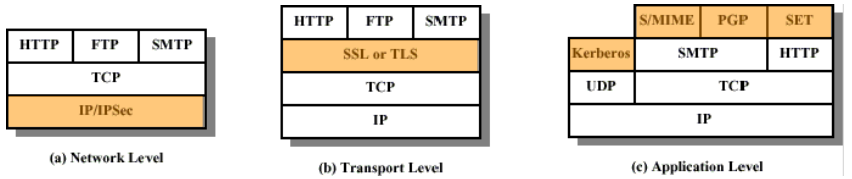
Cybersecurity: IPSec

Ozalp Babaoglu

ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA

Introduction

- Security in the Internet:
  - at which (OSI, TCP/IP) level?



Introduction

- Security at the application level
  - *Pros*: designed for application requirements
  - *Cons*: requires multiple security mechanisms
- Security at the transport level
  - *Pros*: provides common interface to security services
  - *Cons*: requires (minor) modification to applications
- Security at the network level
  - *Pros*: works also with security-ignorant applications
  - *Cons*: may require modifications at the OS level

IPSec – Introduction

- IPSec is a family of protocols proposed by IETF to secure communications on the Internet
- Weaknesses and attacks to current IP:
  - (Lack of) Integrity — IP Spoofing
  - (Lack of) Authentication — IP Spoofing
  - (Lack of) Confidentiality — Packet sniffing

IPSec – Introduction

- IPSec protocols designed for both
  - IPv4 (optional support)
  - IPv6 (mandatory support)
- Protocols based on *extension headers*
- Quite complex specification
  - Multiple documents among which: RFCs 2401, 2402, 2406, and 2408
- Basic protocols: AH, ESP, IKE

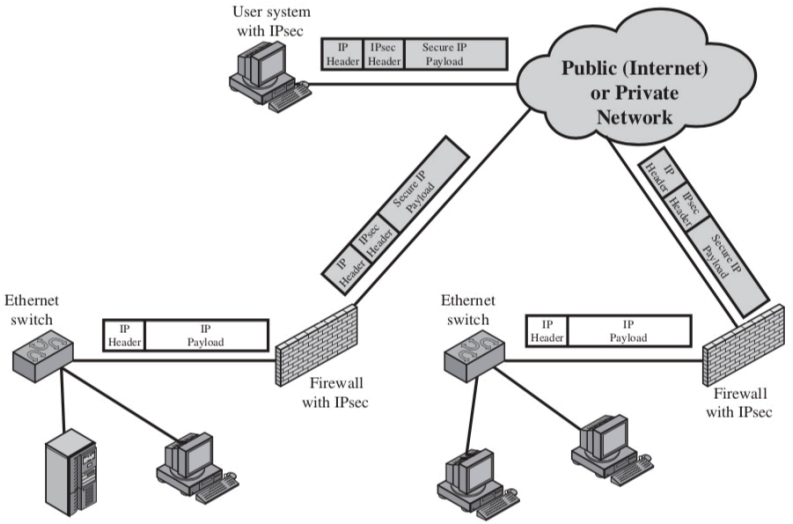
IPSec — Applications

- Virtual Private Networks (VPN) over the Internet
  - A company can build a secure network, built over the public Internet, with private access
- Secure remote access over the Internet
  - An end user may gain access to a company network
- Establishment of extranet and intranet connectivity with partners:
  - Secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism
- Enhancement of higher-level applications security
  - E-commerce

IPSec — Benefits

- When implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter
  - No impact on internal traffic
- Transparent to applications (below TCP/UDP)
- No need to change software on a user or server system when IPSec is implemented in the firewall or router
- Transparent to end-users
  - No need to train users on security mechanisms

IPSec — IP Security Scenario



IPSec — Protocols

- *Authentication Header* (AH) for message authentication and integrity
- *Encapsulating Security Payload* (ESP) for confidentiality (combined authentication/encryption)
- *Internet Security and Key Management Protocol* (IKE) for key exchange
- AH/ESP are applied "per packet"
- Both AH and ESP support two different modes of use
  - Transport mode
  - Tunnel mode

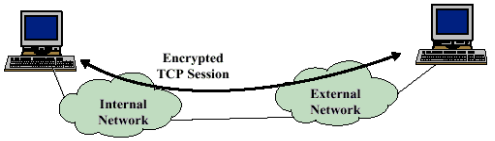
IPSec — Transport Mode

- Transport Mode
  - provides protection to the upper-layer protocols (IP packet payloads)
  - normally used for end-to-end communication
- AH in Transport Mode
  - authenticates the IP payload and selected portions of the IP header
- ESP in Transport Mode
  - encrypts and optionally authenticates the IP payload
  - IP header not protected

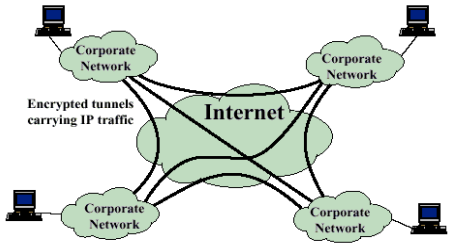
IPSec — Tunnel Mode

- Tunnel mode
  - provides protection to the entire IP packet
  - normally used in "gateway-to-gateway" communication
- How does it work?
  - AH/ESP headers are added to the IP packet
  - the entire packet is treated as the payload of a new outer IP packet with a new outer IP header
- Packets travel through a "tunnel"
  - No routers along the way are able to examine the original packet

IPSec — ESP



(a) Transport-level security



(b) A virtual private network via Tunnel Mode

IPSec — Transport and Tunnel Modes

- Transport
  - Low overhead
  - Some information can be sniffed (e.g., user connecting to a host)
- Tunnel
  - More secure
  - Intermediate entities
  - Higher overhead

IPSec — Tunneling Example

- Host A on network N_{A} wants to communicate with host B on network N_{B}
- A generates a packet with A as the sender and B as the destination
- Packet is routed to the *security gateway* (firewall with IPSec) of network N_{A}
- The security gateway encapsulates the packet in an outer IP header with N_{A} as the sender and N_{B} as the destination
- The new packet is routed by the public network (Internet) to the security gateway of network N_{B}
- The security gateway extracts, decrypts and authenticates the original packet
- The original packet is routed and delivered to B on N_{B}

IPSec — ESP