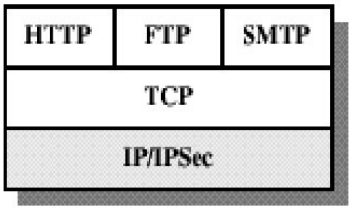
IP Security

- Objectives
- IPSec architecture and concepts
- IPSec authentication header
- IPSec encapsulating security payload

http://www.ietf.org/html.charters/ipsec-charter.html

Web Security: Network Level

- Provide security using IPSec
- Advantages:
  - Transparent to users and applications
  - Filtering : only selected traffic need incur the overhead of IPSec processing



Why IP Security?

- Problem:
  - Traditional IP does not directly handle encryption/authentication of traffic …
  - …There was a need as identified in 1994 to "secure the network infrastructure from unauthorized monitoring and control of network traffic … and … end-to-end-user traffic" (Stallings, 1999)
- Recommendations of Internet Architecture Board
  - Include authentication/encryption in next-generation IP
    - concepts compatible both with IPv4 and IPv6
  - These features are **MANDATORY** for IPv6 implementations and **OPTIONAL** for IPv4 implementations
  - Both implementations use the "*extension header*" method

IPSec Objectives

Band-aid for IPv4: known vulnerabilities

- Replay
- Wiretap
- Spoofing and Masquerading
- Hijacking of connections

- IP layer mechanism for IPv4 and IPv6
  - Not all applications need to be security aware
- Can be transparent to users
- sometimes used interchangeably with IPv6, but it is more correct to think of IPv6 as a protocol incorporating IPSEC philosophies

IPv6 'includes' IPSEC

- Protocol to support
  - authentication of data origin,
  - data integrity, and
  - encryption for privacy
- Techniques
  - Authentication Header and Encapsulating Security Payload
  - Security associations between connections, connection sets

Benefits of IPSec

- In a firewall/router, it provides strong security to all traffic crossing the perimeter (no overhead for local)
- It is below transport layer, hence transparent to applications
- It can be transparent to end users
- It can provide security for individual users if desired

Security Depends Upon

- secure protocols but also (among others)
  - cryptographic strength
  - implementation quality
  - good random number sources
  - end system security
  - system management
  - … .

IP Security Architecture

The specification is quite complex, defined in numerous RFC's (Main ones RFC 2401/2402/2406/2408)

There are seven groups within the original IP Security Protocol Working Group, based around the following:

- **Architecture** (general issues, requirements, mechanisms)
- **Encapsulating Security Payload**, ESP (packet form and usage for encryption and some auth)
- **Authentication Header**, AH (packet form and usage for auth)
- **Encryption Algorithm** (how different ones are used)
- **Authentication Algorithm** (using algorithms for AH and ESP)
- **Key management** (schemes)
- **Domain of Interpretation** (relating the other ones)

Next level

IPSec lets systems do the following:

- Allow selection of required security protocols
- Decide on which algorithms to use on which services,
- Deal with the "key" issue

These choices are guided by the two protocols:

- Authentication Header
  - authentication and integrity of payload and header
- Encapsulating Security Payload
  - without authentication: confidentiality of payload
  - with authentication: confidentiality, authentication and integrity of payload

Some services can only be provided with certain combinations of AH, ESP "with" and ESP "without".

Components and Concepts

- Host or gateway implementation
- Tunnel vs. Transport mode
- Security association (SA)
  - Security parameter index (SPI)
  - Security policy database (SPD)
  - SA database (SAD)
- Encapsulating security payload (ESP)
- Authentication header (AH)

Hosts and Gateways

- Hosts can implement IPSec to :
  - Other hosts in transport or tunnel mode
  - Gateways with tunnel mode
- Gateways to gateways - tunnel mode

IPSEC Security Association

- SA is a one-directional relationship between sender and receiver
- Determines IPSec processing for sender and IPSec decoding for destination
- SAs are not fixed, but generated and customized per traffic flows
- SA applies to AH or ESP but not both
- two-way secure exchange of IP packets requires two SAs
- SAs are established by
  - management protocols (IKE)
  - manually

IPSEC Security Association

- referenced by a 32 bit Security Parameter Index (SPI) carried in header of each IPSEC packet
- The SPI allows the destination to select the correct SA under which the received packet will be processed (according to the agreement with the sender)
- SA for an IP packet uniquely identified by
  - SPI
  - destination IP address
  - IPSec protocol (AH or ESP)

SA Parameters

- sequence number counter: 32 bit
- overflow flag: indicating abort or not on overflow
- anti-replay window: to check inbound replay
- AH information:
  - algorithm, key, key lifetime
- ESP information:
  - algorithm, key, key lifetime for encryption and authentication
- lifetime of SA: time interval or byte count
- IPSEC protocol mode: transport, tunnel, wildcard (allows same SA to be used, for either tunnel or transport, on a per-packet basis, specified by the application)
- path MTU (maximum transmission unit)

SA Database - SAD

- Holds parameters for each SA
  - Lifetime of this SA
  - AH and ESP information
  - Tunnel or transport mode
- Every host or gateway participating in IPSec has own SA database (not specified how expected functionalities are provided)

IPSEC Traffic Protocols

- both IP AH and IP ESP can operate in
  - transport mode
    - end-to-end
  - tunnel mode
    - security-gateway to security-gateway
- transport mode and tunnel model can coexist

Transport Mode

- Transport Mode
  - good for upper layer protocols
  - authentication is between the client and server workstations
  - workstation may be either local or remote
  - workstation and server share a protected secret key

Tunnel Mode

- Tunnel Mode
  - protects entire IP packet
  - authentication is between remote workstation and corporate firewall
  - authentication for access to entire internal network or because the server doesn't "speak authentication"
    - (called "standards based tunneling" as opposed to some other forms which do not adhere to any specific standard).

"Protection" is at different levels

- **The transport mode is "end-to-end"**
  - AH is used to authenticate the IP payload and certain parts of the headers
  - ESP is used to encrypt the IP payload
    - not headers for IPv4, but includes extension header info for IPv6
  - ESP with authentication encrypts IP payload and the extension headers; authenticates IP payload but not IP header
- **The tunnel mode is not end-to-end**
  - AH: authenticates the inner IP packet including header plus some of the outer IP header and IPv6 extensions
  - ESP: encrypts inner IP packet (which includes header info)
  - ESP "with": encrypts inner IP packet, authenticates inner IP packet

Security Policy Database - SPD

- What traffic to protect?
- Has incoming traffic been properly secured?
- Policy entries define which SA or SA Bundles to use on IP traffic
- Each host or gateway has own (nominal) SPD
- Index into SPD by **Selector fields**
  - Dest IP, Source IP, UserId, DataSensitivityLevel, Transport Protocol, IPSec Protocol, Source & Dest Ports, …

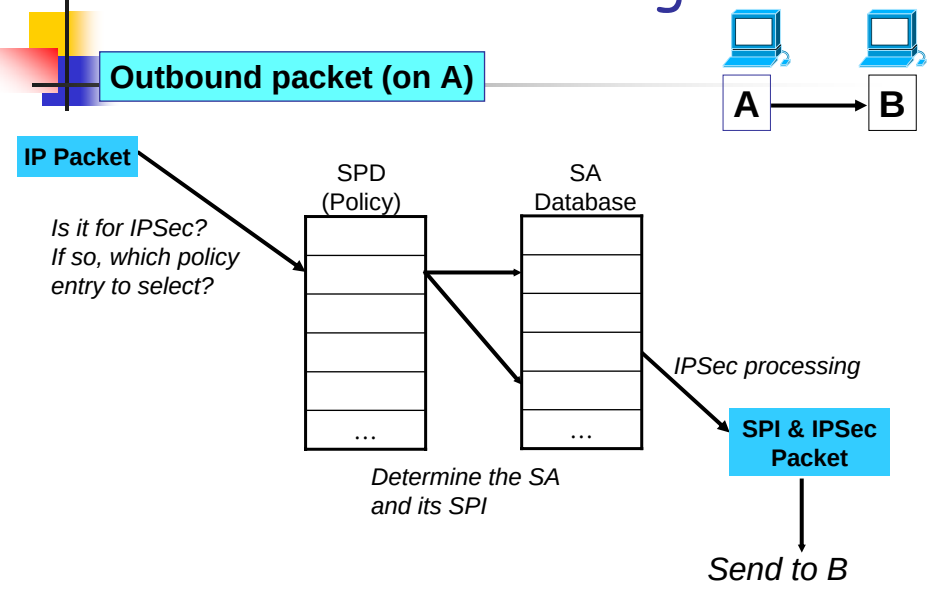
SPD Entry Actions

- Discard
  - Do not let in or out
- Bypass
  - Outbound: do not apply IPSec
  - Inbound: do not expect IPSec
- Protect – will point to an SA or SA bundle
  - Outbound: apply security
  - Inbound: check that security must have been applied

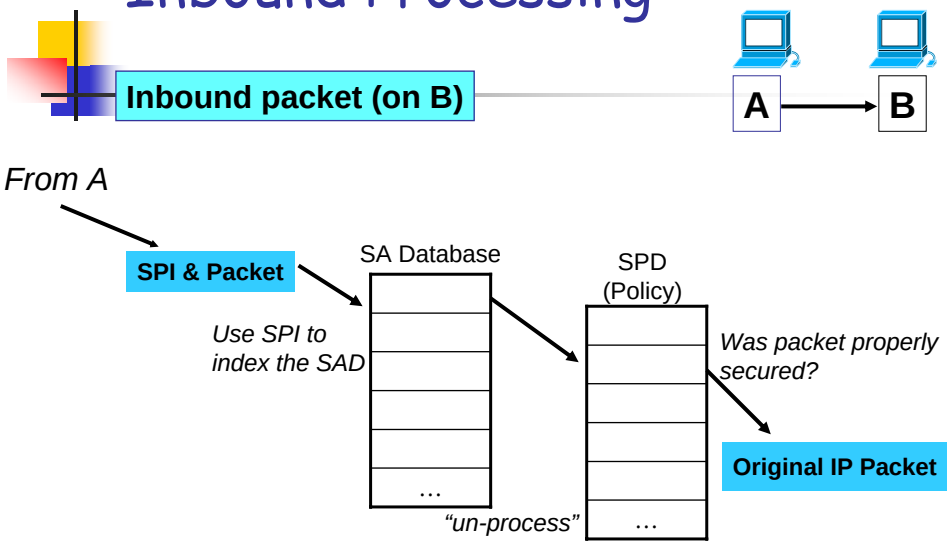
If the SA does not exist…

- Outbound processing: use IKE to generate SA dynamically
- Inbound processing: drop packet

Outbound Processing



Inbound Processing



IP Authentication Header

- Data integrity
  - Entire packet has not been tampered with
- Authentication
  - Can "trust" IP address source
  - Use MAC on IP packet header and data payload to authenticate
- Anti-replay feature
- Integrity check value

Authentication Header

- Provides support for data integrity and authentication (MAC code) of IP packets.

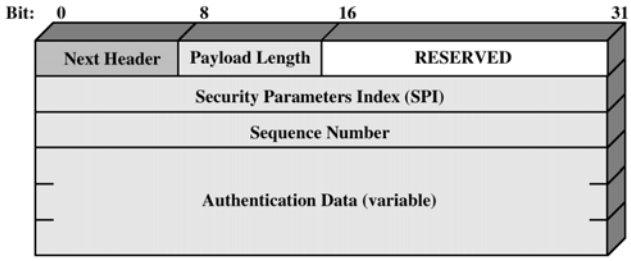


Figure 6.3 IPSec Authentication Header

IP AH Fields

- next header: 8 bit protocol field
- length: 8-bit field specifying length of authentication data in 32-bit words
- Unused (so far): 16 bit set to 0
- SPI: 32 bit to identify a SA
- sequence number: 32 bit
- integrity check value (ICV): some multiple of 32 bits, e.g., 96, 128, 160

Anti-replay Feature

- Optional (default is ON)
- Information to enforce held in SA entry
- Sequence number counter – 32-bit for outgoing IPSec packets
- From sender's side, sequence number starts at 1 and cannot go past $2^{32}-1$ (if reached, SA terminated and new one negotiated)
- Anti-replay window
  - 32-bit
  - Bit-map for detecting replayed packets

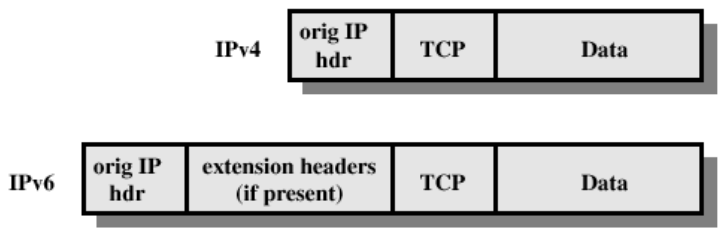
Anti-replay Mechanism

- receiver keeps a window of min size 32 (64 preferred and default, larger is ok)
  - packets to the left of window are discarded
  - repeated packets within window are discarded
  - authentic packets to the right of window cause window to move right
- Window should not be advanced until the packet has been authenticated
- Without authentication, malicious packets with large sequence numbers can advance window unnecessarily
  - Valid packets would be dropped

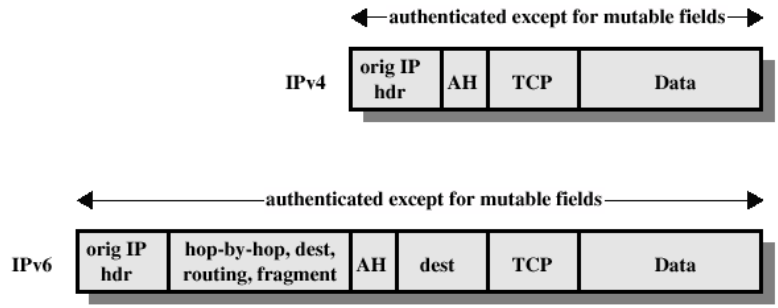
Integrity Check Value - ICV

- ICV is a message authentication code produced by a MAC algorithm
- The ICV is calculated over
  - IP header fields that do not change (e.g., source address) or are predictable (e.g., destination address); those that do change (e.g., Time-to-Live) are set to zero for calculation
  - AH header minus Authentication Data (where the ICV value goes)
  - Upper-level data (assumed not to change in transit)
- Code may be truncated to first 96 bits
- Compliant implementations must support HMAC-MD5-96, HMAC-SHA-1-96

Before applying AH

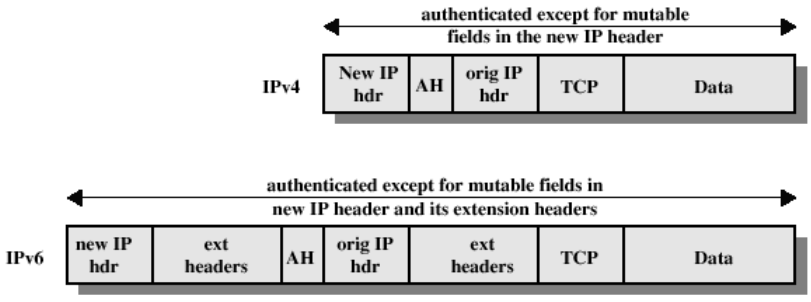


Transport Mode AH



- protocol field of IP header is 51 (for AH payload)
- AH in turn contains protocol field specifying protocol of actual payload, e.g., TCP or UDP or ICMP or IP

Tunnel Mode AH



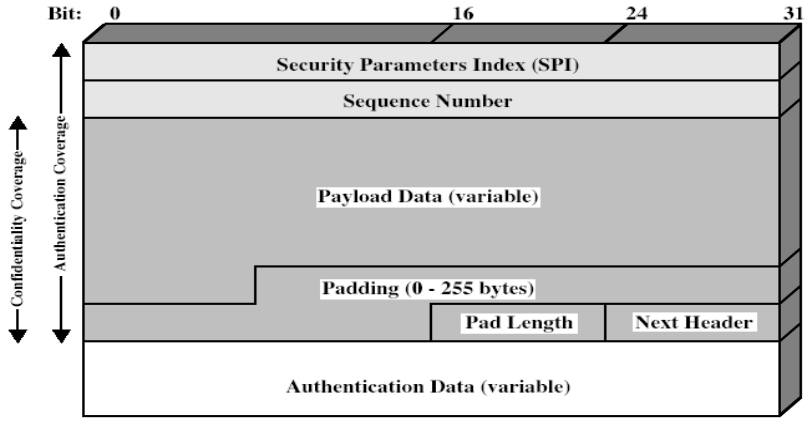
IP Encapsulating Security Payload (ESP)

- IPv4 and IPv6
  - ESP: confidentiality
  - ESP w/Auth: confidentiality, authentication, integrity
  - ESP w/Auth is an option within ESP
- ESP header (cleartext)
  - security parameter index (SPI)
  - sequence number: 32 bit
  - Initial Value for CBC (if algorithm requires it)
- ESP trailer (encrypted)
  - padding
  - next header (identifies payload protocol)
- ESP w/Auth authentication
  - ICV: for authentication option
  - applies only to encrypted payload and not to header
- Format varies based on encryption type

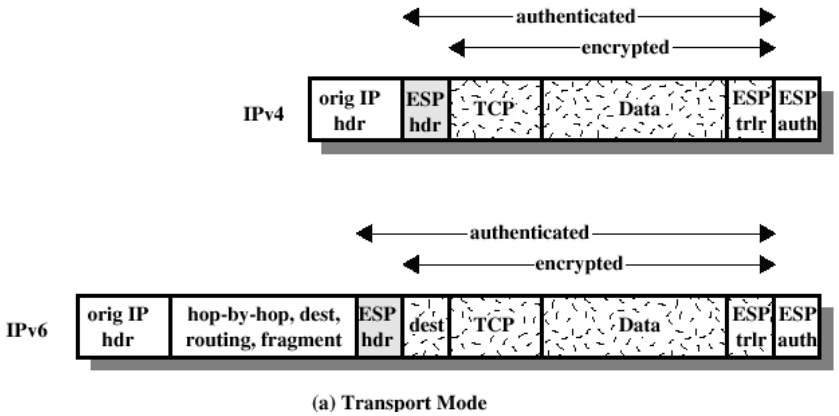
Encapsulating Security Payload

- provides message content confidentiality and limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- Modes supported by ESP:
  - **Tunnel** mode: encrypt entire IP packet plus headers inside another IP packet
  - **Transport** mode: do not encrypt headers
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC most common
  - pad to meet blocksize, for traffic flow

Encapsulating Security Payload

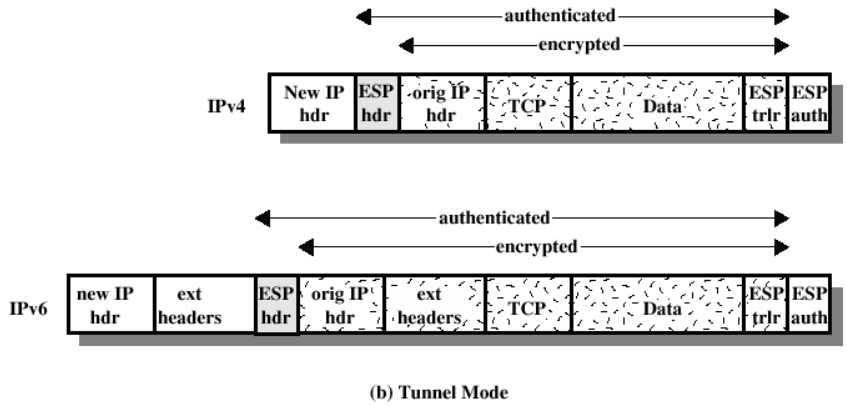


ESP Encryption and Authentication



(a) Transport Mode

ESP Encryption and Authentication



(b) Tunnel Mode

Outbound Packet Processing

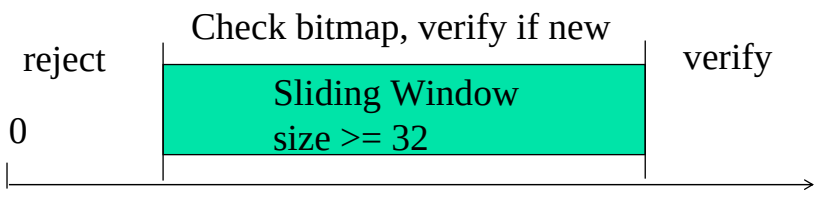
- Form ESP payload
- Pad as necessary
- Encrypt result [payload, padding, pad length, next header]
- Apply authentication
  - Allow rapid detection of replayed/bogus packets
  - Allow potential parallel processing - decryption & verifying authentication code

Outbound Packet Processing

- Sequence number generation
  - Increment then use
  - With anti-replay enabled, check for rollover and send only if no rollover
  - With anti-replay disabled, still needs to increment and use but no rollover checking
- ICV calculation
  - ICV includes whole ESP packet minus *authentication data* field
  - Implicit padding of '0's between *next header* and *authentication data* is used to satisfy block size requirement for ICV algorithm

Inbound Packet Processing

- Sequence number checking
  - Anti-replay is used only if authentication is selected
  - Sequence number should be the first ESP check on a packet upon looking up a SA
  - Duplicates are rejected



Inbound Packet Processing

- Packet decryption
  - Decrypt quantity [ESP payload, padding, pad length, next header] per SA specification
  - Processing (stripping) padding per encryption algorithm; in case of default padding scheme, the padding field should be inspected
  - Reconstruct the original IP datagram
- Authentication verification (optional) precedes decryption to avoid denial of service attacks

Key Management

- AH and ESP require encryption and authentication keys
- Process to negotiate and establish IPSec SA's between two entities
  - handles key generation and distribution
  - typically need 2 pairs of keys
    - 2 for each direction, for AH and ESP

IPSEC Key Management

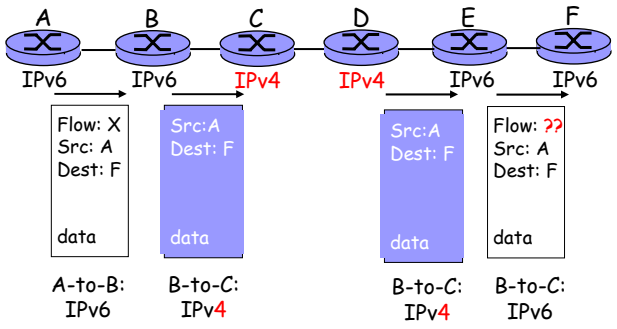
There are three possibilities for Key Management

- **Manual** keying
  - manually distribute crypto information, sysadmin configures
- **SKIP**: Simple Key Interchange Protocol (Sun)
  - Not session oriented
- **ISAKMP**: Internet Security Association and Key Management Protocol (NSA)
  - General-purpose security exchange protocol, provides framework for key management and policy negotiations
  - defines procedures and packet formats to establish, negotiate, modify and delete SAs
  - independent of key exchange protocol, encryption algorithm and authentication method

Transition From IPv4 To IPv6

- Not all routers can be upgraded simultaneous
  - no "flag days"
  - How will the network operate with mixed IPv4 and IPv6 routers?
- Two proposed approaches:
  - *Dual Stack*: some routers with dual stack (v6, v4) can "translate" between formats
  - *Tunneling:* IPv6 carried as payload in IPv4 datagram among IPv4 routers

Dual Stack Approach



Tunneling