Enhancing Network Security at the Data Link Layer

Sadiqah Mushtaq Student ID: sm07512

***Abstract*—This paper discusses the vulnerabilities in the Data Link layer of the OSI model and proposes security measures to mitigate these vulnerabilities. The vulnerabilities include CAM Table Overflow Attack, Spanning Tree Protocol (STP) Attacks, CDP Attacks, VLAN Attacks, MAC Spoofing Attack, DHCP Starvation Attack, Wireless 802.11 (Wi-Fi) Attacks, Man-in-the-Middle (MITM) Attacks, Identity Misbinding, Replay Attacks, Puzzle Mechanism, and Forward Secrecy.**

I. Introduction

Network security is an essential component when designing a network model. In the case of the OSI model, network designers often tend to ignore the data link layer. Traditional security measures and research focus on protecting against trojans, malicious emails, infected documents, and application-layer threats. These frequently revolve around the network or transport layers, while the data link layer remains unnoticed, with the majority of security efforts focusing on individual devices rather than the broader network infrastructure [1]. However, it is essential to note this fact alone renders the data layer the most vulnerable among others. While it may seem that it is difficult to seize this layer, and well, it may be true to some extent, it is not entirely impossible. It is high time now that we start focusing on this layer to enhance the security of the OSI model.

II. Enhancing Network Security at the Data Link Layer

In this section, we will discuss various vulnerabilities and security measures related to the Data Link layer in the OSI model.

A. CAM Table Overflow Attack

1) Vulnerability

This attack refers to a situation where the attacker bombards the switch with several different MAC addresses, causing the Content Addressable Memory (CAM) table to become filled. Consequently, the switch operates like a hub, i.e., it broadcasts frames to all ports [1]. Figure 1 shows a CAM table overflow attack.

2) Security Measure

A possible way to bypass this vulnerability is implementing port security [1]. Thankfully Cisco networks do offer this feature, which essentially allows administrators to define the maximum number of MAC addresses permitted on each switch port. Switch can then be configured to shut down or perform other predefined actions to protect against CAM table overflow attacks, in case the number of MAC addresses exceed the permitted limit.

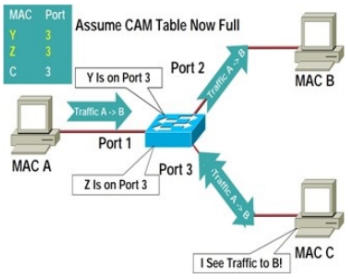

Figure 1. CAM attack [1]

B. Spanning Tree Protocol (STP) Attacks

1) Vulnerability

STP is a layer 2 network protocol that identifies redundant connections and disables any such link that leads to looping in switches and bridges, given that such loops cause a disastrous broadcast storm [1]. While STP is essential, attackers find a weak link in it and can easily manipulate it by sending incorrect Bridge Protocol Data Units (BPDUs), trying to be the root bridge. This can cause network instability as well as a Denial of

Service attack. Figure 2 shows how attacker is able to illegally listen the traffic by manipulating STP

2) Security Measure

One way to mitigate this issue, network administrators should configure proper STP settings on their switches and routers [1]. It is important to ensure that only trusted devices are participating in the STP process. Moreover, they should implement BPDU Guard and Root Guard to shield against unauthorized changes to the network topology.

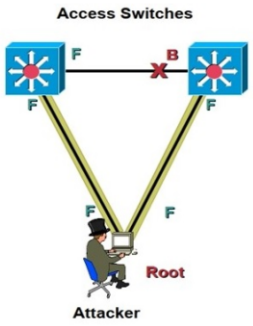

Figure 2. STP attack [1]

C. Cisco Discovery Protocol (CDP) Attacks

1) Vulnerability

False CDP announcements are another common tactic used by attackers to illegally gather information about the network, thus leading to network misconfiguration and security breaches [1].

2) Security Measure

Network administrators often disable CDP on ports that do not require it and filter CDP packets at the network perimeter [1]. One way to do this is implementing Access Control Lists (ACLs), which restrict CDP traffic. This can further improve security.

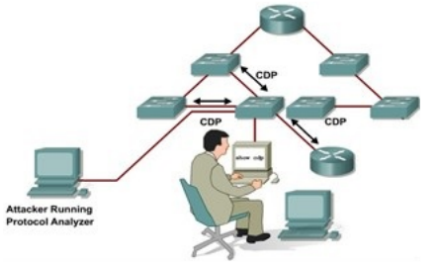

Figure 3. CDP attack [1]

D. VLAN Attacks

1) Vulnerability

Attackers often send incorrect VLAN information to switches, potentially leading to changes or disruption in network configuration [1]. Additionally, When a switch port is configured in trunking mode or implements the Dynamic Trunking Protocol, VLAN spoofing can occur. By utilising 802.1q trunk tagging, an attacker can impersonate a switch, create a trunk connection, and access all VLANs [2]. This type of attack is frequently used to spread malware.

2) Security Measure

Better practices for VLAN configuration, as well as proper VLAN memberships to switch ports, can be used to mitigate this issue. They should also use VLAN management tools and limit unauthorized access to switch configurations. We can also disable auto negotiation and avoid using default VLAN settings on ports to mitigate this issue [2].

E. MAC Spoofing Attack / ARP Poisoning

1) Vulnerability

Attackers can use ARP poisoning to redirect network traffic through a rogue gateway by delivering bogus Gratuitous ARP (GARP) packets to manipulate ARP caches [1]. To elaborate over it further, in a local network, when one host needs to communicate with another, it looks up the target's MAC address in its ARP cache. If it's not there, the requesting host sends an ARP Request to the network, asking for the target's MAC address. The target responds with an ARP Reply containing its IP and MAC addresses, which the requester stores for future use [2].

However, ARP lacks authentication. This ultimately makes it vulnerable to attacks. Malicious hosts can send fake ARP requests or replies, poisoning ARP caches and potentially redirecting network traffic to unauthorized hosts.

2) Security Measure

Network monitoring and intrusion detection systems can assist in detecting and preventing ARP spoofing attacks. Network segmentation and VLANs can also help to limit the scope of such assaults [1]. Apart from this, Network administrators can implement MAC address filtering, where only authorized MAC addresses are allowed to communicate on the network [3]. These filters, however, need to be regularly updated to include new devices.

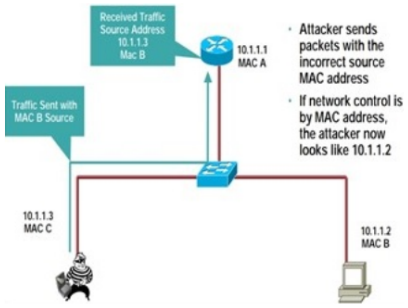

Figure 4. MAC Spoofing Attack [1]

F. DHCP Starvation Attack

1) Vulnerability

DHCP is used to assign IP addresses in LANs. A client broadcasts a DHCPDISCOVER message, and the server replies with DHCPOFFER. Once the client accepts, a DHCPACK is sent, and the client verifies IP availability using ARP. Improper DHCP configurations can lead to attacks like DHCP starvation, rogue server insertion, and traffic interception [2]. Subsequently, attackers can easily deplete the DHCP server's capacity by flooding the network with multiple IP address assignment requests [1]. This, in turn, prevents legitimate clients from acquiring IP addresses.

2) Security Measure

One way to prevent rogue DHCP servers from appearing on the network, techniques such as DHCP snooping, rate limitation, and use of IP source guard can limit the quantity of DHCP queries and prevent DHCP starvation attacks.

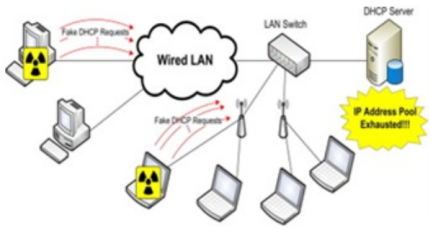

Figure 5. DHCP starvation attacks [1]

G. Wireless 802.11 (Wi-Fi) Attacks

1) Vulnerability

Wi-Fi networks are vulnerable to a variety of assaults, such as rogue access points, deauthentication attacks, and eavesdropping [1].

2) Security Measures

Protecting Wi-Fi networks entails utilizing strong encryption (e.g., WPA2, WPA3), strong authentication techniques (e.g., EAP-TLS), updating Wi-Fi passwords on a regular basis, and deploying intrusion detection and prevention systems [1].

H. Man-in-the-Middle (MITM) Attacks

1) Vulnerability

Attackers can position themselves between two communicating devices to intercept, alter, or inject data [3].

2) Security Measure

To mitigate this issue secure key exchange mechanisms during the key establishment protocol (this protocol refers to a set of procedures and rules used to negotiate and establish cryptographic keys between two entities, typically between a host (initiator) and an authentication server (responder) in the context of securing communication at the data link layer of a network) [3]. This can be done by Implementing cryptographic techniques to ensure the authenticity and integrity of data.

I. Identity Misbinding

1) Vulnerability

Attackers may attempt to forge the identities of network users or network components and conduct identity misbinding attacks [3].

2) Security Measure

One way to mitigate this issue is to protect identities by revealing them only after there is some form of mutual authentication [3]. This can be done using cryptographic techniques for identity protection.

J. Replay Attacks

1) Vulnerability

Attackers can capture and replay data frames to gain unauthorized access, making the data link layer highly susceptible [3].

2) Security Measure

Replay protection strategies may be used to mitigate this security concern. Examples of such strategies can be the use of sequence numbers and timestamp-based validation [3].

K. Puzzle Mechanism

1) Vulnerability

Distributed Denial of Service (DDoS) attacks and resource exhaustion can occur during the key establishment protocol [3].

2) Security Measure

Utilize a puzzle mechanism to delay state creations at servers and mitigate DDoS threats [3]. Monitor for multiple puzzle failures to detect attacks.

L. Forward Secrecy

1) Vulnerability

Past session keys can easily get exposed if the network administrator slightly compromises in the long term [3].

2) Security Measure

Forward secrecy can be employed by deriving session keys that are independent of long-term secrets.

III. Conclusion

In conclusion, enhancing network security at the data link layer in the OSI model is crucial to protect against a variety of vulnerabilities and attacks. By implementing the security measures discussed in this paper, network administrators can significantly improve the overall security of their networks at the data link layer.

References

[1] S. Mahmood, S. M. Mohsin, and S. M. A. Akber, "Network security issues of data link layer: An overview," in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2020, pp. 1–6.

[2] M. Z. Nasir Siddique, Mustafa Ali, "Data link layer security problems and solutions," 2015.

[3] H. Altunbasak and H. Owen, "An architectural framework for data link layer security with security inter-layering," in *Proceedings 2007 IEEE SoutheastCon*, 2007, pp. 607–614.