International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:8, 2007

DHCP Message Authentication with an Effective Key Management

HongIl Ju, and JongWook Han

***Abstract*—**In this paper we describes the authentication for DHCP (Dynamic Host Configuration Protocol) message which provides the efficient key management and reduces the danger replay attack without an additional packet for a replay attack. And the authentication for DHCP message supports mutual authentication and provides both entity authentication and message authentication. We applied the authentication for DHCP message to the home network environments and tested through a home gateway.

***Keywords*—**DHCP, authentication, key management, replay attack, home network.

I. Introduction

IN recent years with the rapid development of the wireless internets and mobile communication systems, the use of notebook computers, PDAs and portable systems is gradually increasing and has become popular. And most of the users may want to access the internet from anywhere in the world. However, when these mobile hosts move from one network to another, users have to change system configuration, including host IP address, default gateway, and name servers. In order to support the automatic configuration changes on these hosts, several technologies such as dynamic host configuration mechanisms or mobility support in the IP layer have been developed[1]. The DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers[2]. The DHCP is an internet protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. Without the DHCP, the IP address must be entered manually at each host in an organization and a new IP address must be entered each time a host moves to a new location on the network.

However, some network administrators may wish to provide authentication of the source and contents of DHCP message during an exchange between a DHCP server and a DCHP client. And they may want 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[1][3]. So, the authentication for DHCP message is necessary securely to assign IP addresses in these environments. The document RFC3118 defines a technique that can provide both entity authentication and message authentication and current security mechanisms for DHCPv4.

Manuscript received August 31, 2005.

Hongll Ju is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-5988; fax: 82-42-860-5611; e-mail: juhong@etri.re.kr).

JongWook Han is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (phone: 82-42-860-4940; fax: 82-42-860-5611; e-mail: hanjw@etri.re.kr).

II. DHCP

The DHCP is an internet protocol for automatically assigning TCP/IP information to computers and other network devices that use the TCP/IP protocol. Client computers configured to use DHCP for IP assignment do not need to have a statically assigned IP address. In addition, they generally do not need to have addresses configured for DNS servers or WINS servers, as these are also set by the DHCP serverPlease submit your manuscript electronically for review as e-mail attachments.

A. DHCP Overview

The DHCP is based on a client-server model and is an extension of an earlier network IP management protocol, BOOTP(Bootstrap Protocol), adding the capability of automatic allocation of reusable network addresses and additional configuration options. And the DHCP provides two services. The first is to provide persistent storage of network parameters for network clients. The model of DHCP persistent storage is that the DHCP service stores a key-value entry for each client, where the key is some unique identifier and the value contains the configuration parameters for the client. The client's unique identifier may be an IP subnet number and a unique identifier within the subnet. The second is the allocation of temporary or permanent network addresses to clients. The allocation mechanism guarantees not to reallocate that address within the requested time and attempts to return the same network address each time the client requests an address. It means that DHCP should not assign the same IP address to more than one host at the same time. And although a host is rebooted, DHCP should maintain the configuration of the host[2].

B. DHCP Mechanism

The DHCP supports three mechanisms for IP address allocation. The first is an automatic allocation method which

assigns a permanent IP address to a client. The second is a dynamic allocation method which assigns an IP address to a client for a limited period of time or until the client explicitly relinquishes the address. The third is a manual allocation method which allows the network administrator to assign an IP address to a client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

The DHCP starts that the client sends to a DHCP server a broadcast request called DHCPDISCOVER message containing their MAC addresses, looking for a DHCP server to answer. After receiving the DHCPDISCOVER message, the server determines an appropriate address (if any) to give to the client according to availability and usage policies set on the server. Then the server temporarily reserves that address for the client and sends back to the client a DHCPOFFER message with an IP address information and other TCP/IP settings that the client can use to communicate on the network. The client sends a DHCPREQUEST message, letting the server know that it intends to use the address. The server sends a DHCPACK message, confirming that the client has been given a lease on the address for a server-specified period of time. Fig.1 shows the timeline diagram of messages exchanged between a DHCP client and servers when allocating a new network address [2].

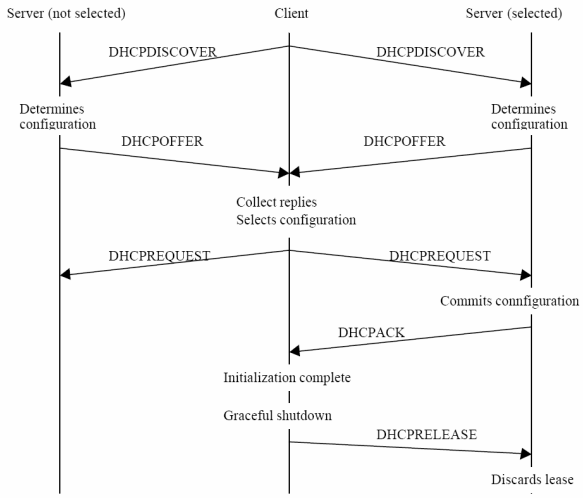

Fig. 1 Timeline diagram of messages exchanged between a DHCP client and servers

If a host uses a static IP address, the host is manually configured to use a specific IP address. One problem with static assignment, which can result from user error or inattention to detail, occurs when two computers are configured with the same IP address. This creates a conflict that results in loss of service. So, the DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, as well as address conflicts caused by a currently assigned IP address accidentally being reissued to another host. And the DHCP provides benefits of the reduced network administration. It means that TCP/IP configuration is centralized and automated, network administrators can centrally define global and subnet-specific TCP/IP configurations and clients can be automatically assigned a full range of additional TCP/IP configuration values by using DHCP options.

III. Authentication of the DHCP Message

Although DHCP servers are critical to the operation of most enterprise networks, DHCP server security is often one of the most overlooked areas of network security. If there is no authentication processing during an DHCP message exchange between a DHCP server and DCHP client, the DHCP server has no way of knowing if the client requesting the address is a legitimate client on the network, and the client has no way of knowing if the DHCP server that assigned the address is a legitimate DHCP server. The possibility of rogue clients and servers on network can create all kinds of problems. For example, the clients may be subject to DoS(Denial of Service) attacks through the use of bogus DHCP servers, or may simply be misconfigured due to unintentionally instantiated DHCP servers[4-5].

A. DHCP Threat

The threat to DHCP is inherently an insider threat. Regardless of the gateway configuration the potential attacks by insiders and outsiders are the same. The attack specific to a DHCP client is the possibility of the establishment of a "rogue" server with the intent of providing incorrect configuration information to the client. And there is another threat to DHCP clients from mistakenly or accidentally configured DHCP servers that answer DHCP client requests with unintentionally incorrect configuration parameters. The threat specific to a DHCP server is an invalid client masquerading as a valid client. The motivation for this may be for "theft of service", or to circumvent auditing for any number of nefarious purposes. The threat common to both the client and the server is the resource DoS attack. These attacks typically involve the exhaustion of valid addresses, or the exhaustion of CPU or network bandwidth, and are present anytime there is a shared resource[3]. Although it is possible to prepare against the DoS attack with limited IP addresses, there is in need of additional authentication mechanism for preparing against the attack of a rogue DHCP server or DHCP client.

B. Authentication Mechanism

In RFC3118, the purpose of the authentication for DHCP message is to protect any interference by malicious hosts and establish secure associations between DHCP servers and clients. In order to validate DHCP message, the receiver checks the MAC(message authentication code) contained in an incoming DHCP message. If the received MAC value does not match the computed MAC value, the receiver discards the following DHCP message. When computing the MAC value, a sender or a receiver uses keyed-hashing for message authentication (HMAC) [5-6]. Fig. 2 shows the procedure of

message exchanged between DHCP clients and a DHCP server and Fig. 3 shows the procedure of message exchanged between a DHCP client and DHCP servers.

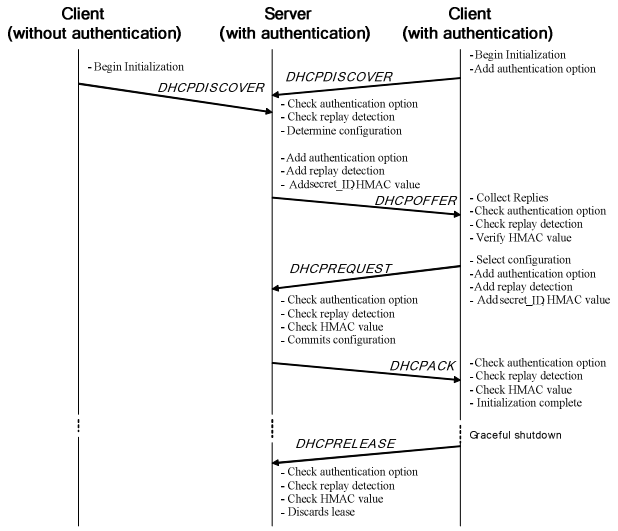

Fig. 2 Timeline diagram of message exchanged between DHCP clients and a DHCP server

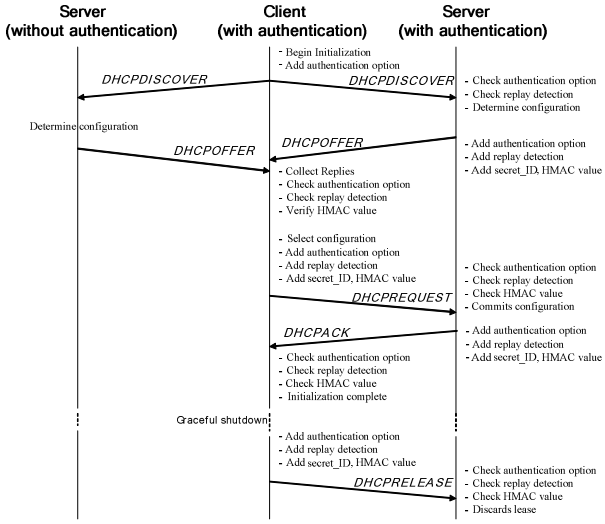

Fig. 3 Timeline diagram of message exchanged between a DHCP client and DHCP servers

In Fig. 2, there are one DHCP server and two DHCP clients. Although several DHCP clients may request the IP address, the DHCP server assigns IP address to only the authenticated DHCP client after authentication procedure. In the contrary fig.3 shows one DHCP client and two DHCP servers. Although several DHCP servers may send a DHCPOFFER message to allocate an IP address, the DHCP client is allocated the IP address by only the authenticated DHCP server after authentication procedure.

IV. Design and Implementation

In this paper we designed and implemented the authentication for DHCP message using keyed one-way function algorithm, HMAC-MD5. And we implemented it in Linux system based on DHCP version 2.0pl5. The authentication method using a HMAC requires a shared secret key for each client on each DHCP server. In other words, each DHCP server has to a shared key for each DHCP client to compute the HMAC of DHCP message. It brings a key management problem of a DHCP server. However, in this paper there is no need the centralized key management in a DHCP server. A DHCP server has only one unique secret master key which can allow to derive all keys for each DHCP client and a DHCP client does not need to have a master key. The unique master key of a DHCP server is generated from the HMAC value which must be unique to that server and generated from server's unique identifier, RN(Random Number) and others. Because a DHCP server has not a shared secret key, if a new client access to a DHCP server, the DHCP server regenerates the shared secret key from a new client identifier and uses to validate an incoming message from a new client. Fig.4 shows processing of message interaction between a DHCP client and a DHCP server with authentication option.

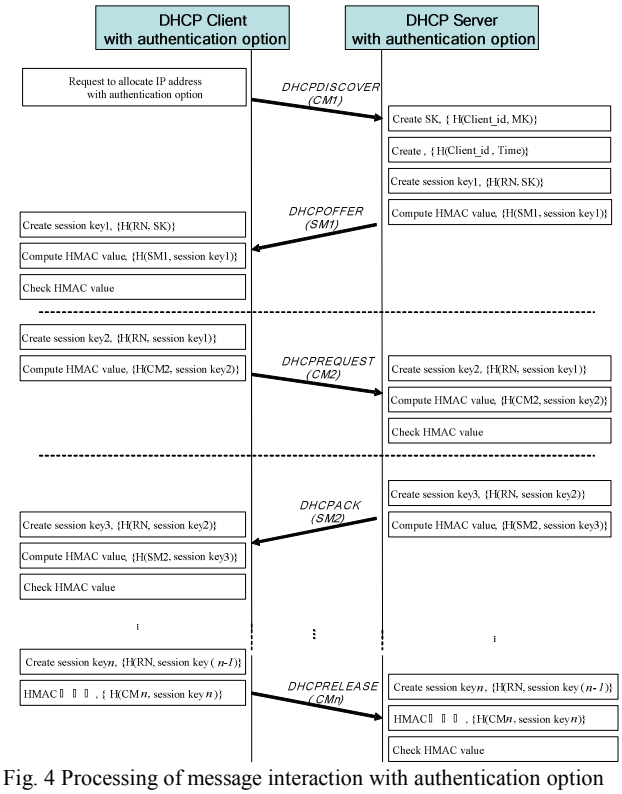

Fig. 4 Processing of message interaction with authentication option

When each DHCP client is registered on DHCP server, a DHDP server issues the shared secret key which is generated from master key of that DHCP server. That is, SK = HMAC (MK, client identifier), where SK is a share secret key and MK

is a master key. Also, each secret key for each client is unique because a client identifier is unique-id. In DHCP message interaction between DHCP servers and clients, the shared secret key is used for generating a new secret session key which generated from the HMAC value of a random number and a shared secret key. That is, Session_Key = HMAC(RN, SK), where RN is random number generated from a client unique identifier, the current access time and others. In addition the generated session key is used only in current transaction, in the next transaction the new session key is generated and used. In other words, the session key is changed in every transaction and generated from the previous session key. Therefore it allows to protect the replay attack without an additional packet for replay attack and an unauthorized client cannot generate the shared secret key without knowledge of the master key.

V. Conclusion

In this paper, we proposed and implemented the authentication for DHCP message which provides the efficient key management and reduces the danger replay attack without an additional packet for a replay attack. And it supports the mutual authentication between a DHCP client and a DHCP server and provides both entity authentication and message authentication. It conforms to RFC3118 which defines current security mechanisms for DHCPv4. And we applied the proposed authentication method for DHCP message to the home network environments and tested through a home gateway. So, this method can be used for the device authentication without an additional authentication methed in home network environments. In future, it is necessary for security mechanisms in DHCPv6.

References

[1] Kaaumasa Kobayashi and Suguru Yamaguchi, “Network Access Control for DHCP Environment”, *INET97 Proceedings*, 1997.
[2] R. Droms, "Dynamic Host Configuration Protocol", *RFC 2131*, March 1997.
[3] R. Droms, W. Arbaugh, "Authentication for DHCP messages", *RFC 3118*, June 2001.
[4] Mitch Tulloch, “DHCP Server Security (Part 1)”, *Articles::Misc Network Security*, Jul 2004.
[5] M. Stapp, T. Lemon, “The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option”, *RFC 4030*, March 2005.
[6] Rivest, R., "The MD5 Message-Digest Algorithm", *RFC 1321*, April 1992.
[7] Krawczyk H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", *RFC 2104*, February 1997.