Different Possibilities of DHCP Attacks and Their Security Features

R. Natarajan
Department of Unified Communications
Accenture Services Pvt Ltd, Tamilnadu

Abstract

This Paper deals with the Possibilities of DHCP attacks and their security features by creating and aging DHCP snooping entries, DHCP Trusted Ports, ARP Attack Detection, IP Filtering, DHCP Packet Rate Limit.
Keywords- DHCP, DHCP Client, DHCP Server, DHCP Snooping

I. INTRODUCTION

The Dynamic Host Configuration Protocol (DHCP) was developed based on the Bootstrap Protocol (BOOTP). The format of DHCP messages is based on the format of Bootstrap Protocol (BOOTP) messages, which ensures support for BOOTP relay agent functionality and interoperability between BOOTP clients and DHCP Servers.

BOOTP relay agents eliminate the need for deploying a DHCP Server on each physical network segment. The DHCP Server feature is a full DHCP Server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the DHCP Server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP Servers defined by the network administrator.

A DHCP client may receive offers from multiple DHCP Servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP Server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. The client returns a formal request for the offered IP address to the DHCP Server in a DHCPREQUEST broadcast message. The DHCP Server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. The formal request for the offered IP address (the DHCPREQUEST message) that is sent by the client is to broadcast so that all other DHCP Servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client. If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP Server are invalid (a misconfiguration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP Server. The DHCP Server will send to the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, if an error has occurred during the negotiation of the parameters or the client has been slow in responding to the DHCPOFFER message(the DHCP Server assigned the parameters to another client) of the DHCP Server. DHCP defines a process by which the DHCP Server knows the IP subnet in which the DHCP client resides, and it can assign an IP address from a pool of valid IP addresses in that subnet text.

The DHCP Server identifies which DHCP address pool to use to service a client request as follows:

- If the client is not directly connected (the giaddr field of the DHCPDISCOVER broadcast message is non-zero), the DHCP Server matches the DHCPDISCOVER with a DHCP pool that has the subnet that contains the IP address in the giaddr field.
- If the client is directly connected (the giaddr field is zero), the DHCP Server matches the DHCPDISCOVER with DHCP pool(s) that contain the subnet(s) configured on the receiving interface. If the interface has secondary IP addresses, the subnets associated with the secondary IP addresses are examined for possible allocation only after the subnet associated with the primary IP address (on the interface) is exhausted.

II. TYPES OF DHCP ATTACKS

No authentication mechanism is provided by DHCP clients and DHCP servers, as a result network security problems arises if multiple DHCP servers exist on a network. For example, an unauthorized DHCP server may assign invalid IP addresses, DNS server information or gateway addresses to clients to intercept traffic. To solve such problems, the DHCP relay agent and DHCP snooping features are enabled on switches. With the DHCP relay agent at the network layer or DHCP snooping at the data link layer enabled, a switch can record clients' IP-to-MAC bindings from DHCP messages and cooperate with other modules to enhance network security.

Table 1: DHCP Attacks and Their Security Features

Attacks	*Security Features*
Unauthorized DHCP Server attacks.	*DHCP Snooping, DHCP snooping Trusted Port Features.*
ARP man in the middle attack.	*DHCP snooping, ARP detection Features.*
IP/MAC Spoofing Attack.	*DHCP snooping, IP filtering Features.*
DHCP packet Flooding Attack	*DHCP Packet rate Limit Features.*

A. Unauthorized DHCP Server Attacks

Denial of Service (DoS): When a successful DoS attack has been launched against a company's DHCP server, the server can no longer assign the IP Addresses that network resources require to communicate. Key business functions such as email or internal web applications go offline while administrators scramble to restore order.

1) Malware:

Malicious code, such as worms or Remote Access Trojans (RATs), can infect DHCP servers across various operating systems, including Microsoft Windows, Linux, and Solaris, with little or no user interaction required. Attacks can be executed by an attacker outside your company or by an insider with privileged information about your environment. When successfully launched, the malicious code can take advantage of known and unknown vulnerabilities existing at the operating system level or in the DHCP services, allowing remote execution of code or a denial of service.

2) Vulnerabilities:

Vulnerabilities in software are an unfortunate reality in our world today. The DHCP service assigning IP addresses is nothing more than application code written to perform a specific function. Vulnerabilities have been reported in the common DHCP service code included with all of the major operating systems running the DHCP service. Software vendors provide patches to cover up these security holes. However, DHCP servers are rarely brought down for maintenance, such as patching. The longer a DHCP server goes without security updates, the more vulnerable it is to attack. Attacks on DHCP servers exploit vulnerabilities to cause buffer overflows. Malicious code can trigger buffer overflows to execute additional code or alter the way the program operates. Attackers can then elevate privileges or launch DoS.

3) Remote Code Execution:

If an attacker successfully exploits vulnerability, they are granted unfettered access to the operating system and its configuration. Attackers will launch additional malicious code designed to manipulate data on a server, steal information, or route users to an alternate rogue DHCP server that will provide a false sense of security for the users while allowing the attacker to sniff traffic for desirable information

B. ARP Man in the Middle Attack

All the others attacks except for this are considered to be passive since they do not involve altering the behavior of the systems being targeted causing the switch to fail-open can be seen as an active attack on the switch, but the network traffic is merely observed, not intercepted or modified en route. A Man-in-the-Middle attack is an active attack since the attacking host plays an important role managing the network traffic between the source and destination targets.

A Man in the middle attack is the target host is fooled by making it think that it is connecting to a desired destination host when in fact it is connecting to the attacker host, the attacker host handles the connection to the desired destination host and proxies traffic between the two from that point on. The attacker host completely controls the connection and can view and/or modify information passing between the connection it has forged with the source and destination hosts.

This type of attack is particularly effective when dealing with connections encrypted with public-key cryptography. Public-key cryptography is an extremely effective encryption concept, but it does have a condition that connecting host must have a copy of the public key from the host being connected to. If the connecting host does not already have the public key from a previous connection with that host then it will have to get it from somewhere – with protocols such as Secured Shell Hosts, the destination host will supply its public key itself. Man in the Middle attacks take advantage of this by intercepting the initial connection attempt and substituting their own "forged" public key (which the attacker has from an earlier session and can Therefore decrypt the data). If the user at the connecting end has never seen the correct public key before, then the forgery will not be noticed and the attack will be a success. Even in the case where the user does have the correct public key to compare with it, often it just results in a small warning being printed saying the key has changed and if they want to continue connecting. Most users will simply click OK without another thought. This is not the fault of the protocol. This is a problem with user education and also with implementations that print simple warnings when an event as serious as a key change occurs. Executing the MITM attack is more

complex than the others, but d sniff's tools make it almost as easy. It is hard to study D sniff without being at least slightly troubled by the ease at which we can gather passwords, emails, files, and eavesdrop on encrypted connections, even on switched networks

C. IP/MAC Spoofing Attacks

MAC spoofing, IP spoofing, and IP/MAC spoofing attacks are common spoofing attacks. In such an attack, a hacker sends a packet with a forged source address to access networks or to obtain some privilege related to IP/MAC. This method is also used in deny of service attacks.

To guard against IP/MAC spoofing attacks, low-end Ethernet switches provide the IP filtering feature. With this feature enabled on a port, a switch can filter packets on the port by matching the source addresses of the packets against the dynamic and static DHCP snooping entries, and unqualified packets are thus discarded. The feature can also help in avoid address conflicts.

D. DHCP Packet Flooding Attack

If an attacker sends a large number of DHCP requests to a DHCP server, all IP addresses on the server will be assigned, and therefore many DHCP clients cannot obtain IP addresses. In addition, if a DHCP snooping switch exists between the attacker and the server, both the DHCP snooping switch and the DHCP server may be over-loaded when processing the DHCP packets.

To guard against DHCP Packet flooding attacks, low-end Ethernet switches provide the DHCP packet rate limit feature, which can shut down any ports under such attacks.

III. DHCP SECURITY FEATURES

There are two DHCP security features available: DHCP relay agent information option (Option-82) and DHCP Snooping. The DHCP Option-82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information.

Although DHCP Option-82 is a subcomponent of DHCP Snooping, these two features are mutually exclusive. If the DHCP Option-82 feature is enabled for the switch, then DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, then DHCP Option-82 is not available. In addition, the following differences exist between these two features:

- DHCP Snooping does require and use the Option-82 data insertion capability, but does not implement any other behaviors defined in RFC 3046.
- DHCP Snooping is configurable at the switch level and on a per-VLAN basis, but DHCP Option-82 is only configurable at the switch level.

A. Creating and Aging DHCP Snooping Entries

With DHCP snooping enabled, low-end Ethernet switch listens to either the DHCP-REQUEST broadcasts or the DHCP-ACK unicasts according to the network environment to record the configuration information of clients in a DHCP snooping table, including IP addresses, MAC addresses, VLAN IDs, ports, and lease time.

Low-end switches support aging and removing DHCP snooping entries based on their leases to save system resources and ensure network security. When a DHCP snooping entry is recorded, a 20-second timer is started. That is, the DHCP snooping entry is checked every 20 seconds. The system determines whether the entry expires by comparing the entry's lease time with the difference value between the current system time and the entry adding time. If the lease time of the entry is smaller than the difference value, the entry is aged out. The disadvantage is that if an IP address has an unlimited or very long lease time, the corresponding DHCP snooping entry cannot not be aged out timely.

B. DHCP Snooping Trusted Ports

1) Trusted:

A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses sections.

2) Untrusted:

An untrusted port is connected to an unauthorized DHCP server. DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

After DHCP snooping is enabled on a switch, all the ports on the switch are configured as untrusted ports by default. The DHCP-ACK, DHCP-NAK, and DHCP-OFFER messages will neither be forwarded nor delivered to the CPU. If a port is configured as a trusted port, the DHCP-ACK, DHCP-NAK, and DHCP-OFFER messages received on this port will be delivered to CPU for processing.

Currently, the DHCP snooping function must work with the DHCP snooping trusted port function. If you have enabled DHCP snooping on a device, you need to specify any port connected to an authorized DHCP server as a trusted port, and configure the trusted port and ports connected to DHCP clients to be in the same VLAN.

C. ARP Detection

1) Mechanism of ARP Attack Detection:

To guard against ARP man-in-the-middle attacks, low-end Ethernet switches can deliver ARP (request or reply) packets to the CPU to check the validity of the packets based on DHCP snooping entries If the source IP and MAC addresses of the ARP packet, and the receiving port and its VLAN ID match a DHCP snooping entry or a manually configured binding entry, the switch will forward the ARP packet If not, the switch will discard the ARP packet and display the corresponding debugging information.

2) Configuring Static Bindings:

DHCP snooping tables can only record information for clients that have obtained IP addresses through DHCP. If you manually configure a fixed IP address for a host, the IP and MAC addresses of the host will not be recorded in the DHCP snooping table. Consequently, the host cannot pass ARP attack detection to solve this problem; you can configure static binding entries on the DHCP snooping device. Such an entry should contain the IP and MAC address of a host and the port connected to the host.

3) Configuring ARP Trusted Ports:

The upstream ports of a DHCP snooping switch can receive ARP request or reply packets from other devices, in which the source IP and MAC addresses may not be recorded in the DHCP snooping table or static binding table. In order for these ARP Packets to pass ARP attack detection you can configure these ports as ARP trusted Ports. ARP packets received from ARP trusted ports are not checked, while ARP packets received from other ports are checked.

D. IP Filtering

IP filtering allows a DHCP snooping switch to filter IP packets based on the DHCP-snooping table and IP static binding table After IP filtering is enabled on a port, the switch applies an ACL to discard all IP packets except DHCP packets on the port. (If the port is not a DHCP snooping trusted port, DHCP reply packets received on it will be discarded; otherwise, DHCP reply packets can pass). Then, the switch applies another ACL to permit packets with source IP addresses matching specific DHCP snooping entries or static binding entries.

Filtering the source IP address in a packet. If the source IP address and the receiving port match an entry in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.

Filtering the source IP address and the source MAC address in a packet. Source IP address and source MAC address, and the receiving port match an entry in the DHCP-snooping table or static binding table, the switch regards the Packet as a valid packet and forwards it, otherwise the switch drops it directly.

E. DHCP Packet Rate Limit

To prevent DHCP packet flooding attacks, low-end Ethernet switches provide the DHCP packet rate limit function. After the function is enabled on an Ethernet port, the switch counts the number of DHCP packets received on this port per second .If the number of DHCP packets received per second exceeds the specified value, the switch will shut down its port. In addition, the switch supports port state auto-recovery. After a port is shut down, it will be brought up automatically after a configurable period of time.

IV. CONCLUSION

This paper describes the Possibilities of DHCP attacks and their security features. I am very careful to protect server and client anonymity at every step of the process. In addition to the standard DHCP extension mechanisms, the major contributions of the paper are solutions to the several DHCP attacks.

REFERENCES

[1] Ralph Droms and Bill Arbaugh,"Authentication for DHCP messages", RFC 3118, IETF, June 2001.
[2] International Telecommunication Union. ITU-T recommendation X.509 (1997 E): Information technology—open systems Interconnection—the directory: "Authentication framework", June 1997.
[3] Denise Donohue, Russ White, "The Art of Network Architecture", May 2014.
[4] Hamacher vranesic Zaky,"Computer organization,"August 2007.
[5] William stalings,"High speed Networks", December 2009.
[6] Cisco press,"Ip addressing:DHCP cisco IOS XE release 3S(Cisco ASR 1000)",August 2010.
[7] Juniper Networks, Technical documentation on "DHCP Options and selective traffic processing", April 2014.
[8] Mcafee, White paper on "DHCP attacks and their detection", Jan 2005.
[9] H3C Technologies, White Paper on "DHCP Security Policy", Apr 2008.