The Centralized management method to increase the security of ARP

Qinggui Hu

Neijiang Teachers College, Neijiang 641112, Szechwan Province, China

hu646100177@126.com

Keywords: ARP; OPNET; Lan; Buffer table; Concentration Management

Abstract. This study puts forward the new centralized management method to strengthen the security of ARP. The switch is the core of the LAN, it could manage ARP in concentration. When the switch receives the ARP request message， the switch will check the source address is legal or not. If the source address is legal, the ARP request message would be dealt with by the switch. Otherwise, the ARP request message would be discarded.

Introduction

With the development of communications and Internet technology, network security becomes more and more important. Although the address resolution protocol (ARP) [1] is one of the oldest (e.g. RFC 826 was defined in 1982) and most widely used (e.g. IEEE 802.11 and Ethernet), it is also one of the most vulnerable protocols. Every host, including gateways, maintains the ARP cache table which contains information on all valid pairs of media access control (MAC) and IP addresses on the local network. ARP cache management scheme includes static and dynamic modes. The former requires operator intervention in maintaining currency of all the cache entries which stay permanently until manually removed. Although known to be secure enough, it is seldom used in practice [2].

In this paper, the new centralized management method is put forward to strengthen the security of ARP. The switch is the core of the LAN, it could manage ARP in concentration. According to the author, when the switch receives the ARP request message，the switch will check the source address is legal or not. If the source address is legal, the ARP request message would be dealt with by the switch. Otherwise, the ARP request message would be discarded.

Working principle of ARP

ARP is the abbreviation of “Address Resolution protocol”. It is a TCP/IP protocol, which is used to interpret IP address into MAC address. With the protocol of ARP, one host could communicate with others. Every host has an ARP cache table, in which MAC and IP have the one-to-one relationship. When host A wants to communicate with host B, firstly, he could search the MAC of host B in his ARP cache. If he finds the right MAC, he could communicate directly. If he could not find the MAC, he could send out the ARP broadcast to look for the MAC of host B. When other hosts receive this ARP broadcast, if someone discovers he is the very host that the broadcast is looking for, he will send out ARP reply. When host A receives the reply, he will believe it without doubt and update his ARP cache. Then, the two hosts could communicate directly.

The new ARP management method: the centralized management

According to the opinion of the author, the cause of ARP security flaw lies in the decentralized management on ARP. If we adopt centralized management method, the security could be enhanced. The switch is the core of the LAN, it could manage ARP in concentration [3].

According to the author, when the switch receives the ARP request message，the switch will check the source address is legal or not. If the source address is legal, the ARP request message would be dealt with by the switch. Otherwise, the ARP request message would be discarded. As the following Fig.1 shows, the new protocol could work like the following steps.

Firstly, the switch has a cache table, which recording the ARP information of ‘IP-MAC-switch_port’. Secondly, when the switch receives the ARP request message, it does not broadcast the ARP request in LAN. However, the switch will check the source address is legal or not. If the MAC of the source address exists in the ARP cache table already, at the same time, both IP and switch_port of the source address are same with that of the ARP cache table, then, the source user is legal.

If the MAC of the source address exists in the ARP cache table, but IP or switch_port are NOT same with that of the ARP cache table, in this case, the source address is illegal, its ARP request message will be discarded. If the MAC of the source address DOES NOT exist in the ARP cache table, in this case, to suppose IP of the source address is A, MAC is B, then, the switch will broadcast the ARP package to ask ‘whose MAC is B, please reply your IP’. If the switch receives only one ARP reply, at the same time, the IP is just A, then, the source user is legal. The switch will update its ARP cache table. Otherwise, the source user is illegal. Its ARP request message will be discarded.

After the switch confirms the source user is legal, then, the switch will manage its ARP request message like the following steps. Firstly, the switch will check its ARP cache table. If the IP of the destination client exists in the ARP cache table, the switch will reply the ARP request message directly. If the IP of the destination client DOES NOT exist in the ARP cache table, the switch will broadcast ARP request to look for the destination client. If the switch receives only one reply, it will forward this ARP reply to the source host. At the same time, the switch will update its ARP cache table. If the switch receives two different ARP replies, those ARP replies would be discarded, and the switch will inform the source host that ARP query failure. If the switch receives no ARP replies, after a period of time, it will broadcast the ARP request again[4].

In addition, the switch will discard all ARP reply whose destination addresses are not the switch itself.

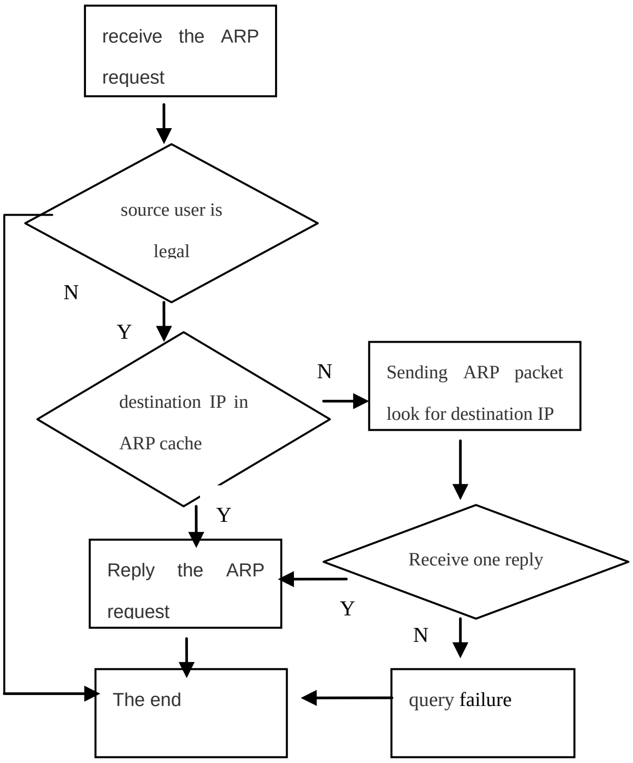

Fig. 1 work process of the new ARP management method

The simulation with OPNET

OPNET is a common network simulation software, it adopts three-layer model, which are process model, node model and network model respectively. The simulation result could reflect the performance of the network. Commonly, the network simulation includes the following steps, which are setting topology, design node model and proceeding model, setting traffic，run simulation etc[5].

To set the topology. In order to research the performance of the improved ARP protocol, the following simple network structure model is set up. As Fig.2 shows, 4 hosts connect a switch, the switch connects a router, the router connects another switch that connects 4 hosts also.

We suppose Wkstn1 send out lots of ARP spoofing packages to all other clients. According to traditional ARP protocol, all other clients will trust the ARP spoofing packages without doubt. But according to the improved ARP protocol, all the ARP packages will be dealt with by the switch. When the switch discovers the ARP packages are illegal, it will discard those ARP packages [6].

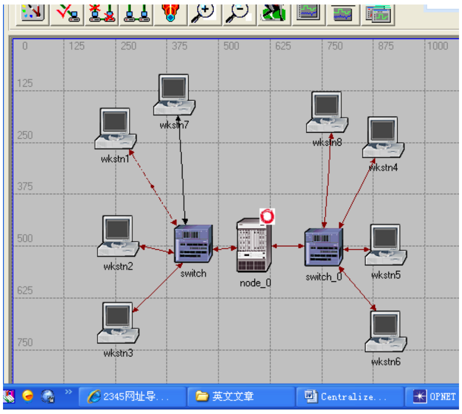

Fig. 2 The topology

The node model and the proceeding model. In above network structure model, the node model of all the client computers adopt 'ethernet_wkstn_adv' node model, which is carried by OPNET the software itself. At the same time, the node models of both the switch and the router are provided by the software itself.

In order to compare the different performance between the traditional ARP protocol and the improved ARP protocol, in above node model, for ARP module process, we adopt traditional ARP proceeding model, named 'ip_arp_v4', which is carried by the software itself,

Configure the business and simulation result. After the network structure model is set up and the process is designed, we configure the business for the network and determine the statistics. In order to compare the different performance between the traditional ARP protocol and the improved ARP protocol， We let Wkstn1 send out lots of ARP spoofing packages to all other clients. Under the different ARP protocols, we study the different simulation result.

In this simulation experiment, firstly, we gather the queuing delay from Wkstn2 to Wkstn6 as the statistics. As the Fig.3 shown, with the traditional ARP protocol, the value is about 0.000011 sec. But with the improved ARP protocol, the value is about 0.000007 sec. The simulation result shows the performance of the improved ARP protocol could be better. According the author's opinion, with the new ARP protocol, when Wkstn1 send out lots of ARP spoofing packages to all other clients, those ARP packages will be discarded by the switch. Those ARP spoofing packages could not influence the whole network. Then, the queuing delay from Wkstn2 to Wkstn6 is smaller.

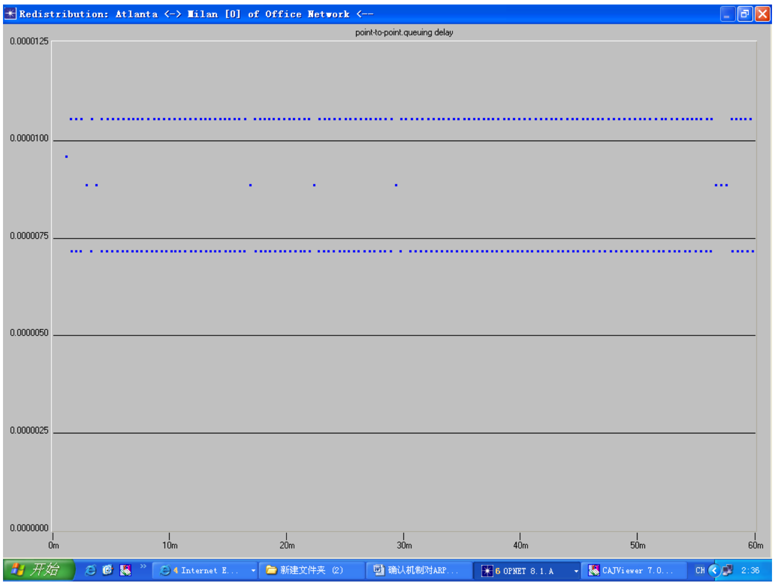

Fig.3 The queuing delay from Wkstn2 to Wkstn6

Conclusion

In this paper, we addressed how ARP attacks can be effectively defeated without modification of the ARP kernel software. Many approaches have attempted to address vulnerability associated with ARP cache management in dynamic mode. Yet, the security risk remained the same. We developed the new centralized management method is to strengthen the security of ARP. The switch is the core of the LAN, it could manage ARP in concentration. When the switch receives the ARP request message， the switch will check the source address is legal or not. If the source address is legal, the ARP request message would be dealt with by the switch. Otherwise, the ARP request message would be discarded. At last, the performance of the new protocol is simulated with OPNET software, which shows the new protocol could guard against the majority of ARP deceit.

References

[1] RFC-826: ‘An ethernet address resolution protocol’, 1982

[2] Kozierok, C.M.: ‘TCP/IP guide’ (No Starch Press, 2005, 1st edn.)

[3] http://arpspoof.sourceforge.net, accessed July 2011

[4] http://www.oxid.it/cain.html, accessed July 2011

[5] http://ettercap.sourceforge.net/index.php, accessed July 2011

[6] http://sid.rstack.org/arp-sk/, accessed July 2011

[7] http://www.toolcrypt.org/tools/tratt/index.html, accessed July 2011