IPSec

AH, ESP and IKE

IPSec Overview

- AH – Authentication Header – RFC 2402
  - provides for integrity protection
- ESP – Encapsulating Security Payload – RFC 2406 – provides for encryption an/or integrity
- IKE – Internet Key Exchange – RFC 2407/8/9 – provides for mutual authentication and a shared secret for security association

Security Association (SA)

- IPSec SA is a one-way cryptographically protected connection involving
  - cryptographic key
  - cryptographic algorithm
  - security services (e.g. encryption and/or integrity)
  - sequence number and ID of other end
- SPI (security Parameter Index) is field in IP Header which with destination address uniquely identifies SA in database

Security Association Database

- SA database at transmitter A holds following for B:
  - SPI
  - key
  - algorithm
  - sequence number
- SPI of received packet tells B where to look for above info required to process packet

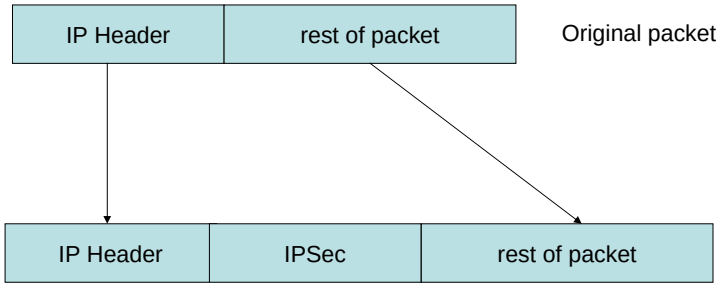
Security Policy Database

- Database specifies types of packets
  - to be dropped
  - to be forwarded or accepted under IPSec protection
  - to be forwarded or accepted without IPSec protection
  - to be encrypted or integrity protected
- Policy decision can be made on IP addresses (source or destination), protocol type or IP Header

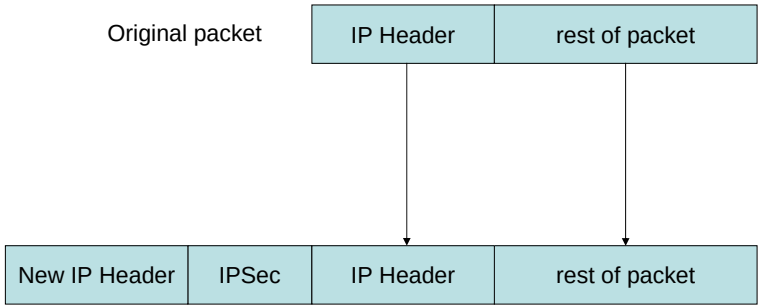
Modes in IPSec

- Transport Mode – suitable for end to end security
- Tunnel Mode – designed for protection over part of path but can be used for entire path
- Tunnel Mode requires additional header
- Firewall to firewall uses tunnel mode

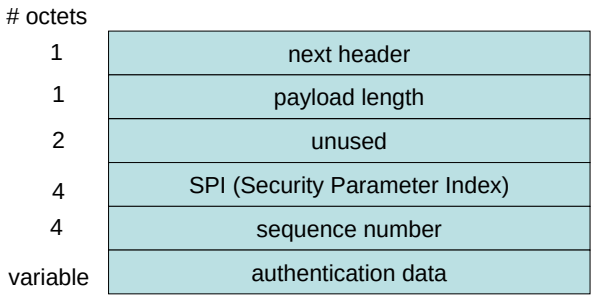
Transport Mode



Tunnel Mode



Authentication Header (AH)



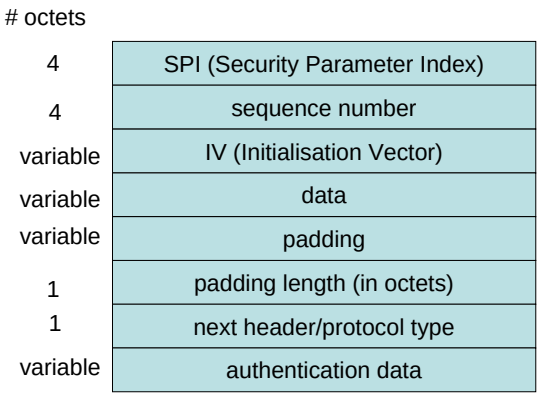
Authentication Header (II)

- Next header – specifies what follows – e.,g if TCP, Next Header = 6
- Payload length – total length of header in 32 bit words – not including first 8 octets
- Sequence number – defined by AH (i.e. not TCP sequence number) and protects against replay
- Authentication Data – cryptographic identity check on data

Mutable and Immutable Fields

- Fields which may be changed by routers along path cannot be included in integrity check
- Mutable fields are
  - Type of Service
  - Fragment Offset
  - Time to Live
  - Header Checksum

ESP Envelope



Encapsulating Security Payload (II)

- IV – e.g. as in CBC
- Data – the data to be protected by encryption or integrity
- Padding – to make data a multiple of block size for encryption
- Padding Length – number of octets of padding
- Authentication Data – cryptographic integrity check – zero if encryption only
- NB (i) encryption covers data, padding, padding length and next header, and (ii) integrity covers all from SPI to Next Header

AH and ESP Comparison

- ESP can provide integrity
- AH protects IP Header, ESP protects only beyond ESP Header
- AH possible more exportable
- AH allows intermediate devices to look at layer 4 ports

Internet Key Exchange (IKE)

- ISAKMP – Internet Security Association & Key Management Protocol – RFC 2408
- IKE – Internet Key Exchange – RFC 2409
- DOI – Domain of Interpretation – RFC 2407

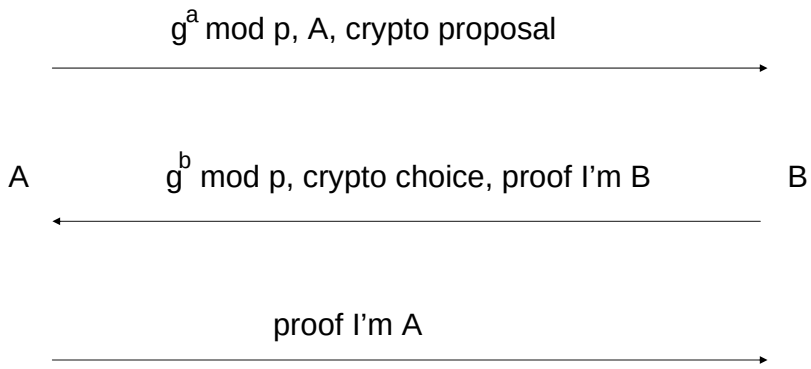
IKE Phases

- Phase 1 provide mutual authentication and establishes session key
- Phase 2 allows for multiple security associations for same Phase 1 pair
- Phase 1 exchange is ISAKMP SA
- ESP/AH SA is Phase 2

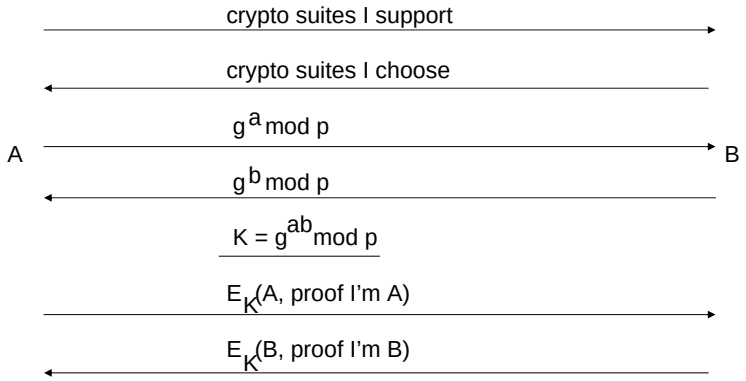
Phase 1 IKE

- Aggressive Mode – 3 messages used for mutual authentication and establishing session key
- Main Mode – uses 6 messages for above but has endpoint identifier hiding and can negotiate cryptographic parameters

Phase 1 EKE Aggressive Mode



Phase 1 IKE Main Mode



Phase 1 Key Types

- pre-shared secret key
- public encryption key pair
- public signature key pair
- two variants of public key
- each key variant used in main and aggressive mode
- 8 variants of Phase 1 IKE

Proof of Identity

- Intended to show that sender knows pre-shared secret or private signature key
- Proof is Hash (key, Diffie-Hellman values, names, crypto choices and cookies)
- Different proofs for different key variants

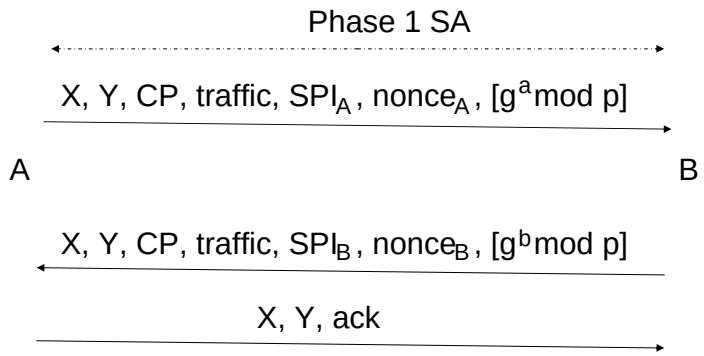
Negotiating Crypto Parameters

- A proposes suite of algorithms
- B chooses
- Encryption (DES, 3DES, IDEA)
- Hash (MD5, SHA-1)
- Authentication (private key MAC, RSA, DSS)

Session Keys

- Phase 1 establishes session key for integrity and session key for encryption
- Keys used for last Phase 1 IKE message and all Phase 2 IKE messages
- Keys are hashes of Diffie-Hellman numbers, names, cookies and long-term secrets

Phase 2 IKE: Establishing IPSec Security Associations



Phase 2 IKE

- X – pair of cookies generated in Phase 1
- Y- 32-bit number unique to Phase 2 session set up
- CP – crypto parameters proposed and accepted
- traffic – description of trtaffic (IP address pair, ports allocated, protocols allowed