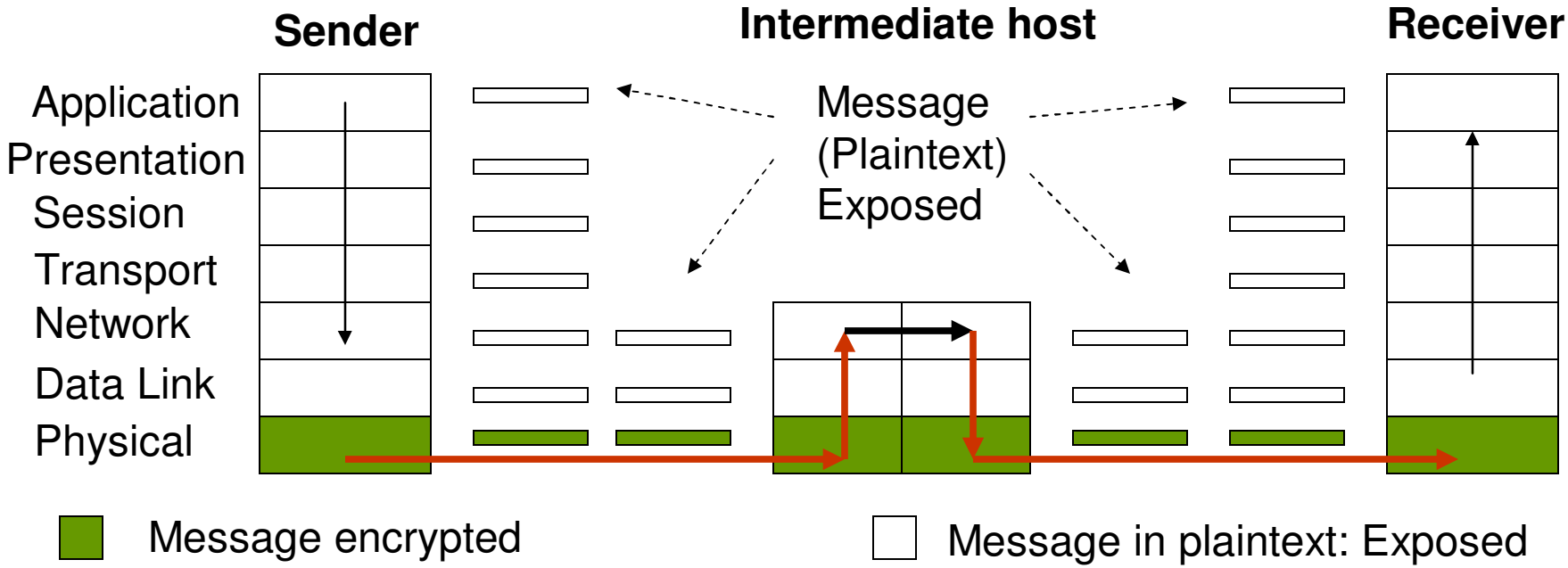
Network Security

Dr. Natarajan Meghanathan
Associate Professor of Computer Science
Jackson State University
Jackson, MS 39217
Phone: 601-979-3661
E-mail: natarajan.meghanathan@jsums.edu

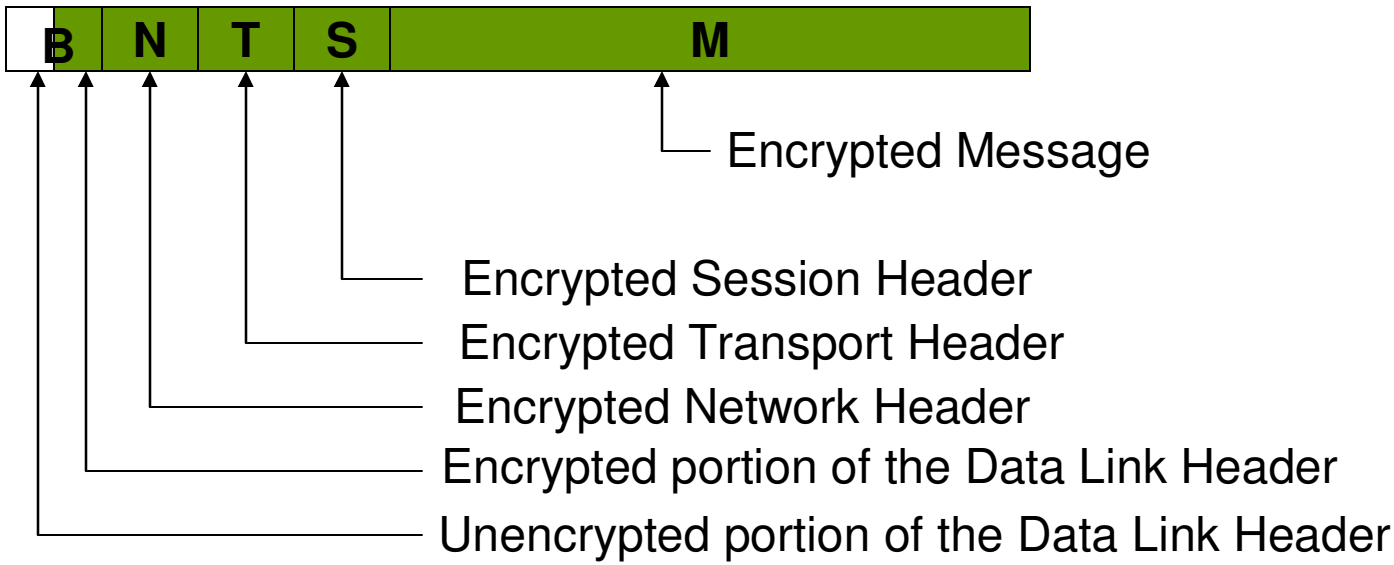
Link Encryption

- Link encryption is more appropriate when the transmission line is the point of greatest vulnerability.
  - In other words, all hosts on a network are reasonably secure, but the communications medium shared with other users of the network or is not secure.
- Data is encrypted just before the system places them on the physical communications link and decryption occurs just as the communication arrives at and enters the receiving computer.
  - Encryption occurs at layer 1 or 2 of the ISO OSI model.



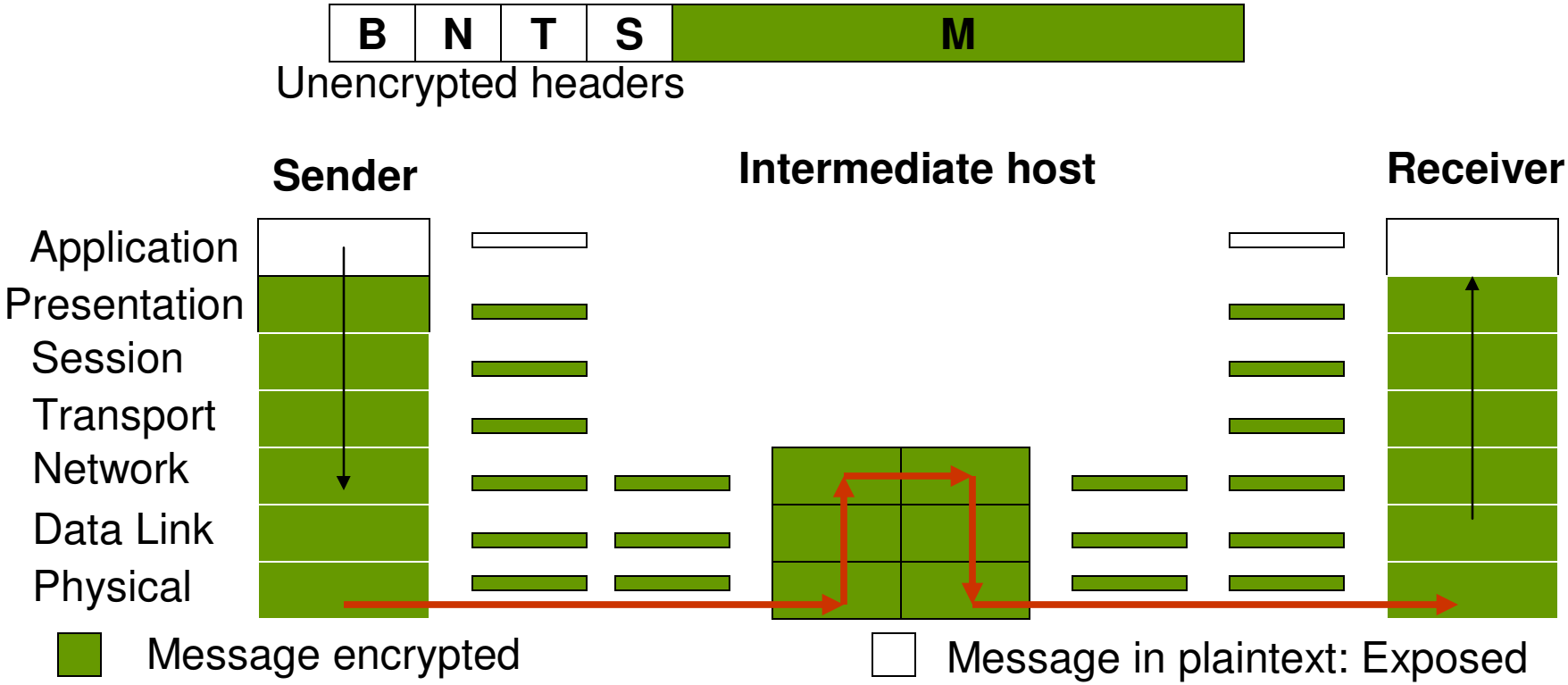
Link Encryption

- Encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts.
  - Since encryption is at the bottom protocol layer, the message is exposed in all other layers of the sender and receiver.
  - The message is also exposed at the 2nd and 3rd layers of the intermediate hosts through which the message passes. This is to facilitate hardware addressing and routing.
    - The message is in the clear at the intermediate hosts and one or more of these hosts may not be trustworthy.



End-to-End Encryption

- Encryption is performed at the highest level (application layer).
- Provides security for a message from one end of transmission to the other.
- Since encryption precedes all the routing and transmission processing, the message is transmitted in encrypted form throughout the network.
  - The message could go through potentially insecure intermediate nodes. The message is protected against disclosure while in transit.



Comparison of Encryption Methods

- If encryption is done for a link, every communication initiated by a host on the link will be encrypted and the host at the other end of the link should be able to decrypt the communication.
- The two end hosts of a link should share a key to facilitate link-level encryption.
- In order to fully take advantage of link-level encryption, it should be performed on all links in the network. Otherwise, a message could go through certain links in clear text.

- End-to-end encryption is basically applied to “logical links”, which are channels between two processes, at a level well above the physical path.
- Since the intermediate hosts along a transmission path do not need to encrypt or decrypt a message, they have no need for cryptographic facilities.
  - Encryption is used only for those messages and applications for which it is needed. Thus, it is more flexible than link-level encryption.
  - Encryption can be done with software, selectively for one application at a time, or even to one message within a given application.

Comparison of Encryption Methods

- With end-to-end encryption, there is a virtual cryptographic channel between each pair of users.
- If we use symmetric cryptography,
  - Each pair of users should share a unique cryptographic key.
  - For n users, the number of unique keys required is n(n-1)/2.
- If we use public key cryptography,
  - We need a pair of keys (public & private) per user. So, 2n keys for n users.
- The number of keys required in link-level encryption is normally far less than the number of keys required for end-to-end encryption.
- If there are N hosts in a network, the number of link-level keys required would be N(N-1)/2.
- Each host can support several applications run by several users.
  - So, $N << n$.
- Neither form of encryption is right for all situations.
  - A user who does not trust the quality of the link-level encryption provided by the system can apply end-to-end encryption as well.
  - A system administrator who is concerned about the security of an end-to-end encryption scheme supplied by an application program can also apply link-level encryption.

Comparison of Encryption Methods

Link Encryption	End-to-end Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate hosts	Data encrypted in intermediate hosts
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One encryption algorithm for all users / link	User selects encryption algorithm
Typically done in hardware	Either hardware or software implementation
All or no data encrypted	User chooses to encrypt or not for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

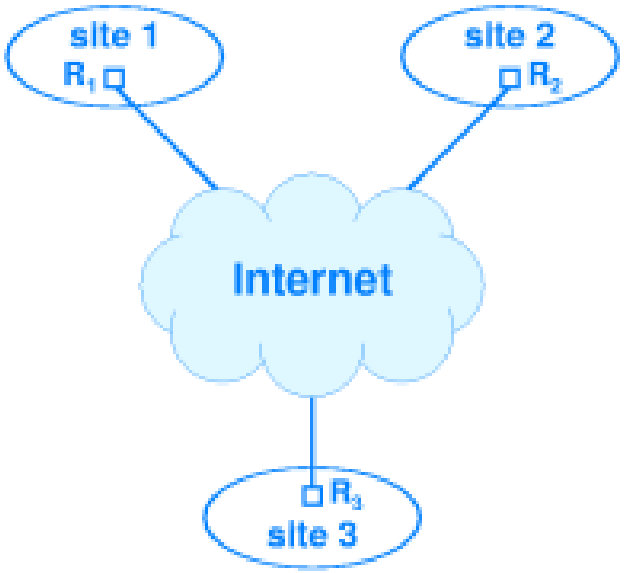
Virtual Private Network (VPN)

- An organization with multiple geographically distributed sites can take either of the following two approaches to interconnect the sites:

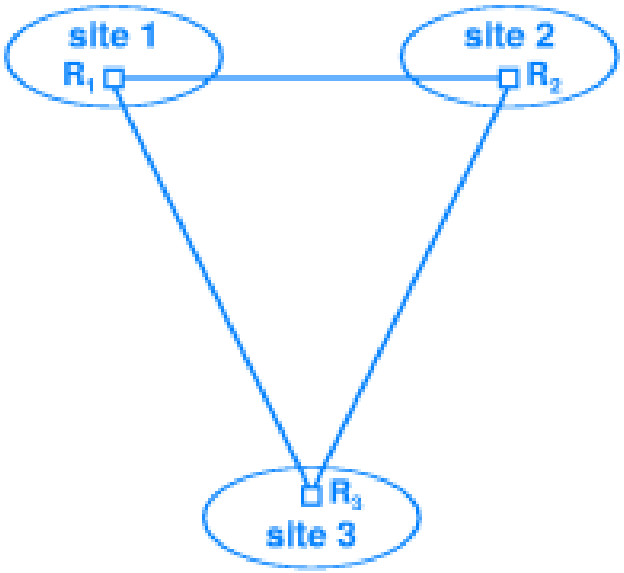
- **Private network connections:**
  - Lease serial lines (possibly from telephone companies) to connect the sites. A router at a site is directly connected to a router at another site using a leased line and data directly passes from one site to another.
- **Public Internet connections:**
  - Each site signs up with a local ISP for Internet service and data is passed from site to another across the global Internet.

- Although the serial lines are more costly than subscribing to a local ISP, they guarantee confidentiality of data, which is not possible when data is passed across the global Internet.
- VPN is the technology used to build an organization's intranet that provides confidentiality and at the same time is economical as encrypted data is tunneled from one site to another site across the global Internet.

Virtual Private Network (VPN)



Physical interconnection between routers at three sites of an organization



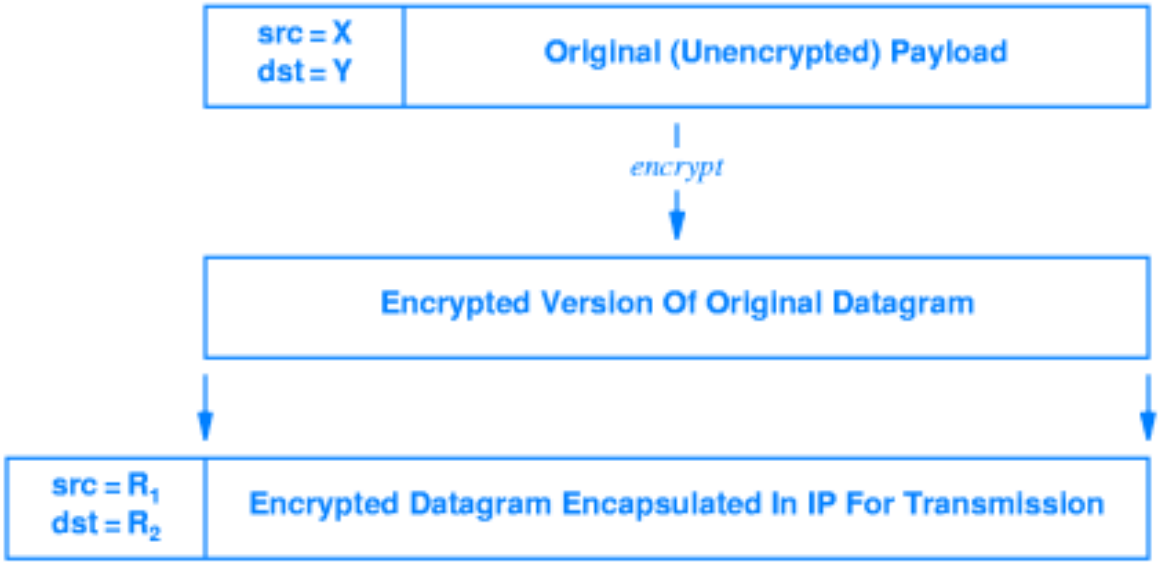
The equivalent logical connections created by VPN software running on the routers

Virtual Private Network (VPN)

- The VPN software installed at each of the routers R1, R2 and R3, does the following three functions:
  - Make sure the next hop for each outgoing datagram is a router at another site of the organization and nothing else.
  - Encrypt the IP datagram arriving from the host before forwarding to another site and decrypt the IP datagram received from another site before forwarding to the local host.
  - Perform IP-in-IP tunneling to facilitate the encryption of the actual source and destination IP addresses in the IP datagram by encapsulating it into another IP datagram whose source and destination addresses are that of the routers at the two participating sites.

X at site 1 is the original source of the unencrypted datagram

Y at site 2 is the target destination of the unencrypted datagram



IPSec

- The IP Security Protocol suite (IPSec) is implemented at the IP layer, so it does not require any change to existing TCP, UDP and application layer protocols.
- IPSec is designed to address the fundamental shortcomings of the IP layer such as being subjected to spoofing, eavesdropping and session hijacking.
- The basis of IPSec is called a security association, which is basically the set of security parameters for a secured communication channel.
- Each host can have several security associations in effect for current communications with different remote hosts.
- A security association is identified using a security parameter index (SPI) – a 32-bit identifier and the IP address of the partner host on the other side of the association.
- The SPI and the partner IP address are used to index to the security association database (SADB) that has information about the other characteristics of the different security associations
- Two protocols have been developed to provide packet-level security for both IPv4 and IPv6:
  - IP Authentication Header, AH (Next Header protocol ID: 51) provides integrity, authentication and non-repudiation.
  - IP Encapsulating Security Payload, ESP (Next Header protocol ID: 50) provides confidentiality, along with authentication and integrity protection.

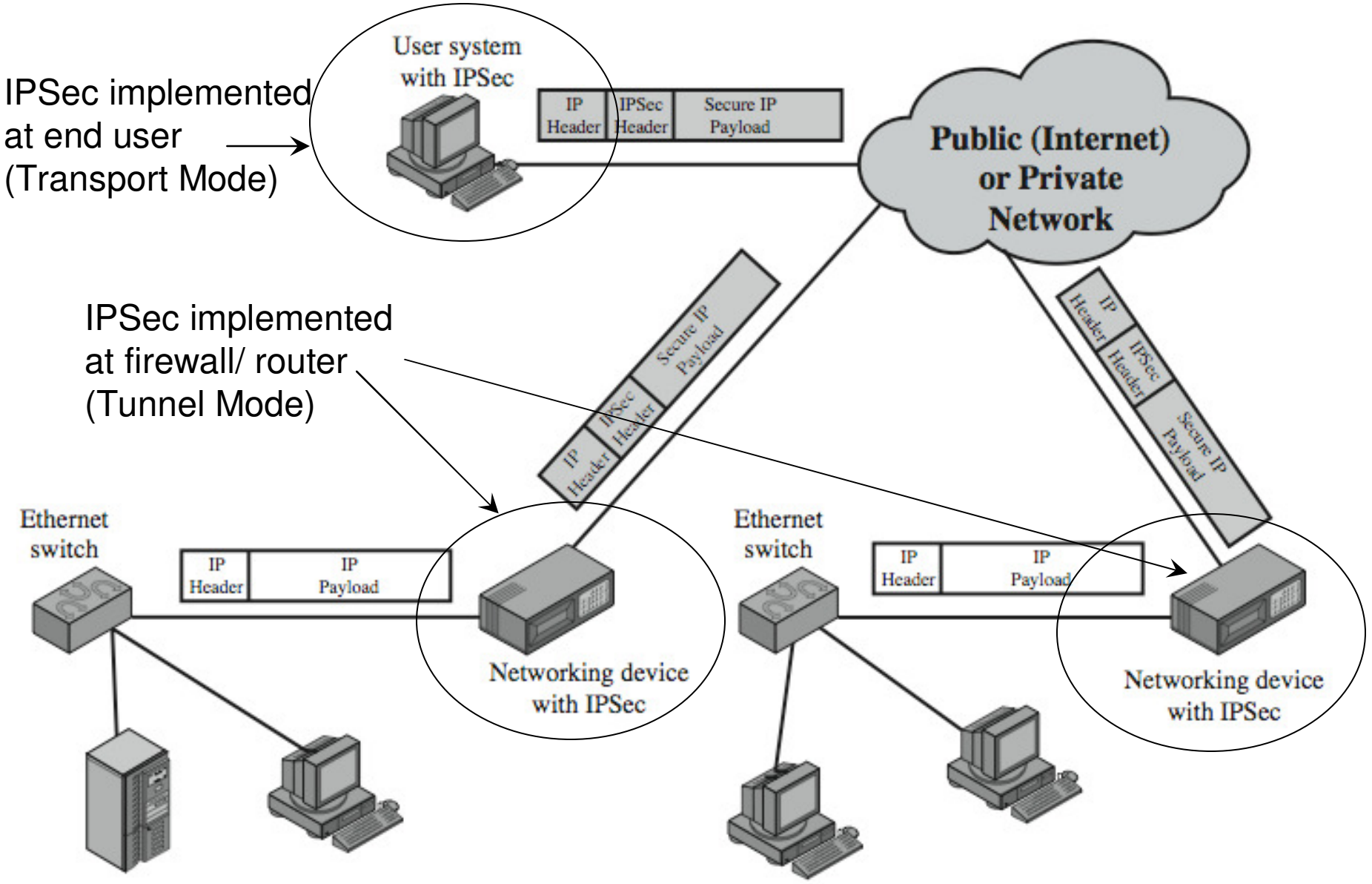
IPSec

- By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms (like PGP, Kerberos, TLS); but, also for the many security-ignorant applications.

- When implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

- Note: IPSec is optional for IPv4; but, mandatory for IPv6.

Typical IPSec Scenario



Source: Figure 19.1 from William Stallings – Cryptography and Network Security, 5th Edition

IPSec

- A security association is characterized by the following parameters:
  - Encryption algorithm (DES, AES and etc.)
  - Encryption key
  - Encryption parameters such as the Initialization Vector
  - Integrity/ Authentication algorithms (keyed-HMAC algorithms) and the key
  - Lifespan of the association
- We cannot simply use a cryptographic hashing algorithm like SHA or MD5 that gives a message authentication code dependent only on the message to be sent.
- Note that to achieve both integrity and authentication simultaneously with the Authentication header, we want to compute a message authentication code that is dependent on both the message and the authenticity of the sender of the message.
- If the two communicating parties can agree on a shared secret session key, then the secret key could be used in combination with a cryptographic hash function to obtain what is called a keyed-Hash Message Authentication Code (HMAC).
- Any iterative cryptographic hash function like SHA-1 or MD5 may be used in the calculation of an HMAC; the resulting MAC algorithm would be accordingly termed as HMAC-SHA-1 or HMAC-MD5.
- The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size and quality of the key and the size of the hash output.

IPSec

- A security association (SA) is uni-directional. For two hosts to communicate in either directions, SAs have to be established separately in either directions.
- For host A to securely send data packets to host B, and make host B to believe that the data packet did come from host A, it should establish a SA with host B. Such a SA is said to be “outbound” at A and “inbound” at B.
- An IPSec header of a datagram sent from host A to host B, should have the secure features of the SA that is “inbound” at B and similarly the IPSec header of a datagram sent from host B to host A should have the secure features of the SA that is “inbound” at A.
- Prior to establishing a IPSec SA, the two end hosts need to exchange their public-key certificates digitally certified by a trusted third-party certificate authority (CA). This is done through the Internet Key Exchange (IKE) protocol. Once two hosts have exchanged each other’s public-key certificates, then they are said to have established an IKE Security Association (IKE SA).
  - Establishing an IKE SA is a pre-requisite to establish an IPSec SA.

IPSec

- Establishing a Security Association
  - Host A wishing to send data packets to host B needs to establish an "inbound security association" with host B
  - Host A picks a SPI that has not been yet chosen for communications with host B and sends a "SA Establishment Request" to B. This message is encrypted with the public key of Host B and contains the following:
    - SPI for the inbound SA channel at host A (i.e., the outbound SA channel at host B)
    - Lifespan of the association.
      - This could be negotiated by host B.
    - The packet-level security protocol chosen (protocol ID: 51 for AH or 50 for ESP)
      - This could be also negotiated by host B.
    - If AH is chosen, then the list of keyed-HMAC algorithms that could be used is specified. Host B will choose one from this list if it wishes to receive packets from host A.
    - If ESP is chosen, then the list of keyed-HMAC algorithms along with the list of encryption algorithms and key-derivation functions that could be used will be sent.
  - Hosts A and B will basically exchange a series of messages negotiating the lifespan of the association, the packet-level security protocol to be used and the appropriate keyed-HMAC and encryption algorithms, key-derivation function to be used.

IPSec

- Establishing Security Associations
  - All negotiation messages will be encrypted at the sender side using the public key of the receiver and will be decrypted with the private key of the receiver at the receiver side.
  - Hosts A and B agree on a shared session key using the Diffie-Hellman exchange algorithm.
  - The shared session key would be used for the keyed-HMAC algorithm.
  - Each host would use the shared session key and the key-derivation function agreed upon to derive the secret key that would be used for encryption of the data at host A and decryption of the data at host B.

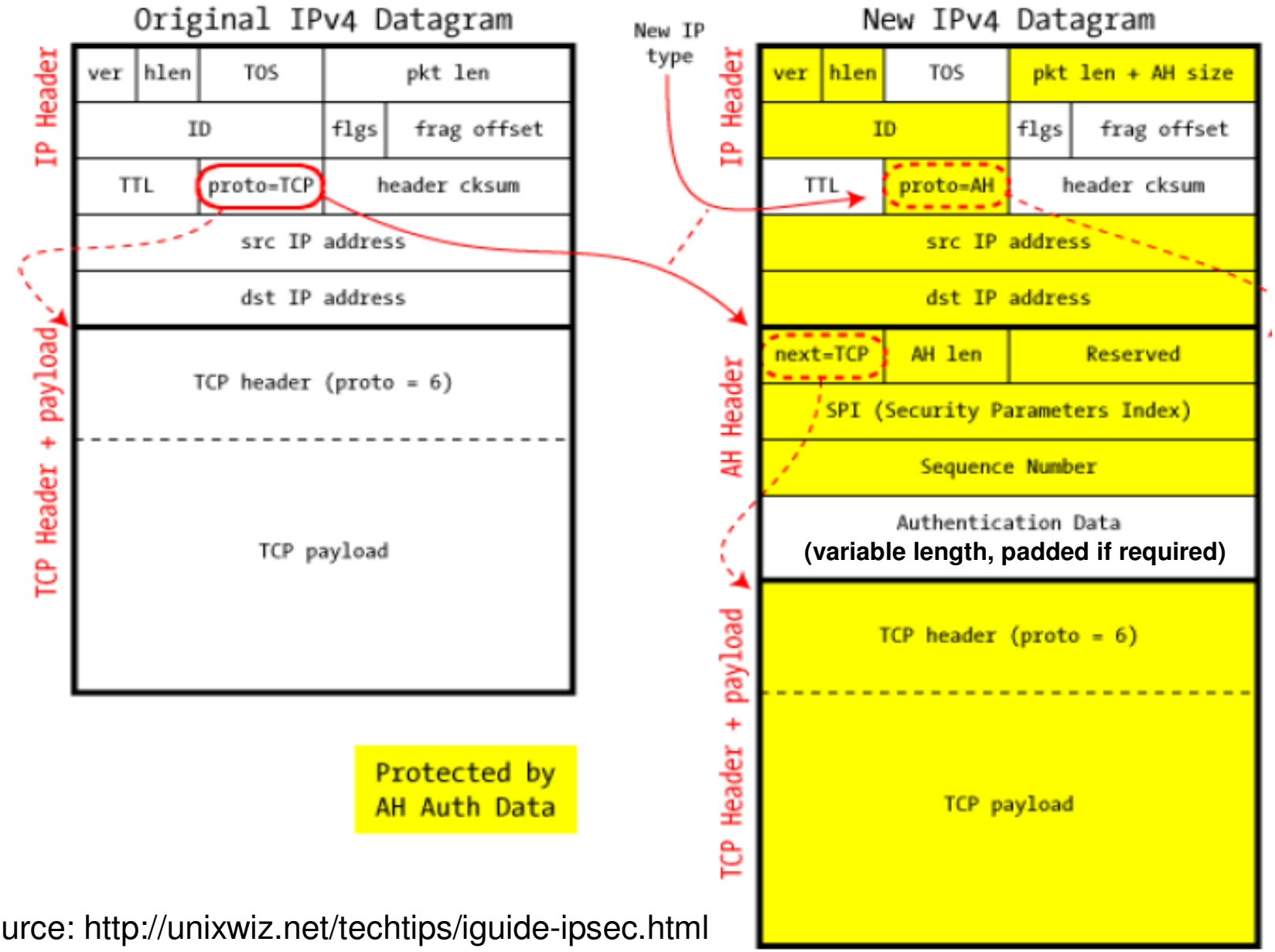
- Summary of Steps to establish a security association from host A to host B
  - IKESA: Exchange of public-key certificates between hosts A and B
  - Sending the “SA Establishment Request” from host A to B.
  - Negotiation of the parameters, algorithms and key-derivation functions for $SA_{A->B}$
  - Diffie-Hellman exchange algorithm to agree on a shared session key that will also be used for keyed-HMAC algorithm
  - Generation of the shared secret key for encryption/decryption using the session key and the agreed upon key-derivation function

IPSec Authentication Header

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

- Next Header – identifies the transport layer protocol
- Payload length (AH length) – The length of the whole Authentication Header (AH) in 32-bit words
- Reserved – This field is reserved for future use and must be zero.
- SPI – 32-bit field to identify the SA
- Sequence Number – This is a monotonically increasing identifier (incremented, starting from 0, for every datagram sent on the SA) that is used to assist in anti-replay protection. If the sequence number value reaches 2^{32-1}, the SA has to be terminated and a new SA has to be formed. This prevents replay attacks.
- Authentication Data: This is the integrity/ authentication check value (keyed-HMAC) calculated over the entire packet – including the header fields that do not change at the intermediate hosts.
  - The size of the keyed-HMAC may vary with each SA and may not be exactly multiple of 32-bits. If this is the case, the HMAC will be padded.

IP4 Datagram with Authentication Header



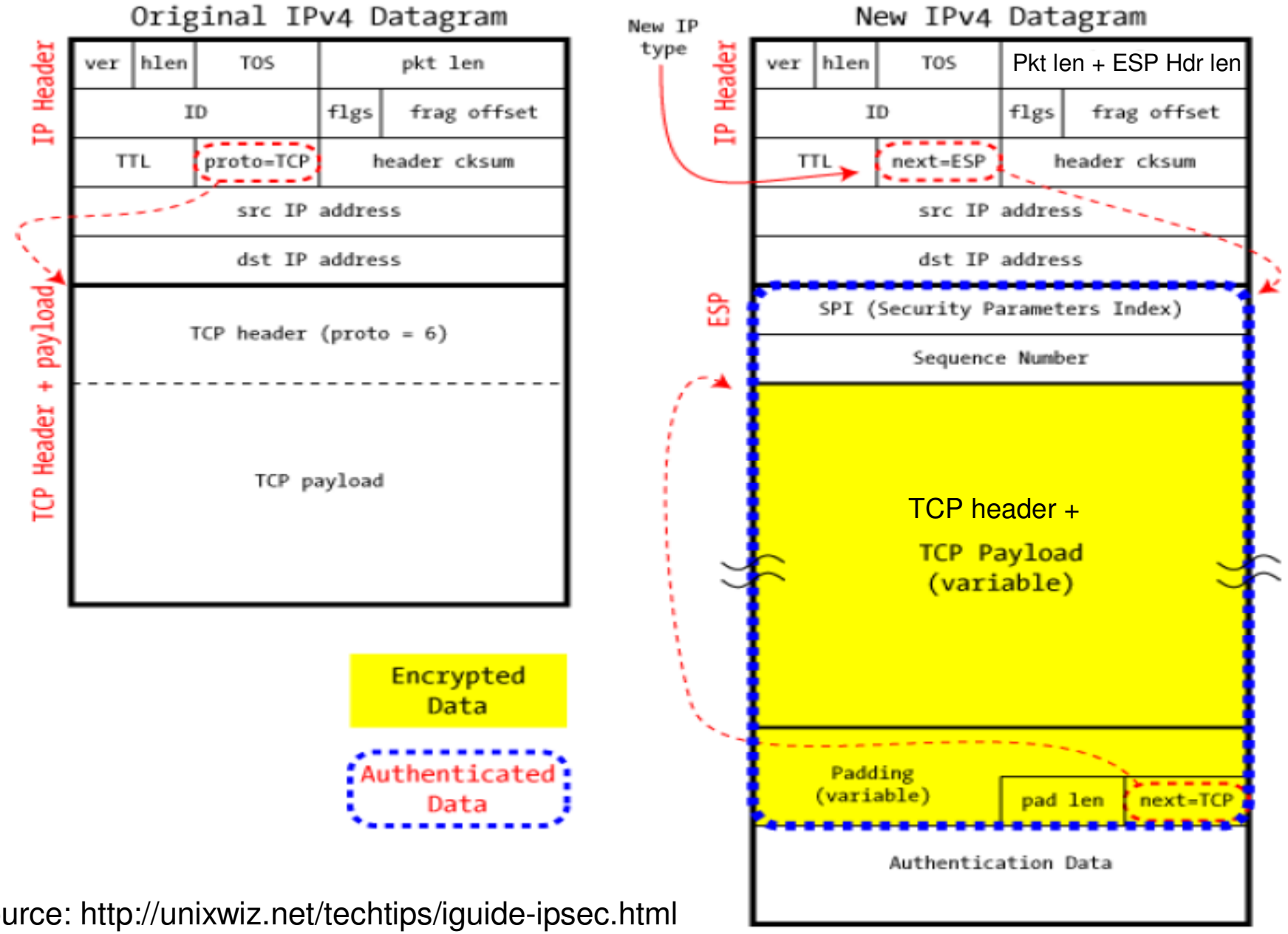
Source: http://unixwiz.net/techtips/iguide-ipsec.html

IPSec ESP Header

<table>
<tr><th>0 - 7 bit</th><th>8 - 15 bit</th><th>16 - 23 bit</th><th>24 - 31 bit</th></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (variable)</td></tr>
<tr><td></td><td colspan="2">Padding (0-255 bytes)</td><td></td></tr>
<tr><td></td><td></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (variable)</td></tr>
</table>

- SPI – 32-bit field to identify the SA
- Sequence Number – This is a monotonically increasing identifier (incremented for every datagram sent on the SA) that is used to assist in anti-replay protection.
- Payload data – the data to be transferred.
- Padding – Used with some block ciphers to pad the data to the full length of a block.
- Pad length – size of padding in bytes.
- Next header – identifies the transport layer protocol
- Authentication Data: This is the integrity/ authentication check value (keyed-HMAC) calculated over only the SPI, Sequence Number in the ESP header, the actual data, padding data, pad length and the next header field.

IP4 Datagram with ESP Header



Source: http://unixwiz.net/techtips/iguide-ipsec.html

Firewalls

- A firewall is a device that filters traffic between a “protected” or inside network and a “less trustworthy” or outside network.
- A firewall is basically an executable code run on a dedicated computer.
- As all traffic should pass through the firewall, it should not be a point of bottleneck for system performance and hence non-firewall functions are not performed on that machine running the firewall.
- Also, since non-firewall code does not exist in the computer, it is hard for an attacker to make use of any vulnerability to compromise the firewall.

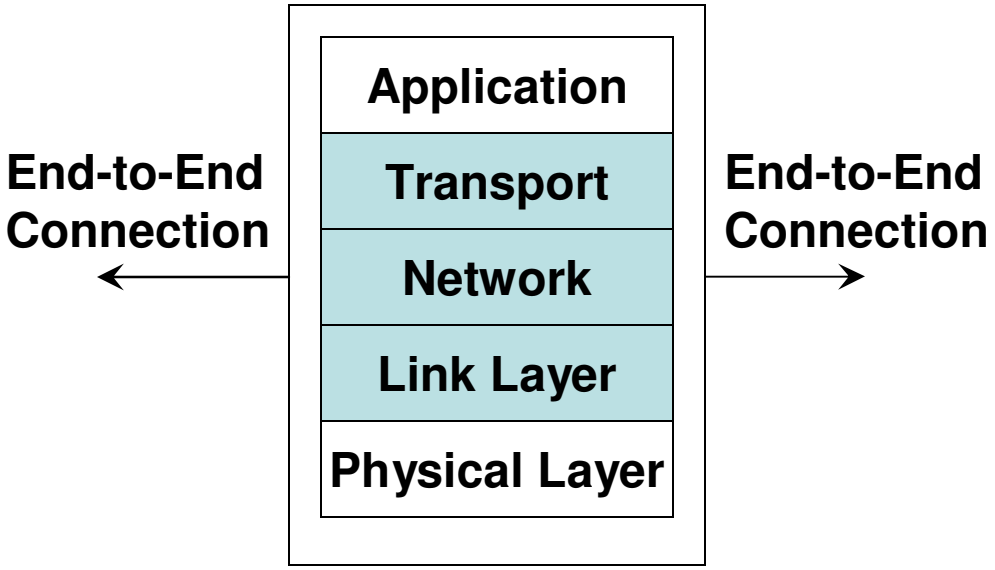
- Design idea:
  - Firewalls implement a security policy that is specifically designed to address what bad things that should not happen in a “protected environment”
  - Security policies that dictate what to allow: Standard security practices dictate a “default-deny” ruleset for firewalls, implying that the only network connections allowed are the ones that have been explicitly stated to be allowed.
  - Security policies that dictate what not to allow: Users and business community who lack such a detailed understanding to explicitly state what should be allowed in prefer a “default-allow” ruleset, in which all traffic is allowed unless it has been specifically blocked.
    - Even though this configuration is relatively more prone to inadvertent network connections and system compromise, it is more commonly used because of mere lack of knowledge and new applications that come into existence.

Firewalls

- Not all firewalls need to have the same capability.
- One cannot compare the “goodness” of two firewalls based on the security policies they are configured with.
  - **The key factor that drives the selection of a security policy for a firewall is the threats that an installation (network) needs to avoid happening.**
- **Packet Filters**
- A packet filtering firewall controls access to packets on the basis of packet address (source or destination) or specific transport protocol type (such as HTTP, Telnet, etc)
  - **Egress filtering:** Packets would be sent out (or not to be sent out) only to specific networks and/ or belonging to specific transport layer protocols.
  - **Ingress filtering:** Packets belonging to (not belonging to) only certain source networks and/ or specific transport layer protocols could be let in.
- A common strategy to avoid IP spoofing attacks is to have the packet filter configured not to let in packets having a source address that corresponds to the internal network.
  - In other words, the attacker has spoofed the source IP address to be the IP address of a machine belonging to the network being protected by the firewall.
- The code for packet filters will become lengthy as we want to block traffic belonging to specific networks, IP addresses and transport layer protocols.

Attacks Prevented using Packet Filter Firewalls

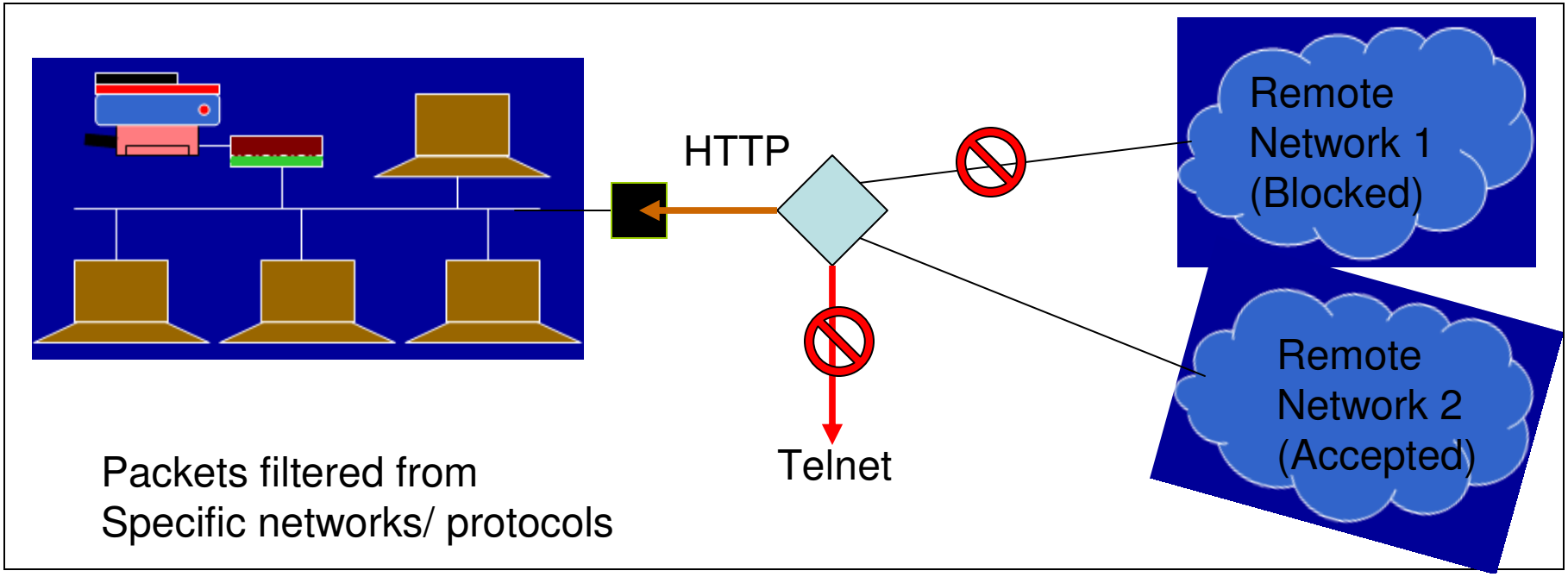
- In addition to IP spoofing attacks, packet filter firewalls could also be configured to avoid source routing and tiny fragmentation attacks.
- Source routing attacks: where source specifies the route that a packet should take to bypass security measures, should discard all source routed packets
- Tiny fragment attacks: intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into fewer separate fragments to circumvent filtering rules needing full header info; can enforce minimum fragment size to include full header.

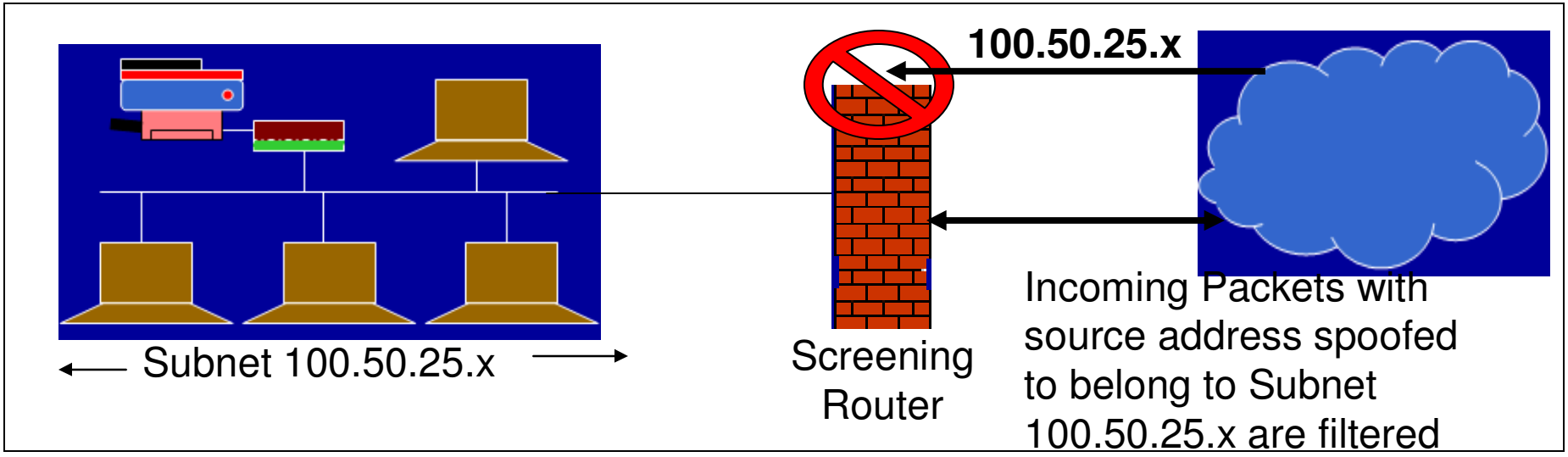


Layers supported by Packet Filter and Stateful Firewalls

Source (adapted from): Figure 22.1(b) from William Stallings – Cryptography and Network Security, 5th Edition

Packet Filters



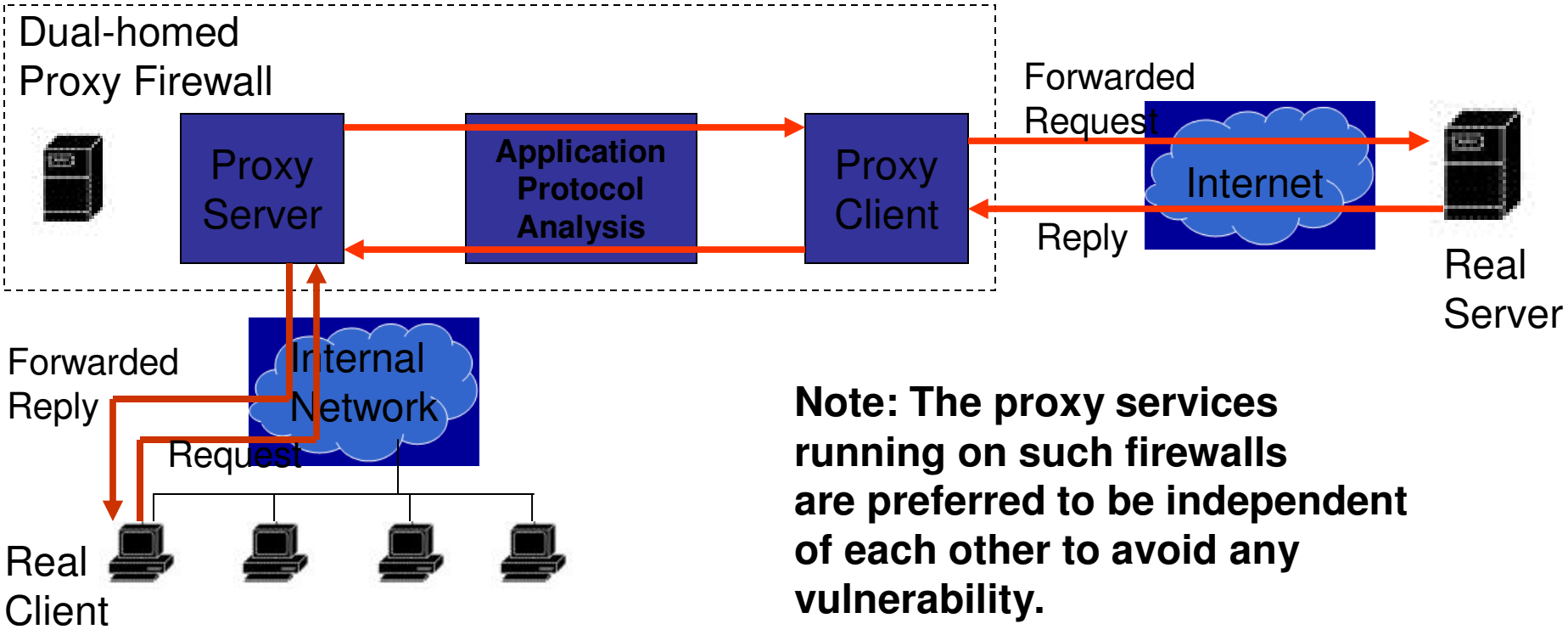


Stateful Inspection Firewalls

- Firewalls based on packet filters operate on packets on an individual basis and do not store the state information pertaining to the action taken on a packet processed earlier.
- Stateful firewalls (also called circuit firewalls) examine the contents of each packet with regards to their placement within the packet series belonging to a specific connection.
- Stateful firewalls maintain records of all connections passing through the firewall and is able to determine whether a packet is the start of a new connection or part of an existing connection.
- Stateful firewalls can remember the sequence numbers expected on both sides as part of a TCP session and can block attempts to hijack the session, when an intruder sends several TCP segments with different sequence numbers (trial-and-error).
- The state of a connection will be a criteria to trigger specific rules of the firewall.
  - Examples:
    - Data packets for a connection cannot get in before the connection is completely established and after a connection is completely teardown.
    - Do not let more than a certain number of simultaneous TCP connections to originate per IP address.
    - Do not let more than a specific amount of data to be transferred per day from the inside network to any outside IP address.

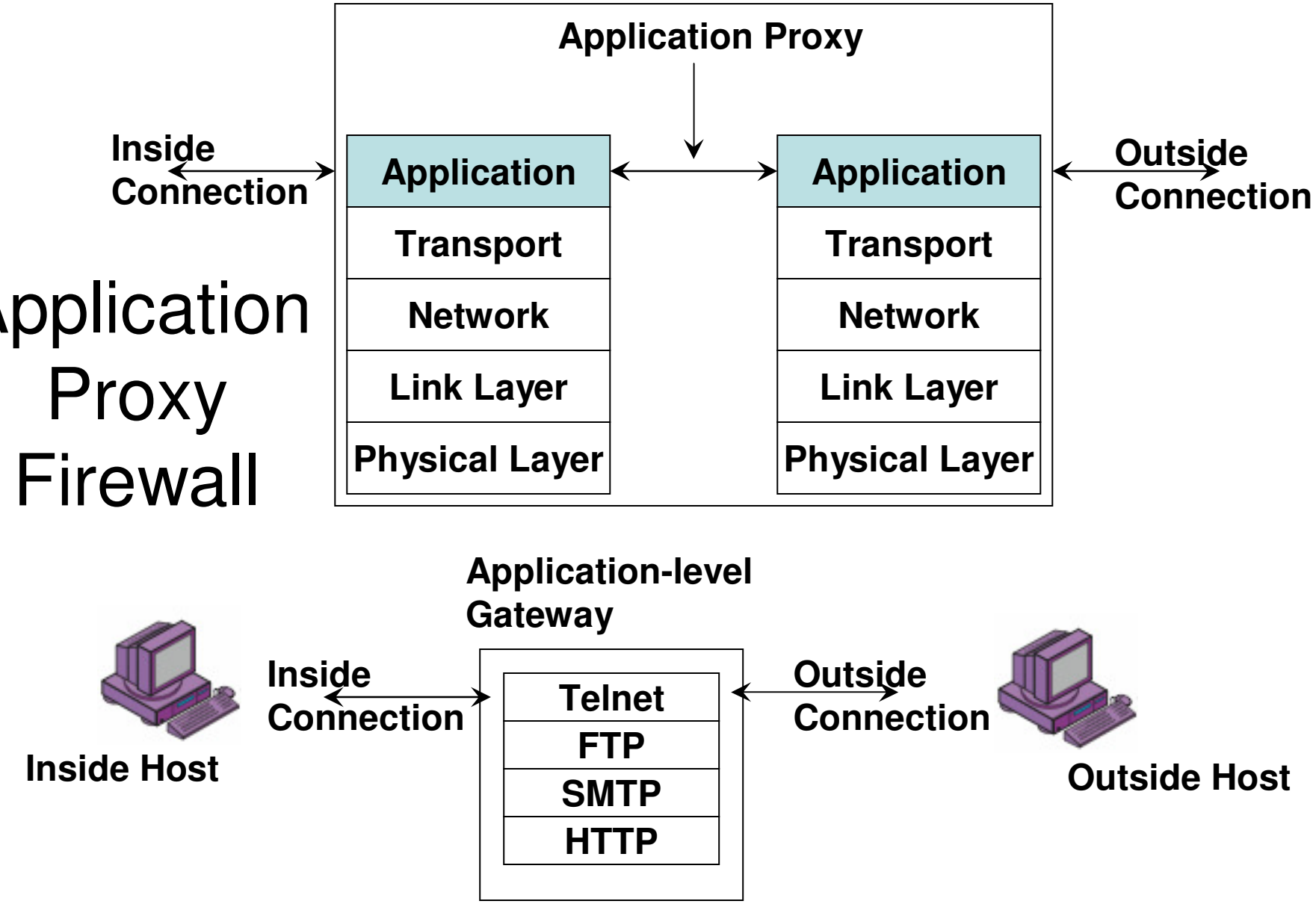
Application Proxy Firewall

- Packet filters look only at the headers of the packets, not at the data inside the packets.
- An application layer firewall (proxy; also called as bastion) simulates the proper effects of an application so that the application receives only requests to act properly.
- A proxy gateway is a two-headed device: It looks to the inside as if it is the outside (destination) connection; while to the outside, it responds as it is from the inside.



Note: The proxy services running on such firewalls are preferred to be independent of each other to avoid any vulnerability.

Application Proxy Firewall



Source (adapted from): Figure 22.1(d) from William Stallings – Cryptography and Network Security, 5th Edition

Application Proxy Firewall

- Each application proxy in the firewall requires two components: a proxy server and a proxy client.
- All communication between internal users and the Internet passes through the proxy server rather than allowing users to directly communicate with servers on the Internet.
- An internal user (client) sends a request to connect to an external service. The request goes through the Application Proxy Firewall that runs a proxy server for that particular service being requested.
- The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service.
- Proxy servers allow only those packets that comply with the services of the application protocol.
- Proxy servers are also useful to collect audit records of session information
- If the proxy server approves the request, it forwards that request to the proxy client.
- The proxy client then contacts the real server on behalf of the real client and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server.
- The proxy server relays requests and responses between the proxy client and the real client.

- Note: The above discussion assumes the client is in the internal network and the server is in the external network. The same discussion applies for the other scenario too:
  - The real client (from the outside network) contacts the proxy server, the proxy server evaluates the request and forwards to the proxy client, the proxy client contacts the real server (running in the internal network).
  - The proxy client forwards the response from the real server to the proxy server, which forwards the response to the real client (in the outside network).

Examples of using Proxy Firewall

- Scenario 1: A company wants to allow dial-in access by its employees, without exposing its company resources to login attacks from remote non-employees. Suppose the internal network has a mixture of operating system types, none of which support strong authentication through a challenge-response system.
- Solution:
  - The requirement could be handled by a specifically written proxy that requires strong authentication such as a challenge-response, in addition to a valid username and corresponding password.
  - The proxy validates the challenge-response itself, and then pass on only the username and password in a form required by the internal host's operating system.
- Scenario 2: A company wants to set up an online price list so that outsiders can see the products and prices offered. It wants to be sure that (a) no outsider can change the prices or product list and (b) outsiders can access only the price list and not any of the more sensitive files stored inside.
- Solution:
  - The requirement could be handled by a specifically written proxy that monitors the file transfer protocol data to ensure that only the price list file was accessed, and that the file could be only read, not modified.

- Note: A proxy firewall can also function more as a guard, monitoring the amount and quality of data exchanged.
  – It could keep track of the amount of data exchanged per user from the internal network and deny access if exceeded a pre-defined limit.
  – A proxy firewall could also run a virus scanner to scan all the incoming files and if required outgoing files too.

Personal Firewalls

- Motivation: Home users, individual workers, and small businesses use cable modems or DSL connections with unlimited, always-on access.
- These people need a firewall, but a separate firewall computer to protect a single workstation can seem too complex and expensive.

- A workstation could be vulnerable to malicious code or malicious active agents (ActiveX controls or Java applets), leakage of personal data stored in the workstation, and vulnerability scans (like nmap) to identify potential weaknesses.
- A personal firewall is an application program that runs on a workstation to screen traffic on the workstation and block unwanted traffic leaving or entering the workstation to the network to which it is connected.
- A user could configure the personal firewall to accept traffic only from certain sites, and not from specific sites, and to generate logs of activities happened in the past
- A personal firewall could be also configured with a virus scanner which would be then automatically invoked to scan any incoming data to the workstation.

- A static machine is a vulnerable target for the attack community and adding a personal firewall can save it more secure compared to machines that are not behind such a firewall.

Comparison of Firewall Types

Packet Filtering	Stateful Inspection	Application Proxy	Personal Firewall
Simplest	More complex	Even more complex	Similar to packet filtering firewall
Sees only network addresses and service protocol types	Can see either addresses or data	Sees full packet	Can see full packet
Auditing difficult	Auditing possible	Can audit activity	Can and usually does auditing activity
Screens based on connection rules	Screens based on information across packets – in either header or data field.	Screens based on behavior of proxies	Screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually pre-configured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	User adds trusted addresses to the firewall as they appear

What Firewalls Can and Cannot Block

- Firewalls cannot alone secure an environment.
- A firewall protects only the perimeter of its environment against attacks from outsiders who want to execute code or access data on the machines in the protected environment.
- Firewalls cannot protect from internal threats (through disgruntled employees).
- Firewalls cannot protect against malware imported via laptop, PDA, or portable storage device infected outside the network, then attached and used internally.
- Firewalls can be held responsible for any security breach in if they are the only means to control the entire network perimeter.
  - If a host in the inside network has a connection to the outside network through a modem, the whole of the inside network is exposed to the outside network through the modem and the host. A firewall cannot be responsible for any attack
- Firewalls cannot protect data after they have left them.
- A firewall is often a single point of failure for a network.
  - A more layered approach like a screening router, followed by a proxy firewall, followed by a personal firewall may be more helpful.
- Firewalls must be frequently configured and updated to take into account the changes in the internal and external environment and based on the review of the firewall activity reports that may indicate intrusion attempts.
- The machine hosting the firewall code will not have any other software like an editor, compiler, etc. in order to reduce the chances of an attack.

Secure Shell (SSH)

- Goal: To allow the user to securely interact with remote machines.
- Three steps:
  - Host identification: The client needs to establish that it is talking to the machine it is asked to, and not another machine that is spoofing it.
    - (Optional) The server on the remote machine may also want to establish that the user is connecting from the machine it appears to be, and not another machine that is spoofing it.
  - Encryption: Establishing an end-to-end link whose data transfers are encrypted, so that no-one who is observing the network can derive any information from it.
    - Note that this happens before authentication occurs, so any passwords or other authentication information will not be transmitted in clear text.
  - Authentication: The user proves to the server that he/she has the right to perform operations as a particular user on the server machine.

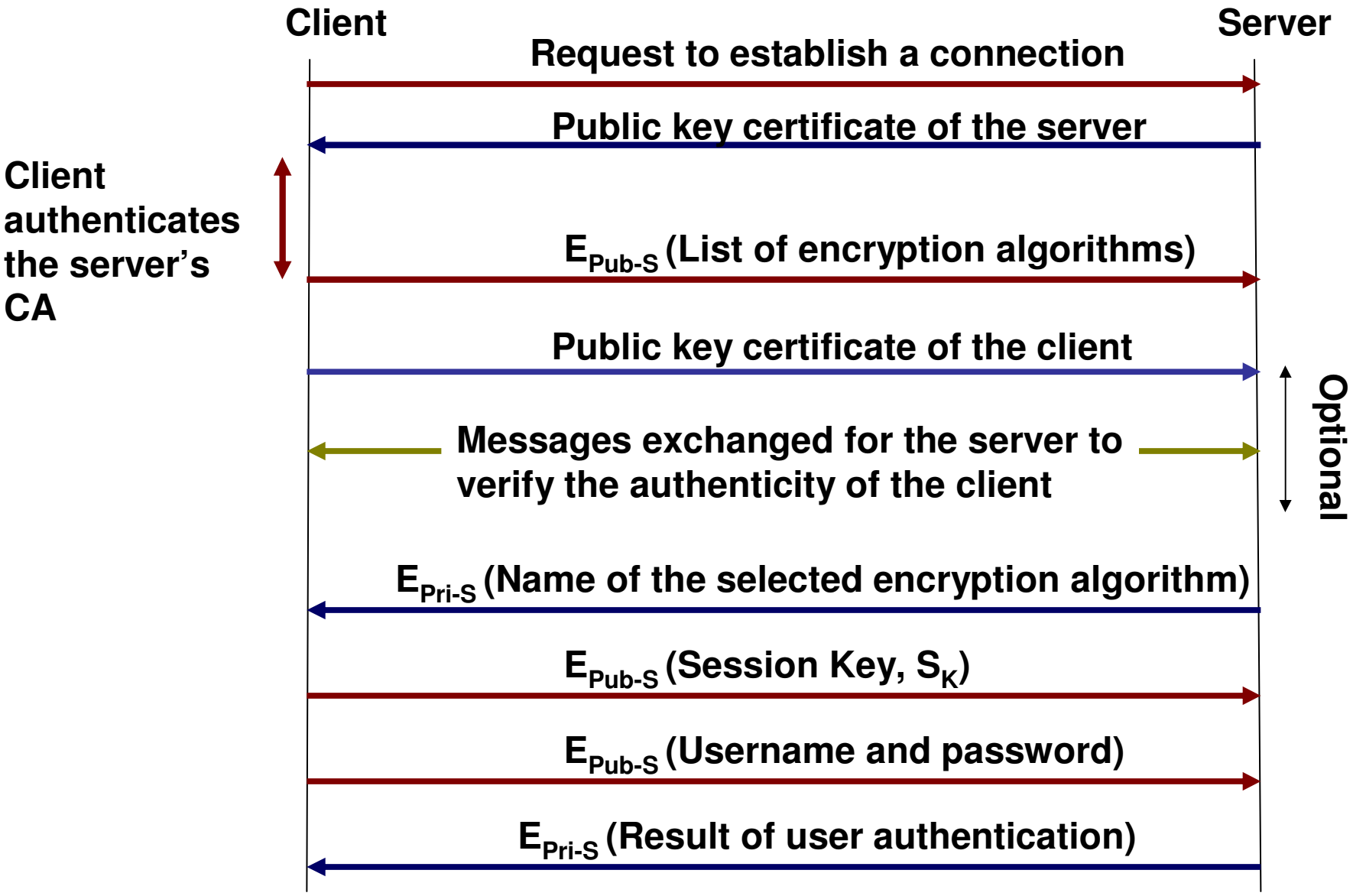
Secure Shell (SSH)

- Host identification:
  - The client contacts the server and requests for its public key certificate
  - The client maintains a list of public keys for server machines available to it. If it is asked to contact a machine for which it does not have a public key locally held, it will warn the user with a message telling that the public key reported by the server is not in the list of known hosts and ask the user whether the user wants to continue connecting
  - If the user agrees to continue connecting, the client verifies the authenticity of the CA issuing the public key certificate and if satisfied, accepts the public keys. The server's public key will be added to the machine's personal list of host public keys.
  - When the administrator has included the public key for the client machine in the per-machine list of known host public keys on the server machine, the server may want the client machine to prove that it is what it claims to be.
    - The server will create a "challenge" encrypted with the client's host public key and sends it to the client.
    - Only if the client machine is genuine, it will be able to decrypt this message with its own private key.
    - The client machine then sends the same "challenge" encrypted with the public key of the server.
    - The server when decrypting the message gets the same "challenge" it sent, the client is genuine.

Secure Shell (SSH)

- Encryption:
  - Once the host identification is successfully done, the client sends a list of encryption algorithms it could use and their corresponding keys. This is sent encrypted with the public key of the server.
  - The server decrypts the list with its private key and chooses the most strongest encryption algorithm that it could handle from the list sent by the client.
  - The server then notifies the selected encryption algorithm to the client by encrypting the notification using its private key.
  - The client then generates the appropriate secret session key that will be used for the encryption algorithm selected. The client notifies the secret session key to the server by encrypting the notification with the server's public key.
  - The server decrypts the notification with its private key and extracts the secret session key.
- User Authentication:
  - The client asks for the username and password from the user, encrypts them with the server's public key and sends to the server.
  - The server checks the validity of the username and password and if everything is fine, okays the connection by sending the confirmation that is encrypted with its private key.
  - The client decrypts the confirmation with the server's public key and the client and server are all set to exchange data securely using the encryption algorithm selected and the secret session key agreed upon

Secure Shell (SSH)



Wireless Security

- Wireless computing requires measures to protect communications between a client computer and a wireless base station or access point.
- As communication in a wireless network happen on predefined frequencies, an eavesdropping attacker can attempt to intercept and impersonate.
- Pieces to protect: Finding the access point, authenticating the remote computer to the access point, and protecting the communication stream.
- Service Set Identifier (SSID): The SSID is a 32-character unique identifier attached to the header of the packets transmitted in a Wireless LAN.
  - The SSID uniquely identifies a Wireless LAN (WLAN).
  - The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.
  - The SSIDs of WLANs in a given area need to be unique to distinguish the WLANs.
  - Mode of joining a WLAN:
    - Open Mode: The Access point of a WLAN keeps broadcasting its SSID. A user will intercept and pick the SSID he/she wants to join; Same applies to an attacker.
    - Closed or Stealth Mode: The user picks up an SSID to join and broadcasts the request. The Access point (AP) configured for the particular SSID will respond.
  - SSID cannot be used for authenticating a mobile user trying to connect to a WLAN as it could be easily sniffed during the initial set up phase or during the joining phase.

Wired Equivalent Privacy (WEP)

- WEP is a flawed algorithm to secure IEEE 802.11 wireless networks.
- Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks.
- WEP uses a stream cipher called RC4 for confidentiality and CRC-32 for integrity.
- WEP is available in 64-bit (WEP-40), 128-bit (WEP-104) and 256-bit (WEP-232) forms:
  - All these forms use a 24-bit initialization vector (IV)
  - The advantage of an initialization vector is that two different IVs when used with the same plaintext and same encryption key will result in two different cipher texts.
  - WEP-40, WEP-104 and WEP-232 use respectively the first 40 bits, the first 104 bits and the first 232 bits of the user entered key for encryption
- A four-way challenge-response handshake is used for authentication:
  - The client station sends an authentication request to the access point.
  - The access point sends back a clear-text challenge.
  - The client has to encrypt the challenge text using the configured WEP key, and send it back as the challenge response.
  - The access point decrypts the challenge response using the WEP key configured for the client and compares it with the clear-text it had sent.
  - Depending on the success of this comparison, the access point sends back a positive or negative response.

Working of WEP

- The 24-bit IV is randomly generated at the sender side.
- The 40-bit or 104-bit user encryption key will be concatenated with the 24-bit ICV and used in the RC4 stream cipher.
- The output of the RC4 stream is XORed with the plaintext to get the final encrypted data, the ciphertext.
- A 32-bit Integrity Check Value (ICV) is computed on the plaintext using the CRC algorithm and the 32-bit generator $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$
- The transmitted frame has the 24-bit IV (in clear) as the first 3 bytes of the payload portion, the encrypted cipher text of the original plaintext data and the 32-bit ICV of the plaintext computed using the CRC algorithm.
- The receiver uses the 24-bit IV and the WEP key to decrypt the encrypted data using RC4 stream cipher and extract the plaintext. This provides confidentiality.
- The receiver runs the CRC algorithm on the extracted plaintext and determines the ICV based on the extracted plaintext. If this ICV value matches with the ICV received from the sender, then the plaintext is assumed to have been received without any tampering.

Weaknesses of WEP

- The 24-bit IV is sent in clear text on the wireless channel and is prone to interception.
- An attacker who could obtain several cipher text messages for the same 24-bit IV, use them for cryptanalysis and determine the plaintext or the WEP key
- The WEP key is often not changed until the user enters a new key at the client and access point.
- The size of the Integrity check value needs to be increased to 64-bits or 128-bits and a more stronger hashing algorithm like SHA-1 or MD5 is needed to compute the ICV.
- The four frames exchanged during challenge-response handshake can be captured and used in a brute-force attack to derive the WEP key.
- Since the encrypted portion of the frame could be subjected to an cryptanalytic attack, an attacker could change portions of the extracted text, compute the ciphertext and a 32-bit CRC using the modified text and send it to the other side.

WiFi Protected Access (WPA)

- The alternative to WEP is WiFi Protected Access (WPA), approved in 2003. The IEEE standard 802.11i, now known as WPA2, was approved in 2004 and is an extension of WPA2.
- Users are asked to enter a passphrase that could be from 8 to 63 printable ASCII characters. A hash function reduces the 504 bits (63 characters * 8 bits per character) to 256 bits.
  - To prevent brute-force attacks users are required to enter at least a 20-character passphrase.
- A 128-bit initial temporal key for encryption and 64-bit key for computing message integrity check would be derived from the 256-bit passphrase.
- Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit Initialization vector
- Temporal Integrity Key Protocol:
  - Using the passphrase, the client and the access point will derive 128-bit temporal keys (valid for only a certain time) using sophisticated key-derivation functions.
  - The 48-bit initialization vector is basically a 48-bit sequence number used per temporal key and is not sent as clear-text.
  - The sequence number is initialized to 0 and is incremented for every packet sent with a temporal key.
  - When the temporal key is changed, the sequence number is reverted to 0.
- The message integrity check (MIC) is 64-bits in size and is computed using an algorithm called “Michael” and is similar to the CRC.

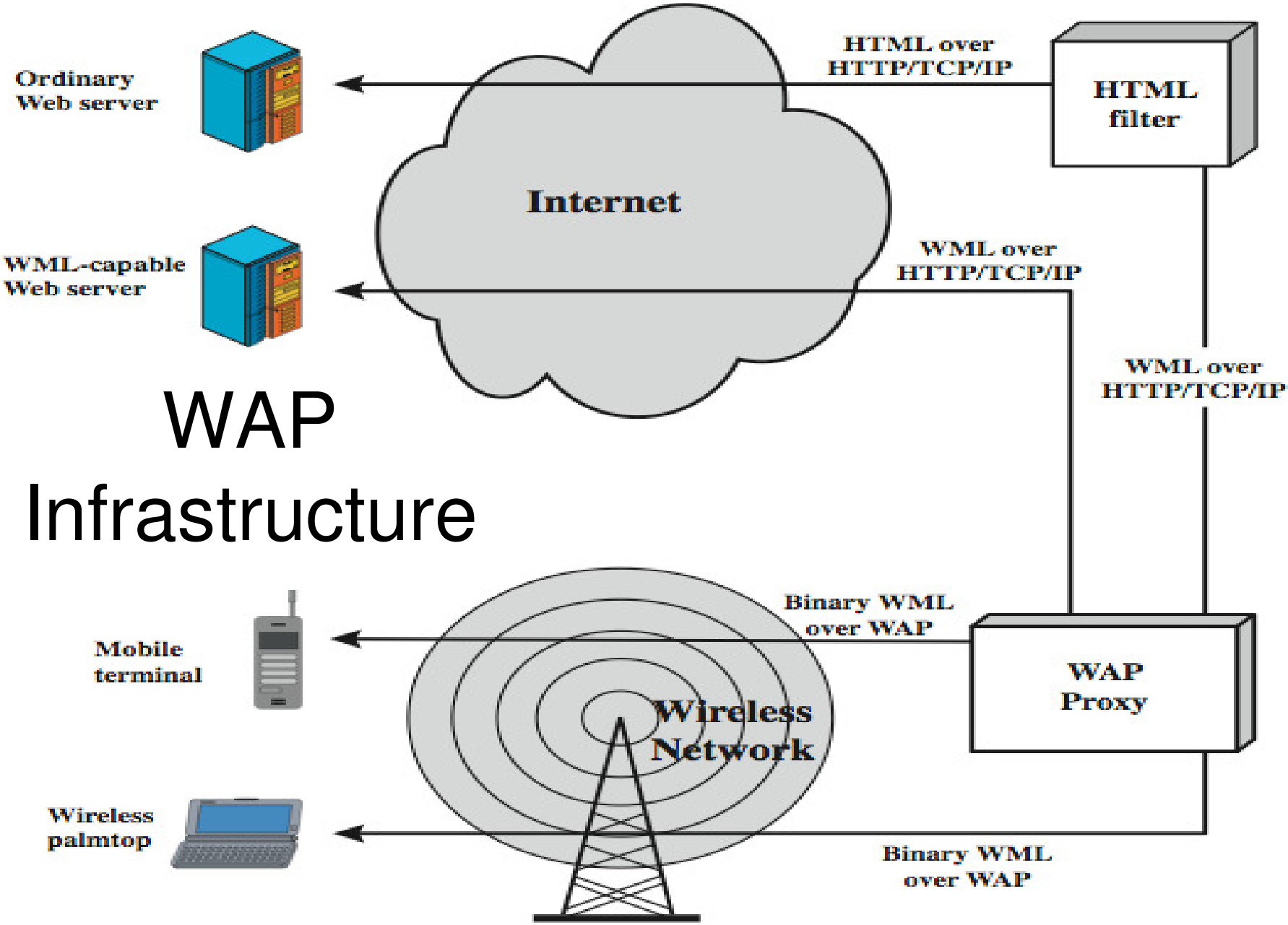
Mobile Phones and Standards

- Almost all current mobile phones have wireless networking features built-in.
- Strongly affecting the use of mobile phones and terminals for data services are the significant limitations of the devices (in processors, memory, and battery life) and the networks (relatively low bandwidth, high latency, and unpredictable availability and stability) that connect them.
- The user interface is also limited, displays are small, and all these features vary widely across terminal devices and networks.
- The Wireless Application Protocol (WAP) is a well-known standard for data communication through mobile devices.
- Mobile phones have advanced with new technologies and services, causing phone and the carrier networks that support them to be described in generations:
  - 1G: refers to the original analog cellular standard (Advanced Mobile Phone System, AMPS).
  - 2G: refers t o the digital cellular network
  - 3G: system of mobile networks allowing carriers to offer a wide variety of services to the consumer, including broadband data service and video calling.
  - 4G: refers to the planned move to an entirely IP-based network for all services, running voice over IP (VoIP) on the mobile phone.

Wireless Application Protocol (WAP)

- The Wireless Application Protocol (WAP) is a universal, open standard developed by the WAP Forum to provide mobile users of wireless phones and other wireless devices, access to telephony and information services.
- WAP is designed to work with all wireless network technologies (e.g., GSM, CDMA, TDMA).
- The current release of the WAP specification is version 2.0.
- The WAP Programming Model is based on three elements: the client, the gateway, and the original server.
- The gateway acts as a proxy server for the wireless domain. Its processor(s) provide services that offload the limited capabilities of the hand-held, mobile, wireless terminals.
- For example, the gateway provides DNS services, converts between WAP protocol stack and the WWW stack (HTTP and TCP/IP), encodes information from the Web into a more compact form that minimizes wireless communication, and, in the other direction, decodes the compacted form into standard Web communication conventions.
- The gateway also caches frequently requested information.

WAP Infrastructure

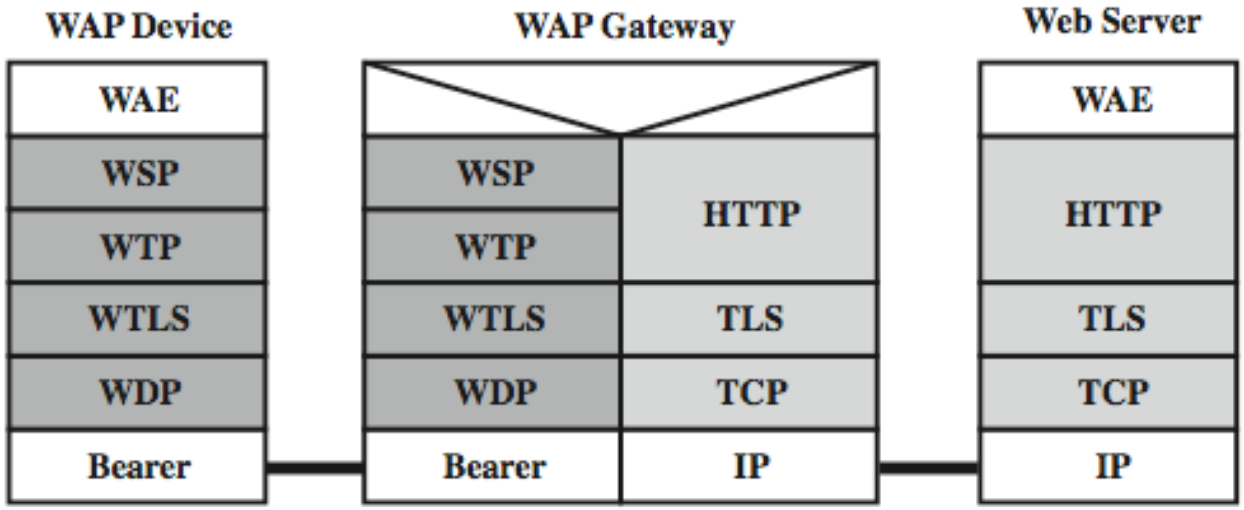


Source: Figure 17.12 from William Stallings – Cryptography and Network Security, 5th Edition

WAP Protocol Suite

Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)
**** Any Wireless Data Network ****

Source: Wikipedia



Source: Figure 17.14 from William Stallings – Cryptography and Network Security, 5th Edition

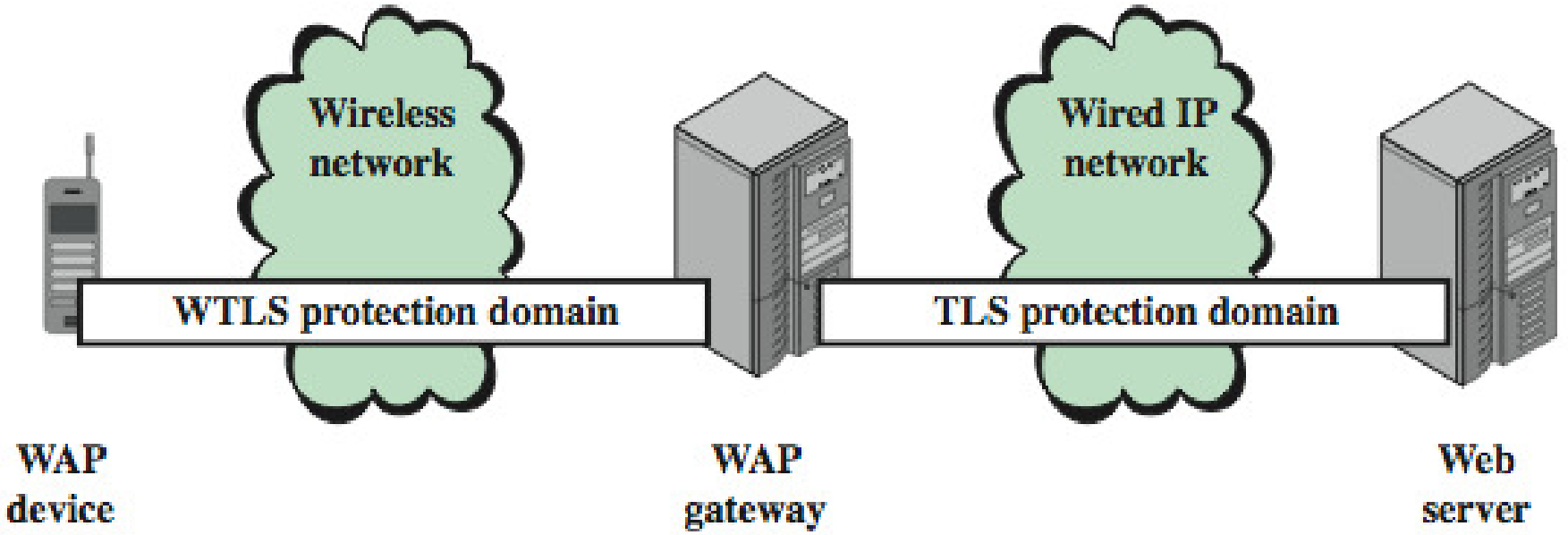
WTLS

- WAP uses the Wireless Transport Layer Security (WTLS) scheme to offer confidentiality in wireless communications.
- The originator and the recipient, both have the keys the decrypt the data and extract the plaintext.
- The TLS protocol that WTLS is based on is designed around Internet-based computers, machines that have relatively high processing power, large amounts of memory, and sufficient bandwidth available for Internet applications.
- The PDAs and other devices that WTLS must accommodate are limited in all respects. Thus, WTLS has to be able to cope with small amounts of memory and limited processor capacity, as well as long round trip times that TLS could not handle well.
- The above requirements are the primary reasons for WTLS to have security issues.
- WTLS supports the encryption algorithms: DES, 3DES and IDEA encryption algorithms; the SHA and MD5 algorithms for generating message authentication codes. All of these algorithms are agreed (between the client and WAP gateway) during the handshake period.

WTLS

- Owing to low memory and/or CPU capabilities, the mobile devices can support only weak encryption (if at all possible) as well as optional authentication. The above weaknesses, combined with the inherent vulnerabilities (such as the alert message truncation attack) of the WTLS algorithm, result in little to no security.
- The “Alert Message Truncation Attack,” is related to terminating a WTLS connection using an unencrypted TCP FIN message that could be inserted (by an attacker) in the middle of a communication session through session hijacking.
- WAP Gap Problem: As WTLS and TLS are used as the security protocols for the WAP network and the Internet respectively, the WAP gateway has to perform translation from one encryption standard to the other. This translation forces all messages to be seen by the WAP gateway in plaintext. A WAP gateway is hence an appealing target to attackers as plaintext messages from all wireless devices (not just a single user) are processed at it.

WAP Gap Problem

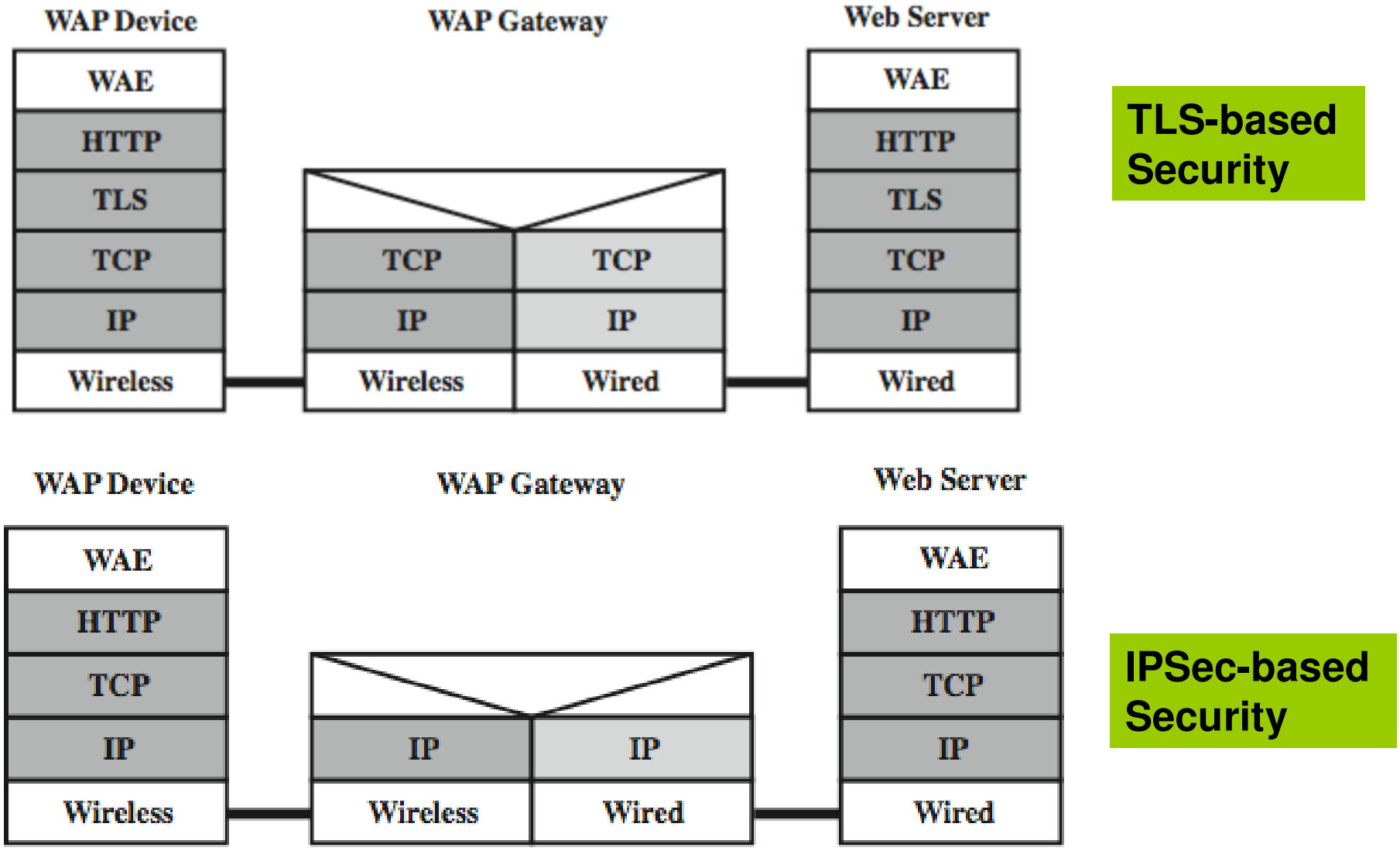


Source: Figure 17.19 from William Stallings – Cryptography and Network Security, 5th Edition

Solution to the WAP Gap Problem

- The preliminary version of WAP (v. 1) assumed a simplified set of protocols (the WAP protocol suite) over the wireless network and assumed that the wireless network does not support IP.
- The more recent WAP 2.0 version provides the option for the mobile devices to implement the full TCP/IP-based communication protocols, optimized for wireless networks.
- With the option of supporting TCP/IP as well as HTTP at the mobile devices, end-to-end security between the wireless WAP client and the wired server can be realized, with the WAP gateways merely used as a TCP-level gateway or simple-Internet routers.
  - TCP-level Gateway: A TLS session can be set up between the wireless WAP client and the wired server and the TLS data would be the TCP payload that could stay encrypted while passing through the WAP gateway.
  - The WAP gateway can be merely used as an end-point of two TCP connections (one TCP connection from the mobile device to the WAP gateway over the wireless network and another TCP connection from the WAP gateway to the application server through a wired network).
  - Internet Router: End-to-end security can be provided at the IP-level using IPSec. The IP payload data would be encrypted.

End-to-End Security in WAP 2



Source: Figure 17.20 from William Stallings – Cryptography and Network Security, 5th Edition