Ethernet LAN Security

Ethernet is one of the most widespread LAN infrastructures in the world. Its simplistic nature and easy integration policy are the primary reasons for its popularity. The simplistic nature gives rise to the question of security. Does it compromise the security of the system for its simplistic nature? The quick answer is YES - Naive Ethernet is vulnerable to security problems.

1. **Known Attacks**

The vulnerability of Ethernet arises primarily due to its Self-Configuring nature and the Broadcast nature of some Ethernet protocols like ARP, STP etc. Attackers can use various ways to infiltrate the systems and take control. Some known methods of attack and their counteractions are listed below.

# Attacks to Gain Control of a Network Segment or a System in a Network

### Unauthorized Joins to the Network

Problem: Someone connects to a free Port in a switch by directly connecting to a wall socket of the port or the switch itself?

Solutions:

Such Problems can be resolved by:

* + - * Physically restraining access to a switch by locking the room.
      * Limit the port’s access to a specific/group of MAC addresses and limit access to only a certain number of MAC addresses per unit time.
      * Use secure protocols like MACsec/Extensible Authentication Protocol to authenticate the user. Such protocols use the user's public key to verify if the user's private key is valid.

### Unauthorized Expansion of the Network

Problem: Someone expands a Port by connecting another Switch to an existing Port or by tapping into an existing wire?

Solution:

This can be prevented by configuring the switches to lock on to a single MAC address on the Port using some strategy for a considerable time.

### The attacker pretends to be a switch and joins all VLAN networks.

Solution: Authentication can also be used between switches to form a trusted internal network. This can be used to prevent attacks where a host acts as a switch.

### Access to other VLANs in the network

Problem: The attacker adds a custom VLAN tag or double tags VLAN packets to hop VLAN networks.

Solution: Double Tagging can only be exploited on switch ports configured to use native VLANs. Trunk ports configured with a native VLAN don't apply a VLAN tag when sending these frames. This allows an attacker's fake VLAN tag to be read by the next switch.

### The attacker uses TCP Connection to establish a remote connection with one of the computers on the network.

Solution: This problem can only be solved with higher-layer protocols as the Ethernet layer cannot identify the source of the malicious packets as the host in the network or a remote host. Higher layer protocols must ensure with features like Session timeout, Duplex communication fairness etc., that they are not being used for malicious purposes.

### Scanning Attacks

Problem: The attacker tries to identify the topology and vulnerabilities by scanning packets passing through a specific host.

Solution: There must be a proper authentication mechanism for someone joining the network.

# Attacks on Traffic Confidentiality (Sniffing)

Problems:

* The attacker can passively eavesdrop on the frames by tapping into the wires using a special device.
* Moreover, an attacker can force broadcast by MAC-flooding, i.e., sending random MAC addresses to the switch to make its MAC table obsolete, causing the switch to broadcast its messages, which can then be eavesdropped on.
* Switches often have Port-mirroring features, which the attacker can use for eavesdropping.

Solution: Encryption of the data is the only solution for all problems related to Sniffing.

# Attacks that try to modify traffic content

### ARP and DHCP Poisoning

Problems:

* + - * ARP requests sent by a host are broadcasted to all of them. Here it is possible that the attacker pretends to be the true recipient of the ARP message and responds before the actual recipient can respond.

*Sakshi Shashikant Yeole (20CS01047)*