Address Resolution Protocol (ARP) Spoofing: Attacks and Defenses

Bruno Duarte

Lusofona University of Porto, Portugal
a21802084@mso365.ulp.pt

Abstract. Nowadays, address resolution protocol spoofing attacks are becoming more and more, so it is necessary to know how to defend ourselves from it. With this work will be addressed several topics within ARP Spoofing, firstly will be started by explaining what the address resolution protocol (ARP) is as well as the constituents of it. Next, will be explained the types of ARP (ARP caching, Inverse Arp, Reverse Arp, among others). In a second part, will focus my work on ARP Spoofing explaining how it is well to say the types of attacks of the same, last presented the defenses that the user can use to be able to prevent these same attacks.

Keywords: ARP, Spoofing, Attacks, Defenses.

1 Introduction

With the desire to improve the security of the users, the address resolution protocol (ARP) Spoofing comes increasingly to be topic of conversation by the worse reasons since this is one of the ways of the people being attacked by hackers, being possible that the same ones obtain steal data, steal passwords using them to perform larger crimes, even get DoS attack to deploy servers below with the successive sending of multiple packets to the network.

ARP operates by sending out “ARP request” packets. An ARP request asks the question, “Is your IP address x.x.x.x? If so, send your MAC back to me.” These packets are broadcast to all computers on the LAN, even on a switched network. Each computer examines the ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply containing its MAC address.[1]

2 Address Resolution Protocol (ARP)

The address resolution protocol (ARP) is a low-level network protocol for translating network layer addresses into link layer addresses. [2] ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapping to IP addresses. [3]

IP addressing occurs at Layer 2 (data link) and Layer 3 (network) of the Open System Interconnection (OSI) reference model Layer 2, addresses are used for local transmissions between devices that are directly connected. The use of Layer 3 addresses is for indirectly

10.11228/dpsc.01.01.013

connected devices in an internetwork environment. Each network uses addressing to identify and group devices so that transmissions can be sent and received. [3]

For devices to be able to communicate with each other when they aren´t part of the same network, the 48-bit MAC address must be mapping to an IP address. Some of the Layer 3 protocols used to perform the mapping is:

- Address Resolution Protocol (ARP);
- Reverse ARP (RARP);
- Serial Line (SLARP);
- Inverse ARP

The ARP was developed to enable communications on an internetwork and is defined by RFC 826. Layer 3 devices need ARP to map IP network addresses to MAC hardware addresses so that IP packets can be sending across Network. [3]

Before a device sends a datagram to another device, it looks in its ARP cache to see if there are a MAC address and corresponding IP address for the destination device. If there is no entry, the source device sends a broadcast message to every device on the network. Each device compares the IP address to its own. Only the device with the matching IP address replies to the sending device with a packet containing the MAC address for the device (except in the case of "proxy ARP"). The source device adds the destination device MAC address to its ARP table for future reference, creates a datalink header and trailer that encapsulates the packet, and proceeds to transfer the data. [3]

The ARP request message has the following fields:

- HLN, Hardware address length. Specifies how long the hardware addresses are in the message. For IEEE 802 MAC addresses (Ethernet) the value is 6.
- PLN, Protocol address length. Specifies how long the protocol (Layer 3) addresses are in the message. For IPv4, the value is 4.
- OP, Opcode specifies the nature of the message by code:
    - ARP request
    - ARP reply
    - through 9 -- RARP and Inverse ARP requests and replies
- SHA, Sender hardware address specifies the Layer 2 hardware address of the device sending the message.

- SPA, Sender protocol address specifies the IP address of the sending device.
- THA, Target hardware address specifies the Layer 2 hardware address of the receiving device.
- TPA, Target protocol address specifies the IP address of the receiving device.

3 Types of ARP

3.1 Arp Caching

All operating systems maintain ARP caches that are check before sending an ARP request message. Each time a host needs to send a packet to another host on the LAN, it first checks its ARP cache for the correct IP address and matching MAC address. The addresses will stay in cache for a couple of minutes. You can display ARP entries in Windows by using the arp -a command. [4]

3.2 Static and dynamic entries in the ARP Cache

The ARP cache takes the form of a table containing matched sets of hardware and IP addresses. Each device on the network manages its own ARP cache table. There are two different ways that cache entries can put into the ARP cache [5]:

- Static ARP Cache Entries: These are addressing resolutions that are manually added to the cache table for a device and are keeping in the cache on a permanent basis. Static entries are typically managed using a tool such as the arp software utility.
- Dynamic ARP Cache Entries: These are hardware/IP address pairs that are added to the cache by the software itself resulting in successfully-completed past ARP resolutions. They are kept in the cache only for a period and are then removing.

A device's ARP cache can contain both static and dynamic entries, each of which has advantages and disadvantages. However, dynamic entries are used most often because they are automatic and don't require administrator intervention.

3.3 Inverse ARP (InARP)

The inverse Arp is the opposite of ARP. Instead of using Layer-3 address (IP address) to find MAC address, Inverse ARP uses MAC address to find the IP address. This same method is only used for device configuration and is enabled by default in ATM (Asynchronous Transfer Mode) networks. Inverse ARP is used to find Layer-3 address from Layer-2 address (DLCI in frame relay) dynamically mapping local DLCIs to remote IP addresses when you configure Frame Relay. When using inverse ARP, we know the DLCI of a remote router but do not know its IP address sending a request to obtain that IP address and map it to the Layer 2 frame-relay DLCI. [6]

3.4 Reverse ARP (RARP)

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-routers ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address. When a new machine is configuring or any engine which doesn't have memory to store the IP address, needs an IP address for own use[7].

3.5 Proxy ARP

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or default gateway. [8]

3.6 Serial Line Address Resolution Protocol (SLARP)

Serial Line Address Resolution Protocol (SLARP) requests. AutoInstall will use the first available method (DHCP, BOOTP, RARP, or SLARP) for configuration. If all LAN interface configuration options fail, AutoInstall will attempt to configure an available serial interface using SLARP. Though DHCP is the preferred method for AutoInstall over LAN interfaces, these other options remain enabled to ensure backward compatibility with older network topologies. SLARP is an extension of Cisco HDLC, where if the remote router of the serial link does not yet have a config saved in NVRAM, the router will SLARP on the connected serial link to obtain a valid IP address. This feature benefits the Cisco autoinstall feature where an admin can connect a recent router to the network and have limited connectivity with little effort.[8]

3.7 Authorized ARP

Authorized ARP addresses a requirement of explicitly knowing when a user has logged off, either voluntarily or due to a failure of a network device. It is implemented for Public wireless LANs (WLANs) and DHCP.[3]

4 ARP Spoofing

Address Resolution Protocol (ARP) spoofing attack is a type of network attack where an attacker sends fake Address Resolution Protocol (ARP) messages inside a Local Area Network (LAN), with an aim to deviate and intercept network traffic.

In normal Address Resolution Protocol (ARP) operation, when a network device sends an ARP request (as broadcast) to find a MAC address corresponding to an IPv4 address, ARP reply comes from the legitimate network device which is configuring with the IPv4 address which matches the ARP request.

The ARP reply is caching by the requesting device in its ARP table. A network attacker can abuse Address Resolution Protocol (ARP) operation by responding ARP request, posing that it has the requested IPv4 address.

Once the attacker's MAC address is mapping to an authentic legitimate IPv4 address, the attacker will begin receiving any data that is intended for that legitimate IPv4 address.

Now the attacker can launch a man-in-the-middle attack can start capturing the network traffic for any sensitive user data. [9]

Arp Spoofing is different from Spoofing because the spoofing is fraudulent or malicious practice in which communication is sending from an unknown source disguised as a source known to the receiver. [10]

4.1 ARP Spoofing - Attacks

A man-in-the-middle attack requires three players. There’s the victim, the entity with which the victim is trying to communicate, and the “man in the middle,” who are intercepting the victim’s communications. Critical to the scenario is that the victim isn’t aware of the man in the middle.

How does this play out? Let’s say you received an email that appeared to be from your bank, asking you to log in to your account to confirm your contact information. You click on a link in the email and are taking to what appears to be your bank’s website, where you log in and perform the requested task.

In such a scenario, the man in the middle (MITM) sent you the email, making it appear to be legitimate. The attacker also created a website that looks just like your bank’s website, so you wouldn’t hesitate to enter your login credentials after clicking the link in the email. But when you do that you’re not logging into your bank account, you’re handing over your credentials to the attacker.[11]

A “denial of service” or DOS attack is used to tie up a website’s resources so that users who need to access the site cannot do so. Many major companies have been the focus of DOS attacks in recent years. Because a DOS attack can be easily engineered from nearly any location, finding those responsible can be next to impossible.

Unlike a virus or malware, a DOS attack doesn’t depend on a special program in order to run. Instead, it takes advantage of a natural vulnerability in the way computer networks communicate.

Here’s an example: suppose that you wish to visit an e-commerce site in order to shop for a gift. Your computer sends a small packet of information to the website. This packet works as a “hello” – basically, your computer says, “Hi, I’d like to visit you, please let me in.”

When the server receives your computer’s message, it sends a short one back, saying, in a sense, “Okay, are you real?” Your computer responds – “Yes!” – and communication is established. The website’s homepage then pops up on your screen, and you can explore the site. Your computer and the server continue communicating as you click links, place orders, and carry out other business.

In a DOS attack, a computer is rigged to send not just one “introduction” to a server, but hundreds or sometimes thousands. The server—which cannot tell that the “introductions” are fake sends back its usual response, waiting up to a minute in each case in order to hear a reply. When it gets no reply, the server shuts down the connection, and the computer executing the attack repeats, sending a new batch of fake requests.[12]

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resources, and cause a denial of service for users of the targeted resource. [13]

The session hijacking is a type of web attack. It works based on the principle of computer sessions. The attack takes advantage of the active sessions.

The session refers to a certain time period that communication of two computer systems or two parts of a single system takes place. The session will be valid up to the end of the communication. In some cases the session is user-initiated. However, many of the active sessions will be hidden from the users. They will not know when a session starts and ends. The session is an important factor in Internet communications.

Coming to the session hijacking, as we’ve seen earlier, the attacker uses the active session for implementing the attack. For most Internet communications, authentication will be needed. Authentication can be done in different methods. The most used method is the user be asked to enter a predefined username and password by the website. When the user enters this credentials, the system will check the same with the stored details. If the entered details match with the stored details, the system grants access to the particular user to the particular database or part of the website.[14]

4.2 Arp Spoofing - Defenses

Most importantly, always make sure you're browsing securely. By encrypting the traffic between the network and your device using browsing encryption software, you can help fend off potential man in the middle attacks.

Always make sure the sites you're visiting are secure. Most browsers show a lock symbol next to the URL when a website is secure. If you don't see this symbol, check to see if the web address is preceded by "https." The "S" stands for secure, and this ensures your data won't be open to hacker interception.

Using a firewall is also a reliable way to help defend your browsing data. Although it's not foolproof, a firewall provides an extra layer of security when you're using public Wi-Fi. If you browse public Wi-Fi often, it's prudent to set up a virtual protected network (VPN). This type of network secures your traffic and makes it much more difficult for hackers to intercept it.

Keep your security solution software up to date. Cybercriminals won't stop adapting and honing their craft—and neither should the good guys. By ensuring your security solution is up to date, you always have access to the latest cutting-edge tools to keep a watchful eye on your online activity for safe, fun, secure browsing. [15]

The most effective way to protect against the impact of DoS attacks is to stop them before they even reach a company’s network. That means partnering with the contracted ISP to block the attack at the gateway. This blunts their impact by protecting even network border devices from being overwhelmed by the flood of malicious traffic. Many ISPs offer a “clean pipes” service-level agreement that commits to a guaranteed bandwidth of legitimate traffic rather than just total bandwidth of all traffic.

In addition to this possibility it exist protection devices to further guard their networks against attack. These devices sit at the network perimeter and process traffic before it. They may be used in conjunction with a clean-pipes ISP service or a stand-alone solution when ISP protection is not available. Solutions in this category include the CheckPoint DDoS Protector and Radware DefensePro. [16]

The following are some of the ways to safeguard against session hijacking[17]:

- Use secure shell (SSL) to create a secure communication channel
- Use encrypted protocols that are offered at OpenSSH suite
- Pass authentication cookies over the HTTPS secure connection
- Implement the log-out functionality for each user to invalidate the session
- Generate different session ID after each successful login and logout
- Always pass the encrypted information between the users and the web servers
- Use string or long random variables as a session key
- Use different username and password for each account
- Configure the suitable internal and external spoof rules on gateways
- Do not transport session ID within the query string
- Limit incoming connections and Minimize remote access

5 Demonstration

In this section, I will demonstrate at the practical level how to make an email spoofing attack for this, we will use a PHP script. This script is very easy to use as I'll demonstrate below. This tool can be found in GitHub with the name email-spoofer being that the author of this tool has the name of Shumbham Badal in GitHub being, for this reason, the creator of this script.

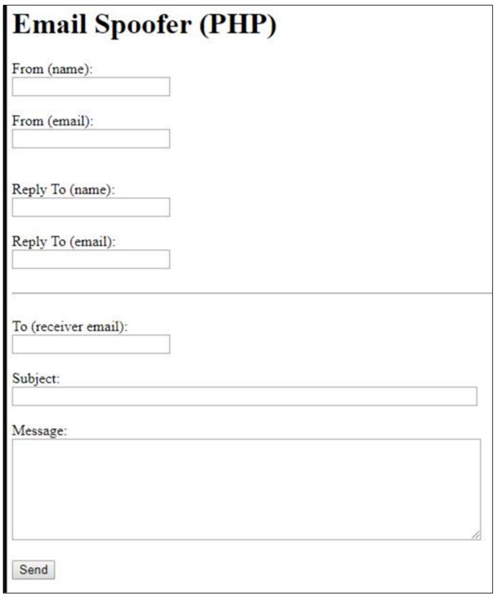
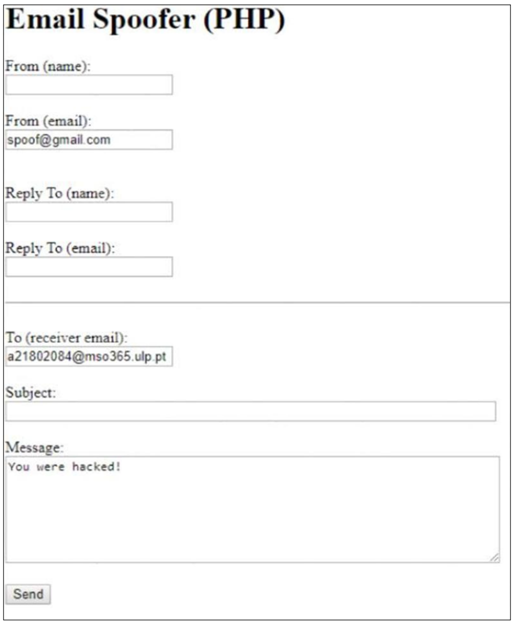


Fig.1. Email Spoofer tool.

For the test, I will put a fake email so that it is presented with the same "spoof@gmail.com" and I will send a message "You were hacked!" and send it to one of my emails thus ensuring that it works.

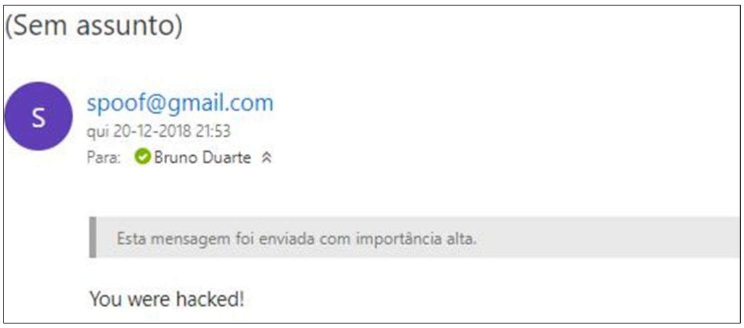


From (email): spoof@gmail.com

To (receiver email): a21802084@mso365.ulp.pt

Message: You were hacked!

Fig.2. Email Spoofer pre-filled



(Sem assunto)

spoof@gmail.com
qui 20-12-2018 21:53
Para: Bruno Duarte

Esta mensagem foi enviada com importância alta.

You were hacked!

Fig.3. Email received.

With this test we can note that, in fact, this same script works well as it becomes easy to use, being only necessary to know the email of the person we want to attack. This script consists of 3 "pages" of PHP, the first one called index is the main page, in the other words, how the tool appears to us when opening. The second page consists of the direct-mailer which is the page where we will show the result of the sending, that is, if the email was sent or if there was an error. The third page is where the sending of this same email, is an intermediate page and is dubbed form-mailer. On the other hand, Gmail, for example, can send these emails directly to the spam box, ignoring them.

6 Conclusion

With this document, it is possible to realize that there are several strategies of attack to a certain user, in contrast, it is also demonstrated all the types of defenses for each one of these possible attacks to do. Besides these aspects, that give more emphasis to the defense as well as the attack by the hacker, one also begins to perceive better all types of ARP as well as the differences between each of the same.

Finally, with this final demonstration, we can see that this type of attack is easy to make the user aware so he can fight to always have the protection of the same in mind.

References

1. Whalen, Sean, "An Introduction to ARP Spoofing", (2001).
2. Techopedia.com Homepage "Address Resolution Protocol (ARP)", accessed (2018).
3. Cisco.com Homepage "IP Addressing: ARP Configuration Guide, Cisco IOS Release 15M&T"), accessed (2018).
4. study-ccna.com Homepage "ARP (Address Resolution Protocol) explained", accessed (2018).
5. tcpipguide.com Homepage "ARP Caching", accessed (2018).
6. GeeksforGeeks.org Homepage " Computer Network | ARP, Reverse ARP(RARP), Inverse ARP(InARP), Proxy ARP and Gratuitous ARP", accessed (2018).
7. Cisco.com Homepage "Proxy ARP", accessed (2018).
8. Link4securenetwork.blogspot.com Homepage "SLARP (Serial Line Address Resolution Protocol)", accessed (2018).
9. Omnisecu.com Homepage "ARP Spoofing Attack", accessed(2018).
10. Techopedia.com "Spoofing", accessed(2018).
11. Us.Norton.com Homepage "What is a man-in-the-middle attack?", accessed (2018).
12. Us.Norton.com Homepage "DOS Attacks explained", accessed (2018).

13. SearchSecurity.techtarget.com “Distributed denial of services (DDoS) attack”, accessed(2018).
14. Internetsaver.net Homepage “What is session Hijacking and how to prevent it?”, accessed(2018).
15. Kaspersky.com Homepage “Defend yourself from Man in the middle attack”, accessed(2018).
16. Biztechmagazine.com Homepage “The three elements of defenses against Denial-of-Service attacks”, accessed(2018).
17. Securitycommunity.tcs.com Homepage “Session Hijacking: Introduction and measures to safeguard”, accessed(2018).