Network Working Group
INTERNET DRAFT
Obsoletes: draft-ietf-dhc-authentication-02.txt

R. Droms, Editor
Bucknell University

November 1996
Expires May 1997

Authentication for DHCP Messages
<draft-ietf-dhc-authentication-03.txt>

Status of this memo

Abstract

The Dynamic Host Configuration Protocol (DHCP) [1] provides a framework for passing configuration information to hosts on a TCP/IP network. In some situations, network administrators may wish to constrain the allocation of addresses to authorized hosts. Additionally, some network administrators may wish to provide for authentication of the source and contents of DHCP messages. This document defines a new DHCP option through which authorization tickets can be easily generated and newly attached hosts with proper authorization can be automatically configured from an authenticated DHCP server.

1. Introduction

DHCP transports protocol stack configuration parameters from centrally administered servers to TCP/IP hosts. Among those parameters are an IP address. DHCP servers can be configured to dynamically allocate addresses from a pool of addresses, eliminating a manual step in configuration of TCP/IP hosts.

Some network administrators may wish to provide authentication of the source and contents of DHCP messages. For example, clients may be subject to denial of service attacks through the use of bogus DHCP servers, or may simply be misconfigured due to unintentionally instantiated DHCP servers. Network administrators may wish to constrain the allocation of addresses to authorized hosts to avoid denial of service attacks in "hostile" environments where the network medium is not physically secured, such as wireless networks or college residence halls.

This document defines a technique that can provide both entity authentication and message authentication.

1.1 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

- "MUST"

  This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.

- "MUST NOT"

  This phrase means that the item is an absolute prohibition of this specification.

- "SHOULD"

  This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

- "SHOULD NOT"

  This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

o "MAY"

This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

1.2 Terminology

This document uses the following terms:

o "DHCP client"

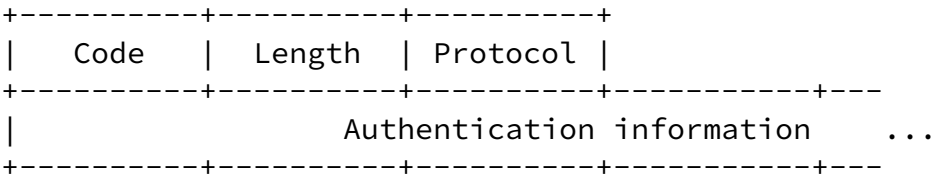
A DHCP client or "client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

o "DHCP server"

A DHCP server of "server"is an Internet host that returns configuration parameters to DHCP clients.

2. Format of the authentication option

The following diagram defines the format of the DHCP authentication option:



The code for the authentication option is TBD, and the length field

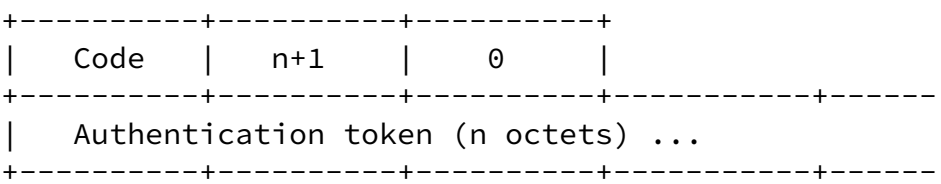
contains the length of the protocol and authentication information fields in octets. The protocol field defines the particular technique for authentication used in the option.

This document defines two protocols in sections 3 and 4, encoded with protocol field values 0 and 1. Protocol field values 2-254 are reserved for future use. Other protocols may be defined according to the procedure described in section 5.

3. Protocol 0

If the protocol field is 0, the authentication information field

holds a simple authentication token:



The authentication token is an opaque, unencoded value known to both the sender and receiver. The sender inserts the authentication token in the DHCP message and the receiver matches the token from the message to the shared token. If the authentication option is present and the token from the message does not match the shared token, the receiver MUST discard the message.

Protocol 0 may be used to pass a plain-text password and provides only weak entity authentication and no message authentication. This protocol is useful for rudimentary protection against, e.g., inadvertently instantiated DHCP servers.

DISCUSSION:

> The intent here is to pass a constant, non-computed token such as a plain-text password. Other types of entity authentication using computed tokens such as Kerberos tickets or one-time passwords will be defined as separate protocols.

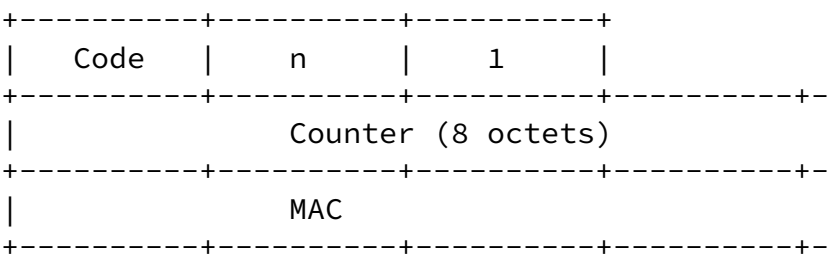
4. Protocol 1

If the protocol field is 1, the authentication information contains an encrypted value generated by the source as a message authentication code (MAC) to provide message authentication and entity authentication.

This technique is based on the HMAC protocol [3] using the MD5 hash {2].

4.1 Format

The format of the authentication information for protocol 1 is:



The following definitions will be used in the description of the authentication information for protocol 1:

K - a secret value shared between the source and destination of the message
Counter - the value of a 64-bit monotonically increasing counter
HMAC-MD5 - the MAC generating function as defined by [3] and [2]

The sender computes the MAC as described in [3]. The 'counter' field

of the authentication option MUST be set to the value of a monotonically increasing counter and the 'MAC' field of the authentication option MUST be set to all 0s for the computation of the MAC. Because a DHCP relay agent may alter the values of the 'giaddr' and 'hops' fields in the DHCP message, the contents of those two fields MUST also be set to zero for the computation of the message digest. Using a counter value such as the current time of day (e.g., an NTP-format timestamp [4]) can reduce the danger of replay attacks.

DISCUSSION:

Protocol 1 specifies the use of HMAC-MD5. Use of a different technique, such as HMAC-SHA, will be specified as a separate protocol.

4.2 Message validation

To validate an incoming message, the receiver checks the 'counter' field and computes the MAC as described in [3]. If the 'counter' field does not contain a value larger than the last value of 'counter' used by the sender, the receiver MUST discard the incoming message. The receiver MUST set the 'MAC' field of the authentication option to all 0s for computation of the MAC. Because a DHCP relay agent may alter the values of the 'giaddr' and 'hops' fields in the DHCP message, the contents of those two fields MUST also be set to

zero for the computation of the MAC. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver MUST discard the DHCP message.

4.3 Key utilization

Each DHCP client has a key, K. The client uses its key to encode any messages it sends to the server and to authenticate and verify any messages it receives from the server. The client's key must be initially distributed to the client through some out-of-band mechanism, and must be stored locally on the client for use in all authenticated DHCP messages. Once the client has been given its key, it may use that key for all transactions even if the client's configuration changes; e.g., if the client is assigned a new network address.

Each DHCP server must know the keys for all authorized clients. If all clients use the same key, clients can perform both entity and message authentication for all messages received from servers. Servers will be able to perform message authentication. To authenticate the identity of individual clients, each client must be configured with a unique key. Appendix A describes a technique for key management.

5. Definition of new authentication protocols

The author of a new DHCP option will follow these steps to obtain acceptance of the option as a part of the DHCP Internet Standard:

1. The author devises the new authentication protocol.
2. The author documents the new protocol as an Internet Draft.
3. The author submits the Internet Draft for review through the IETF standards process as defined in "Internet Official Protocol Standards" (STD 1). The new protocol will be submitted for eventual acceptance as an Internet Standard.
4. The new protocol progresses through the IETF standards process; the new option will be reviewed by the Dynamic Host Configuration Working Group (if that group still exists), or as an Internet Draft not submitted by an IETF working group.

This procedure for defining new authentication protocols will ensure that:

* new options are reviewed for technical correctness and appropriateness, and
* documentation for new options is complete and published.

6. References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 1541, Bucknell University, October 1993.

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

[3] Krawczyk H., M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication" <draft-ietf-ipsec-hmac-md5-01.txt> (work in progress), August 1996.

[4] Mills, D., "Network Time Protocol (Version 3)", RFC-1305, March 1992.

7. Acknowledgments

Jeff Schiller and Christian Huitema developed this scheme during a terminal room BOF at the Dallas IETF meeting, December 1995. The author transcribed the notes from that discussion, which form the basis for this document. The editor appreciates Jeff's and Christian's patience in reviewing this document and its earlier drafts.

Thanks also to John Wilkins, Ran Atkinson and Shawn Mamros for reviewing this document, and to Thomas Narten for reviewing earlier drafts of this document.

8. Security considerations

This document describes authentication and verification mechanisms for DHCP.

9. Author's address

Ralph Droms
Computer Science Department
323 Dana Engineering
Bucknell University
Lewisburg, PA 17837

Phone: (717) 524-1145
EMail: droms@bucknell.edu

Appendix A - Key Management Technique

To avoid centralized management of a list of random keys, suppose K for each client is generated from the pair (client identifier, subnet address), which must be unique to that client. That is, K = MD5(MK, unique-id), where MK is a secret master key and MD5 is some encoding function.

Without knowledge of the master key MK, an unauthorized client cannot generate its own key K. The server can quickly validate an incoming message from a new client by regenerating K from the client-id. For known clients, the server can choose to recover the client's K dynamically from the client-id in the DHCP message, or can choose to precompute and cache all of the Ks a priori.