IP vulnerabilities

Password sniffing

IP Spoofing

- **host rename (LAN)**
- **DNS**
- **source routing**
- **TCP sequence number guessing / splicing**

Session hijacking

Denial of service

- **ICMP bombing, redirects, unreachable**
- **application(ftp,mail,echo) bombing**
- **TCP SYN flooding**

Port probes

AT&T attacks Feb/Mar '92

guest/demo/visitor logins	**296**
rlogins	**62**
FTP passwd fetches	**27**
NNTP	**16**
portmapper	**11**
whois	**10**
SNMP	**9**
X11	**8**
TFTP	**5**
systat	**2**
NFS	**2**

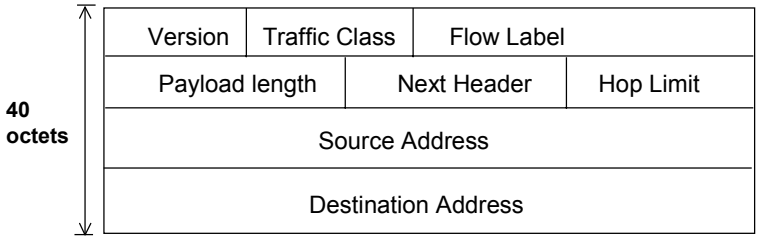
Number of evil sites 95

IPv6

next generation TCP/IP

- Larger addresses (128 bits)
- Improved performance
  - expanded routing
  - header format simplification
  - flow labeling
  - priority (QoS)
- Security
- Interoperability with IPv4

IPv6 Header

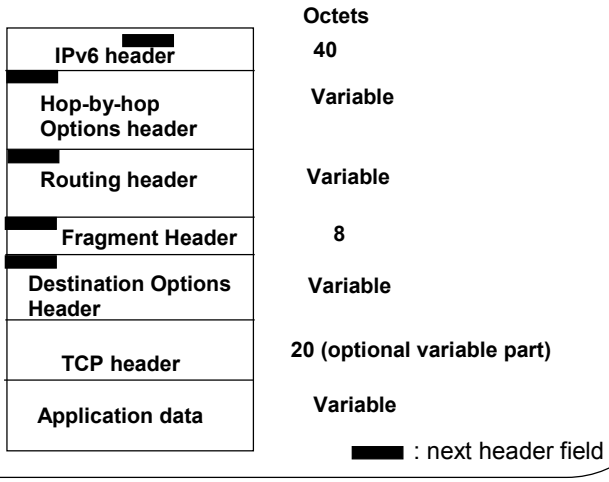


V. (4bit) : 6
T. C.(8bit) : distinguish between different classes or priorities of IPv6 packet(under study)
F. L.(20bit) : used by a host to label packet for special handling
P. L.(16bit) : length of remainder of IPv6 packet following the header
N. H.(8bit) : Identify the type of header immediately following IPv6 packet
H. L.(8bit) : remaining number of allowable hops for this packet
S.A. (128bit) , D.A(128bit)

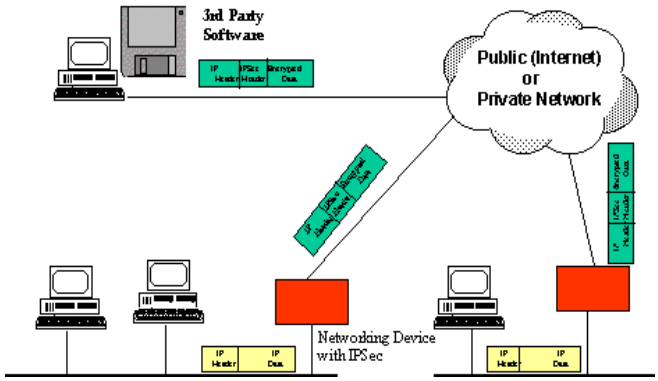
IPv6 Extension Headers

- Hop-by-hop Options header : define special options that require hop-by-hop processing consisting of Next Header (8bit), Header Extension Length (8bit),and Options
- Routing Header : Provides extended routing
- Fragment Header : Contains fragmentation and reassembly information
- Authentication Header : Provides packet integrity and authentication
- Encapsulating Security Payload : provides integrity and privacy
- Destination Option Header : contain optional information to be examined by the destination node

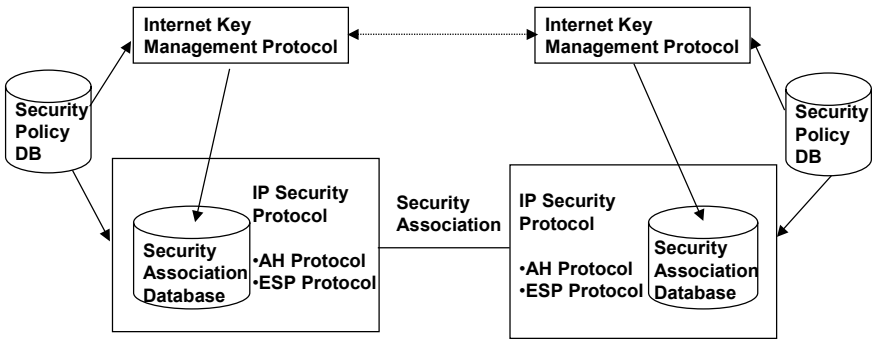
IPv6 Packet with Extension Headers (containing TCP Segment)



IP Security Scenario

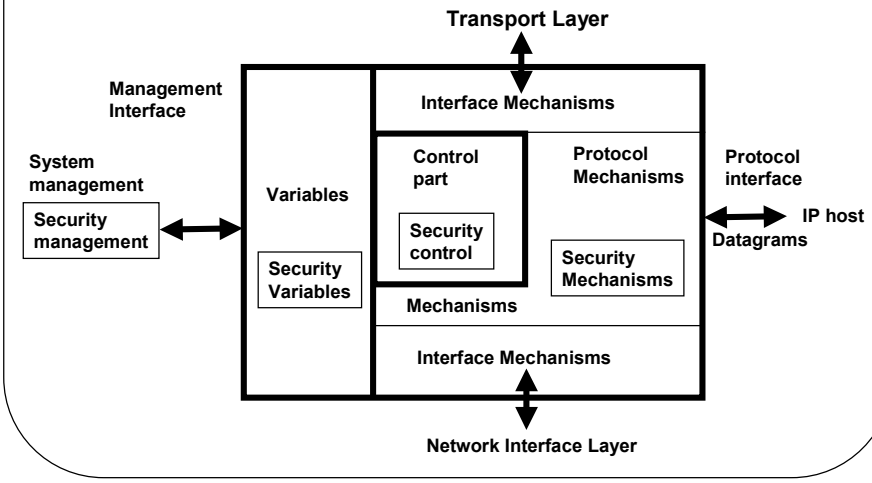


Architecture of IPSec(I)

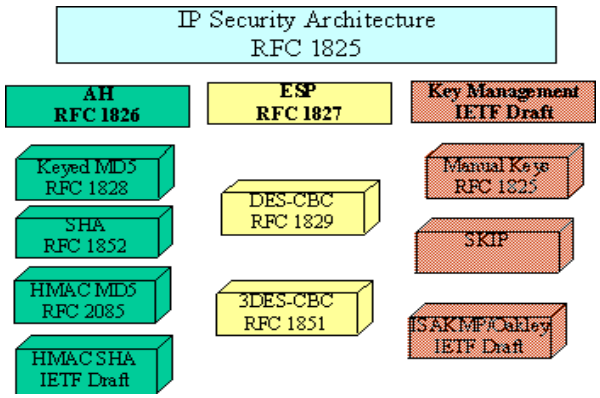


AH : Authentication Header
ESP : Encapsulating Security Payload

Architecture of IPSec(II)



Overview of IPSec protocol



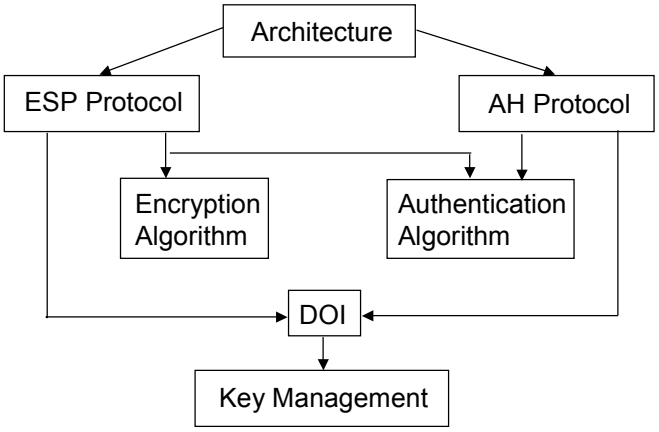
Applications of IPSec

- Secure branch office connectivity over the Internet : VPN
- Secure remote access over the Internet via ISP
- Establishing extranet and intranet connectivity with partners :+SSL
- Enhancing electronic commerce security : SET

IPSec Document

- RFC1636 : Report of IAB Workshop on Security in the Internet Architecture, Feb. 8-10,'94
- RFC1825 : Security architecture for the Internet Protocol
- RFC1826 : IP Authentication Header
- RFC1827 : IP Encapsulating Security Payload
- RFC1828 : IP Authentication using Keyed MD5
- RFC1829 : The ESP DES-CBC Transform
- RFC1851 : The ESP Triple DES Transform
- RFC1852 : IP Authentication using Keyed SHA
- RFC2085 : HMAC-MD5 IP Authentication with Replay Prevention
- RFC2104 : HMAC : Keyed-hashing for Message Authentication
- I-D : Internet Security Association and Key Management Protocol (ISAKMP) etc 23 documents

IPSec Document Overview(I)



DOI : Domain of Interpretation

IPSec document overview(II)

- **Architecture : general concepts, security req't, definitions and mechanisms defining IPsec tech.**
- **Encapsulating Security Payload (ESP) : covers packet format and general issues for packet encryption**
- **Authentication Header (AH) : packet authentication**
- **Encryption Algorithm : various algorithms for ESP**
- **Authentication Algorithm: various algorithms for AU**
- **Key Management : key management**
- **Domain of Interpretation (DOI) : values for the other documents to relate to each other**

Security Association(I)

- Sender/receiver security info
- SA for each direction
- Maintained by kernel
- Uniquely identify
  - ✓ SPI (Security Parameter Index)
  - ✓ IP destination address
  - ✓ Security Protocol Identifier
- Specifies
  - ✓ encryption key, IV, algorithm
  - ✓ authentication algorithm
  - ✓ key lifetimes
  - ✓ SA lifetime
  - ✓ security labels

Security Association(II)

Security Parameter	Example value
SPI(Security Parameter Index)	2916
AH Algorithm	MD5
AH Algorithm Mode	Keyed
AH Transform	RFC1828
AH Key(s)	a 128 bit MD5 Key
AH Mode	Entire Datagram
ESP Algorithm	DES
ESP Algorithm Mode	CBC
ESP Transform	RFC1829
ESP Key(s)	a 56 bit DES key
ESP Mode	Transport
ESP Synch/Init. Vector Size	64
Lifetime	an absolute time in Unix time format

Security Policy Record

Security Parameter	Example Values
SPI(Security Parameter Index)	2916
IP Destination Address	128 bit IPv6 address value
IP Source Address	128 bit IPv6 address value
Protocol	TCP
TCP/UDP Destination Port	23
TCP/UDP Source Port	1234
UserID	Unix UID or other credentials

AH format

Inbound datagram

IPv6 Header	Hop-by-Hop/ Routing	Others	Upper Protocol (e.g. TCP, UDP)

AH calculation

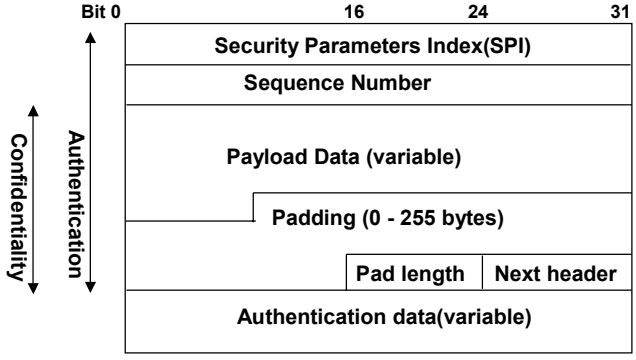
IPv6 Header	Hop-by-Hop/ Routing	Auth Header	Others	Upper Protocol (e.g. TCP, UDP)

AH Syntax

Next Header	Length	RESERVED
Security Parameters Index		
Authentication Data (variable number of 32-bit words)		

8bit Next header : next payload after Authentication payload
8 bit length : length of authentication data in 32 bit word
16 bit reserved field
32 bit SPI : SA of this datagram
Aut. Data : variable length depending on specification of auth. transfrom

ESP format



SPI (32bit): Identifies SA
S.N. (32 bit) : decreasing counter values
P.D. (var.) : transport-level segment (transport m.) or IP packet (tunnel m.)
P. : for encryption of CBC mode

Algorithms

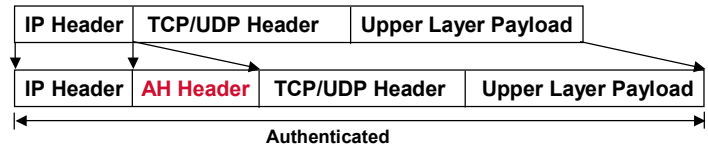
- Confidentiality and authentication
  - 3DES
  - RC5
  - IDEA
  - CAST
  - Blowfish
- MIC (Message Integrity Check)
  - HMAC-MD5-96
  - HMAC-SHA-1-96

Modes(I)

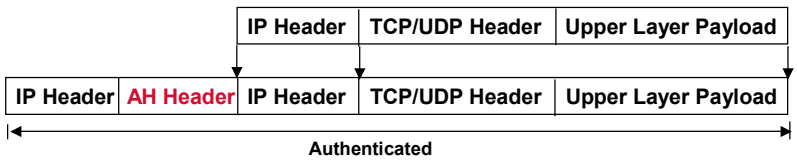
- Transport Mode
  - protection for upper-layer protocol like TCP, UDP or ICMP packet
  - end-to-end btw 2 hosts (e.g. C/S, or 2 W/S)
- Tunnel Mode
  - protect entire IP packet
  - host-to-subnet or subnet-to-subnet

Modes(II)

AH Transformation



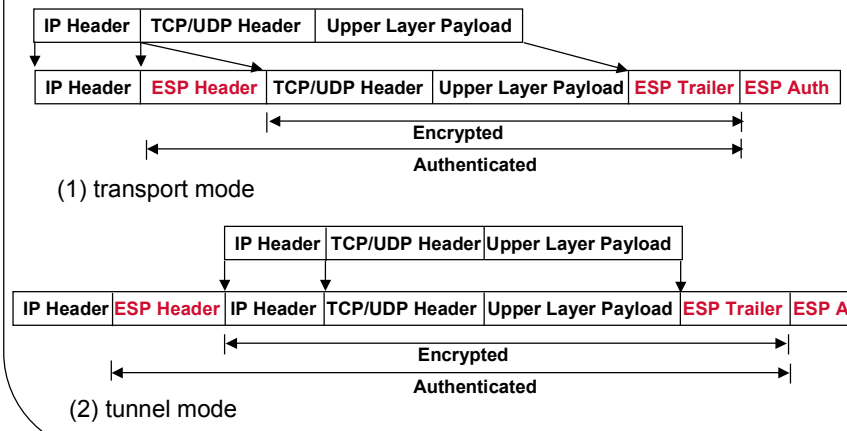
(1) transport mode



(2) tunnel mode

Modes(III)

ESP transformation



(1) transport mode

(2) tunnel mode

Modes(IV)

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticate entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	IPv6 extension headers. Encrypts inner IP packets
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts inner IP packet. Authenticate inner IP packet.

IPSec Services

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

IPSec Services

	AH	ESP(e. only)	ESP (e. + a.)
Access Control	X	X	X
Connectionless Integrity	X		X
Data origin authentication	X		X
Rejection of replayed packets	X	X	X
Confidentiality		X	X
Limited Traffic flow confidentiality		X	X

IP Sec benefits

- Implemented in firewall/router, provides strong security
- Traffic can't bypass firewall with IPsec
- Below transport layer (TCP, UDP) and transparent to applications
- Transparent to end users
- Provide security for individual users if needed.

Limitations

- Don't provide traffic analysis
- Don't provide non-repudiation
- Don't provide denial-of-service attack

key/SA management

active research, not standard

- manual keying
- proposals (SKIP, ISAKMP, Photuris)
  - SKIP (Simple Key Interchange Protocol)
    - light-weight
    - in-band
    - Diffie-Hellman (signed public keys)
  - ISAKMP (Internet Security Association and Key Management Protocol)
    - out-of band, daemon
    - negotiate (Oakley)
    - Diffie-Hellman, public keys

Group key parameter by Oakley

- Modular exp. (a=2) with p
  - 768bit
  - 1024bit
- Elliptic curves over
  - 2^{155}
  - 2^{185}

Features of Oakley

- employ mechanism known as cookies* to thwart clogging attack
- enable 2 parties to negotiate a group
- use nonces to ensure against replay attack
- enable to exchange DH public key values
- authenticate DH exchange to thwart man-in-the-middle attack

* cookie : low level ID carrying in each packet to drive classification or electronic tags placed on your computer by web site.

Example of Oakley(I)

I -> R : CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, $S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

R -> I : CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, $S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^y \| g^x \| EHAS]$

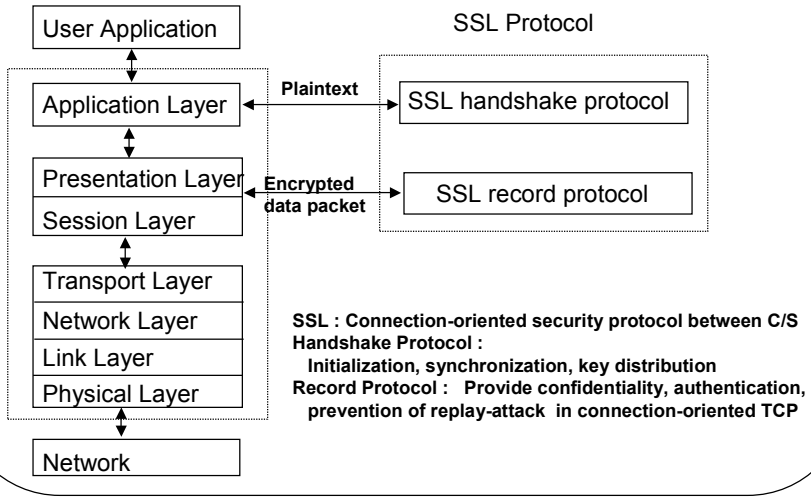
I -> R : CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, $S_{KI}[ID_I \| ID_R \| N_I \| N_R \| GRP \| g^y \| g^x \| EHAS]$

I : Initiator, R:Responder
CKY_I, CKY_R : Initiator, responder cookies, OK_KEYX : Key exchange message type
GRP : Name of DH group for this exchange
EHAO, EHAS : Encryption, hash, authentication functions, offered and selected
NIDP : Indicates encryption is not used for remainder of this message
ID_I, ID_R : Identifier for initiator, responder
NI, NR : Random nonce supplied by initiator, responder for this exchange
$S_{KI}[X]$, $S_{KR}[X]$: Indicates the signature over X using private key (signing key) of initiator, responder

Example of Oakley(II)

- (step1) transmit cookie, group to be used, I's public key and others
- (step2) R verifies signature using I's public key and echoing adding signature
- (step 3) verifies R's signature, check nonce against replay attack
- (step 4) complete the exchange, I send message back to R to verify that I have received R's public key

SSL(I)



SSL : Connection-oriented security protocol between C/S
Handshake Protocol :
Initialization, synchronization, key distribution
Record Protocol : Provide confidentiality, authentication, prevention of replay-attack in connection-oriented TCP

SSL(II)

- Handshake Protocol
  - (Step 1) Selection of algorithm, distribution of master key, authentication of server
  - (Step 2) Authentication of client if necessary
- Record Protocol
  - If no use session ID, no need authentication of client
  - If use of Session ID, no need authentication of client
  - If use of Session ID, need authentication of client

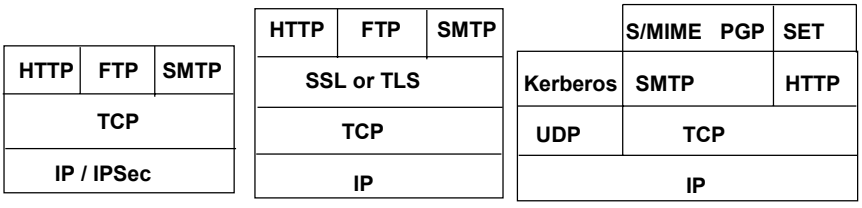
SSL(III)

- Confidentiality : Fortezza, IDEA, RC2-40, RC4-40, DES, 3DES
- Anti-traffic attack
- Message Authentication : HMAC-MD5

Comparison of IPv6 and SSL

Classification		IPv6	SSL
Layer		• Network layer • Applicable to transport layer	• Transport layer • Limited privacy and authentication serivices
Style of usage		• host-to-host • host-to-subnet • subnet-to-subnet	host-to-host
Key exchange		• IKMP • Hard to define exchange mechanism for large network	• Server key exchange message • Client key exchange message • secure WWW-based
Algorithm	Privacy	• No limitation • DES, 3DES, IDEA, Blowfish, RC5	•No limitation •Fortezza, IDEA, RC2, RC4, DES, 3DES
	Authentication	• Keyed MD5, SHA-1 • packet authentication on network layer • origin and destination address	• MD5 • Packet authentication on transpor t layer
	Integrity	• Tunnel mode ESP • Transparent mode ESP	• Protocol (HTTP, NNTP, SMTP) dependent

Security Facilities in TCP/IP



(a) Network level (a) transport level (c) application level