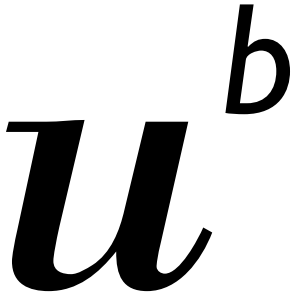


b

UNIVERSITÄT
BERN

UNIVERSITÄT
BERN

Network Security

VIII. IP Security

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 11.04.2022 – 25.04.2022

IP Security

Table of Contents

1. IPsec Overview

1. Architecture

”Security in the Internet Architecture” (RFC 1636)

- issued in 1994 by Internet Architecture Board
- Goals: to secure
  - network infrastructure from unauthorized monitoring and control of network traffic
  - end-user-to-end-user traffic using authentication and encryption
- Design for IPv6 and IPv4

IPsec specification now exists as a set of Internet standards.

UNIVERSITÄT BERN

1. IPsec Overview

2. Documents

- Architecture
  - general concepts, security requirements, definitions, and mechanisms defining IPsec technology, **RFC 4301**
- Authentication Header
  - is an extension header to provide message authentication, **RFC 4302**
  - Because message authentication is provided by ESP, use of AH is deprecated. It is included in IPsecv3 for backward compatibility but should not be used in new applications.
- Encapsulating Security Payload
  - consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication, **RFC 4303**
- Internet Key Exchange
  - collection of documents describing key management schemes, **RFC 7296**
- Cryptographic algorithms

  Documents to describe
  - cryptographic algorithms for encryption
  - message authentication
  - pseudorandom functions
  - cryptographic key exchange.
- Other
  - IPsec-related RFCs, dealing with security policy and Management Information Base content.

1. IPsec Overview

3. Applications

IPsec

- allows to secure communications over LANs, public WANs, Internet
- supports applications to encrypt and/or authenticate all traffic at IP level

Example applications

- Secure branch office connectivity over the Internet using virtual private networks
- Secure remote access over the Internet to ISPs or companies
- Establishing extranet and intranet connectivity with partners and organizations
- Enhancing electronic commerce security independent on application layer

1. IPsec Overview

4. Applications in IP Related Protocols

- Mobile IP
- Routing Protocols
- Address Resolution
- ICMP

1. IPsec Overview

5. Services

IPsec provides **security services** at IP layer by enabling a system to

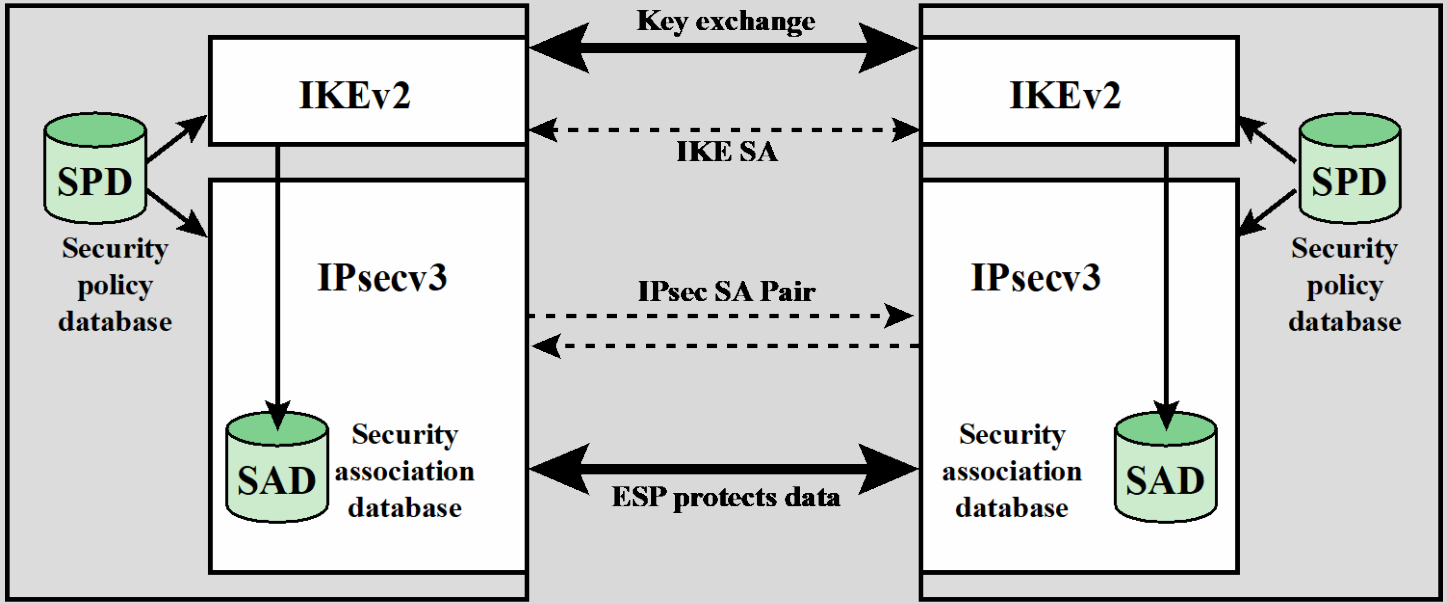
- select required security protocols
- determine algorithms for the services
- put in place any cryptographic keys required to provide the requested services

RFC 4301 services

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

2. IPsec Policy

1. IPsec Architecture



UNIVERSITÄT BERN

2. IPsec Policy

2. Security Association

one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.

Identification Parameters

- Security Parameter Index
  - 32-bit unsigned integer assigned to this SA and having local significance only
  - carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- IP Destination Address
  - Address of SA's destination endpoint
  - may be an end-user system or a network system such as a firewall or router.
- Security Protocol Identifier
  - This field from the outer IP header indicates whether the association is an AH or ESP security association.

2. IPsec Policy

3. Security Association Database

- defines the parameters associated with each SA
- SA is defined by several parameters in an SAD entry.

Parameters

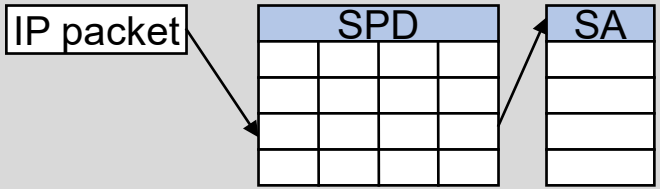
- Security parameter index
- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- AH information (algorithms, key, key lifetime)
- ESP information
- SA Lifetime
- IPsec protocol mode
- Path MTU

UNIVERSITÄT BERN

2. IPsec Policy

4. Security Policy Database

- means by which IP traffic is related to specific SAs
- Each SPD entry
  - is defined by a set of IP and upper-layer protocol field values called selectors.
  - These are used to filter outgoing traffic in order to map it into a particular SA for outbound processing
- in more complex environments:
  - multiple SPD entries relate to a single SA or
  - multiple SAs are associated with a single SPD entry



2. IPsec Policy

5. Selectors Determining an SPD Entry

- Remote IP Address
  - single IP address, enumerated list or range of addresses, or wildcard (mask) address.
  - The latter two are required to support more than one destination system sharing the same SA, e.g., behind a firewall
- Local IP Address
  - single IP address, enumerated list or range of addresses, or wildcard (mask) address.
- Next Layer Protocol
  - IPv4 Protocol or IPv6 Next Header designates the protocol operating over IP.
  - If AH or ESP is used, then this IP protocol header immediately precedes the AH or ESP header in the packet.
- Name
  - a user identifier from the operating system
  - not a field in the IP or upper-layer headers, but available if IPsec is running on the same OS as the user.
- Local and Remote Ports
  - individual TCP or UDP port values,
  - an enumerated list of ports, or
  - wildcard port.

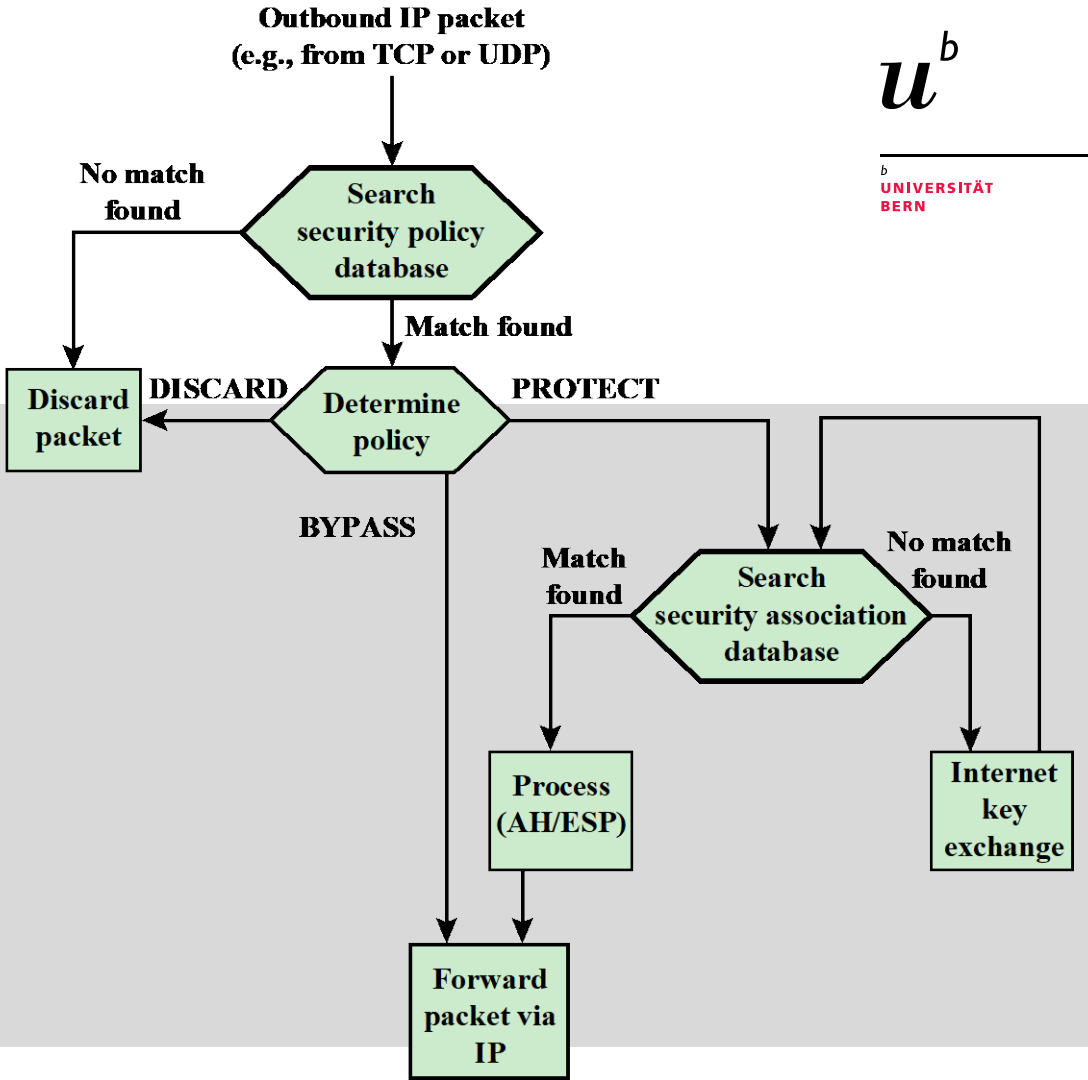
2. IPsec Policy

6. SPD Example

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

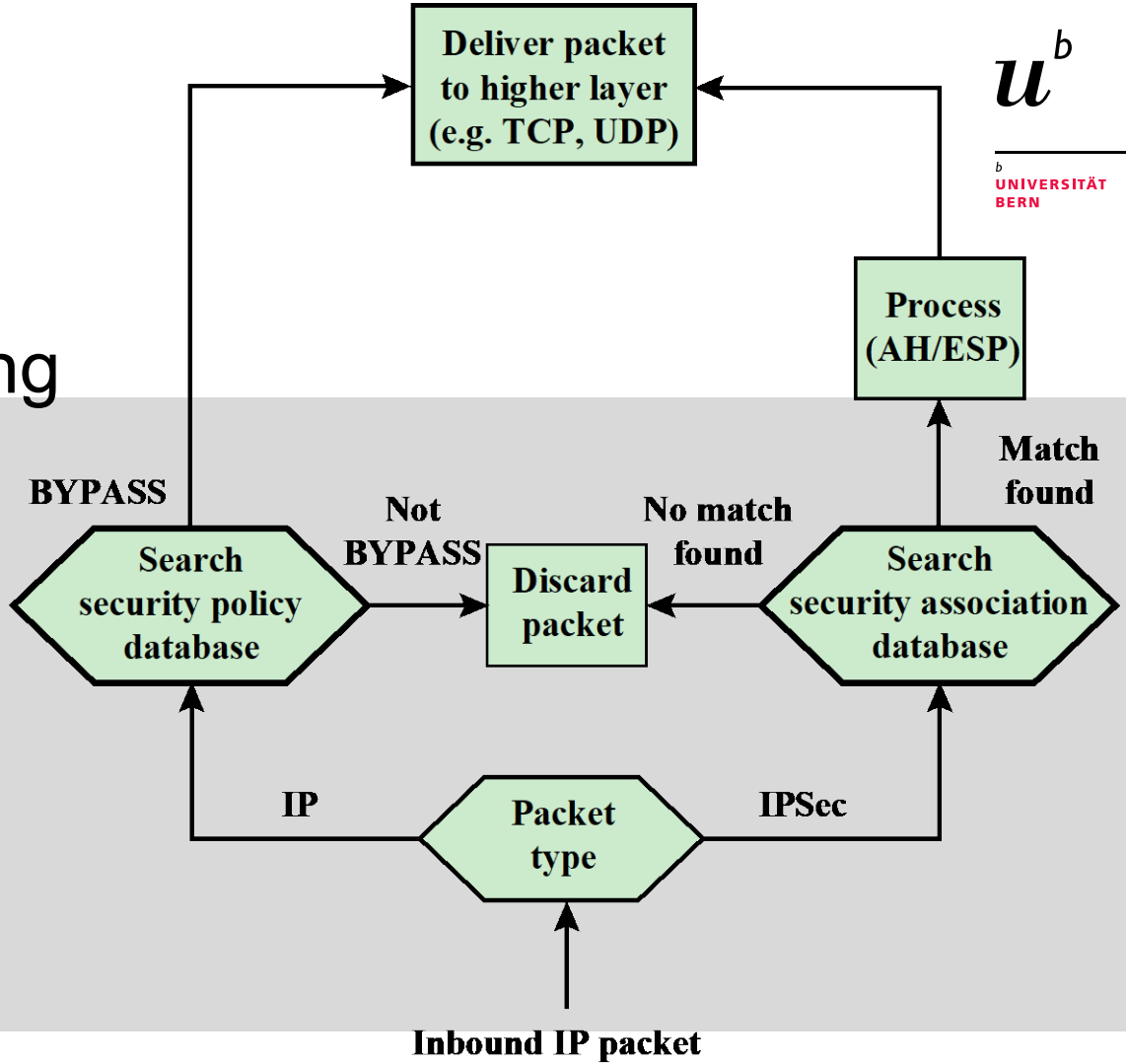
2. IPsec Policy

7. Outbound IP Traffic Processing



2. IPsec Policy

8. Inbound IP Traffic Processing

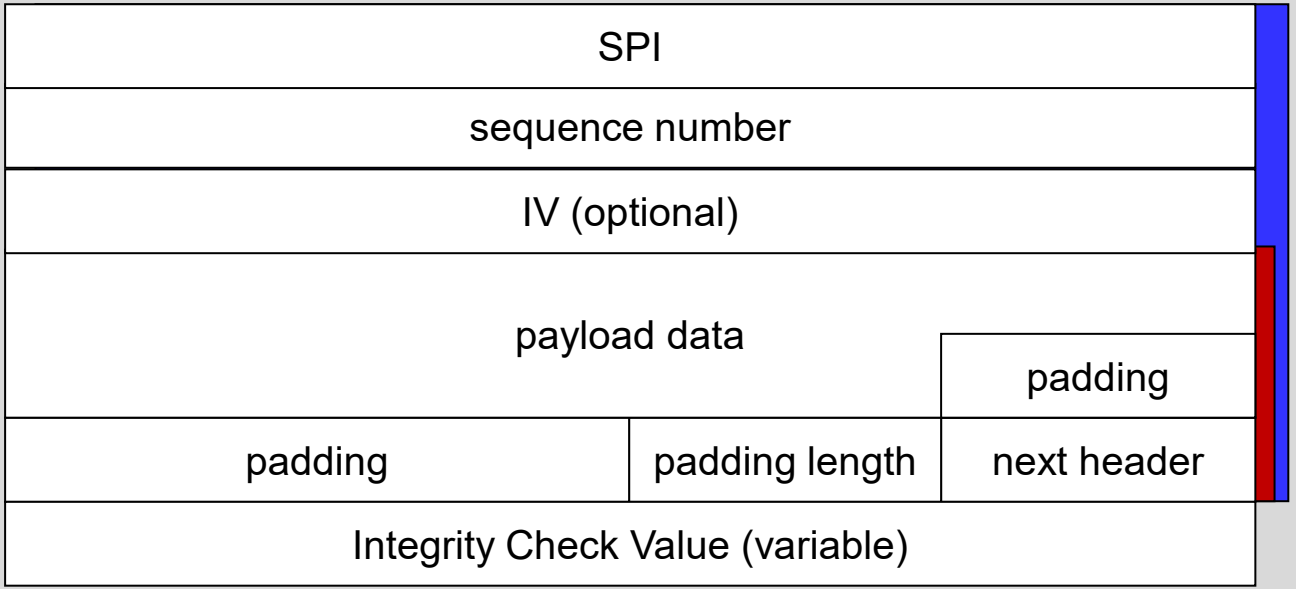


UNIVERSITÄT BERN

3. Encapsulation Security Payload

1. Packet Format

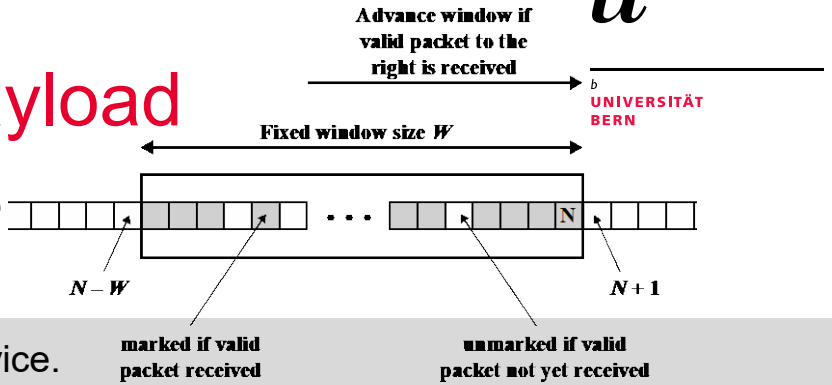
- Optional Initialization Vector at beginning of payload data
- Padding to
  - achieve certain block length
  - align padding length and next header
  - conceal packet length



encryption / authentication

3. Encapsulation Security Payload

2. Anti Replay Attack Service

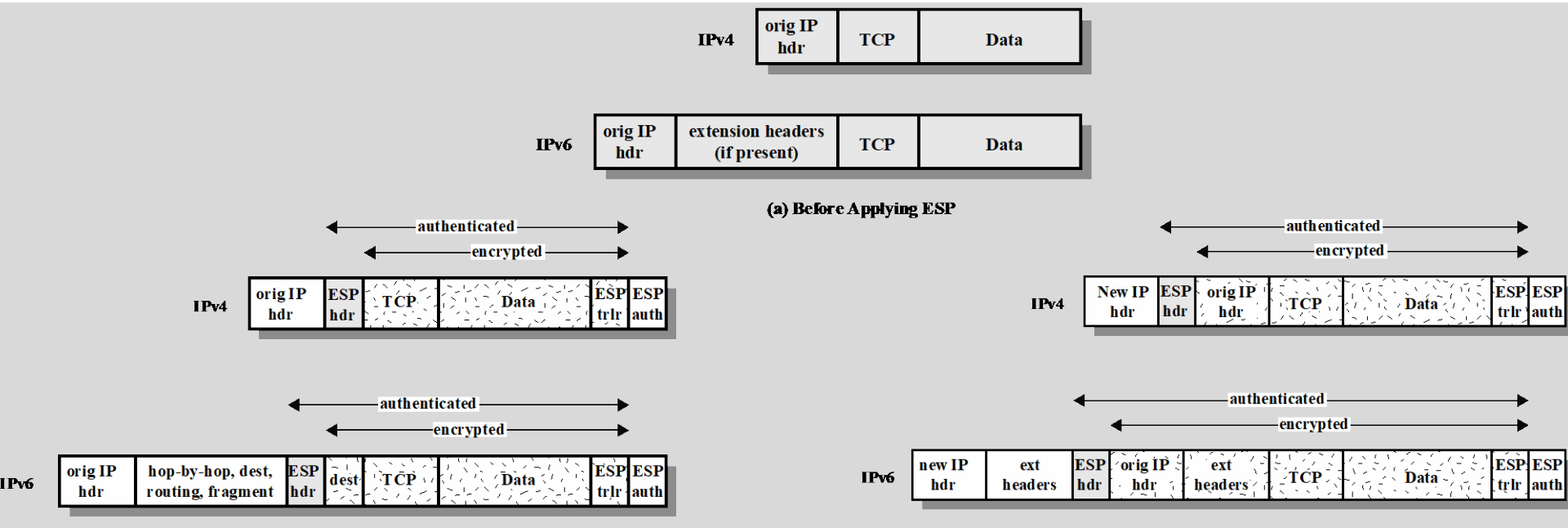


- Receipt of duplicate, authenticated IP packets may harm service.
- Sequence Number field is designed to thwart such attacks.
  - When a new SA is established, the sender initializes a sequence number counter to 0.
  - For each packet on an SA, the sender increments the counter and places the value in the Sequence Number field.
  - If the limit of 2^{32}-1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.
- Receiver implements a window of size W, default W = 64. The right edge of the window represents the highest sequence number, N, so far received for a valid packet.
- For any properly authenticated packet with a sequence number in (N-W+1 … N) processing is as follows:
  1. If the received packet falls within the window and is new, the MAC is checked. If packet is authenticated, the corresponding slot in the window is marked.
  2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
  3. If the received packet is to the left of the window or if authentication fails, it is discarded.

UNIVERSITÄT BERN

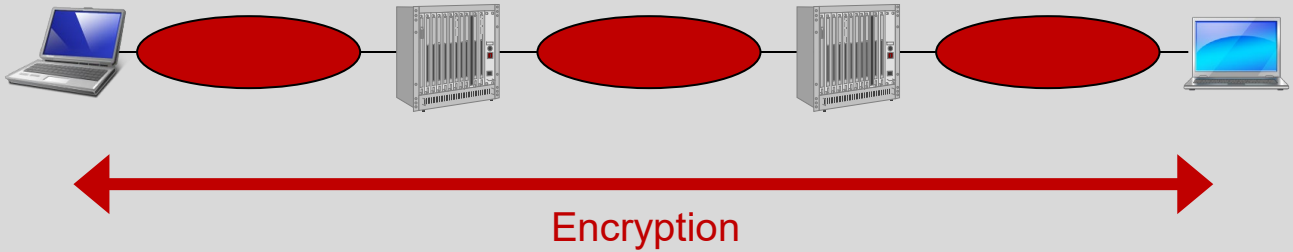
3. Encapsulation Security Payload

3. Transport and Tunnel Mode



3. Encapsulation Security Payload

4.1 End-to-End IPsec Transport Mode



3. Encapsulation Security Payload

4.2 Transport Mode Operation

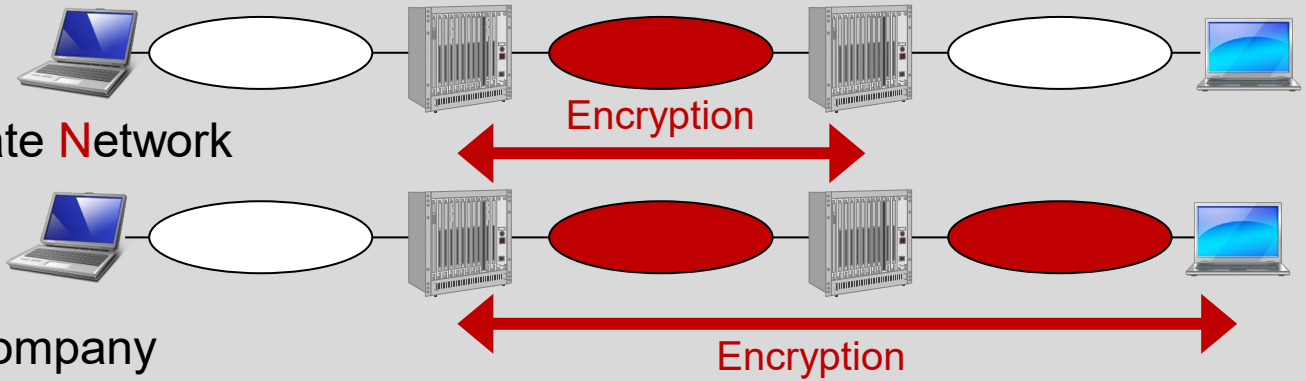
- Source
  - Block of data consisting of ESP trailer + entire transport-layer segment is encrypted.
  - Plaintext of block is replaced by its ciphertext to form IP packet for transmission.
  - Authentication is added, if this option is selected.
- Routing
  - Packet is routed to destination.
  - Each intermediate router needs to process IP header + any plaintext IP extension header, but does not need to examine ciphertext.
- Destination node
  - processes IP header + any plaintext IP extension headers.
  - decrypts the remainder of the packet to recover the plaintext transport-layer segment based on the SPI in the ESP header.

UNIVERSITÄT BERN

3. Encapsulation Security Payload

5.1 Tunnel Mode

- Security gateway to security gateway
  - Example: Virtual Private Network
- End system to security gateway
  - Example: access to company / university network



3. Encapsulation Security Payload

5.2 Tunnel Mode

- After the AH or ESP fields are added to IP packet, the entire packet + security fields are treated as payload of new outer IP packet with new outer IP header.
- Entire original (inner) packet travels through a tunnel from one point of an IP network to another.
  No routers along the way can examine the inner IP header.
- Because original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to security.
- Tunnel mode is used when one or both ends of a SA are a security gateway, such as a firewall or router implementing IPsec.
- With tunnel mode, several hosts on networks behind firewalls may engage in secure communications without implementing IPsec.
  Unprotected packets generated by such hosts are tunneled through external networks by tunnel mode SAs set up by IPsec software in the firewall or secure router at the boundary of the local network.

3. Encapsulation Security Payload

5.3 Tunnel Mode

- Tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway that protects a trusted network from external networks.
- Encryption occurs only between external host and security gateway or between two security gateways.
  - This relieves hosts on the internal network of the processing burden of encryption and simplifies key distribution task by reducing the number of needed keys
  - It thwarts traffic analysis based on ultimate destination.

3. Encapsulation Security Payload

6. Virtual Private Network

- Tunnel mode can be used to implement a secure VPN, i.e., a private network configured within a public network.
- Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN.

VPNs are used to

- create wide area networks that span large geographic areas.
- provide site-to-site connections to branch offices.
- allow mobile users to dial up their company LANs.

4. Authentication Header

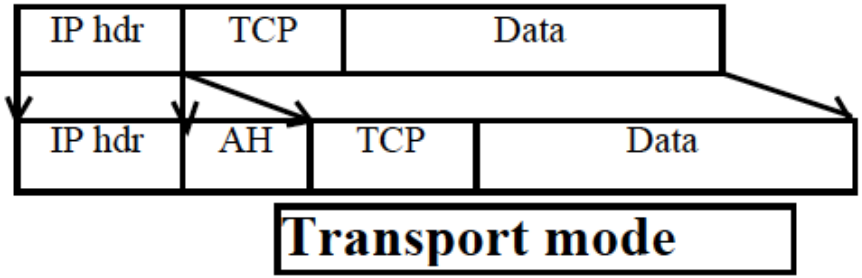
1. Packet Format

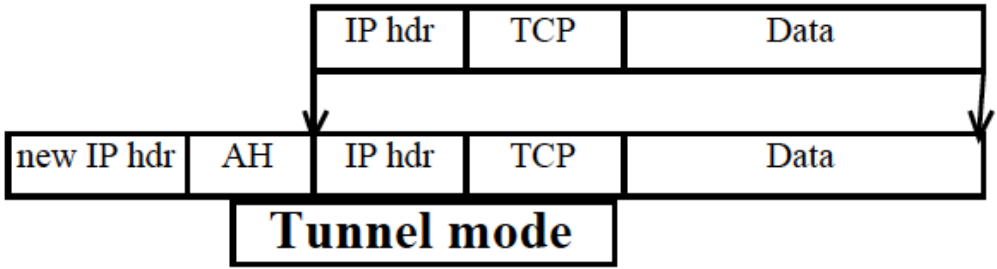
- Authentication of all IP header fields that can not change on the path between sender and receiver.
- Default algorithm: keyed MD5 calculates 128-bit authentication data over
  - Immutable IP header fields
  - AH header except authentication data
  - Higher protocols and data
  - Secret key

next header	payload length	reserved
SPI		
sequence number		
authentication data (n · 32 bit)		

4. Authentication Header

2. Transport and Tunnel Mode





UNIVERSITÄT BERN

4. Authentication Header

3. AH vs ESP Authentication

- AH protects IP header, ESP protects anything beyond IP header.
- There may be export issues with ESP.
- With ESP, routers and firewalls can not look on anything beyond layer 3 (IP layer) header.

4. Authentication Header

4. Tunnel and Transport Mode Functionality

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

5. Combining Security Associations

1. Transport Adjacency and Iterated Tunneling

Transport Adjacency

– Applying more than one SA to the same IP packet without tunneling

Iterated Tunneling

– Application of multiple layers of security protocols effected through IP tunneling.

– allows for multiple levels of nesting

UNIVERSITÄT BERN

5. Combining Security Associations

2.1 Authentication and Confidentiality: ESP with Authentication Option

- User first applies ESP to the data to be protected and then appends authentication data field.
- Authentication applies to ciphertext rather than plaintext.

Subcases

- Transport mode ESP
  - Authentication and encryption apply to IP payload, but IP header is not protected.
- Tunnel mode ESP
  - Authentication applies to entire IP packet delivered to the outer IP destination address (e.g., a firewall). Authentication is performed at destination.
  - Entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination.

5. Combining Security Associations

2.2 Authentication and Confidentiality: Transport Adjacency

- Two bundled transport SAs
  - inner SA: ESP SA (without authentication option), i.e., transport SA → encryption is applied to IP payload.
  - outer SA: AH SA.
- Resulting packet: IP header followed by ESP
- AH is then applied in transport mode, so that authentication covers the ESP plus the original IP header except for mutable fields.

- Advantage
  - Authentication covers more fields, incl. source / destination IP addresses.
- Disadvantage
  - Overhead of two SAs vs. one SA

5. Combining Security Associations

2.3 Authentication and Confidentiality: Transport-Tunnel Bundle

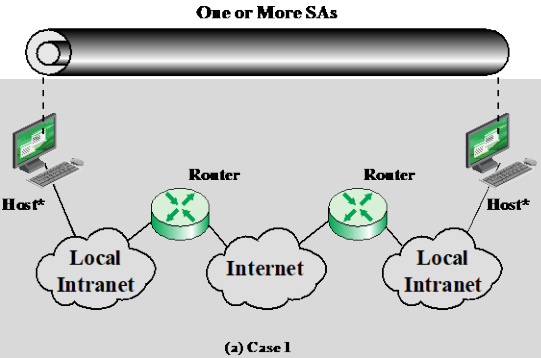
Use of authentication prior to encryption might be preferable for several reasons.

1. Because authentication data are protected by encryption, it is impossible for anyone to intercept the message and alter the authentication data without detection.
2. It may be desirable to store the authentication information with the message at the destination for later reference. It is more convenient to do this if the authentication information applies to the unencrypted message; otherwise, the message would have to be re-encrypted to verify the authentication information.

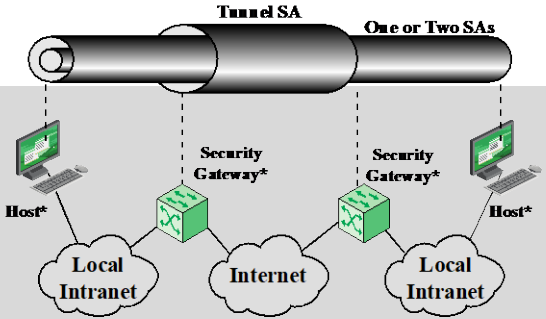
- Applying authentication before encryption between two hosts is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA.
- Authentication is applied to the IP payload plus the IP header (and extensions) except for mutable fields.
- The resulting IP packet is then processed in tunnel mode by ESP; the result is that the entire, authenticated inner packet is encrypted and a new outer IP header (and extensions) is added.

5. Combining Security Associations

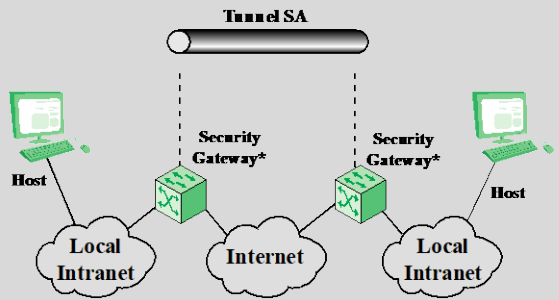
3. Basic Combinations of Security Associations



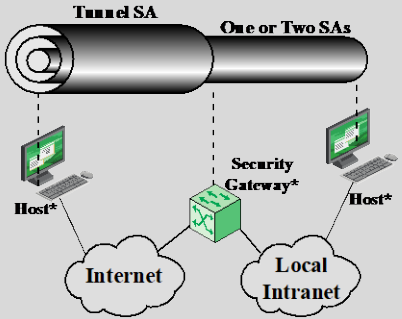
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

1. All security provided between IPsec end systems, possible combinations:
   a) AH in transport mode
   b) ESP in transport mode
   c) ESP followed by AH in transport mode
   d) a, b, c inside AH or ESP in tunnel mode
2. Security between gateways
3. 2.) plus end-to-end security
4. Support for a remote host to reach servers behind firewall

6. Internet Key Exchange

1. Key Management Types

- determination and distribution of secret keys.
- Typical requirement: 4 keys for communication between 2 applications
  - transmit and receive pairs for both integrity and confidentiality

Key Management Types

- Manual
  - A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
  - practical for small and relatively static environments
- Automated
  - Automated system enables on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with evolving configuration.

6. Internet Key Exchange

2. Key Determination Protocol

Refinement of Diffie-Hellman key exchange
retaining DH advantages and counter its disadvantages.

- **Advantages**
  - Secret keys generated when needed
  - Exchange does not require pre-existing infrastructure.
- **Disadvantages**
  - Does not provide any information about identities of parties
  - Subject to man-in-the-middle attack
  - Computationally expensive

6. Internet Key Exchange

3. Clogging Attack

- An opponent forges the source address of a legitimate user and sends a public DH key to victim.
- Victim then computes secret key.
- Repeated messages of this type can clog the victim's system with useless work.

6. Internet Key Exchange

4. IKE Key Determination

- uses cookies to thwart clogging attacks.
- enables the two parties to negotiate a *group* to specify the global parameters of the Diffie-Hellman key exchange.
- uses nonces against replay attacks.
- enables the exchange of DH public key values.
- authenticates DH exchange to thwart man-in-the-middle attacks

6. Internet Key Exchange

5.1 Cookie Exchange

1. Cookie exchange requires that each side sends a pseudorandom number (cookie) in the initial message.
2. The other side acknowledges initial message.
3. Acknowledgment must be repeated in the first message of DH key exchange.

- If the source address was forged, the opponent gets no answer.
- Thus, an opponent can only force a user to generate acknowledgments and not to perform the DH calculation

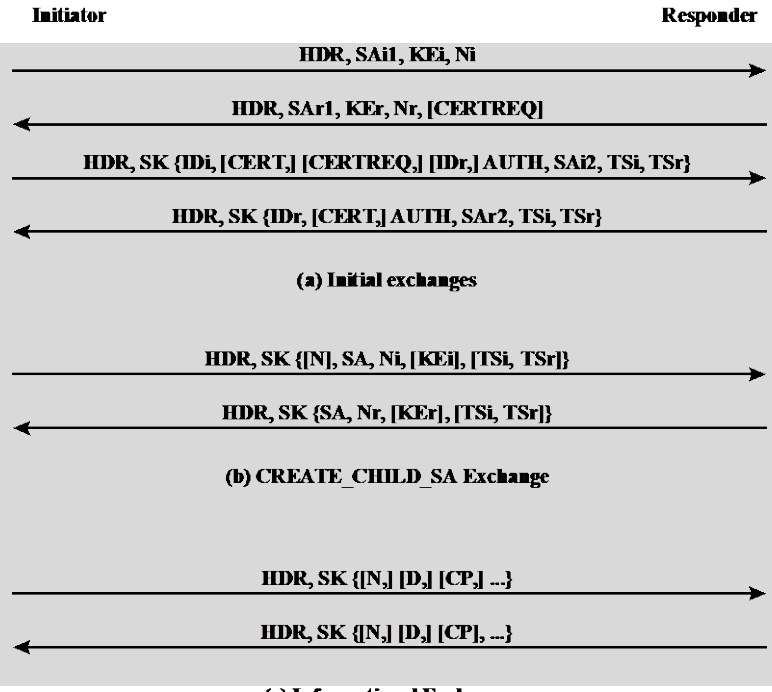
6. Internet Key Exchange

5.2 Cookie Generation

- Requirements
  1. Cookie must depend on the specific parties. This prevents an attacker from obtaining a cookie using a real IP address and UDP port and then using it to swamp the victim with requests from randomly chosen IP addresses or ports.
  2. It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity. This implies that the issuing entity will use local secret information in the generation and subsequent verification of a cookie.
     It must not be possible to deduce this secret information from any particular cookie.
  3. Cookie generation and verification methods must be fast to thwart attacks intended to sabotage processor resources.
- Recommended method
  - Perform fast hash, e.g., MD5, over source and destination IP address, source and destination UDP ports, and a locally generated secret value

6. Internet Key Exchange

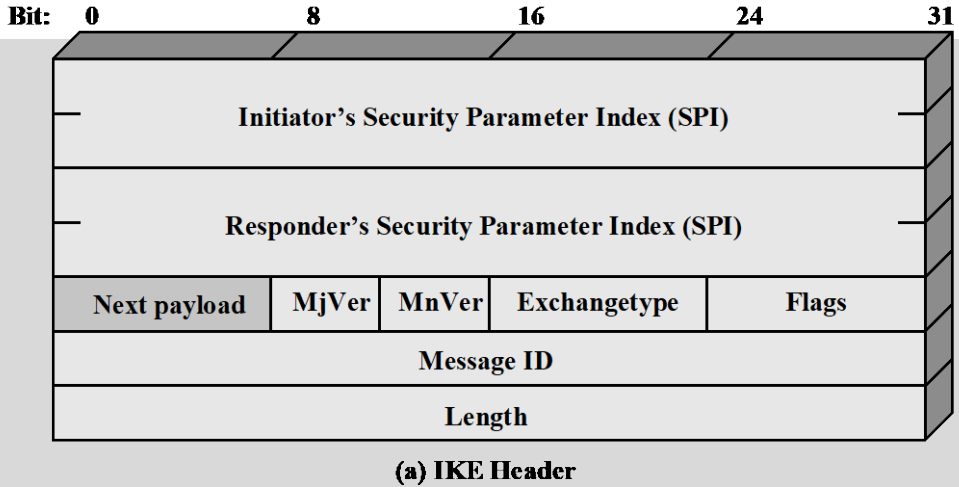
6. IKEv2 Exchanges



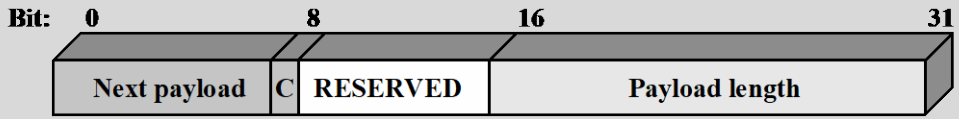
- Initial Exchange
  1. Parties exchange information concerning cryptographic algorithms and other security parameters along with nonces and DH values. Result: IKE SA, which defines parameters for a secure channel over which subsequent message exchanges take place. All subsequent IKE message exchanges are protected by encryption and message authentication.
  2. Parties authenticate each other and set up a first IPsec SA to be placed in the SAD and used for protecting ordinary (i.e., non-IKE) communication.
- CREATE_CHILD_SA Exchange
  - to establish further SAs for protecting traffic
- Informational Exchange
  - to exchange management information

6. Internet Key Exchange

7. Formats



(a) IKE Header



(b) Generic Payload Header

6. Internet Key Exchange

8. Payload Types

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message

Thanks a lot

for your Attentation

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 11.04.2022 – 25.04.2022