

# ISA 666

## Internet Security Protocols

### IPSEC

#### Virtual Private Network

## Outline

- Secure channel” concept
- Pros and cons of providing security at different layers
- IPsec objectives
- IPsec architecture & concepts
- IPsec authentication header
- IPsec encapsulation security payload
- Virtual Private Network (VPN)

## Security Requirements for Communication Across Insecure Networks

- We want to provide the following security services for communication across **insecure** networks
  - Confidentiality
  - Authentication
  - Data integrity
  - Resistance against replay-attack
  - Non-repudiation
  - ...

## Security Requirements for Communication Across Insecure Networks

- Applications
  - Transaction across distributed financial institutions
  - Connecting to business partners at remote site
  - Remote access for employees
  - Protecting credit card numbers in e-commerce transactions
  - Electronic voting, tax returns
  - ...

## The 'Secure Channel' Concept

- We achieve this by building a “secure channel” between two end points on an insecure network.
- Typically offering:
  - Data origin authentication
  - Data integrity.
  - Confidentiality.
  - Resistance against replay-attack
- But usually not:
  - Non-repudiation.
  - Any services once data received.

## The 'Secure Channel' Concept

- Secure channel built usually built as follows:
- An authenticated key establishment protocol.
  - During which one or both parties is authenticated.
  - And a fresh, shared secret is established.
- A key derivation phase.
  - MAC & bulk encryption keys are derived from shared secret.
- Then further traffic protected using derived keys.
  - MAC gives data integrity mechanism and data origin authentication.
  - Encryption gives confidentiality.
- Optional: session re-use, fast re-keying, ...

## Typical Cryptographic Primitives for Security Services

- Data confidentiality
  - Symmetric encryption algorithms used for speed.
- Data origin authentication, integrity
  - MAC algorithms.
  - Usually built from hash functions, also fast.
- Entity authentication and key establishment
  - Asymmetric encryption and signature algorithms
  - Diffie-Hellman.
  - Nonce
- Key derivation
  - (Keyed) pseudo-random functions.

## Typical Cryptographic Primitives for Security Services (Cont'd)

- Resistance against replay attack
  - MAC-protected sequence numbers
  - Nonces and timestamps often used for freshness in entity authentication exchanges.

## Security and Network Layers

- But where shall we put security?
  - Depending on the security services intended
  - Depending on engineering tradeoffs
    - Security level
    - Deployment and run-time costs
    - Usability
- Security can be applied at any of the network layers
- What are the pros and cons of applying security at each of these layers?

## Security and Network Layers

- Data Link (Network Interface) layer:
  - ✓ covers all traffic on that link, independent of protocols above
    - e.g. link level encryption
  - ✗ protection only for one 'hop'.
- Network (Internet) layer:
  - ✓ covers all traffic, end-to-end.
  - ✓ transparent to applications.
  - ✗ little application control.
    - application has no visibility of Internet layer.
  - ✗ unnatural, since network layer is stateless and unreliable.
    - order of data in secure channel may be crucial.
    - difficult to maintain if IP datagrams are dropped, re-ordered,...

## Security and Network Layers

- Transport layer:
  - ✓ end-to-end, covers all traffic using the protected transport protocol.
  - ✓ applications can control when it's used.
    - application has greater visibility of transport layer.
  - ✓ transport layer may be naturally stateful (TCP).
  - ✗ applications must be modified (unless proxied).
- Application layer:
  - ✓ security can be tuned to payload requirements.
    - different applications may have radically different needs.
    - eg VoIP applications versus sensitive data transfer.
  - ✗ no leveraging effect – every application must handle it's own security.

## Recommendations of Internet Architecture Board

- Provide authentication and encryption security services in IP – IPSec
- Mandatory for IPv6
- Optional for IPv4
- Based on “extension header”

## Why Do We Need IPSec?

- IP V4 has no authentication
  - IP spoofing
  - Payload could be changed without detection.
- IP V4 has no confidentiality mechanism
  - Eavesdropping
- Denial of service (DoS) attacks
  - Cannot hold the attacker accountable due to the lack of authentication.
- Replay attack
- Connection hijacking

## IPSec Functionalities

- (Point-to-point) security services
  - Authentication of data origin
  - Data integrity
  - Data confidentiality
  - Partial flow confidentiality
  - Resistance against replay-attack
- Algorithm-independent with standard defaults

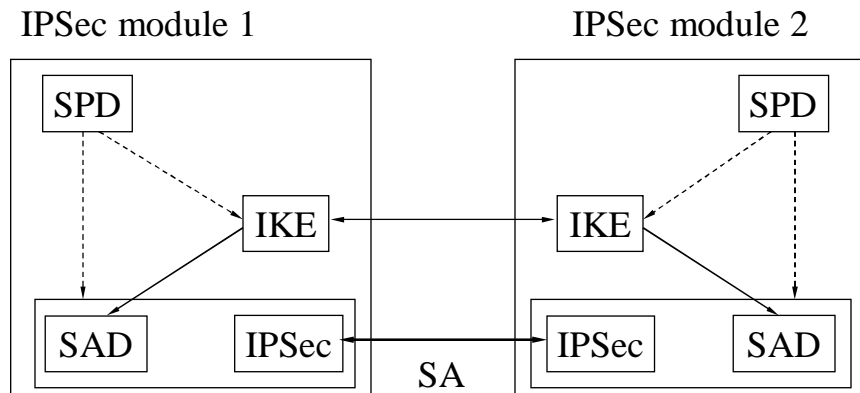
## IPSec Benefits

- IPSec is “attached upon” IP layer, and is below any layer upon IP
  - Transparent to transport layer, and any upper layer applications (i.e. telnet, ftp, email, HTTP)
  - Could be transparent to end users
  - Can provide point-to-point security services
  - Can provide security services at firewall or gateways to all passing traffic – VPN
  - Compatible with traditional IPv4
  - Support incremental deployment

## IPSec Specifications

- IPSec is specified in a number of RFCs
  - RFC 2401: Security Architecture for the Internet Protocol
  - RFC 2402: IP Authentication Header
  - RFC 2406: IP Encapsulation Security Payload (ESP)
  - RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
  - RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 2409: The Internet Key Exchange (IKE)
  - RFC 2411: IP Security Document Roadmap
  - RFC 2412: The OAKLEY Key Determination Protocol
  - ...

## IPSec Architecture



*SPD: Security Policy Database; IKE: Internet Key Exchange;  
SA: Security Association; SAD: Security Association Database.*

## IPSec Architecture (Cont'd)

- IPSec does the following
  - Allow selection of security protocols
  - Decide which crypto algorithm to use on which services selected
  - Provide interface for manually or automatically generate keys
  - Provide mechanisms to specify what security services on what traffic
  - Provide mechanisms to manage security parameters needed for the security service
- Two Protocols (Mechanisms)
  - Authentication Header (AH)
    - Authentication and integrity of payload and header
  - Encapsulating Security Payload (ESP)
    - With authentication: confidentiality, authentication and integrity of payload
    - Without authentication: confidentiality of payload
- IKE Protocol
  - Internet Key Management

## IPSec Concepts

- Security association (SA)
  - Security parameter index (SPI)
  - Security policy database (SPD)
  - SA Database (SAD)
- Host or gateway implementation
- Tunnel vs transport mode

## Security Association (SA)

- An unidirectional, point-to-point association between a sender and a receiver
  - Consists of a set of security related parameters
  - E.g., crypto algorithm selected, crypto keys, sequence number
- Determine IPSec processing for senders and receivers
- SA applies to AH or ESP but not both
- A bidirectional IPSec channel needs 2 different SAs
- SAs are not fixed! Generated and customized per traffic flows
- SAs can be manually, or automatically established
  - Internet Key Exchange (IKE)

## Security Association (SA) Content

- 32-bit sequence number counter
- Sequence counter overflow flag: indicating whether to abort if the sequence number counter overflows
- Anti-replay window
- AH information
  - Algorithm, key, key life time
- ESP information
  - Algorithm, key, key life time
- Lifetime of SA
- IPSec mode: transport, tunnel
- Path MTU (Maximum Transmission Unit)
  - To avoid fragmentation

## Security Parameters Index (SPI)

- A 32-bit string used to index SA.
- Carried in AH and ESP headers to enable the receiving system to select the SA under which the packet will be processed.
- **SPI + Dest IP address + IPsec Protocol**
  - Uniquely identifies each SA in SA Database (SAD)
- Why need destination IP address, rather than source IP address?

## SA Database (SAD)

- Holds parameters for each SA
  - Sequence number counter
  - Lifetime of this SA
  - AH and ESP information
  - Tunnel or transport mode
- Every host or gateway participating in IPsec has their own SA database

## Security Policy Database (SPD)

- Decide
  - 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 their own SPD
- Index into SPD by **Selector** fields
  - Selectors: IP and upper-layer protocol field values.
  - Examples: Dest IP, Source IP, Transport Protocol, IPsec Protocol, Source & Dest Ports, ...

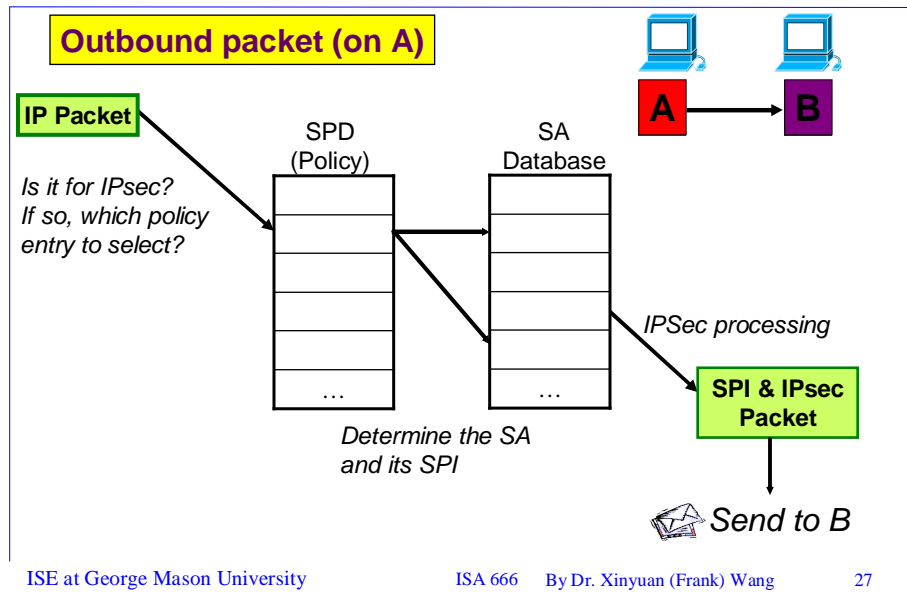
## SPD Entry Actions

- 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: security must have been applied

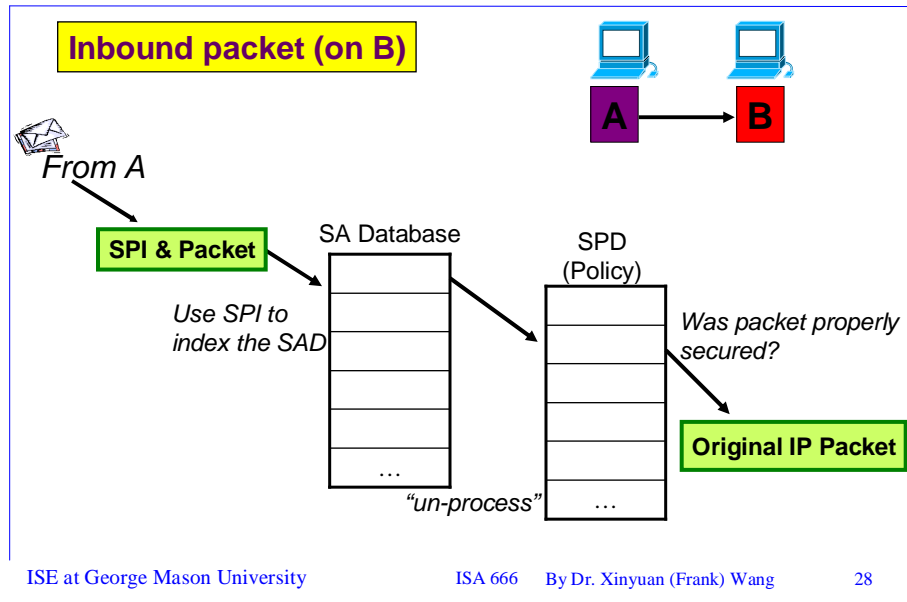
## SPD Protect Action

- If the SA does not exist...
  - Outbound processing
    - Trigger key management protocols to generate SA dynamically, or
    - Request manual specification, or
    - Other methods
  - Inbound processing
    - Drop packet

# Outbound Processing



# Inbound Processing



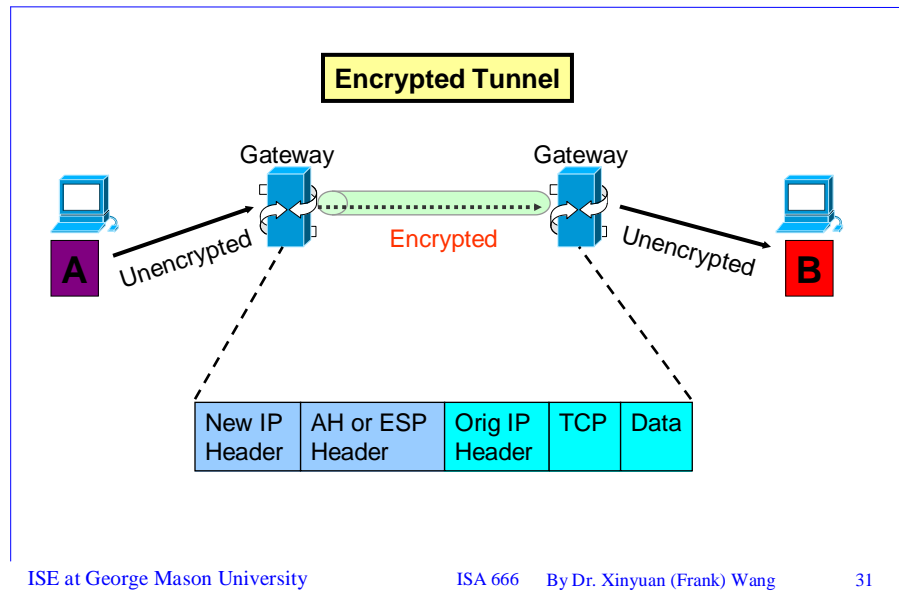
## Hosts & Gateways

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

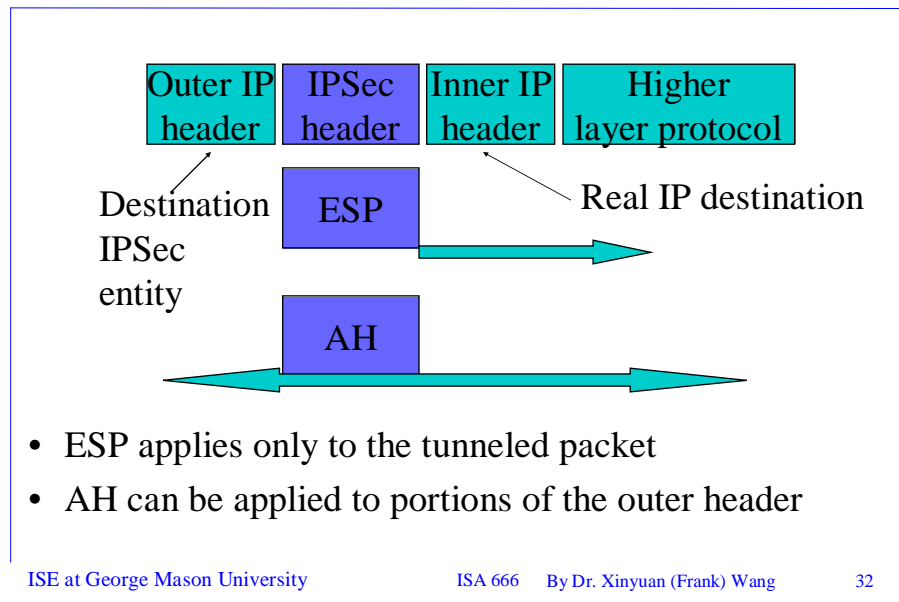
## IPSec Tunnel Mode

- Protection for entire IP datagram.
- Add another (outer) layer IP header
- Encapsulate the original IP packet into the outer layer IP packet
- The original IP packet is treated as payload of the new IP packet
- When encryption is used, the eavesdropper can not see anything about the original IP packet
  - Partial flow confidentiality
- When running between 2 gateways, security services by IPSec tunnel mode can be shared by multiple hosts
  - Hosts behind IPSec gateways do NOT need to support IPSec

## Tunnel Mode



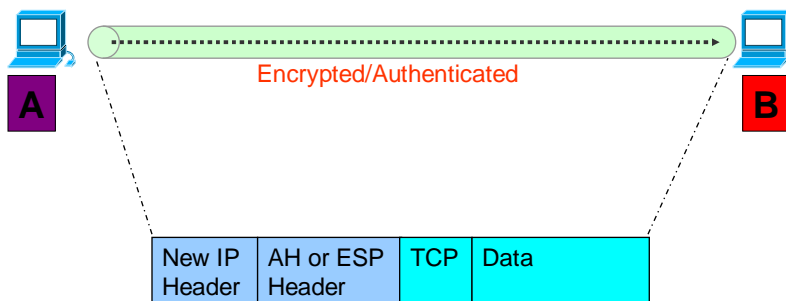
## Tunnel Mode (Cont'd)



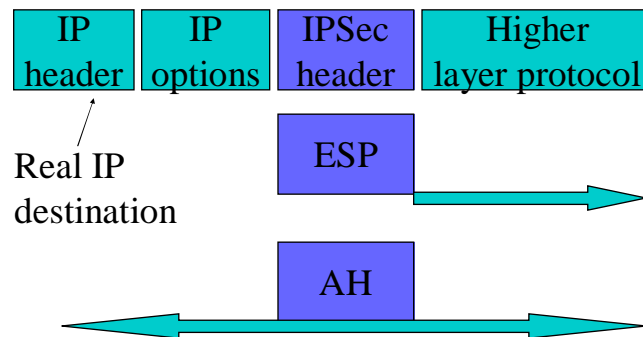
## IPSec Transport Mode

- Protection for upper-layer protocols
  - UDP, TCP, ICMP
- Protection covers IP datagram payload and some header fields
- IPSec transport mode only provide host-to-host (end-to-end) security:
  - IPSec processing performed at endpoints of secure channel.
  - So endpoint hosts must be IPSec-aware.
  - Can't be shared by other hosts

## Transport Mode



## Transport Mode (Cont'd)



- ESP protects higher layer payload only
- AH can protect IP headers as well as higher layer payload

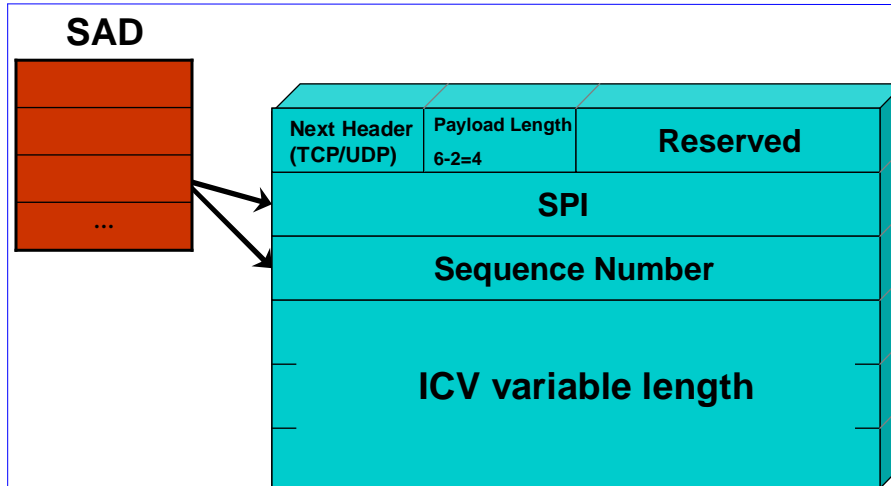
## Authentication Header (AH)

- Data integrity
  - Entire packet has not been tampered with
- Authentication
  - Can “trust” IP address source
  - Use MAC to authenticate
- Creates a stateful channel
  - Use sequence number
- Anti-replay feature
- Sequence number is authenticated
- Integrity check value

## Integrity Check Value - ICV

- Message authentication code (MAC) calculated over
  - IP header fields that do not change or are predictable
  - IP header fields that are unpredictable are set to zero.
  - IPsec AH header with the ICV field set to zero.
  - Upper-level data
- Code may be truncated to first 96 bits

## IPsec Authentication Header



## Encapsulated Security Protocol (ESP)

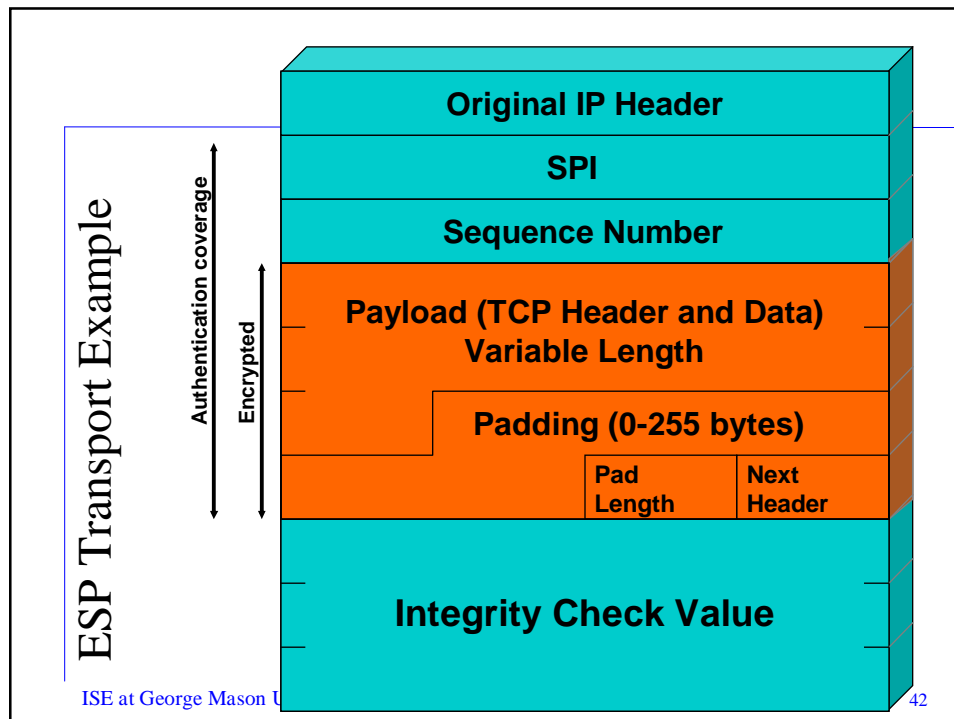
- Confidentiality for upper layer protocol
- Partial traffic flow confidentiality (Tunnel mode only)
- Data origin authentication and connectionless integrity (optional)
  - Authentication of payload
  - No authentication of (inner or outer) header fields
- Defines a header and trailing fields to be added to IP payload

## Outbound Packet Processing

- Form ESP payload
- Pad as necessary
- Encrypt result [payload, padding, pad length, next header]
- Apply authentication

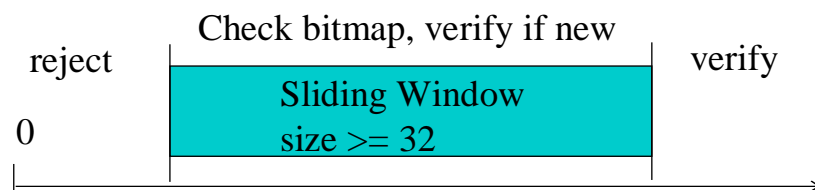
## Outbound Packet Processing...

- 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 except for authentication data field.
  - Implicit padding of '0's between next header and authentication data is used to satisfy block size requirement for ICV algorithm
  - *Not include the IP header.*



## 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 an SA
  - Duplicates are rejected!



## Anti-replay Feature

- Optional
- 32 bit sequence number for outgoing IPsec packets
  - Initialized to zero
  - Increment on packet by packet basis
  - Overflow results in auditable event and re-keying
  - Protected by MACs in AH and ESP
- Recipient uses “sliding windows” to track packet arrival
  - Recommended window length is 64.
  - Packets can be dropped if delayed too long (by network latency or deliberately).

## Anti-replay Sliding Window

- 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!

## ESP 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 (option)

## ESP Processing - Header Location...

- Transport mode IPv4 and IPv6

IPv4



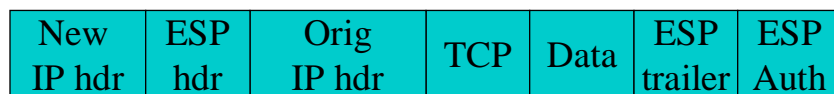
IPv6



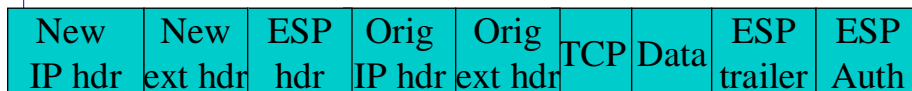
## ESP Processing - Header Location...

- Tunnel mode IPv4 and IPv6

IPv4



IPv6



## AH and ESP Algorithms

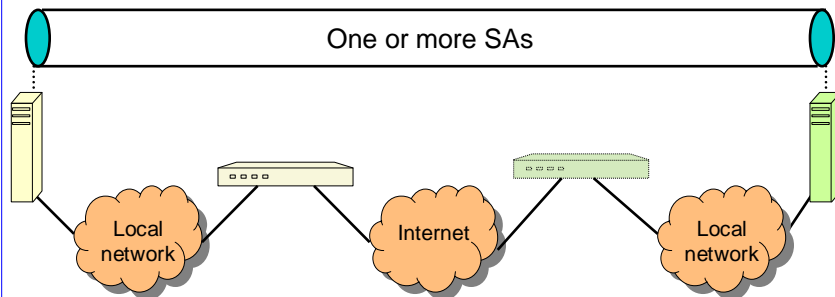
- IPSec supports the use of a number of algorithms for ESP and AH
- AH
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- ESP
  - DES, tripple DES
  - RC5
  - IDEA
  - Null
  - ...

## SA Bundle

- More than 1 SA can apply to a packet
- Example: ESP does not authenticate new IP header. How to authenticate?
  - Use SA to apply ESP w/out authentication to original packet
  - Use 2<sup>nd</sup> SA to apply AH

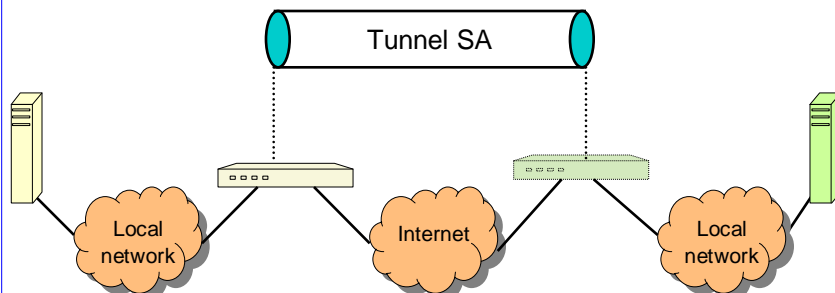
## Host to Host SA Combinations

- End-to-end application of IPSec between IPSec-aware hosts:
  - One or more SAs, one of the following combinations:
    - AH in transport
    - ESP in transport
    - AH followed by ESP, both transport
    - Any of the above, tunnelled inside AH or ESP.



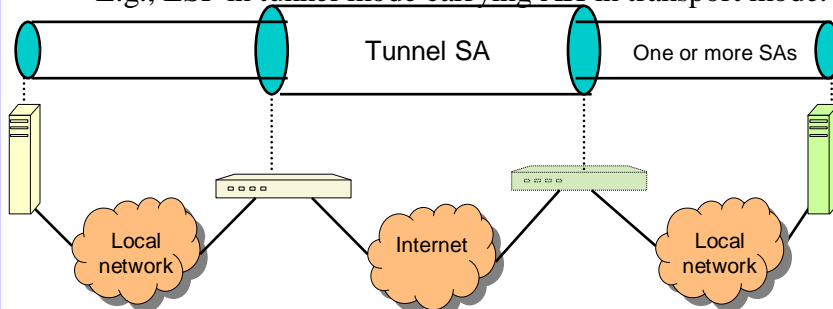
## Gateway to Gateway SA Combinations

- Gateway-to-gateway only:
  - No IPSec at hosts.
  - Simple Virtual Private Network (VPN).
  - Single tunnel SA supporting any of AH, ESP (conf only) or ESP (conf+auth).



## SA Combinations

- A combination of 1 and 2 above:
  - Gateway-to-gateway tunnel as in 2 carrying host-to-host traffic as in 1.
  - Gives additional, flexible security on local networks (between gateways and hosts)
  - E.g., ESP in tunnel mode carrying AH in transport mode.



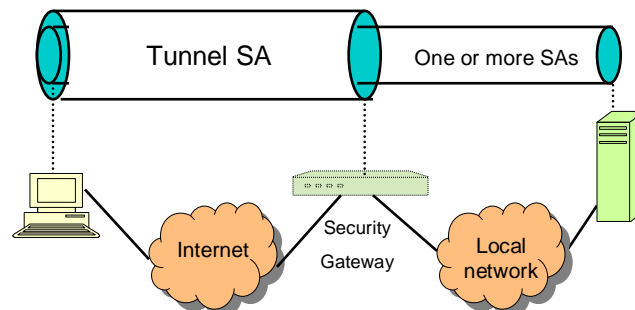
ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

53

## Another SA Combinations

- Remote host support:
  - Single gateway (typically firewall).
  - Remote host uses Internet to reach firewall, then gain access to server behind firewall.
  - Traffic protected in inner tunnel to server as in case 1 above.
  - Outer tunnel protects inner traffic over Internet.



ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

54

## IPSec Key Management

- IPSec is a heavy consumer of symmetric keys:
  - One key for each SA.
  - Different SAs for:  
    {ESP,AH} x {tunnel,transport} x {sender, receiver}.
- Where do these SAs and keys come from?
- Two sources:
  - Manual keying.
    - Fine for small number of nodes but hopeless for reasonably sized networks of IPSec-aware hosts; requires manual re-keying.
  - IKE: Internet Key Exchange, RFC 2409.
    - RFC documentation hard to follow.
    - IKE is a specific adaptation of more general protocols (“Oakley” and “ISAKMP”).
    - Protocols have many options and parameters.