Architecture and Protocols for Secure LAN

Thawatchai Chomsiri,

Faculty of Informatics, Mahasarakham University, Thailand

Summary
A lack of security is a problem of LAN systems in the present time since hackers can set a fake MAC Address and conduct ARP Spoof in order to capture the data by using the vulnerability of ARP: Address Resolution Protocol. The hackers in the same LAN as the victims can capture Cookies and Session ID and use them to access the system by the right of the victims. Moreover, hackers can also conduct MITM: Man in the Middle to hack HTTPS (decoding the password sent through HTTPS).

This research presents a design of "architecture and protocols" for the LAN security preventing the process of MAC Address spoofing, ARP Spoof and MITM. Each Network Card is designed to have Certificate issued by the product vendor in order to certify the MAC Address value. In addition, each Network Card has a Private Key and a Public Key. DHCP is redesigned to authenticate each Network Card before delivering IP Address. Besides, a new ARP protocols is presented in order to work correspondingly with DHCP Server. DHCP Server is assigned to be the "MAC-IP database center" which stores the data about matching between MAC Address and IP Address. When any Hosts want to enquire the MAC Address (for interested IP Address) an ARP Request will be sent to DHCP Server instead. In addition, the conditions of ARP Request and ARP Reply are modified so that they will be able to resist ARP Spoof and MITM.

Key words:
LAN Security, ARP Spoof, MAC Spoof, MITM, Certificate.

1. Introduction

In the present internet systems, to authenticate the members, websites use Session ID [1] sent with Cookies (Session ID is in Cookies). If hackers can capture the victims' Cookies, they will be able to access the victims' systems. Moreover, it is easy to conduct MITM [2][3] to deliver fake certificates to the victims and deceive them in order to gain important data sent via HTTPS [4]. Meanwhile, Password capturing in websites which send Passwords via HTTP and capturing the Password of POP3 and IMAP of LAN users still exist. All of the above, the problem is from the ARP Vulnerability [5] which does not have the authentication of the Network Card (whether or not the ARP Reply/Request sender is the real owner of that MAC Address). In addition, ARP also updates ARP Cache as soon as it receives ARP Reply or ARP Request.

This research aims at solving the problem about capturing data on LAN systems by ARP Spoof and the problem about a lack of authentication of Network Card. Each Network Card is designed to have a Certificate issued by the product vendor, and each will have a Private Key and a Public Key (using PKI [6]: Public Key Infrastructure). ARP enquiry (such as sending ARP Request to find the MAC Address value of IP Address which wants to communicate) will be sent to the center. DHCP Server will be used as "MAC-IP database center" (or we called ARP Server) to store the data about matching between IP Address and MAC Address. DHCP Server also has a function to answer and send ARP Reply. Besides, since each Network Card has a Private Key and a Public Key, they will be able to safely communicate with each other in Layer-2. This communication can be chose to be "Normal Mode" or "Secure Mode".

2. Background

2.1 ARP Spoofing

Hackers who are on the same LAN system as the victim or hackers who can remote hack any computers on the victims' LAN system will be able to sniff [7] the victims' data by using ARP Spoof [2][3][5] techniques. ARP Spoof is the process of sending ARP Request or ARP Reply to deceive the victims' computers which the hackers are Gateway Router. Then, hackers will send ARP Request or ARP Reply to deceive Gateway Router that the hackers' computers are the victims' computers. This technique uses weak point of ARP Protocol which no has a mechanism to authenticate. Another weak point is that ARP Table (ARP Cache) of any Host will be changed when receiving ARP Request or ARP Reply. This ARP Table will be instantly changed according to the data it receives (such as receiving ARP Reply as IP Address 192.168.1.1 containing MAC Address as AA-BB-CC-DD-EE-FF). The value in ARP Table will remain for 15 seconds, so the program used for conducting ARP Spoof must send ARP Packet to deceive the victims continually. The popular programs used for ARP Spoof are "arpspoof" on Linux (Auditor Security Tools and Back Track 3) and "Switch Sniffer" program. Besides, there is "Win ARP Spoof"

Manuscript received July 5, 2008.
Manuscript revised July 20, 2008.

program which runs on Windows. If on the Host which Static ARP is assigned such as using the command

```
arp –s 192.168.1.1 00-0C-85-72-05-FF
```

on Windows XP/2003/2008, the Host will have a permanent memory that IP Address 192.168.1.1 has MAC Address as 00-0C-85-72-05-FF. When hackers send ARP Packet to deceive that 192.168.1.1 has other values of MAC Address, the Host which the Static ARP is assigned, will not update the value in ARP Table accordingly. Therefore, Static ARP is a good method to prevent ARP Spoof.

2.2 HTTPS Background

The communication is triggered when a client send a request to the end-host by specifying an URL on HTTPS protocol [6] using port number 443. The web-server, providing a service for HTTPS, responds the client by sending the certificate to the client side. By this, web browser signifies a Public Key of the web-server, which packed in the certificate. The key is used to encode the information that the client sends consecutively to the web-serve. Technically, the initial information that the client sends to the web-server is a “session key”, which would be utilized for further data transmission between the client and the web-server. Consequently, web-server uses its Private Key to decode the information (session key) transmitted by the client. As a consequence, only either the web-server or the client understands the session key and that the further transmission is secured.

2.3 SSL MITM Background

Decoding HTTPS using SSL Man in the middle [4] has following steps:

2.3.1 Notifying a gateway-router that hacker-machine is victim-machine.

2.3.2 Notifying the victim-machine that the hacker-machine is gateway-router.

2.3.3 Enabling packet routing feature on hacker-machine.

2.3.4 Running DNS Spoof to enforce the victim to connect to HTTP/HTTPS port at hacker machine.

2.3.5 Distributing fake certificate to the victim.

2.3.6 Communicating with the victim using fake certificate

2.3.7 Communicating with the HTTPS web-site using genuine certificate obtained from the HTTPS web-site.

2.3.8 Transmitting the parameters and data between the victim and the HTTPS web-site.

2.3.9 Recording data transferred between two end-hosts.

2.3.10 Decode the data.

3. Design

In this research, the system was designed under the following conditions.

3.1 Network Card

In the Hardware level of Network Card, the data about MAC Address, Private Key, Public Key and Certificate (which certifies the matching between MAC Address and Public Key issued by the vendor and created in the production process in the factory), were build in Network Card. The Network Card has the following features.

- Use Private Key certified by the vendor.
- In the database of NIC Driver (Network Interface Card), there will be a Public Key of all vendors in order to claim the ownership of MAC Address (in ARP Packet and DHCP Packet, there will be certificate data).

3.2 DHCP Server

There must be a DHCP Server in the system to be the database of the matching between MAC Address and IP Address

- Identify the MAC Address value of the DHCP Server in the case that the Clients either use Dynamic IP Address or Static IP Address. (This design, we modify the OS-Network to have the channel (Text Box) to specify the DHCP Server’s MAC Address such as

DHCP Server MAC Address = [………………….])

- For Clients using Static IP Address (such as the Server Host), the values of MAC Address and IP Address must be set to the database of DHCP directly. (add in DHCP Service level to have the channel to specify the MAC Address and IP Address value of the Hosts which use Static IP Address) .

3.3 DHCP Protocol

DHCP Protocol must be modified as follows.

- DHCP must be added more function concerning answering the question in resolving MAC Address from known IP Address by using the existing data.
- Design that inside the DHCP Packet, there is a Certificate that certifies the matching between MAC Address and Public Key.
- Detect whether the IP Address requester is the real MAC Address owner before delivering the IP Address (checking from Certificate).

3.4 ARP Protocol

ARP Protocol must be modified as follows.

- For ARP Request, it is enquired from DHCP Server instead of Broadcast Enquiry from all Hosts.
- Design the ARP Packet to have a Certificate that certifies the matching between MAC Address and Public Key inside.
- When ARP Reply appears, it needs to be checked whether it comes from DHCP Server or not. If it does not come from DHCP Server, do not update the value in ARP Cache.
- When ARP Request appears, do not update Cache and do not send ARP Reply to respond.

3.5 The System Operation

To make it easy to understand, scenarios in different situations will be presented as follows.

3.5.1 Scenario 1: when there are one DHCP Server and one Host.

This scenario is the beginning step that we install DHCP Server to be ready to use, and the first user enters (Host-A). DHCP Server will deliver IP Address to Host-A, and DHCP is redesigned to authenticate each party. This will enable the system to prevent the attack in the case that hackers trick DHCP Server to deliver IP Address to them. In addition, it will also prevent DoS [8] (Denial of Service) which hackers pretend to do in order for DHCP Server to decode Packets deriving from the attack.

(a.) Host-A informs DHCP Server that it needs IP Address.

(b.) DHCP Server offer IP Address in return and authenticate Host-A by its Certificate.

(c.) Host-A authenticates DHCP Server (use vendor Public Key of DHCP Server's Network Card, in driver of Host-A to prove DHCP Server's MAC Address) and requests the IP Address as well as authenticates itself.

(d.) DHCP Server confirms that Host-A can use the IP Address.

In this case, if hackers want to pretend to conduct DoS [8] in order for DHCP Server to decode the unnecessary Packets, they (hackers) must decode to check in (c.) first. Then, DHCP Server will decode in (d.). Thus, it is equal in workload. If hackers want to conduct DoS to the full efficiency, they must use the Host with higher speed than that of DHCP Server or use several Hosts.

Details

1) Host-A is assigned to work as DHCP Client (assign "DHCP Server's MAC Address" on OS so that the Request will be sent to the real DHCP Server). Request IP Address by sending ARP Request direct to MAC of the known DHCP Server (we called DHCP Discovery). It is assumed that the Switch functions correctly (DHCP Discovery Packet will be sent to DHCP Server only).

2) DHCP Server check for available IP Address, and then offers to Host-A (we called DHCP Offer).

- In DHCP Offer, there is a sent along Certificate which certifies the matching between MAC Address and Public Key of DHCP Server.

3) When Host-A receives DHCP Offer, it will send DHCP Request as following details.

- Decode the Certificate of DHCP Server by Public Key of the vendor to make sure that the sent Public Key is from the MAC Address of DHCP Server.
- In this DHCP Request Packet, Host-A sends DHCP Packet along with Certificate which certifies the matching between MAC Address and Public Key of Host-A.

4) DHCP Server detects MAC Address of the requester whether it is the real one or not.

- The requester can be checked from the Certificate which is in DHCP Packet. (If the MAC Address decoded from Certificate matches with the MAC Address of Layer-2 frame, it is certain that the Request is from Host-A.)
- If it is correct, DHCP response will be sent to Host-A.

5) DHCP Server memorizes the data of Host-A (e.g. MAC Address, IP Address, Public Key and Type=Dynamic).

6) Host-A memorizes MAC Address and IP Address of DHCP Server in the form of Static and memorizes Public Key of DHCP Server as well.

Authentication is needed because the system must prevent the MAC Address false claim to get the IP Address. For the old DHCP Server, hackers can write a program to change MAC Address, and then request IP Address continuously until all IP Addresses are used up. An example of the programs used for this kind of attack is dhcpx [10] which comes with Back Track 3 [10]. In our new design, hackers cannot create MAC Address by themselves because they do not have the Private Key of the vendor. However, they can capture (collect data) the MAC Address value and Certificates of the Hosts. Still, they will not be able to request for IP Address because they do not know the Private Key value of each Network Card. (for this part we will get benefits in item 4.7)

3.5.2 Scenario 2: when the Host that used Dynamic IP Address (used DHCP Server) wants to find the MAC Address of other Hosts

Supposing that in the system, there are two Hosts which receive IP Address from DHCP Server, these two Hosts are Hosts A and Host-B.

1) Host-B sends a Request to DHCP Server, it needs to find MAC Address of Host-A. (This Request is named “IP2MAC Request.” (Modified of ARP Request))

2) DHCP Server searches for the reply and sends it to Host-B (This Reply is named “IP2MAC Reply.” (Modified of ARP Reply))

In this process, Host-B can send IP2MAC Request to DHCP Server correctly because it has the MAC Address of DHCP Server. However, hackers can attack the system by looping to false claim that they are the DHCP Server, and then they will send a false reply all the time in the process. Therefore, more conditions are added as the following details.

Details

1) Host-B sends a Request to DHCP Server (Host-B needs to find MAC Address of Host-A) by designing the Request to have the data in a field on IP2MAC Request to have a number randomly chosen by Host-B.

2) DHCP Server searches for the reply and sends it along with the random number to Host-B.

3) Host-B checks in the field if there is a random number matching with the number sent at the first time. If match, Host-B will accept that Reply.

The period from step 1 to step 3 must have the Time Out value (such as assigning to be 100 ms) in order to cut down the chance to encounter IP2MAC Reply Spoof sent by hackers who can correctly guess the number. Such Time Out value is adjustable. The less the value is, the more the security is. Supposing that hackers want to deceive Host-B, they need to send IP2MAC Reply Spoof all the time in the process. And supposing that the LAN system has Bandwidth = 1 Gbps, and the size of IP2MAC Reply is 1024 byte (8192 bit), the random numbers that hackers send to DHCP Server in 1 second is
(1*1024*1024*1024) / 8192 = 131,072 numbers.

If the number of bit is assigned to be 32 bit (gain 4,294,967,296 numbers), the chance for hackers to successfully attack the system is only
131,072 / 4,294,967,296 = 0.003%
(Time Out = 1 sec).

Thus, if the Time Out is assigned to be 100 ms, the chance for hackers to attack the system is only 0.0003%.

3.5.3 Scenario 3: when any Hosts want to find MAC Address of the Hosts using Static IP Address

Supposing that in the system, two Hosts-- Host-A and Host-B have already received IP Address from DHCP Server, and Host-C is assigned to be Static IP Address, when Hosts A wants to find MAC Address of Host-C, the operation will be similar to Scenario 2. However, after Host-A found MAC Address of Host-C; it must update the value in ARP Table (ARP Cache) to be Static ARP because Host-C does not need to change IP Address. In addition, the process that DHCP Server searches for MAC Address of Host-C will be conducted in the same way because specifying to Static has been conducted to the database on DHCP Server already. Besides, Type=Static is identified (Type=Static and Type=Dynamic are the additions in new DHCP design).

3.5.4 Scenario 4: IP Release

When any Dynamic Hosts want to return the IP Address value (e.g. command “ipconfig /release” on Windows), the Release Packet senders must authenticate themselves. This can be done by encrypt data by using Private Key of them. DHCP Server will decode by the Public Key of that Host. If it can be decoded, it is proved to be the real one (that is the benefit in item 4.8).

Details

1) Host-A sends Request for Release to DHCP Server.

2) DHCP Server randomly chooses a number and sends direct to Host-A.

3) Host-A accesses that code number and sends it to DHCP Server.

4) DHCP Server decodes by the Public Key of Host-A. If it found the correct number matching with the number sent at the first time, the IP Address of Host-A is allowed to be released.

3.6 Communication in Normal Mode and Secure Mode

Although the designed system can prevent ARP Spoof to capture the data, if the Network Administrator assigns some ports of switch to work as "monitoring ports" [10], hackers will be able to receive the frame of other people. The System is designed to be able to communicate in Layer 2, both in "Normal Mode" and in "Secure Mode".

The communication in Normal Mode is the regular communication (without encryption) which offers speed in sending and receiving the data. For Secure Mode, it is the communication with the process of data encryption which senders will encrypt the data by using the Public Key of the receivers. Therefore, it is certain that nobody can decrypt the data except the real receivers which have the Private Key.

We propose to encrypt/decrypt data by using ECC [11] Algorithm (Elliptic Curve Cryptography algorithms) which works faster than RSA Algorithm. ECC no need height performance of CPU to process. In the same security level (in the same "successful – crack time"), ECC will use less bit numbers of the Key than RSA does.

4. Benefits

If this design is authentically implemented in Network Card, and the new DHCP and ARP as presented are used, the benefits will be as follows.

4.1 It can be checked whether the Host that we are communicating with is the owner of the claimed MAC Address or not. (Preventing MAC Address Spoofing)

4.2 It can be checked whether the Host that we are communicating with is the owner of the claimed IP Address or not. (Preventing IP Address Spoofing)

4.3 From items 4.1 and 4.2, ARP Spoofing can be prevented. The result is that data capture on LAN can be prevented.

4.4 From item 4.3, MITM: Man in the Middle and HTTPS Decoding/Hacking [4] can be prevented. (HTTPS Decode uses the MITM technique.)

4.5 Illegal DHCP Servers can be prevented (rough DHCP Servers cannot disturb the LAN system) because every Client will identify MAC Address of DHCP Server which is used.

4.6 It is unnecessary to use other more Servers. (For example, S-RAP [12] Protocol needs to use AKD [12]: Authoritative Key Distributor.)

4.7 DHCP Server can be protected in the case that hackers deceive DHCP Server to deliver all IP Address to them.

4.8 Hosts can be protected in the case that hackers send DHCP Release IP by deceiving that they are Hosts.

4.9 There is an alternative to be able to communicate in Normal Mode for the speed in sending the data and communicate in Secure Mode which has the process of data encryption which can be decrypt by only the frame owner (the owner of destination MAC Address).

5. Related Work

There are some researches to solve the ARP Spoof problem by S-ARP [12], but it is found that S-ARP still encounters some problems as follows.

1) Hackers can fake MAC Address.

2) S-ARP is designed to have AKD [12]: Authoritative Key Distributor to keep and distribute the Public Keys of all Hosts in the system. However, the problems are found as follows.

- It is needed to add one more Servers although the data about the matching between IP Address and MAC Address already exists in DHCP Server.

- If AKD crashes down, the system cannot be used.

- AKD needs to be modified in order to be able to communicate with DHCP Server.

- Clients need to contact ADK every time they receive ARP Reply in order to request the Public Keys of ARP Request senders. Then, bring it to work load.

- There could be more than one AKD, so it is possible that attackers will be able to fake an AKD to allow them to access the system.

3) S-ARP will check only ARP Reply while the Netcut [13] program will deceive the victims by sending ARP Request.

4) It is inconvenient in the first installation. That is, a Private Key and a Public Key need to be created for each Host. Besides, the value of Public Keys and IP Address of AKD must be identified for all Hosts.

5) Clients need to communicate with AKD every time they receive ARP Reply, and this may decrease the system performance.

6) It is possible that the system will be attacked by ARP Reply Attack which causes the victimized Host to focus only on decoding. Although S-ARP is designed to possess Time Stamp to solve the problem, hackers can also set the Time Stamp value in order for the system to evaluate the Packets used to attack.

7) S-ARP cannot be used with other Gateways which are not Linux.

8) Kernel of all clients must be modified, and other programs must be installed. (For example, sarpd [12] daemon program must be installed.)

6. Conclusion and Future Work

This research presents the design of the communication in the LAN system which has high security. This is to authenticate the MAC Address owners, preventing hackers to fake MAC Address and use it to attack the system. The system is also designed to have the protection against ARP Spoof and MITM attack by assigning each Network Card to have a Certificate issued by the vendor. Each Network Card also has a Private Key and a Public Key build in, which were created during the production process (in the factory) and store in the Hardware level (Network Card). DHCP Server is used as the IP-MAC database center about the matching between MAC Address and IP Address. At the same time, DHCP Server also functions as the ARP Reply sender to answer for the ARP Request. In the presented system, the operation in Protocol level of DHCP and ARP will be modified to suit and match with each other in order to co-work efficiently and safely. In addition, users can choose to communicate in Normal Mode for the speed in sending the data, or in Secure Mode which needs to have the process of data encryption for the security. This data can be decrypt by only the frame owners (the owners of destination MAC Address).

References

[1] Michael Cross, Developers Guide to Web Application Security, Syngress Publishing Inc., 800 Hingham Street Rockland, MA 02370, 2007.

[2] D. Song. A suite for man in the middle attacks. http://www.monkey.org/~ dugsong/dsniff.

[3] R. Wagner. Address resolution protocol spoofing and manin-the-middle attacks. http://rr.sans.org/threats/address.php, 2001.

[4] "HTTPS Hacking Protection". Thawatchai Chomsiri. Proc. of the IEEE 21st International Conference on Advanced Information Networking and Applications (AINA-07), Volume 1, IEEE CS Press, May 2007, Niagara Falls, CANADA.

[5] B. Fleck. Wireless access points and arp poisoning. http://www.cigitallabs.com/resources/papers/download/arpp oison.pdf

[6] "Computer Networking: a top-down approach featuring the Internet", Keith W. Ross, James F. Kurrose., Addison Wesley Longman, Inc. ISBN 0-201-47711-4. USA.

[7] Ethereal Packet Sniffing. Angela D. Orebaugh, Gilbert Ramirez. ISBN: 1932266828. February 2004. Publisher: Syngress Publishing

[8] Hacking Exposed 5th Edition Author(s): Stuart McClure Joel Scambray George Kurtz. ISBN: 0072260815, April 19, 2005.

[9] Remote-Exploit.org - Supplying offensive security products to the world
(URL: http://www.remote-exploit.org/backtrack.html)

[10] Cisco Systems - Catalyst Switched Port Analyzer (SPAN) Configuration Example
(URL: http://www.cisco.com/warp/public/473/41.html)

[11] "Use of elliptic curves in cryptography ", Lecture Notes in Nomputer Sciences; 218 on Advances in cryptology---CRYPTO, Santa Barbara, California, United States, pp: 417 - 426, 1986, ISBN:0-387-16463-4

[12] "S-ARP: a secure address resolution protocol", Bruschi, D. Ornaghi, A. Rosti, E., Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003), 2003, pp 66 – 74.

[13] www.sgc.co.th/netcut.php

Thawatchai Chomsiri is a lecturer at department of Information and Communication Technology, Faculty of Informatics, Mahasarakham University Thailand. He received the B.Sc. degree in Statistical Science from Faculty of Science, Mahasarakham University in 1995. He obtained his M.Sc. degree in Information Technology from Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang (KMITL) Thailand in 2005. During 1995-2005, he works in the field of Computer and Information Technology. He has experience in many positions such as Programmer, System Engineer and Network Administrator. He is an author of the book "HACK Step by Step" – best seller computer book in Thailand (year 2003).