The new method to prevent ARP spoofing based on 802.1X protocol

Qinggui Hu

Neijiang Teachers College, Neijiang 641112, Szechwan Province, China

hu646100177@126.com

Keywords: ARP; 802.1X protocol; authentication; MAC

Abstract: Address resolution protocol (ARP) is widely used to maintain mapping between data link (e.g.MAC) and network (e.g. IP) layer addresses. But it is well-known to be vulnerable to spoofing or denial of service (DoS) attacks. 802.1X protocol is the authentication standard for user access network released by IEEE. It is a port authentication protocol. This study utilizes 802.1X protocol to control ARP data packets. If MAC/IP authentication is successful, the protocol opens the port. Otherwise, the protocol shuts down the port. The simulation result shows the new method could guard against most ARP deception.

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 ARP management method is put forward to strengthen the security of ARP. 802.1X protocol is the authentication standard for user access network released by IEEE. It is a port authentication protocol. This study utilizes 802.1X protocol to control ARP data packets. If MAC/IP authentication is successful, the protocol opens the port. Otherwise, the protocol shuts down the port. The simulation result shows the new method could guard against most ARP deception.

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[3].

The work principle to prevent ARP spoofing with 802.1X protocol

802.1X protocol is the authentication standard for user access network released by IEEE. It is a port authentication protocol. Its purpose is to control a port is available or not. If authentication is successful, the protocol opens the port. Otherwise, the protocol shuts down the port, in this situation, only EAPOL (Extensible Authentication Protocol over LAN) messages could pass by the port.

802.1X system is a typical Client/Server Architecture. It includes Client、Device and Server[4].

Fig.1 The 802.1X system

As shown in Fig.1, the client is an entity located in LAN end. It is the user terminal equipment. The user can start 802.1X certification process. Usually , the client adopts Extensible Authentication Protocol over LAN (EAPOL) to start the certification.

The device is another entity located in LAN. Often, it is switch that provides the LAN ports for the client. Those ports could be physical port or logical port. Additionally, the switch should support 802.1X protocol, so that it could execute the certification for the client.

The authentication server is to provide certification services for the client. It could judge one client is legal or not. Typically, it is Remote Authentication Dial-In User Service (RADIUS).

Due to the defect design of ARP protocol, ARP spoofing occurs frequently in the network. In fact, we could adopt 802.1X protocol to strengthen ARP security management. According to the opinion of the author, as the Fig.2 shows, the new method could work like the following steps.

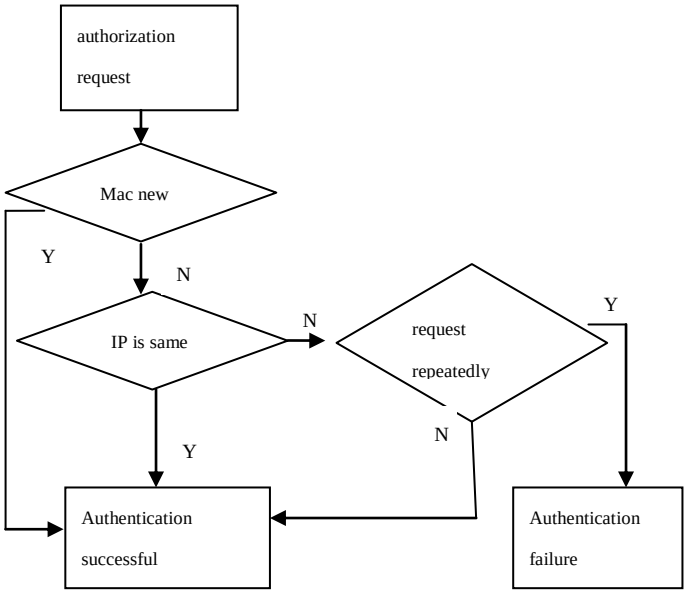

Fig.2 ARP authorization process

1. When the client start to connect other computers, the ARP certification process will run automatically. The ARP certification program will send a requesting authentication message to the switch, start the ARP certification process.

2. when the switch receives the request message, it will send back a message to request the Mac of the client.
3. when the client receives this information, it will send back the information of the Mac of the client to the switch.
4. When the switch receives the Mac information, it will convey the information to the server. When the server receives the Mac information, the server will compare it with the user information database. If the server finds this Mac in the database, then, the corresponding IP will be encrypted with a random character. The server will send the encrypted information back to the client through the switch. If the server finds No same Mac in the database, then, the information of 'This is a new user' will send back to the client through the switch.
5. When the client receives the encrypted information, it will calculate out the encrypted character through decrypting the information. Then, after the IP address is encrypted with the same character, it will be sent to the server through the switch.
6. when the server receives the IP address of the username, it will compare it with the user information database. If the IP address is correct, the verification is successful. If the IP address is different with that in the database, at the same time, the ARP certification requesting is the first time, it shows the user has changed his IP address, in this case, the verification is successful. If the client is a new user, the verification is successful. If the IP address is different with that in the database, at the same time, the ARP certification requesting is NOT first time, it shows one Mac is in correspondence with several IP addresses, in this case, the verification is failure.

The above steps show how the server judge one client is legal or not. On the whole, if the Mac is new, it shows the client is new user. If both the Mac and IP address are same with that in the database, it shows the client is a common user. If the IP address is different, at the same time, the ARP certification requesting is the first time, it shows the user has changed his IP. If the IP address is different, at the same time, the ARP certification requesting is NOT first time, it shows the client is illegal.

The simulation with OPNET

OPNET is an 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.3 shows, 4 wireless hosts connect the wireless switch, the switch connects the server. The server connects another switch, the switch connects 4 hosts also.We suppose Wkstn2 send out lots of ARP spoofing packages to all other Wkstns. According to traditional ARP protocol, all other clients will trust the ARP spoofing packages without doubt. But according to the improved ARP protocol, those ARP packages could not gain authentication successfully. Then, other Wkstns could not be influenced by the malicious ARP spoofing packages.

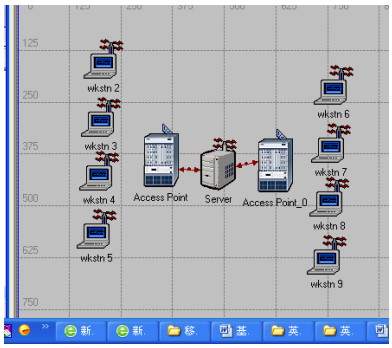

Fig. 3 The topology

The node model and the proceeding model. In above network structure model, the node model of all the Wkstns 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[6]. For the Wkstn’s node model, its ARP module proceeding is carried by the software itself also, named ‘wlan_mac’.

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 Wkstn2 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 average of requesting client custom application response time as the statistics. As the Fig.4 shown, with the traditional ARP protocol, the value is about 0.065 sec. After 802.1X protocol is adopted by the server, the value is about 0.012 sec. The simulation result shows the performance of the improved ARP protocol could be better. According the author’s opinion, after 802.1X protocol is adopted by the server, when Wkstn2 send out lots of ARP spoofing packages to all other clients, those ARP packages could not gain authentication successfully. Then, other Wkstns could not be influenced by the malicious ARP spoofing packages. So, the custom application response time is quicker.

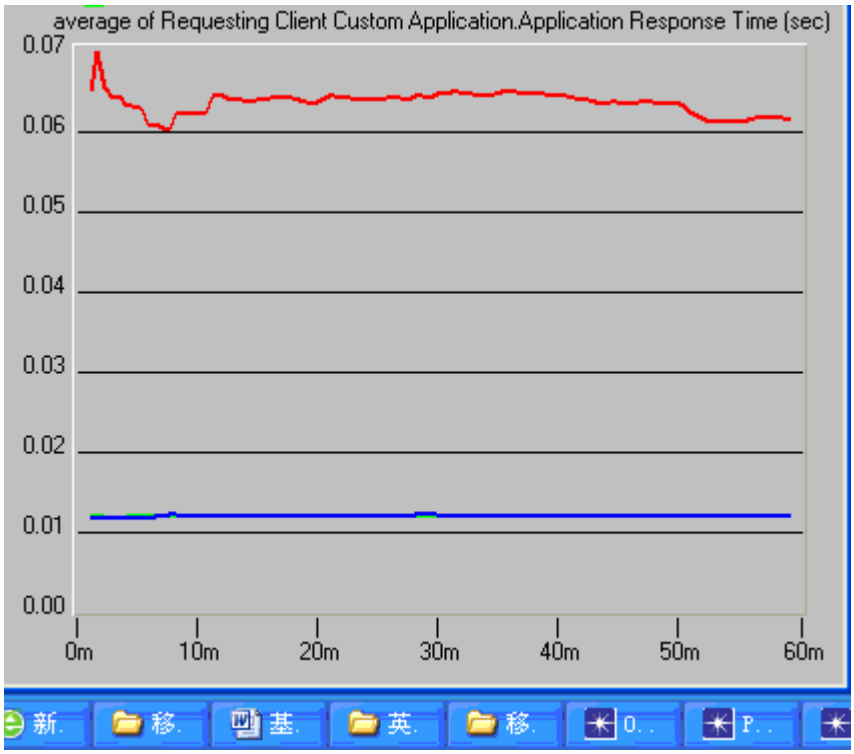

Fig.4 average of requesting client custom application response time (sec)

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. When 802.1X protocol is adopted by the server to control ARP data packets. The situation becomes better. If MAC/IP authentication is successful, the protocol opens the port. Otherwise, the protocol shuts down the port. In this case, the deception ARP packet could not go out. At last, the performance of the new protocol is simulated with OPNET software, the simulation result shows the new method could guard against most ARP deception.

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