CSE 410/565: Computer Security

Instructor: Dr. Ziming Zhao

Last Class

- Internet Control Message Protocol (ICMP)
  - Applications
  - How to exploit

Internet Protocol

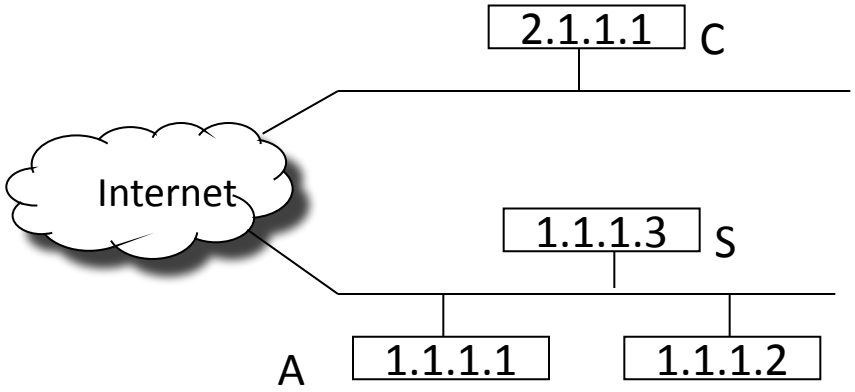
- IP protocol was designed in the late 70s to early 80s
  - Part of DARPA Internet Project
  - Very small network
    - All hosts are known!
    - So are the users!
    - Therefore, security was not an issue

Security Flaws in IP

- No data integrity or confidentiality
  - No encryption to protect payload (TCP, UDP, User data)
- Source spoofing
  - No host authentication
- IP fragmentation can be exploited

Source Spoofing

- The IP addresses are filled in by the originating host
  - Address spoofing



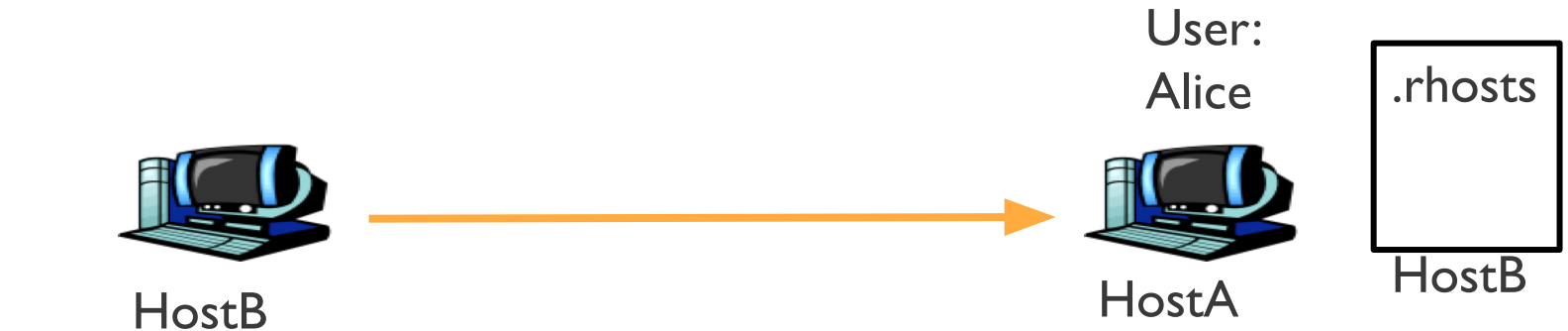
- Can A claim it is B to the server S?
- Can C claim it is B to the server S?

rlogin

- rlogin is a software utility for Unix-like computer operating systems that allows users to login on another host via a network, communicating via TCP port 513. (like Telnet, ssh)

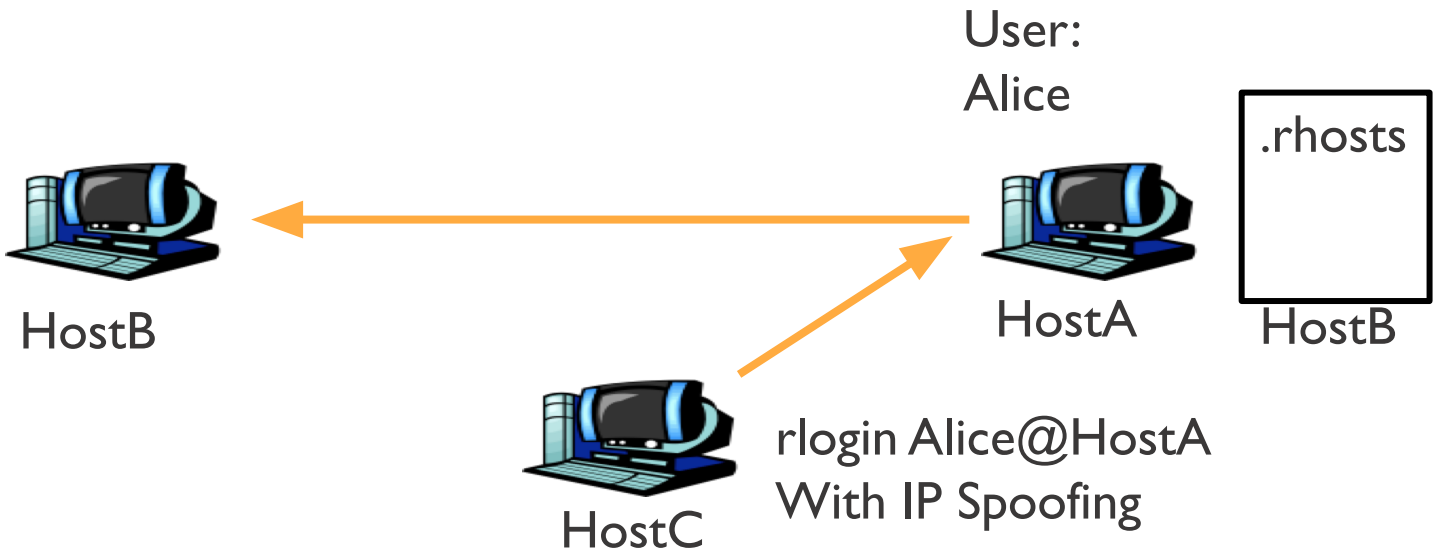
rlogin

- Alice can specify trusted hosts in ~/.rhosts.
- If a connection is from a trusted host, permission is granted to log in remotely without having to supply a password.



rlogin

- Attacker from HostC can execute commands on HostA



r-utilities

- rlogin: remote login
- rsh: remote shell
- rcp: remote copy

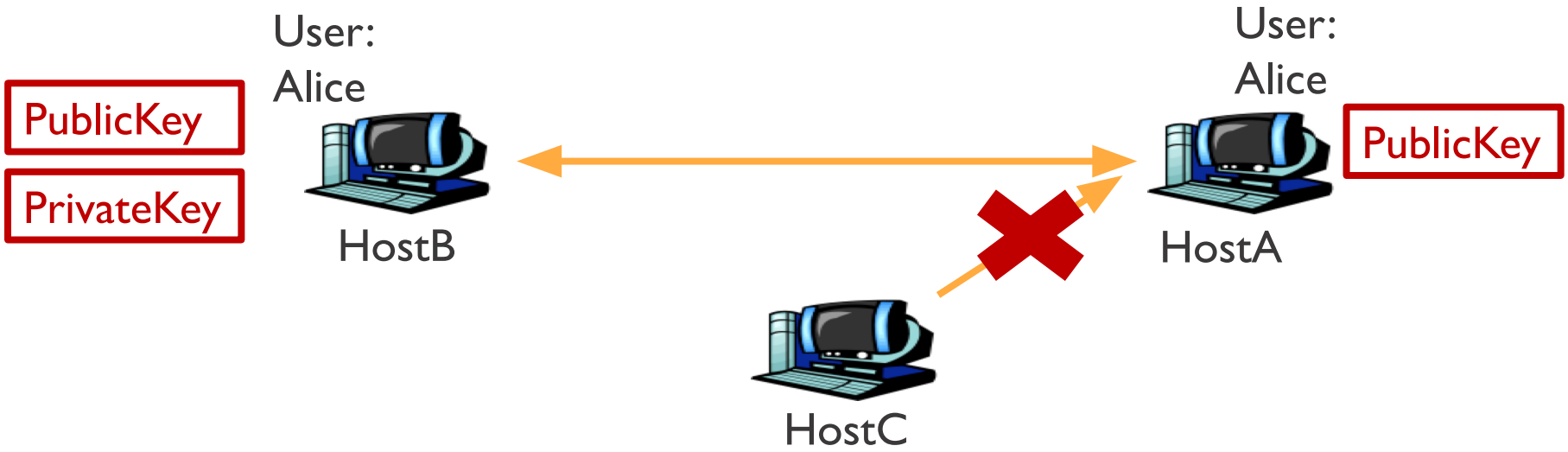
- Use them in a network environment where all hosts are trusted (No such environment exists!)

- Do not use them. Use *ssh*, *scp* instead

ssh

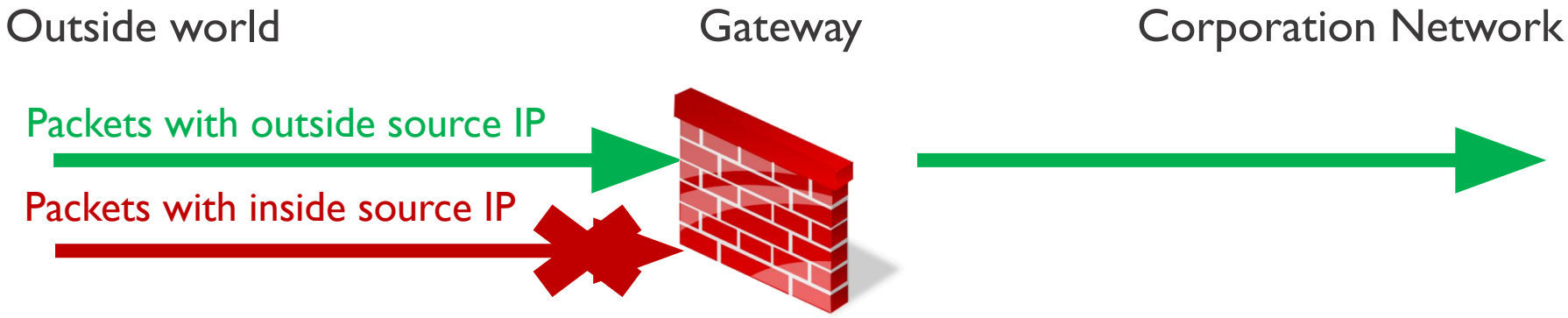
- Use it without password

Challenge/response
- HostA sends a random number
- HostB encrypts with PrivateKey
- HostA verfies by decrypting



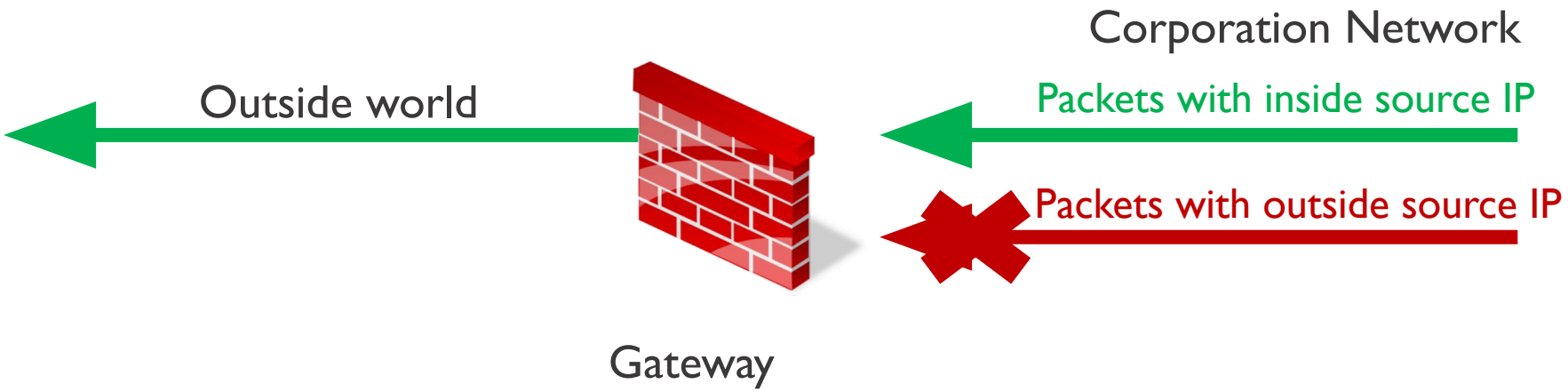
Defend Against Spoofing - Packet filtering

- The gateway blocks packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine.



Defend Against Spoofing - Packet filtering

- The gateway would also blocks packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.

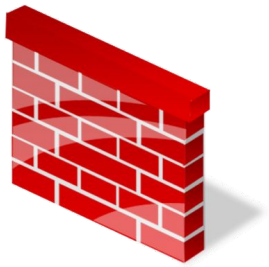


Defend Against Spoofing - Packet filtering

- It does not work, if an inside host is compromised and it tries to spoof another inside host.

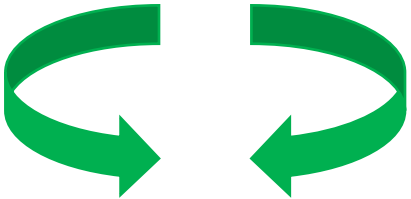
Outside world

Gateway



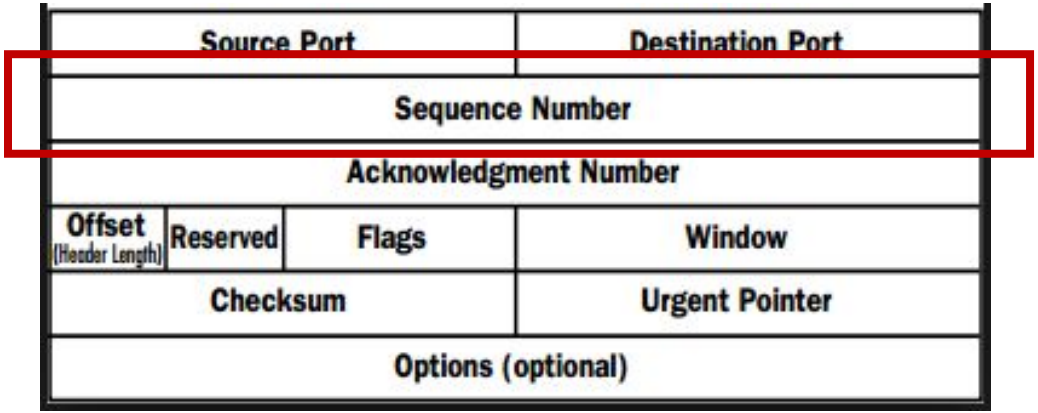
Corporation Network

Insider Spoofing



Defend Against Spoofing – Upper Layer

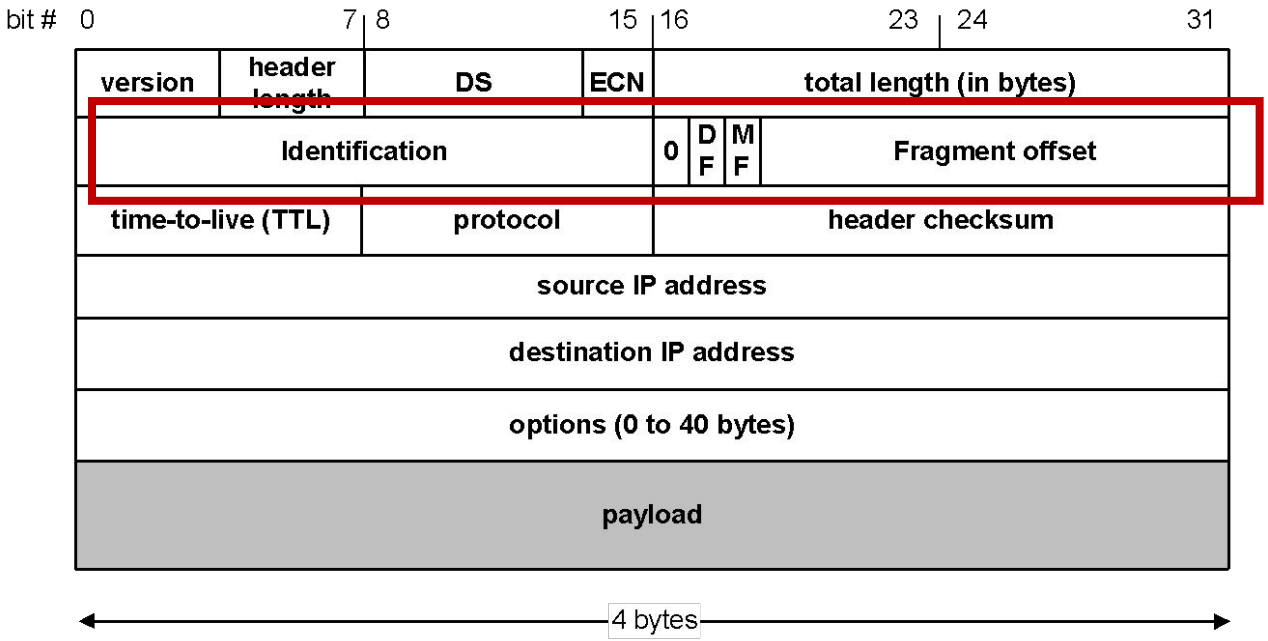
- Transmission Control Protocol (TCP) uses sequence numbers negotiated with the remote machine to ensure that arriving packets are part of an established connection.



Defend Against Spoofing - IPSec

- Internet Protocol Security (IPSec) Protocol Suite
  - Authentication Header (AH) to verify sources of IP packets

Exploit IP Fragmentation



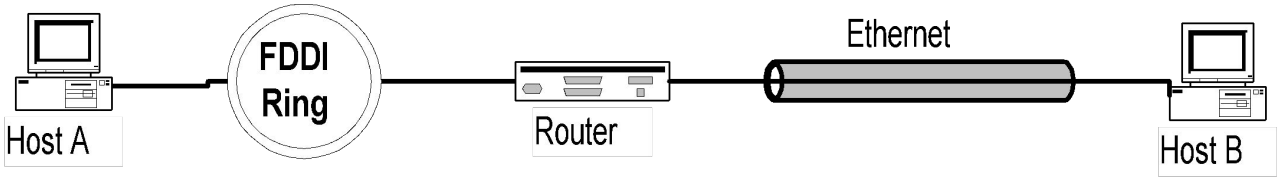
Maximum Transmission Unit (MTU)

Largest IP packet a *physical network* will accept

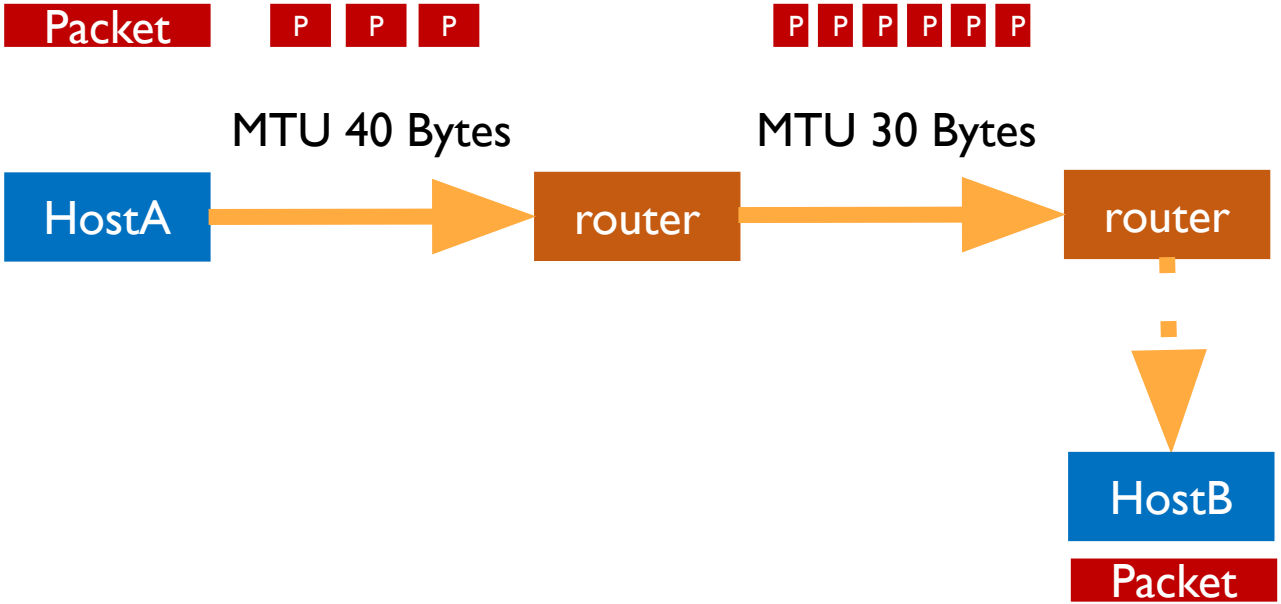
Media	Maximum Transmission Unit (bytes)
Internet IPv4 Path MTU	At least 68,[4] max of 64KB[5]
Internet IPv6 Path MTU	At least 1280,[7] max of 64KB, but up to 4GB with optional jumbogram[8]
Ethernet v2	1500[10]
Ethernet with LLC[11] and SNAP,[11] PPPoE[12]	1492[13]
Ethernet Jumbo Frames	1501 - 9198[14]
PPPoE over Ethernet v2	1492[16]
PPPoE over Ethernet Jumbo Frames	1493 - 9190[17]
WLAN (802.11)	7981[18]
Token Ring (802.5)	4464
FDDI	4352[6]

IP Fragmentation

- If IP packet is longer than the MTU, the NIC or router breaks packet into smaller packets
  - Called IP fragments
  - Fragments are still IP packets

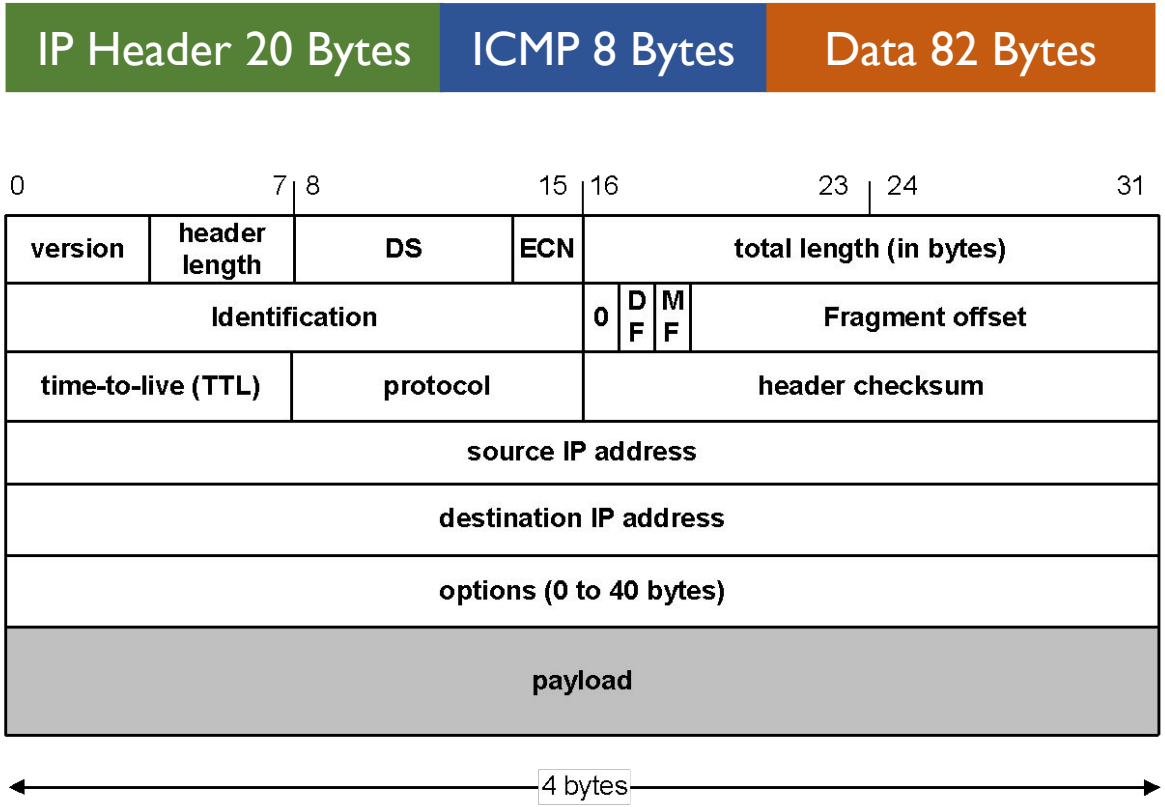


IP Fragmentation



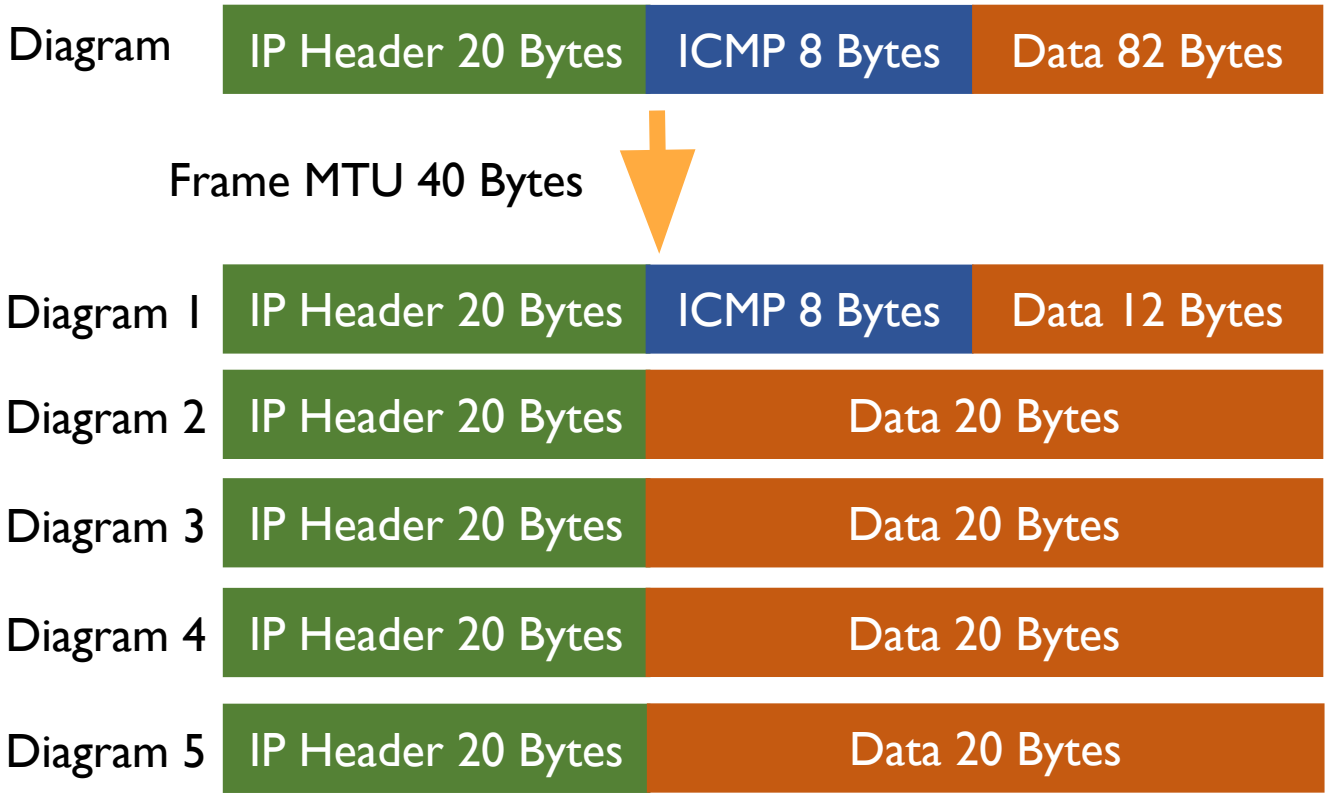
IP Fragmentation

Diagram



110 Bytes

IP Fragmentation



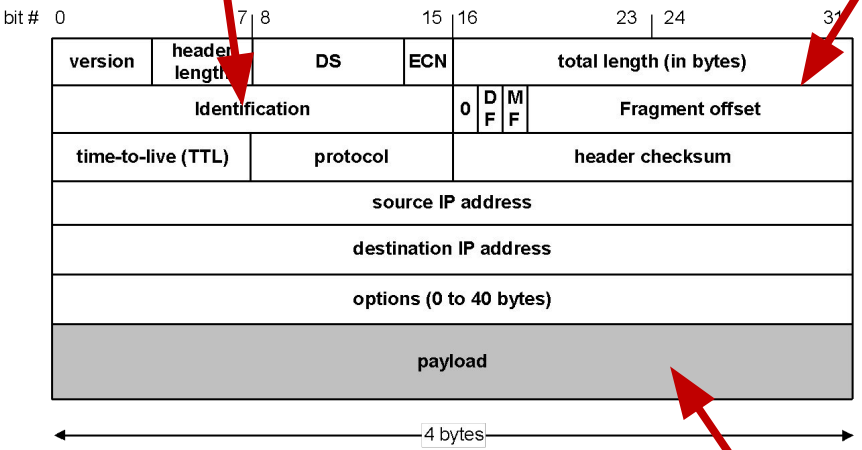
IP Fragmentation – Diagram 1

Unique identification of a datagram from a host

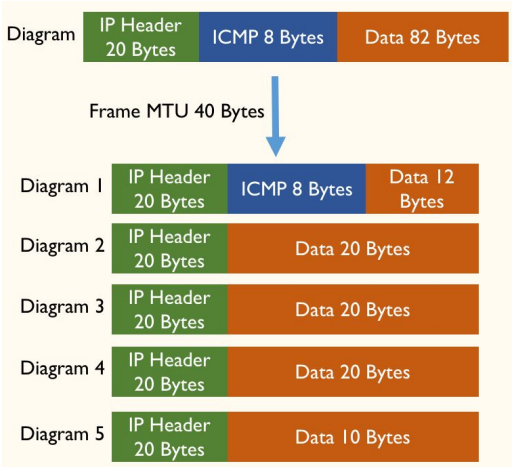
MF bit (More fragments)

Random-Number, R

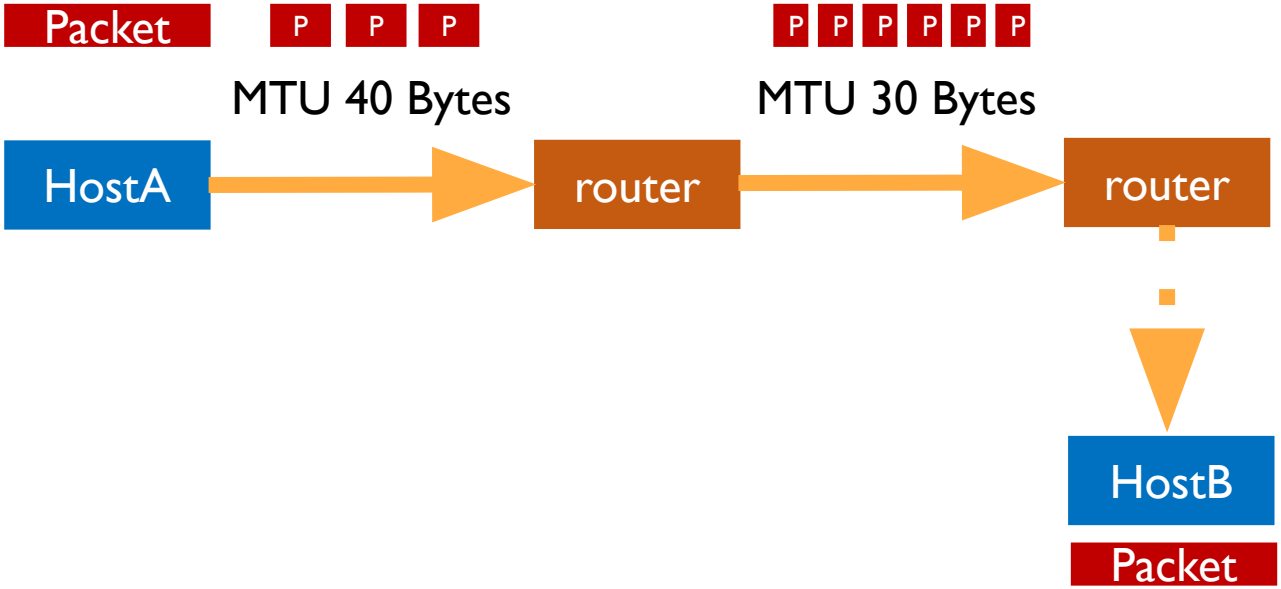
0



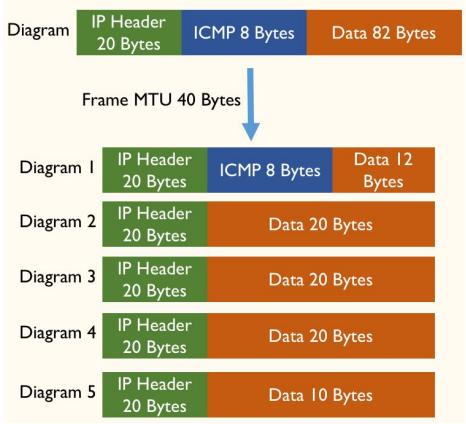
ICMP 8 Bytes and Data 12 Bytes

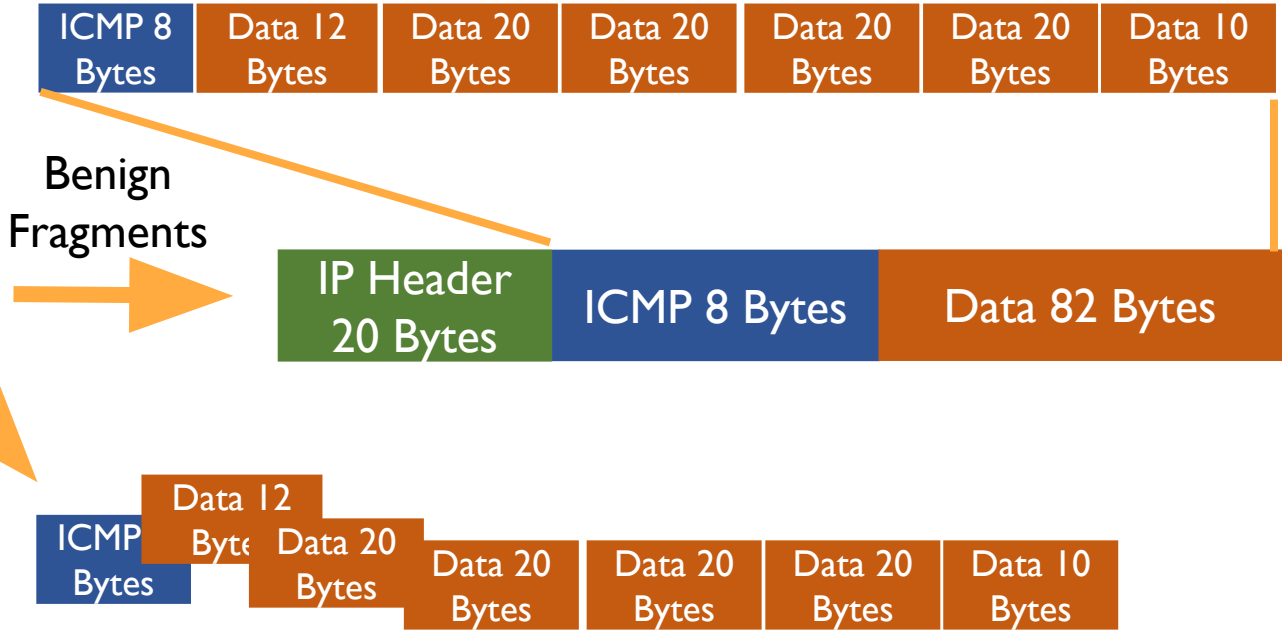


IP Fragmentation



IP Fragment Overlap





IP Fragment Buffer Full

The IP fragmentation buffer full exploit occurs when there is an excessive amount of incomplete fragmented (MF=1).

IP Fragment Incomplete Datagram

This exploit occurs when a datagram can not be fully reassembled due to missing data. This can indicate a denial of service attack or an attempt to defeat packet filter security policies.

IP is not Secure

- IP protocol was designed in the 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

Security Flaws in IP

- No data integrity or confidentiality
  - No encryption to protect payload (TCP, UDP, User data)

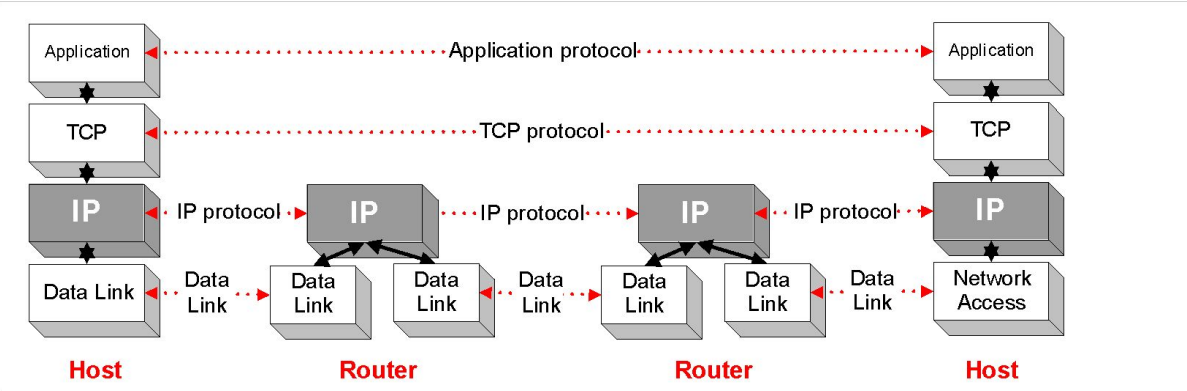
- Source spoofing
  - No host authentication

What is IPSec

- IPSec is an Internet standard for network layer security
  - Is below transport layer, hence transparent to applications
  - Can be transparent to end users
  - Can provide security for individual users
- To protect integrity and/or confidentiality of packets
  - Data Integrity/Data Encryption
- To verify sources of IP packets
  - Authentication
- Mandatory in IPv6, optional in IPv4

What is IPSec

- Protection of the IP and/or upper layer protocols (tcp, udp)
- Applicable to use over LANs, across public & private WANs, & for the Internet
- Host-to-host, host-to-gateway and gateway-to-gateway (router or firewall)



What is IPSec

- Specification is quite complex

- Main components:
  - An authentication protocol: Authentication Header (AH) RFC 2402
  - A combined encryption and authentication protocol: Encapsulating Security Payload (ESP) RFC 2406
  - Key Management and Exchange Protocols (the default is ISAKMP/Oakley)

AH and ESP

- Both can be used alone

- Can be combined as well
  - Apply ESP first, then apply AH again

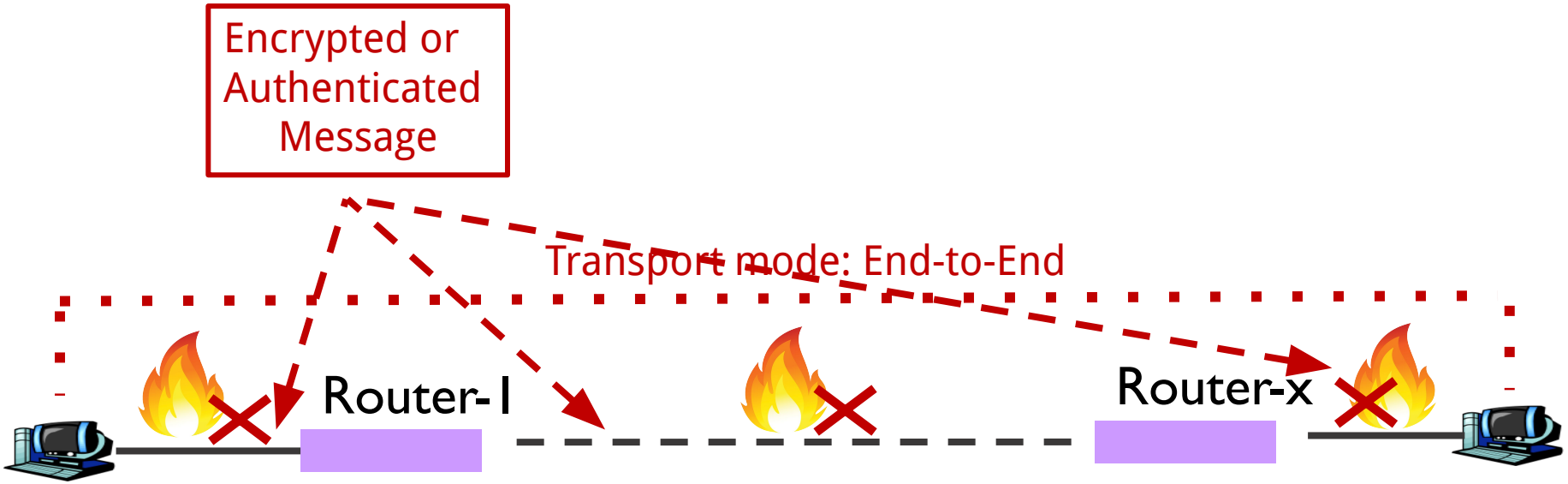
- Why?
  - Example: ESP does not authenticate new IP header. How to authenticate?
    - Use SA to apply ESP w/out authentication to original packet
    - Use 2nd SA to apply AH

Comparison

	AH	ESP (encryption only)	ESP (encryption and authentication)
integrity	x		x
data origin authentication	x		x
replay detection	x	x	x
confidentiality		x	x
limited traffic flow confidentiality		x	x

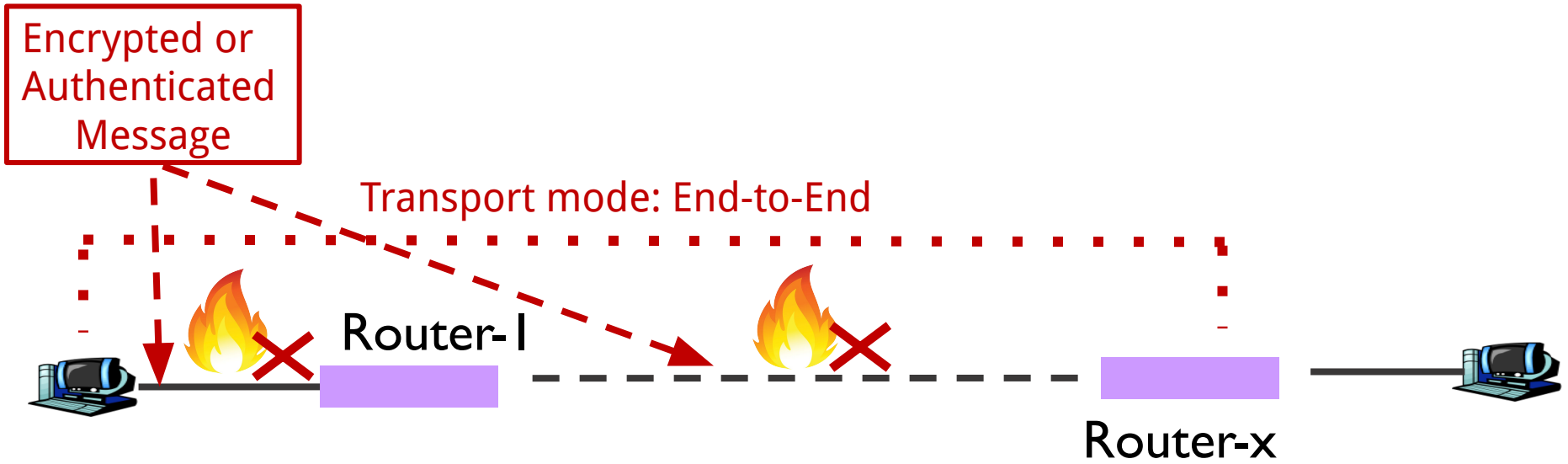
IPSec Modes

- Transport mode
  - End-to-end
  - Is used between end-stations



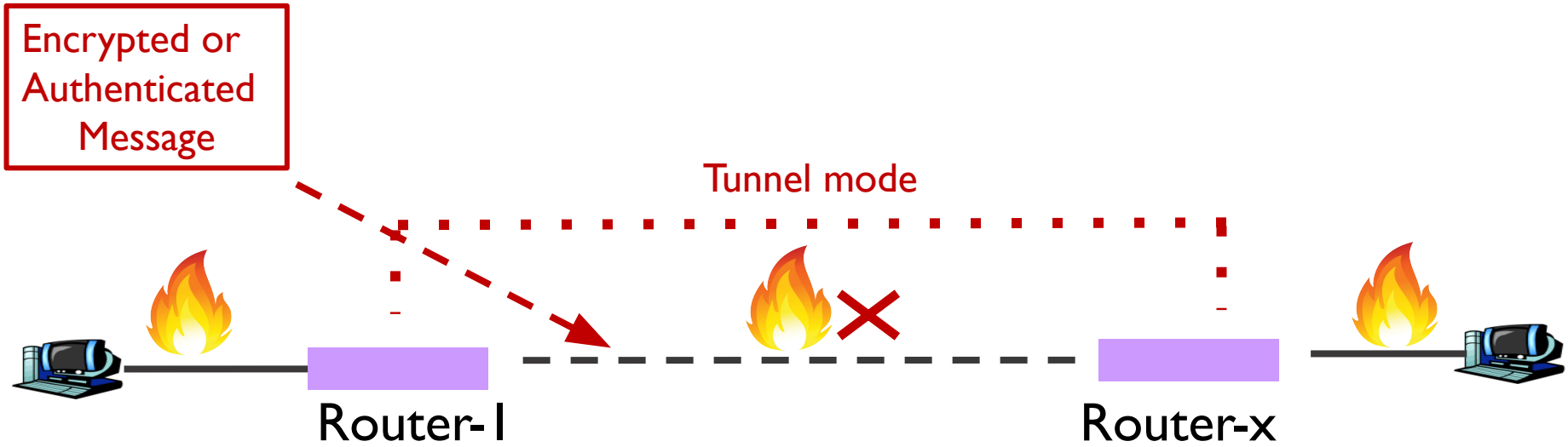
IPSec Modes

- Transport mode
  - End-to-end, host-to-host
  - Between an end-station and a gateway, if the gateway is being treated as a host
    - For example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.



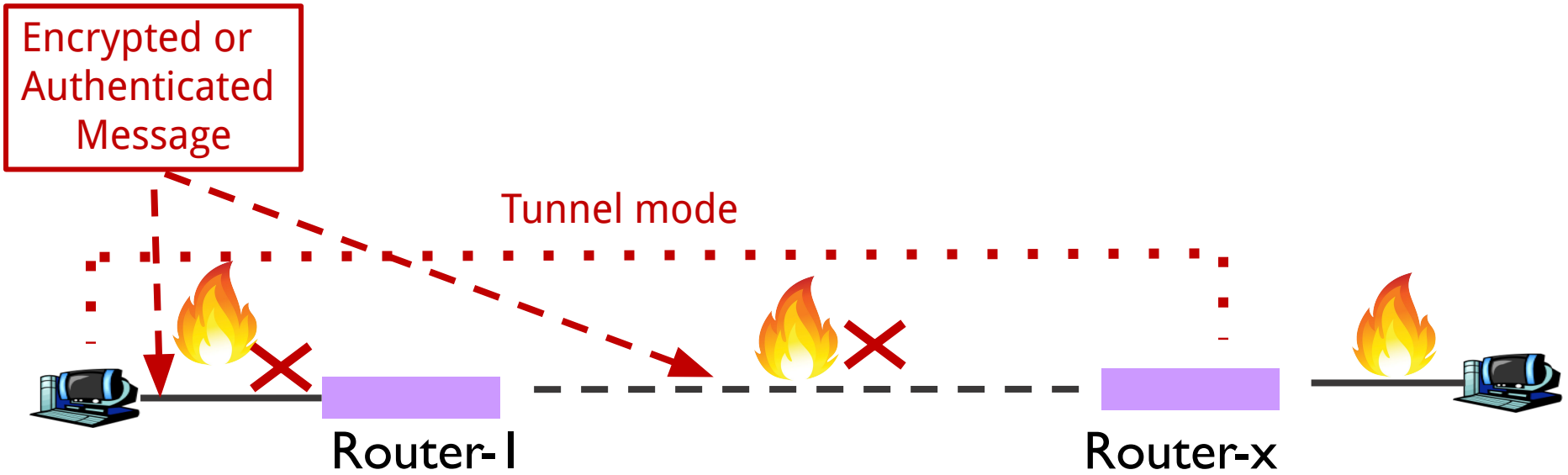
IPSec Modes

- Tunnel mode
  - gateway-to-gateway or host-to-gateway
  - is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.



IPSec Modes

- Tunnel mode
  - gateway-to-gateway or host-to-gateway
  - is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.



Virtual Private Networks (VPNs)

- Virtual
  - It is not a physically distinct network
- Private
  - Tunnels are encrypted to provide confidentiality

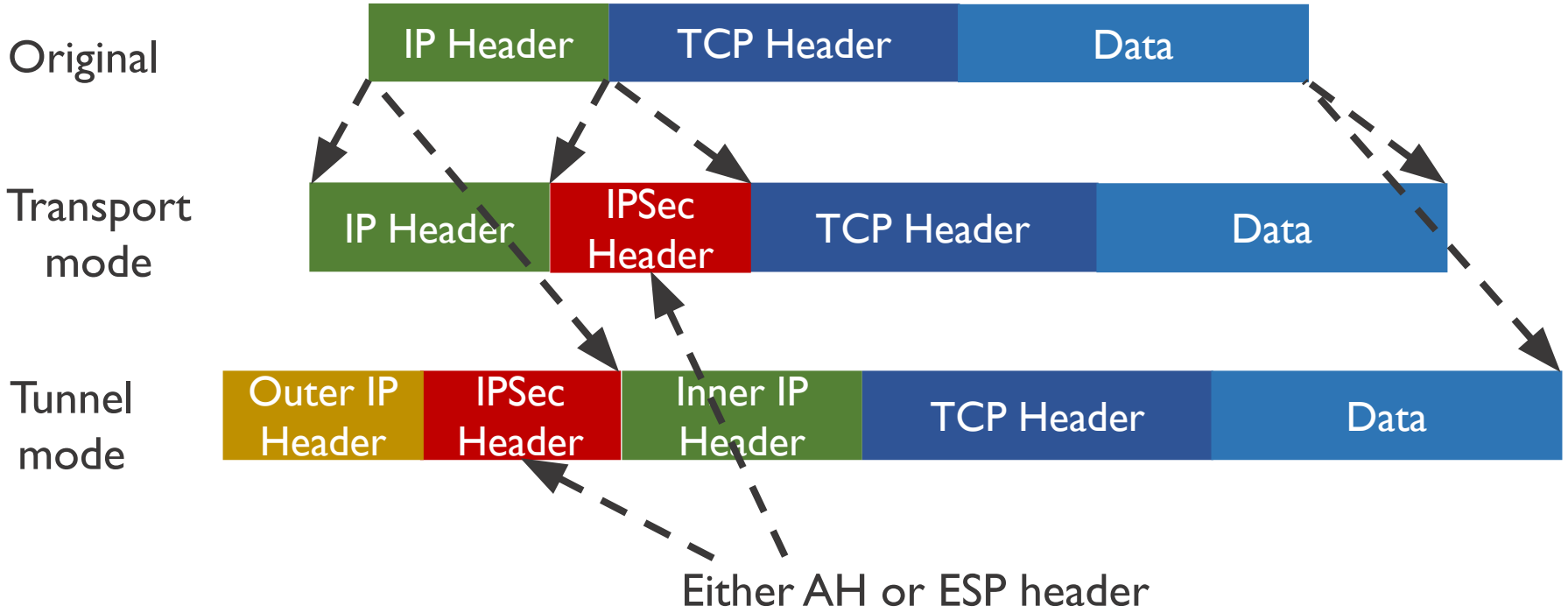
Alice is Traveling

- Alice works for the mergers and acquisitions (M&A) department of abc.com
- She is on a business trip taking over a plant
- She wants to access the M&A server and other servers at her company (confidentially of course)

- Which IPSec mode is most convenient for her?

Transport and Tunnel Packets

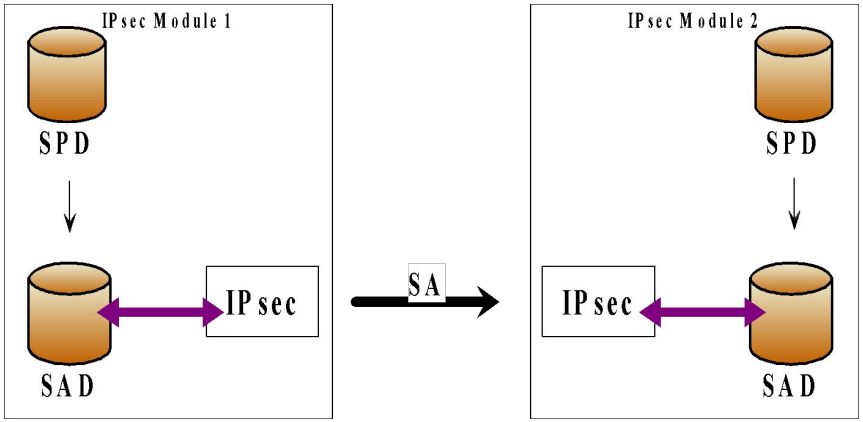
- Transport: Original IP payload can be encrypted. IP header can only be authenticated
- Tunnel: Entire original entire IP Packet can be encrypted and authenticated



IPSec Architecture

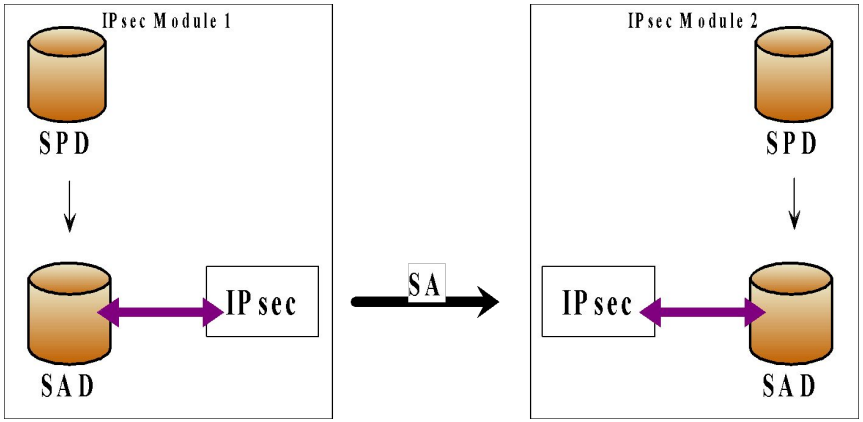
- IPSec module is used to manage security for individual connections to other modules
  - Security Policy Database (SPD) provides specifications of the security services to be applied to each packet
  - Security Association Database (SAD) contains the security parameters (encryption algorithms, mode used, initialization data, session keys) used to enforce a specific policy
  - A connection from one module to another is created through a security association (SA) that corresponds to an entry in the SAD
  - An SA is a unidirectional connection that defines the type of security services and mechanisms used between two modules

IPSec Architecture



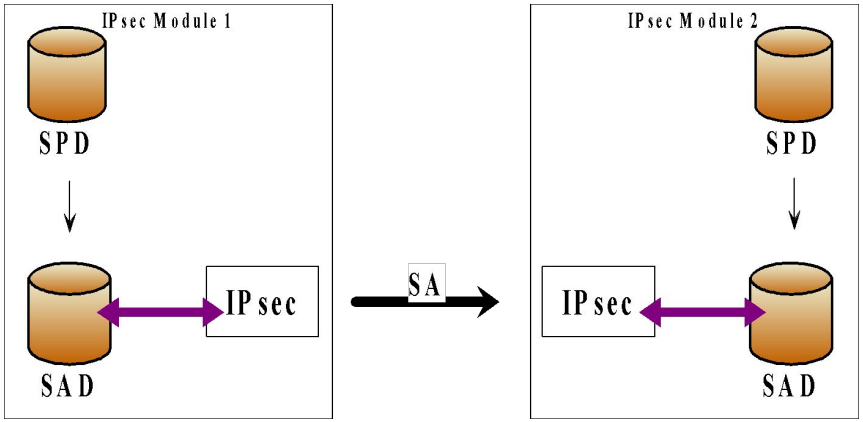
- Security Association is an association between a sender and a receiver
  - Consists of a set of security related parameters E.g., sequence number, encryption key
- One way relationship
- SAs are not fixed! Generated and customized per traffic flows

IPSec Architecture



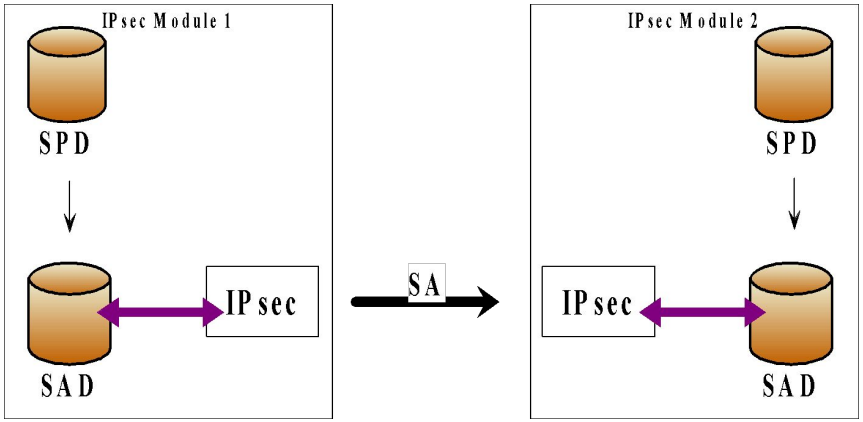
- An SA is uniquely identified by three parameters
  - Security Parameters Index (SPI)
    - a bit string assigned to the SA
    - carried in AH and ESP headers to allow the receiving party to select the SA which must be used to process the packet
  - IP destination address
    - address of an end-system or a network element (e.g., router)
  - security protocol identifier
    - indicates whether the SA is an AH or an ESP SA

IPSec Architecture



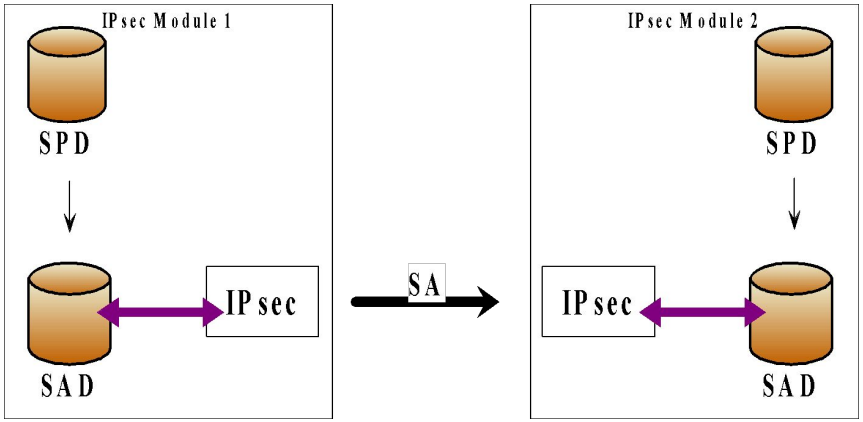
- SA bundle
- More than 1 SA can apply to a packet
- Example: ESP does not authenticate new IP header. How to authenticate?
  - Use SA to apply ESP w/out authentication to original packet
  - Use 2nd SA to apply AH

IPSec Architecture



- Security Association Database (SAD)
- Every host or gateway participating in IPsec has their own SA database
  - A database of SAs.
- Holds parameters for each SA
  - Sequence number counter
  - Lifetime of this SA
  - AH and ESP information
  - Tunnel or transport mode

IPSec Architecture



- Security Policy Database (SPD)
- Decide 1)What traffic to protect? 2) 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, …

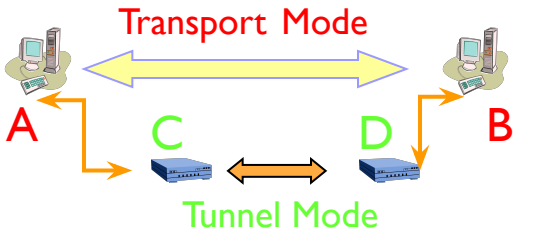
SPD Entry Actions

- 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

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]

SPD and SAD Example



A's SAD

A's SPD

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

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

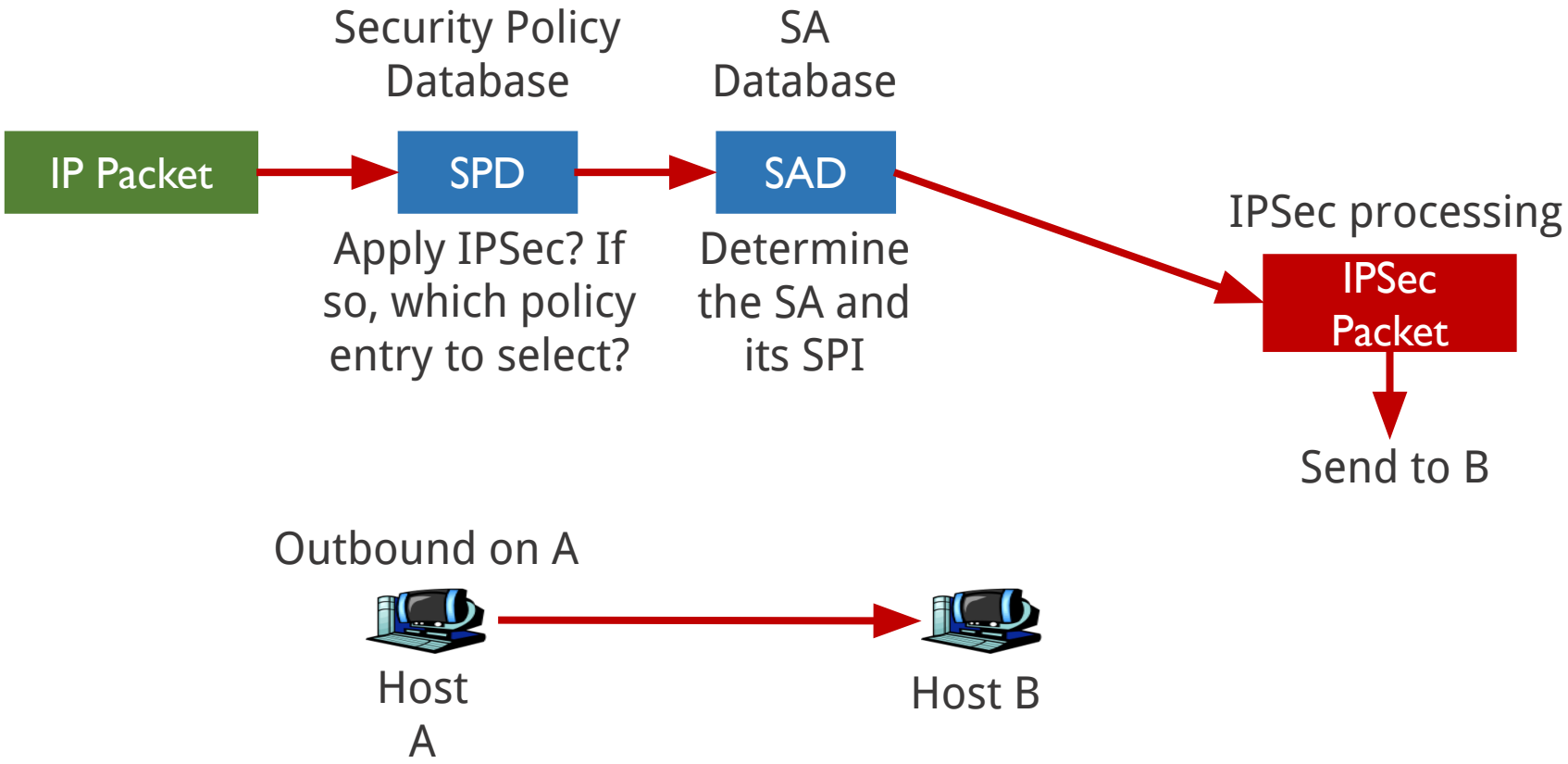
C's SAD

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

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