Network Security Network 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] 4. Identify the appropriate defense mechanism(s) and its limitations given a network threat. [Familiarity]

Dependencies

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

Summary

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

Estimated Time

[Provide the estimated amount of lecture time to cover this module, using the notion of time as defined in CS2013.]

Materials

How does this layer affect the security goal of confidentiality?

- IP does not automatically encrypt its payload.

How does this layer affect the security goal of integrity?

- Header checksum is used only to verify the IP header has been transmitted correctly.
- Each router must re-compute the header checksum since TTL (time to live) has been changed.

How does this layer affect the security goal of availability?

- No flow control at this layer; packets 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?

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

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

- Network layer protocols do not include any type of digital signature. These protocols have no notion of user identity. While an IP address is associated with a device, any type of user could be using this device.
- IP spoofing allows an attacker to pretend they are someone else.

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

- Network layer protocols do not include any type of digital signature. These protocols have no notion of user identity.
- Thus, network 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 network layer have no notion of user identity, non-repudiation is not supported.

What type of risks are known about the Network layer?

The information below is from Chapter 11 in [2] and Chapter 1 in [3].

The Network layer protocols include the following:

- IPv4, IPX and VINES provide no security precautions.
- IPv6 is a complete redesign of IP, it supports authentication and data encapsulation via encryption.
- IPsec provides extensions to IP to address security.

The Network layer security should address the following:

- Network incompatibility. Protocols operate in a particular layer, but most protocols still rely on features of a protocol at a higher or lower layer. This makes it more difficult to change a protocol at a specific layer.
- Server filtering. A server should filter network traffic coming in to it. An attacker must know a valid address in order to gain access.
- Firewalls and egress filtering. Routers can include firewalls to restrict incoming and outgoing packets to specific IP addresses and subnets.

The Network layer routing risks include the following:

- Direct router attacks. A denial of service (DoS) attack or a system compromise prevents router from performing basic routing function.
- Router table poisoning. Forged or compromised network traffic can overwrite, insert, or remove valid routing table entries.
- Router table flooding. Router table size is limited (i.e., router’s hard drive/RAM not very large). An attacker generates fake data to populate router table. When the router tables fills, router can either ignore new routes, discard routes not used, or discard less desirable routes.
- Routing metric attacks. These are applicable when router uses dynamic metrics. An attacker forges quality-of-service packets that modify dynamic metrics. This may cause slower throughput, longer paths, more expensive networking costs, disabling a desirable path.
- Router looping attacks. These are hard for attacker to accomplish. A router interface is setup to send packets back to the same router.

The Network layer addressing risks include the following:

- Address impersonation. In this risk, two nodes have same address i.e., an unplanned impersonation.
- Address hijacking. In this risk, two nodes on same subnet have same address. The node that responds quicker can maintain a network connection.
- Dynamic allocation consumption. This affects addressing schemes that support dynamic addressing e.g,. VINES, IPv4, IPv6 with DHCP. This attack requests all available addresses to be marked as allocated.

- False release attacks. An attacker impersonates an allocated address and specifies release of the address. The victim node begins to operate with an unallocated address and is now vulnerable to impersonation attacks.
- False dynamic allocation. An attacker configures their own allocation server. Any broadcast request for allocation may be responded by attacker's allocation server.

Assessment Methods

Below are questions that have been used on quizzes and exams.

What is the purpose of a packet-filtering firewall?

a. To drop packets based on their source or destination IP address.

b. To configure port numbers to allow or prevent network access.

c. To drop packets based on their ICMP message type.

d. All of the above.

e. None of the above.

Answer: d. All of the above.

References

[1] J.F. Kurose & K.W. Ross, (2005). *Computer Networking: A top-down approach featuring the Internet*. Addison Wesley.

[2] Krawetz, N. (2007). Introduction to Network Security. Cengage Charles River Media. Accessed via Books 24x7 Digital Library.

[3] Xiao, Y. & Pan, Y, eds, (2007). Security in Distributed and Networking Systems: Computer and Network Security, Vol. 1. World Scientific Publishing Company. Accessed via Books 24x7 Digital Library.