Classification of DHCP Spoofing and Effectiveness of DHCP Snooping

Shigeo Akashi and Yao Tong
Department of Information Sciences, Faculty of Science and Technology
Tokyo University of Science
2641, Yamazaki, Noda City, Chiba Prefecture,
278-8510 JAPAN

Keywords: DHCP spoofing, DHCP snooping, DHCP relay agent, The longest matching prefix rule.

Abstract: It is well known that DHCP snooping is a famous countermeasure against DHCP spoofing. Actually, to what extent DHCP snooping can protect the authenticated DHCP clients from being given malicious DHCP transactions through the network where the authenticated DHCP clients and the malicious DHCP servers share with each other? The answer to this question is that DHCP snooping can protect DHCP spoofing to a certain extent, though DHCP snooping cannot protect DHCP spoofing completely. In the former half of this paper, it is shown that DHCP spoofing can be classified into two cases, namely DHCP spoofing from inside and DHCP spoofing from outside, and in the latter half of this paper, it is shown that DHCP snooping can protect the former attack from being implemented but cannot protect the latter attack from being implemented. More exactly speaking, it is shown that DHCP snooping cannot prevent DHCP spoofing from outside from being implemented, while applying the longest matching prefix rule to leading a malicious network segment which is constructed on the basis of the leaked DHCP transactions beforehand.

1 INTRODUCTION

The longest matching prefix rule is defined as the dynamic routing rule that any packet should be transferred through the interface advertising the network segment whose address matches longest with the prefix of the destination IP address of the packet. Since each entry in the routing table may specify each subnetwork, it is probable that one destination address may match more than one in the table entry. If such a case happens, it is reasonable that the most specific entry of the matching table entries, which is the entry with the longest subnet mask, should be adopted as the optimal destination. Therefore, if malicious application of the longest matching rule can be used for the implementation of the disguised packet transfer, then the authenticated DHCP clients to be led to another DHCP server which is not authenticated, and eventually, they may receive malicious DHCP transactions. Such an misorigination as this results in DNS cache poisoning, which is caused by the di□erent way from Kaminsky attack. In this paper, though DHCP snooping is still e□ective in DHCP spoofing from inside, in other words, in exclusion of malicious DHCP servers from being connected directly, it is shown that DHCP spoofing from outside can be implemented according to the method based on the fact that DHCP snooping cannot protect DHCP transactions from being leaked outside, because DHCP relay agent is incompatible with the longest matching prefix rule.

2 MISORIGINATION CAUSED BY THE LONGEST MATCHING PREFIX RULE

In this section, we explain the sequential process of the misorigination occurring in the course of disguised packet transfer in the following network topology:

Akashi, S. and Tong, Y.
Classification of DHCP Spoofing and Effectiveness of DHCP Snooping.
DOI: 10.5220/0008099002330238
In *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications (CTISC 2019)*, pages 233-238
ISBN: 978-989-758-357-5

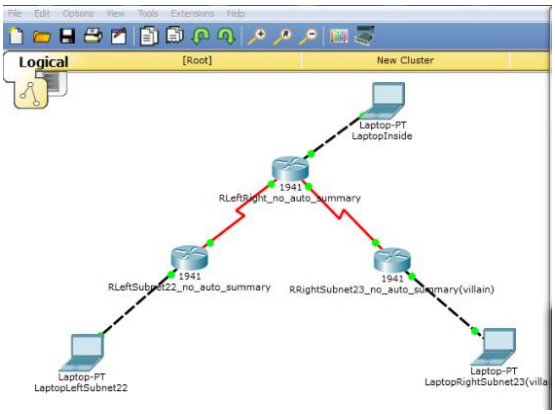

Figure 1: The structure of a sample network.

In Figure 1, it is shown that the router located in the upper central area forwards packets according to the longest prefix matching rule. The authenticated PC with its IP address 192.168.0.2/22 is located in the lower left area and the malicious PC with its IP address 192.168.1.2/23, for wiretapping the packets streaming on the communication line connecting these two PCs, is located in the lower right area. The other authenticated PC with its IP address 172.16.0.2/24 is located in the upper central area.

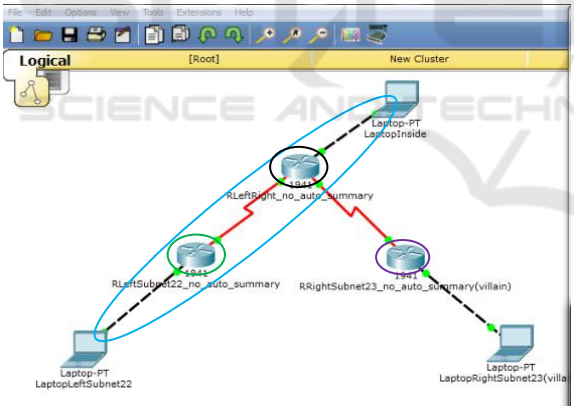

Figure 2: The optimal communication route connecting the authenticated PC located in the lower left area and the authenticated PC located in the upper central area.

In Figure 2, we assume that the authenticated PC located in the lower left area sends ICMP packets to the other authenticated PC located in the upper central area and receive the response. It is most optimal for the ICMP packets commuting these two authenticated PCs to take the route encircled in blue.

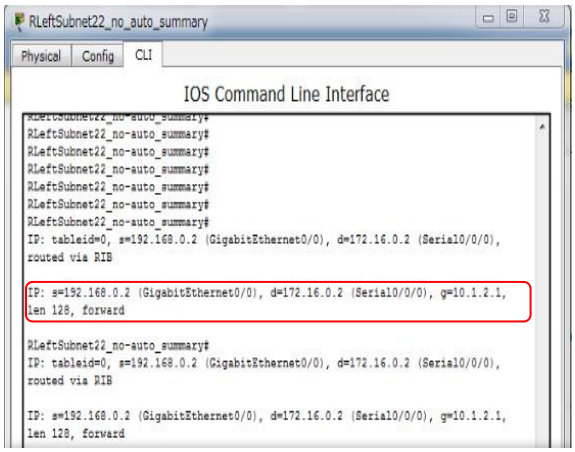

Figure 3: The record showing one-way packet streaming.

In Figure 3, it is shown that the router encircled in green in Figure 2 can catch the ICMP packets from the sender with its IP address 192.168.0.2, nevertheless, and that this router cannot catch the response from the receiver with its IP address 172.16.0.2.

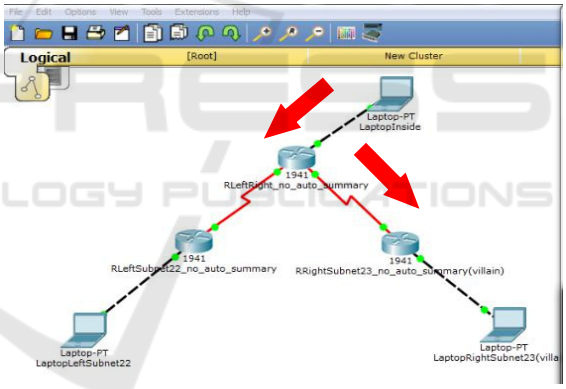

Figure 4: Misorigination applied to the response from the PC located in the upper central area.

In Figure 4, it is illustrated the route which the response from the PC located in the upper central area has taken. Since the router located in the lower left area advertises 192.168.0.0/22 to the upper central router and the router located in the lower right area advertises 192.168.0.0/23 to the same router, the router located in the upper central area forwards this response bound for 192.168.0.2 to the lower right area along the route followed by the above red arrows.

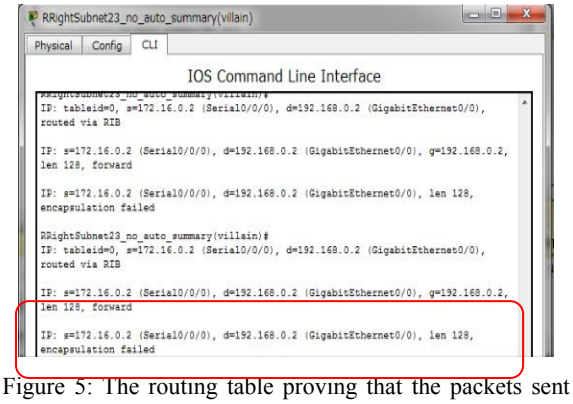

Figure 5: The routing table proving that the packets sent back for the response are misoriginated.

In Figure 5, it is shown that the router encircled in purple in Figure 2 catches the ICMP packets from the sender whose IP address is 172.16.0.2, which are bound for the receiver whose IP address is 192.168.0.2, even though this router exists in the outside of the optimal route, which is stated in Figure 2, connecting the lower left PC which is the destination with its IP address 192.168.0.2 and the upper central PC which is the origin with its IP address 172.16.0.2.

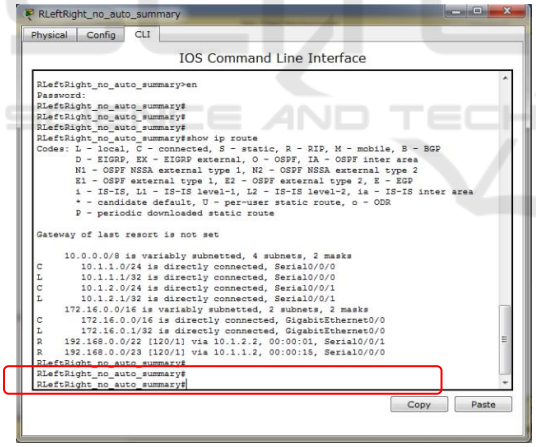

Figure 6: The routing table recording a malicious route for disguised transfer.

In Figure 6, the routing table of the upper central router encircled in black in Figure 2 shows that there exists simultaneously the route leading to the left-hand area which a serial interface with its IP address 192.168.0.0/22 advertises and the route leading to the right-hand area which another serial interface with its IP address 192.168.0.0/23 advertises. This is the reason why the longest matching prefix rule forces all the response to transfer at the disguised route whose destination is different for the original sender.

3 MALICIOUS APPLICATION OF THE MISORIGINATION TO DHCP SPOOFING

DHCP relay agent is defined as the function for packet transfer enabling any gateway router to forward DHCP transactions, to an authenticated and designated DHCP server, on condition that the this DHCP server cannot share its network segment with the authenticated DHCP clients. By the way, the DNS server translates a human-readable domain name such as example.com into a numerical IP address which is used to route communications between nodes. Normally, if the server does not know a requested name translation, it will ask another server, which is designated as this master server, and the process for inquiry continues recursively. To increase high quality performance, any DNS server will typically remember or cache these name translations for a certain amount of time. This means, if it receives another request for the same name translation, it can reply without asking any other DNS servers, until that cache expires. When a DNS server has received a false translation and caches it for the DNS server's performance optimization, it is considered poisoned, and it supplies the false data to the authenticated clients. If a DNS server is poisoned, it may return with an incorrect IP address, diverting tra□c to another computer administrated by a certain malicious attacker. These facts show us that mis- origination leading to malicious DNS servers, which is called DNS cache poisoning, can be broght about by DHCP spoofing. In this section, we can see the sequential process of misorigination in the course of establishing DHCP session by commuting DHCP packets such as DHCP discover, DHCP o□er, DHCP request and DHCP acknowledge, as the following:

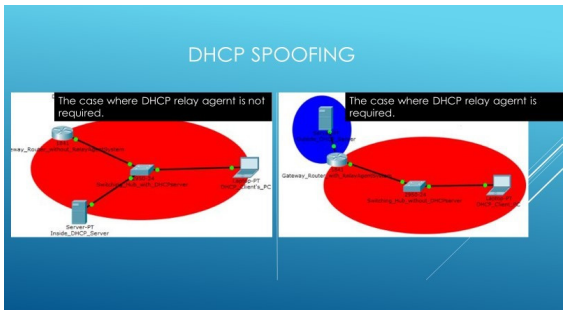

Figure 7: The difference he network segment requiring DHCP relay agents and the network segment not requiring DHCP relay agents.

In Figure 7, it is shown that, while the DHCP server situated in the left area shares its network segment with the authenticated DHCP client, the DHCP server situated in the right area and encircled in blue does not share its network segment with the authenticated DHCP client.

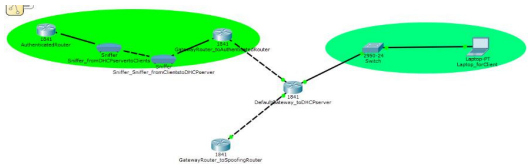

Figure 8: The role of the DHCP relay agents.

In Figure 8, we assume that the DHCP router situated in the upper left area whose network segment is 192.168.0.0/22 plays the role of the authenticated DHCP server and assume that there does not exist any intersection of the network segment where the authenticated PC situated in the upper right area belongs and the network segment where the authenticated DHCP router belongs.

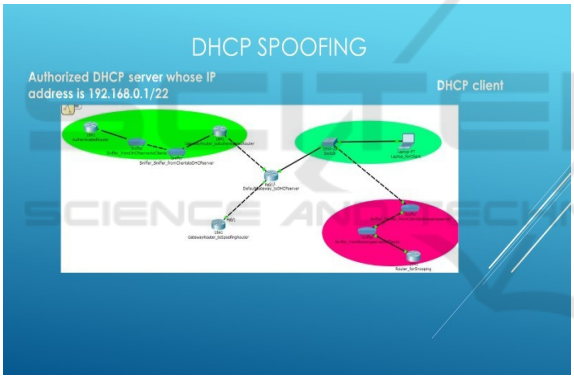

Figure 9: The network with malicious PC for sni□ng.

The procedure for DHCP spoofing from outside can be divided into two partial procedures, namely, the first partial procedure for sni□ng packets informing how to connect the authenticated clients to Internet and the second partial procedure for constructing a malicious DHCP server outside. More exactly speaking, the malicious PC can wiretap any DHCP transactions easily, even if DHCP snooping is equipped in the switch where the malicious PC is connected directly, because DHCP cannot prevent DHCP transactions from being leaked outside.

Step 1. As Figure 9 illustrates, the malicious router being situated in the red ellipsoid and sharing the network segment with the authenticated DHCP clients, must sniff to collect the DHCP transactions which are issued by the authenticated router and broadcast to the authenticated DHCP clients. The present way of broadcasting cannot prevent any malicious client from wiretapping DHCP transactions and from constructing another malicious DHCP server outside.

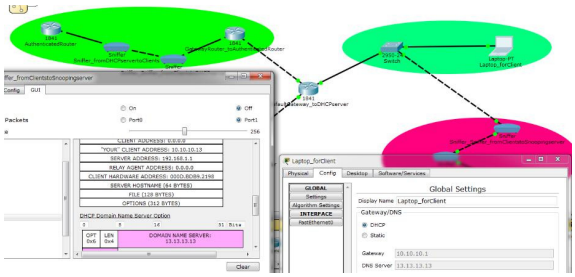

Figure 10: The proof showing DHCP spoofing succeeds.

In Figure 10, if we compare the table situated in the left area and the table situared in the right area , we can see that the authenticated DHCP transactions have sni□ed successfully.

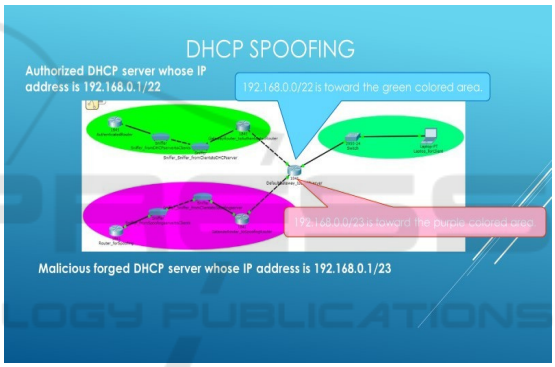

Figure 11: The location of a malicious DHCP server.

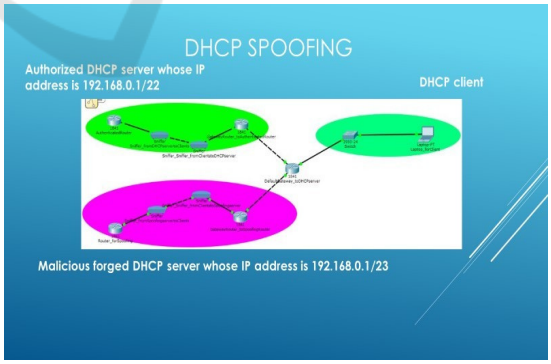

Figure 12: The role of the longest prefix matching rule.

Step 2. In Figure 11, it is shown that another malicious router which has been equipped with the DHCP transactions which have been wiretapped and collected in Step 1, issues fake DHCP transactions

for the purpose of leading the authenticated DHCP clients to another malicious network segment.

In Figure 12, it is shown that the route situated in the upper central area advertises the route bound for 192.168.0.0/22 and the route bound for 192.168.0.0/23 in its routing table simultaneously.

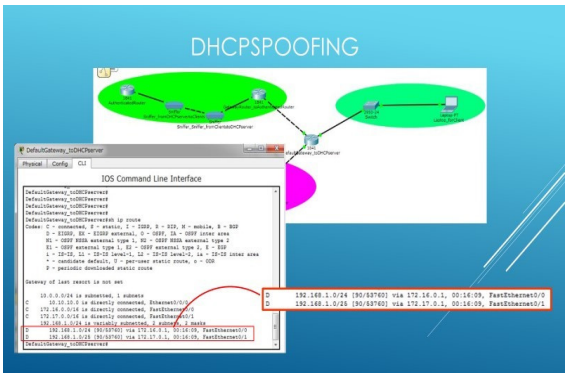

Figure 13: The routing table proving the disguised transfer of packets succeeds.

In Figure 13, it is shown that the DHCP transactions issued by the malicious DHCP router include an IP address assigned for another malicious DNS server for the purpose of leading DHCP clients to the malicious network segment which has been prepared beforehand. Since the network segment assigned for the authenticated DHCP router and the network segment assigned for the malicious DHCP router are 192.168.1.0/24 and 192.168.1.0/25, respectively, the longest matching prefix rule forces all the packets which are bound for 192.168.1.1 not to the network segment corresponding to 192.168.1.0/24 but to the network segment corresponding to 192.168.1.0/25, eventually.

4 A COUNTERMEASURE AGAINST DHCP SPOOFING FROM OUTSIDE AND CONCLUSION

Of course, any countermeasure should be based on the network devices under the control of the authenticated network administrators, and moreover, it should be realized without any di□cult preparation. Here, if we can assume that ICMP commands such as ping and traceroute can be used, there exists a countermeasure for the purpose of detecting the existence of DHCP spoofing, which can be illustrated as the following:

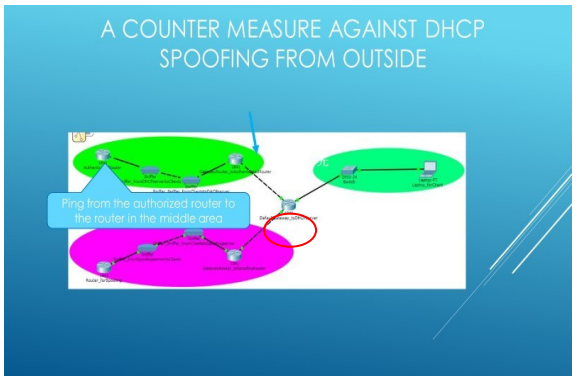

Figure 14: A countermeasure against DHCP spoofing.

In Figure 14, when the authenticated network administrator sends ICMP packets from the authenticated router to the gateway router encircled in red and located in the central area, the way of response from this router can be divided into two cases as the following:

Case 1. If any other malicious DHCP server is not connected from outside, then the response from the central gateway router can reach the authenticated router.

Case 2. If a malicious DHCP server is connected from outside, then the response from the central gateway router cannot reach the authenticated router.

This countermeasure cannot force the attackers to give up DHCP spoofing from outside, because this countermeasure cannot point out the exact topological location of the malicious DHCP servers, but this can detect the existence of DHCP spoofing from outside as we see. Actually, DHCP snooping has little e□ects on DHCP spoofing from outside, if the network segment where the authenticated DHCP servers exist is in the outside of the network segment where the authenticated clients exist, because the modern network constructing methods regulate that longest matching prefix rule should be prior to the DHCP relay agent.

REFERENCES

G. Ferrari, G. Colavolpe and R. Raheli, 2004, Detection Algorithms for Wireless Communications, John Wiley and Sons Ltd., West Sussex, 1st edition.

J. G. Gersting, 1982, Mathematical Structures for Computer Science, W. H. Freeman and Company, New York, 1st edition.

C. Hopps, 2000, Analysis of an Equal-Cost Multi-Path Algorithm, RFC 2992.

D. E. Knuth, 1973, The Art of Computer Programming, Addison-Wesley Publishing Company, Massachusetts, 2nd edition.

O. Santos and J. Muniz,2017, CCNA Cyber Ops Secfnd 210-250, Cisco Press, Indianapolis, 1st edition.

O. Santos and J. Muniz,2017, CCNA Cyber Ops Secops 210-255, Cisco Press, Indianapolis, 1st edition.

Cisco Systems, Inc., Catalyst 3750-X and Catalyst 3560-X Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later, 2013.