DHCP working Group
INTERNET DRAFT
July 11, 1997

Baiju V. Patel
Intel Corporation
Expires in 6 months

Securing DHCP

<draft-ietf-dhc-securing-dhc-00.txt >

Status of this Memo

Abstract

This proposal describes methods of securing DHCP based on IETF DHCP and IPSEC protocols. This protocol achieves security goals for DHCP client and servers without having to define a new security protocol. Instead, it first bootstraps the DHCP client in un-trusted mode using existing DHCP protocol and then proceeds to secure configuration of the client using existing DHCP and IP protocol features.

1. Introduction

In this draft, we present a method of securing DHCP protocol

and use notation DHCPSEC for the proposed method. The servers and clients that implement the proposed method are denoted by DHCPSEC servers and clients, respactively.

The objective behind securing DHCP is to securely configure a DHCP client with an IP address(es) and configuration parameters. The DHCPSEC does not protect against an unauthorized client from arbitrarily selecting an address and using it. Instead, if a client obtains IP address(es) and configuration parameters using DHCPSEC protocol, it is assured that the IP address and configurations obtained using DHCPSEC are the ones provided by an authenticated DHCPSEC server and the integrity of the parameters is not compromised by an adversary in the network. The subsequent renewal of the lease, and acquiring of the additional configuration parameters, as well as release of the lease of an address(es) is authenticated as well. Thus, the protocol protects the client from an adversary who may release the lease of its IP address. The DHCPSEC server also authenticates the DHCPSEC clients. This allows an DHCPSEC server to determine if a client should be allocated an address at all, and to help determine configuration parameters for the client. Moreover, it prevents an adversary from renewing or releasing an address assigned to an authorized client.

2. Securing DHCP Protocol

The DHCPSEC is comprised of several phases: 1) start-up phase, 2) trusted configuration phase, 3) trusted renew, and 4) trusted release phase.

2.1. Start-up phase

In start-up phase, the DHCPSEC client brings up an un-trusted configuration using the DHCP protocol defined in

[1]. The configuration supplied by the DHCP server in this phase is the minimal configuration required to execute subsequent phases of the protocol. The server MUST supply an IP address, and optionally, provide default gateway and DNS server information. If the DHCP server is not on the same subnet as the client, the default gateway information MUST be provided. The lease time (configurable) for the IP address should be relatively small for the efficient use of the addresses. The recommended duration of the lease is hundreds of milliseconds.

In many environments, there may be a concern that an adversary may be able to launch a denial of service attack by quickly requesting too many addresses (short lease in this case) and thus denying a legitimate client an IP address. There are several alternatives that may be deployed to protect against some forms of such denial of attacks. For example, if the DHCPSEC server is on the same subnet as the

client, it may allocate a non-routable temporary address to a DHCP client. Since the non-routable address space is large, an authorized client is likely to get an address even when this type of attack is in progress (it may result in a fairly large short lived state in the server). Broadband cable network environment may use such configuration by deploying DHCPSEC server at the head-end. In a switch based network, the monitors may be deployed in the hubs to detect both unauthorized use of IP addresses and denial of service attacks. If the attack in progress is detected, the ports may be deactivated. This is by no means a complete list of protection mechanisms against denial of service attack and the implementers must take appropriate actions to protect against such attacks. Note that the proposed method does not attempt to protect against denial of service attack.

2.2. Trusted configuration phase

In this phase, the DHCPSEC client proceeds with establishing a secure communication channel (as defined in section 2.4) between itself and a known DHCPSEC server (the address of

the server is known after the start-up phase). If the DHCPSEC client fails to establish a secure channel with the DHCPSEC server, the DHCPSEC fails and MUST be terminated with appropriate messages. Naturally, the process may be repeated again as often as desired. Once the trusted channel is established, the DHCPSEC client proceeds to renew the IP address using DHCP renew message. The communication for DHCP renew phase MUST be based on the unicast messages over the secured communication channel between the DHCPSEC client and server. If the renew completes successfully, the IP address allocated to the DHCPSEC client is authenticated.

Note: As suggested earlier, if the temporary address is not same as the address assigned in the trusted configuration phase, then the DHCP protocol may have to be modified so that instead of sending a NACK for the renew message, the server can ACK with an alternate address. The other approach is to modify the protocol so that instead of issuing a DHCP renew, the client can do a DHCP discover and, instead of sending a discover message as a broadcast, it is sent as a unicast message over the trusted communication channel. If the new trusted address is not identical to the un-trusted address assigned to a client, the DHCPSEC server SHOULD not automatically reclaim address before the duration of the temporary lease (it could lead to some race conditions). The client may issue an un-trusted release for the temporary address is no longer needed.

2.3. Trusted Renew and Release

The DHCPSEC server MUST ignore any renew or release request over clear channel for securely allocated IP address. Lease of a securely allocated IP address may be renewed or

released only over a secure channel between the DHCPSEC server and client to whom the address was allocated in the trusted configuration phase of the DHCPSEC protocol. The identity of the client is verified by the secure channel protocol. In summary, the trusted release phase is essentially same as the trusted configuration phase.

2.4. Authenticated Secure Channel

The DHCPSEC compliant servers and clients MUST implement the secure channel based on IPSEC AH [2] and ISAKMP/OAKLEY [3,4,5]. IPSEC ESP [6] MAY be used when the situation warrants. DHCPSEC clients and servers must conform to the interoperability requirements of IPSEC protocol suit (including ISAKMP/OAKLEY, IPSEC AH, and IPSEC ESP). In future other secure communication channels may be defined.

The IPSEC security association is used by the DHCPSEC protocol during the trusted configuration phase. Therefore, at the end of this phase, the security association SHOULD be discarded by both the DHCPSEC client and servers. In some cases (e.g., when the temporary address is same as the securely assigned address), the same security association MAY be used for further communication between the two systems.

3. Security Considerations

The proposed protocol does not address security requirements for tftp function that is part of the bootp protocol. It is assumed that the integrity of the files tftp'd will be verified using means external to this protocol. An example of such means would be to use signed files for software download using tftp so that the client would be able to authenticate and verify integrity of the copied software. The server may enforce licensing requirements on the software by external means such as a license servers.

4. Acknowledgments

The author would like to thank Thomas Narten, Ralph Droms, Peter Ford, Eric Dittert, Dave Chouinard, Charlie Perkins, and Throop Wilder, Munil Shah and many others for helping improve this draft.

5. References

[1] Droms, R, "Dynamic Host Configuration Protocol", RFC 1531. Bucknell University, 1993.

[2] Atkinson, R., "IP Authentication Header", RFC 1826.

[3] Maughan, D., Schrtler, M. Schneider, M., and Truner, J., "Internet Security Association and Key Management Protocol (ISAKMP)".

[4] Piper, D., The Internet IP Security Domain of Interpretations, Internet Draft.

[5] Carel, D., Harkins, D., "The Resolution of ISAKMP with Oakley".

[6] Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC 1827.

6. Authors' Address

Baiju V. Patel
Intel Corporation
MS JF3-206
2111 NE 25th Ave.
Hillsboro, OR, USA 97124
+1(503)264-2422
baiju@mailbox.jf.intel.com