COMPUTERS & SECURITY 65 (2017) 387–404

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A closer look into DHCP starvation attack in wireless networks

Neminath Hubballi *, *Nikhil Tripathi*

Discipline of Computer Science and Engineering, School of Engineering, Indian Institute of Technology Indore, India

ARTICLE INFO

Article history:
Received 4 February 2016
Received in revised form 28 July 2016
Accepted 10 October 2016
Available online 19 October 2016

Keywords:
DHCP
DHCPv6
SLAAC
DHCP starvation attack
ARP poisoning
802.11 Wi-fi network
Hellinger distance

ABSTRACT

Dynamic Host Configuration Protocol (DHCP) is used by clients in a network to configure their interface with IP address and other network configuration parameters such as Default Gateway and DNS server IP addresses. This protocol is vulnerable to a Denial of Service (DoS) attack popularly known as classic DHCP starvation attack. In this paper, we make three-fold contribution. First, we highlight the practical difficulty in generating classic DHCP starvation attack in wireless networks. Secondly, we propose a stealth starvation attack which is effective in wireless networks, easier to launch, requires fewer number of messages to be transmitted and difficult to detect by known detection methods. We also show a structurally similar attack in IPv6 networks which can affect address configuration protocols such as DHCPv6 and *StateLess* Address Autoconfiguration (SLAAC). Subsequently, we also describe an anomaly detection method to detect the proposed attack. We design and generate the attacks in a real network setup and report the results. The proposed detection method uses the Hellinger distance between two probability distributions generated from training and testing data to detect starvation.

1. Introduction

Dynamic Host Configuration Protocol (DHCP) is used for automatic IP address allocation to DHCP enabled clients. It also enables DHCP clients to configure themselves with other network parameters like subnet mask, default gateway IP address, etc. This protocol is vulnerable to a Denial of Service (DoS) attack popularly known as DHCP starvation attack. In this case, a malicious insider can launch a DoS attack preventing other clients from acquiring an IP address. There are open source tools like Gobbler (2016) and DHCPIG (2016) to launch this attack. These tools use MAC address spoofing to generate large number of IP requests and for every request, a new IP address is released by a DHCP server and this exhausts the address pool. However this method is not effective in a wireless network as described in Section 2.2.

In this paper, we propose a new DHCP starvation attack termed as *Induced DHCP Starvation* that does not require a malicious client to inject large number of IP request messages using random MAC addresses to exhaust IP address pool. Instead, the attack is intended to exploit a loophole present in DHCP client-side IP address conflict detection scheme. According to RFC 2131 (Droms, 1997), a DHCP enabled client should probe an allocated IP address to check if IP address is already in use. To launch the proposed attack, a malicious client injects a fake reply in response to probe request sent by the client. Once the DHCP client receives the corresponding reply, it declines the IP address offered and informs DHCP server by sending a decline message. When DHCP server receives this decline message, it

* *Corresponding author.*
E-mail addresses: neminath@iiti.ac.in (N. Hubballi), phd1401101002@iiti.ac.in (N. Tripathi).
http://dx.doi.org/10.1016/j.cose.2016.10.002
0167-4048/

marks the offered IP address as unavailable for the length of the lease period. This set of operations is repeated for every probe request sent to detect IP address conflict, thereby, preventing a DHCP client from acquiring an IP address which is a case of DoS. This attack is equally effective in both wired and wireless networks. We show that the proposed attack is effective also in DHCPv6. We also propose a statistical abnormality measurement technique that uses the Hellinger distance between two probability distributions generated from training and testing data to detect starvation. We evaluate proposed detection method to detect *Induced DHCP Starvation* attack presented in this paper and the attack we proposed in one of our previous works (Tripathi and Hubballi, 2015).

The rest of the paper is organized as follows. We provide an overview of DHCP working and two variants of classic DHCP starvation attacks in Section 2. In Section 3, we describe our proposed DHCP starvation attack. Experimental studies are presented in Section 4. Relevance of proposed starvation attack in IPv6 networks is discussed in Section 5. We provide the overview of other DHCP starvation detection methods in Section 6. We also describe a method for detecting proposed attack in Section 7. Finally, the paper is concluded in Section 8.

2. Background

2.1. DHCP working

In a network, a DHCP server is configured with a pool of IP addresses and other network parameters (Droms, 1997). To get an IP address, four messages are exchanged between a DHCP client and the DHCP server as shown in Fig. 1. The complete process of automatic IP address allocation is known as *DORA* process where "D", "O", "R" and "A" stand for "Discover", "Offer", "Request" and "Acknowledgement" respectively. RFC 2131 (Droms, 1997) describes few other DHCP messages that are exchanged during unsuccessful IP address configuration. DHCPDECLINE is one such message that is sent by a client to DHCP server if client finds that the assigned IP address is already in use by any other client in the network. DHCP clients usually detect such IP address conflicts by sending probe requests destined to the IP address allotted.

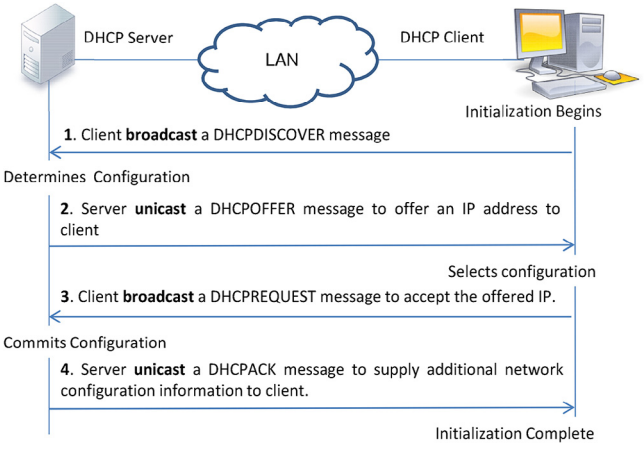

Fig. 1 – Exchange of messages in DHCP operation.

2.2. Classic DHCP starvation attacks

Due to the absence of an in-built authentication in DHCP, it is vulnerable to an attack popularly known as DHCP starvation attack. In this subsection, we describe two popular methods of generating DHCP starvation attack along with few limitations of these methods.

2.2.1. Using similar (random) MAC address in Ethernet header and DHCP header (Type-1)

In this case, a malicious client sends large number of DHCPDISCOVER messages using spoofed source MAC addresses to a DHCP server. Same MAC address (spoofed) is used in the Ethernet header and CHADDR field of DHCP header. The server allots IP address to each of these requests using *DORA* process. This results in the exhaustion of IP address pool present at DHCP server. As a result, new legitimate clients will be denied from obtaining an IP address from the DHCP server. In wireless networks this attack can not be so easily generated. IEEE 802.11 standard has an association phase of a wireless client with Access Point (AP) and also session key generation phase (WPA 2) which uses client's MAC address. The sequence of operations done while a client connects to AP in WPA2 is shown in Fig. 2 (Xing et al., 2008). AP drops packets sent or received with random MAC addresses as these are not associated with it. As a result, this type of attack does not work in wireless networks unless the malicious client precedes an association with AP for each spoofed address. However, considering the association phase and the session key exchange using 4-way

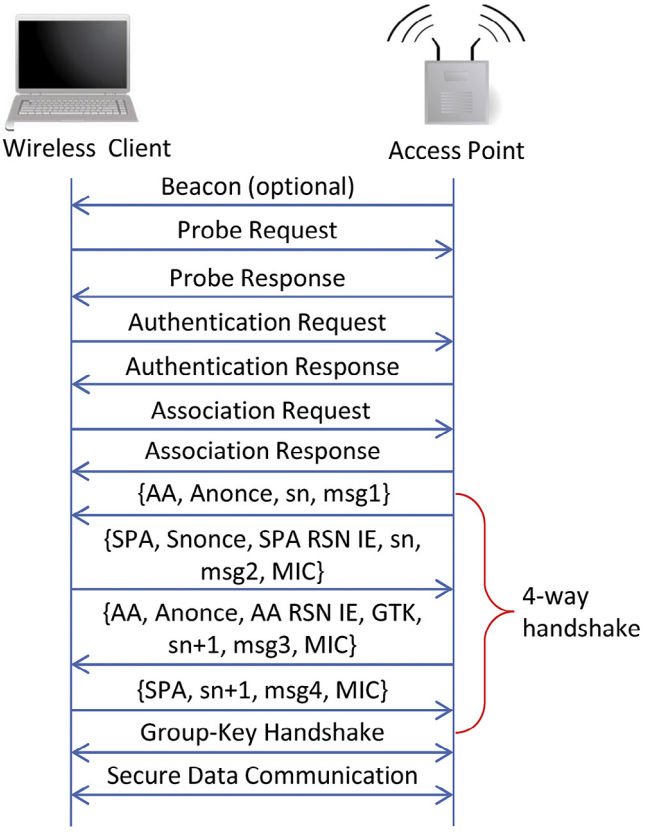

Fig. 2 – Association of client with AP.