

IP Security

Yuan Xue



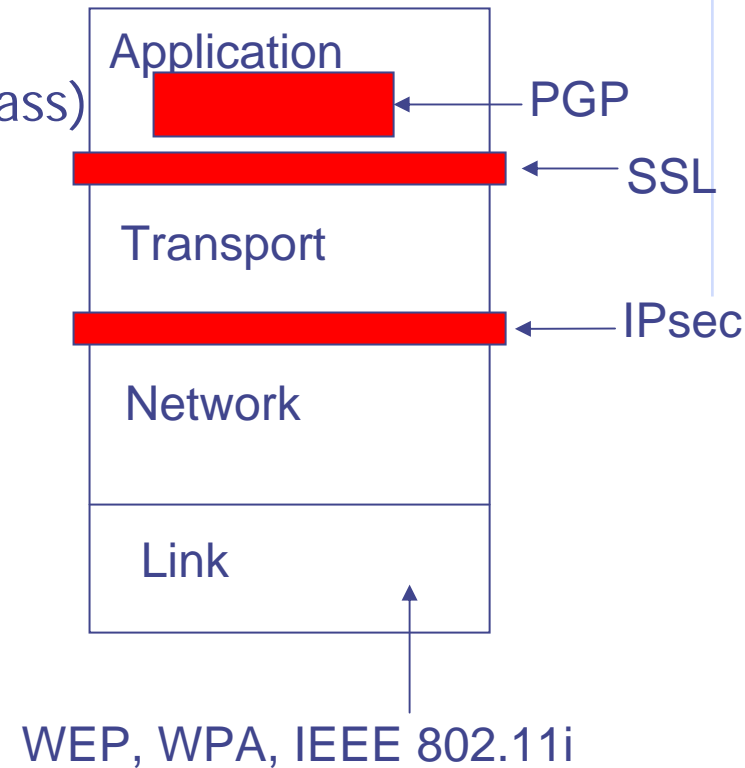
Where to Place Security

◆ Application/Transport layer based solutions

- Secure network-based applications
 - ◆ Web – SSL, transportation layer solution
 - ◆ Email – PGP, application layer solution

◆ Network/Link layer based solutions (this class)

- Secure network + support for application
 - ◆ IPsec
 - ◆ Internet Security
 - BGP security
 - ◆ Wireless Security
 - IEEE 802.11 security



IPSec

◆ Background

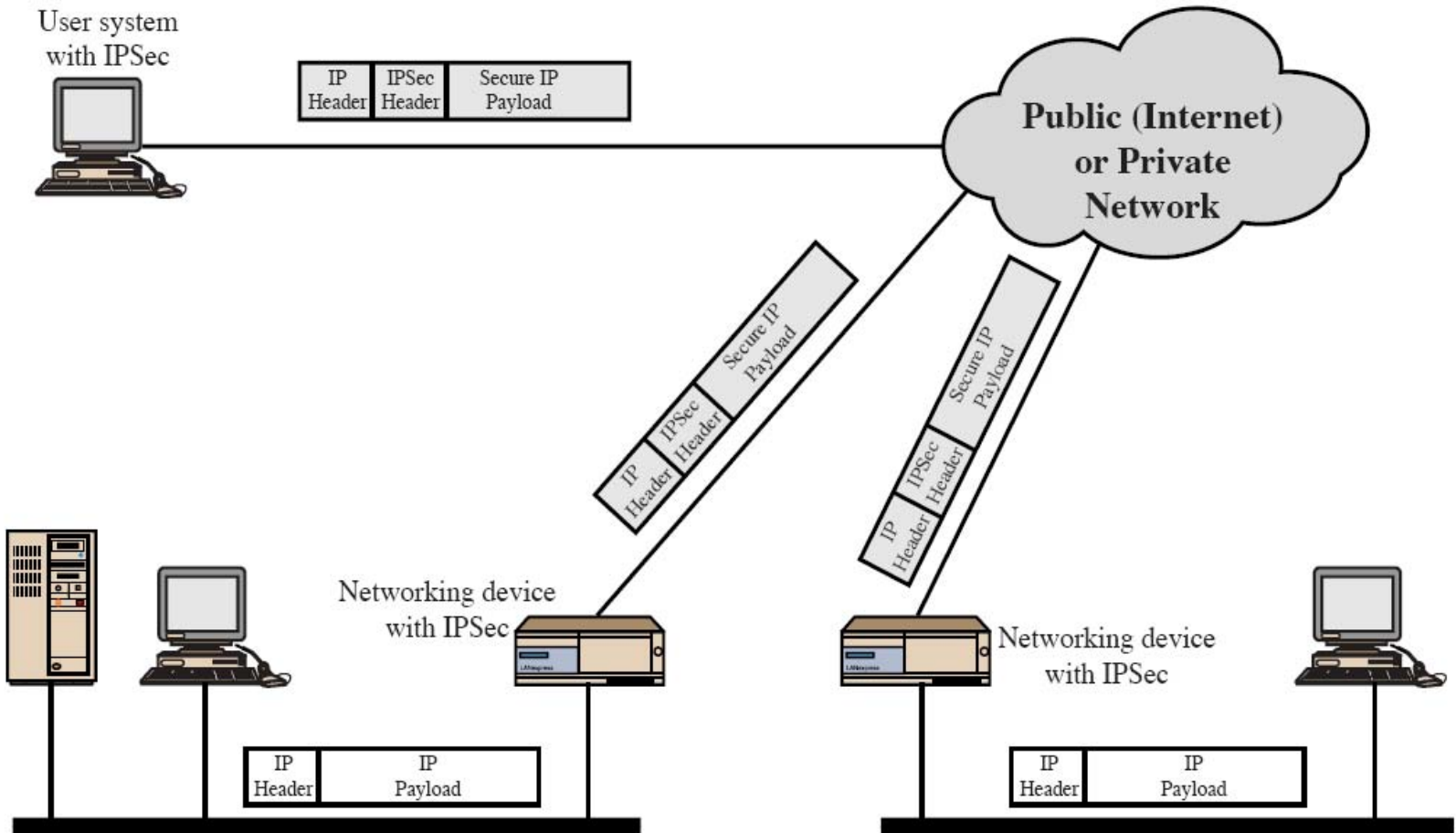
- A collection of protocols and mechanisms
 - ◆ RFC 2401, RFC 2402, RFC 2406, RFC 2408

◆ Goal

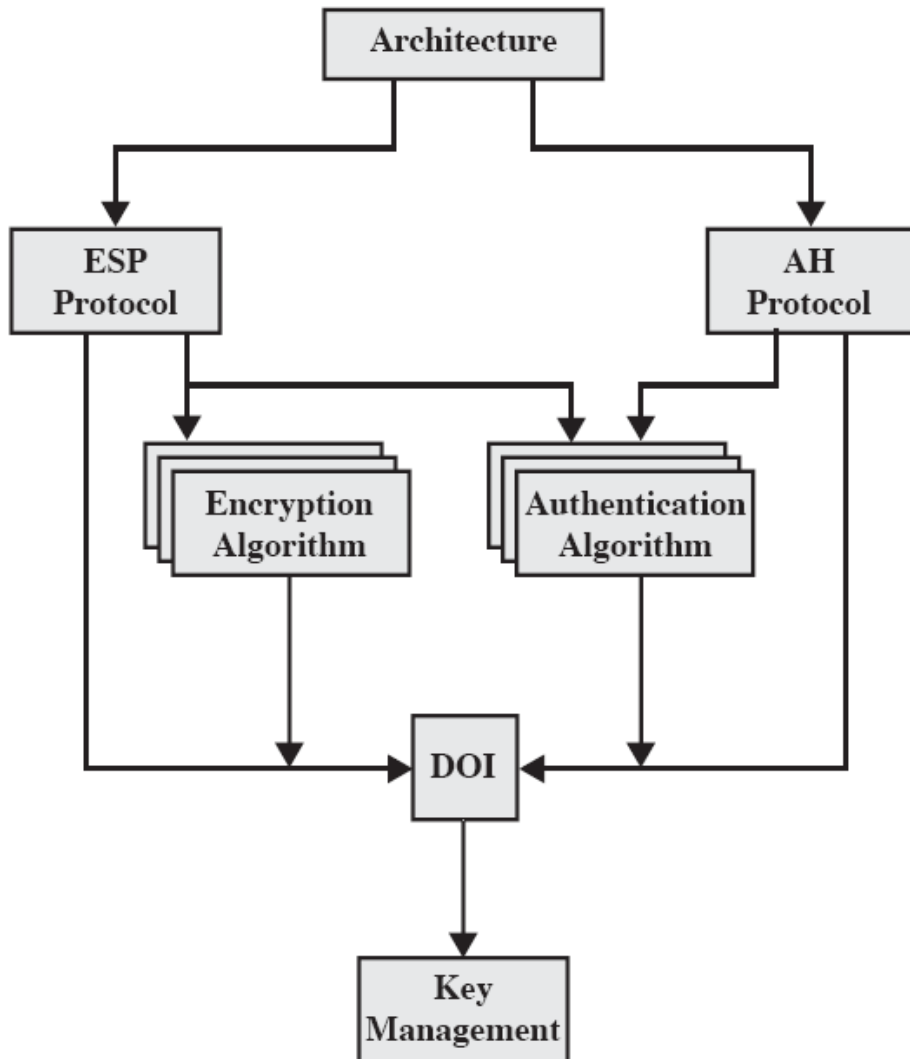
- Secure data communication
 - ◆ Data confidentiality
 - ◆ Data integrity
- Prevent IP spoofing
- Guard against packet replay



Scenario



Overview



◆ Security Association

- One-way relationship between a sender and a receiver
- For two-way security exchange, two SA are required
- Parameters
 - ◆ Security Parameters Index (SPI) – carried in AH/ESP headers to enable the receiving system to select the SA to process the packet
 - ◆ IP Destination Address
 - ◆ Security Protocol Identifier – whether an AH or an ESP

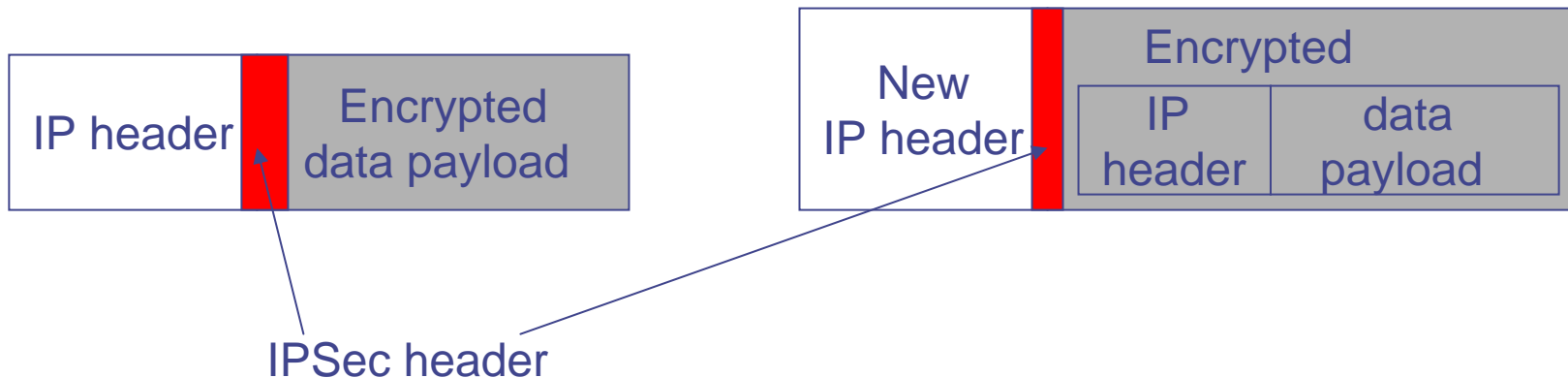
Transport Mode vs. Tunnel Mode

◆ Transport mode

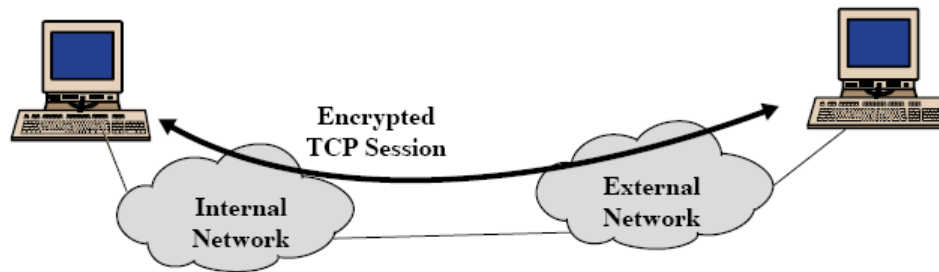
- Encrypts the payload data from upper-layer protocol
- IP header in clear text

◆ Tunnel-mode

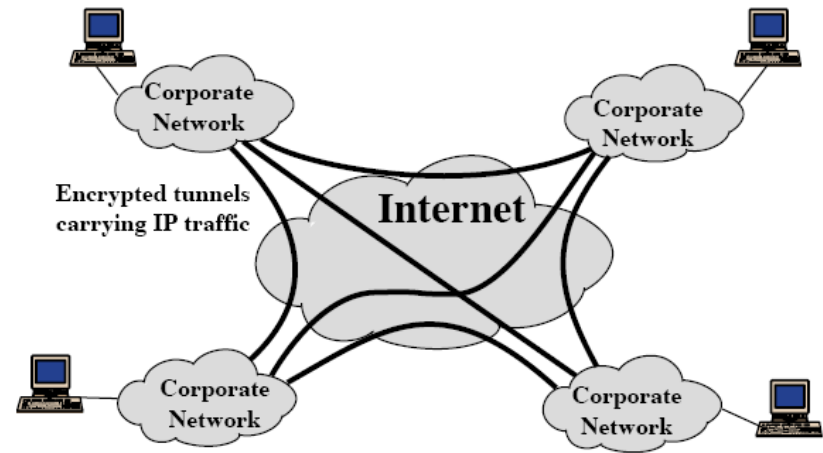
- Encrypts the entire IP packets including the IP header
- Adding a new IP header



An example



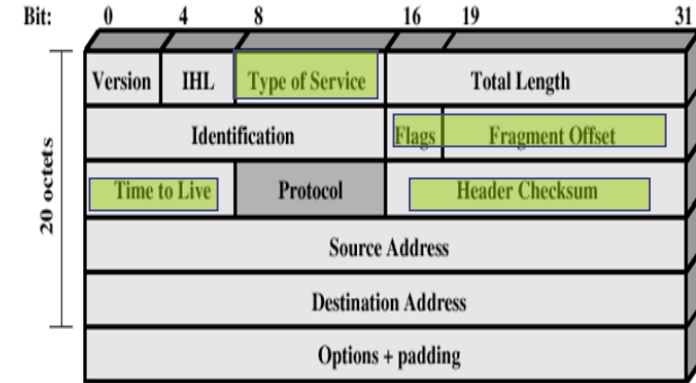
(a) Transport-level security



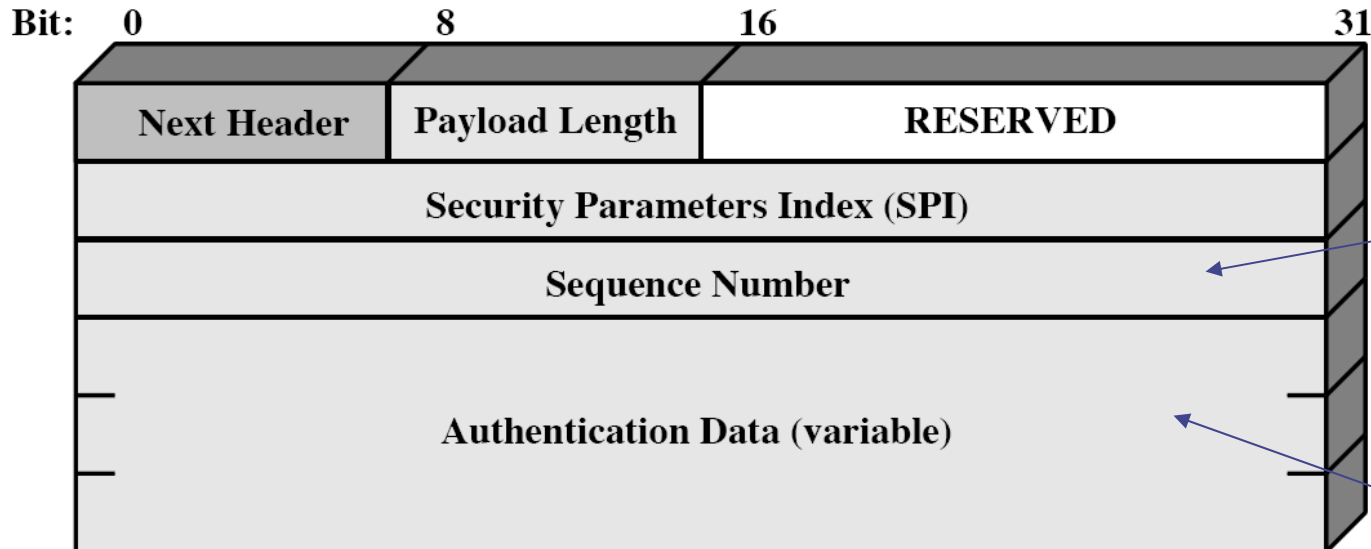
(b) A virtual private network via Tunnel Mode

Authentication Header

- ◆ Security Service
 - Data integrity
 - Source authentication -- Prevent IP spoofing
 - Guard against replay attack
- ◆ Integrity check value
 - MAC -- HMAC-MD5-96/HMAC-SHA-1-96
 - Calculated over
 - ◆ Immutable IP header field, set the mutable field to zero
 - ◆ AH header other than AD field
 - ◆ Upper-level protocol data
- ◆ Anti-Replay



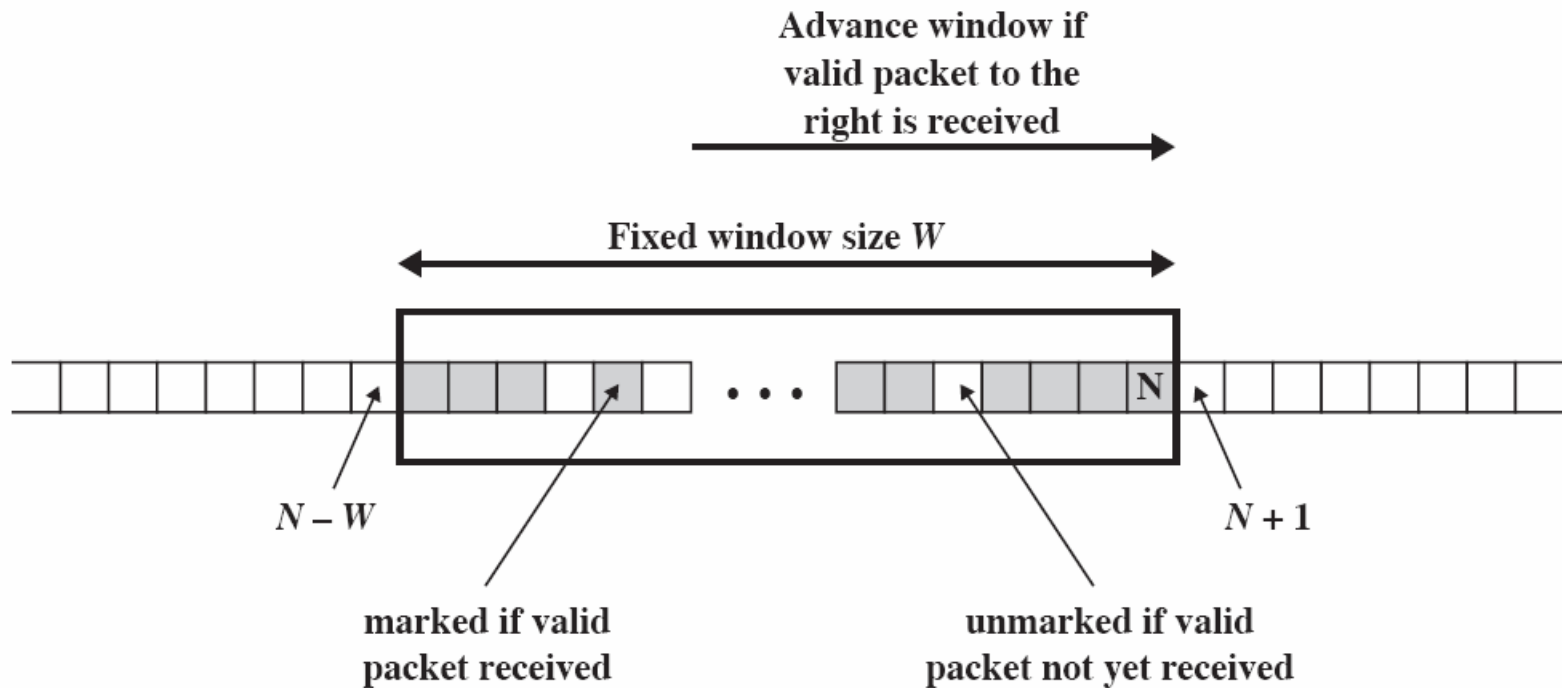
IP v4



Anti-Replay

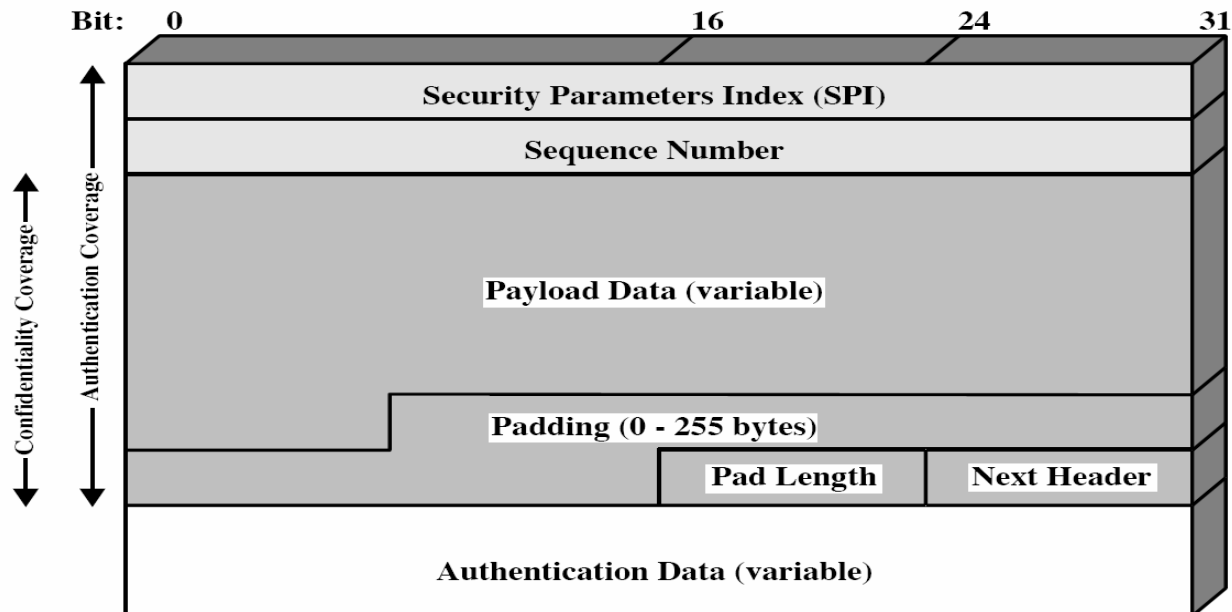
Integrity check value

Anti-Replay



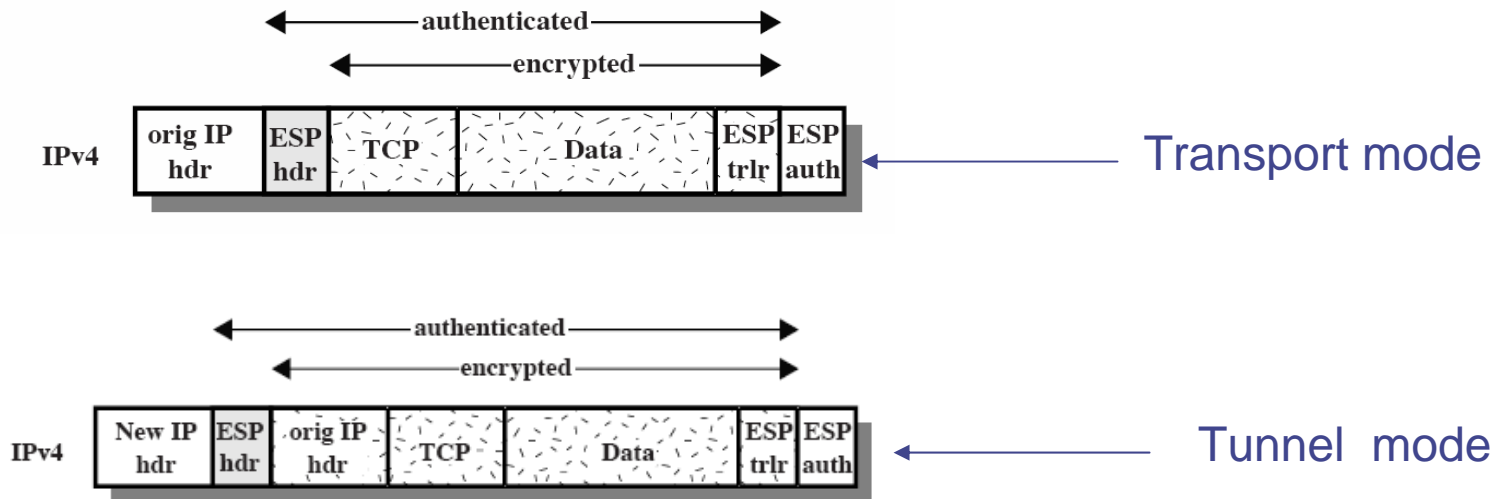
Encapsulating Security Payload

- ◆ Security Service
 - Confidentiality
 - Authentication (optional)
- ◆ Encryption Algorithm
 - 3DES, RC5, IDEA, CAST, Blowfish... +CBC mode
- ◆ Authentication Algorithm
 - MAC -- HMAC-MD5-96/HMAC-SHA-1-96



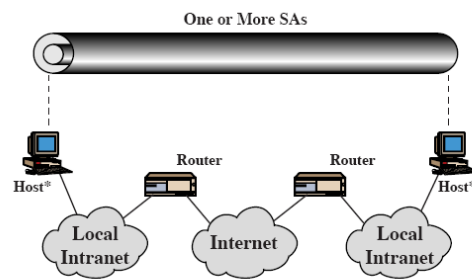
Encapsulating Security Payload

- ◆ Scope of ESP encryption and authentication
- ◆ AH vs. ESP
 - AH protects some of the field in IP header
 - ESP only protects everything beyond the ESP header
 - Separation of authentication and encryption
 - ◆ Port information in clear text for firewall

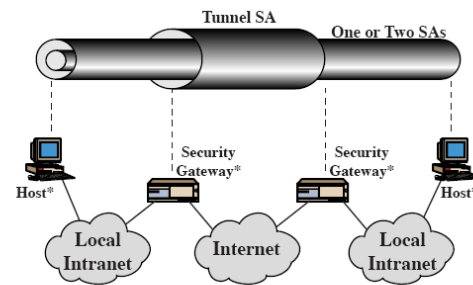


Combination of SA

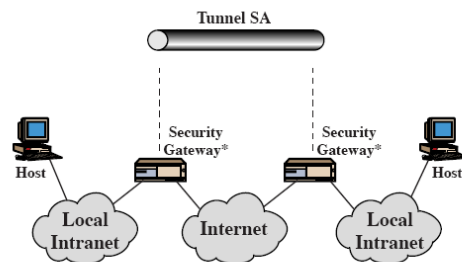
- ◆ Authentication + confidentiality
 - ESP with authentication option
 - AH SA + ESP SA bundle
- ◆ Transport + Tunnel Bundle



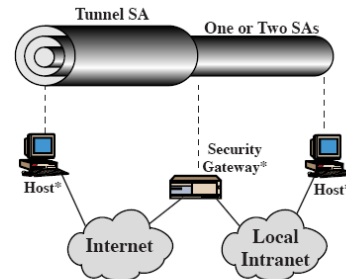
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

Key Management

- ◆ Oakley Key Determination Protocol
 - Based on Diffie-Hellman algorithm
- ◆ Internet Security Association and Key Management Protocol (ISAKMP)
 - A framework for Internet key management
- ◆ Internet Key Exchange Protocol (IKE)
 - The first phase establishes an ISAKMP SA
 - ◆ based on pre-shared keys (PSK), RSA keys and X.509 certificates, even via Kerberos.
 - In the second phase the ISAKMP SA is used to negotiate and setup the IPsec SAs.



BGP

◆ Overview

- AS: Internet routers are grouped into management domains called Autonomous Systems (AS).
- BGP: Routing information between AS is exchanged via BGP UPDATE messages.

◆ Threat

- BGP does not have any security protection over routing information, for example:
 - ◆ Routing information source authentication
 - ◆ UPDATE message integrity protection
- If malicious attacker injects or modifies routing information (UPDATE messages), BPG routing will be interrupted and packets will get dropped.



S-BGP

- ◆ Three security mechanisms are employed
 - Public Key Infrastructure (PKI) is used to support the authentication of AS's identity, and BGP router's identity.
 - BGP transitive path attribute is employed to carry digital signatures covering the routing information in a BGP UPDATE message.
 - IPsec is used to provide data and partial sequence integrity, and to enable BGP routers to authenticate each other for exchanges of BGP control traffic.
- ◆ Further reading
 - Stephen Kent, Charles Lynn, and Karen Seo, Secure Border Gateway Protocol (Secure-BGP), IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000, pp. 582-592
 - Stephen Kent, Charles Lynn, J. Mikkelsen, and Karen Seo, Secure Border Gateway Protocol (S-BGP) -- Real World Performance and Deployment Issues, in ISOC Symposium on Network and Distributed System Security, 2000.



Security in Wireless LAN

- ◆ WEP (Wireless Equivalent Privacy)
 - a link-level security mechanism defined in IEEE 802.11
 - Stream cipher RC4 used in a nonstandard way
 - ◆ A base key is concatenated with a 24-bit per-packet nonce, and is used as a per-packet RC4 key.
 - CRC checksum is used for integrity protection
- ◆ Fluher, Mantin, and Shamir Attack
 - An eavesdropping can deduce the base RC4 key based on several millions encrypted packets whose first byte of plaintext is known.
 - Stubblefield, Ioannidis, and Rubin demonstrated its feasibility
- ◆ Problems with WEP: A summary
 - 24-bit IVs are too short to provide confidentiality
 - CRC checksum is insecure, and can not protect packet integrity
 - The way that IV is combined with the key is subject to cryptanalysis. Passive eavesdroppers can learn the key after observing a few million encrypted packets
 - Lack of source and destination address authentication



Countermeasures

◆ Countermeasures

- Use higher-level security mechanism such as IPSec, VPN, SSL, and SSH for security
- WPA (Wi-Fi protected access) – an intermediate solution.
- IEEE 802.11i
 - ◆ IEEE 802.11X for authentication
 - ◆ CCMP for confidentiality integrity and source authentication

◆ Further readings

- [Security flaws in 802.11 data link protocols](#), Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. Communications of the ACM, 46(5), May 2003, Special Issue on Wireless networking security, pp.35-39.
- [Intercepting Mobile Communications: The Insecurity of 802.11](#) Nikita Borisov, Ian Goldberg, David Wagner, INFOCOM 2001.
- [Using the Fluhrer, Mantin, and Shamir Attack to Break WEP](#), Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, NDSS 2002.

