Advanced Network Security

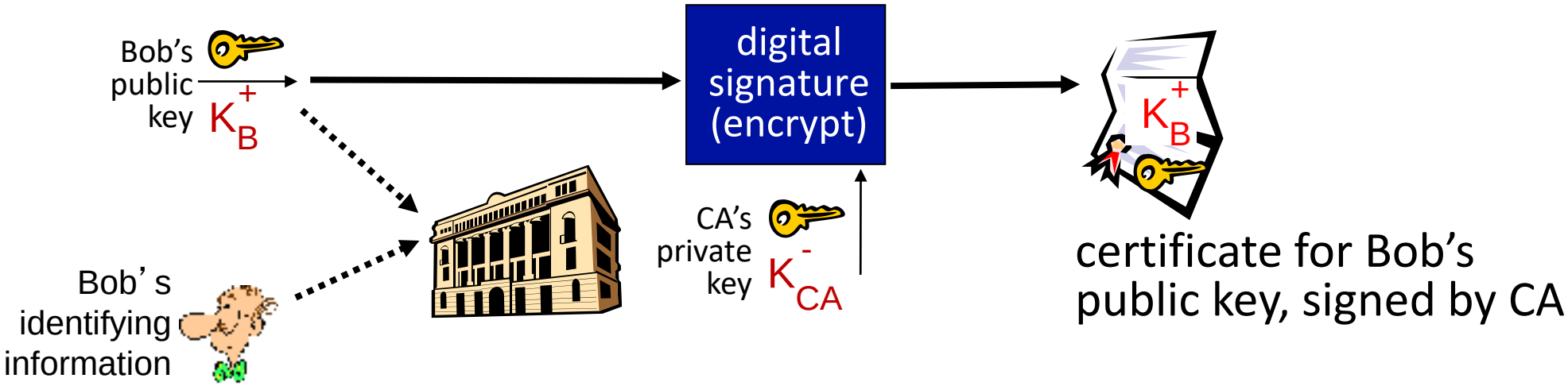
Amir Mahdi Sadeghzadeh, Ph.D.

Public key Certification Authorities (CA)

- certification authority (CA): binds public key to particular entity, E
- entity (person, website, router) registers its public key with “proof of identity” to CA
  - CA creates certificate binding identity E to E’s public key

Public Key Certification

- Certificate containing E's public key digitally signed by CA: CA says "this is E's public key"

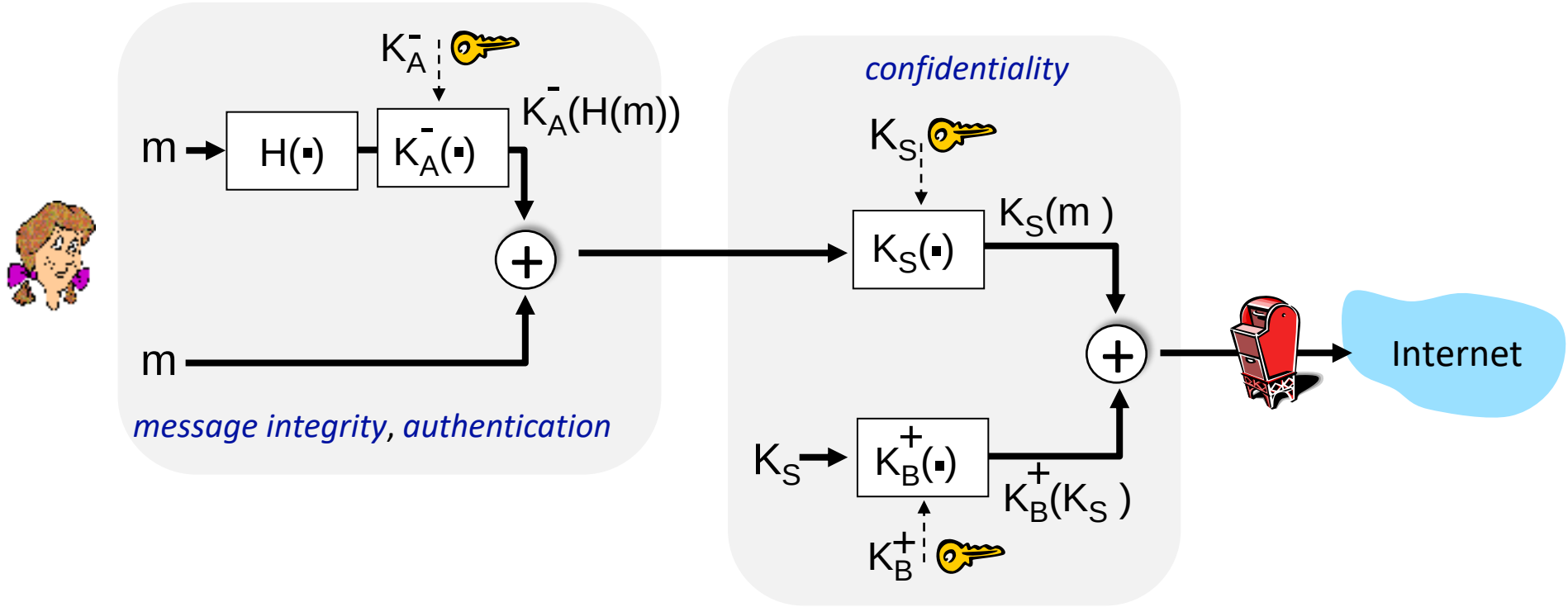


Outline

- What is network security?
- Principles of cryptography
- Authentication, message integrity
- **Securing e-mail**
- Securing TCP connections: TLS
- Network layer security: IPsec

Secure e-mail: confidentiality, integrity, authen.

Alice sends m to Bob, with *confidentiality, message integrity*, *authentication*



Alice uses three keys: her private key, Bob's public key, new symmetric key

What are Bob's complementary actions?

Outline

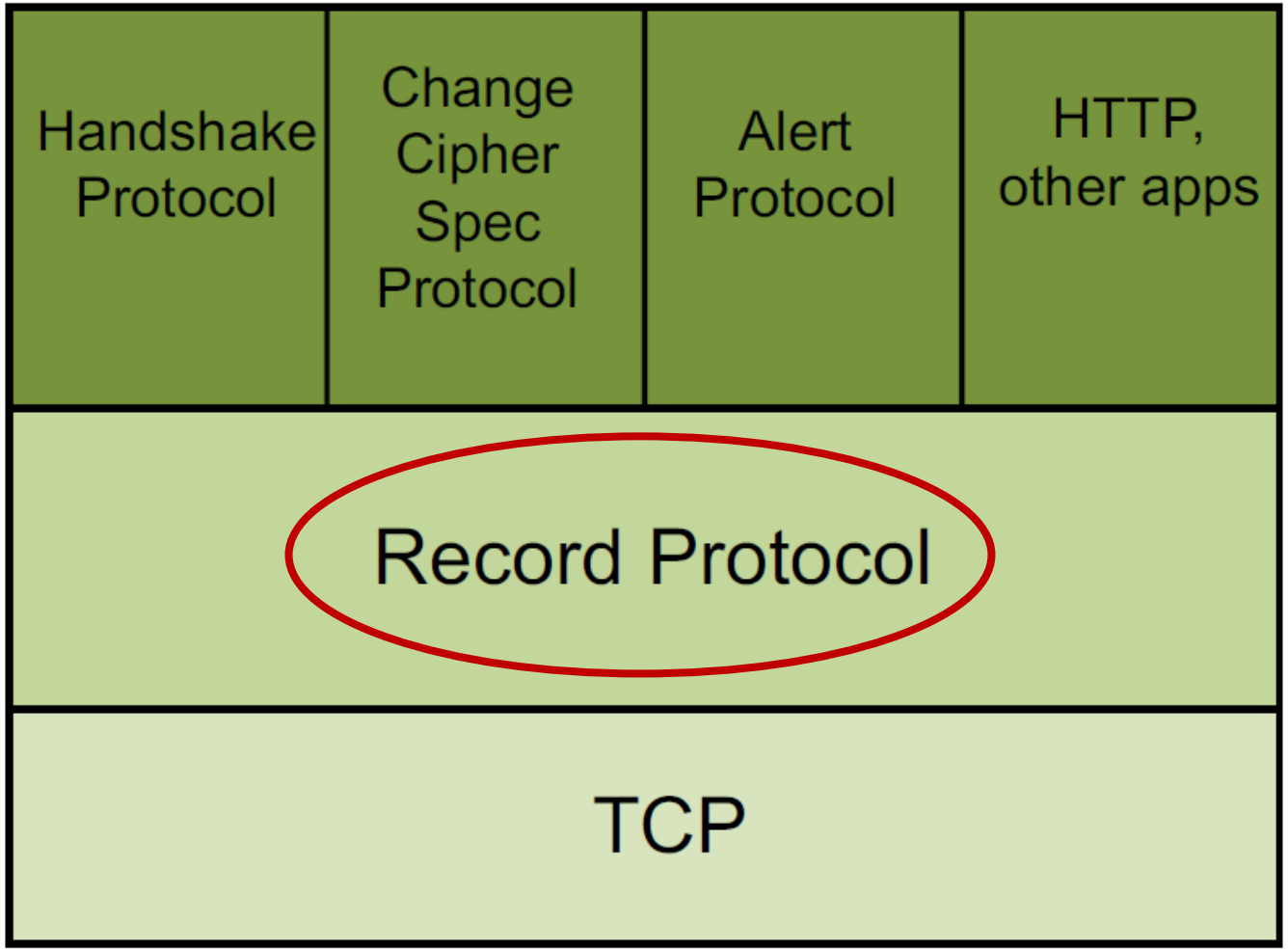
- What is network security?
- Principles of cryptography
- Authentication, message integrity
- Securing e-mail
- **Securing TCP connections: TLS**
- Network layer security: IPsec

Transport-layer security (TLS)

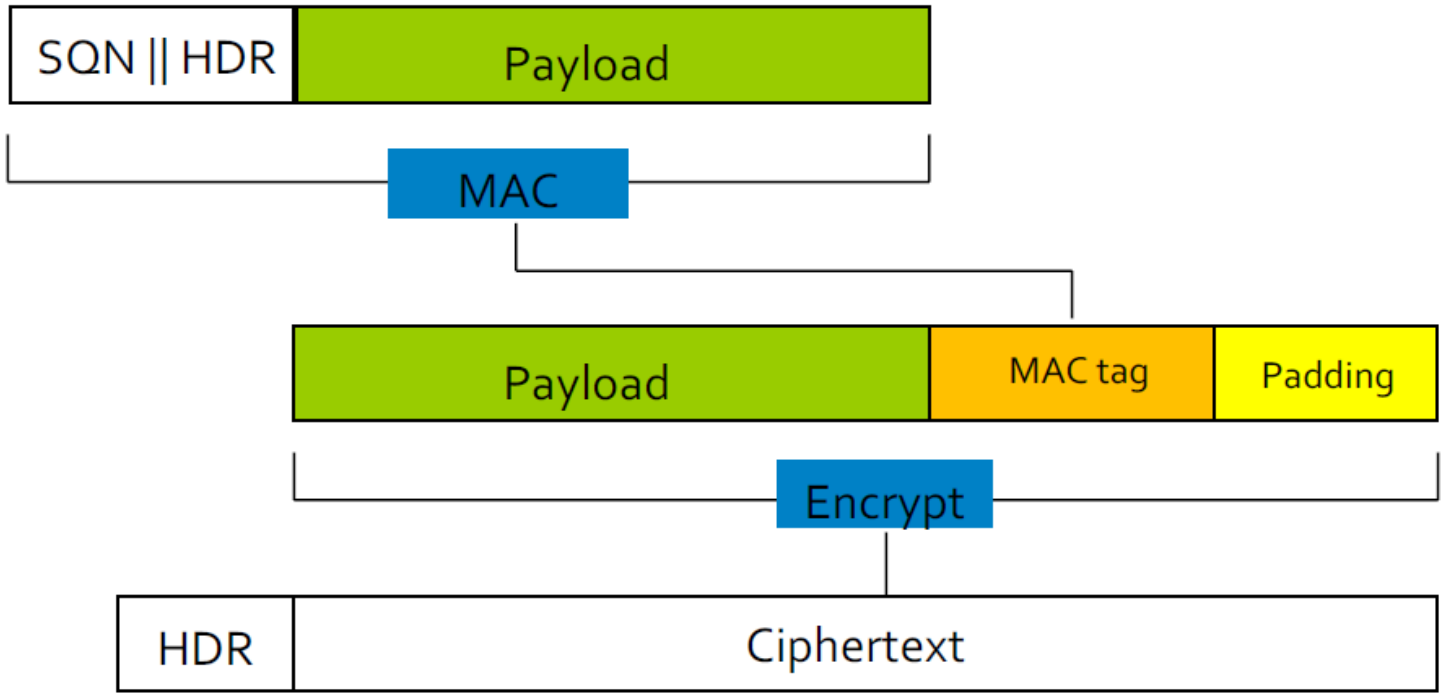
- widely deployed security protocol above the transport layer
  - supported by almost all browsers, web servers: https (port 443)
- provides:
  - confidentiality: via *symmetric encryption*
  - integrity: via *cryptographic hashing (MAC)*
  - authentication: via *public key cryptography*

} *all techniques we have studied!*

TLS Protocol Architecture



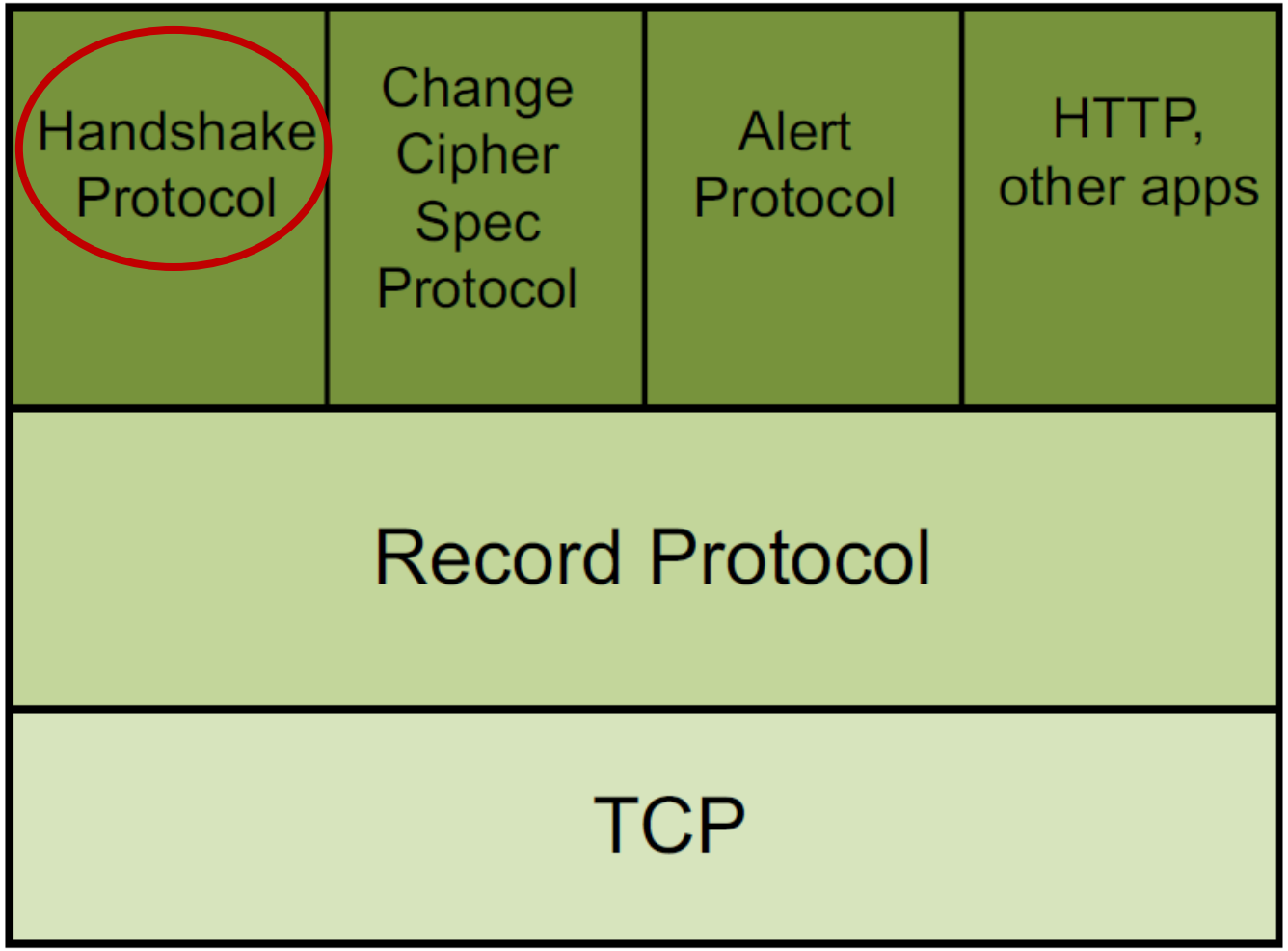
TLS Record Protocol Operation



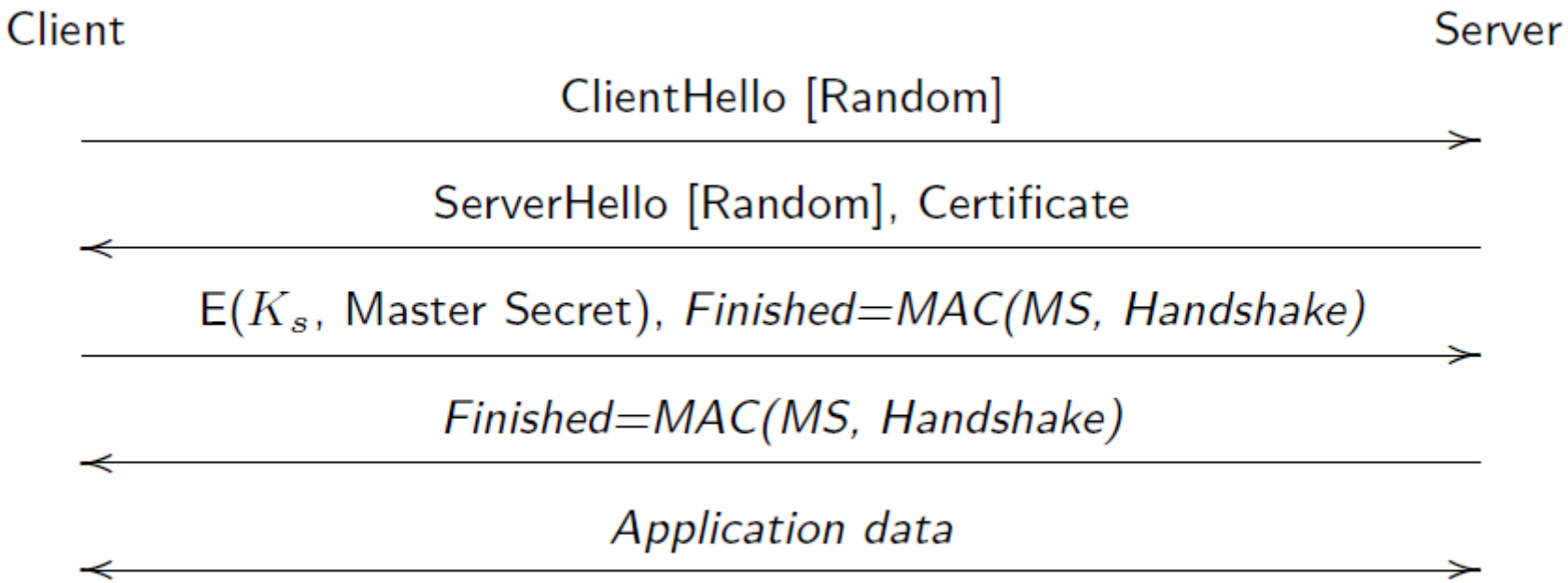
MAC HMAC-MD5, HMAC-SHA1, HMAC-SHA256,…

Encrypt CBC-AES128, CBC-AES256, CBC-3DES, RC4-128,…

TLS Protocol Architecture



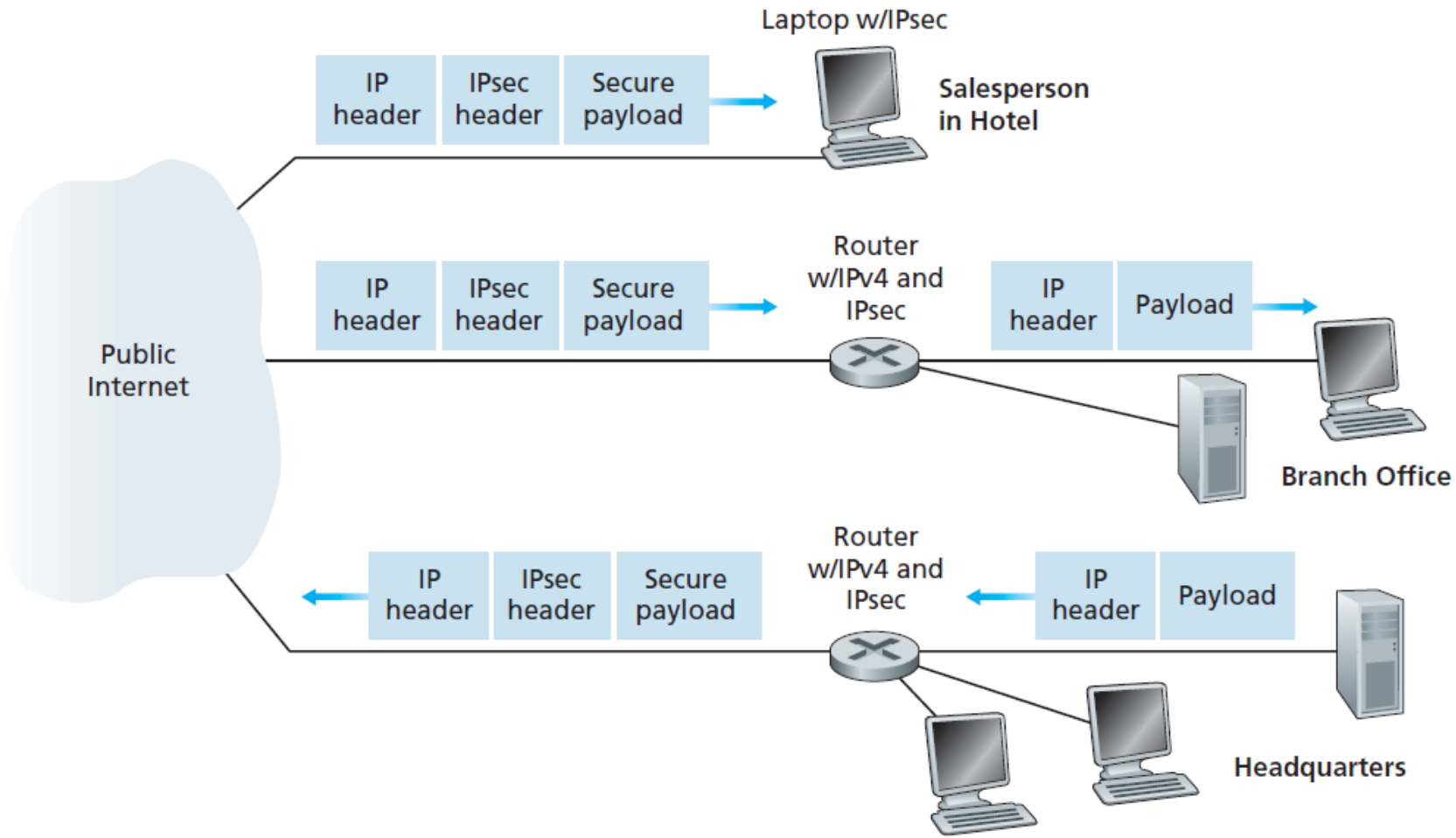
TLS 1.2: RSA Handshake Skeleton



Outline

- What is network security?
- Principles of cryptography
- Authentication, message integrity
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec

IPSec (Virtual Private Network (VPN))



Why do we need IPSec?

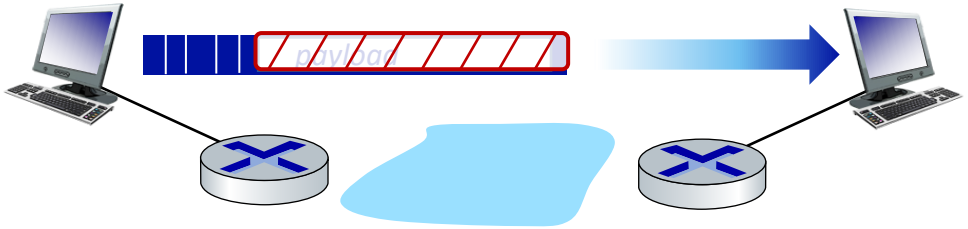
- Network-to-Network Security
  - Site-to-site VPNs use IPsec to create secure connections between different physical locations or networks, which is vital for interconnecting remote offices or data centers securely.
  - In today's interconnected world, data often traverses public or untrusted networks. IPsec is essential for securing data as it crosses these potentially insecure pathways.
- Compliance and Regulatory Requirements
  - Many industries and organizations are subject to data protection regulations that require the secure transmission of sensitive information.
- Protection Against Network Threats
  - IPsec can be a defense against various network threats, such as eavesdropping, sniffing, and packet interception.

Two IPsec protocols

- Authentication Header (AH) protocol [RFC 4302]
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP) [RFC 4303]
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

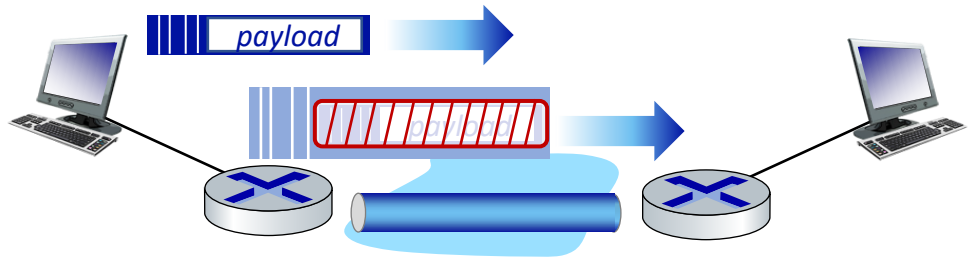
IP Sec

- provides datagram-level encryption, authentication, integrity
  - for both user traffic and control traffic (e.g., BGP, DNS messages)
- two "modes":



transport mode:

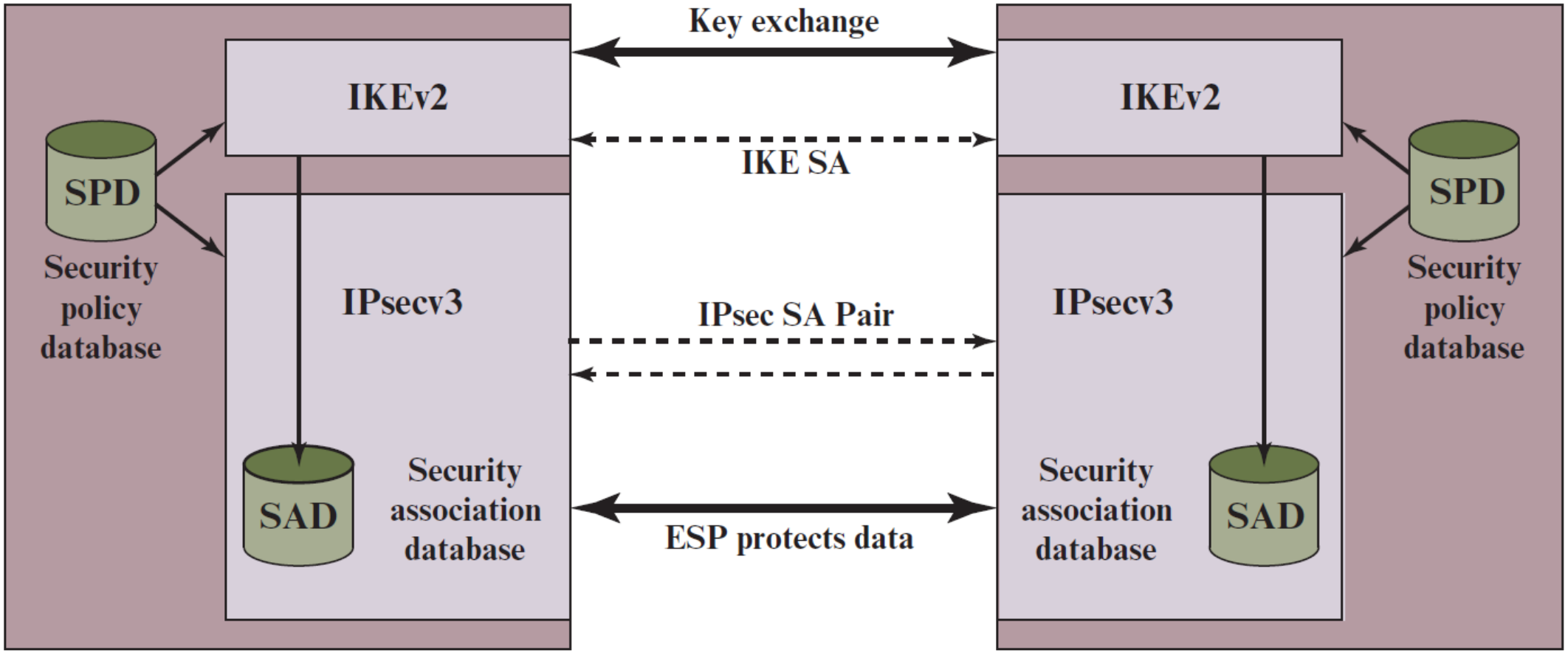
- *only* datagram *payload* is encrypted, authenticated



tunnel mode:

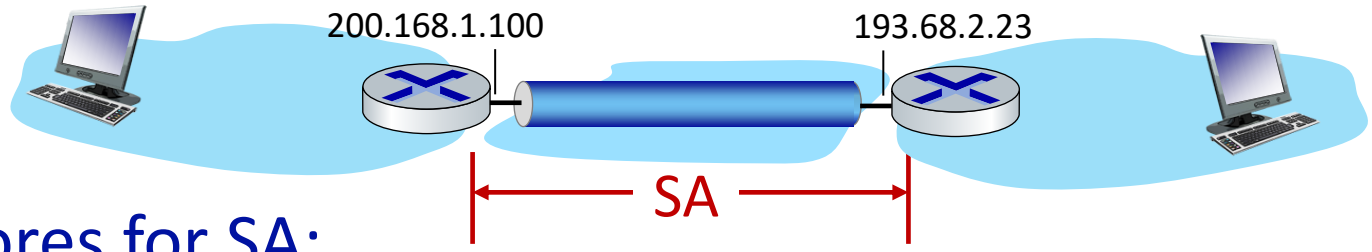
- entire datagram is encrypted, authenticated
- encrypted datagram encapsulated in new datagram with new IP header, tunneled to destination

IPsec Architecture



Security associations (SAs)

- before sending data, security association (SA) established from sending to receiving entity (directional)
  - Two security associations are required
- sending, receiving entities maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!



R1 stores for SA:

- *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used and encryption key
- type of integrity check used and authentication key
- Security Protocol Identifier

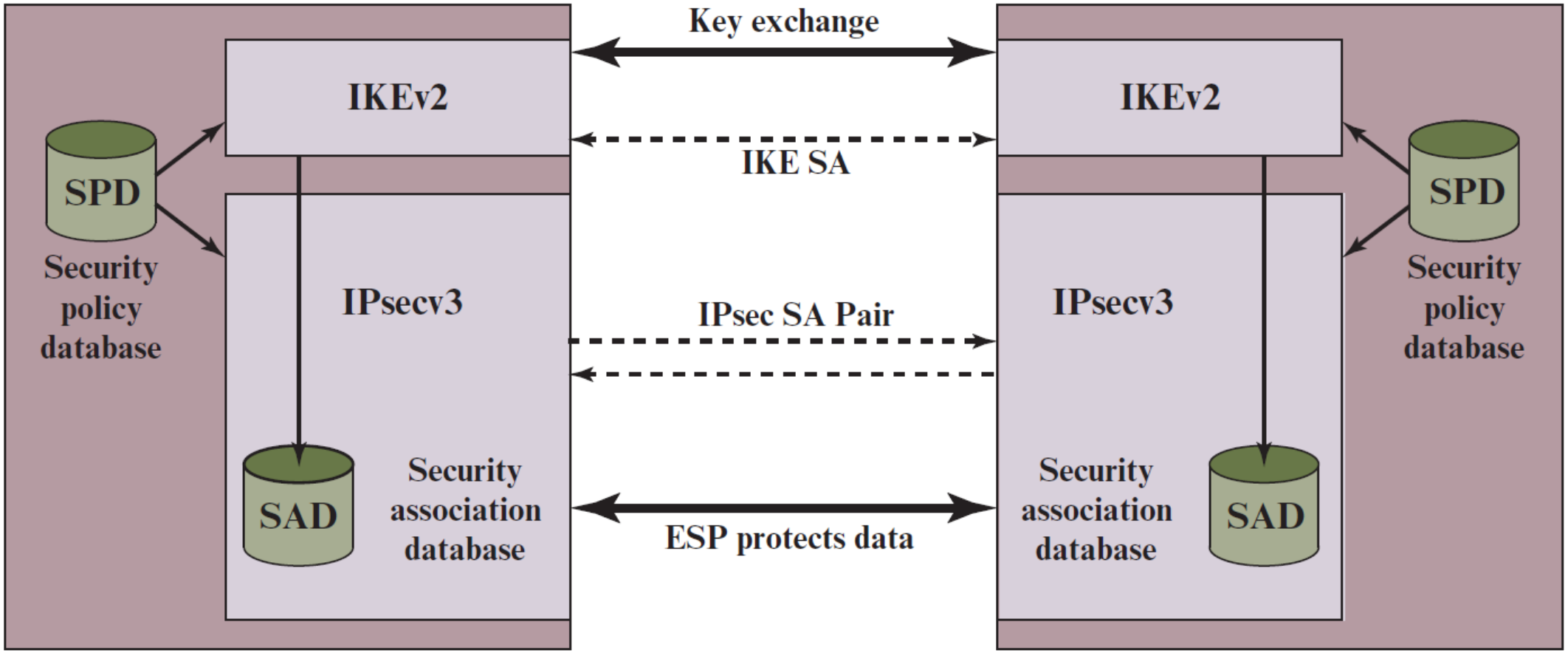
Security Associations (SAs)

- A security association is uniquely identified by three parameters.
  - Security Parameters Index (SPI)
    - A 32-bit unsigned integer assigned to SA and having local significance only.
    - The SPI is 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
    - This is the address of the destination endpoint of the SA, which 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.

Security Association Database (SAD)

- Security Association Database (SAD) defines the parameters associated with each SA, including
  - Security Parameter Index
  - Sequence Number Counter
    - A 32-bit value used to generate the Sequence Number field in AH or ESP headers
  - AH Information
  - ESP Information
    - Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP
  - IPSec Protocol Mode
    - Tunnel, transport
  - Path MTU

IPsec Architecture



Security Policy Database (SPD)

- The SPD indicates what types of datagrams (as a function of source IP address, destination IP address, and protocol type) are to be IPsec processed; and for those that are to be IPsec processed, which SA should be used.

Table 20.1 Host 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

IPsec security databases

Security Policy Database (SPD)

- policy: for given datagram, sender needs to know if it should use IP sec
- policy stored in security policy database (SPD)
- needs to know which SA to use
  - may use: source and destination IP address; protocol number

SAD: "how" to do it

Security Assoc. Database (SAD)

- endpoint holds SA state in security association database (SAD)
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, processing datagram accordingly.

SPD: "what" to do

Outbound Packets

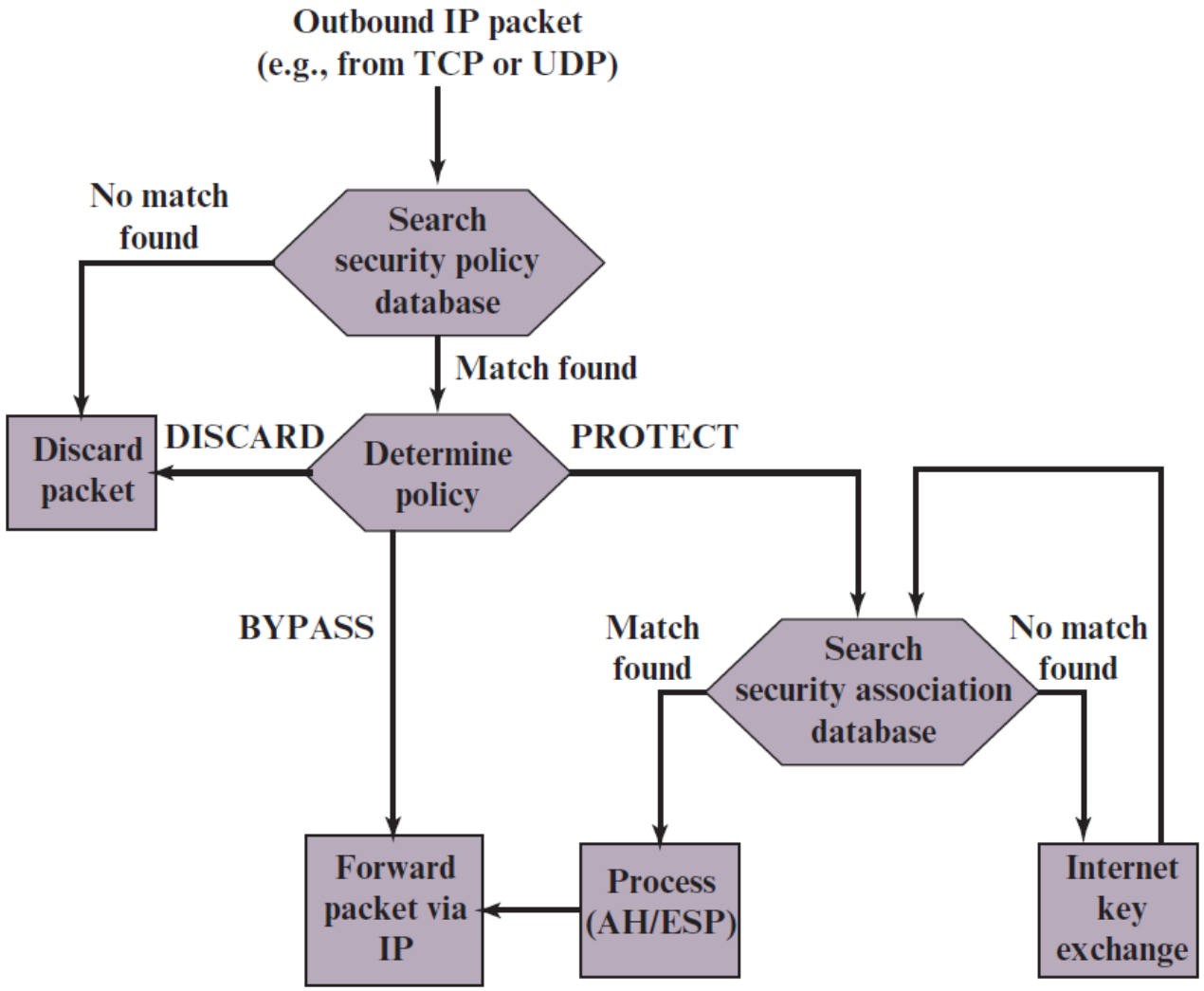


Figure 20.2 Processing Model for Outbound Packets

Inbound Packets

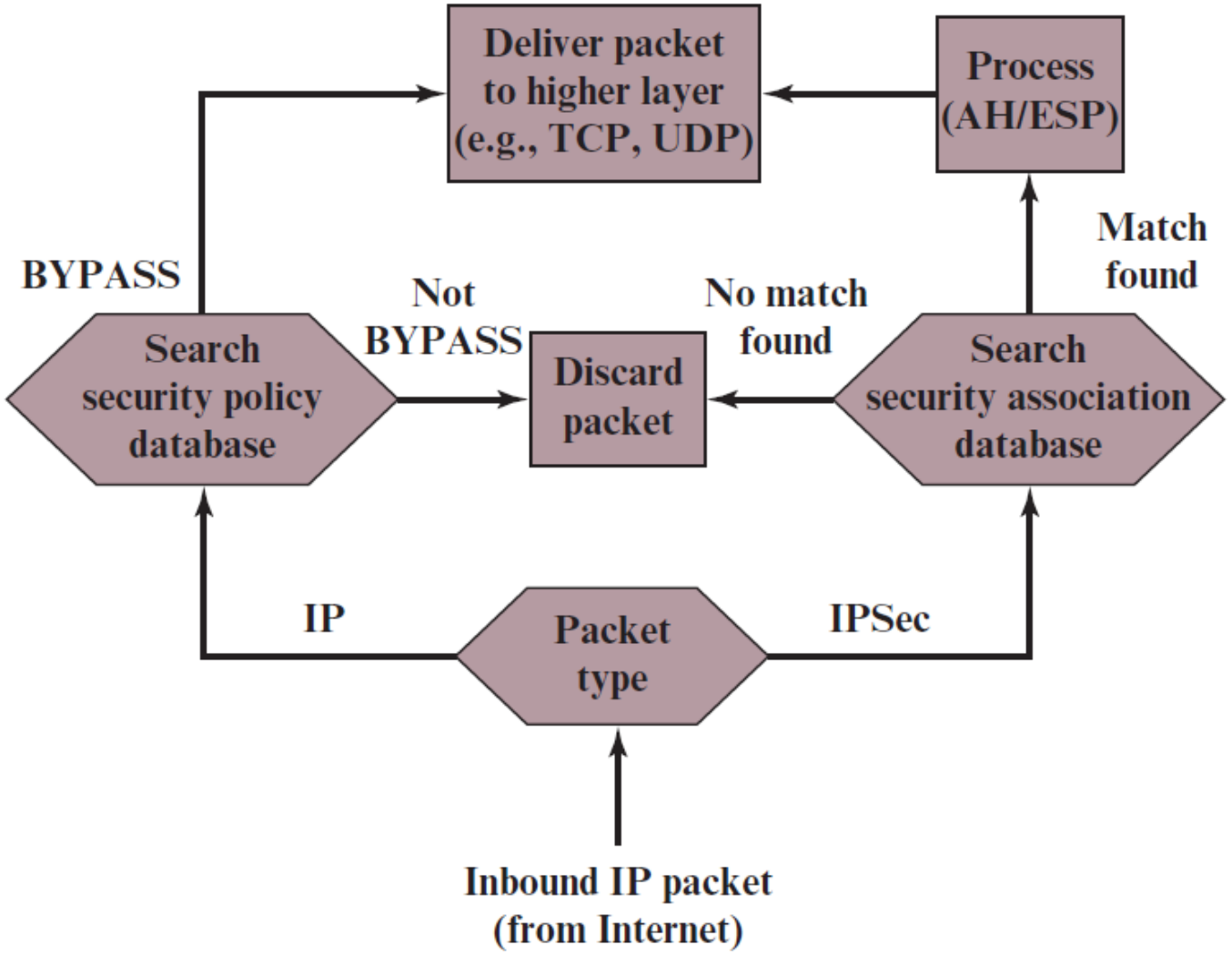


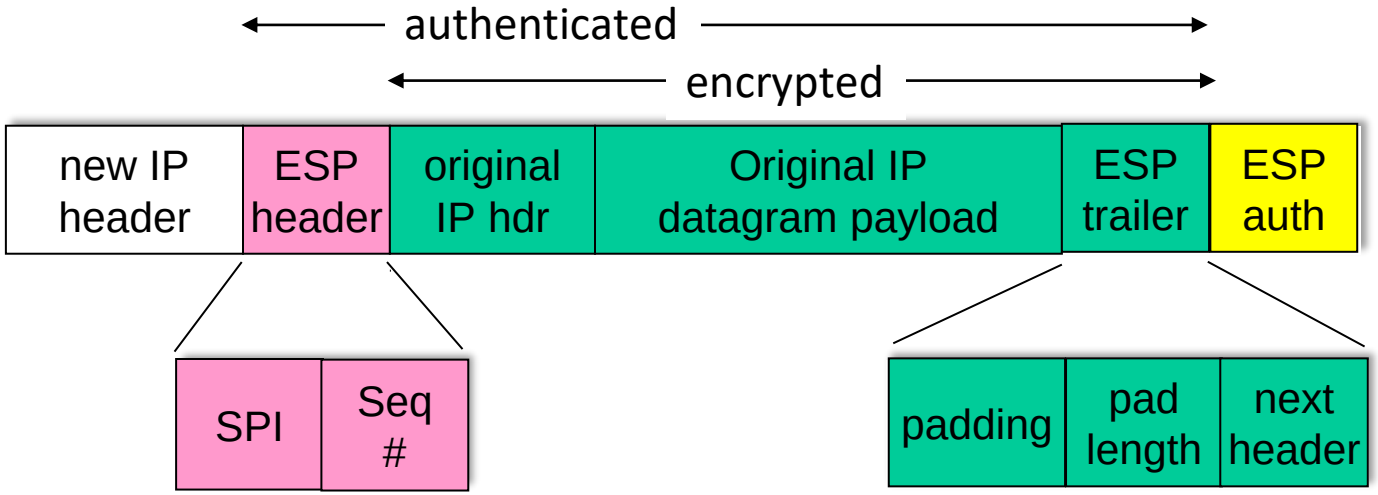
Figure 20.3 Processing Model for Inbound Packets

Encapsulating Security Payload (ESP)

- ESP can be used to provide
  - confidentiality
  - data origin authentication
  - Connectionless integrity
  - anti-replay service
  - (limited) traffic flow confidentiality.

ESP Datagram

- ESP header:
  - SPI, so receiving entity knows what to do
  - sequence number, to thwart replay attacks
- ESP trailer
  - padding for block ciphers
  - Next Header: extension header in IPv6, or an upper-layer protocol such as TCP
- MAC in ESP auth field created with shared secret key
- The MAC (ESP auth) is computed after the encryption is performed. Why?

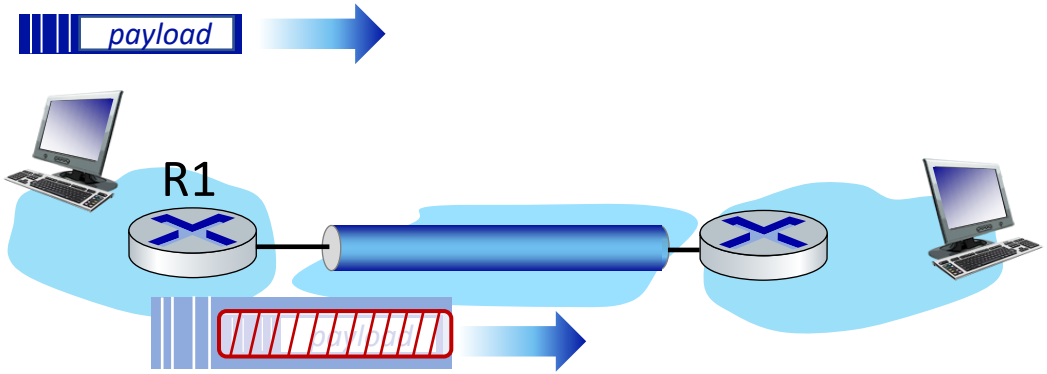


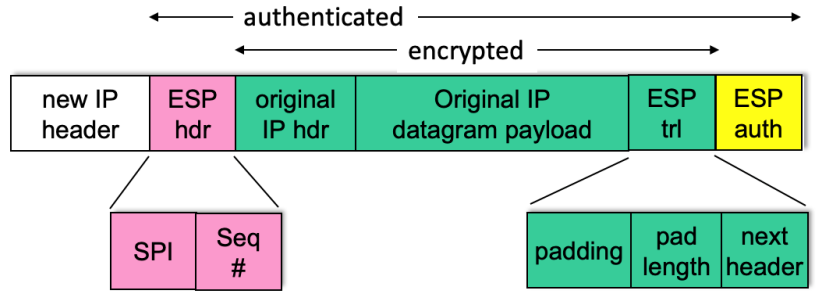
tunnel mode ESP

ESP tunnel mode: actions

at R1:

1. appends ESP trailer to original datagram (which includes original header fields!)
2. encrypts result using algorithm & key specified by SA
3. appends ESP header to front of this encrypted quantity
4. creates authentication MAC using algorithm and key specified in SA
5. appends MAC forming *payload*
6. creates new IP header, new IP header fields, addresses to tunnel endpoint





IPsec sequence numbers

- goal:
  - prevent attacker from sniffing and replaying a packet
  - receipt of duplicate, authenticated IP packets may disrupt service

- for new SA, sender initializes seq. # to 0
- each time datagram is sent on SA:
  - sender increments seq # counter
  - places value in seq # field
- method:
  - destination checks for duplicates
  - doesn't keep track of *all* received packets; instead uses a window

IPsec sequence numbers

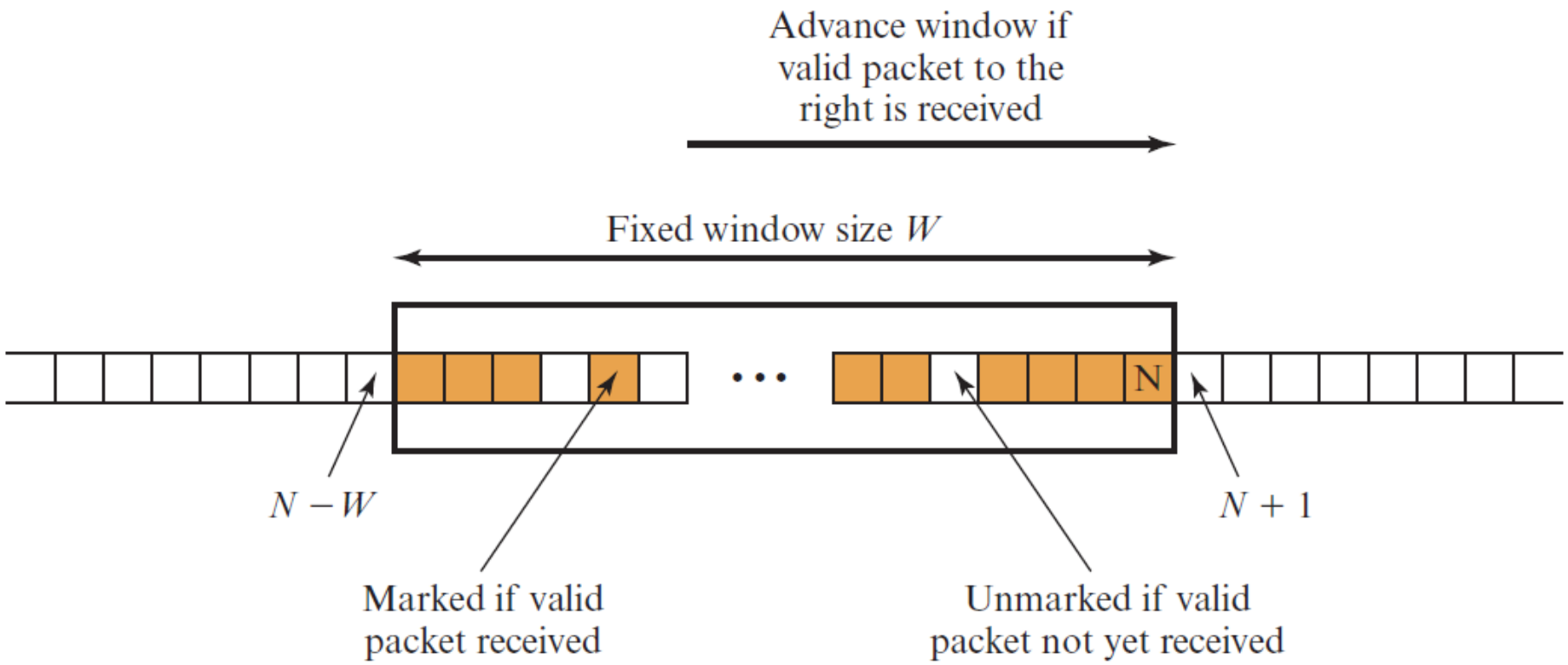
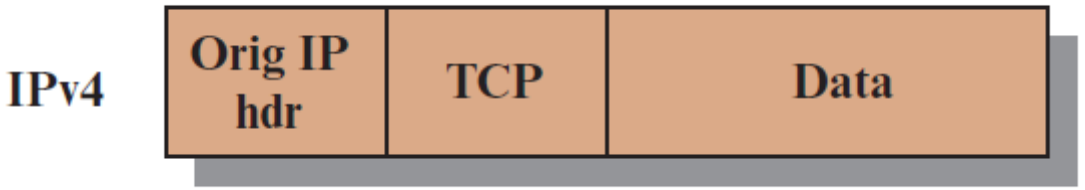


Figure 20.5 Anti-replay Mechanism

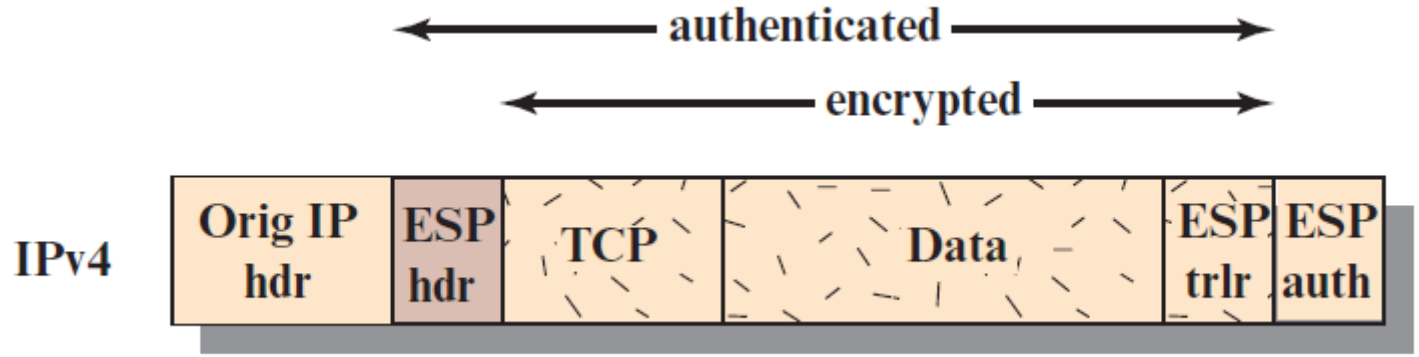
Transport Mode ESP

- Typically, transport mode is used for end-to end communication between two hosts.

Original IP datagram



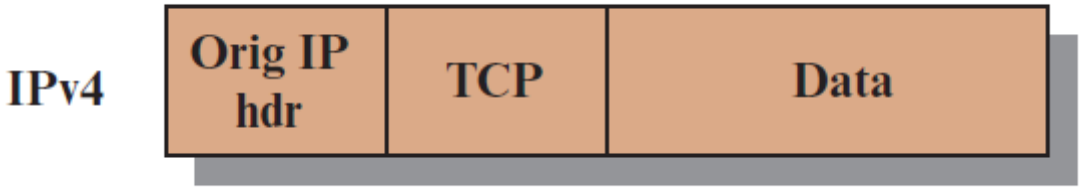
Transport mode ESP



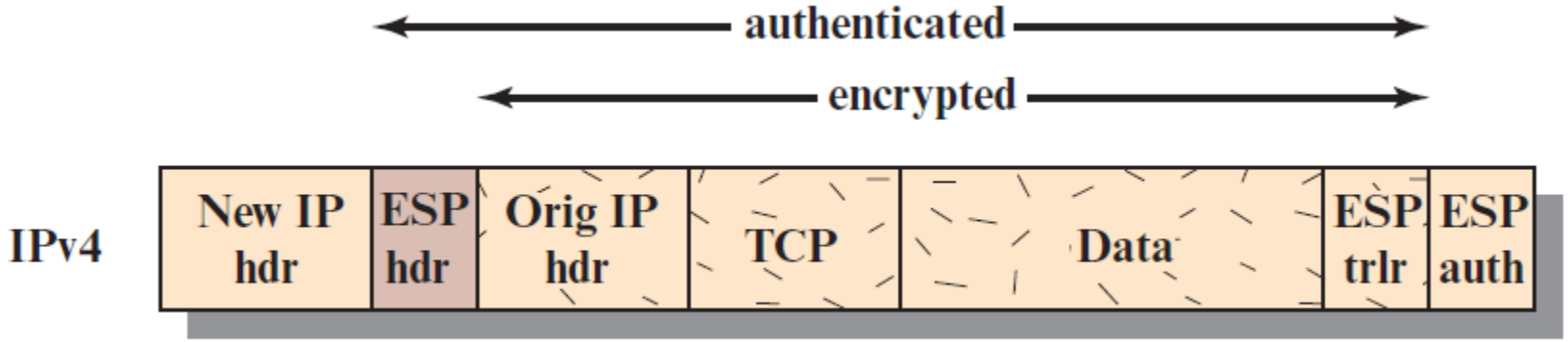
Tunnel Mode ESP

- Tunnel mode is used when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec.
  - Tunnel mode can be used to implement a secure Virtual Private Network (VPN).

Original IP datagram



Tunnel mode ESP



Example of Virtual Private Network Implemented with IPsec Tunnel Mode

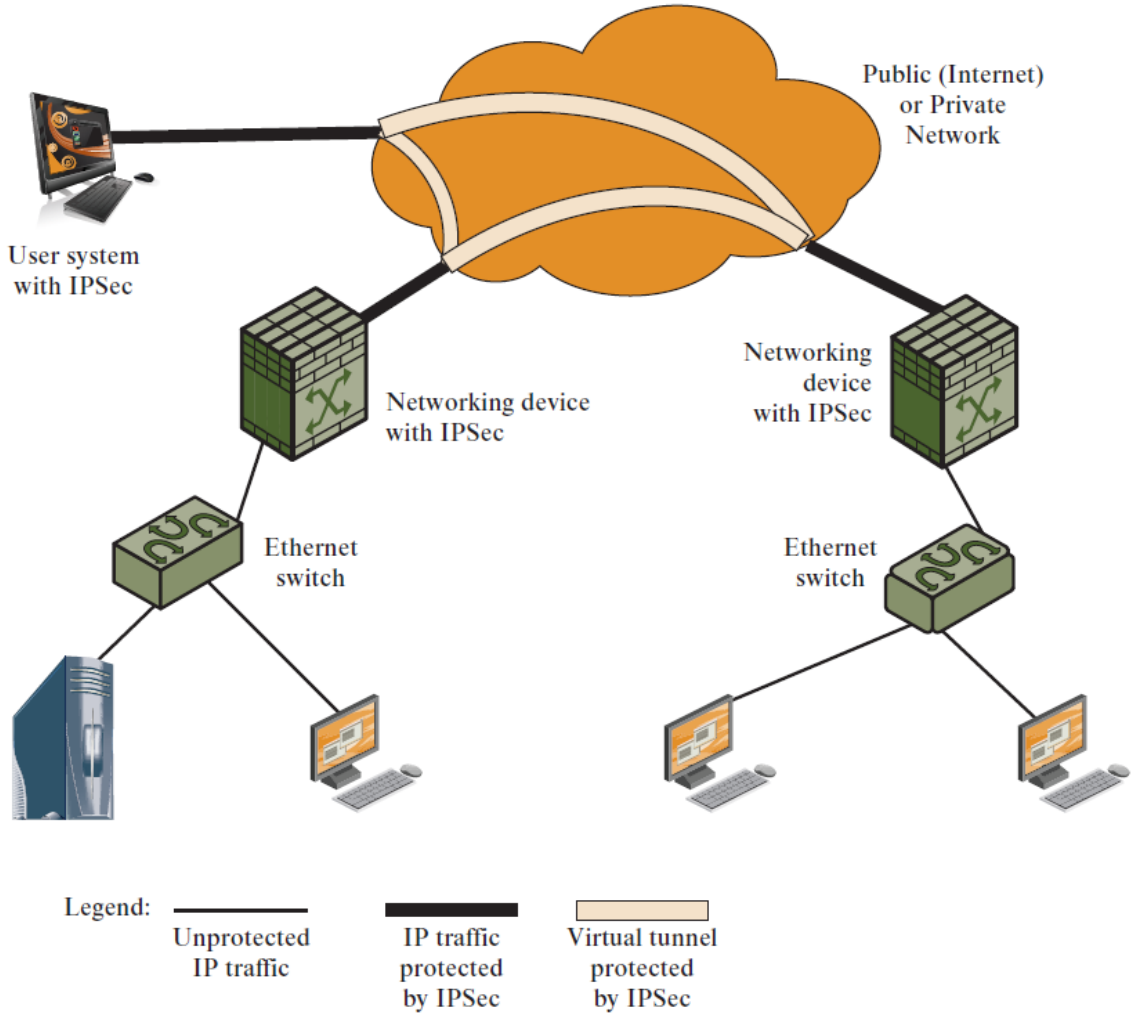


Figure 20.8 Example of Virtual Private Network Implemented with IPsec Tunnel Mode

Tunnel Mode 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.

NO Authentication

Our Focus

IKE: Internet Key Exchange

- *previous examples:* manual establishment of IPsec SAs in IPsec endpoints:

  Example SA:

  SPI: 12345
  Source IP: 200.168.1.100
  Dest IP: 193.68.2.23
  Protocol: ESP
  Encryption algorithm: 3DES-cbc
  HMAC algorithm: MD5
  Encryption key: 0x7aeaca…
  HMAC key:0xc0291f…

- manual keying is impractical for VPN with 100s of endpoints
- instead use IPsec IKE (Internet Key Exchange)

IKE: PSK and PKI

- authentication (prove who you are) with either
  - pre-shared secret (PSK) or
  - with PKI (pubic/private keys and certificates).
- PSK: both sides start with secret
  - run IKE to authenticate each other and to generate IPsec SAs (one in each direction), including encryption, authentication keys
- PKI: both sides start with public/private key pair, certificate
  - run IKE to authenticate each other, obtain IPsec SAs (one in each direction).
  - similar with handshake in SSL.

IKE phases

- IKE has two phases
  - *Oakley Key Determination Protocol:* establish bi-directional IKE SA
    note: IKE SA different from IPsec SA
  - *Internet Security Association and Key Management Protocol (ISAKMP)* is used to securely negotiate IPsec pair of SAs

References

- Kurose, James F., and Keith W. Ross. "Computer networking: A top-down approach edition." Addision Wesley (2007), chapter 8.
- Cryptography and Network Security: Principles and Practice, William Stallings, Pearson, 2022.