Detecting the Auto-configuration Attacks on IPv4 and IPv6 Networks

Li, He

(出版者 / Publisher)
法政大学大学院情報科学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 情報科学研究科編 / 法政大学大学院紀要. 情報科学研究科編
(巻 / Volume)
10
(開始ページ / Start Page)
1
(終了ページ / End Page)
6
(発行年 / Year)
2015-03-24
(URL)
https://doi.org/10.15002/00011586

Detecting the Auto-configuration Attacks on IPv4 and IPv6 Networks

He Li
Hosei University, Tokyo 184-8584, Japan
he.li.ge@stu.hosei.ac.jp

***Abstract*— Auto-configuration is a mechanism, which assigns IP address, default gateway address and DNS server address to a node for accessing to the network. On IPv4 network, auto-configuration is done by using DHCP protocol, but IPv6 network has two ways to assign auto-configuration information to a node, which are stateless address configuration by routers and stateful address configuration by DHCPv6 servers. On the auto-configuration phrase, some attackers may be able to inject a counterfeit information, which may cause DOS, DNS hijacking, and man-in-the-middle attack, to the client. In this paper, we propose a method to detect DHCP attack and man-in-the-middle attack both on IPv4 and IPv6 network by collecting and analyzing the auto-configuration phrase. This approach is also able to detect the location of attacker in the network, and also works for both of IPv4 network and IPv6 network.**

Keywords—Auto-configuration; Detect; Packet Sequence; DHCP; Man-in-the-middle

I. INTRODUCTION

In the early time when computers and networks were introduced to the world, there were a small number of computers and networks, the configuration can be done by manual. Administers simply type IP addresses, router addresses and other information into computers, and then computers can communicate with each other. However, when the number of computer is getting large, it becomes unrealistic to configure all nodes manually. Auto-configuration could address that situation. Users just have the cable plugged into a computer; the computer can get the configuration information from the network.

The auto-configuration is realized by using DHCP protocol on IPv4 network. It assigns IP address from address pool and extra information, such as network mask, DNS server address, is provided. On IPv6 networks, a node can obtain configuration information by two methods, which are stateless address configuration by routers and stateful address configuration by DHCPv6 protocol [1]. The stateless configuration does not keep the mapping between the assigned address and the client host, thus the administrator could hardly get the information that how many addresses have been used in the stateless address configuration network. Meanwhile stateless address configuration does not provide DNS server address information. Stateful auto-configuration by DHCPv6 server, however, must keep track of the address information, such as which address has been assigned to which client, how much time the address can be used. Therefore how many nodes has been connected to the network and how much time a IP addresses can be obtained by each node can be known to network administration. On IPv6 network, a client want to know the DNS server address to access to the Internet. This leads that stateful configuration is used more than stateless configuration. This paper concerns on auto-configuration both on IPv4 and IPv6 network, especially stateful auto-configuration on IPv6.

A bogus DHCPv6 server is a critical issue on the auto-configuration phase on IP network. It can give an illegal IPv6 address and then dress up as a router. That situation leads to man-in-the-Middle attack [2], that all information will be sent to the malicious server for forwarding when the victim suffers the Internet. A bogus DHCPv6 server also can provide an illegal DNS server address to the client. This sort of attack is called DNS hijacking [3]. This leads to phishing attack [4], which will easily succeed by giving a fake IP address in DNS response packet. The fake IP address can guide the victim to a particular website without conscious. Similar problem also occurs by users' misconfiguration. Auto-configuration will relax the administrators' burden on address assignment, but it also cause another security issue. A method to detect these illegal sequences is important to ensure the safety. This paper focuses on detecting auto-configuration attacks, and trying to find out on which network the malicious DHCP servers and routers are reside.

The paper consists of five parts. Section II briefly describes the related works about the security of DHCPv6. Basic knowledge of auto-configuration by DHCP will be introduced in Section III. Section IV gives the ideas of discovering and locating the malicious server. The result of experiment and evaluation is shown in Section V. Conclusion, discussion and future work are given in the last section.

II. RELATED WORK

Stephen Groat discussed the threat of static DUID, which is an essential part of DHCPv6 message [5]. An attacker, who can capture network traffic, spoofs a DHCP packet, which contains fake information, with the DUID information, and then sends this packet to the server. The server regards this packet as it is sent by the client and the server respond as the packet request. The attacker also can construct a fake packet sent to the client. The client think this packet as the one sent by the server, and it will do as the information in that packet. By this way, the server or the client can be leaded to an unimagined state.

Supervisor: Prof. Toshio Hirotsu.

Joseph Tront addressed this threaten by using dynamic DUID which cost too much [6]. Because this solution needs to have all client and server implemented the algorithm that can produce and verify the dynamic DUID. The lease time of that approach is much worse than traditional method, which may open another door to the attackers.

Zhiyang Su introduced a method to protect DHCP phrase by using encryption in the paper "Secure DHCPv6 that uses RSA Authentication integrated with Self-Certified Address" [7]. A new option for DHCPv6 protocol is created to store the result of RSA. The problem is the same as prior one. If they want the approach to work well, all nodes need to have RSA and their program installed. The stability is another concern. Jiang Whai Dai provides an idea to find an abnormal node in "A New Method to Detect Abnormal IP Address on DHCP" [8]. The abnormal means a node who according to the network environment gives itself an address that can be used in that network. If the address has already been given to another node, this leads to two nodes having same address in the network, which influences the stable of the network. Comparing the ARP table and DHCP table is the solution. However, the process need a human being involved. If the DHCP released table has a great number of entries, distinguishing by eyes will be boring and time consuming.

Saugat Majumdar created another option on DHCP Packet in the paper "DHCP Origin Traceback" [9]. Routers should fill in the option before a DHCP packet forwarded. Experimenters can get the route as long as the packets arriving at the server or the client. This approach is a little expensive, for it needs all routers to support this option. It also may cause fragment, which is a big hole in UDP, for there is no acknowledge mechanism in UDP when one piece of fragment is lost.

There are many threats of Neighbor Discovery listed in RFC3756 [10]. Some of them can cause Man-In-The-Middle attack.

The approaches which has been intorduced above fouce on proection DHCP phrase, whereas our approach targets on attack detection and attacker orientation. In our approach, packet trace needs to be monitored and analyzed. No new option or encryption algorithm is involved. Detection Scheme may depend on the network topology, especially the position of server, client, attacker and the monitor. The detection scheme first detects DHCP attack and then locates the attacker. The monitor should be connects to real DHCP server's network so that DHCP attack detection can be detected no matter where the attacker and the client are. After an DHCP attack detecting, man-in-the-middle attack detection should be used when the server and the attacker locate on the same network. If the attacker does not locate on real server's network, the monitor should be moved into the victim's network, then DHCP attack should be detected again for finding attacker's information, and traceroute can help us to find where the attacker is.

III. AUTO-CONFIGURATION USING DHCP

A. DHCP Basic

Auto-configuration information is sent from a server to a node who tries to connect to the network. The process of leasing an IP address from the DHCPv4 server involves four steps, including DISCOVER, OFFER, REQUEST, and ACK, which are shown in Figure 1. In general, the process of DHCPv6 is similar to DHCPv4. The difference between DHCPv4 and DHCPv6 is that a client of DHCPv6 should use multicast whereas broadcast is used on DHCPv4. The other difference is the message type names. In DHCPv6, these are SOLICIT, ADVERTISEMENT, REQUEST, and REPLY, which are corresponding to DISCOVER, OFFER, REQUEST and ACK in DHCPv4.

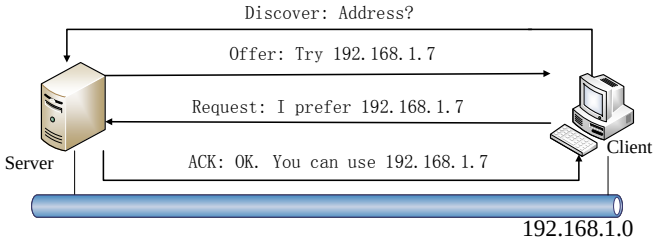


Fig. 1. DHCPv4 messages exchange

B. Relay Agent

If both the DHCPv4 client and the DHCPv4 server reside on the same network segment, the process proceeds exactly as previously denoted. However, if they are located on the different networks, as shown in Figure 2, the process becomes more complicated, for a router should act as a relay agent. A relay agent is a special router, which has been configured to forward DHCP packets to other networks. It will add its address into the packet before forwarding the packet.

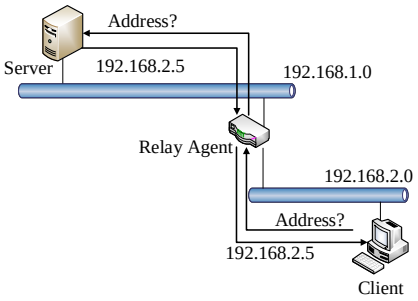


Fig. 2. DHCPv4 messages exchange by a relay agent

On configuring the DHCP relay, managing network and forwarding direction are defined. Relay agent should forward the packets in one direction. The direction of packets sent by clients should be forwarded towards the server's network. In Figure 3, that direction is from the bottom to the top. For example, the packets sent by client_1 on network2 are forwarded to network1, and is never forwarded to network3. When these packets reach network1, relay3 does not forward it to network4 and network5. The direction of packets sent by a server is just opposite of the client, which is from the top to the bottom. The packets sent by the server, on network1, can be forwarded to anywhere, but as long as these packets leave network1, they have no possibility come back to network1. In addition, if relay1 is picked for forwarding, these packets cannot show up on network4 and network5.

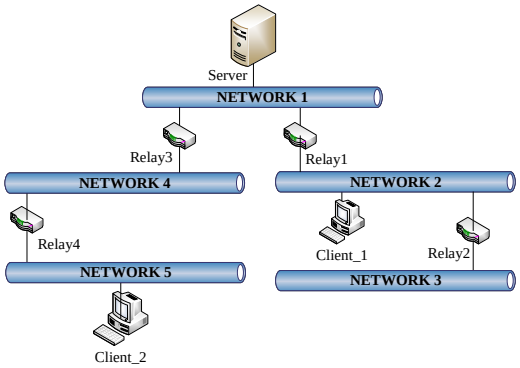


Fig. 3. A traditional network topology

C. DHCP attacks

A malicious DHCP server may exist on anywhere on a network. On a simple hierarchical network shown in Figure 3, there are following three cases on relative allocation of entities.

- An attacker locates on the same network with the DHCP server (Attacker 1 in Figure 4).
- An attacker on the different network from the DHCP server, and locates on the same network with the client or between the client and DHCP server. (Attacker 2 in Figure 4).
- An attacker on the different network from the DHCP server, and locates far from the client network (Attacker 3 in Figure 4).

An attack may success when the ADVERTISEMENT packet sent by a malicious DHCP server arrives earlier than the one sent by the real server. In Figure 4, client 1 on network 2 may be attacked by Attacker 1, but never be affected by Attacker 3, which is on Network 3. Client 2 on network 4 and client 3 on network 5 may be attacked by Attacker 2 or Attacker 1.

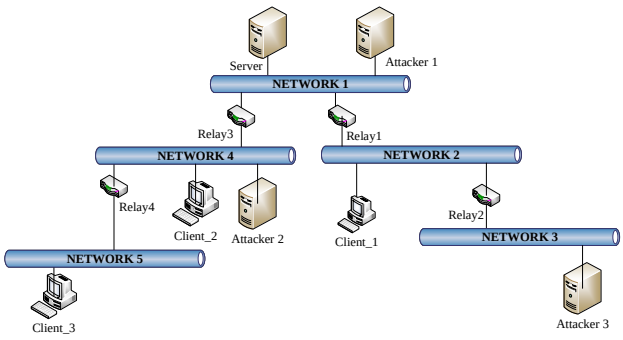


Fig. 4. Some attackers exist in a traditional network topology

Because relay agents use unicast on IPV4 network, the malicious DHCPv4 server only can reside on the client's network segment, just like client 2 and attacker 2 on network 4. However, the malicious DHCPv6 server can be anywhere when the multicast is used by DHCPv6 relay agents for forwarding packets to the DHCPv6 server.

IV. DETECTION STRATEGY

Auto-configuration attacks detection on IPv6 network will be exhaustively introduced in this part. The mechanism on IPv4 is almost the same as IPv6. In the next section, the difference between IPv4 and IPv6 are also referred.

The detection scheme, which is shown in Figure 5, can be divided into two main parts, which are DHCP Attack Detection and Attacker Location Detection. The first part, which is DHCP Attack Detection, consists of two parts, which are monitor and analysis. Attacker Location Detection part has two methods, which is decided by the result of analysis, to locate the attacker.

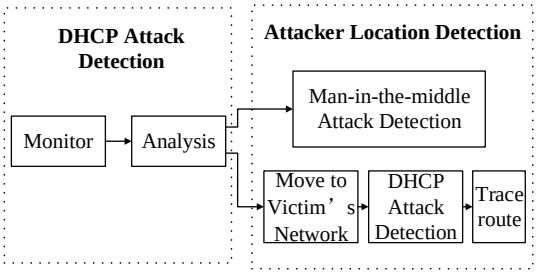


Fig. 5. Detection scheme

Two steps of DHCP attack detection is introduced as follows. A monitor system, which locates on real server's network, captures the packet sequence and extracts the information in each packet. All communication between a DHCP client and a DHCP server can be seen on the server's network. DHCP packet sequence is the four-step communication. We can obtain client's mac address, server's mac address, leased IP address, leased DNS server addresses , and default router addresses (Only on IPv4). These addresses, which are used as source data for analyzing, are the most important messages among all information.

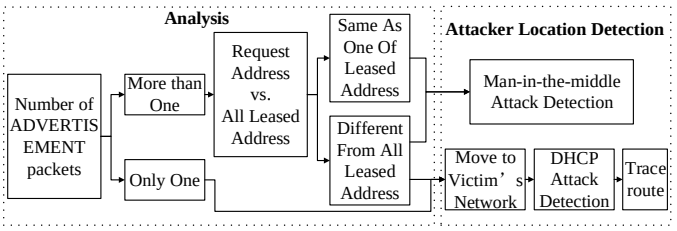


Fig. 6. Two results of analysis

Figure 6 shows the detail steps of the analysis that support Attacker Location Detection. The analysis result, which is depended on network topology, decides which method should be used to find the attacker. If there is only the real DHCP server in the network, the leased address will be equal to the request address. If there is another malicious DHCP server or multiple malicious DHCP servers reside on network, an attack is detected by comparing the requested address in REQUEST packet with the leased address in the ADVERTISEMENT packet, which is the nearest to the REQUEST packet. The number of ADVERTISEMENT packets depends on the topology of the network and how many attackers locate on the

network. If only one attacker locate on the network, the explanation is based on the topology in Figure 7.

- If the attacker locates on the same network with the monitor just as Attacker1 in Figure 7, two ADVERTISEMENT packets can be monitored. The request IP address in REQUEST packet should be the same as the leased address, which is in the earliest ADVERTISEMENT packet, and should be different from the one in the other ADVERTISEMENT packet, which is nearer to REQUEST packet. So an attack can be detected by comparing addresses. At the same time, this is the first situation in Figure 5, thus man-in-the-middle attack detection should be chosen to find the attacker. This leads to the second method to find the attacker
- If the attacker locates on different network from the monitor, just as Attacker 2 on Network 4 in Figure 7, only one ADVERTISEMENT packets can be monitored on real server's network. This situation leads to another method in Figure 5.

If multiple attackers coexist on the network, both of two methods may be used at the same time to find all attackers. If more than one ADVERTISEMENT packets has been found, but the request address is different from all of leased address, this attacker is attacked by the attacker locate on other networks, just as client 2 on network 4. It is attacked by Attacker 2, so the request address is different from the leased address from the server and Attacker 1. So man-in-the-middle attack is used to find the attacker who is on the same network with the real server, and the other method is used to find the attacker who is on the other network.

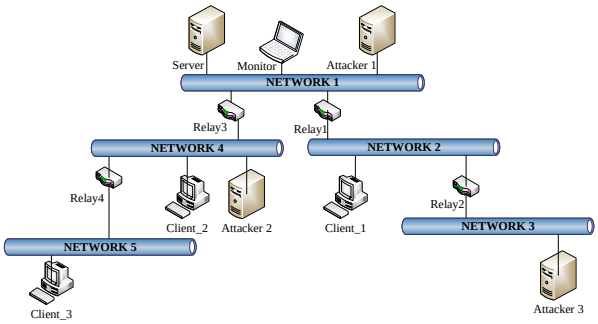


Fig. 7. Network topology

V. Experimental Result

This section consists of two results. The first result shows an attacker locates on the same network with the monitor, and second result shows the attacker locates on different network from the monitor. All results are based on only one attacker on the network, because multiple attackers are the combination of two results. In addition, as the limited of pages, only result on IPv6 network will be shown.

A. More Than One ADVERTISEMENT packets.

1) DHCP Attack Detection

A packet sequence has been captured and its details are shown in snapshot (a) in Figure 8. There are two ADVERTISEMENT packets in this figure. The requested address is addr_A, and addr_B belongs to the ADVERTISEMENT packet which is the nearest to the REQUEST sequence. As they are different, there is an attack. Two ADVERTISEMENT packets indicate that the attacker is on the real server's network. We got two server's mac addresses as well, but cannot distinguish which belongs to the attacker. Another mechanism should be imported in order to pick the real one from two mac addresses. As shows in Figure 5, Man-in-the-middle attack detection supports this work.

Detected	Information
Solicit	00:0c:29:a2:75:0e
Adv_A	00:0c:29:f1:4e:85
	Leased addr_A
Adv_B	00:0c:29:f2:53:ff
	Leased addr_B
Request	00:0c:29:f1:4e:85
	Request addr_A
Reply_A	00:0c:29:f1:4e:85
	Leased addr_A
	DNS addr_A

(a) Multiple ADVERTISEMENT

Detect	Information
Solicit	00:0c:29:a2:75:0e
Adv_A	00:0c:29:f1:4e:85
	Leased addr_A
Request	00:0c:29:a2:75:0e
	Request addr_B
	Relay addr 4000::1

(b) Single ADVERTISEMENT

Fig. 8. Information records

2) Attacker Location Detection – Man-In-The-Middle Attack Detection On IPv6

We begin with the feature of man-in-the-middle attack, and then introduce the strategy of detecting man-in-the-middle attack. Experimental environment was established to simulate man-in-the-middle attack, which can be found in Figure 9.

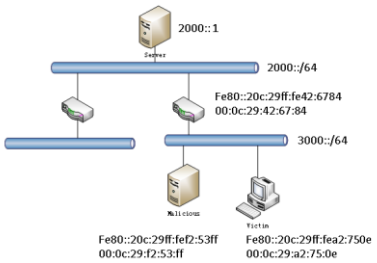
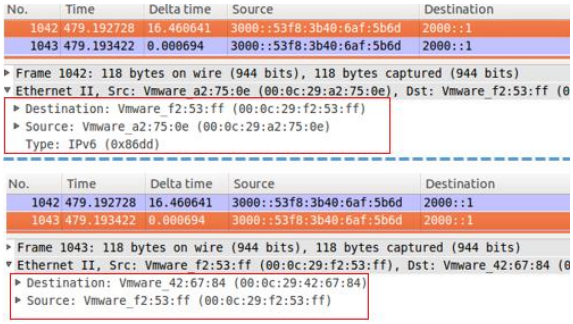


Fig. 9. Experimental topology

Snapshot (a) in Figure 10 shows the feature of man-in-the-middle-attack. We used ping6 function to send packets from the victim computer to the real server with the 2000::1 address. The 3000::5386:3b40:6af:5b6d is the global IPv6 address assigned by malicious server. Looking through snapshot (b) in Figure 10, it is obvious that there are two Echo (ping) sequences, and these two sequences seem like the victim has sent out the packet twice. Snapshot (b) in Figure 10gives us some details of these two "Echo (ping)".

No.	Source	Destination	Protocol	Length	Info
1042	3000::53f8:3b40:6af:5b6d	2000::1	ICMPv6	118	Echo (ping) request id=0x0b7c
1043	3000::53f8:3b40:6af:5b6d	2000::1	ICMPv6	118	Echo (ping) request id=0x0b7c
1045	fe80::20c:29ff:fe42:6784	ff02::1:ffaf:5b6d	ICMPv6	86	Neighbor Solicitation for 300
1046	3000::53f8:3b40:6af:5b6d	fe80::20c:29ff:fe42:6784	ICMPv6	86	Neighbor Advertisement 3000::5
1047	2000::1	3000::53f8:3b40:6af:5b6d	ICMPv6	118	Echo (ping) reply id=0x0b7c,

(a) Message sequence of man-in-the-middle attack



(b) Details of first two sequences

Fig. 10. Man-in-the-middle attack sequence

In the first sequence with number 1042, the destination mac address is the malicious server's mac address, and the source mac address is the victim's mac address. In the second sequence, the destination mac address is the router's mac, and the source mac address is the malicious mac address. These information shows that the ping6 message is transferred from the victim to the malicious DHCP server and then the message is sent to the router from the malicious DHCP server. It is obvious that the victim has been acted as a router. The strategy of man-in-the-middle attack detection is two packets with same source and destination IP addresses should be compared. If two mac addresses are different but the rest of parts of two packets are same, there is a man-in-the-middle attack. The result shows in Figure 11.

Seeing from Snapshot (a) in Figure 8, we have known the client's mac address, therefore the other one belongs to the attacker. So far, we have found the attacker's location and its mac address when the attacker and the real server on the same network.

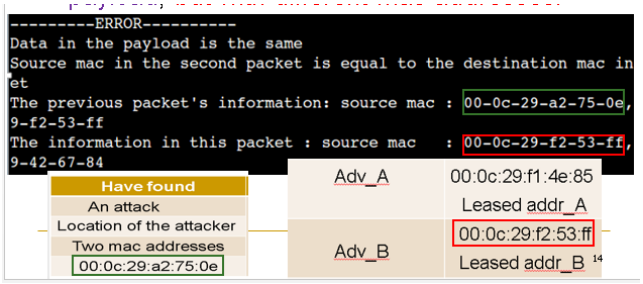


Fig. 11. Result of man-in-the-middle attack detection

3) Attacker Location Detection – Man-In-The-Middle Attack Detection On IPv4

The malicious DHCPv4 server detection on IPv4 network is similar to IPv6. However, a little difference should be known about man-in-the-middle attack detection on IPv4 network. Because the malicious DHCPv4 server could be a NAT router. The simulation topology can be found in Figure 12.

The malicious DHCPv4 server is configured with two interface cards so that it can pretend as a NAT server. Two interface cards connect to the same network. Both of them will be given an IP address, which is identical to addresses leased by real DHCPv4 server. In our example, the network to which the malicious DHCPv4 server connects is 192.168.2.0. We give interface cards two IP addresses 192.168.2.2 and 192.168.2.3 respectively. The leased address given by the malicious DHCPv4 server also belongs to 192.168.2.0, but router address will be 192.168.2.3 in malicious DHCPv4 packets. This type of NAT router does not assign other network's IP address to victims, for other network's IP address can be easily detected by administer using subnet mask. The malicious NAT server will use 192.168.2.3 to receive the victim's packets and forward it through the interface with the address of 192.168.2.2. We also examine the source IP address, destination IP address, protocol in header part, data payload, and mac addresses. If only mac addresses are different, we can make sure there is the man-in-the-middle-attack. And the result will be given in Figure 13.

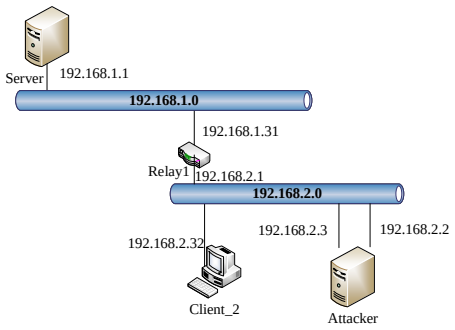


Fig. 12. Malicious NAT server on IPv4

No matter it is a NAT server or a normal router, the malicious DHCPv4 server will use one of two mac addresses to assign addresses to victim. Therefore, we can find out which mac address belongs to the attacker on IPv4 network as well.

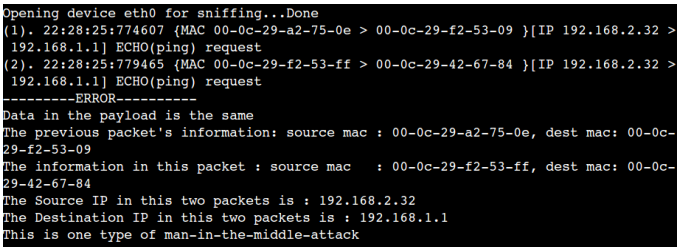


Fig. 13. Man-in-the-middle-attack detection on IPv4

B. Only One ADVERTISEMENT

1) DHCP Attack Detection

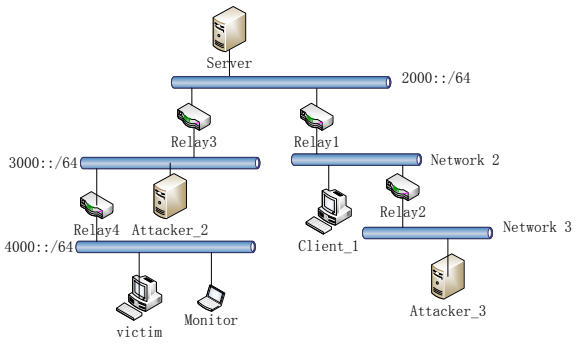
A packet sequence has been captured and its detail can be found in snapshot (a) in Figure 8, the right one. We can detect an attack by comparing two addresses. Client's mac address and real server's mac address are known. Server's mac address and its location are both unknown. But this time a new discovery, the address of the relay agent, has been discovered. We have introduced that the relay agent will add its address into the packet before forwarding the packet. So this packet REQUEST comes from 4000::1. It is no doubt that the malicious ADVERTISEMENT packet can be captured on that network. Therefore, we have to move our monitoring system into victim's network, 4000::1.

2) Attacker Location Detection On IPv6

On victim's network, we can capture the packet sequence just like snapshot (a) in Figure 8. The attacker's mac address can be directly found out, for we have known real server's mac address. And we found out the malicious DNS server address is 3000::23. Snapshot (a) in Figure 14 shows the result of traceroute, which indicates the attacker residing on 3000::/64. The whole topology shows in snapshot (b) in Figure 14.

```
relay2@relay2:~/Desktop$ traceroute6 3000::23
traceroute to 3000::23 (3000::23) from 3000::31, 30 hops max, 24 byte packets
 1  3000::23 (3000::23)  4.908 ms  0.962 ms  1.609 ms
```

(a) Result of traceroute6



(b) Attacker locates on 3000::/64

Fig. 14. Result of attacker location detection

3) Attacker Location Detection On IPv4

A malicious DHCPv4 server must be on the same network with the client. As the server's mac address can be known from DHCP Attack Detection, the malicious mac address can be found easily.

VI. Conclusion Discussion and Future Work

This paper has proposed a detection scheme, which can detect auto-configuration attack and locate the attacker. It does not need to be implemented on the routers or servers, but simply installed on a computer, which connects to the real DHCP server's network. This feature eases the burden of routers and servers, and indicates the scheme is cheaper than protection scheme, and it can be used in the real world.

Section V shows the result on IPv6 network. The detection scheme also can work well on IPv4 network. When the attacker and the real server reside on the same network, we should combine the DHCP attack detection with man-in-the-middle attack detection for locating the attacker. When they are on different networks, we should detect DHCP attack and move to victims' network for locating the attacker. In this situation, all routers on the IPv6 network should support traceroute program for locating the attacker. DHCP attack can always be detected on IPv4 and IPv6 network, man-in-the-middle attack only can be detected when the malicious router and the monitor on the same network.

Much work need to be done to refine the detection scheme. The problem about man-in-the-middle attack detection should be solved by other means. Another problem is the scheme needs to have some people involved in the second method of locating the attacker. These two problems can be solved by multiple monitors work together.

References

[1] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney, "Dynamic Host Configuration Protocol for IPv6(DHCPv6). RFC 3315," July 2003.

[2] Heinrich, Stuart, "Public Key Infrastructure Based On Authentication Of Media Attestments," Nov 2013.

[3] M. Janbeglou, M. Zamani and S. Ibrahim, "Redirecting Outgoing DNS Requests Toward A Fake DNS Server In A LAN," Software Engineering and Service Sciences, 2010 IEEE International Conference, pp. 29-32, July 2010.

[4] H. Kim and J.H. Huh, "Deteing DNS-poisoning-based Phishing Attacks From Their Network Performance Characteristics", Electronics Letters, pp. 656-658, May 2011.

[5] S. Groat, M. Dunlop, R. Marchany and J. Tront, "What DHCPv6 Says About You,""Internet Security 2011 World Congress , pp. 146 – 151, 2011.

[6] J. Tront, S. Groat, M. Dunlop and R. Marchany, "Security and Privacy by DHCP Unique Identifiers," Nano, Information Technology and Reliability 2011 15th North-East Asia Symposium, October, 2011.

[7] Z. Su, H. Ma, X. Zhang and B. Zhang, "Secure DHCPv6 that uses RSA Authentication integrated with Self-Certified Address," Cyberspace Safety and Security , September, 2011.

[8] J. W. Dai and L. F. Chiang, "A New Method to Detect Abnormal IP Address on DHCP," 2007 IEEE Region 10th Conference, November, 2007.

[9] S. Majumdar, D. Kulkarni and C. Ravishankar, "DHCP Origin Traceback," Proceedings of the 12th international conference, Distributed computing and networking, January 2011.

[10] P. Nikander, J. Kempf and E. Nordmark, "IPv6 Neighbor Discovery Trust Models and Threats," RFC 3756, May 2004.