Cryptography and Network Security
Chapter 19

Fifth Edition
by William Stallings

Lecture slides by Lawrie Brown

Chapter 19 – IP Security

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

—***The Art of War*, Sun Tzu**

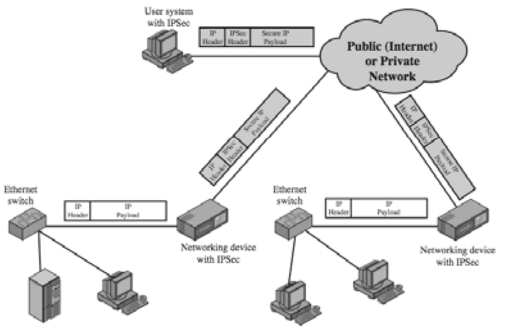
IP Security

- have a range of application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IP Security

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet
- need identified in 1994 report
  - need authentication, encryption in IPv4 & IPv6

IP Security Uses



Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

IP Security Architecture

- specification is quite complex, with groups:
  - Architecture
    - RFC4301 *Security Architecture for Internet Protocol*
  - Authentication Header (AH)
    - RFC4302 *IP Authentication Header*
  - Encapsulating Security Payload (ESP)
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - Internet Key Exchange (IKE)
    - RFC4306 *Internet Key Exchange (IKEv2) Protocol*
  - Cryptographic algorithms
  - Other

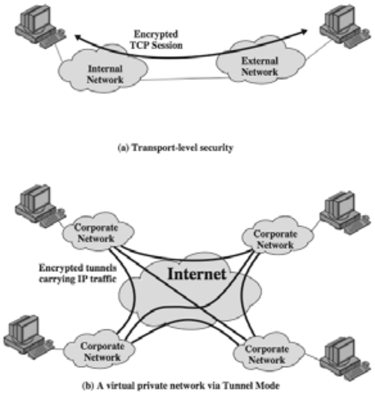
IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Transport and Tunnel Modes

- Transport Mode
  - to encrypt & optionally authenticate IP data
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- Tunnel Mode
  - encrypts entire IP packet
  - add new header for next hop
  - no routers on way can examine inner IP header
  - good for VPNs, gateway to gateway security

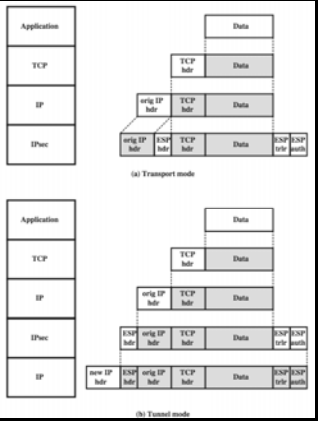
Transport and Tunnel Modes



(a) Transport-level security

(b) A virtual private network via Tunnel Mode

Transport and Tunnel Mode Protocols



(a) Transport mode

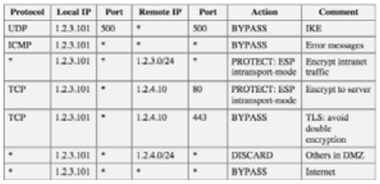
(b) Tunnel mode

Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

Security Policy Database

- ➢ relates IP traffic to specific SAs
  - ● match subset of IP traffic to relevant SA
  - ● use selectors to filter outgoing traffic to map
  - ● based on: local & remote IP addresses, next layer protocol, name, local & remote ports

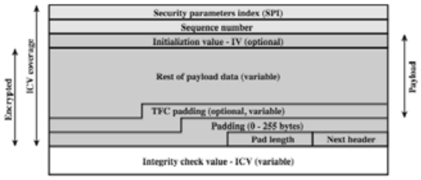


Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Encapsulating Security Payload (ESP)

- provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality
- services depend on options selected when establish Security Association (SA), net location
- can use a variety of encryption & authentication algorithms

Encapsulating Security Payload


Security parameters index (SPI)
Sequence number
Initialiaztion value - IV (optional)
Rest of payload data (variable)
TFC padding (optional, variable)
Padding (0 - 255 bytes)
Pad length
Next header
Integrity check value - ICV (variable)
Encrypted
ICV coverage
Payload

Encryption & Authentication Algorithms & Padding

- ESP can encrypt payload data, padding, pad length, and next header fields
  - – if needed have IV at start of payload data
- ESP can have optional ICV for integrity
  - – is computed after encryption is performed
- ESP uses padding
  - – to expand plaintext to required length
  - – to align pad length and next header fields
  - – to provide partial traffic flow confidentiality

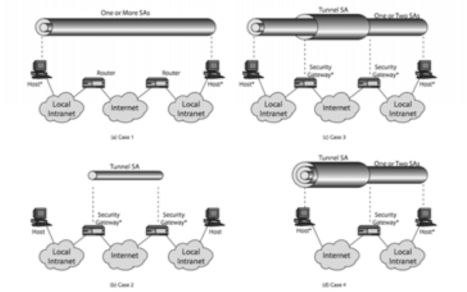
Anti-Replay Service

- replay is when attacker resends a copy of an authenticated packet
- use sequence number to thwart this attack
- sender initializes sequence number to 0 when a new SA is established
  - – increment for each packet
  - – must not exceed limit of $2^{32} – 1$
- receiver then accepts packets with seq no within window of (*N –W+1*)

Combining Security Associations

- SA’s can implement either AH or ESP
- to implement both need to combine SA’s
  - – form a security association bundle
  - – may terminate at different or same endpoints
  - – combined by
    - transport adjacency
    - iterated tunneling
- combining authentication & encryption
  - – ESP with authentication, bundled inner ESP & outer AH, bundled inner transport & outer ESP

Combining Security Associations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

IPSec Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

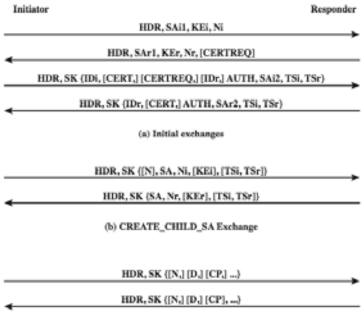
Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - no info on parties, man-in-middle attack, cost
  - so adds cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method
- IKEv2 no longer uses Oakley & ISAKMP terms, but basic functionality is same

IKEV2 Exchanges



HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

(a) Initial exchanges

HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]}

HDR, SK {SA, Nr, [KEr], [TSi, TSr]}

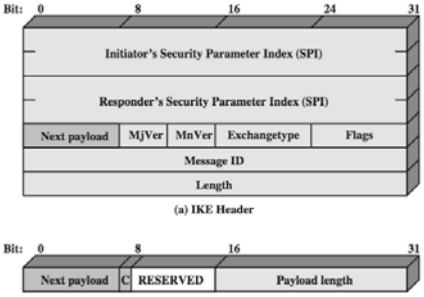
(b) CREATE_CHILD_SA Exchange

HDR, SK {[N,] [D,] [CP,] ...}

HDR, SK {[N,] [D,] [CP], ...}

(c) Informational Exchange

ISAKMP



(a) IKE Header

(b) Generic Payload Header

IKE Payloads & Exchanges

- have a number of ISAKMP payload types:
  - Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- payload has complex hierarchical structure
- may contain multiple proposals, with multiple protocols & multiple transforms

Cryptographic Suites

- variety of cryptographic algorithm types
- to promote interoperability have
  - RFC4308 defines VPN cryptographic suites
    - VPN-A matches common corporate VPN security using 3DES & HMAC
    - VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - provide choices for ESP & IKE
    - AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA

Summary

- have considered:
  - IPSec security framework
  - IPSec security policy
  - ESP
  - combining security associations
  - internet key exchange
  - cryptographic suites used