Assignment 3-1: DHCP Security Assignment
David Thomsen

With the ease of using a DHCP server, it is bound to come with some security issues associated with the requests and demands for IP addresses. One security flaw that comes with DHCP servers is having Unauthorized DHCP servers. This means that if a malicious entity plants a DHCP server, this server could respond to client IP requests and complete the handshake. This allows the malicious DHCP server to not grant access to the network, as well as set up the DHCP clients to be abused further in the future.

As always, with these flaws, come ways to get around them and make sure the end user is safe while using their devices. One major issue is the lack of public knowledge regarding these types of problems leading to much human error. Its a well known fact that you shouldn't connect to random public wifi for fear of malicious users on that network. This is brought up because if the Unauthorized DHCP server is the network that is being connected to, there is a high chance of the end user being affected negatively. However, there are also ways to avoid the issue in the first place. The place that is running the real DHCP server can have stronger network control and keep an eye on the IP and UDP packets, as those are the ones DHCP uses. It is also possible to set up a DHCP authentication method that will replace normal DHCP messages with Authenticated ones.

Another major security flaw is that the DHCP protocol was designed in the 1990's and lacks many new-age security features. The DHCP protocol runs over IP as well as UDP which are both insecure protocols. These issues are more serious security flaws in modern networks due to just how much DHCP is relied upon. DHCP deals with All of the network configuration settings for each client device on the network, and the protocol has the same security features as when it was created almost 30 years ago.

The solution to this issue is much simpler than the last, as it is simply to try and modernize DHCP so that its security features are much more up-to-date. While this is a simple answer, it is not an easy one. There are many issues within DHCP as a protocol that make it unsafe for the end user. For example, It uses UDP which is a much less secure protocol than TCP, but is used as it is much faster when sending and receiving packets. An old solution of people trying to fix this was DHCPv6, which is basically the same thing, but for IPv6. The unfortunate truth is that not much internet traffic uses IPv6 and Much of it heavily relies on IPv4.

Lastly, another big security flaw is known as a DHCP starvation attack. This is where a malicious user will spoof Discover Packets, and exhaust the IP addresses that the DHCP servers can give out. This is an issue as this can be used alongside other known flaws of DHCP and can lead to a man in the middle attack. After the DHCP addresses are completely exhausted, it is easy for someone to set up an unauthorized server for unknowing clients to connect to. The main issue with this sort of flaw is that DHCP starvation attacks are not very difficult to set up and

execute. By learning the steps of how to flood a server with random discovery packets, you are then able to perform this attack on most DHCP servers.

While these attacks are easy to execute, they are also somewhat easy to shut down. Port security is one of the ways to stop these kind of attacks. Port security is able to protect the network from the attack by preventing unknown devices from sending packets out. This allows the server to limit the amount of MAC addresses per port. This is an insanely useful and necessary feature to use for DCHP servers and networks, to make sure that they are not going to get hit with a starvation attack.

Heintzkill, R. (n.d.). *What is a DHCP starvation attack?* CBT Nuggets. Retrieved September 18, 2022, from https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack

Kozierok, C. M. (2005, September 20). *DHCP Security Issues*. The TCP/IP Guide - DHCP security issues. Retrieved September 18, 2022, from http://www.tcpipguide.com/free/t_DHCPSecurityIssues.htm

Support, N.E.T.G.E.A.R. (2016, November 28). *What is Port Security and how does it work with my managed switch?* NETGEAR KB. Retrieved September 18, 2022, from https://kb.netgear.com/21786/What-is-port-security-and-how-does-it-work-with-my-managed-switch