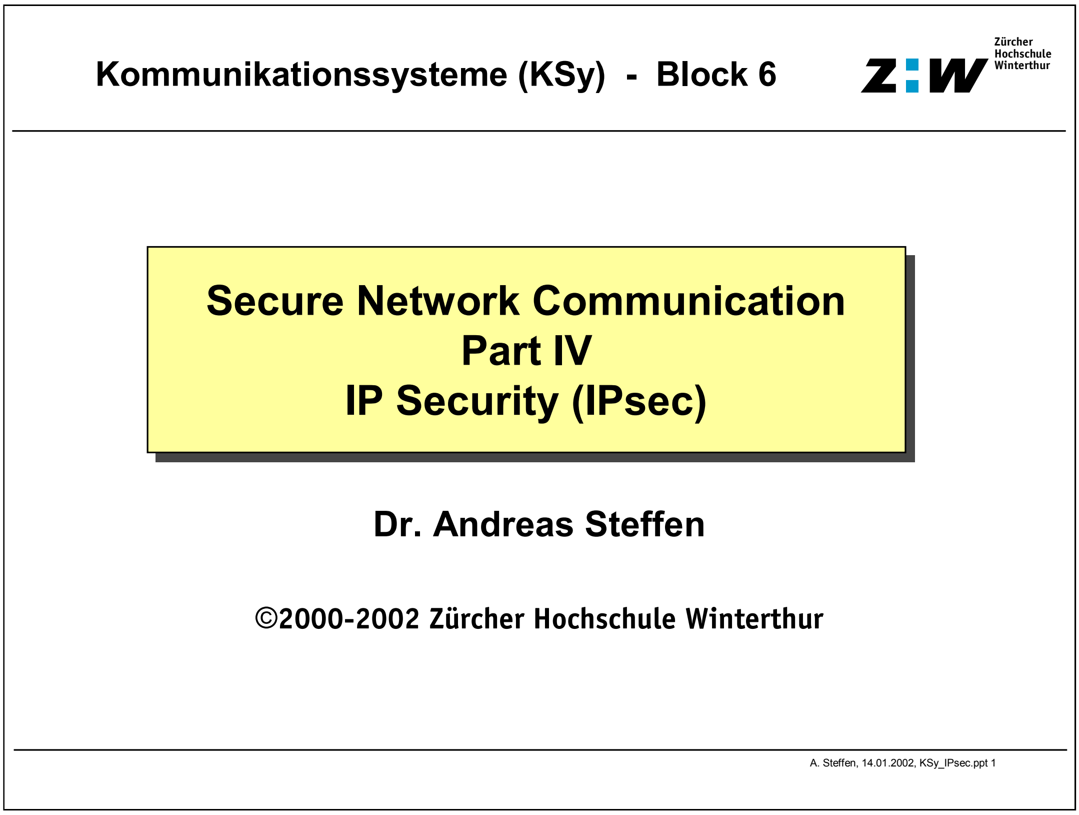


Secure Network Communication Part IV IP Security (IPsec)

Dr. Andreas Steffen

IPsec Transport Mode

- Authentication Header (AH)
- Encapsulated Security Payload (ESP)

IPsec Tunnel Mode

- Virtual Private Networks (VPN)
- Internet tunnel
- Security Gateway (SG)
- Encapsulated Security Payload (ESP)

Internet Key Exchange Protocol (IKE)

- Security Association (SA)
- Security Parameters Index (SPI)
- IKE phase 1 - main mode
- Diffie-Hellman key-exchange algorithm
- Perfect Forward Secrecy

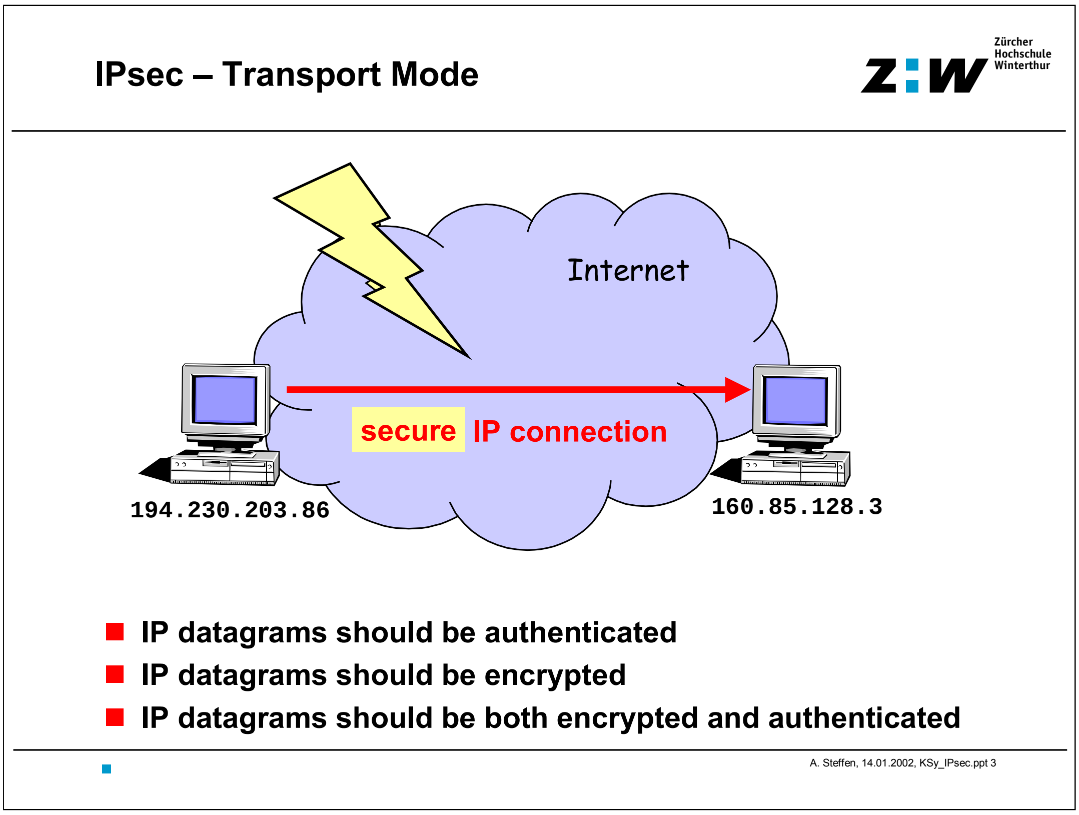
Relevant RFCs

- RFC 2402, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2412

Low-Cost VPN Products based on IPsec

- Windows 2000/XP, SSH Sentinel, SafeNet/Soft-Remote, PGPnet, FreeS/WAN

IPsec Transport Mode



IPsec – Transport Mode

- IP datagrams should be authenticated
- IP datagrams should be encrypted
- IP datagrams should be both encrypted and authenticated

Authenticity of IP connections

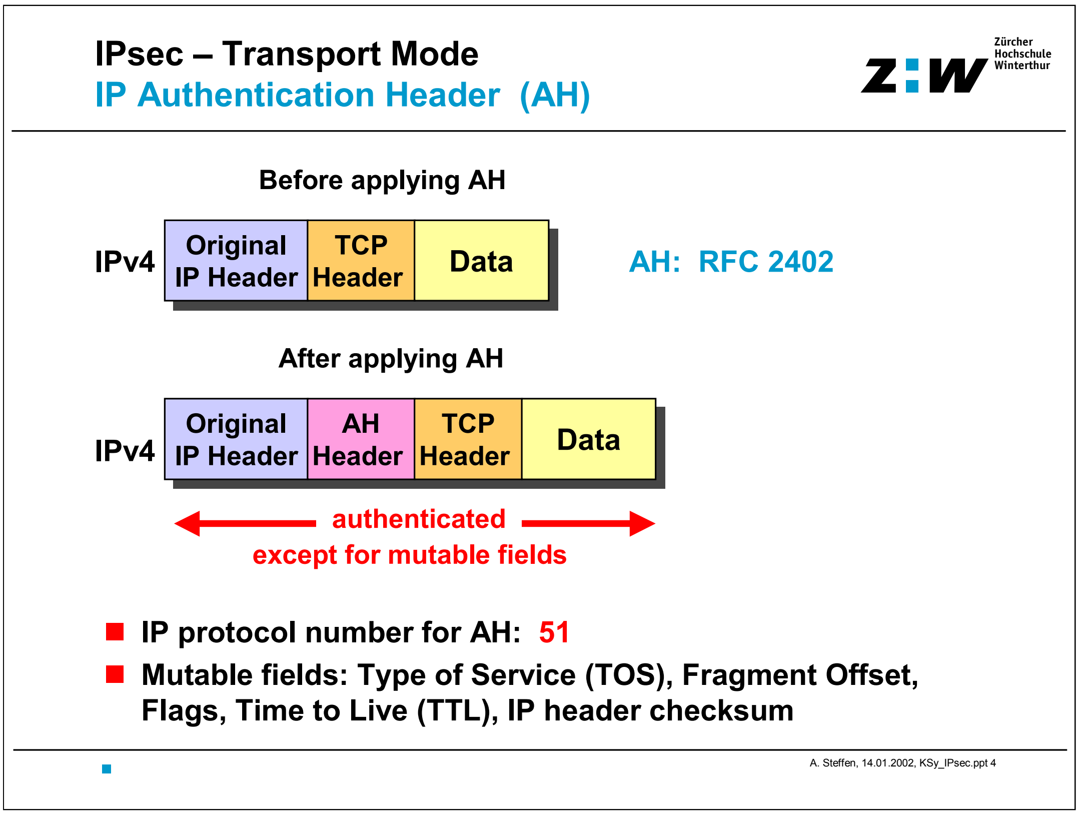
- In order to prevent IP spoofing and connection hijacking, as well as to secure the content of IP datagrams against any unauthorized modifications, all IP datagrams sent over the Internet should be authenticated.

Privacy of IP connections

- In order to guarantee privacy, all IP datagrams sent over the Internet should be encrypted by employing strong cryptography.

Encryption and Authentication

- It is desirable to have both encryption and authentication applied to IP datagrams.



IPsec – Transport Mode
IP Authentication Header (AH)

Zürcher Hochschule Winterthur

Before applying AH

IPv4	Original IP Header	TCP Header	Data

AH: RFC 2402

After applying AH

IPv4	Original IP Header	AH Header	TCP Header	Data

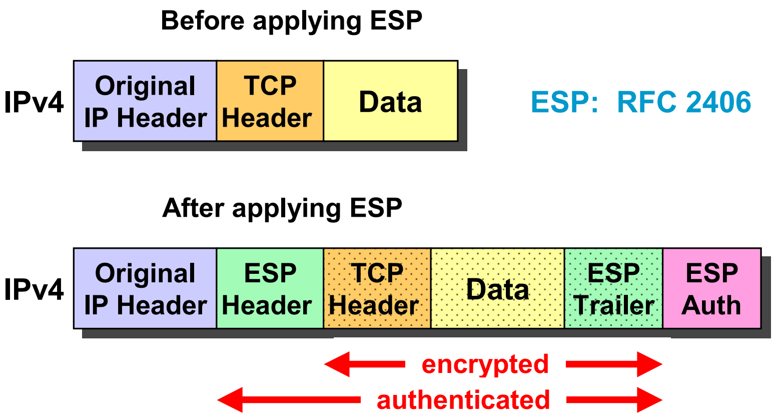
- IP protocol number for AH: 51
- Mutable fields: Type of Service (TOS), Fragment Offset, Flags, Time to Live (TTL), IP header checksum

IP Authentication Header (AH)

- The IPsec AH Protocol is specified in RFC 2402.
- AH protects both IP header and IP payload against modifications by computing a **keyed message authentication code** (**MAC**) over most octets of the IP datagram.
- Excluded from the cryptographic checksum are the following mutable header fields:
  - Type of Service (TOS)
  - Fragment Offset (always zero since AH is applied to non-fragmented packets, only)
  - Flags
  - Time to Live (TTL)
  - IP header checksum

  The above header fields could possibly get modified by intermediate routers **en-route** from source to destination.
- The secured checksum is transmitted in the AH header, together with an arbitrary 32 bit Secure Parameters Index (SPI) uniquely identifying the Security Association and a 32 bit Sequence Number preventing replay attacks.
- The AH header has the structure of an IPv6 extension header but can also be carried over IPv4.
- Not only TCP and UDP but any transport layer protocol can be protected by AH. The **Protocol field** in the original IP header is set to the decimal value **51**, designating the AH protocol and the **Next Header field** in the AH header carries the original protocol number(e.g. 1 for ICMP, 6 for TCP, 17 for UDP), identifying the transport layer payload carried in the IP datagram.

IPsec – Transport Mode
IP Encapsulated Security Payload (ESP)



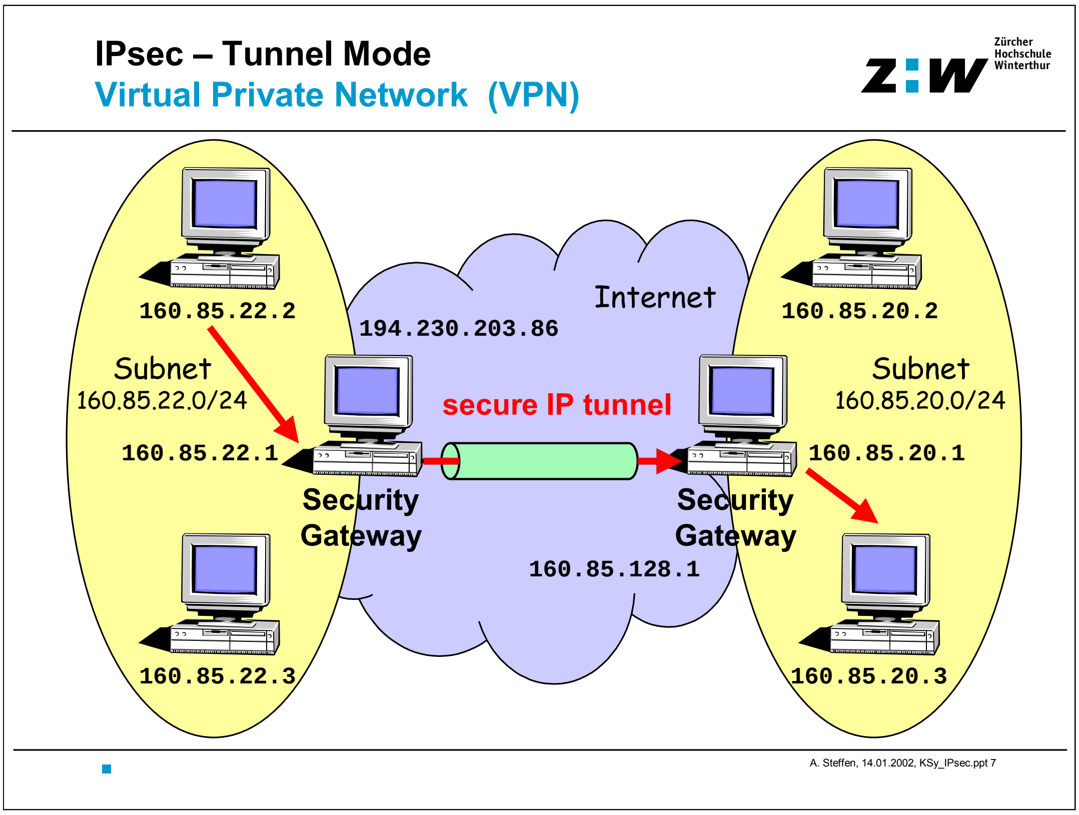
ESP: RFC 2406

- IP protocol number for ESP: 50
- ESP authentication is optional
- With ESP authentication the IP header is not protected.

IP Encapsulated Security Payload (ESP)

- The IPsec ESP Protocol is specified in RFC 2406.
- ESP encrypts the transport payload of the IP datagram using a strong symmetric encryption algorithm (IDEA, 3DES, AES, etc.).
- An ESP trailer is appended prior to encryption in order to align the payload data to a 4-byte boundary required by the ESP packet format. It may also be used to adapt the plaintext size to the block size of the block cipher (e.g. 64 bits for 3DES).
- Since IP packets could get lost, the encrypted payload is usually preceded by an initialization vector (IV) that is used by the receiver to initialize the block cipher algorithm used for the decryption of each IP payload.
- The ESP header has the structure of an IPv6 extension header but can also be carried over IPv4. Similar to the AH header it contains a 32 bit Secure Parameters Index (SPI) and a 32 bit Sequence Number.
- Any transport layer protocol can be encapsulated by ESP. The **Protocol field** in the original IP header is set to the decimal value **50**, designating the ESP protocol and the **Next Header field** in the ESP header carries the original protocol number identifying the transport layer protocol carried in the encrypted IP payload.
- Optionally the ESP payload can be authenticated by computing a keyed message digest over the body of the IP datagram and appending the MAC value as authentication data at the end of the encrypted payload. The IP header is not included in the checksum and therefore is not protected.
- In the case of an IPsec transport mode application where besides encryption also the protection of the IP header is required, the ESP and AH protocols can be cascaded by first encrypting the original IP payload using ESP and then authenticating both the original IP header and the ESP payload using AH.

IPsec Tunnel Mode
Virtual Private Networks



IPsec – Tunnel Mode

Virtual Private Network (VPN)

A. Steffen, 14.01.2002, KSy_IPsec.ppt 7

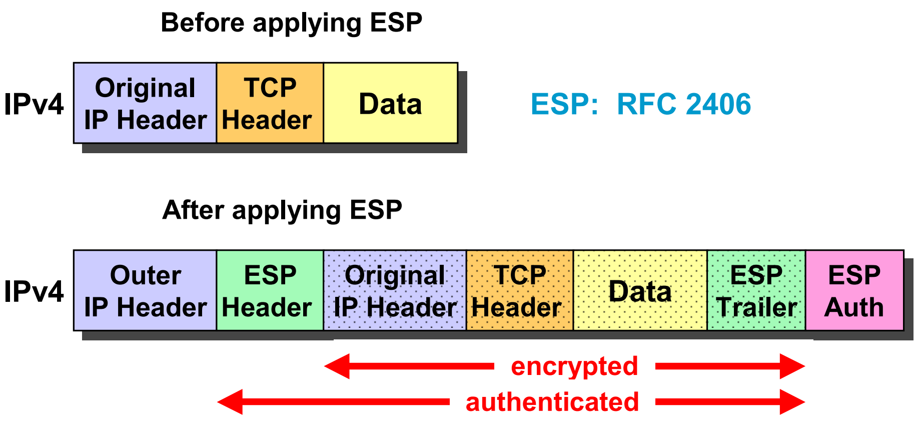
Virtual Private Networks

- A Virtual Private Network (VPN) can be used by an enterprise to connect its subnets or individual hosts located at various sites over shared public or semi-public communication channels. Compared to dedicated leased lines a VPN solution can offer significant cost savings without incurring any compromises regarding security requirements.
- VPNs can be realised using the **Layer 2 Tunneling Protocol** (**L2TP**) defined by the IETF or the now obsolete **Point-to-Point Tunneling Protocol** (**PPTP**).
  Layer 2 tunnels are often transported over IP based networks using UDP as a transport medium but emulating a link layer dial-in line from source to destination.
- An elegant and increasingly popular VPN solution is based on layer 3 mechanisms using secure IP tunnels based on the IPsec protocol suite.

IPsec Tunnels

- Two enterprise subnets can be securely connected with each other over the public Internet using an encrypted and authenticated IPsec tunnel. IP packets from a host on the local subnet to a host on the remote subnet are forwarded to the local **Security Gateway** (SG) which in turn tunnels the IP packets to the Security Gateway on the remote end of the IPsec tunnel where they are delivered to the destination host.
  The hosts belonging to the subnets are not aware of any security mechanisms. For them the Security Gateways have the function of simple routers.
- The encapsulation provided by the IPsec tunnels allows the use of private network addresses (e.g. 10.0.1.0/24 in one subnet and 10.0.2.0/24 in the second subnet) which are normally not routable over the Internet.

IPsec – Tunnel Mode
IP Encapsulated Security Payload (ESP)



Before applying ESP

IPv4 | Original IP Header | TCP Header | Data

ESP: RFC 2406

After applying ESP

IPv4 | Outer IP Header | ESP Header | Original IP Header | TCP Header | Data | ESP Trailer | ESP Auth

encrypted

authenticated

- IP protocol number for ESP: 50
- ESP authentication is optional
- Original IP Header is encrypted and therefore hidden

IPsec - Tunnel Mode

- IPsec tunnel mode usually uses ESP to encrypt and authenticate tunneled IP packets although AH alone or in combination with ESP is also possible.
- The original IP packet is encrypted using ESP. Encryption also covers the original IP header thereby effectively hiding the IP source and destination addresses of the hosts forming the endpoints of the IP connection.
- The ESP header has the same function as in IPsec transport mode by carrying a Security Parameters Index (SPI) uniquely identifying the Security Association and offering replay protection by incrementing a sequence counter.
- Usually the ESP payload is also authenticated by appending an optional authentication data field which consists of a keyed message authentication code computed over the encrypted ESP payload plus the ESP header.
- The encrypted and authenticated ESP payload is transported in an IP datagram possessing an outer IP header which carries the IP addresses of two security gateways. The **Protocol field** of the outer IP header is set to the decimal value **51** designating the ESP protocol.

Information Hiding

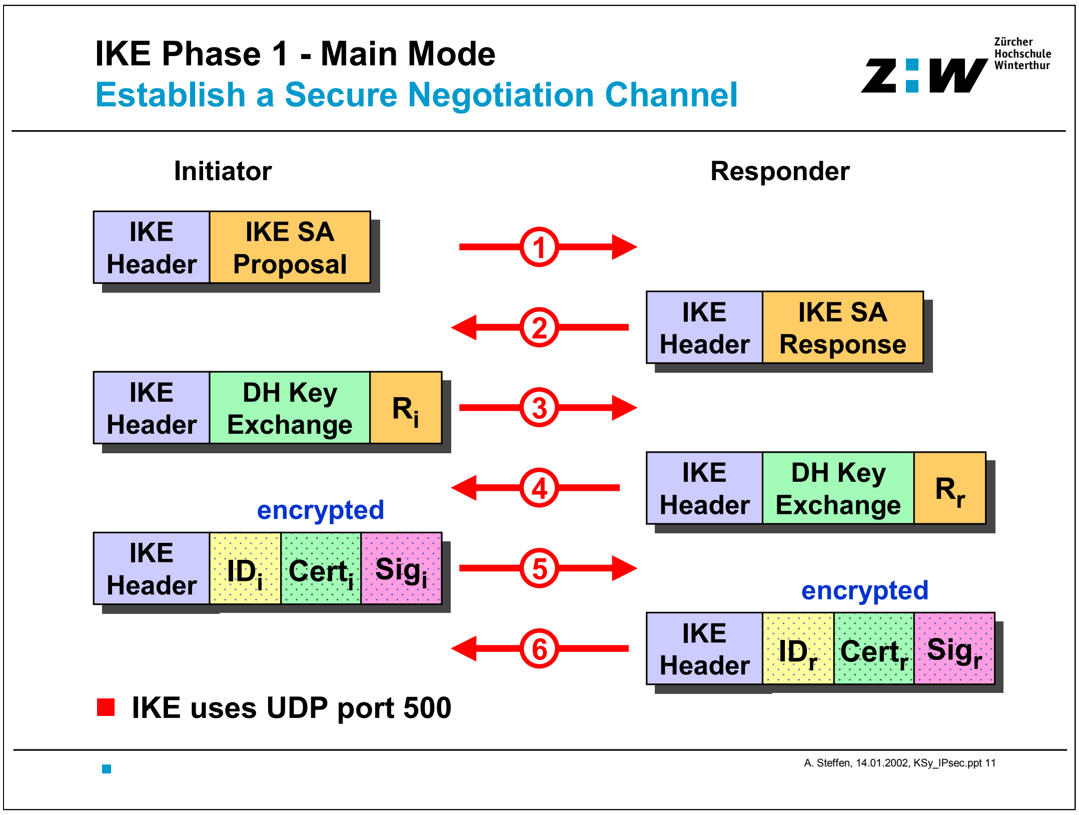
- Since the IP addresses of any two hosts located in the geographically separated subnets are hidden by the encrypted encapsulation, an attacker eavesdropping on the Internet tunnel cannot gain any information about the internal structure of the subnetworks. Detailed traffic analysis based on host and port addresses which can be applied to IPsec transport mode connections fails in the presence of an IPsec tunnel where only the two security gateways and the IPsec traffic exchanged between them are visible.

Internet Key Exchange (IKE)

IPsec - Automatic Key Management

The Internet Key Exchange (IKE)

- Security Association (SA)
  - A Security Association is a contract established between two IPsec endpoints (hosts or security gateways).
  - Automatic negotiation of parameters to be used for the IPsec connection.
  - Separate SA required for each subnet or single host.
  - Separate SA required for inbound and outbound connection.
  - SAs are assigned a unique Security Parameters Index (SPI) and are maintained in a database.
- Negotiated Parameters
  - Authentication Mechanism (secret or public key, certificates)
  - Encryption Algorithm (mode, key length, initialization vector)
  - Hash Algorithm
  - Key values and key lifetimes
  - SA renewal period



IKE Phase 1 - Main Mode

Establish a Secure Negotiation Channel

Zürcher Hochschule Winterthur

Initiator | Responder

1. Initiator → Responder: IKE Header | IKE SA Proposal
2. Responder → Initiator: IKE Header | IKE SA Response
3. Initiator → Responder: IKE Header | DH Key Exchange | R_i
4. Responder → Initiator: IKE Header | DH Key Exchange | R_r
5. Initiator → Responder: IKE Header | encrypted: ID_i | $Cert_i$ | Sig_i
6. Responder → Initiator: IKE Header | encrypted: ID_r | $Cert_r$ | Sig_r

- IKE uses UDP port 500

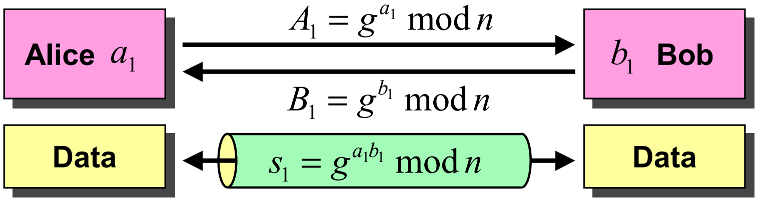
Internet Key Exchange - Phase 1 - Main Mode

- IKE Main Mode consists of six messages that must be exchanged between the initiator and the responder in order to establisch an IKE Security Association or IKE SA. The Internet Key Exchange protocol uses the well-known UDP port 500.
- Msg #1: The initiator sends an IKE SA Proposal listing all supported authentication methods, Diffie-Hellman groups, a choice of encryption and hash algorithms and the desired SA lifetime.
- Msg #2: The responder answers with an IKE SA Response indicating the preferred authentication method, Diffie-Hellman group, encryption and hash algorithm and acceptable SA lifetime.
- If the two parties were able to successfully negotiate a common set of methods the protocol is continued by establishing an encrypted communication channel using the Diffie-Hellman Key-Exchange algorithm (see next slide).
- Msg #3: The initiator sends his part of the Diffie-Hellman secret plus a random value.
- Msg #4: The responder does the same by sending his part of the Diffie-Hellman secret plus a random value.
- The Diffie-Hellman Key-Exchange can now be completed by both parties forming the common shared secret. This shared secret is used to generate a symmetric session key with which the remaining messages of the IKE protocol are going to be encrypted.
- Msg #5: The initiator sends his identity optionally followed by a certificate linking the identity to a public key. This is followed by a hash over all message fields signed by a preshared secret or a private RSA key.
- Msg #6: The same as Msg #5 but formed and sent by the responder.
- If the identity of both peers is successfully authenticated then an IKE SA has been established.

The Diffie-Hellman Key-Exchange Algorithm

Perfect Forward Secrecy

- Session 1: January 26 2001



Alice a_1

$A_1 = g^{a_1} \bmod n$

$B_1 = g^{b_1} \bmod n$

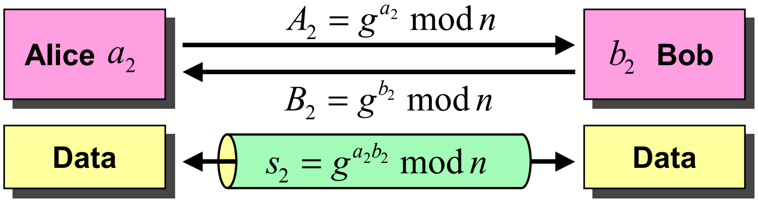
b_1 Bob

Data

$s_1 = g^{a_1 b_1} \bmod n$

Data

- Session 2: February 2 2001



Alice a_2

$A_2 = g^{a_2} \bmod n$

$B_2 = g^{b_2} \bmod n$

b_2 Bob

Data

$s_2 = g^{a_2 b_2} \bmod n$

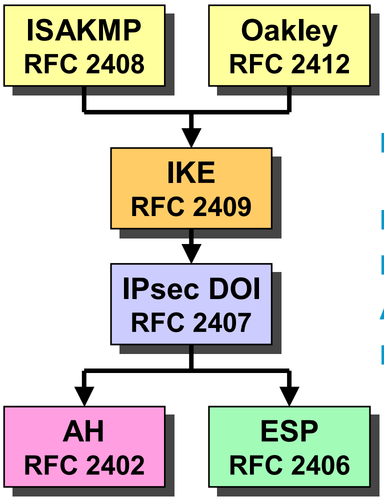
Data

- If key s_1 gets compromised, then key s_2 is still totally secure! (assuming that a_1, b_1, a_2 and b_2 are truly random)

IKE Phase 2 - Quick Mode
Establish or Renew an IPsec SA

- **Encrypted Quick Mode Message Exchange**
  - All Quick Mode negotiations are encrypted with a shared secret key derived from a Diffie-Hellmann key-exchange plus additional parameters.
- **Negotiation of IPsec Parameters**
  - Phase 2 Quick Mode establishes an IPsec SA using the secure channel created by the phase 1 IKE SA.
  - The specific configuration parameters for the IPsec connection are negotiated (AH, ESP, authentication / encryption methods and parameters).
  - Quick Mode can be used repeatedly to renew IPSec SAs about to expire.
- **Optional Perfect Forward Secrecy**
  - If perfect forward secrecy is required, each consecutive Quick Modes will do a fresh Diffie-Hellmann key-exchange.

IPsec - Relevant RFCs



ISAKMP	Internet Security Association and Key Management Protocol
IKE	Internet Key Exchange
DOI	Domain of Interpretation
AH	Authentication Header
ESP	Encapsulating Security Payload

Low Cost VPN Products based on IPsec

- Windows 2000/XP (http://vpn.ebootis.de)
  - Tool from ebootis.de loads configuration into Windows registry
- SSH Sentinel (www.ipsec.com)
  - IPsec Windows client with personal firewall
- SafeNet/Soft-Remote (www.safenet-inc.com)
  - IPsec Windows client with personal firewall (Zone Alarm)
- PGPnet (www.pgpi.org / www.mcafeeb2b.com/)
  - Freeware Version PGP 7.0.3
    IPsec transport mode only, PGP certificates or secret keys only
  - Professional Version PGP Desktop Security 7.1
    IPsec tunnel mode, X.509 certificates, with personal firewall
- Free S/WAN (www.freeswan.org / www.strongsec.com)
  - OpenSource IPsec patch for Linux 2.2 and 2.4 kernels
  - SuSE / Debian distributions offer easy installation via RPM
  - X.509 certificate support partly written by ZHW students !!!