IPSEC
Lecture 19

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

September 13, 2021

Source of some slides: **University of Tennessee** /
Cryptography and Network Security by Behrouz Forouzan

INTERNET SECURITY PROBLEM

- Today's Internet is primarily comprised of
  - Public
  - Un-trusted
  - Unreliable IP networks

- Because of this inherent lack of security, the Internet is subject to various types of threats

INTERNET THREATS

- Unauthorised modification
  - The contents of a packet can be accidentally or deliberately modified
- Identity spoofing
  - The origin of an IP packet can be forged
- Replay attacks
  - Unauthorised data can be retransmitted
- Loss of privacy
  - The contents of a packet can be examined in transit

IPSEC: NETWORK SECURITY LAYER

- IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF)
- IPsec aims at securing communications over IP
- Creates secure, authenticated, reliable communications over IP networks
- It is designed to address fundamental shortcomings, such as being subject to spoofing and eavesdropping

WHY TLS IS NOT ENOUGH?

- Implemented in end-hosts
- Advantages
  - Existing applications get security seamlessly
- Disadvantages
  - Protocol specific

IPSEC ADVANTAGES

- All traffic can be secured regardless of applications
- Provides seamless security to application and transport layers
  - Transparent to applications, no change required in any upper layer
- Transparent to end users, no need to train users on security mechanisms

IPSEC APPLICATIONS

- Site-to-site
  - An organisation with multiple sub-offices
- Host-to-site
  - Travelling employees
  - Contractors

IPSEC SECURITY SERVICES

- Data origin authentication
  - Assurance that traffic is sent by legitimate parties
- Confidentiality (encryption)
  - Assurance that user's traffic is not examined by unauthorised parties
  - Limited traffic flow confidentiality
- Connectionless integrity
  - Assurance that every received IP packet has not been modified
  - Partial sequence integrity - prevents packet replay

IPSEC SPECS

- RFC 2401
  - Security architecture
- RFC 2402
  - Authentication
- RFC 2406
  - Encryption
- RFC 2408
  - Key management

IPSEC MAJOR COMPONENTS

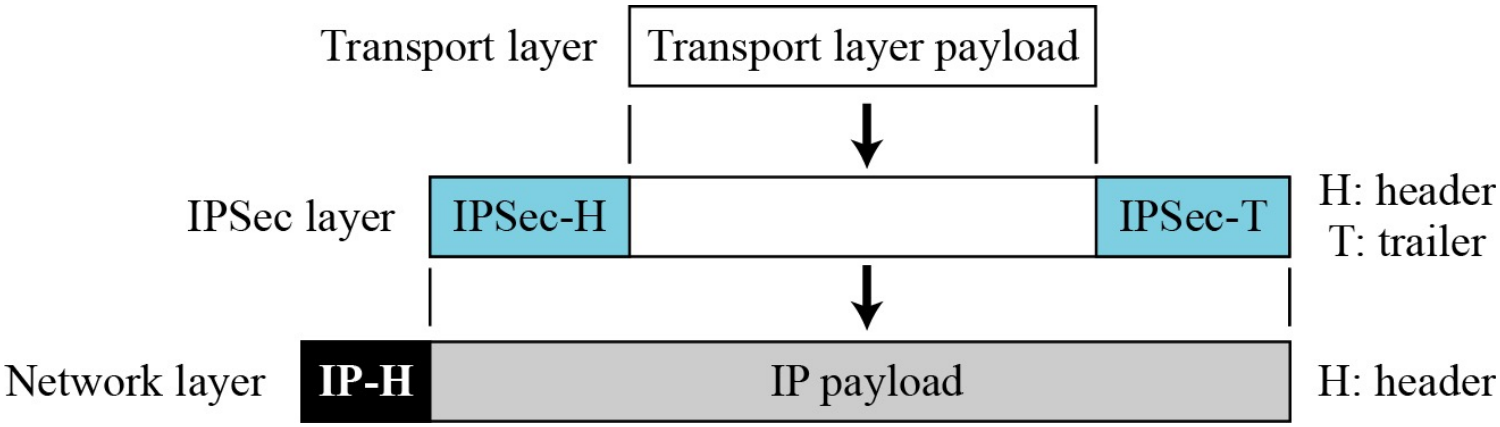
- IPSec modes
- IPSec base protocols
- IPSec Internet Key Exchange (IKE)
- IPSec Security Associations (SA)

IPSEC MODES

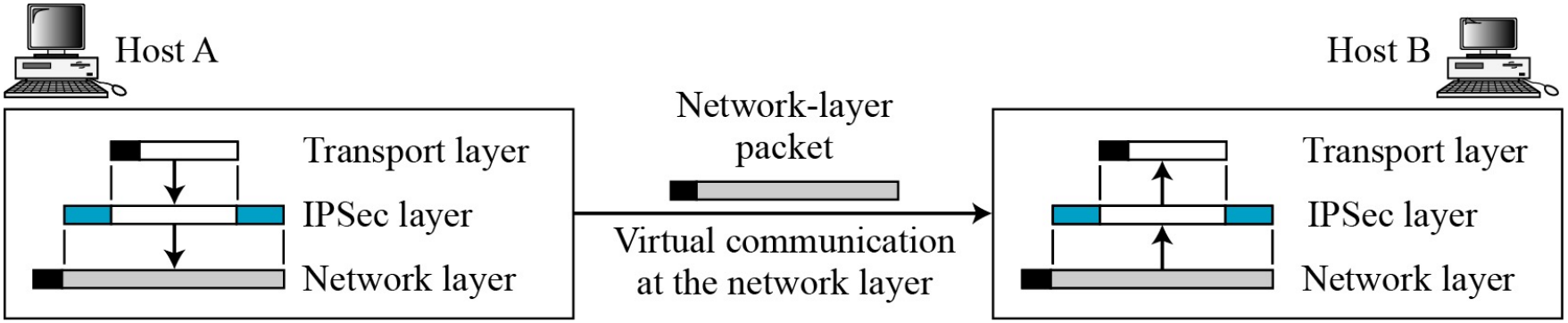
- Transport mode
  - Used to deliver services from host to host or from host to gateway
  - Usually within the same network, but can also be end-to-end across networks
- Tunnel mode
  - Used to deliver services from gateway to gateway or from host to gateway
  - Usually gateways owned by the same organisation
    - With an insecure network in the middle

TRANSPORT MODE

- Protects what is delivered from the transport layer to the network layer
- This mode does not protect the IP header
  - It only protects the information coming from the transport layer

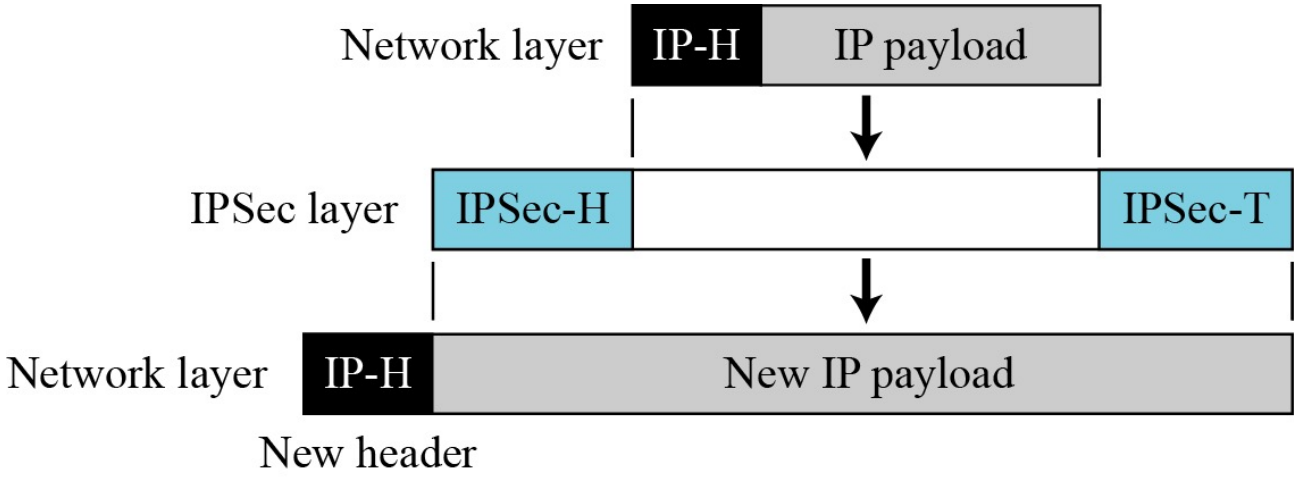


TRANSPORT MODE IN ACTION

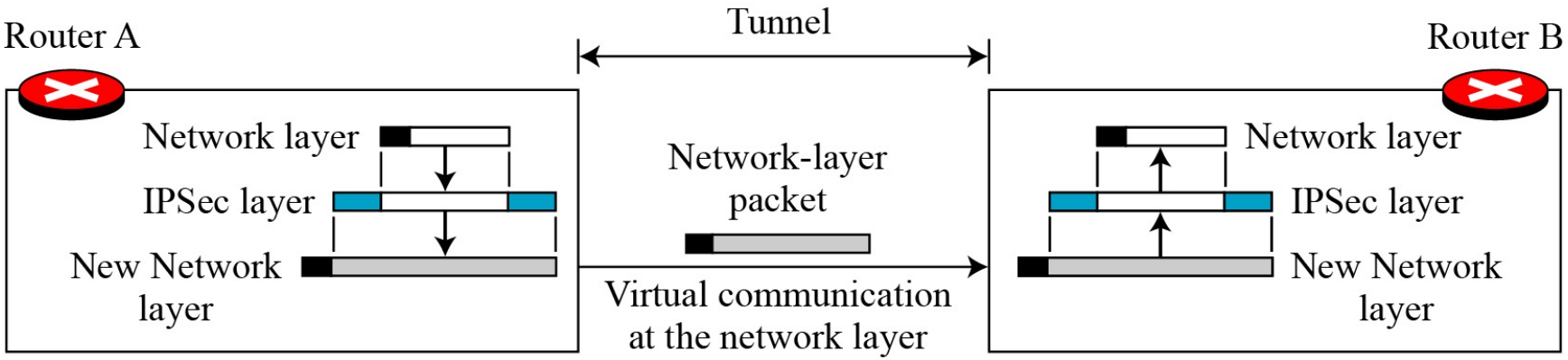


TUNNEL MODE

- Protects the entire IP packet
  - It takes an IP packet applies security methods to the entire packet, and then adds a new IP header
- This mode protects the original IP header



TUNNEL MODE IN ACTION



TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!