Network Level Security: IP Security (IPsec)

Abstract

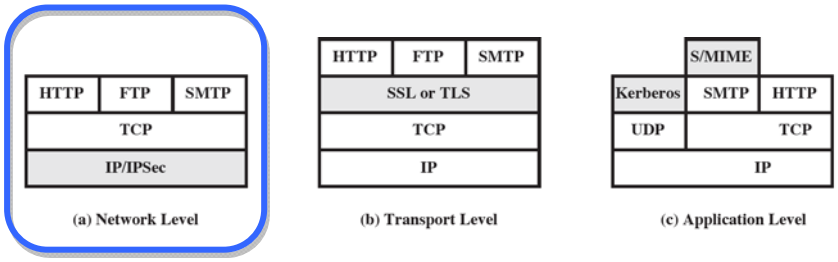
This section presents fundamentals of IP Security (IPsec). After an overview on general aspects of IPsec and its applications, the transport and tunnel modes are outlined. Then, main items of IP Security policy, Internet Key Exchange and IPsec cryptographic suites are briefly reviewed.

Outline

- **Security protocols in the TCP/IP stack**
- Overview on IP Security
- Transport and Tunnel modes
- IP Security policy
- Internet Key Exchange and cryptographic suites

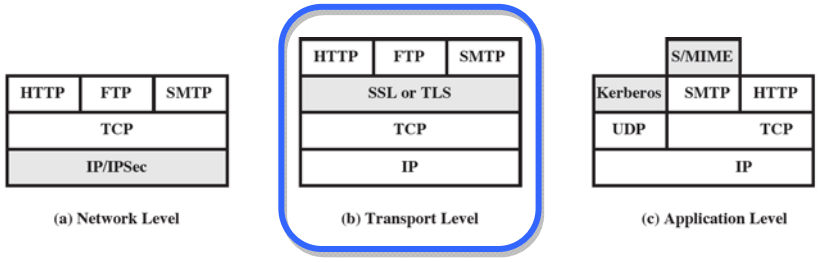
Security Protocols in the TCP/IP Stack

- IP Security (IPsec)
  - transparent to end users and applications
  - general-purpose solution
  - includes filtering so that only selected traffic incurs the overhead of IPsec



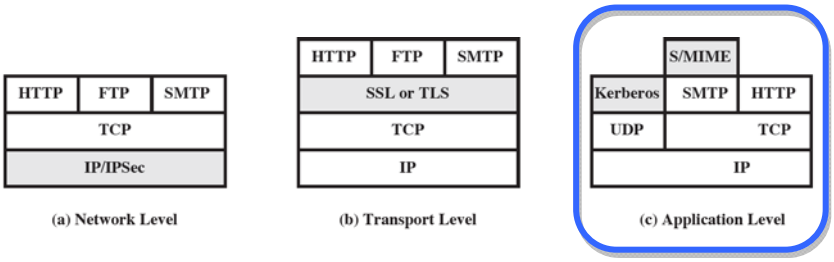
Security Protocols in the TCP/IP Stack

- Secure Sockets Layer (SSL) or Transport Level Security (TLS)
  - could be provided as part of the underlying transport protocol suite (transparent to applications)
  - embedded in specific applications (e.g., web browser)



Security Protocols in the TCP/IP Stack

- Security services embedded within the application
  - each application may implement features to meet its own specific security requirements



Outline

- Security protocols in the TCP/IP stack
- **Overview on IP Security**
- Transport and Tunnel modes
- IP Security policy
- Internet Key Exchange and cryptographic suites

General Aspects of IP Security

- IAB RFC 1636 "Security in the Internet Architecture", 1994
  - authentication and encryption included as necessary security features in the next generation IP (IPv6)
  - security features were designed to be usable also with current IPv4
- By implementing security at the IP level, secure networking is ensured for all applications including security-ignorant ones
- IP-level security encompasses three functional areas
  - authentication
    - ensures that a received packet was transmitted by the source in its header
    - ensures that the packet has not been altered in transit
  - confidentiality
    - enables communicating nodes to encrypt messages to prevent eavesdropping by third parties
  - key management
    - secure exchange of keys

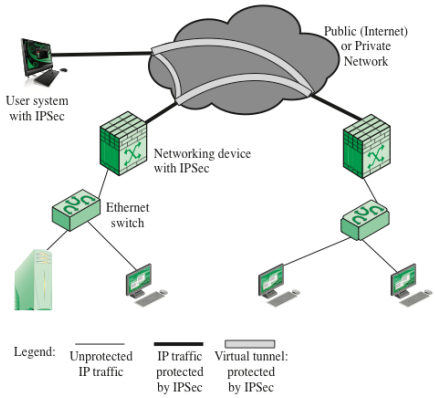
Applications of IPsec

- IPsec secures communication across a LAN, or private and public WANs, or the Internet
- It can secure communication host to host in transport mode or by setting up a Virtual Private Network (VPN) in tunnel mode
  - secure branch office connectivity over the Internet
  - secure remote access over the Internet
  - establishing extranet and intranet secure connectivity with partners
  - enhancing electronic commerce security (additional layer of security to whatever end-to-end security at the application layer)
- IPsec can encrypt and authenticate all traffic at the IP level

Principle of IPsec Tunneling

- Simplified packet format for the *tunnel mode IPsec option*

- Tunnel Mode is based on
  - a combined authentication/encryption function (Encapsulating Security Payload, ESP)
  - a key exchange function
- Tunnel Mode sets up a secure VPN across the public Internet



Benefits of IPSec

- When IPsec is implemented in a firewall or router (tunnel mode), it provides strong security on all traffic crossing the perimeter
  - users do not need to carry the overhead of end-to-end security
- IPsec is below the transport layer (TCP, UDP) and therefore
  - transparent to applications
    - no need to change software on a user or server system
    - upper-layer software and applications are not affected
  - can be transparent to end users
    - no need to train users on security mechanisms or to distribute them keys
  - can provide security for individual users if needed
    - to set up secure communication for sensitive applications, within an organization or for offsite workers
- IPsec can secure messages of routing protocols (e.g., OSPF)
  - run on top of IPsec to ensure that router advertisements, redirect messages, routing updates come from the authorized source

IPsec Specification Documents

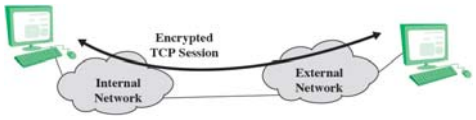
- RFC 6071, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*, February 2011
- IPsec specifications are scattered across dozens of documents
  - Architecture
    - RFC 4301, *Security Architecture for the Internet Protocol*
  - Authentication Header (AH)
    - header used in the past for message authentication (now provided by ESP)
    - RFC 4302, *IP Authentication Header*.
  - Encapsulating Security Payload (ESP)
    - encapsulating header and trailer for packet encryption or encrypt./auth.
    - RFC 4303, *IP Encapsulating Security Payload (ESP)*
  - Internet Key Exchange (IKE)
    - RFC 7296, *Internet Key Exchange (IKEv2) Protocol*, and related RFCs
  - Cryptographic algorithms
  - Other
    - e.g., security policy and management information base (MIB)

Outline

- Security protocols in the TCP/IP stack
- Overview on IP Security
- **Transport and Tunnel modes**
- IP Security policy
- Internet Key Exchange and cryptographic suites

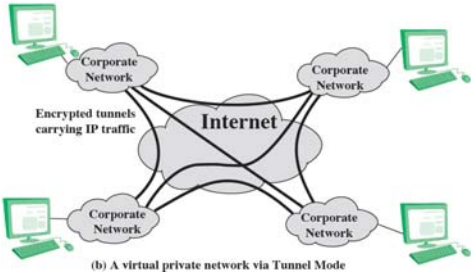
Transport Mode

- Provides protection to upper-layer protocols (i.e., IP packet payload)
  - e.g., TCP or UDP segment, ICMP packet
  - transport-mode ESP encrypts and optionally authenticates the IP payload but not the IP header
  - transport-mode AH authenticates the IP payload and selected portions of the IP header (usage of AH is today deprecated)
- Used for end-to-end communication between two hosts
  - encryption/authentication provided directly between two hosts



Tunnel Mode (1)

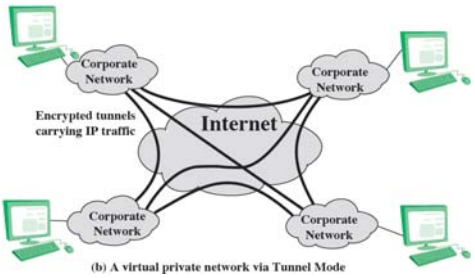
- Provides protection to the entire IP packet
  - after the AH/ESP fields are added, the entire IP packet plus security fields becomes the payload of new outer IP packet
  - the entire original inner packet travels through a tunnel in the IP network
  - no routers along the way are able to examine the inner IP header
  - the outer IP packet may have different source and destination addresses
  - tunnel-mode ESP encrypts and optionally authenticates the entire inner IP packet
  - tunnel-mode AH authenticates the entire inner IP packet and selected portions of the outer header (usage of AH is today deprecated)



(b) A virtual private network via Tunnel Mode

Tunnel Mode (2)

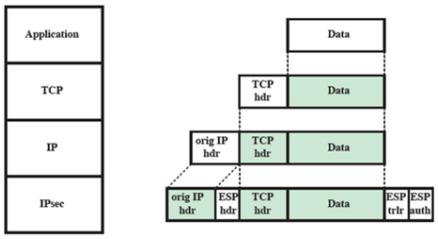
- Used when one or both ends of a Security Association (SA) are a security gateway, such as a firewall or router with IPsec
- Hosts on networks behind firewalls do not need to implement IPsec
  - the unprotected packets generated by no-IPsec external hosts are tunneled across a VPN set up via tunnel mode



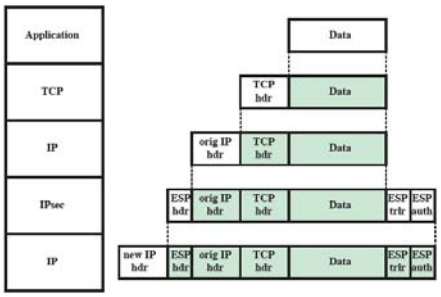
(b) A virtual private network via Tunnel Mode

Protocol Stacks for ESP

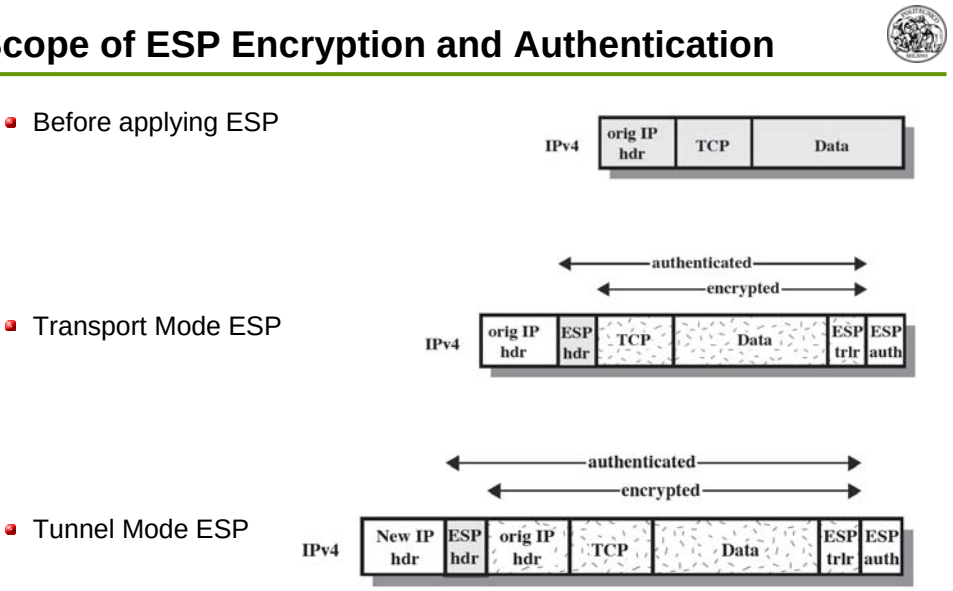
- Transport Mode ESP



- Tunnel Mode ESP



Scope of ESP Encryption and Authentication



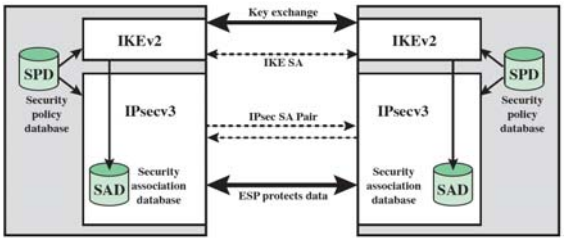
- Before applying ESP
- Transport Mode ESP
- Tunnel Mode ESP

Outline

- Security protocols in the TCP/IP stack
- Overview on IP Security
- Transport and Tunnel modes
- **IP Security policy**
- Internet Key Exchange and cryptographic suites

IP Security Policy

- A security policy is applied to each IP packet that transits from a source to a destination
  - what to do with the packet: secure or not?
- IPsec is executed packet by packet, to each packet
- The IPsec policy is determined by the interaction of two databases
  - the Security Association Database (SAD)
  - the Security Policy Database (SPD)



IP Security Database

- *Security Association* (SA)
  - one-way logical connection between a sender and a receiver that provides secure communication
  - in any IP packet, the SA is identified by the Destination Address and the Security Parameters Index (SPI) in the extension header (AH or ESP)
- The *Security Association Database* defines the security parameters (protocols, keys) of each SA
- The *Security Policy Database* lists the security policies, based on which the incoming and outcoming traffic is treated
  - contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic
  - there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry

Outline

- Security protocols in the TCP/IP stack
- Overview on IP Security
- Transport and Tunnel modes
- IP Security policy
- **Internet Key Exchange and cryptographic suites**

Internet Key Exchange

- IPsec uses
  - X.509 certificates for authentication
  - Diffie-Hellman exchange to determine a shared session secret
    - four keys for communication between two applications (transmit and receive pairs for both integrity and confidentiality) are derived
- IKEv1/IKEv2 is the protocol used to set up a SA and is built upon
  - *Oakley Key Determination Protocol*
    - key exchange protocol based on Diffie-Hellman but providing added security
    - generic in that it does not dictate specific formats
  - *Internet Security Association and Key Management Protocol (ISAKMP)*
    - protocol defined by RFC 2408 for establishing SAs and cryptographic keys
    - provides a framework for authentication and key exchange, is designed to be key-exchange independent, enables a variety of key-exchange algorithms, incl. IKE and Kerberized Internet Negotiation of Keys (KINK)

Cryptographic Suites for IPsec

(a) Virtual Private Networks (RFC 4308)

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

(b) NSA Suite B (RFC 4869)

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP