Overview of IPSec

1

1

IP is not Secure!

- IP protocol was designed in late 70s to early 80s
  - Part of DARPA Internet Project
  - Very small network
    - All hosts are known!
    - So are the users!
    - Therefore, security was not an issue

3

3

Security Issues in plain IP

- Source address spoofing
- Bogus packets
- Replayed packets
- Re-ordered packets
- Eavesdropping on data in packets
- Eavesdropping on addressing info in packets

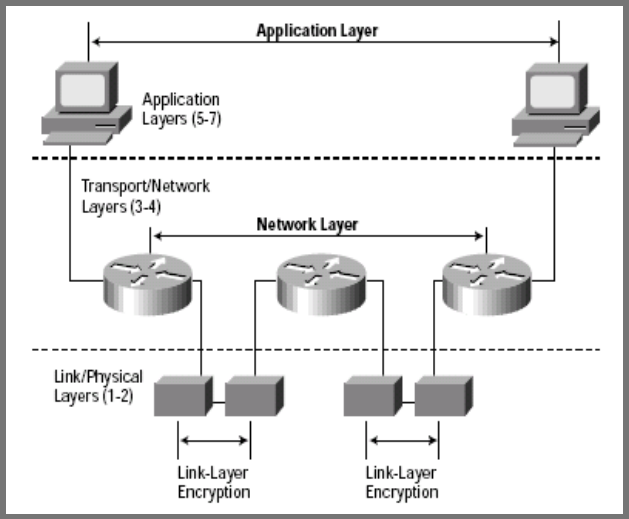
- No origin authentication
- No data integrity
- No data confidentiality
- No meta-data confidentiality

4

4

IPSec Placement

- lives at the network layer
- transparent to applications



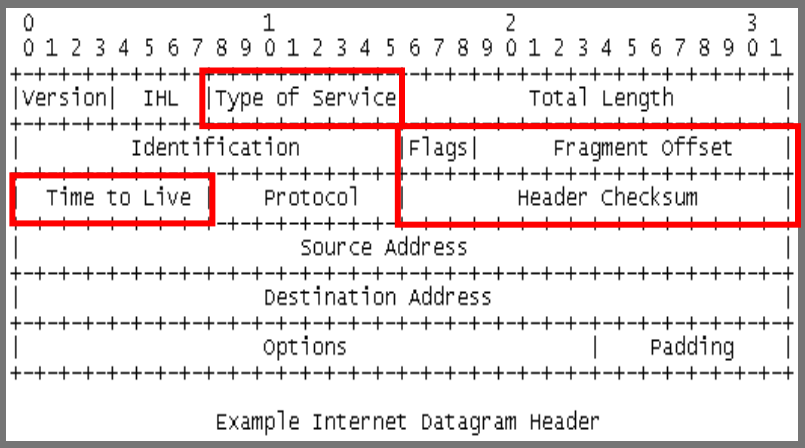
5

Quick recap of IP

6

6

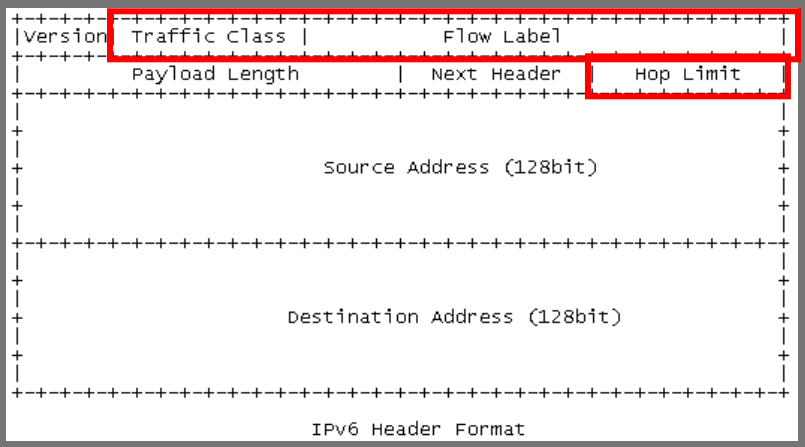
IPv4 Header Format



Mutable, Immutable

7

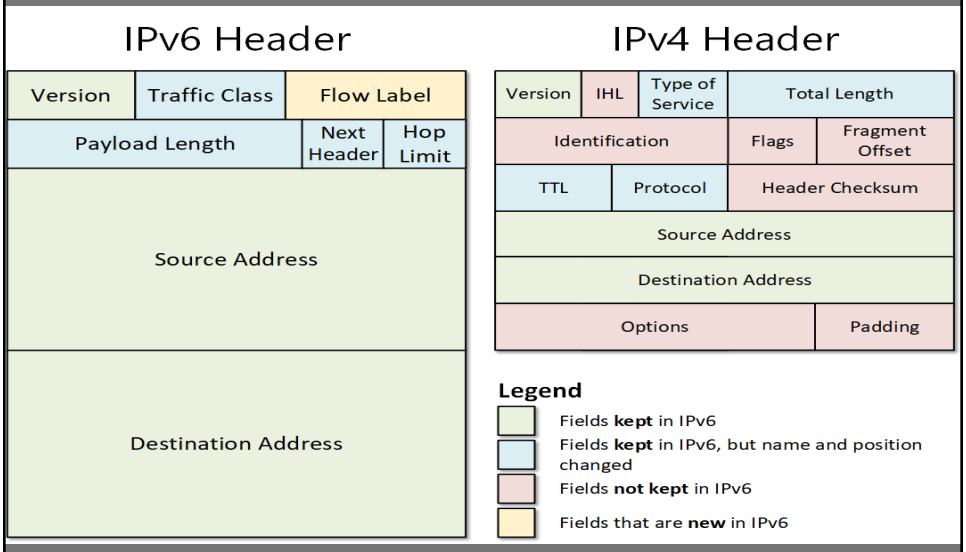
IPv6 Header Format



IPv6 Header Format

8

IPv4 v. IPv6



The rest of this presentation uses IPv4

9

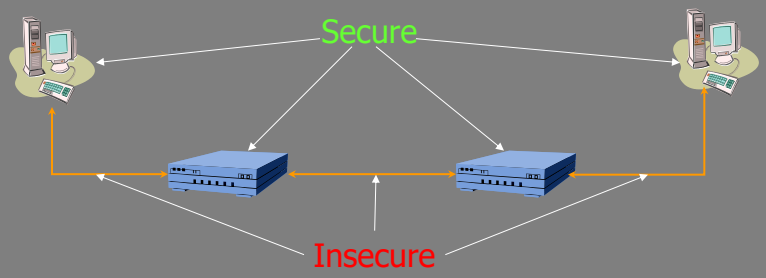
Goals of IPSec

- verify sources of IP packets
  - Origin authentication
- Detect replay and reordering of packets
  - Freshness
- Integrity of packet data
- Confidentiality of packet data
- Confidentiality of packet metadata
  - Eavesdropper can't tell who's talking to whom

10

10

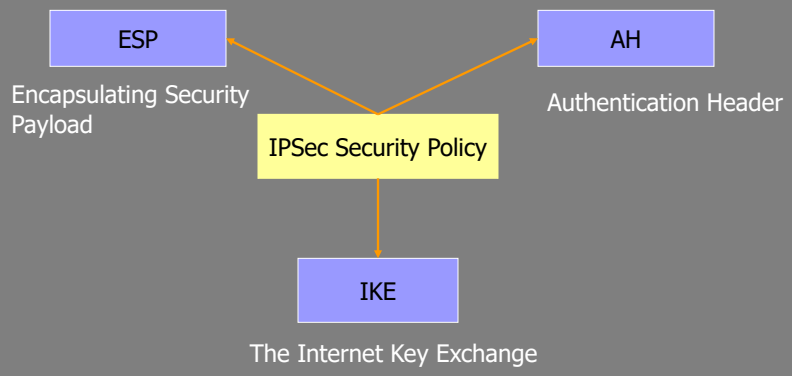
The IPSec Security Model



12

12

IPSec Architecture



13

13

IPSec Architecture

- Provides security in three cases:
  1. host-to-host
  2. host-to-gateway
  3. gateway-to-gateway

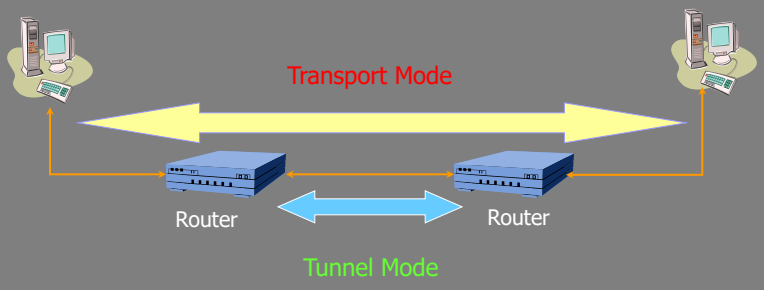
  (host means IP interface)
- Uses 2 formats: AH and ESP
- Operates in two modes: Transport and Tunnel

Note: Gateway is typically a border router of stub AD

14

14

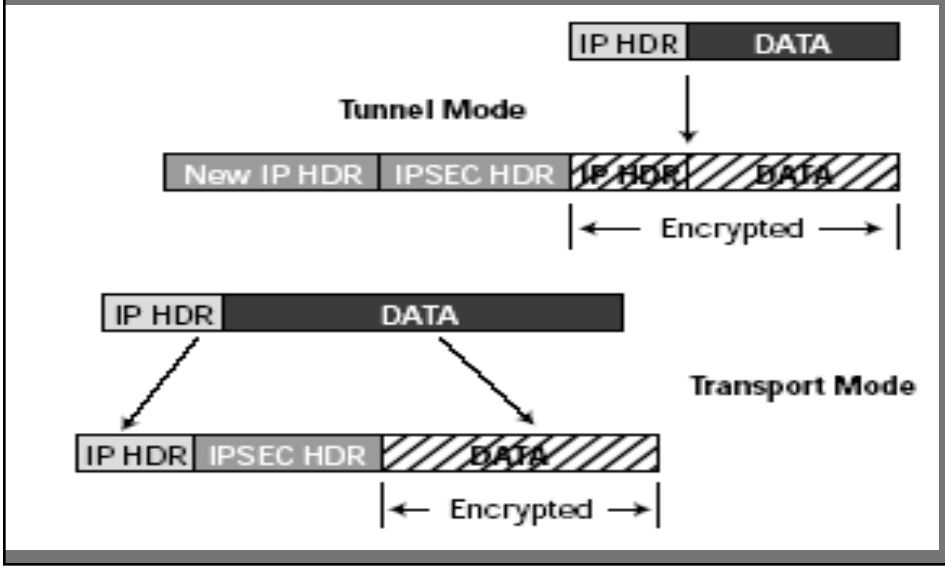
IPsec Architecture: typical use-cases: Modes



15

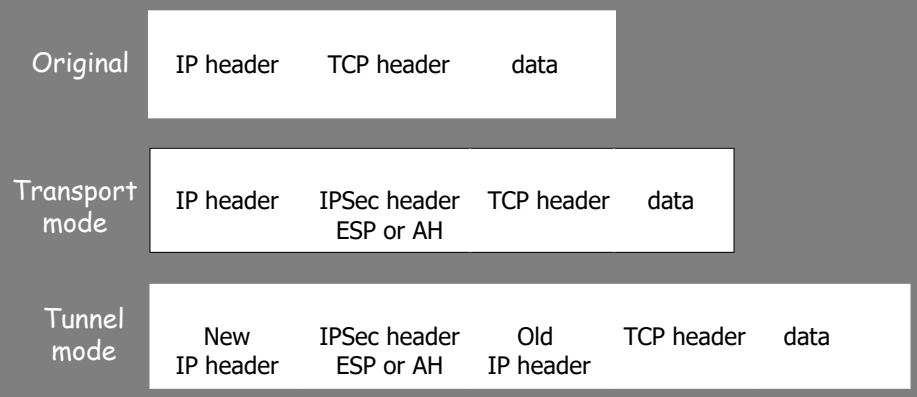
15

IPSec Modes



16

IPSec Modes



17

17

IPSec Specs

- A set of packet formats (RFC 2401)
  - Authentication Header (AH)
    - RFC 2402
  - Encapsulating Security Payload (ESP)
    - RFC 2406
  - Internet Key Exchange (IKE)
    - RFC 2409

18

18

Authentication Header (AH)

- Provides origin authentication
  - Protects against source address spoofing
- Provides data integrity
- Protects against replay attacks
  - Uses monotonically increasing sequence numbers
- NO data or metadata confidentiality!

19

19

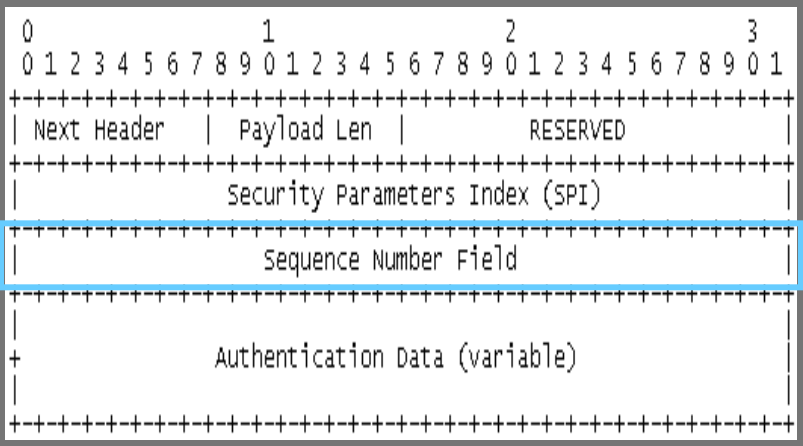
AH Details

- 32-bit monotonically increasing sequence number to detect replay attacks
- Cryptographic hash algorithms to protect data integrity
  - Symmetric cryptography
  - Various flavors of HMAC

20

20

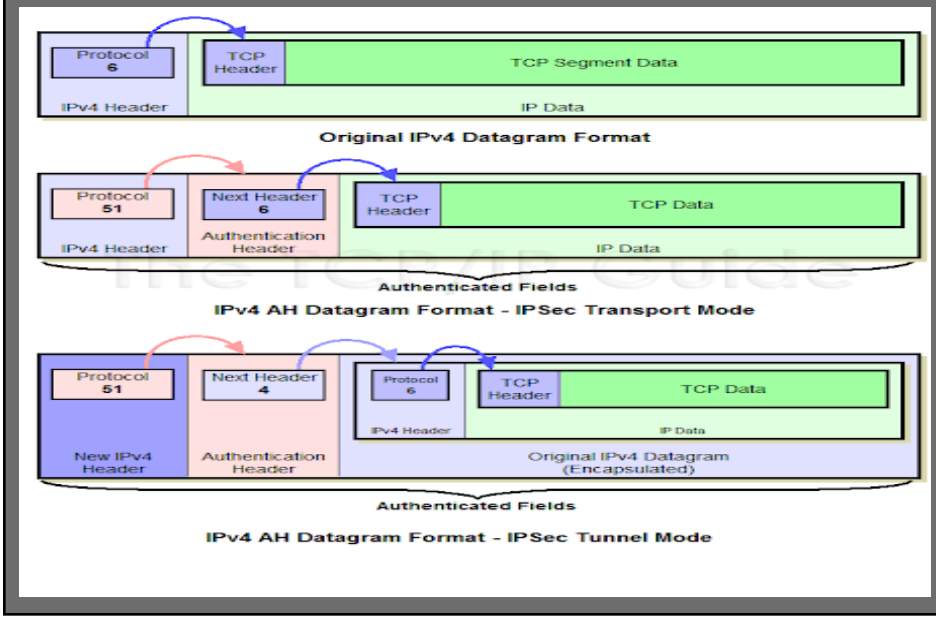
AH Format



The sender's counter is initialized to 0 when an SA is established.

21

AH Packet: Transport v. Tunnel



22

Encapsulating Security Payload (ESP)

- Provides all that AH offers

plus

- Data confidentiality via symmetric encryption

23

23

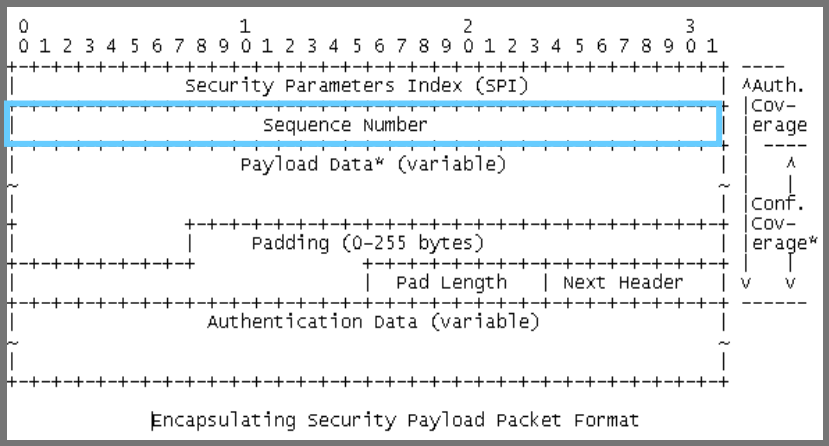
ESP Details

- Same as AH:
  - Use 32-bit sequence number to counter replaying attacks
  - Use integrity check algorithms
- Only in ESP:
  - Data confidentiality:
    - Uses symmetric key encryption algorithms to encrypt packets

24

24

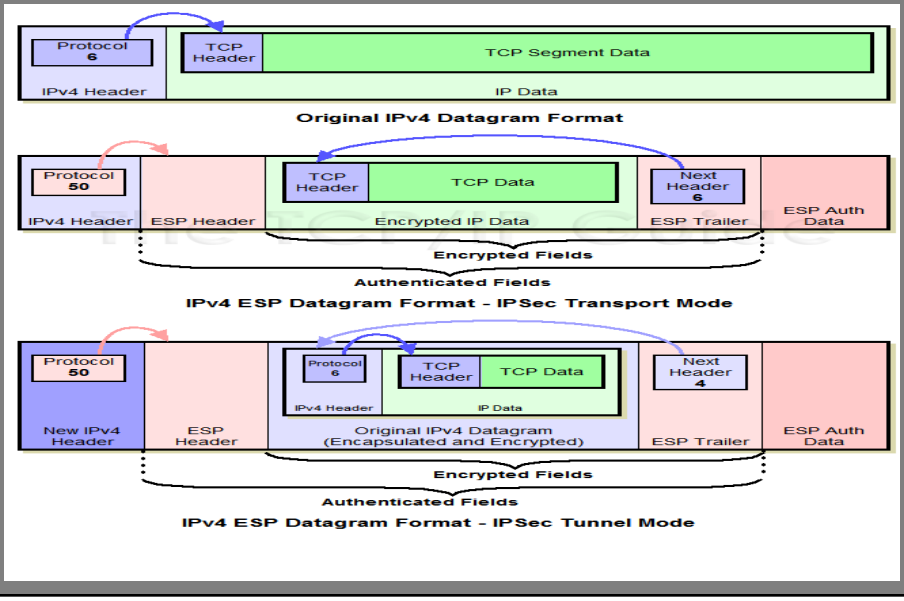
ESP Format



The sender's counter is initialized to 0 when an SA is established.

25

ESP Packet: Transport v. Tunnel



26

Questions?

1. Why have both AH and ESP?
2. Both AH and ESP use symmetric key based algorithms
   - Why not public-key cryptography?
   - How are the keys being exchanged?
   - What algorithms should we use?
   - Similar to deciding on the ciphersuite in SSL

27

27

Discussion

- IPSec authenticates machines/hosts, not users
- Does not stop denial of service attacks
  - In fact, makes DoS easier
- Order of operations: Encryption/Authentication

28

28

Internet Key Exchange (IKE)

- Exchange and negotiate security policies
- Establish security sessions
  - Identified as "*Security Associations" (SA)*
- Key exchange
- Key management
- Can be used outside IPsec as well

29

29

IPsec/IKE Acronyms

- Security Association (SA)
  - Collection of attribute associated with a connection
  - Is one-way
    - One SA for inbound traffic, another SA for outbound traffic
    - Similar to SSL/TLS (different keys used in each direction)
- Security Association Database (SAD)
  - A database of SAs

30

30

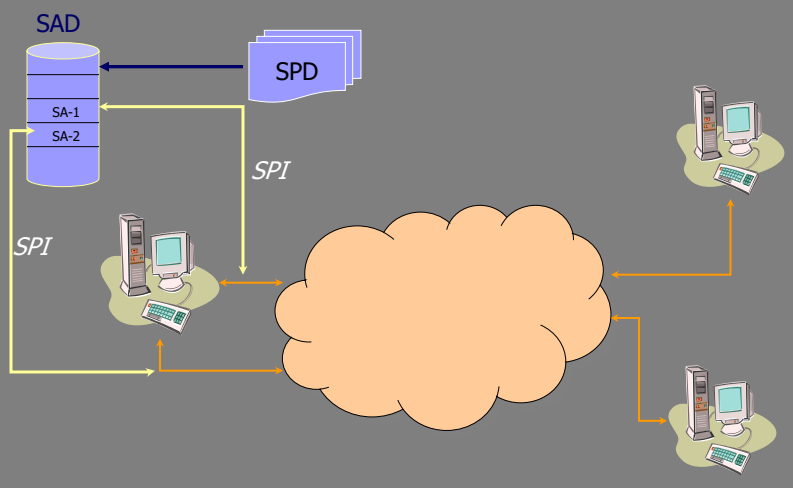
IPsec/IKE Acronyms

- Security Parameter Index (SPI)
  - A unique index for each entry in the SADB
  - Identifies the SA associated with a packet
- Security Policy Database (SPD)
  - Store policies used to establish SAs

31

31

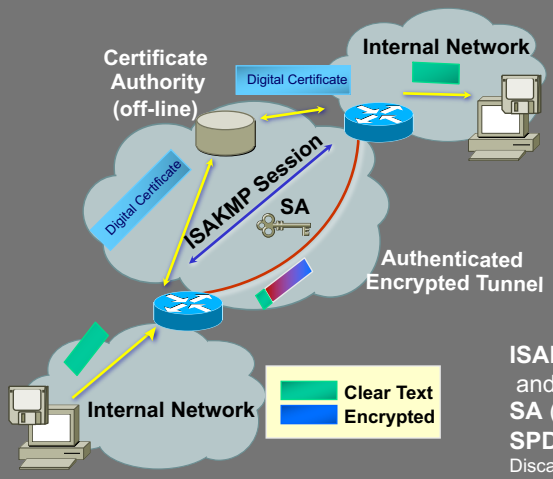
How They Fit Together



32

32

IPSec and IKE in Practice

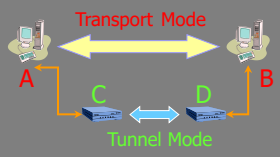


- Sets up a keying channel
- Sets up data channels

ISAKMP (Internet Security Association and Key Management Protocol)
SA (Security Associations)
SPD (Security Policy Database)
Discard,bypass IPsec, apply IPSec (Overhead)

33

SPD and SADB Example



A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

A's SAD

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

C's SPD

From	To	Protocol	Port	Policy	Tunnel Dest
A_{sub}	B_{sub}	Any	Any	ESP[3DES]	D

C's SAD

From	To	Protocol	SPI	SA Record
A_{sub}	B_{sub}	ESP	14	3DES key

34

34

How It Works

- IKE operates in two phases
  - Phase 1: negotiate and establish an auxiliary end-to-end secure channel
    - Used by subsequent phase 2 negotiations
    - Only established once between two end points!
  - Phase 2: negotiate and establish custom secure channels
    - Occurs multiple times
  - Both phases use Diffie-Hellman key exchange to establish a shared key

35

35

IKE Phase 1

- Goal: to establish a secure channel between two end points
  - This channel provides basic security features:
    - Source authentication
    - Data integrity and data confidentiality
    - Protection against replay attacks

36

36

IKE Phase 1

- Rationale: each application has different security requirements
- But they all need to negotiate policies and exchange keys!
- So, provide the basic security features and allow application to establish custom sessions

37

37

Examples

- All packets sent to address mybank.com must be encrypted using 3DES with HMAC-MD5 integrity check
- All packets sent to address www.forum.com must use integrity check with HMAC-SHA1 (no encryption is required)

38

38

Phase 1 Exchange

- Can operate in two modes:
  - Main mode
    - Six messages in three round trips
    - More options
  - Quick mode
    - Four messages in two round trips
    - Less options

39

39

Phase 1 (Main Mode)

Initiator

Responder

[Header, SA_1]

40

40

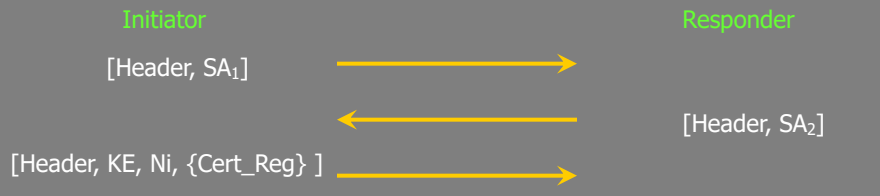
Phase 1 (Main Mode)

Establish vocabulary for further communication

41

41

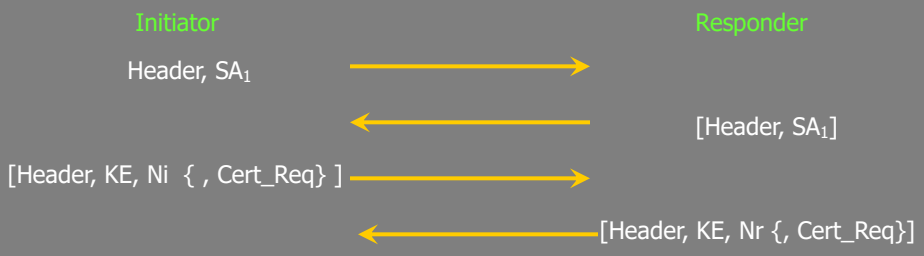
Phase 1 (Main Mode)



42

42

Phase 1 (Main Mode)

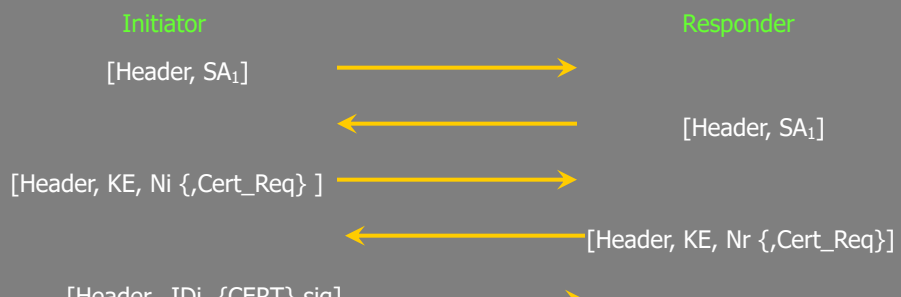


Establish secret key using Diffie-Hellman key exchange
Use nonces to prevent replay attacks

43

43

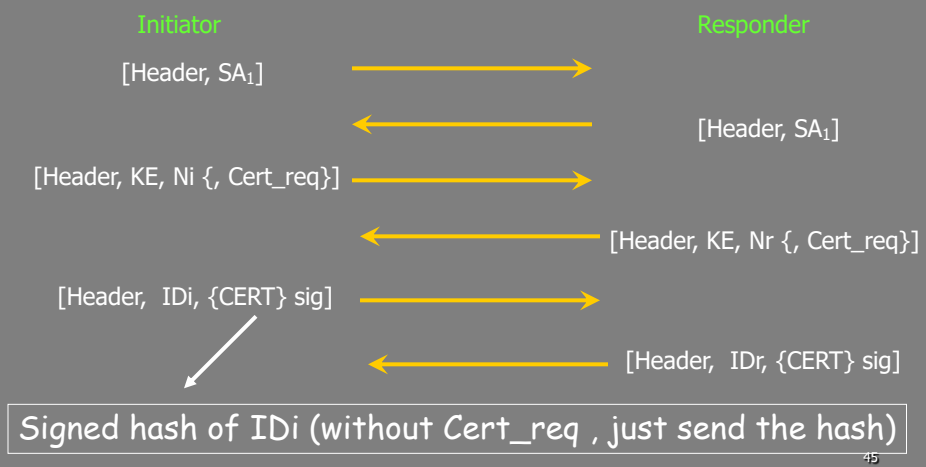
Phase 1 (Main Mode)



44

44

Phase 1 (Main Mode)



45

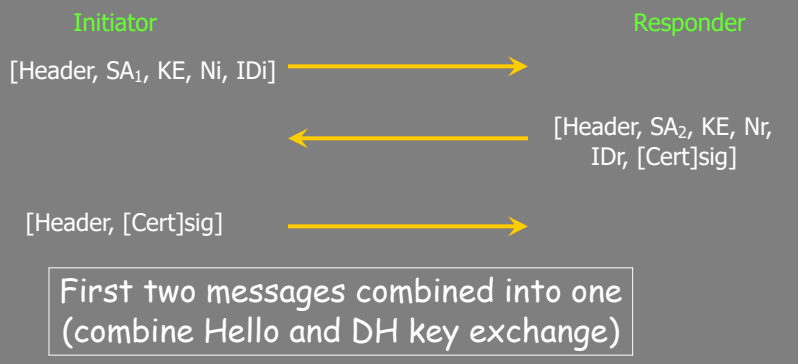
45

Phase 1 (Aggressive Mode)

46

46

Phase 1 (Aggressive Mode)



First two messages combined into one (combine Hello and DH key exchange)

47

47

IPSec (Phase 1)

- Four different way to authenticate (either mode)
  - Digital signature
  - Two forms of authentication with public key encryption
  - Pre-shared key
- NOTE: IKE does use public-key based cryptography for encryption

48

48

IPSec (Phase 2)

- **Goal:** to establish custom secure channels between two end points
  - End points are identified by <IP, port>:
    - e.g. <www.mybank.com, 8000>
  - Or by packet:
    - e.g. All packets going to 128.124.100.0/24
  - Use the secure channel established in Phase 1 for communication

49

49

IPSec (Phase 2)

- **Only one mode:** Quick Mode
- Multiple quick mode exchanges can be multiplexed
- Generate SAs for two end points
- Can use secure channel established in phase 1

50

50

IP Payload Compression

- Used for compression
- Can be specified as part of the IPSec policy
- Will not cover!

51

51

Outline

- Why IPsec?
- IPsec Architecture
- Internet Key Exchange (IKE)
- IPSec Policy
- Discussion

52

52

IPsec Policy

- Phase 1 policies are defined in terms of *protection suites*
- Each protection suite
  - Must contain the following:
    - Encryption algorithm
    - Hash algorithm
    - Authentication method
    - Diffie-Hellman Group
  - May optionally contain the following:
    - Lifetime
    - …

53

53

IPSec Policy

- Phase 2 policies are defined in terms of *proposals*
- Each proposal:
  - May contain one or more of the following
    - AH sub-proposals
    - ESP sub-proposals
    - IPComp sub-proposals
    - Along with necessary attributes such as
      - Key length, life time, etc

54

54

IPSec Policy Example

- In English:
  - All traffic to 128.104.120.0/24 must be:
    - Use pre-hashed key authentication
    - DH group is MODP with 1024-bit modulus
    - Hash algorithm is HMAC-SHA (128 bit key)
    - Encryption using 3DES
- In IPSec:
  - [Auth=Pre-Hash;
    DH=MODP(1024-bit);
    HASH=HMAC-SHA;
    ENC=3DES]

55

55

IPsec Policy Example

- In English:
  - All traffic to 128.104.120.0/24 must use one of the following:
    - AH with HMAC-SHA or,
    - ESP with 3DES as encryption algorithm and (HMAC-MD5 or HMAC-SHA as hashing algorithm)
- In IPsec:
  - [AH: HMAC-SHA] or,
  - [ESP: (3DES and HMAC-MD5) or
    (3DES and HMAC-SHA)]

56

56

Virtual Private Networks (VPNs)

- Virtual
  - It is not a physically distinct network
- Private
  - Tunnels are encrypted to provide confidentiality
- CS dept might have a VPN
  - I can be on this VPN while traveling

57

57

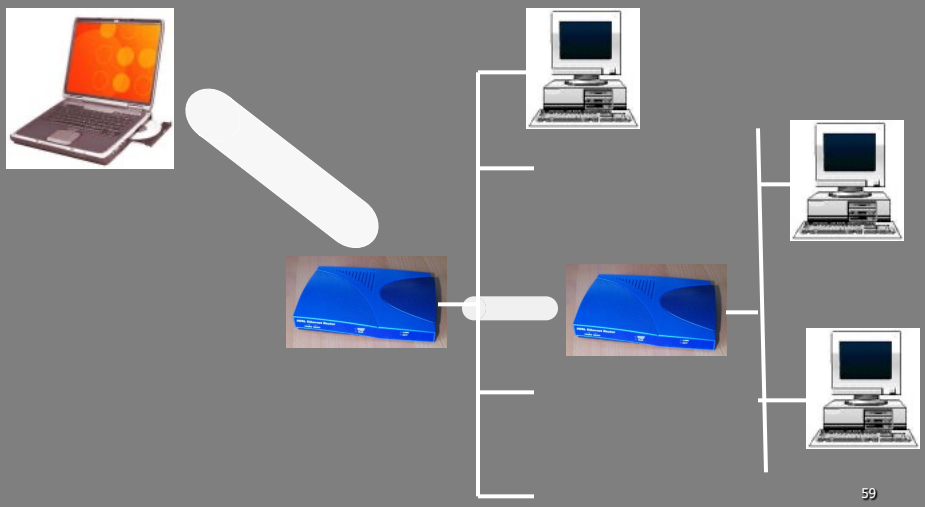
Alice is Traveling

- Alice works for the mergers and acquisitions (M&A) department of takeover.com
- She is at Hicktown taking over a meat-packing plant
- She wants to access the M&A server at her company (confidentially of course)

58

58

Alice is Traveling



59

59

Outline

- Why IPsec?
- IPsec Architecture
- Internet Key Exchange (IKE)
- IPsec Policy
- Discussion

60

60

Discussion

- IPSec is not the only solution!
  - Security features can be added on top of IP!
    - e.g. Kerberos, SSL
- Confused?
  - IP, IPSec protocols are very complex!
    - Two modes, three sub protocols
  - Complexity is the biggest enemy of security

61

61

Discussion

- Has it been used?
  - Yes—primarily used by some VPN vendors
    - But not all routers support it
  - No—it is not really an end-to-end solution
    - Authentication is too coarse (host based)
    - Default encryption algorithm too weak (DES)
    - Too complex for applications to use

62

62

Resources

- IP, IPsec and related RFCs:
  - http://www.ietf.org/html.charters/ipsec-charter.html
  - IPsec: RFC 2401, IKE: RFC 2409
  - www.freeswan.org
- Google search