Network Security Link Layer

Target Course

Networks

Learning Goals

A student shall be able to:

1. Describe foundational security concepts in securing networks and systems.
2. Describe security design principles and identify security issues associated with common threats and attacks.

IAS Outcomes

IAS Knowledge Topic	Outcome
Network Security	3. Describe virtues and limitations of security technologies at each layer of the network stack. [Familiarity]

Dependencies

- Cover after the ***Network Security Concepts*** module.

Summary

Describe how the transport layer may be used to support the security goals of CIA and the fundamental concepts of assurance, authentication, anonymity, and non-repudiation.

Estimated Time

This module takes approximately 15 lecture minutes to cover.

Materials

How does this layer affect the security goal of confidentiality?

- Using Ethernet with hubs means that each frame is sent to all devices within a network segment, making eavesdropping easier.
- MAC address spoofing allows attacker to see frames destined for a specific device.
- ARP spoofing allows attacker to see frames destined for a specific device.

How does this layer affect the security goal of integrity?

- Ethernet frame header includes CRC-32 checksum designed to catch transmission errors.
- Not cryptographically secure, so this checksum does not provide integrity from the perspective of computer security.

How does this layer affect the security goal of availability?

- No flow control at this layer; frames will be sent to a device regardless of whether the device can handle this load.

How does this layer affect the fundamental security concept of assurance?

- Link layer protocols allow frames to be sent between any two devices.
- Link layer protocols do not include any permissions or security policies (e.g., similar to firewall capabilities).
- MAC address spoofing and ARP spoofing allows an attacker to pretend they are someone else.

How does this layer affect the fundamental security concept of authenticity?

- Link layer protocols do not include any type of digital signature. These protocols have no notion of user identity.

- MAC address spoofing and ARP spoofing allows an attacker to pretend they are someone else.

How does this layer affect the fundamental security concept of anonymity?

- Link layer protocols do not include any type of digital signature. These protocols have no notion of user identity.
- Thus, link layer supports anonymity - which is a two-edged sword since an attacker may pretend they are someone else without attribution.

How does this layer affect the fundamental security concept of non-repudiation?

- Since the protocols in the link layer have no notion of user identity, non-repudiation is not supported.

What type of risks are known about the Link layer?

The information below is from Chapter 14 in [1] and Chapter 1 in [2].

The Link layer general risks include the following:

Assessment Methods

None used.

References

[1] M.T. Goodrich & R. Tamassia, (2011). *Introduction to Computer Security*. Addison Wesley.

[2] R. Anderson, (2008). *Security Engineering, Second Edition*. Wiley.