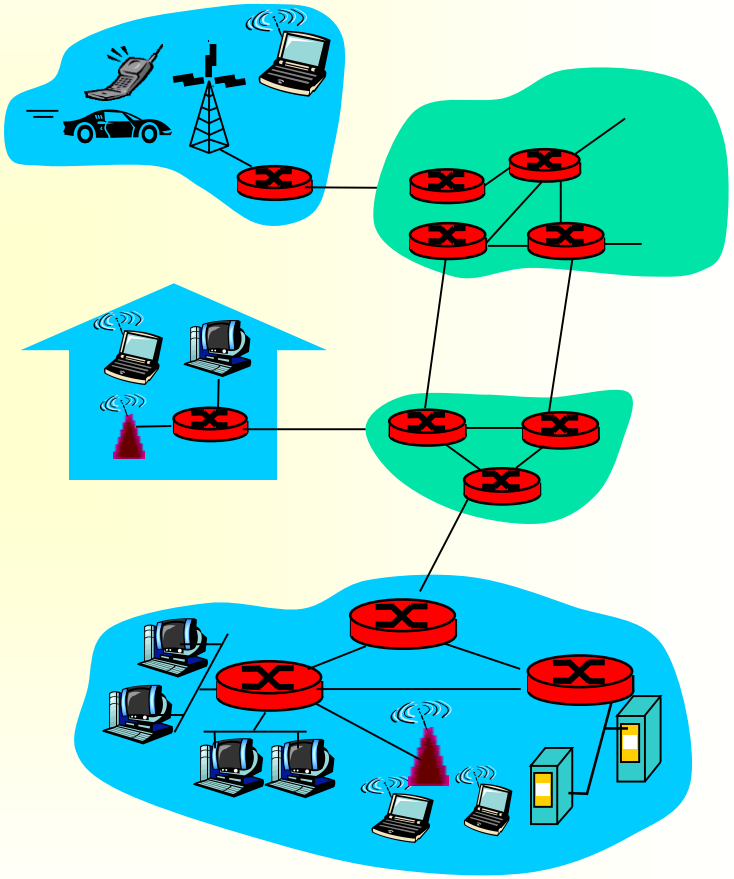
Chapter 4 – Network Security Concepts and Mechanisms

4.1 Introduction

A closer look at the network structure of the Internet

- Three broad components
  - The Network Edge
    - Consists of applications and hosts
  - Access Networks
    - Connect end systems to edge routers through wired or wireless communication links
  - Network Core
    - Interconnected routers creating network of networks



Internet View of Networking

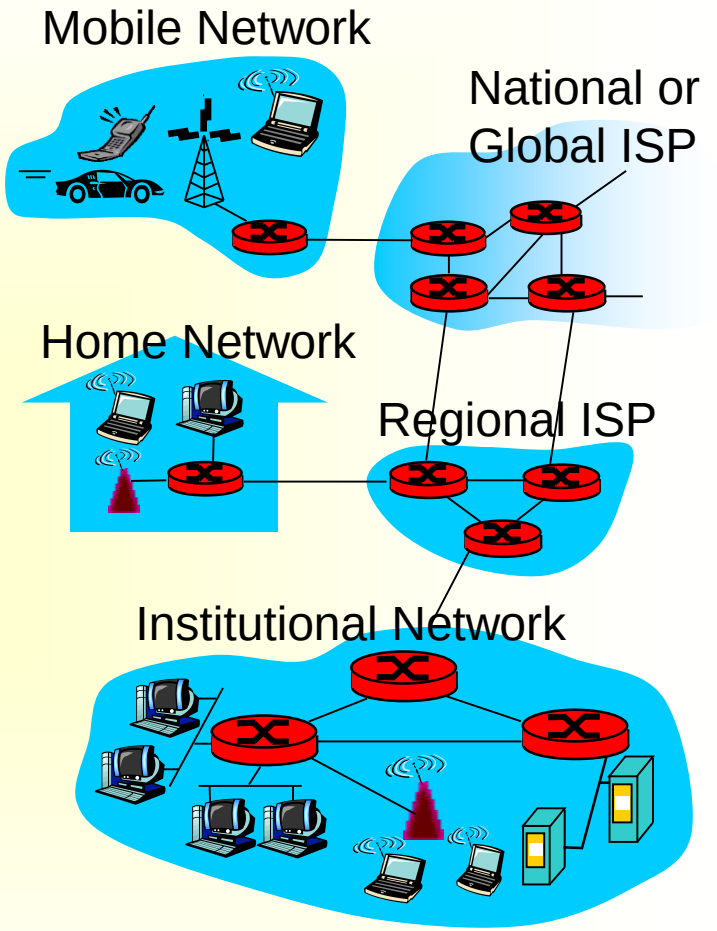
PC

Server

Wireless laptop

Cell phone

- Millions of connected computing devices: hosts (end systems) running network applications



Access points

Wired links

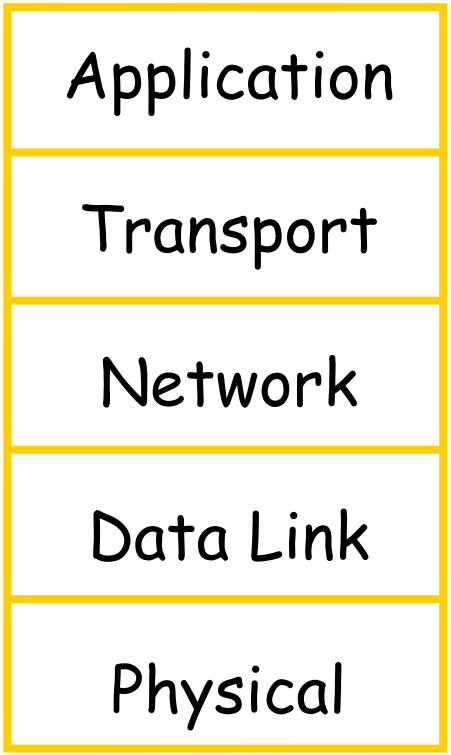
- Communication links
  - Fiber, copper, radio, satellite
  - Transmission rate = bandwidth

Router/Switch

- Routers: forward packets (chunks of data)

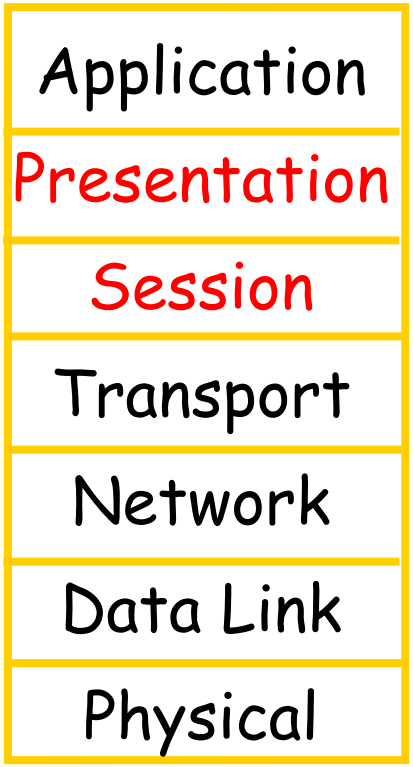
- Protocols control the sending and receiving of messages
  - e.g., TCP, IP, HTTP, Skype, Ethernet
- Internet Protocol Stack (TCP/IP)
  - Application: supports network applications
    - e.g., FTP, SMTP, HTTP
  - Transport: process-to-process data transfer and end-to-end reliability
    - e.g., TCP, UDP
  - Network: routing of datagrams (packets) from source to destination
    - e.g., IP, routing protocols
  - Data Link: reliable data transfer between neighboring network elements
    - e.g., PPP, ARP, Ethernet
  - Physical: bits “on the wire or in the air”

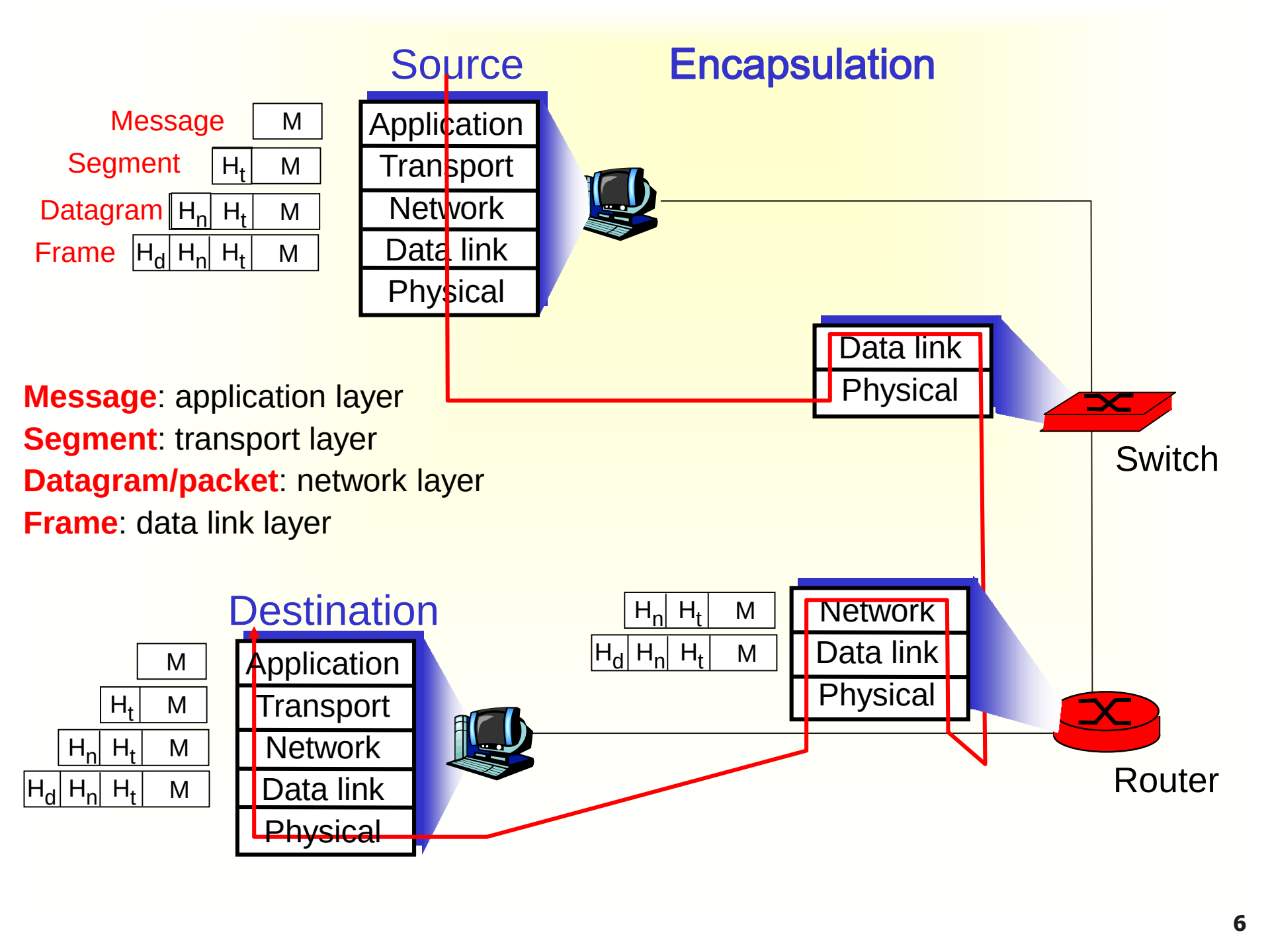
Layers of TCP/IP



- ISO/OSI Reference Model
  - Presentation: allows applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
  - Session: managing sessions such as synchronization, check pointing, recovery of data exchange
  - Internet protocol stack "missing" these layers!
    - These services, if needed, must be implemented in the application layer
  - OSI has never been fully implemented but serves as a good theoretical model

Layers of ISO/OSI



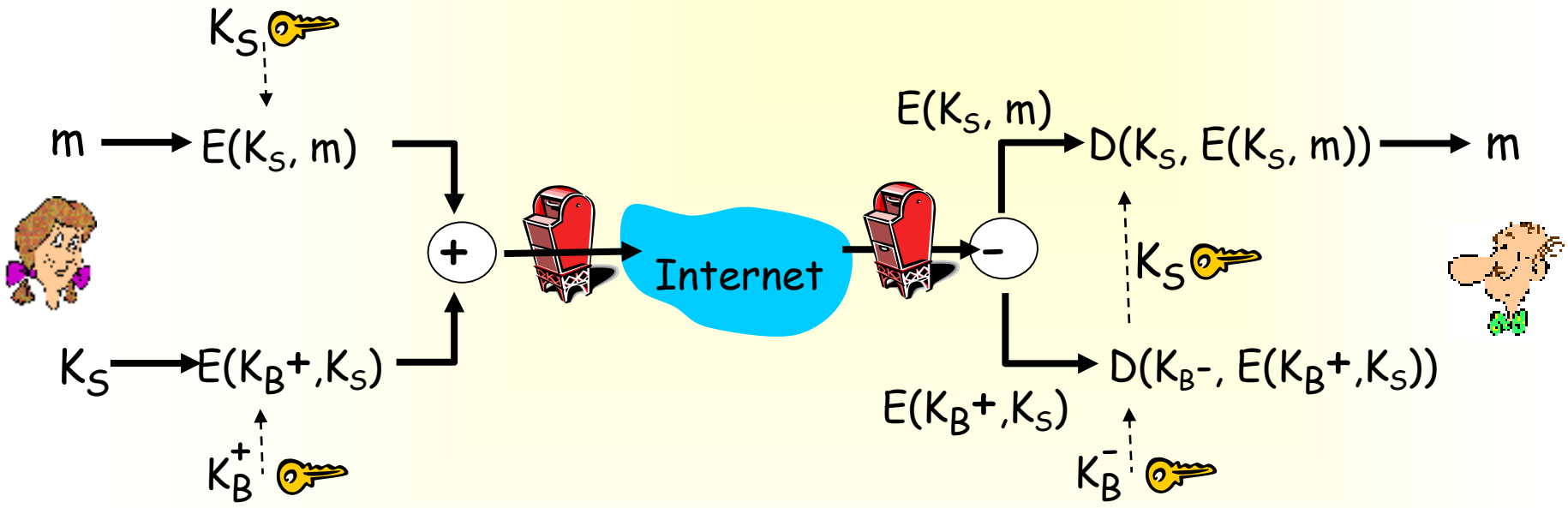

Source
Encapsulation
Message
M
Segment
H_t M
Datagram
H_n H_t M
Frame
H_d H_n H_t M
Application
Transport
Network
Data link
Physical
Data link
Physical
Switch
Message: application layer
Segment: transport layer
Datagram/packet: network layer
Frame: data link layer
Destination
M
H_t M
H_n H_t M
H_d H_n H_t M
Application
Transport
Network
Data link
Physical
H_n H_t M
H_d H_n H_t M
Network
Data link
Physical
Router

- What can “bad guys” do on Networking?
  - Eavesdrop: intercept messages
  - Insert messages into a connection
  - Impersonation: can fake (spoof) source address in packet (or any field in packet)
  - Session Hijacking: “take over” ongoing connection by removing sender or receiver, inserting itself in place
    - The attacker monitors an authenticated session between the client machine and the server, and takes that session over
    - When a TCP connection is established between a client and a server, all information is transmitted in clear and this can be exploited to hijack the session
  - Denial of Service: prevent service from being used by others

4.2 What is Network Security?

- Confidentiality: only sender and intended receiver should "understand" message contents
  - sender encrypts message
  - receiver decrypts message
- Authentication: sender and receiver want to confirm identity of each other
- Message integrity: sender or receiver wants to ensure message is not altered (in transit, or afterwards) without detection
- Access and availability: services must be accessible and available to users

- Network Security: Example
  - Alice wants to send confidential message m to Bob



Alice:

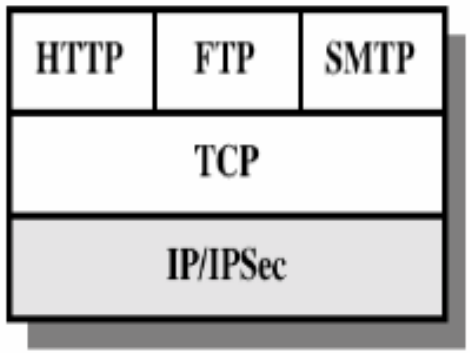
- Generates random *symmetric* key, K_S
- Encrypts message with K_S (symmetric encryption is more efficient)
- Also encrypts K_S with Bob's public key
- Sends both to Bob

Bob:

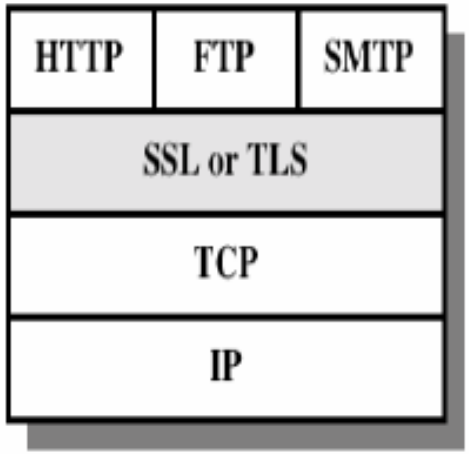
- Uses his private key to decrypt and recover K_S
- Uses K_S to decrypt and recover m

- In today's highly networked world, we can't talk of computer security without talking of network security
- Although there are many types of networks, the focus is this course is on
  - Internet and intranet security (TCP/IP based networks)
  - Attacks that use security holes of the network protocols and their defenses
- We do not discuss attacks that use networks to perform some crime based on human weaknesses (such as scams)

Security Features in the TCP/IP Protocol Stack

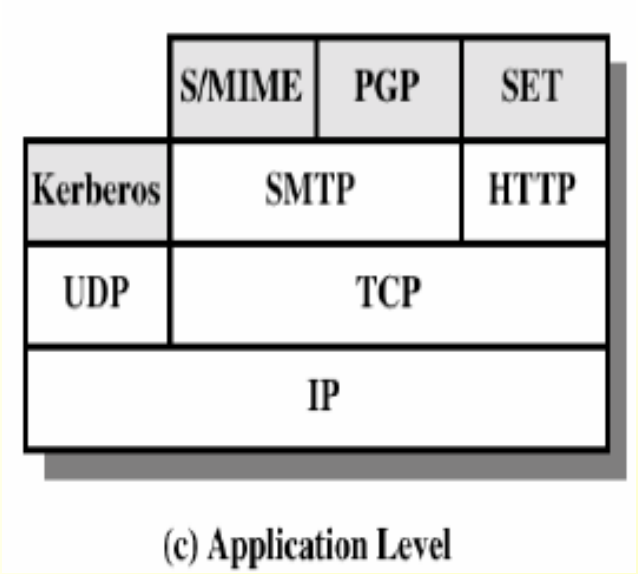


(a) Network Level



(b) Transport Level

- Use of IP Security (IPSec) (Figure a)
  - Transparent to applications
  - Provides general purpose solution
  - Provides filtering capability (rejection of replayed packets)
- Security just above TCP (Figure b)
  - SSL: Secure Sockets Layer
  - TLS: Transport Layer Security
  - SSL/TLS could be provided as part of the underlying protocol suite $\Rightarrow$ Transparent to applications
  - Alternatively, can be embedded into applications
    - Example: Microsoft Explorer is equipped with SSL



(c) Application Level

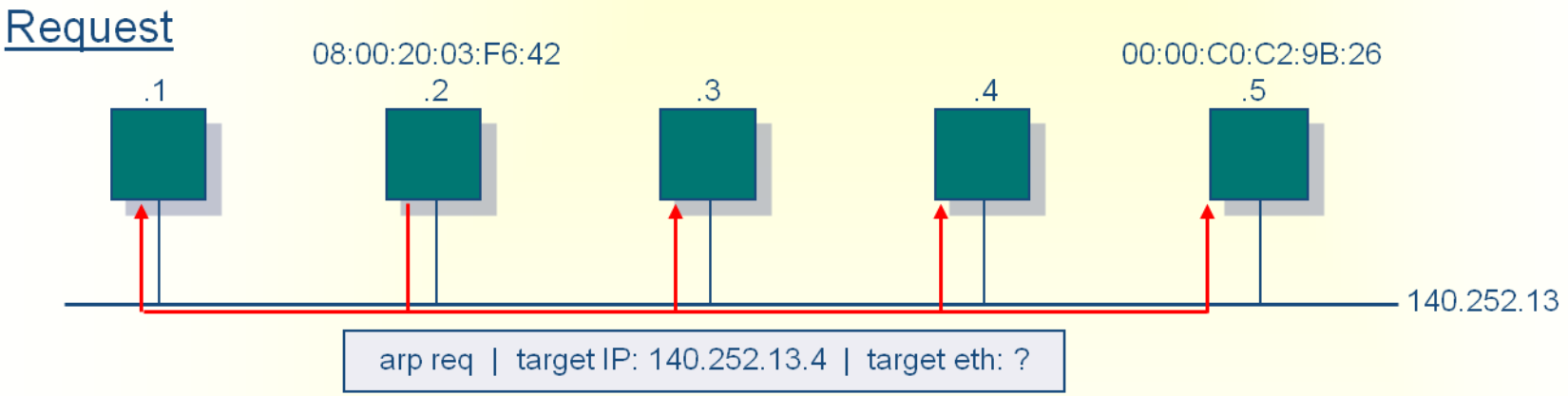
- Application specific security services (Figure c)
  - Embedded within specific applications
  - Examples are
    - Electronic mail - S/MIME (Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) on SMTP (Simple Mail Transfer Protocol)
    - SET (Secure Electronic Transaction) on top of HTTP
    - Client/server – Kerberos

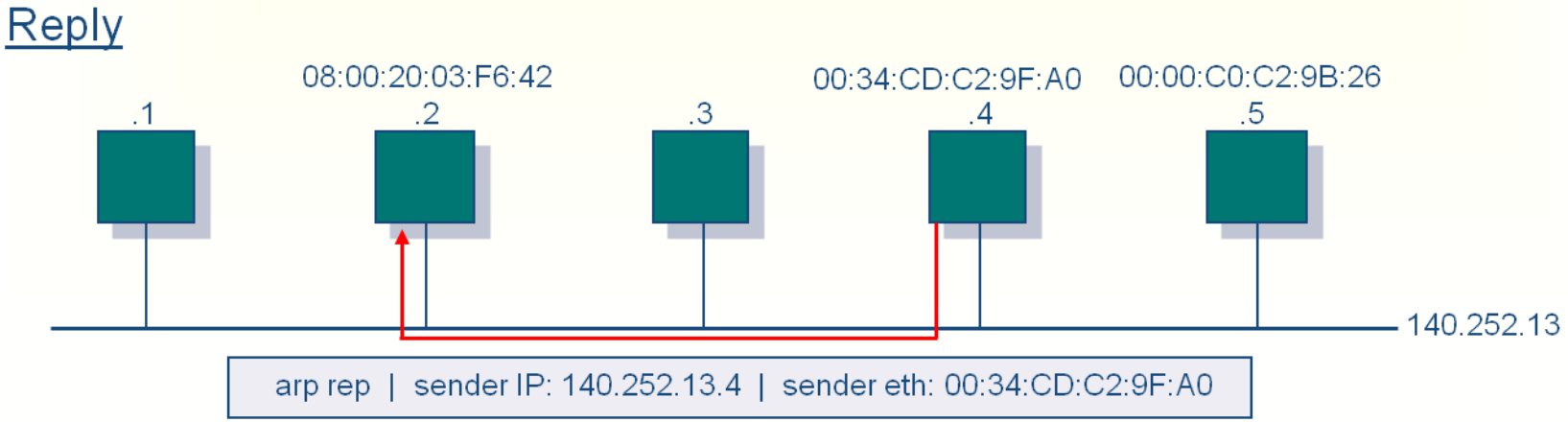
4.3 Network Protocols and Vulnerabilities

- Attacks on TCP/IP Networks
  - The Internet was not originally designed with (much) security in mind
    - It was designed to be used by a trusted group of users
    - *Original vision:* "a group of mutually trusting users attached to a transparent network" ☺, i.e., there is no need for security
  - The protocols are not designed to withstand attacks
  - Internet is now used by all sorts of people
  - Attackers exploit vulnerabilities of every protocol to achieve their goals
  - Hence, security consideration in all layers is important!

4.3.1 Link Layer: ARP Spoofing

- How does ARP work?
  - A computer that wants to access another computer for which it knows its IP address broadcasts this address
  - The owner responds by sending its Ethernet (MAC) address





- ARP Spoofing (also called ARP cache poisoning or ARP poison routing) is a link layer attack
- It is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network
- The aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead
- ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic
- Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks

- How does it happen?
  - Because ARP is a stateless protocol
  - Hosts will automatically cache any ARP replies they receive, regardless of whether they requested them. Even ARP entries which have not yet expired will be overwritten when a new ARP reply packet is received
  - There is no method in the ARP protocol by which a host can authenticate the peer from which the packet originated
  - This behavior is the vulnerability which allows ARP spoofing to occur

4.3.2 Network Layer Security: IPSec

- IP is vulnerable
- IP packets can be intercepted
  - In the LAN broadcast
  - In the router, switch
- Since the packets are not protected they can be easily read
- Since IP packets are not authenticated they can be easily modified
- Even if the user encrypts his/her data it will still be vulnerable to traffic analysis attack
- Information exchanged between routers to maintain their routing tables is not authenticated
  - All sorts of problems can happen if a router is compromised

- IP Security (IPSec) Overview
  - There are application-specific security mechanisms for a number of application areas (slide 12)
  - However, security concerns cut across protocol layers
  - By implementing security at the IP (network) layer, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications
  - IPSec provides
    - Origin authentication (to overcome IP Spoofing)
    - Confidentiality
    - Message integrity
    - Replay detection
    - Key management

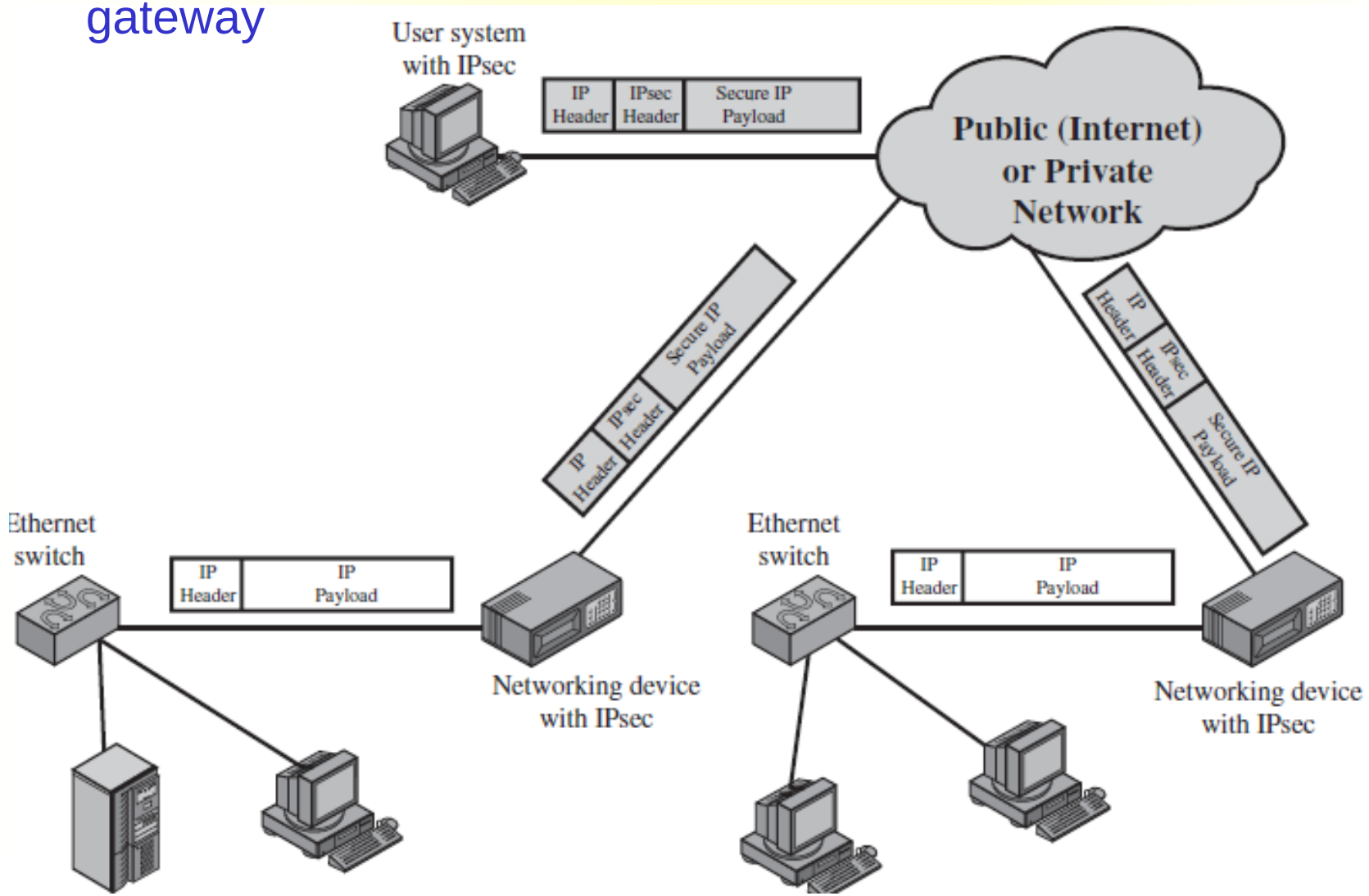
    all at the level of IP packets

- Origin authentication (assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header and the packet has not been altered in transit - message integrity); IP-level authentication is provided by inserting an Authentication Header (AH) into the packets
  - AH also provides anti-replay services
- Confidentiality (encrypts messages to prevent eavesdropping by third parties); IP-level confidentiality is provided by inserting an Encapsulated Security Payload (ESP) header into the packets. An ESP header can also do the job of the AH header in addition to confidentiality – ESP is more complicated and requires more processing time
- Key management (concerned with the secure exchange of keys); Before ESP can be used, it is necessary for the two ends of a communication link to exchange the secret key that will be used for encryption. Similarly, AH needs an authentication key; Keys are exchanged with a protocol called Internet Key Exchange (IKE)
- Note: the use of encryption always means the need for key management

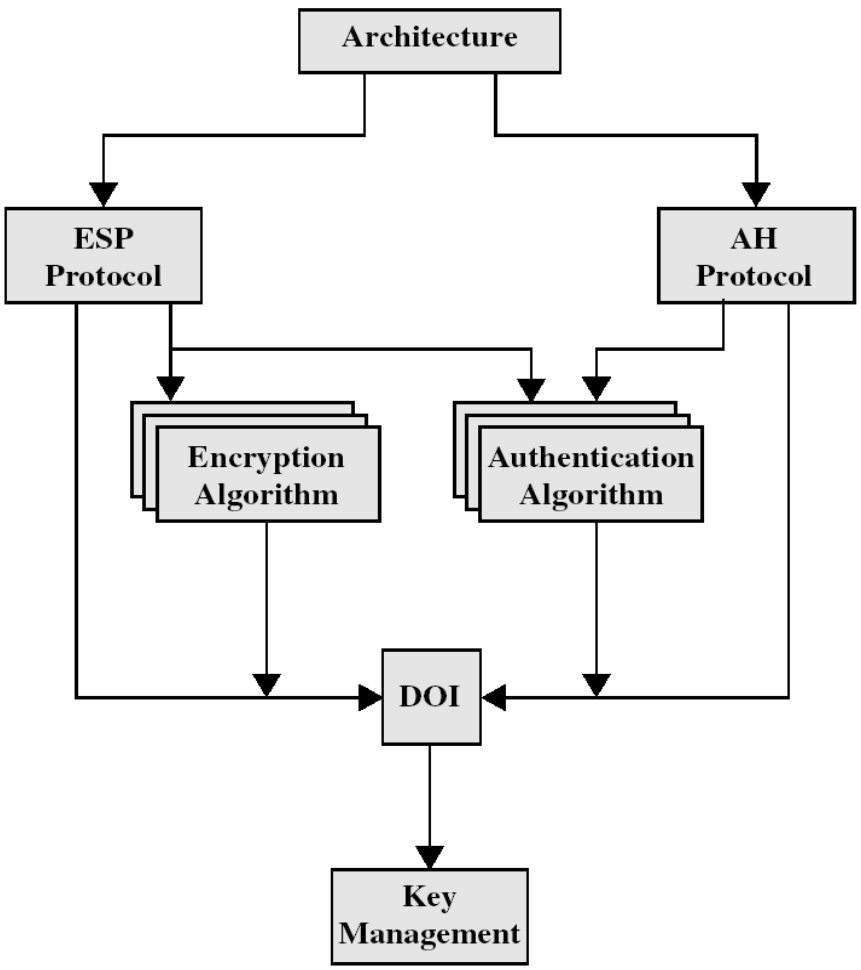
- IPSec is a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication
- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet
  - Secure branch office connectivity over the Internet (secure Virtual Private Network over the Internet or over a public WAN)
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism
  - Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security

- Benefits of IPSec
  - It is transparent to applications since it is below the transport layer (TCP, UDP): There is no need to change software on a user or server system when IPSec is implemented in the firewall or router
  - IPSec can be transparent to end users
  - Provides security for individual users
- In addition to supporting end users and protecting premises systems and networks, IPSec has a role in routing. It assures that
  - A router advertisement (a new router advertises its presence) comes from an authorized router
  - A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router
  - A redirect message comes from the router to which the initial IP packet was sent
  - A routing update is not forged

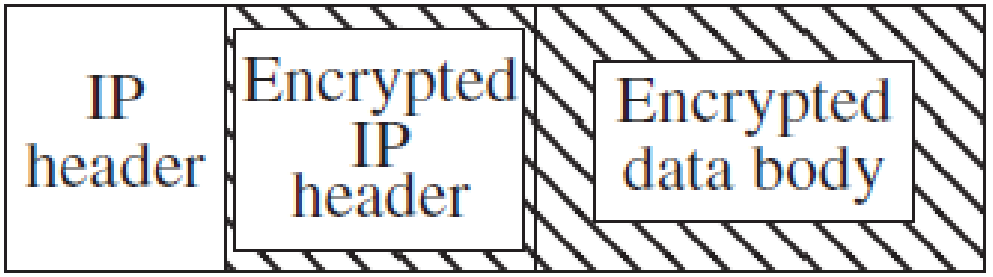
- IP Security Scenario
  - A message passes through intermediate hosts. If the IPSec mechanisms reside on an intermediate host (for example, a router, a firewall or gateway), that host is called a security gateway



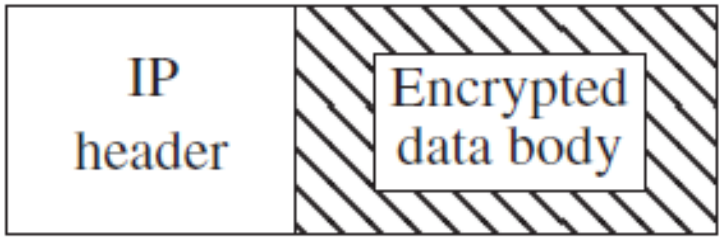
- Components of the IPSec security architecture
  - Two protocols provide message security: ESP and AH
  - Encryption and Authentication Algorithms
  - DOI: Domain of Interpretation: identifiers for approved algorithms, operational parameters like key lifetime
  - Key Management: The distribution of cryptographic keys for use with the security protocols (namely, the Internet Key Exchange, or IKE)



- IPSec can operate in two modes (for both AH and ESP)
  - Tunnel mode
    - Used to tunnel IP traffic between two security gateways, i.e., when either or both endpoints do not support IPSec but two intermediate hosts do
    - It protects the full IP datagram, including the IP header



  - Transport mode
    - Used when both endpoints support IPSec to provide security services for upper layer protocols such as TCP or UDP segments or an ICMP packet
    - The IP header is not protected

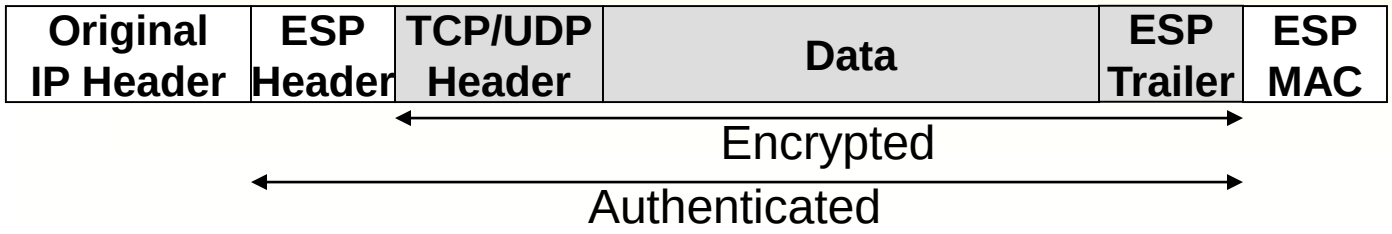


- Transport Mode ESP
  - Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP

    Original IPv4 Packet

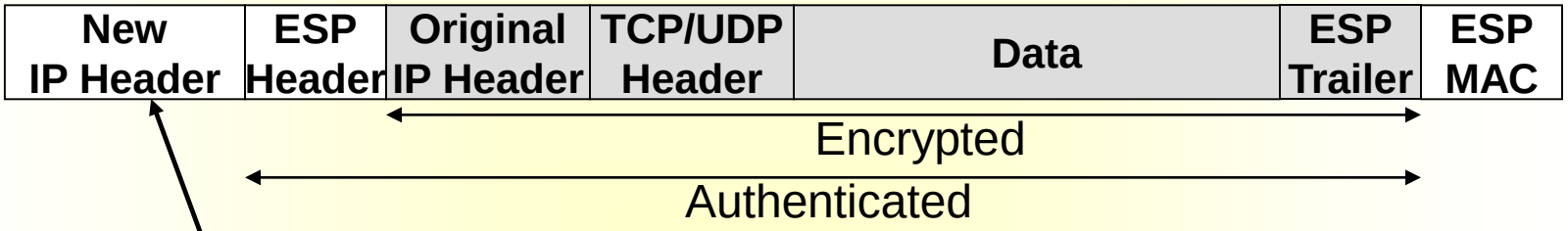
Original IP Header	TCP/UDP Header	Data

  - The ESP header is inserted into the IP packet immediately prior to the transport-layer header (e.g., TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after the IP packet. If authentication is selected, the ESP Authentication Data field (MAC) is added after the ESP trailer. The entire transport-level segment plus the ESP trailer are encrypted. Authentication covers all of the ciphertext plus the ESP header



MAC = Message Authentication Code

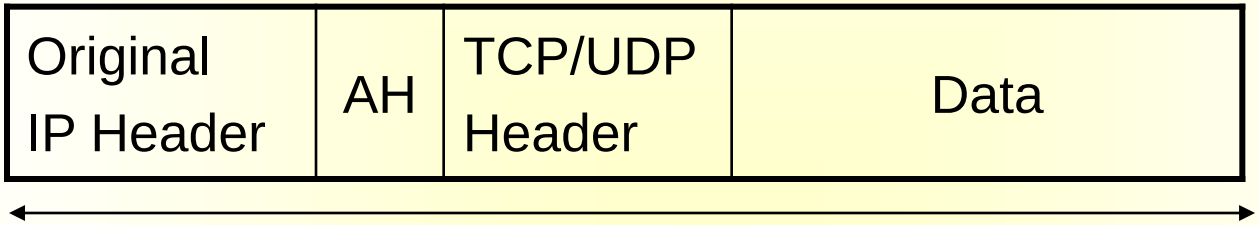
- Tunnel Mode ESP
  - Tunnel mode ESP is used to encrypt an entire IP packet
  - The ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted



  - This method can be used to counter traffic analysis
    - The new IP header may have totally different source and destination addresses (the source address will be the address of the gateway that the source is attached and the destination address will be the address of the gateway that the destination is attached)

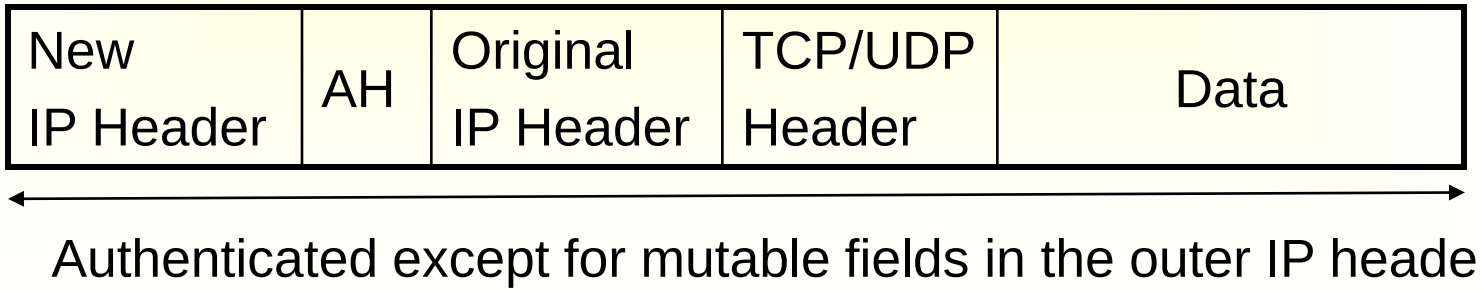
Original IPv4 Packet

- AH in Transport Mode



  - Mutable fields are those that might be altered in transit such as TTL and header checksum

- AH in Tunnel Mode



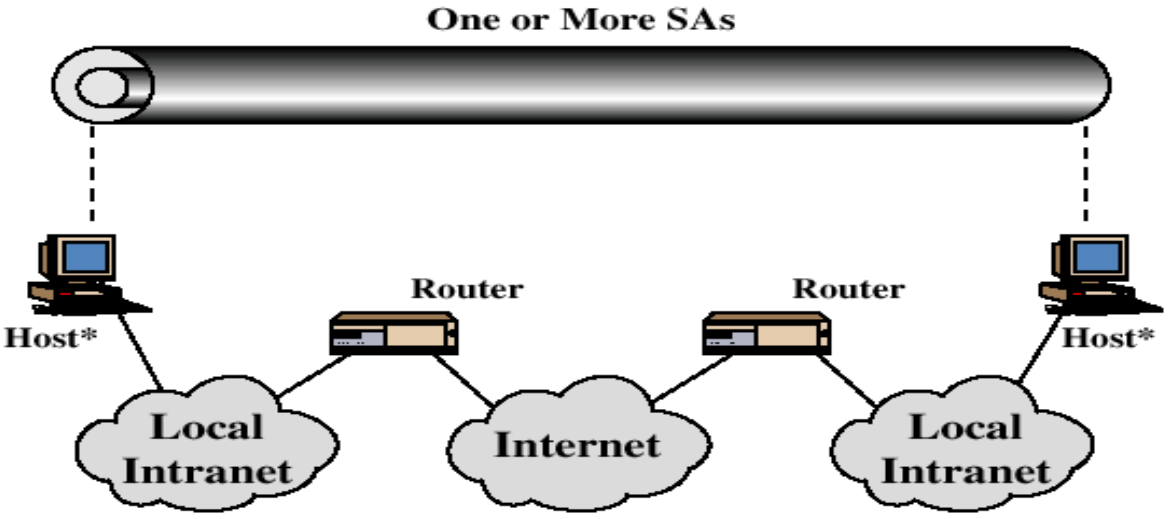
- Security Associations (SAs)
  - In addition to AH and ESP protocols, key management, DOI, and encryption and authentication algorithms, IPSec has SAs to be used by security protocols as they provide security services
  - In both AH and ESP protocols, before secured datagrams are sent from a source host to a destination host, the source and network hosts handshake and create a network-layer logical connection. This logical connection is called a Security Association (SA)
  - Thus IPSec transforms the traditional connectionless network layer of the Internet into a layer with logical connections

- An SA is a relationship between two entities that defines how they are going to use security services to secure their communications
- It includes information on authentication and/or encryption algorithms, cryptographic keys and key lengths
- It is unidirectional or simplex
  - Two SAs are needed for a bidirectional flow: one for inbound (read) traffic and one for outbound (write) traffic

- SA is uniquely identified by the following three items
  - Security Parameter Index (SPI): A 32-bit value selected by the receiving end of an SA to uniquely identify the SA
    - 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
    - All datagrams in the same SA (i.e., in the same logical connection from source to destination host) are stamped with the same SPI
  - Destination IP 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 (either AH or ESP): This field from the outer IP header indicates whether the association is an AH or ESP security association

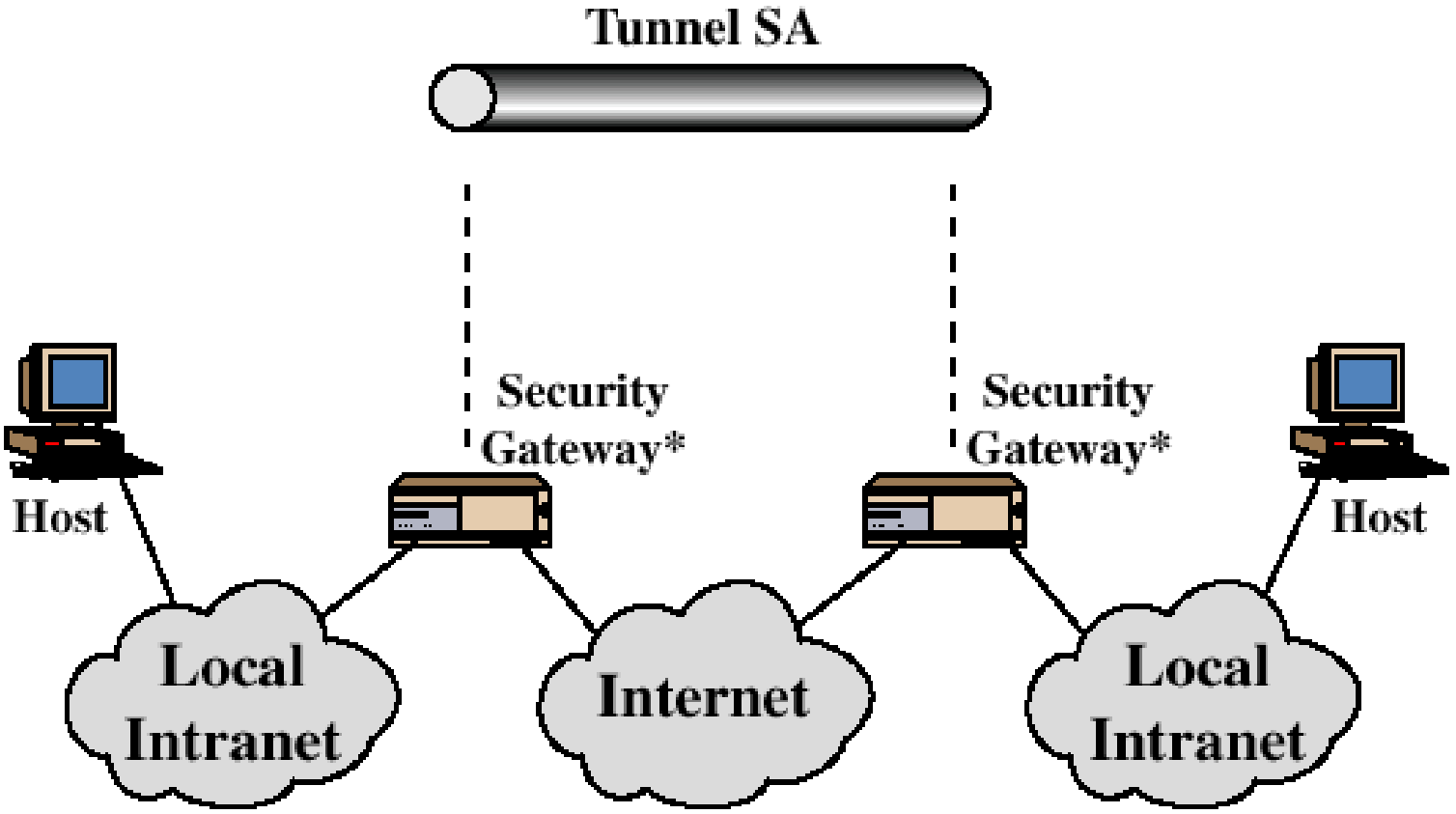
- IPSec Policy
  - Fundamental to the operation of IPSec is the concept of a security policy applied to each IP packet that transits from a source to a destination
  - IPSec policy is determined primarily by the interaction of two databases:
  - SPD (Security Policy Database)
    - Policies by which all inbound and outbound traffic is categorized on a host or a security gateway
    - The SPD is used to determine how to handle messages such as discarding the message, applying security services to the message, and forwarding the message with no change. The action taken depends on information in the IP and transport layer headers
  - SAD (Security Association Database)
    - A container for all active SAs, and related parameters

- Basic Combinations of Security Associations
  - An individual SA can implement either the AH or ESP protocol but not both
  - The IPSec architecture document lists four examples of combinations of SAs that must be supported by compliant IPSec hosts (e.g., workstation, server) or security gateways (e.g. firewall, router)
  - Case 1 - Host-to-Host Security: All security is provided between end systems that implement IPSec



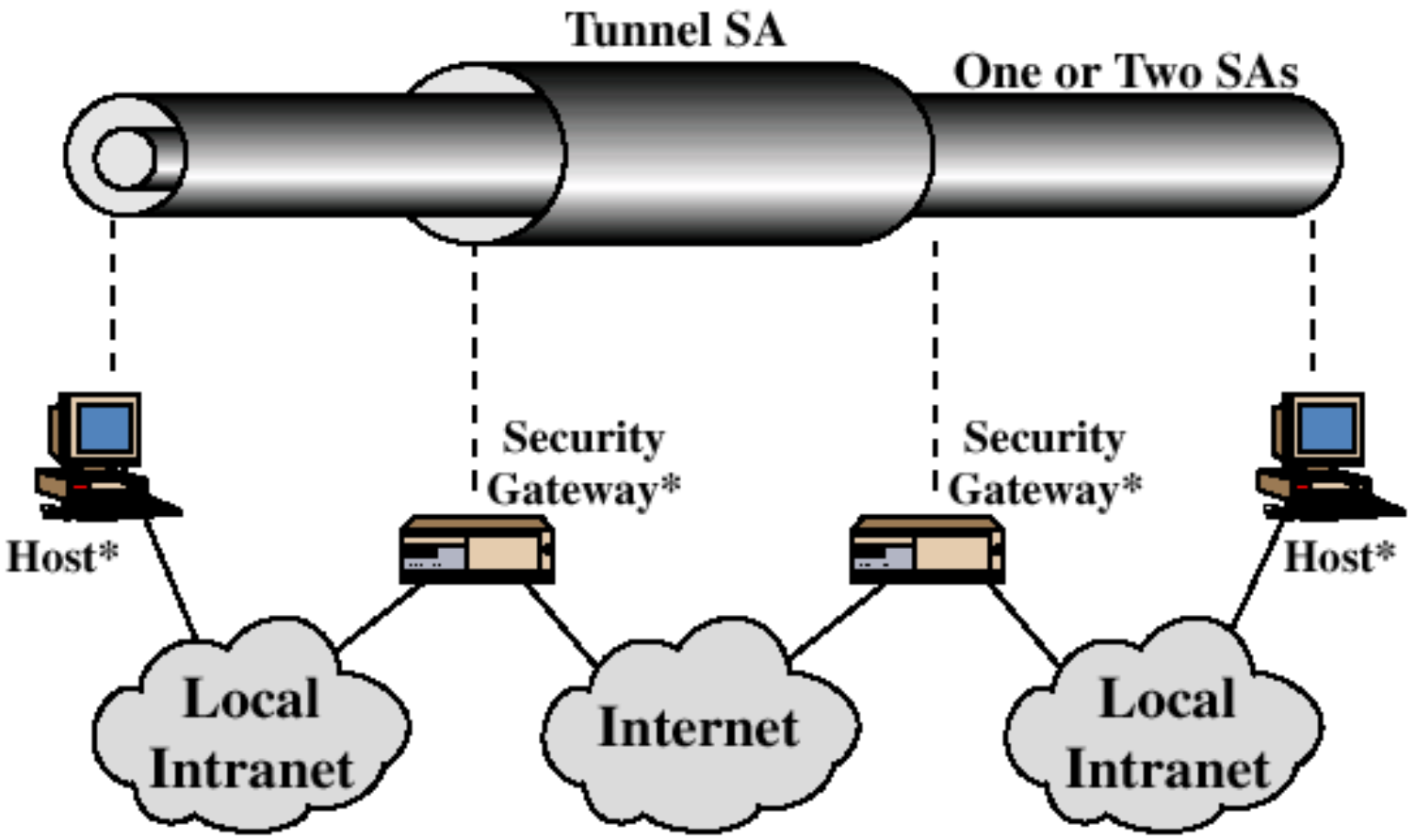
* Implements IPSec

- Case 2 - Gateway-to-Gateway Security: Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPSec. This case illustrates simple virtual private network support



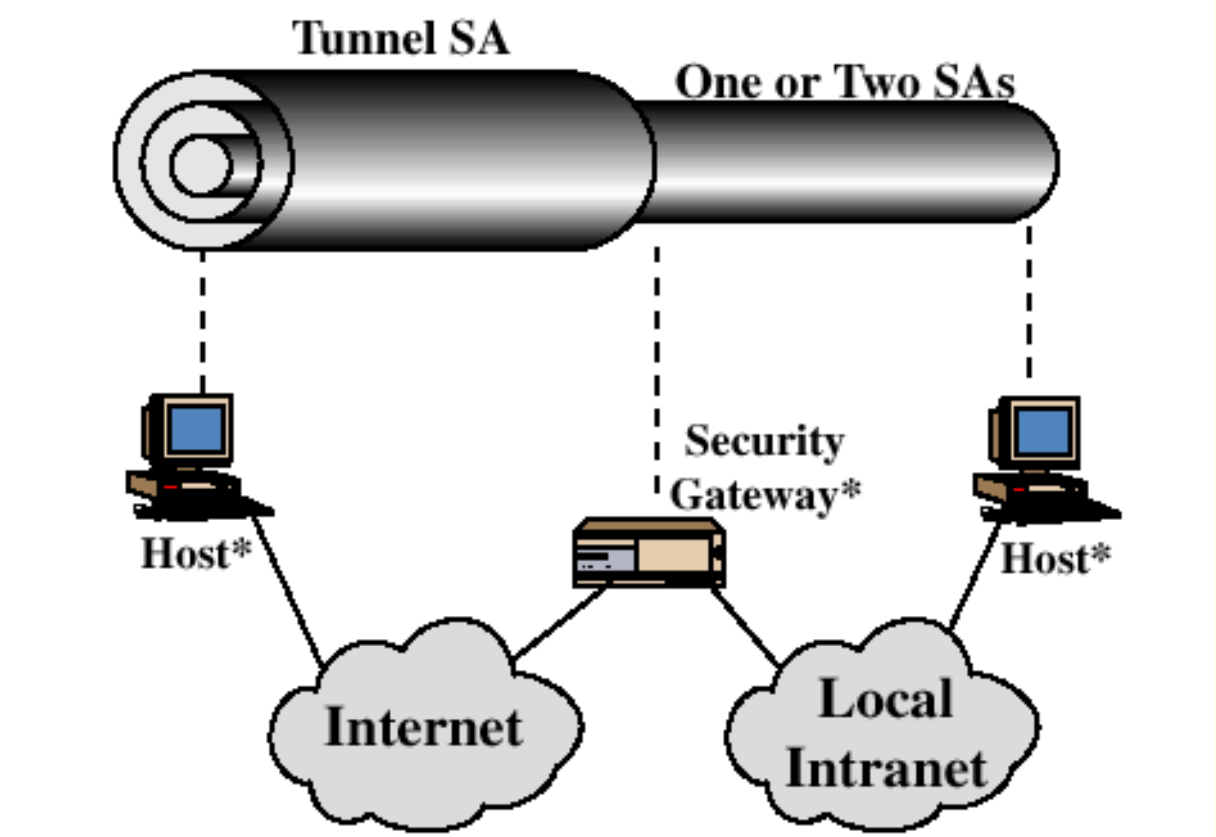
* Implements IPSec

- Case 3 – End-to-End Security: This builds on Case 2 by adding end-to-end security



* Implements IPSec

- Case 4 – Host-to-Gateway Security: This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall



* Implements IPSec

4.3.3 Transport Layer Security

TCP SYN Flood Attacks

- TCP SYN flood (or CYN flood or Synflood) is a type of DDoS attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive
- When a client and server establish a normal TCP three-way handshake, the exchange looks like the following
  - Client requests connection by sending SYN (synchronize) message to the server
  - Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client
  - Client responds with an ACK (acknowledge) message, and the connection is established

- In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address, faster than the targeted machine can process them, causing network saturation
- The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication
- It responds to each attempt with a SYN-ACK packet from each open port
- The attacker either does not send the expected ACK, or - if the IP address is spoofed - never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet

Securing TCP Connections: SSL

- SSL – Secure Sockets Layer
- Widely deployed, “real-world” security protocol
- Considered as the de-facto standard for Internet security
- First designed by Netscape in 1994
- Evolved through versions 1.0, 2.0 and 3.0
- Version 3.0 is renamed to TLS (Transport Layer Service) by IETF (Sometimes called SSL 3.1)
- SSL enhances TCP with confidentiality, data integrity, server authentication, and client authentication

- SSL, like most modern security protocols, is based on cryptography
- When an SSL session is established, the server begins by announcing a public key to the client, no encryption is in use initially
  - Both parties (and any eavesdropper) can read this key
- The client then transmits information to the server using the server's public key; no one else (other than the server) could decode it
- Session key is then negotiated and established between the server and the client to encrypt the rest of the session (see Symmetric Key Distribution Using Asymmetric Encryption in Chapter 3)
- SSL is used extensively by Web browsers, Web servers, and Internet commerce sites (Amazon, eBay, Yahoo!, MSN, etc.) to provide secure connections for transferring sensitive data

- SSL-protected HTTP transfer uses port 443 (instead of port 80), and is identified with a special URL method - https
  - For example: https://www.abc.com/ would cause an SSL-enabled browser to open a secure SSL session to port 443 at www.abc.com
- When HTTPS is used, the following elements of the communication are encrypted
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms (filled in by browser user)
  - Cookies sent from browser to server and from server to browser
  - Contents of HTTP header
- More on SSL in the next section

4.4 Web Security

- The Web (WWW) as a client/server application running over the Internet or TCP/IP intranet presents new challenges not well appreciated in the context of the main stream of computer and network security
  - It is a very visible outlet for corporate and business transactions that may lead to damages and loses; reputations can be damaged and money can be lost if the Web servers are subverted
  - Web servers are easy to configure and web content is easy to develop and manage, but the underlying software is getting extraordinarily complex that may hide many potential security flaws
  - Web servers can be exploited as a launching pad to attack corporate data systems as users are usually not aware of the risks

- Types of Web threats and countermeasures
  - Integrity
    - Data, memory and/or message modification
    - Trojan horse browser

    ⇒ Cryptographic checksums
  - Confidentiality
    - Eavesdropping
    - Theft of data from client & information from server
    - Access to information about network configuration
    - Access to information about which client is communicating

    ⇒ Encryption

- Denial of Service
  - Killing of user thread
  - Machine flooding with bogus requests
  - Filling up disk/memory
  - Isolating machine by DNS attacks

  $\Rightarrow$ Detection (of suspicious pattern) and action
- Authentication
  - Impersonation of legitimate users
  - Data forgery

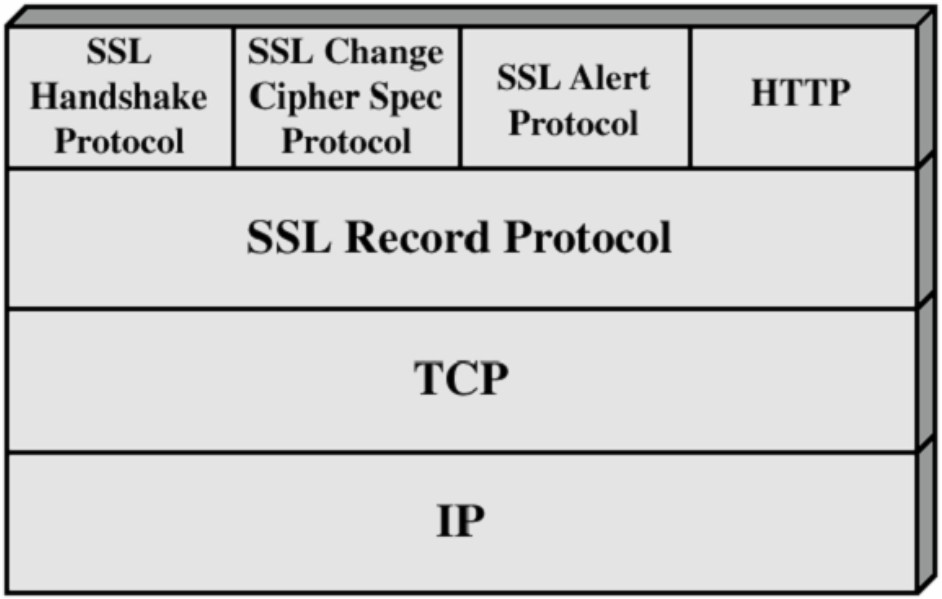
  $\Rightarrow$ Cryptographic techniques

- Types of threats faced in using the Web can also be classified in terms of the location of the threat
  - Web server (computer system security)
  - Web browser (computer system security)
  - Network traffic security between browser and server (network security)
- Web security (Web traffic security) mainly falls into the category of Network traffic security
- Different Web security approaches provide similar services but differ with respect to their scope of applicability and their relative location in the TCP/IP protocol stack

- There are three standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer: SSL/TLS, HTTPS, and SSH
- SSL/TLS
  - Provides security services between TCP and applications that use TCP
  - Provides confidentiality using symmetric encryption and message integrity using a message authentication code
  - It includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use
- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server
- Secure Shell (SSH) provides secure remote login and other secure client/server facilities such as FTP

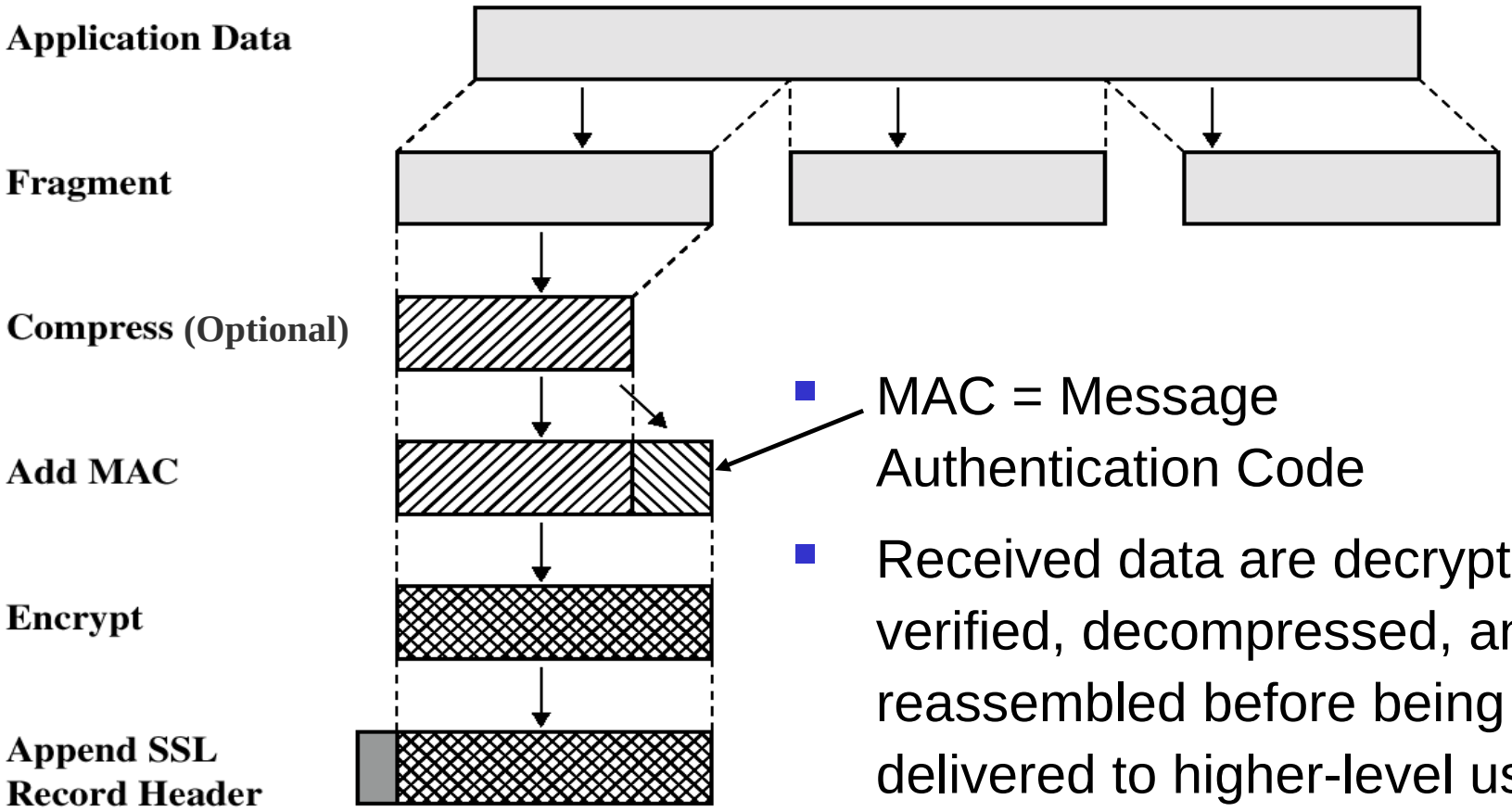
4.4.1 Secure Sockets Layer (SSL)

- SSL consists of two layers of protocols: SSL Record Protocol Layer and Upper Layer Protocols (SSL Handshake, SSL Change Cipher Spec, SSL Alert)
- SSL Handshake: Allows the server and the client to authenticate each other and negotiate on MAC (message authentication code) algorithm and cryptographic key
- SSL Change Cipher Spec: Allows pending state to be copied into the current state
- SSL Alert: Used to convey SSL related alerts to the peer entity



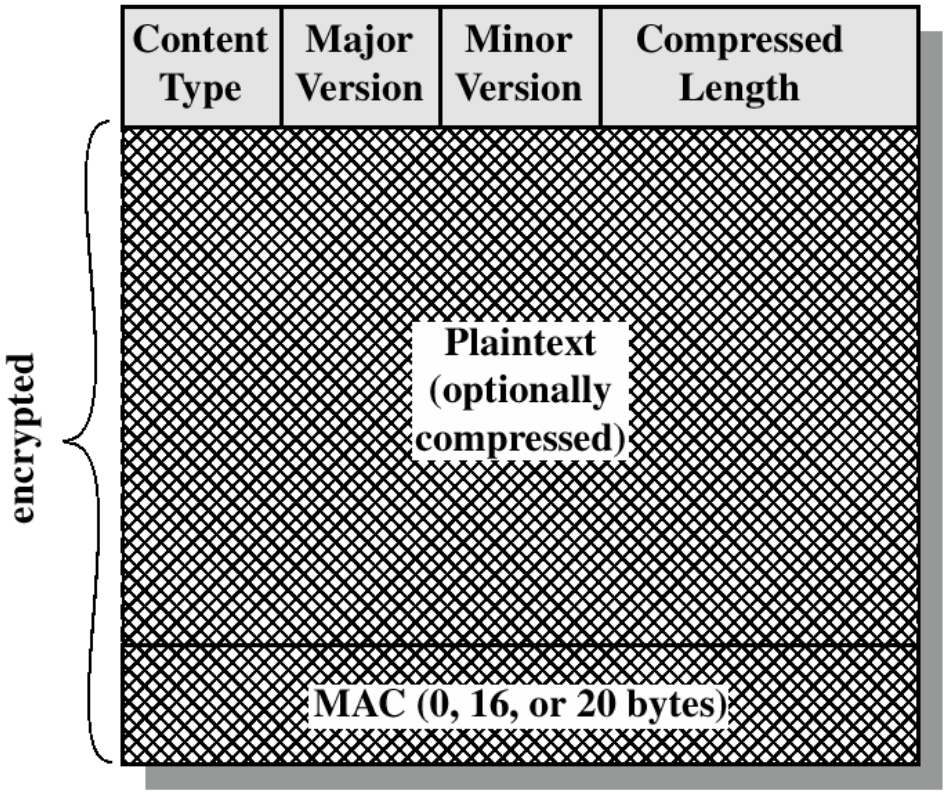
SSL Protocol Stack

- SSL Record Protocol Operation (Process)
  - It provides basic security services (confidentiality and message integrity) to various higher layer protocols
  - HTTP, which provides the transfer service for Web client/server interaction, can operate on top of SSL



- MAC = Message Authentication Code
- Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users

- SSL Record Format

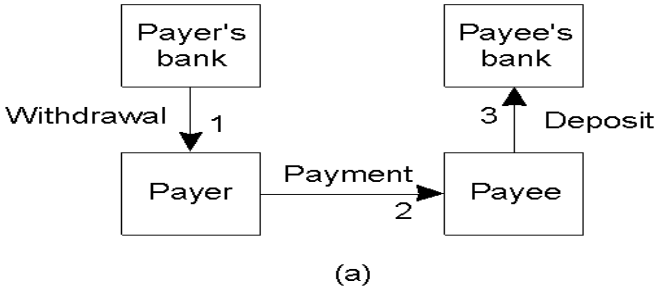


- Content Type (8 bit): The higher layer protocol used to process the enclosed fragment, i.e., whether the record is a handshake or a message that contains application data
- Major/Minor version (8/8 bits): Indicates version of SSL in use; For SSLv3, Major Version is 3 and 0 for Minor Version
- Compressed Length (16 bit): The length in bytes of the plain text fragment (compressed fragment) if compressed
- MAC (0 bytes if no authentication, 16 bytes for MD5 or 20 bytes for SHA)

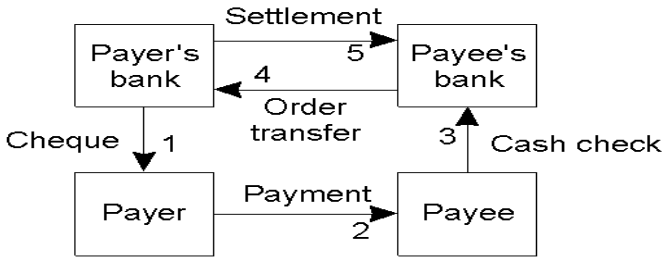
- Security-Enhanced Application Protocols
  - Solution to most application layer security problems are tackled by developing security-enhanced application protocols
  - Examples
    - For FTP - FTPS
    - For HTTP - HTTPS
    - For SMTP - SMTPS
    - For DNS - DNSSEC

4.4.2 Secure Electronic Transaction (SET)

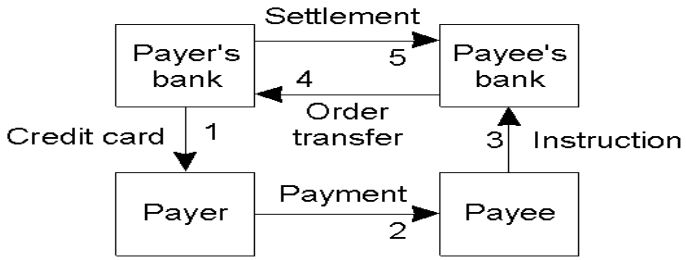
- E-commerce (Electronic Payment)
  - Payment involves a customer (payer), a merchant (payee), and often banks
  - How does the customer ensure that the merchant gets paid?
  - Delivery of goods is in the sphere of Delivery Science ☺
  - Payment systems can be organized based on cash (Fig. a), check (Fig. b), and credit card (Fig. c) – this is not e-commerce



(a)



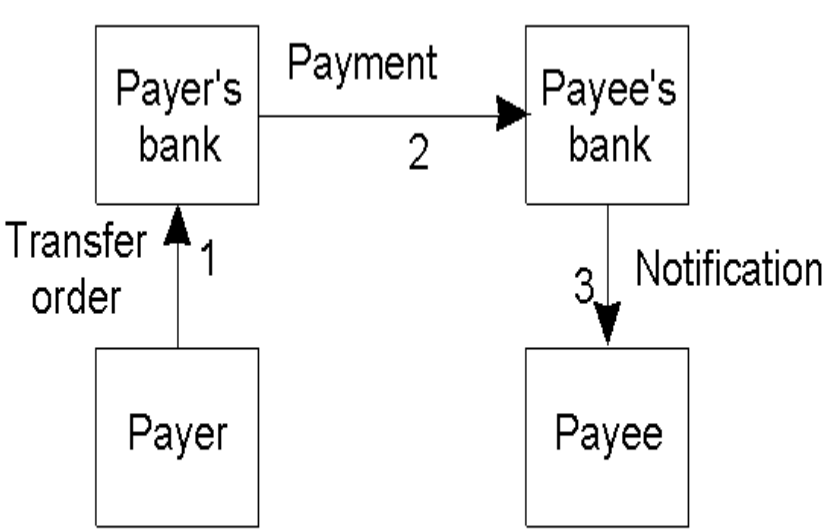
(b)



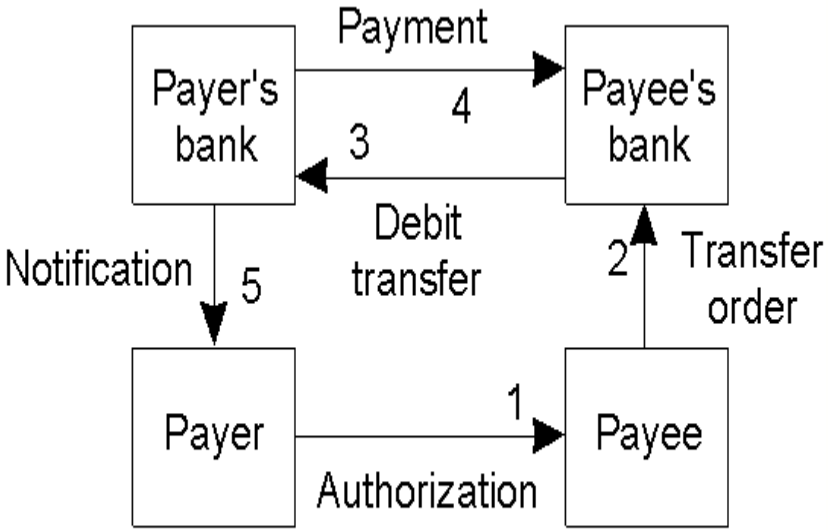
(c)

- In all the three cases, the customer has to personally visit the merchant

- If the merchant doesn't know the customer, it may not be willing to ship the product before paid
- Hence we have payment systems based on money transfer between banks
  - Payment by money order (Fig. a)
  - Payment through debit order (Fig. b); examples are electric and telephone bills where there is a standing order of authorization



(a)



(b)

- Security in Electronic Payment
  - Electronic payment systems are based on the above models
  - Secure payment systems are critical to the success of E-commerce
  - In cash based systems (using ATM), the main issue is authentication
    - Use of magnetic card
    - PIN
  - Credit card or check based system
    - No tampering/alteration
    - Protection against repudiation (the buyer denies having made the order)
  - There are four essential security requirements for safe electronic payments (Authentication, Encryption, Integrity and Non-repudiation)

SET - Secure Electronic Transaction

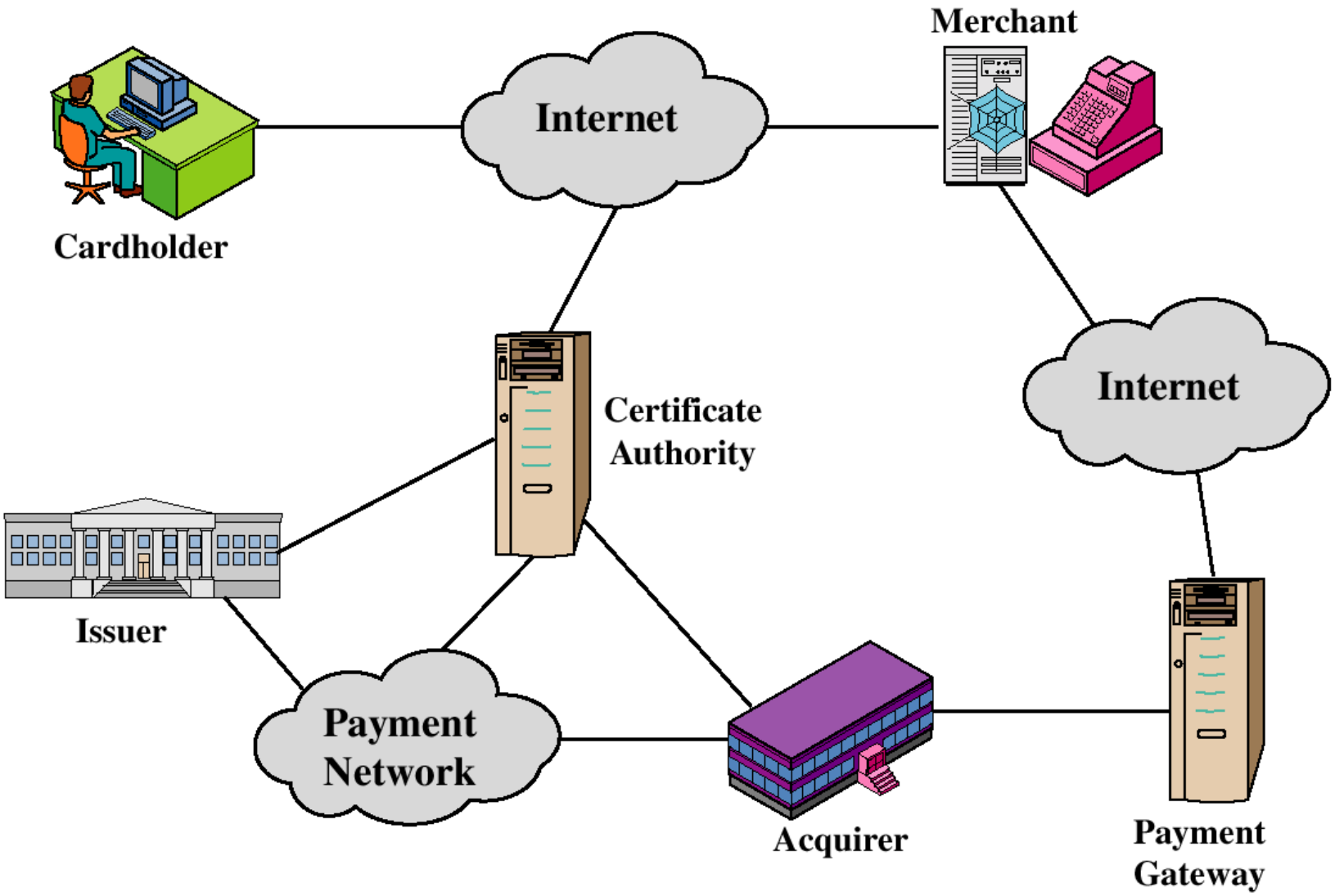
- The Secure Sockets Layer (SSL) protocol, implemented in most major Web browsers used by consumers, has helped create a basic level of security but is not sufficient
- SSL provides a secure channel between the consumer and the merchant for exchanging payment information, i.e., it supports confidentiality
- The customer is protected from eavesdroppers but not from the merchant; some merchants are dishonest, e.g., some just put up an illegal Web site and claim to be the XYZ Corp., or impersonate the XYZ Corp. and collect credit card numbers for personal use (phishing)
- The merchant is not protected from dishonest customers who supply an invalid credit card number or who claim a refund from their bank without cause

- SET is an example of application of cryptography
- Developed by Visa and MasterCard
  - Companies involved: IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Designed to protect credit card transactions on the Internet
- SET is not a payment system but enables users to employ the existing credit card payment infrastructure on an open network (Internet) in a secure manner
- It is an open encryption and security specification (the entire protocol is published)

- SET Features and Business Requirement
  - Provide confidentiality of payment and ordering information
  - Information made available only when and where necessary (privacy)
  - Ensure the integrity of all transmitted data
  - Provide authentication that a cardholder is a legitimate user of a credit card account
  - Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution
  - All parties must have digital certificates (trust)
  - Provides a secure communication channel in a transaction

- SET Participants
  - Cardholder: Authorized holder of payment card (the customer)
  - Merchant: Has goods or services to sell to the Cardholder (the web server)
  - Issuer: Financial institution (cardholder's bank)
  - Acquirer: Verifies that a card account is active and the proposed purchase does not exceed the credit limit – Connected with the Merchant
  - Payment gateway: Operated by the acquirer or a designated third party that processes merchant payment messages
  - Certificate Authority (CA): Trusted entity to issue the X.509v3 public key certificate for card holders, merchants and payment gateways. The success of SET depends on the CA

- Both cardholders and merchants must register with CA first, before they can buy or sell on the Internet, i.e., The customer opens an account and receives a certificate; Merchants have their own certificates



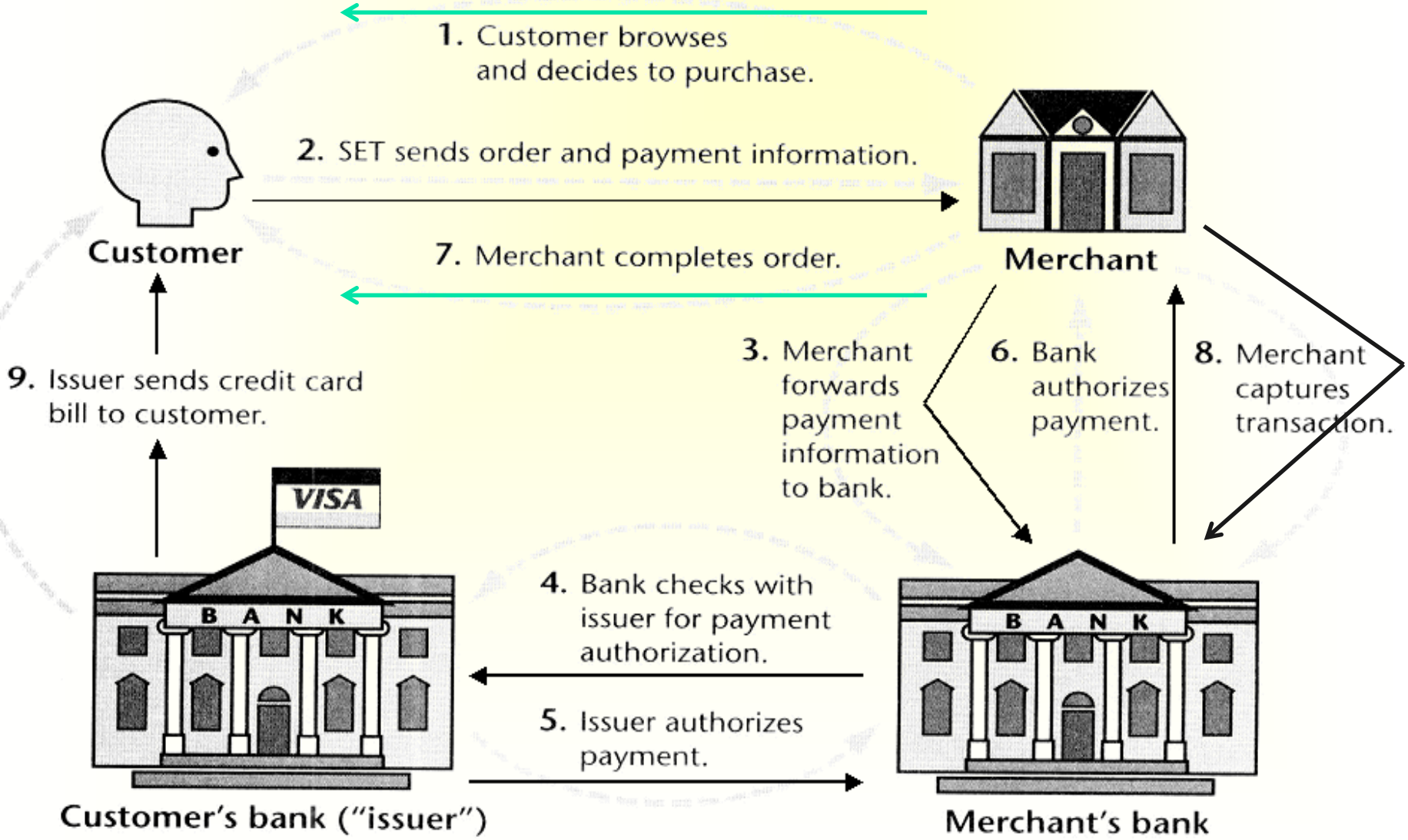
- Sequence of Events for Transactions in SET

1. Customer browses a website and decides what to purchase
2. Customer sends order and payment information, which includes 2 parts in one message

   a. Purchase Order - this part is for the merchant

   b. Payment Information - this pat is for merchant's bank only
3. Merchant forwards card information (part b) to its bank
4. Merchant's bank checks with Issuer for payment authorization
5. Issuer sends authorization to Merchant's bank
6. Merchant's bank sends authorization to merchant
7. Merchant completes the order and sends confirmation to the customer
8. Merchant captures the transaction from its bank
9. Issuer prints credit card bill (invoice) to customer

- SET - Sequence of events for transactions



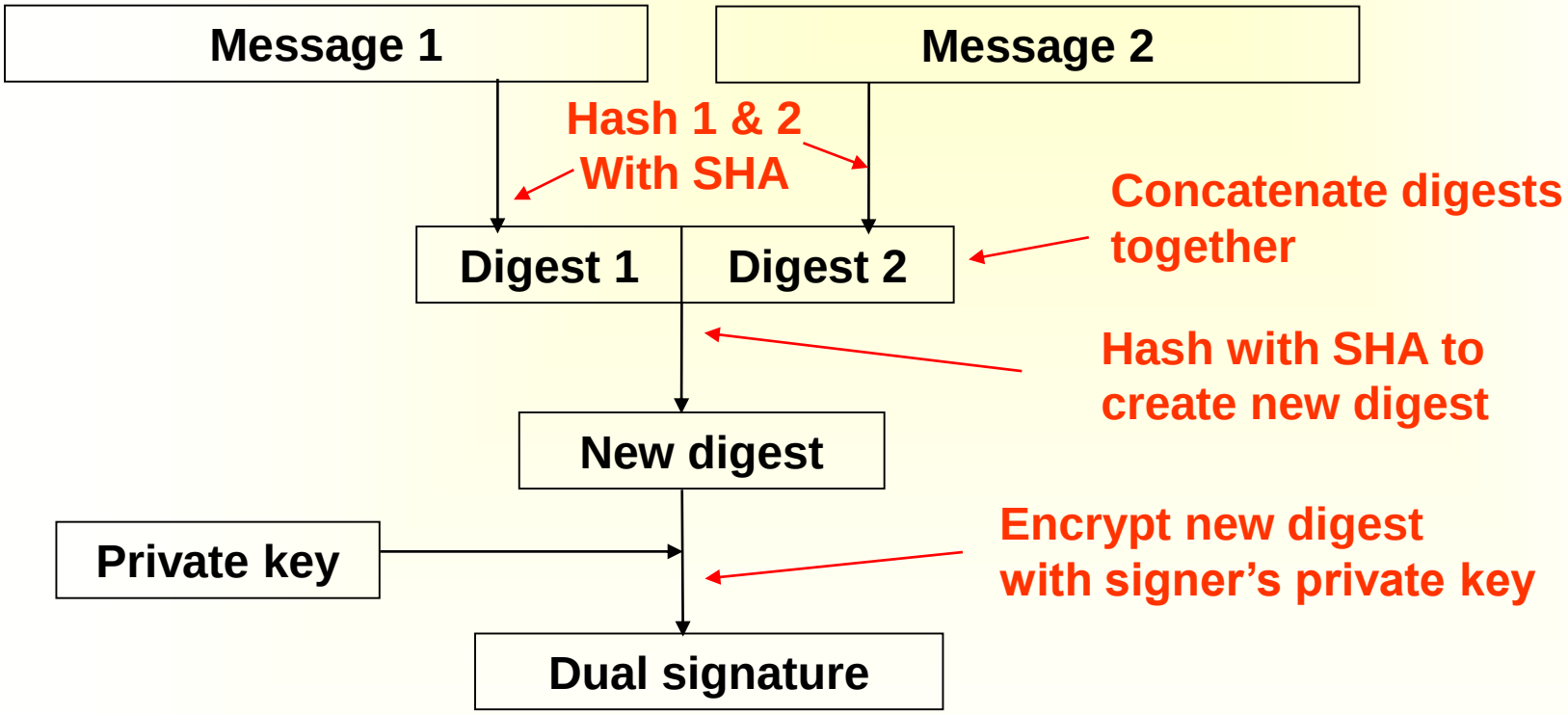
- Key Technologies of SET
  - Confidentiality of information: DES
  - Integrity of data: RSA digital signatures with SHA-1 hash codes
  - Cardholder account authentication: X.509v3 digital certificates with RSA signatures
  - Merchant authentication: X.509v3 digital certificates with RSA signatures
  - Privacy: separation of order and payment information using dual signatures

- SET - Dual Signature
  - Dual signature is an important innovation by SET
  - Used to link two messages that are intended for two different recipients
  - The customer wants to send Order Information (OI) to the merchant and Payment Information (PI) to the bank
  - Merchant does not need to know customer's credit card number
  - Bank does not need to know details of customer's order

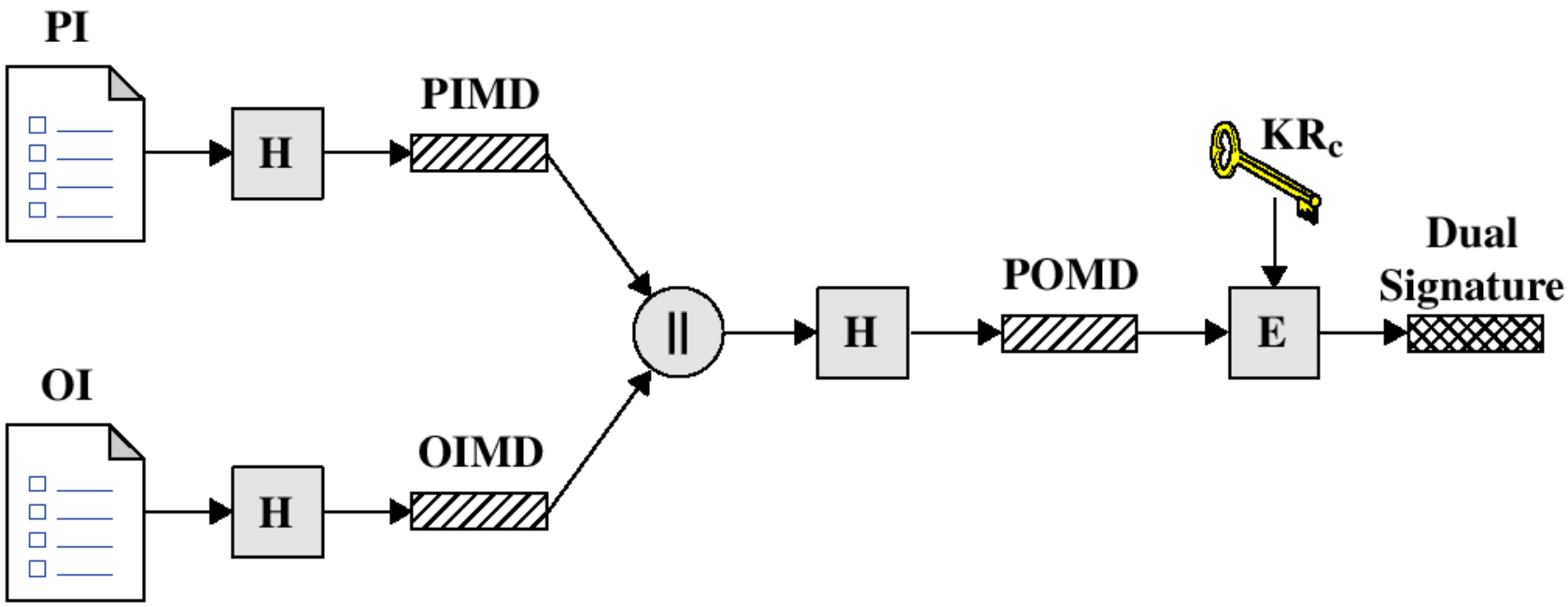
    Privacy!!
  - The two items, however, must be linked somehow to prove that the payment is intended for this order and not for some other
  - SET hides the OI from the bank (payment gateway) and PI from the merchant. But it also makes a link between payment information and order information

- Dual signature links two messages securely but allows only one party to read each

Principle of Dual Signature



Construction of Dual Signature in SET

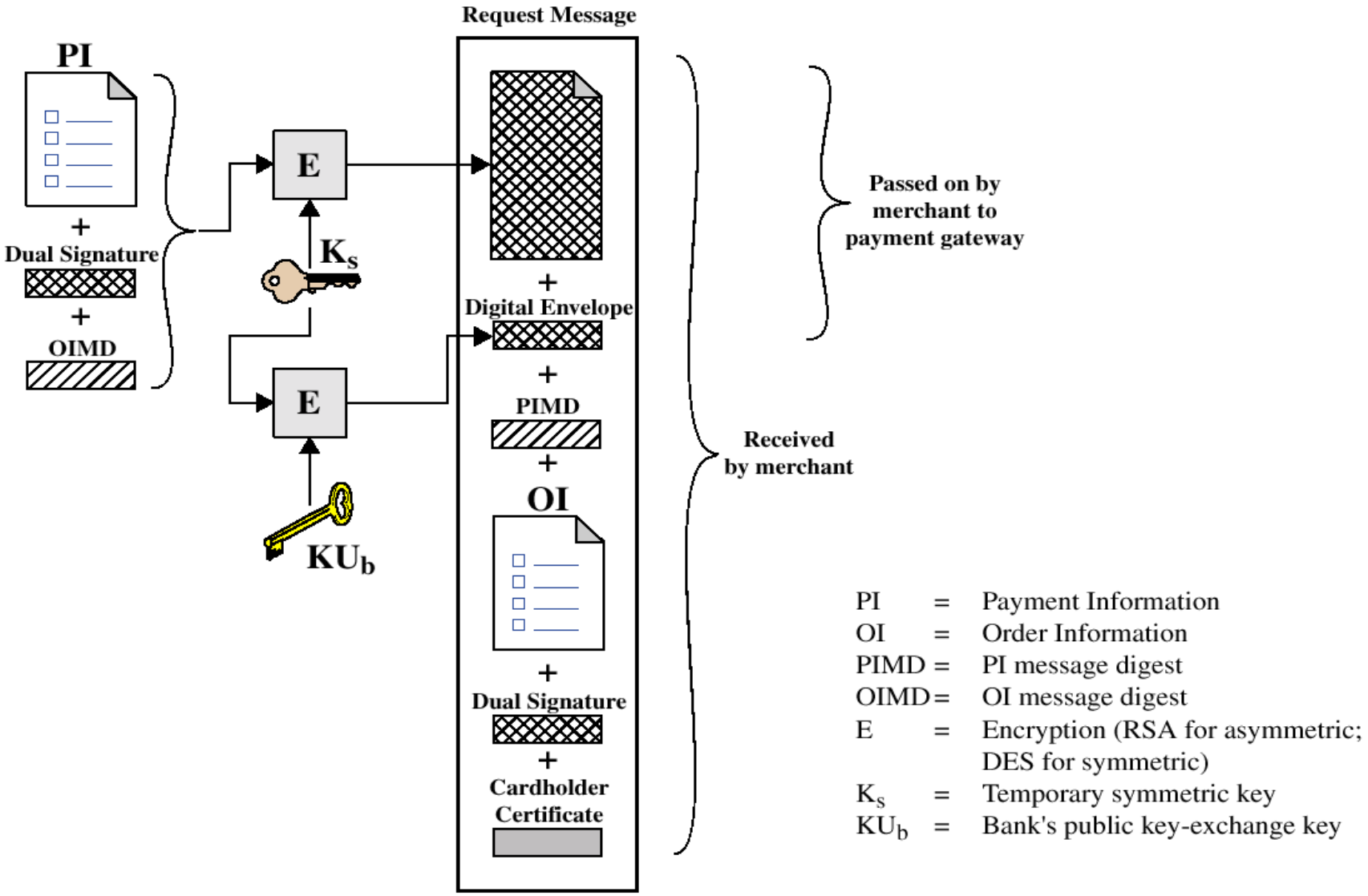


PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

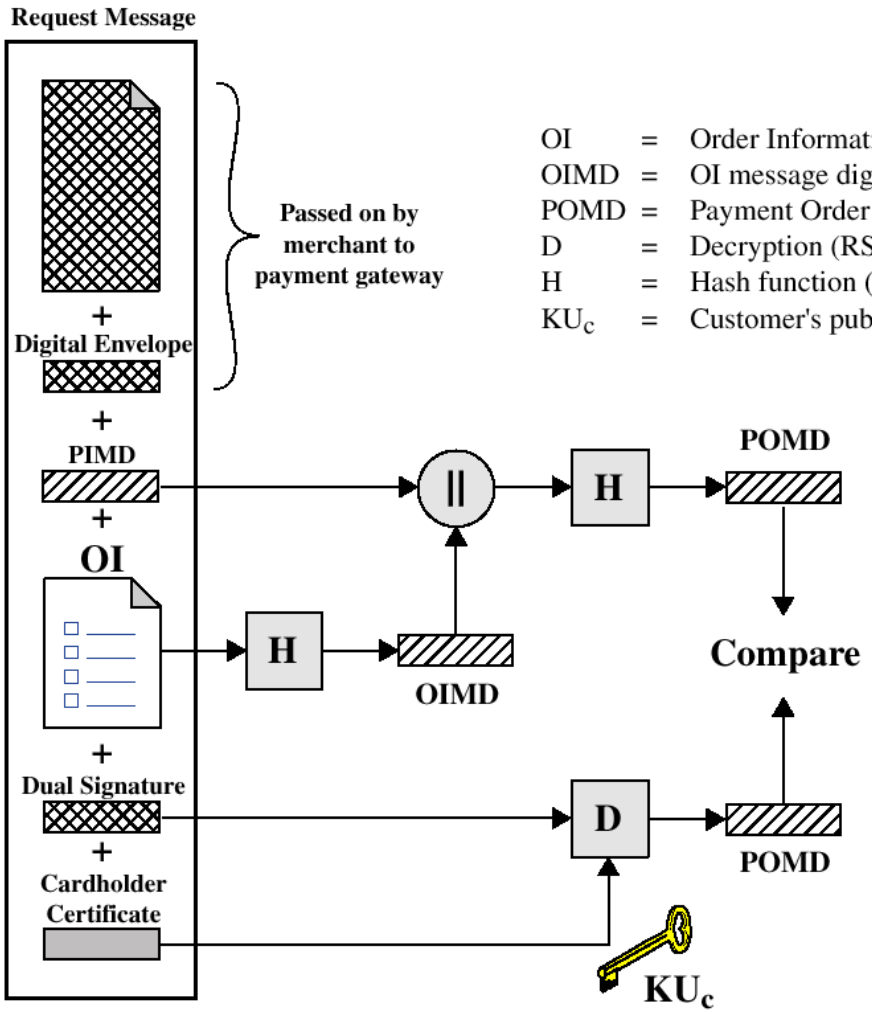
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

Dual Signature = $E(KR_c, H(H(PI) || H(OI))$

Cardholder Sends Purchase Request



Merchant Verifies Customer Purchase Request



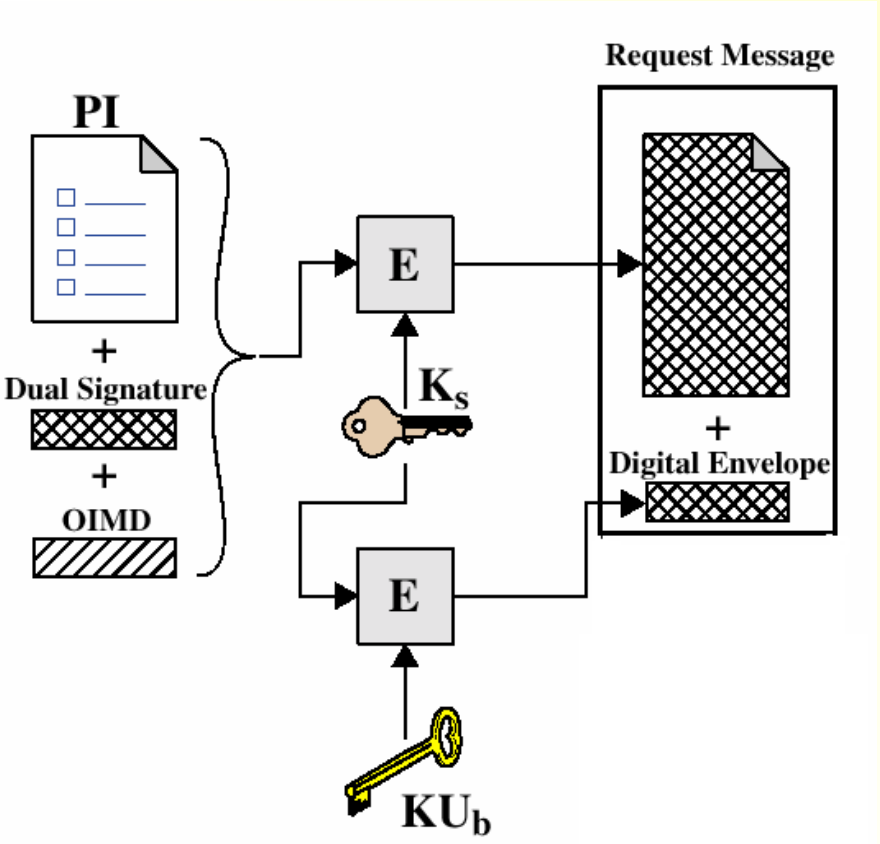
- The merchant has the public key of the customer obtained from the customer's certificate
- Now, the merchant can compute two values:

$H(PIMD \,||\, H(OI)) \Rightarrow POMD$

$D(KU_C, DS) \Rightarrow POMD$

Should be equal!

Payment Gateway Verifies Customer Purchase Request



- The payment gateway can compute two values:

  $H(H(D(K_S, PI)) \| OIMD) \Rightarrow POMD$

  $D(KU_C, DS) \Rightarrow POMD$

  Should be equal!

- Read more details about SET

4.5 Application Layer Security

- DNS Spoofing
  - If the attacker has access to a name server it can modify it so that it gives false information
    - e.g., redirecting www.ebay.com to map to own (attacker's) IP address
  - The cache of a DNS name server can be poisoned with false information using some simple techniques
- Web Browsers as Threats
  - We obtain most of our browsers on-line
  - Potential problems that can come from malicious code within the browser
    - Inform the attacker of the activities of the user
    - Inform the attacker of passwords typed in by the user
    - Downgrade browser security (e.g., reduce key length used in SSL)

- Helper applications are used by browsers
  - A helper application is an external viewer program to display content retrieved using a web browser. Some examples include JPEGview, Windows Media Player, QuickTime Player, Real Player and Adobe Reader
  - The helpers can have Trojan horse code
  - Downloaded data can exploit vulnerabilities of helpers
- Mobile Code: Java Applets (getting outdated) & ActiveX controls
  - Migrating code is an interesting feature
  - However, there is a risk of malicious use of resources of the machine that is running the code
  - Normally run within a controlled environment (sandbox) and access to local resources is strictly controlled by a security manager
  - However, an Applet may escape from the sandbox due to some bugs in the implementation of the Java Virtual Machine

- Cookies
  - Cookies are set by web servers and stored by web browsers
  - A cookie set by a server is sent back to the server when the browser visits the server again
  - Cookies can be used to track what sites the user visits (can lead to serious privacy violation!)
- Server Side Risks
  - Interactive web sites are based on forms and scripts
  - By writing malicious scripts, the client can
    - Crash the server (e.g., buffer overflow)
    - Gain control over the server

4.6 E-mail Security

- E-mails transit through various servers before reaching their destinations
- By default, they are visible by anybody who has access to the servers
- SMTP protocol has security holes and operational limitations
- E-mail security can be improved using tools and protocols like PGP and S/MIME
  - PGP: Pretty Good Privacy
  - S/MIME: Secure Multi-Purpose Internet Mail Extension

- Required security features for e-mail
  - Confidentiality: Trudy shouldn't read Alice's e-mail to Bob
  - Sender Authentication: "I don't Love you anymore. I never want to see you again. Formerly yours, Alice"; Bob would like to make sure that the message came from Alice and not from Trudy
  - Message Integrity: Trudy shouldn't change Alice's e-mail to Bob
  - Receiver Authentication: Alice wants to make sure that she is indeed sending the letter to Bob and not to Trudy who is impersonating Bob

- PGP
  - Philip R. Zimmerman is the creator of PGP
  - PGP is an open-source, freely available software package for e-mail security
  - There are several software implementations available as freeware for most desktop operating systems
  - PGP provides confidentiality and authentication services that can be used for e-mail and file storage applications
  - It provides authentication through the use of digital signature, confidentiality through the use of symmetric encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 (Base 64) encoding scheme
  - PGP incorporates tools for developing a public-key trust model and public-key certificate management

- SMTP
  - SMTP Limitations - Can not transmit, or has a problem with
    - Executable files, or other binary files (e.g., JPEG image)
    - “national language” characters (non-ASCII)
    - Messages over a certain size
    - ASCII to EBCDIC translation problems
    - Lines longer than a certain length (72 to 254 characters)
  - Multipurpose Internet Mail Extension (MIME) is intended to address some of the problems and limitations of the use of SMTP

- S/MIME Functions
  - S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP
  - Enveloped Data: Encrypted content and encrypted session keys for recipients
  - Signed Data: Message Digest encrypted with private key of "signer"
  - Clear-Signed Data: Signed but not encrypted
  - Signed and Enveloped Data: Various orderings for encrypting and signing
- Read about
  - DomainKeys Identified Mail (DKIM) - a specification for cryptographically signing e-mail messages which is a proposed Internet Standard
  - WEP (Wired Equivalent Privacy) and IEEE 802.11i for securing Wireless LANs