Key ID?

6. Procedures for Sending Messages

6.1 Replay Detection

The sender obtains a replay-detection counter value to use, based on the RDM it is using. If the sender is using RDM 1, the default RDM, the value MUST be greater than any previously-sent value.

6.2 Packet Preparation

The sender sets the 'giaddr' field and the 'hops' field to all zeroes. The sender appends the relay-agent information option to the client's packet, including the Authentication suboption. The sender sets the suboption length, places the Replay Detection value into the Replay Detection field of the suboption, and sets the algorithm to the algorithm number that it is using. If the sender is using HMAC-MD5, it sets the Key ID field to the appropriate value. The sender sets the field which will contain the signature to all zeroes. Other algorithms may specify additional preparation steps.

6.3 Signature Computation

The sender computes the signature across the entire DHCP message, using the algorithm it has selected. The sender places the result of the computation into the signature field of the Authentication suboption.

6.4 Sending the Message

The sender restores the 'hops' field's value, and sends the message.

7. Procedures for Processing Incoming Messages

7.1 Initial Examination

The receiver examines the message, the value of the giaddr field, and determines whether the packet includes the relay-agent information option. The receiver uses its configuration to determine whether it should expect an Authentication suboption. The receiver MAY be configured to drop incoming messages which do not contain a valid relay agent information option and Authentication suboption.

If the receiver determines that the Authentication suboption is present and that it should process the suboption, it uses the data in the message to determine which algorithm, key, and RDM to use in validating the message. If the receiver cannot determine which algorithm, key, and RDM to use, or if it does not support the value indicated in the message, it SHOULD be configured to drop the message. Because this situation could indicate a misconfiguration which could deny service to clients, receivers MAY attempt to notify their administrators or log an error message.

7.2 Replay Detection Check

The receiver examines the RDM field. Receivers MUST discard messages containing RDM values which they do not support. Because this may indicate a misconfiguration at the sender, an attempt SHOULD be made to indicate this condition to the administrator, by incrementing an error counter or writing a log message. If the receiver supports the RDM, it examines the value in the Replay Detection field using the procedures in the RDM and in Section 4. If the Replay value is not valid, the receiver MUST drop the message.

DISCUSSION:
Note that the receiver must not update its notion of the last valid Replay Detection value for the sender at this point. Until the signature has been checked, the Replay Detection field cannot be trusted. If the receiver trusts the Replay Detection value without checking the signature, a malicious host could send a replayed message with a Replay Detection value that was very high, tricking the receiver into rejected legitimate values from the sender.

7.3 Signature Check

The receiver prepares the packet in order to check the signature. The receiver sets the 'giaddr' and 'hops' fields to zero, and sets the signature field of the Authentication suboption to all zeroes. Using the algorithm and key associated with the sender, the receiver computes a hash of the message. The receiver compares the result of its computation with the value sent by the sender. If the signatures do not match, the receiver MUST drop the message. Otherwise, the receiver updates its notion of the last valid Replay Detection value associated with the sender, and processes the message.

8. Relay Agent Behavior

DHCP Relay agents are typically configured with the addresses of one or more DHCP servers. A relay agent which implements this suboption requires an algorithm number for each server, as well as appropriate credentials (i.e. keys) to use. Relay implementations SHOULD support configuration which indicates that all relayed messages should include the authentication suboption. This SHOULD be disabled by default. Relays MAY support configuration that indicates that certain destination servers support the authentication suboption, while other servers do not. Relays MAY support configuration of a single algorithm number and key to be used with all DHCP servers, or they MAY support configuration of different algorithms and keys for each server.

8.1 Sending Messages to Servers

When the relay agent receives a broadcast packet from a client, it determines which DHCP servers (or other relays) should receive copies of the message. If the relay is configured to include the Authentication suboption, it determines which Algorithm and RDM to use, and then it performs the steps in Section 6.

8.2 Receiving Messages from Servers

When the relay agent receives a message, it determines from its configuration whether it expects the message to contain a relay-agent information option and an Authentication suboption. The relay MAY be configured to drop response messages that do not contain the Authentication suboption. The relay then follows the procedures in Section 7.

9. DHCP Server Behavior

DHCP servers may interact with multiple relay agents. Server implementations MAY support configuration that associates the same algorithm and key with all relay agents. Servers MAY support

configuration which specifies the algorithm and key to use with each relay agent individually.

9.1 Receiving Messages from Relay Agents

When a DHCP server which implements the Authentication suboption receives a message, it performs the steps in Section 7.

9.2 Sending Reply Messages to Relay Agents

When the server has prepared a reply message, it uses the incoming request message and its configuration to determine whether it should include a relay-agent information option and an Authentication suboption. If the server is configured to include the Authentication suboption, it determines which Algorithm and RDM to use, and then performs the steps in Section 6.

DISCUSSION:
This server behavior represents a slight variance from RFC3046[1], Section 2.2. The Authentication suboption is not echoed back from the server to the relay: the server generates its own suboption.

10. IANA Considerations

Section 3 defines a new suboption for the DHCP relay-agent option, called the Authentication Suboption. IANA is requested to allocate a new suboption code from the relay-agent option suboption number space.

This specification introduces two new number-spaces for the Authentication suboption's 'Algorithm' and 'Replay Detection Method' fields. These number spaces are to be created and maintained by IANA.

The Algorithm identifier is a one-byte value. Algorithm value 0 is reserved. Algorithm value 1 is assigned to the HMAC-MD5 signature as defined in Section 5.1. Additional algorithm values will be allocated and assigned through IETF consensus, as defined in RFC 2434[8].

The RDM identifier is a four-bit value. RDM value 0 is reserved. RDM value 1 is assigned to the use of a monotonically increasing counter value as defined in Section 4. Additional RDM values will be allocated and assigned through IETF consensus, as defined in RFC 2434[8].

11. Security Considerations

This specification describes a protocol to add source authentication

and message integrity protection to the messages between DHCP relay agents and DHCP servers.

The use of this protocol imposes a new computational burden on relay agents and servers, because they must perform cryptographic hash calculations when they send and receive messages. This burden may add latency to DHCP messages exchanges. Because relay agents are involved when clients reboot, periods of very high reboot activity will result in the largest number of messages which have to be signed and verified. During a cable MSO head-end reboot event, for example, the time required for all clients to be served may increase.

11.1 Protocol Vulnerabilities

Because DHCP is a UDP protocol, messages between relays and servers may be delivered in a different order than the order in which they were generated. The replay-detection mechanism will cause receivers to drop packets which are delivered 'late', leading to client retries. The retry mechanisms which most clients implement should not cause this to be an enormous issue, but it will cause senders to do computational work which will be wasted if their messages are re-ordered.

12. Acknowledgements

The need for this specification was made clear by comments made by Thomas Narten and John Schnizlein, and the use of the DHCP Authentication option format was suggested by Josh Littlefield, at IETF 53.

References

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

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

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

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

[5] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[6] Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321, April 1992.

[7] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[8] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, October 1998.

Authors' Addresses

Mark Stapp
Cisco Systems, Inc.
250 Apollo Dr.
Chelmsford, MA 01824
USA

Phone: 978.244.8498
EMail: mjs@cisco.com

Ted Lemon
Nominum, Inc.

950 Charter St.
Redwood City, CA 94063
USA

EMail: mellon@nominum.com

Full Copyright Statement

Acknowledgement

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