INF3510 Information Security

Lecture 10: Communications Security

Audun Jøsang

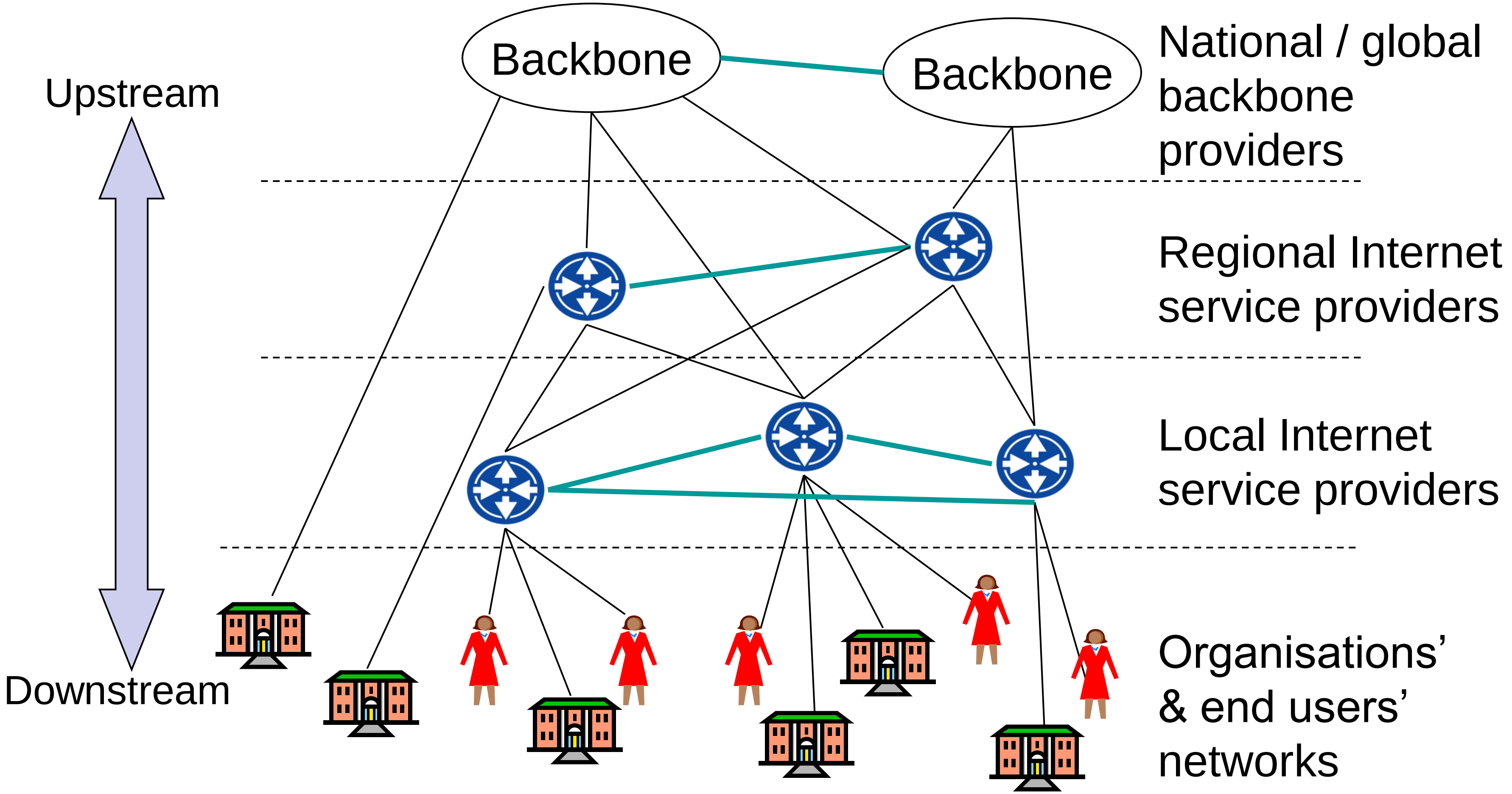
University of Oslo

Spring 2014

Outline

- Network security concepts
  - Communication security
  - Perimeter security
- Protocol architecture and security services
- Example security protocols
  - Transport Layer Security (TLS)
  - IP Layer Security (IPSec)

The Internet provider hierarchy



Network Security Concepts

Assumes that each organisation owns a network

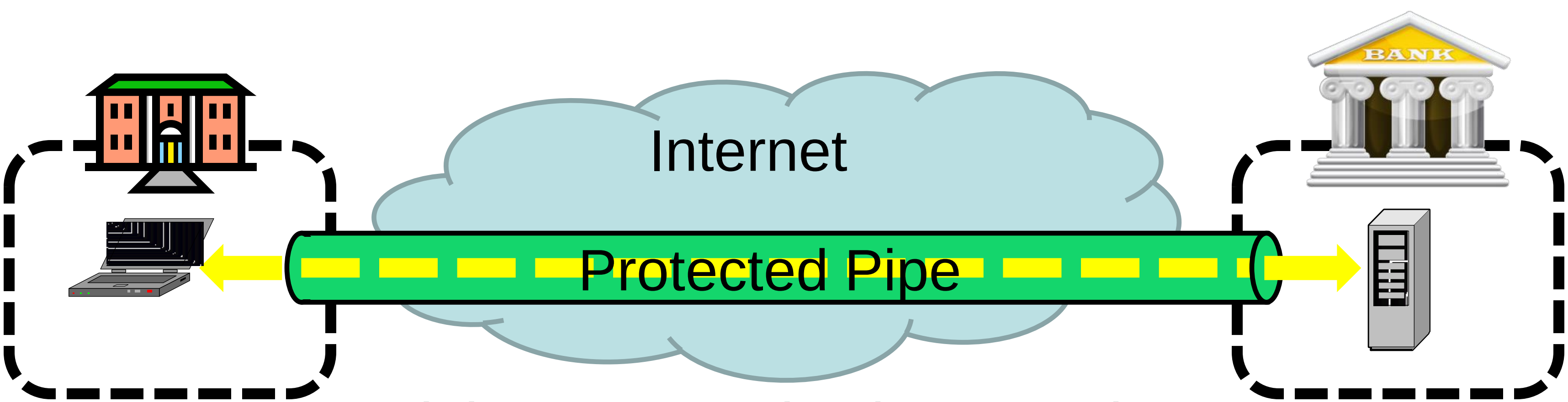
- Wants to protect own local network
- Wants to protect communication with other networks

Network Security: two main areas

- **Communication Security:** measures to protect the data transmitted across networks between organisations and end users
  - Topic for this lecture
- **Perimeter Security:** measures to protect an organization’s network from unauthorized access (theme for next lecture)
  - Topic for next lecture

Communication Security Analogy

Physical transport security



Digital communication security

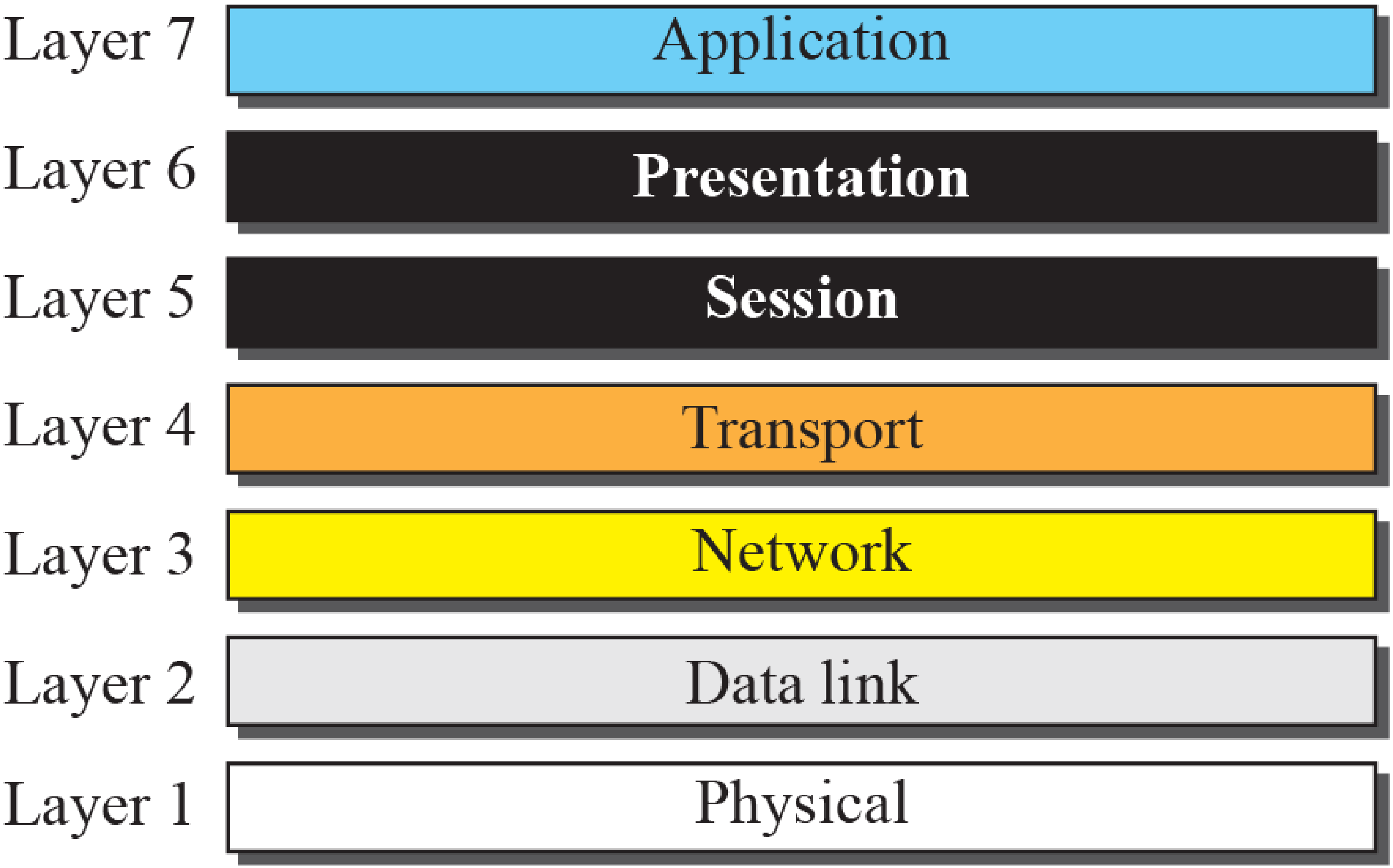
Communication Protocol Architecture

- Layered structure of hardware and software that supports the exchange of data between systems
- Each protocol consists of a set of rules for exchanging messages, i.e. “the protocol”.
- Two standards:
  - OSI Reference model
    - Never lived up to early promises
  - TCP/IP protocol suite
    - Most widely used

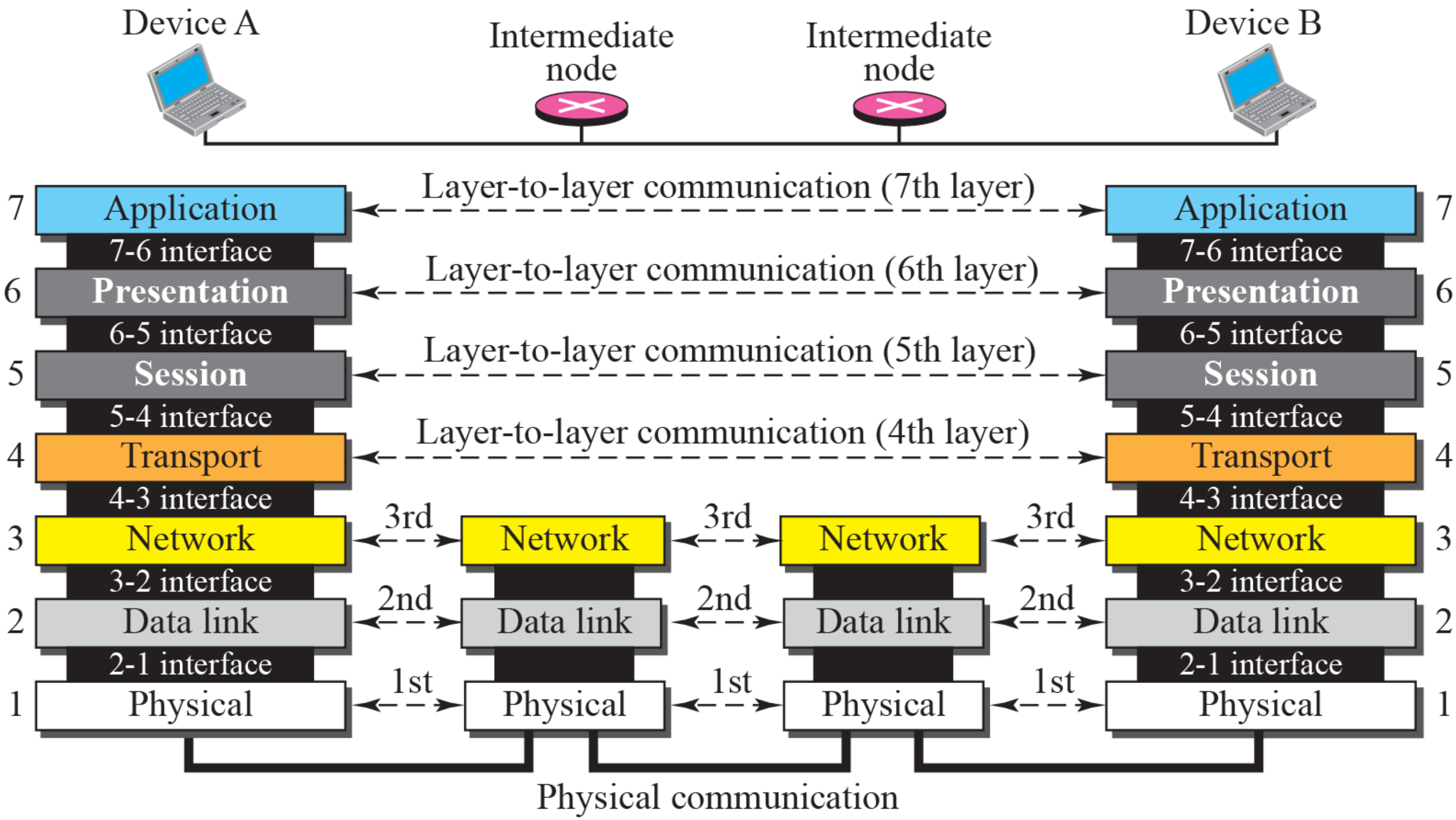
OSI – Open Systems Interconnection

- Developed by the International Organization for Standardization (ISO)
- A layer model of 7 layers
- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers

The OSI Protocol Stack



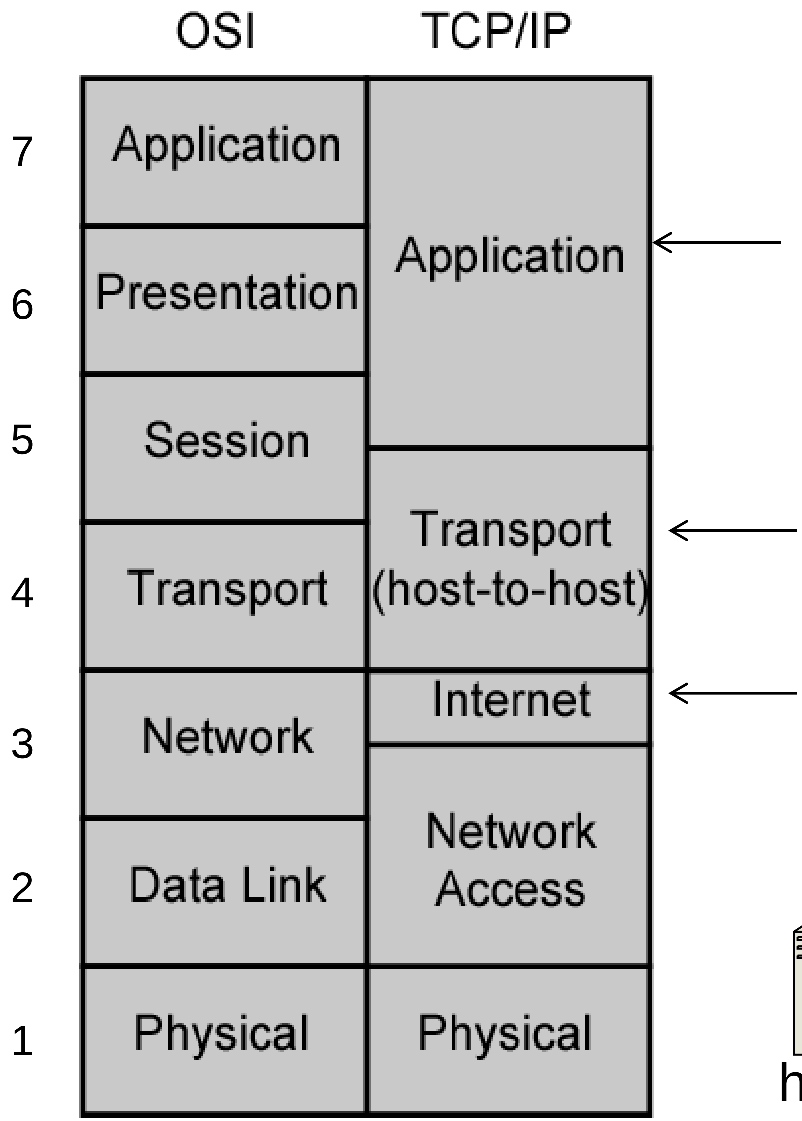
Communication across OSI



TCP/IP Protocol Architecture

- Developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET)
- Used by the global Internet
- No official model, but it's a working one.
  - Application layer
  - Host to host or transport layer
  - Internet layer
  - Network access layer
  - Physical layer

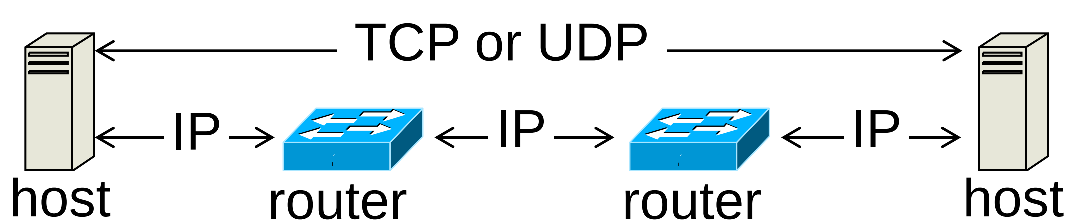
OSI model vs. TCP/IP model (The Internet)



Application protocols,
e.g. http, ftp, smtp, snmp

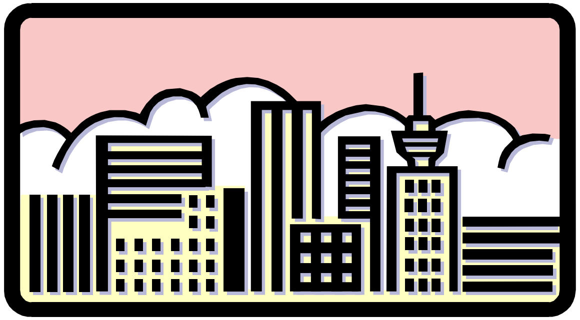
TCP (Transmission Control Protocol)
UDP (User Datagram Protocol)

IP (Internet Protocol)



OSI Security Architecture

- Originally specified as ISO 7498-2
- Republished as X.800 “Security Architecture for OSI”
- Defines a systematic set of security requirements and options for the ISO communication protocol stack
- Also applicable to the TCP/IP protocol stack



Security & Protocol Layers (X.800) with possible placement of security

Security Service	Layer						
	1	2	3	4	5	6	7
Peer entity authentication	·	·	Y	Y	·	·	Y
Data origin authentication	·	·	Y	Y	·	·	Y
Access control service	·	·	Y	Y	·	·	Y
Connection confidentiality	Y	Y	Y	Y	·	Y	Y
Connectionless confidentiality	·	Y	Y	Y	·	Y	Y
Selective field confidentiality	·	·	·	·	·	Y	Y
Traffic flow confidentiality	Y	·	Y	·	·	·	Y
Connection Integrity with recovery	·	·	·	Y	·	·	Y
Connection integrity without recovery	·	·	Y	Y	·	·	Y
Selective field connection integrity	·	·	·	·	·	·	Y
Connectionless integrity	·	·	Y	Y	·	·	Y
Selective field connectionless integrity	·	·	·	·	·	·	Y
Non-repudiation of Origin	·	·	·	·	·	·	Y
Non-repudiation of Delivery	·	·	·	·	·	·	Y

Security Protocols

- A large variety of security protocols have been specified and implemented for different purposes
  - Authentication, integrity, confidentiality
  - Key establishment/exchange
  - E-Voting
  - Secret sharing
  - etc.
- Protocols are surprisingly difficult to get right!
  - Many vulnerabilities are discovered years later
  - … some are never discovered (or maybe only by the attackers)

Protocols Overview

- This lecture discusses the operation of two network-related protocols that are in common use.
  - Transport Layer Security (TLS):
    Used extensively on the web and is often referred to in privacy policies as a means of providing confidential web connections.
  - IP Security (IPSec):
    Provides security services at the IP level and is used to provide Virtual Private Network (VPN) services.

Transport Layer Security

TLS/SSL

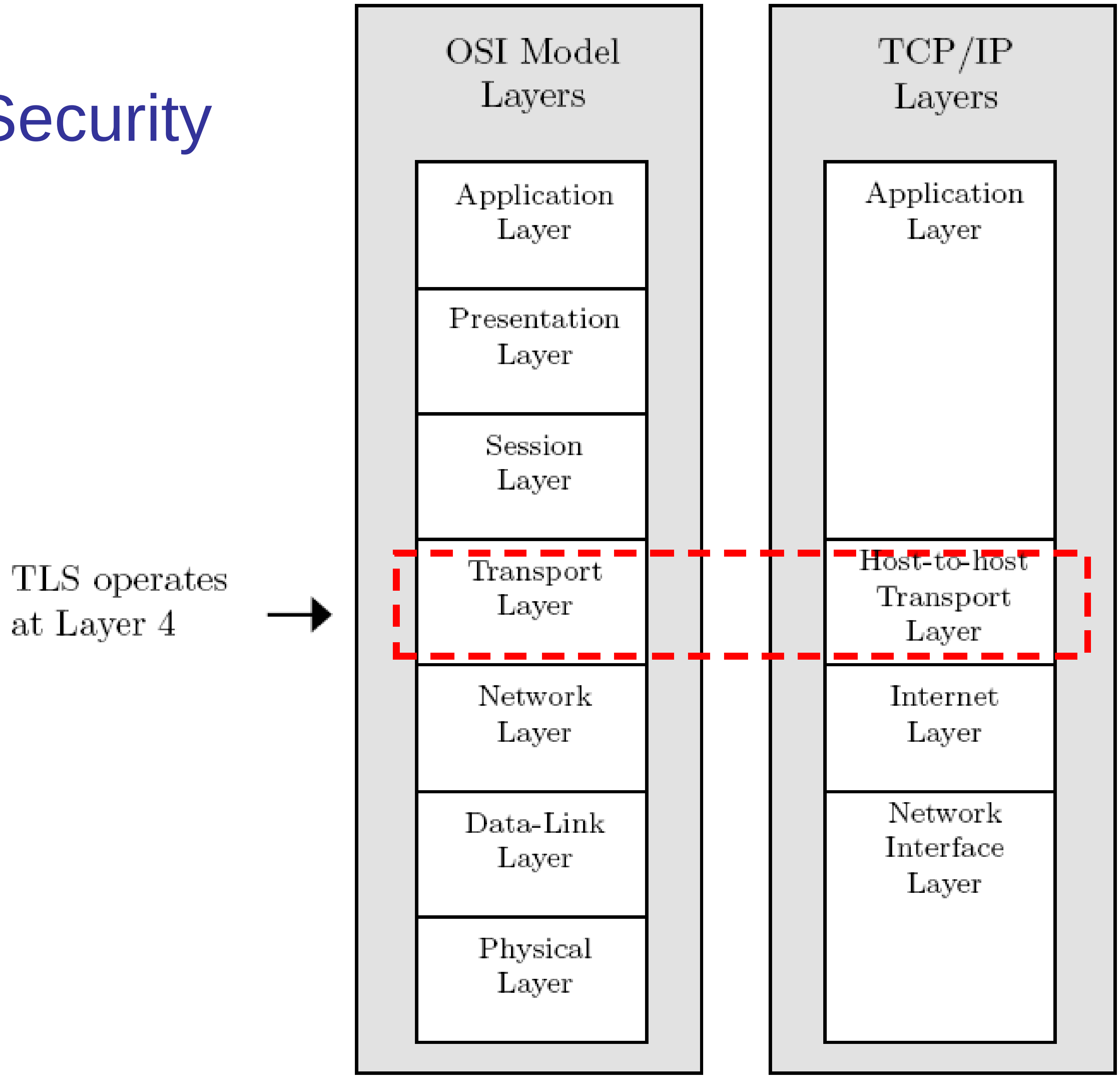
SSL/TLS: History

- 1994: Netscape Communications developed the network authentication protocol Secure Sockets Layer (SSL) 2.0.
  - Badly broken
- 1995: Netscape release their own improvements SSL 3.0
  - Widely used for many years.
- 1996: SSL 3.0 was submitted to the IETF as an Internet draft, and an IETF working group was formed to develop a recommendation.
- In January 1999, RFC 2246 was issued by the IETF, Transport Layer Security Protocol: TLS 1.0
  - Similar to, but incompatible with SSL
  - Currently TLS 1.2 (2008)

TLS: Overview

- TLS is a cryptographic services protocol based on the Browser PKIX, and is commonly used on the Internet.
  - Most often used to allow browsers to establish secure sessions with web servers.
- Port 443 is reserved for HTTP over TLS and HTTPS is the name of the URL scheme used with this port.
  - http://www.develop.com implies the use of standard HTTP using port 80.
  - https://www.develop.com implies the use of HTTP over TLS using port 443.

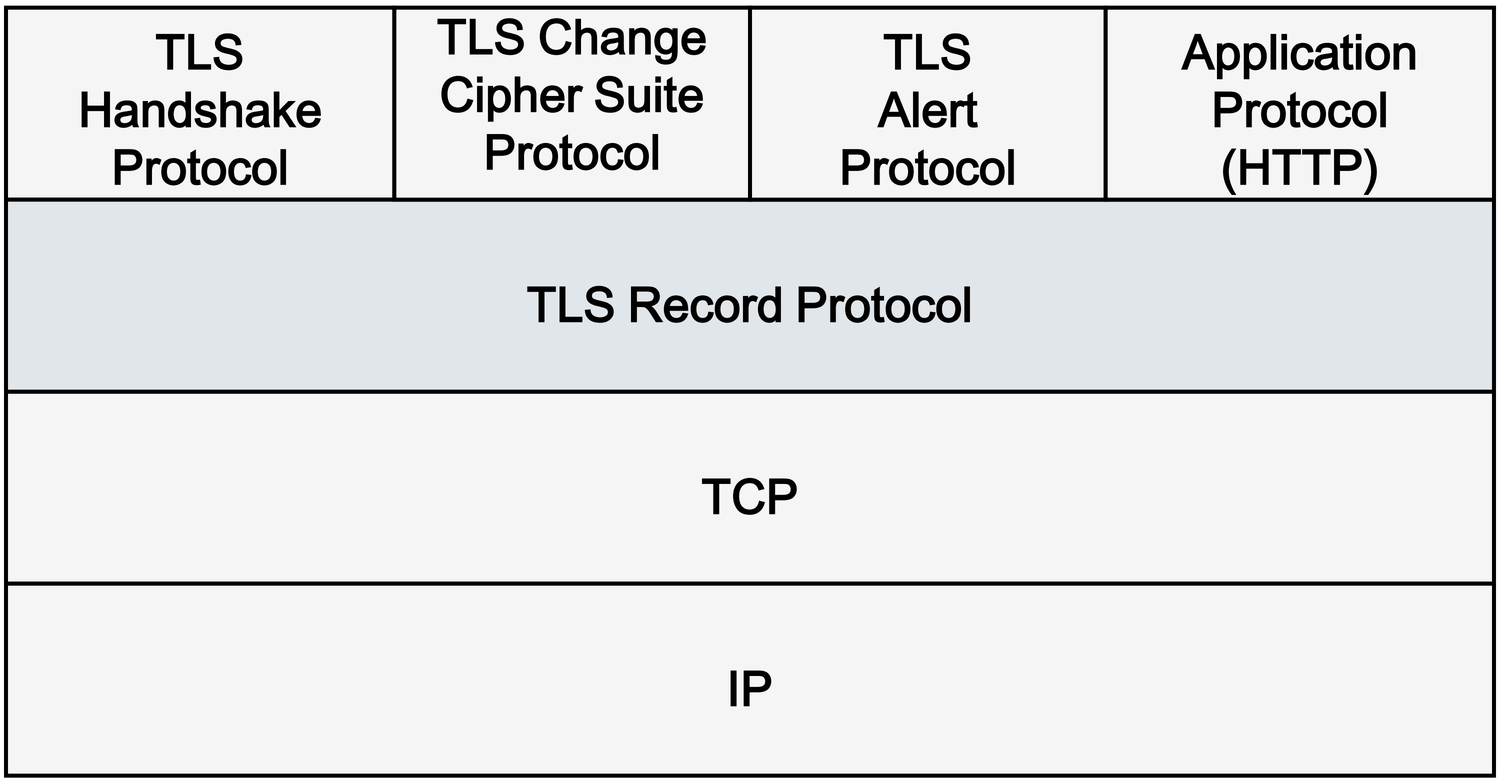
TLS:
Layer 4 Security



TLS: Architecture Overview

- Designed to provide secure reliable end-to-end services over TCP.
- Consists of 3 higher level protocols:
  - TLS Handshake Protocol
  - TLS Alert Protocol
  - TLS Change Cipher Spec Protocol
- The TLS Record Protocol provides the practical encryption and integrity services to various application protocols.

TLS: Protocol Stack

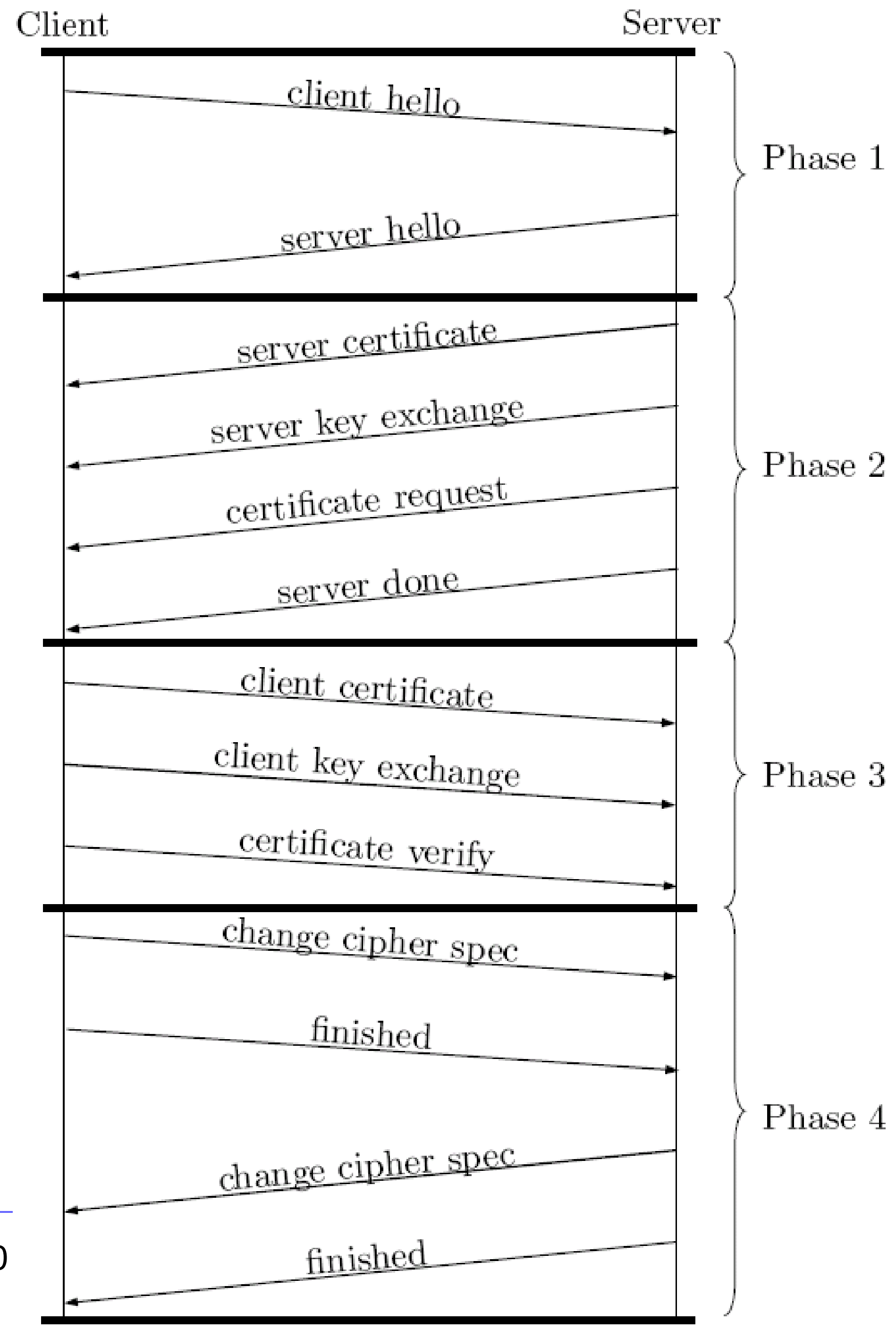


TLS:
Handshake Protocol

- The handshake protocol
  - Negotiates the encryption to be used
  - Establishes a shared session key
  - Authenticates the server
  - Authenticates the client (optional)
  - Completes the session establishment
- After the handshake, application data is transmitted securely
- Several variations of the handshake exist
  - RSA variants
  - Diffie-Hellman variants

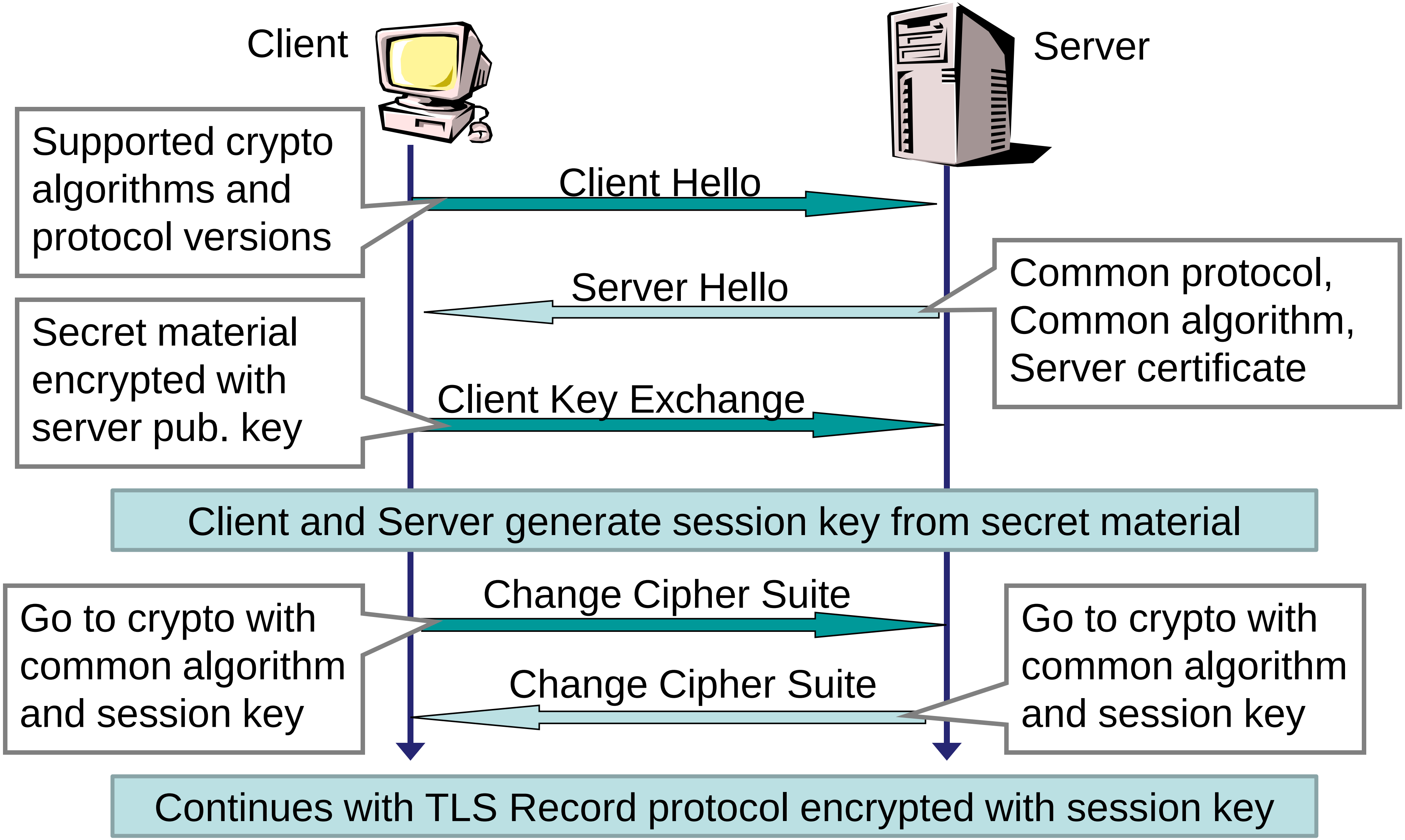
TLS: Handshake
Four phases

- Phase 1: Initiates the logical connection and establishes its security capabilities
- Phases 2 and 3: Performs key exchange. The messages and message content used in this phase depends on the handshake variant negotiated in phase 1.
- Phase 4: Completes the setting up of a secure connection.



Diagram

TLS: Simplified RSA-based Handshake



TLS: Elements of Handshake

- Client hello
  - Advertises available cipher suites (e.g. RSA, RC4/40, MD5)
- Server hello
  - Returns the selected cipher suite
  - Server adapts to client capabilities
- RSA and Server Certificate
  - X.509 digital certificate sent to client, assumes RSA algorithm
  - Client verifies the certificate including that the certificate signer is in its acceptable Certificate Authority (CA) list. Now the client has the server's certified public key.
- RSA and Client Certificate
  - Optionally, the client can send its X.509 certificate to server, in order to provide mutual authentication, assumes RSA algorithm
- Anonymous Diffie-Hellman
  - Optionally, the client and server can establish session key using the Diffie-Hellman algorithm

TLS: Record Protocol Overview

- Provides two services for SSL connections.
  - Message Confidentiality:
    - Ensure that the message contents cannot be read in transit.
    - The Handshake Protocol establishes a symmetric key used to encrypt SSL payloads.
  - Message Integrity:
    - Ensure that the receiver can detect if a message is modified in transmission.
    - The Handshake Protocol establishes a shared secret key used to construct a MAC.

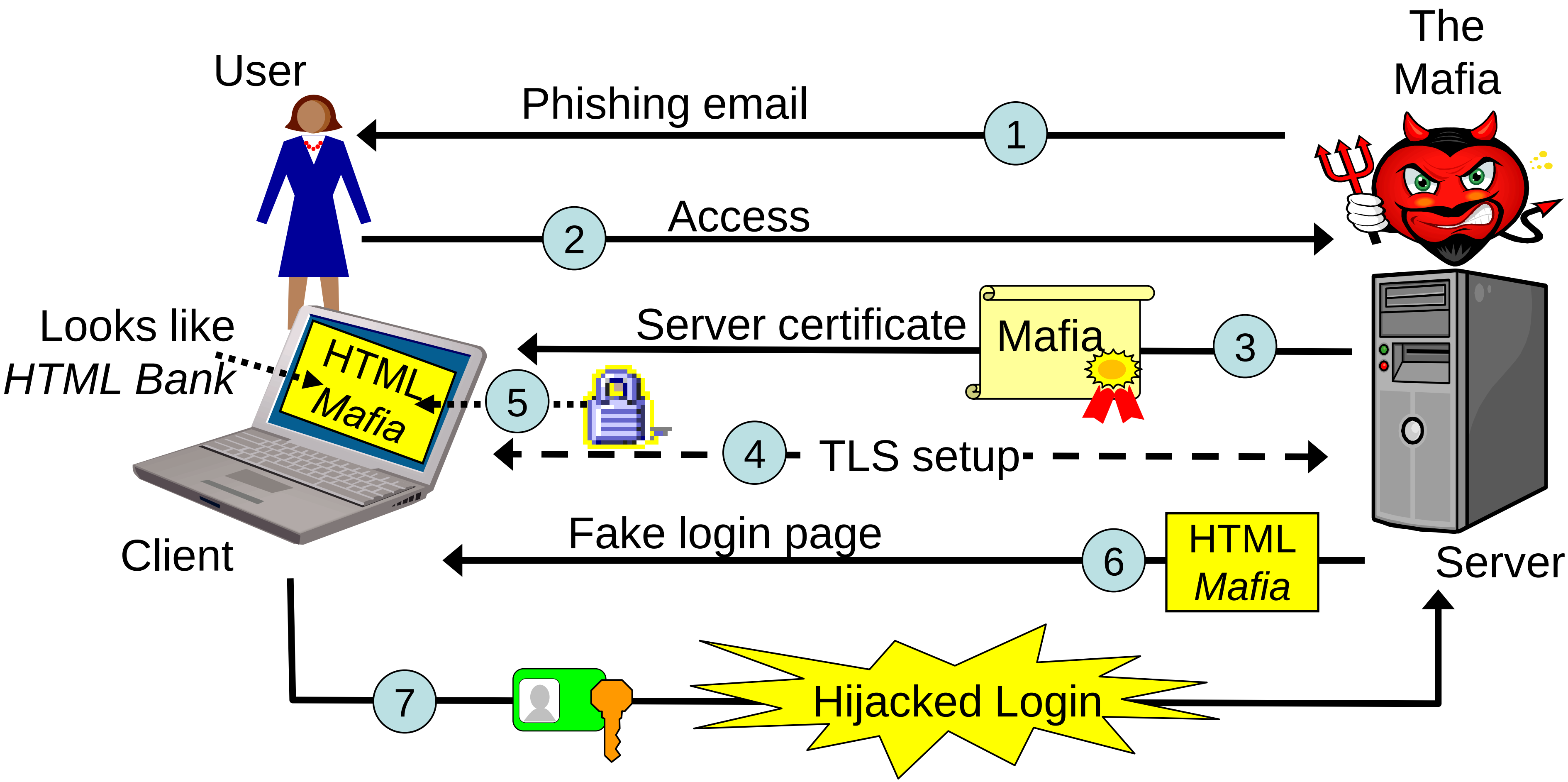
TLS: Record Protocol Operation

- Fragmentation:
  - Each application layer message is fragmented into blocks of 214 bytes or less.
- Compression:
  - Optionally applied.
  - SSL v3 & TLS – default compression algorithm is null
- Add MAC:
  - Calculates a MAC over the compressed data using a MAC secret from the connection state.
- Encrypt:
  - Compressed data plus MAC are encrypted with symmetric cipher.
  - Permitted ciphers include AES, IDEA,DES, 3DES, RC4
  - For block ciphers, padding is applied after the MAC to make a multiple of the cipher's block size.

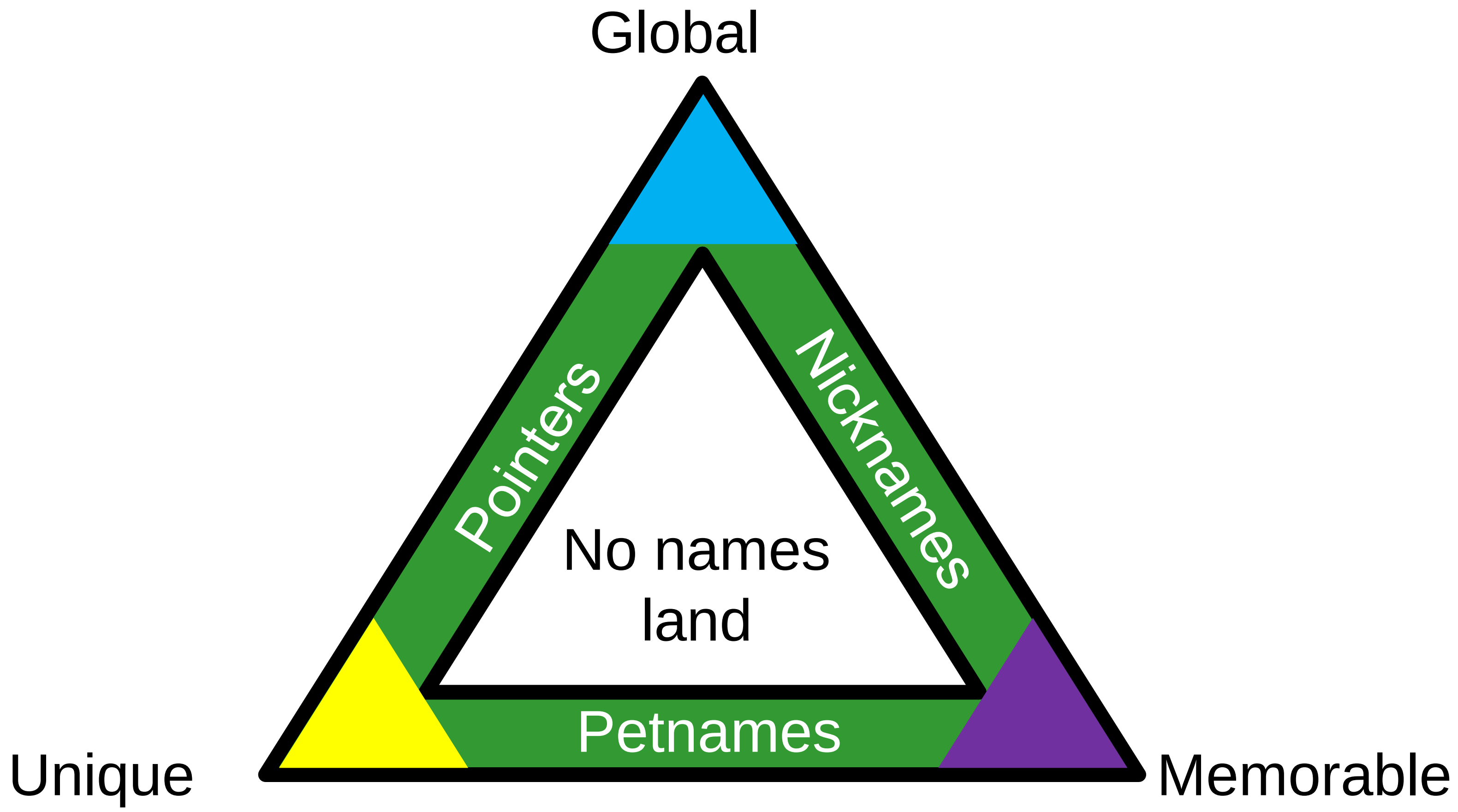
SSL and TLS Limitations

- Higher layers should not be overly reliant on SSL or TLS always negotiating the strongest possible connection between two peers
- Applications should never transmit information over a channel less secure than they require.
- SSL and TLS are only as secure as the cryptographic algorithms determined in the handshake protocol.
- Both require a secure web browser and a secure operating system to be ‘secure’
  - Do these things actually exist?

Phishing and failed authentication

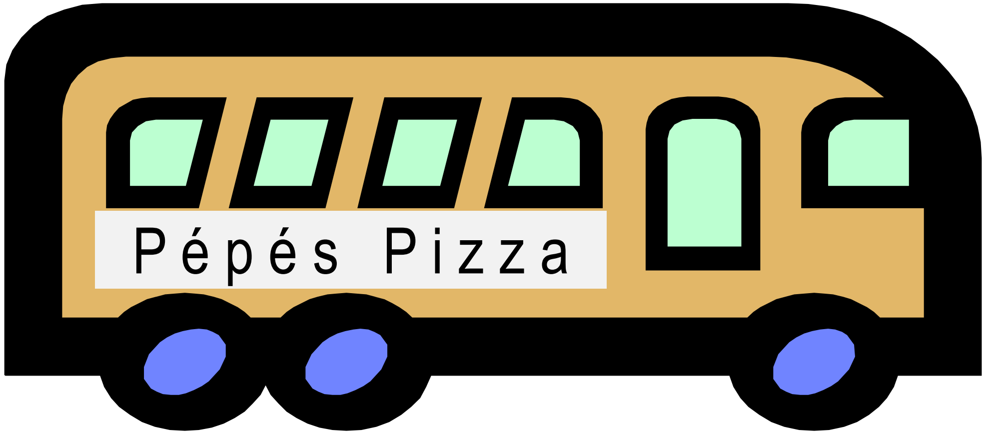


Zooko's Triangle of Id Properties



No identifier can be at the same time global, unique and memorable

Passing bus test for memorability

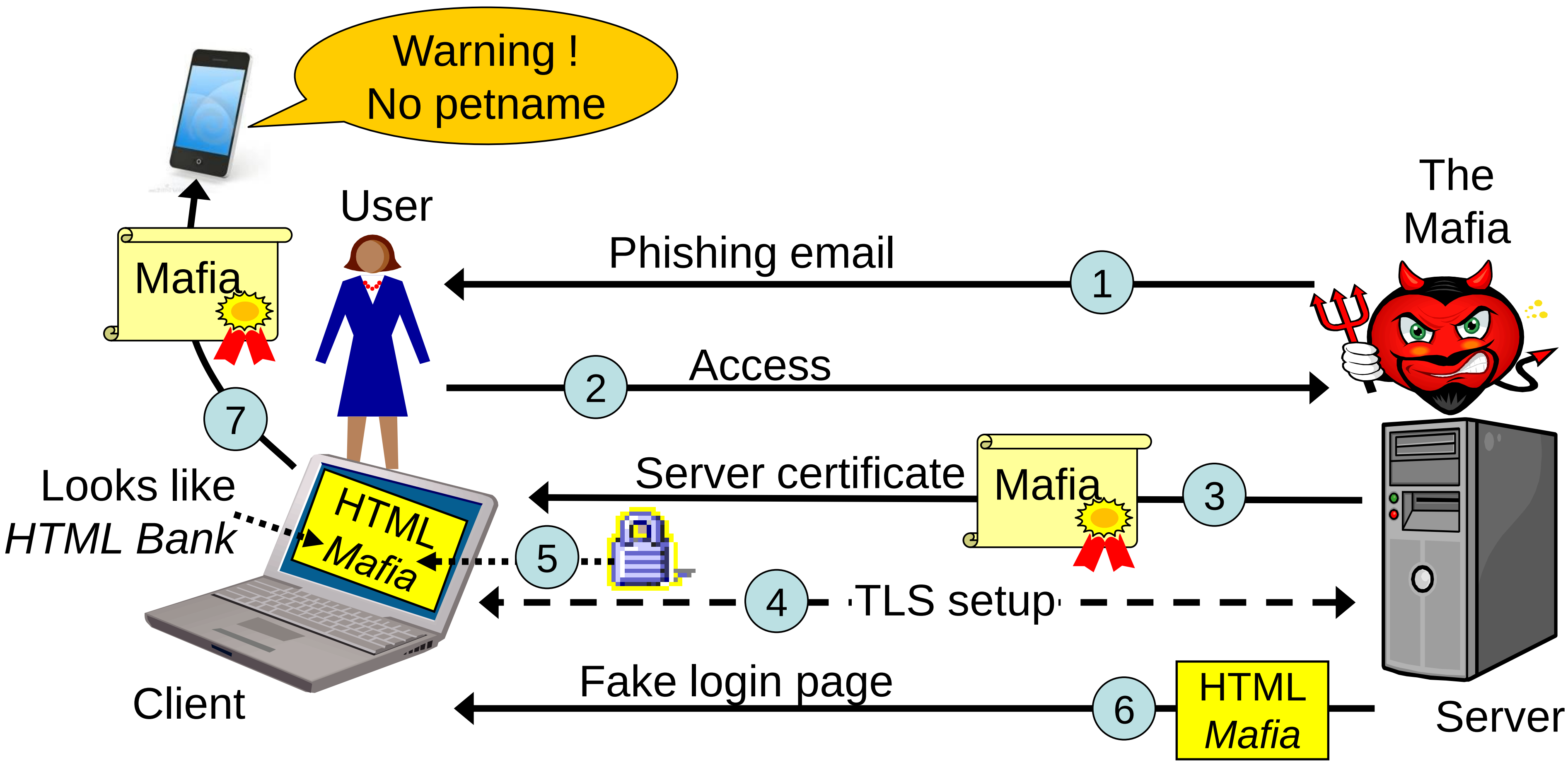


- If you see a name written on a passing bus, and you can remember the name after 5 minutes, then the name is memorable

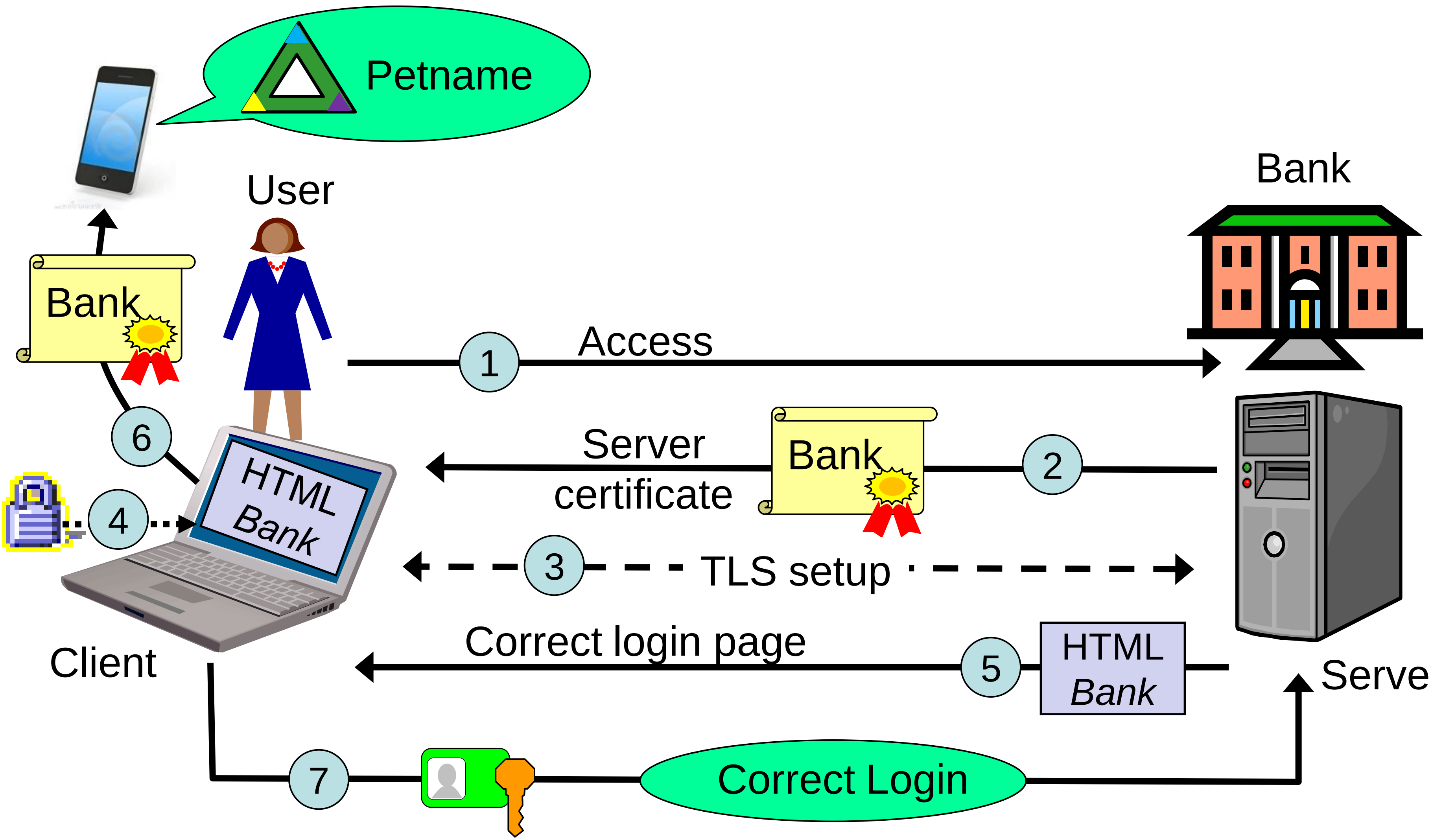
Petname Systems

- **Desirable name properties (Zooko's Triangle)**
  - Global, unique and memorable
  - No name type can have all 3 properties
    - Pointers are unique and global, e.g. domain name
    - Nicknames are global and memorable, e.g. 'Pepes Pizza'
    - Petnames are unique and memorable, e.g. 'PPizza'
- **Petname model** supports 3 properties of Zooko's triangle through mapping between pointer and petname
- **Petname Systems** implement the petname model.
  - Used to enhance security and prevent phishing attacks
- **Petname Tool** extension available for Firefox

Phishing detection with Petname System



Server authentication with Petname System



IP Layer Security

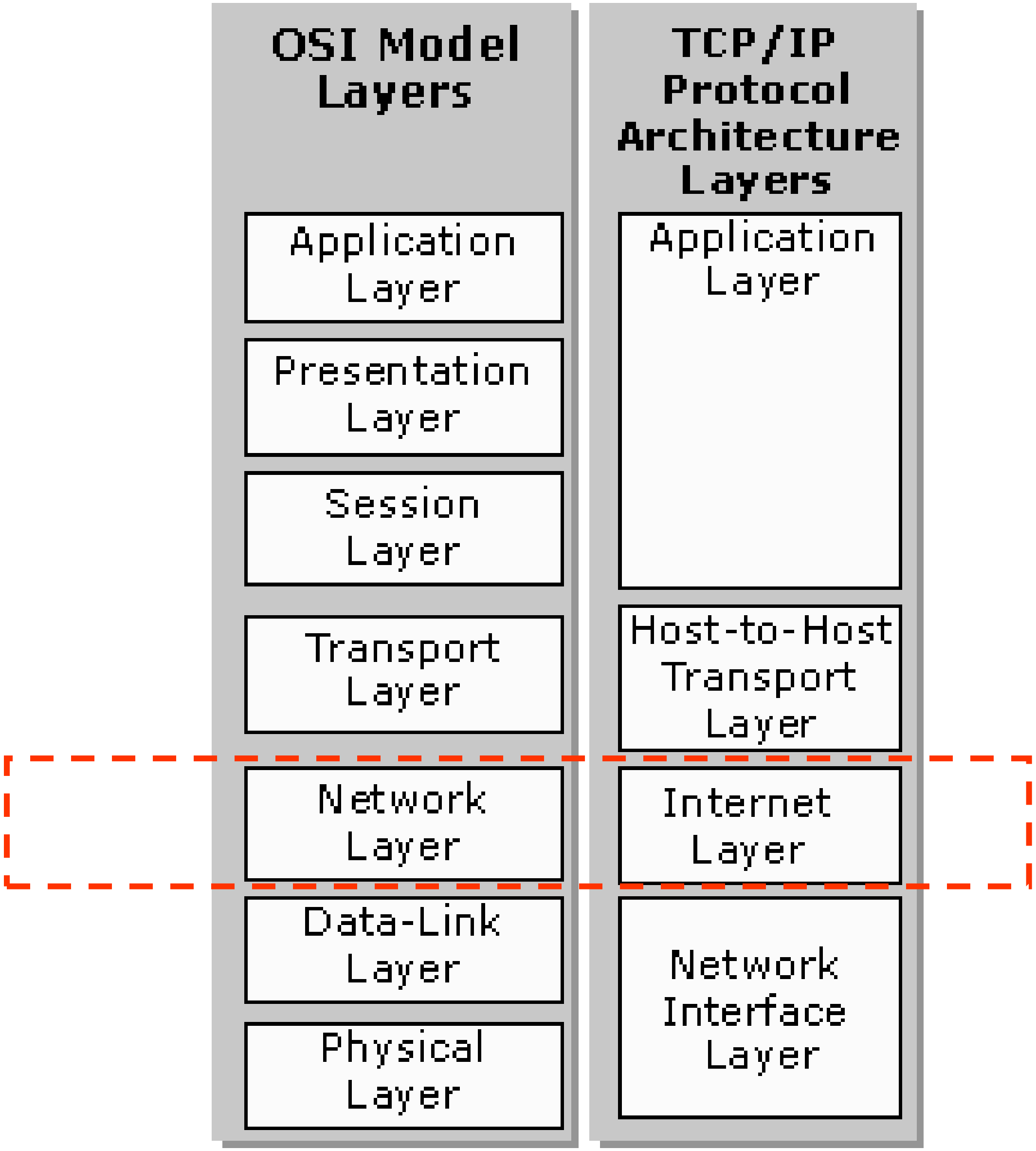
IPSec & Virtual Private Networks

IPSec: Introduction

- Internet Protocol security (IPSec) is standard for secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services.
- Uses encryption, authentication and key management algorithms
- Based on an end-to-end security model at the IP level
- Provides a security architecture for both IPv4 and IPv6
  - Mandatory for IPv6
  - Optional for IPv4
- Requires operating system support, not application support.

Layer 3 Security

IP Sec Operation ⟶



IPSec: Security Services

- Message Confidentiality.
  - Protects against unauthorized data disclosure.
  - Accomplished by the use of encryption mechanisms.
- Message Integrity.
  - IPsec can determine if data has been changed (intentionally or unintentionally) during transit.
  - Integrity of data can be assured by using a MAC.
- Traffic Analysis Protection.
  - A person monitoring network traffic cannot know which parties are communicating, how often, or how much data is being sent.
  - Provided by concealing IP datagram details such as source and destination address.

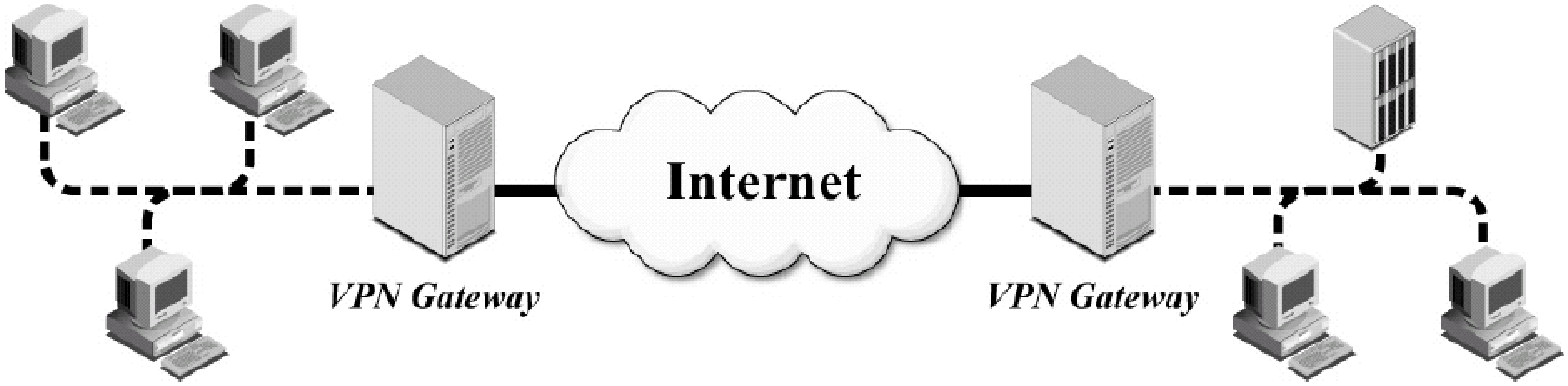
IPSec: Security Services

- Message Replay Protection.
  - The same data is not delivered multiple times, and data is not delivered grossly out of order.
  - However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
- Peer Authentication.
  - Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate.
  - Ensures that network traffic is being sent from the expected host.
- Network Access Control.
  - Filtering can ensure users only have access to certain network resources and can only use certain types of network traffic.

IPSec:
Common Architectures

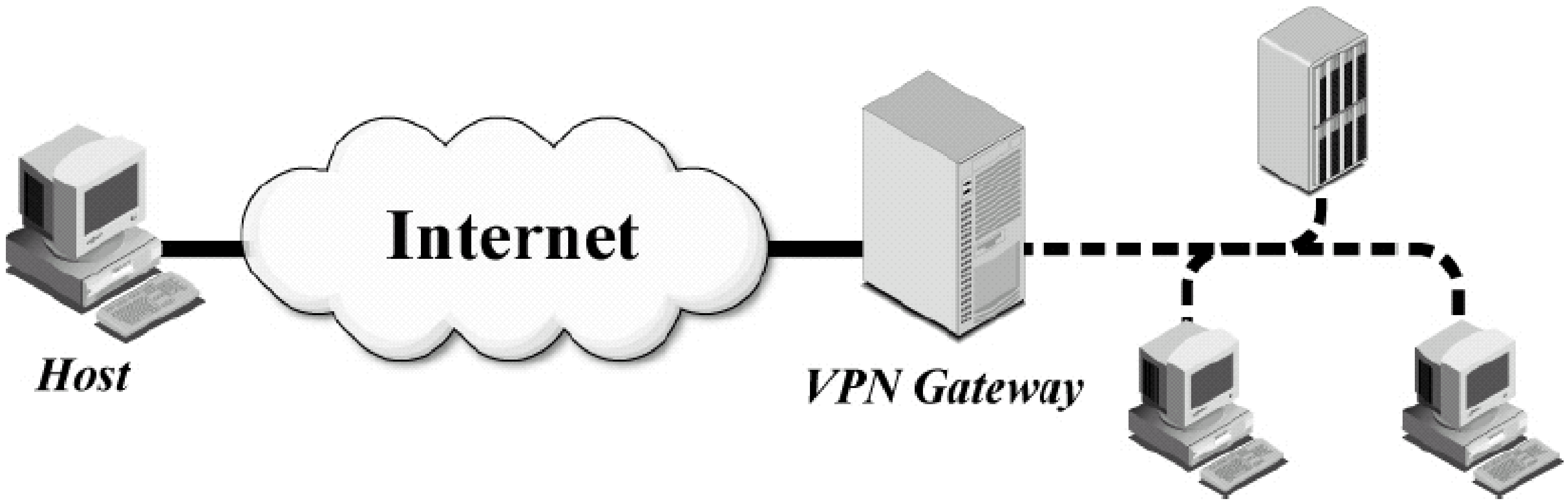
- Gateway-to-Gateway Architecture
- Host-to-Gateway Architecture
- Host-to-Host Architecture

IPSec: Gateway-to-Gateway Architecture



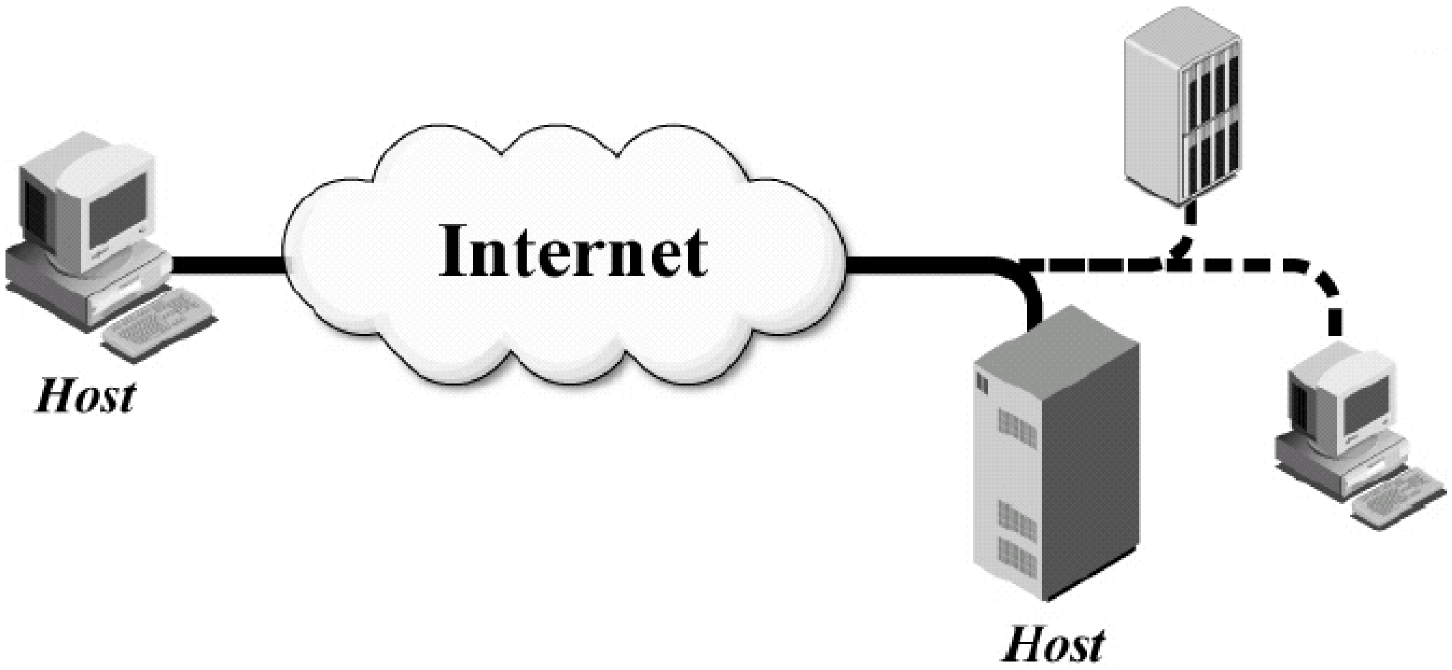
Source: NIST Special Publication 800-77

IPSec:
Host-to-Gateway Architecture



Source: NIST Special Publication 800-77

IPSec:
Host-to-Host Architecture



Source: NIST Special Publication 800-77

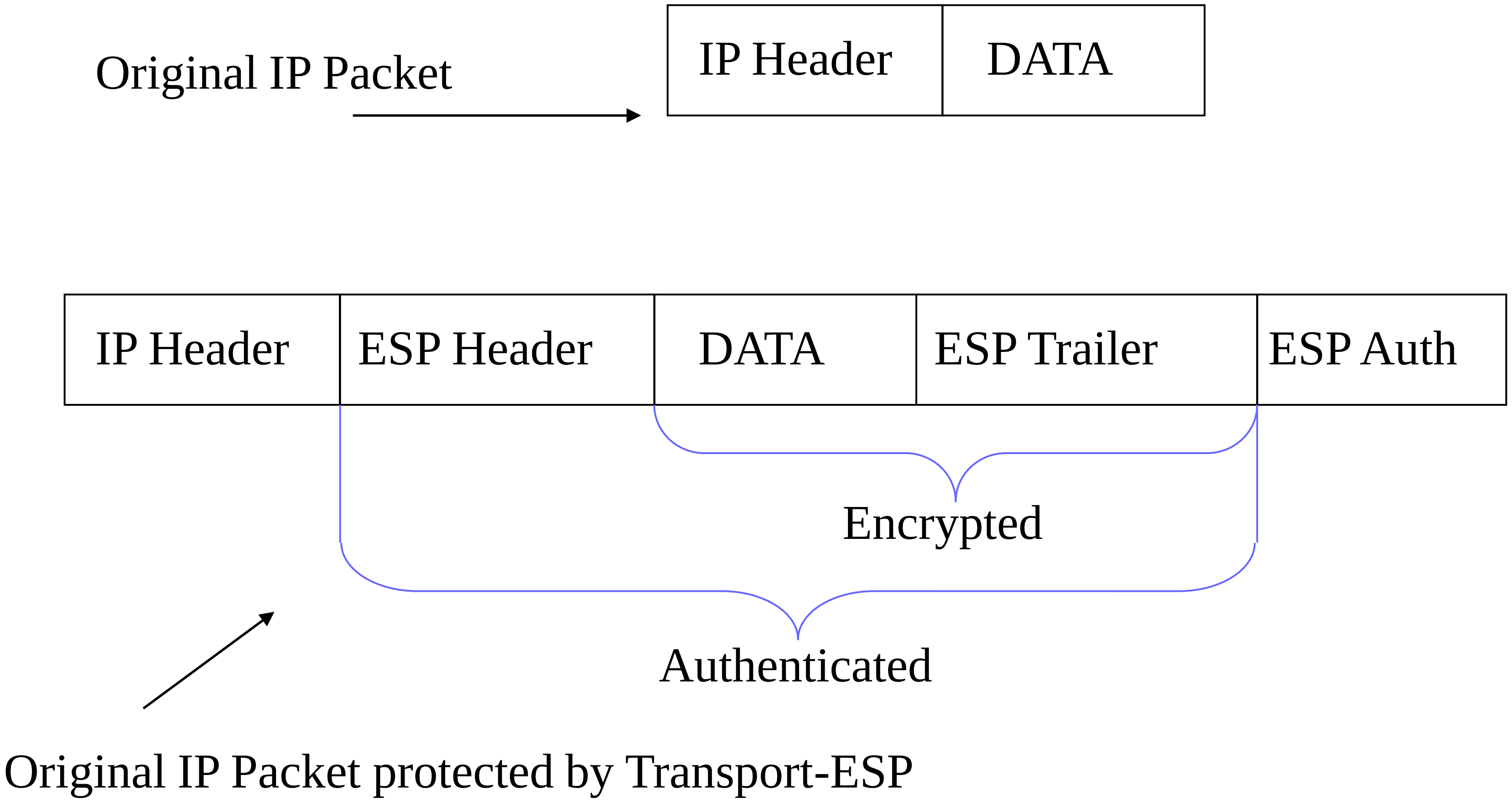
IPSec: Protocols Types

- Encapsulating Security Payload (ESP)
  - Confidentiality, authentication, integrity and replay protection
- Authentication Header (AH)
  - Authentication, integrity and replay protection. However there is no confidentiality
- Internet Key Exchange (IKE)
  - negotiate, create, and manage security associations

IPSec:
Modes of operation

- Each protocol (ESP or AH) can operate in transport or tunnel mode.
- **Transport mode:**
  - Operates primarily on the payload (data) of the original packet.
  - Generally only used in host-to-host architectures.
- **Tunnel mode:**
  - Original packet encapsulated into a new one, payload is original packet.
  - Typical use is gateway-to-gateway and host-to-gateway architectures.

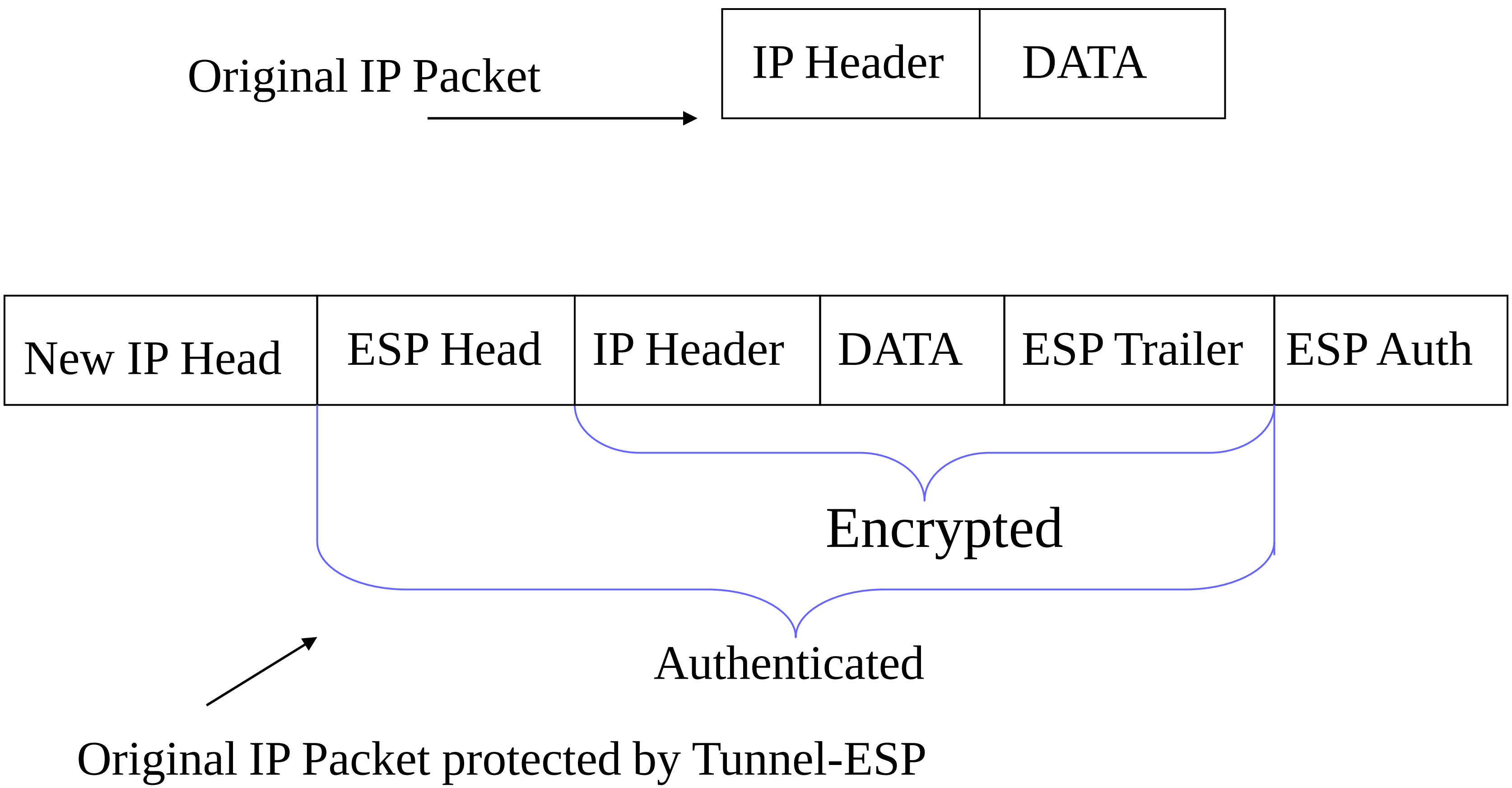
Transport Mode ESP



IPSec - ESP in Transport Mode: Outbound Packet Processing

- The data after the original IP header is padded by adding an ESP trailer and the result is then encrypted using the symmetric cipher and key in the SA.
- An ESP header is prepended.
- If an SA uses the authentication service, an ESP MAC is calculated over the data prepared so far and appended.
- The original IP header is prepended.
- However, some fields in the original IP header must be changed. For example,
  - Protocol field changes from TCP to ESP.
  - Total Length field must be changed to reflect the addition of the AH header.
  - Checksums must be recalculated.

Tunnel Mode ESP



IPSec - ESP in Tunnel Mode: Outbound Packet Processing

- The entire original packet is padded by adding an ESP trailer and the result is then encrypted using the symmetric cipher and key agreed in the SA.
- An ESP header is prepended.
- If an SA uses the authentication service, an ESP MAC is calculated over the data prepared so far and appended.
- A new ‘outer’ IP header is prepended.
  - The ‘inner’ IP header of the original IP packet carries the ultimate source and destination addresses.
  - The ‘outer’ IP header may contain distinct IP addresses such as addresses of security gateways.
  - The ‘outer’ IP header Protocol field is set to ESP.

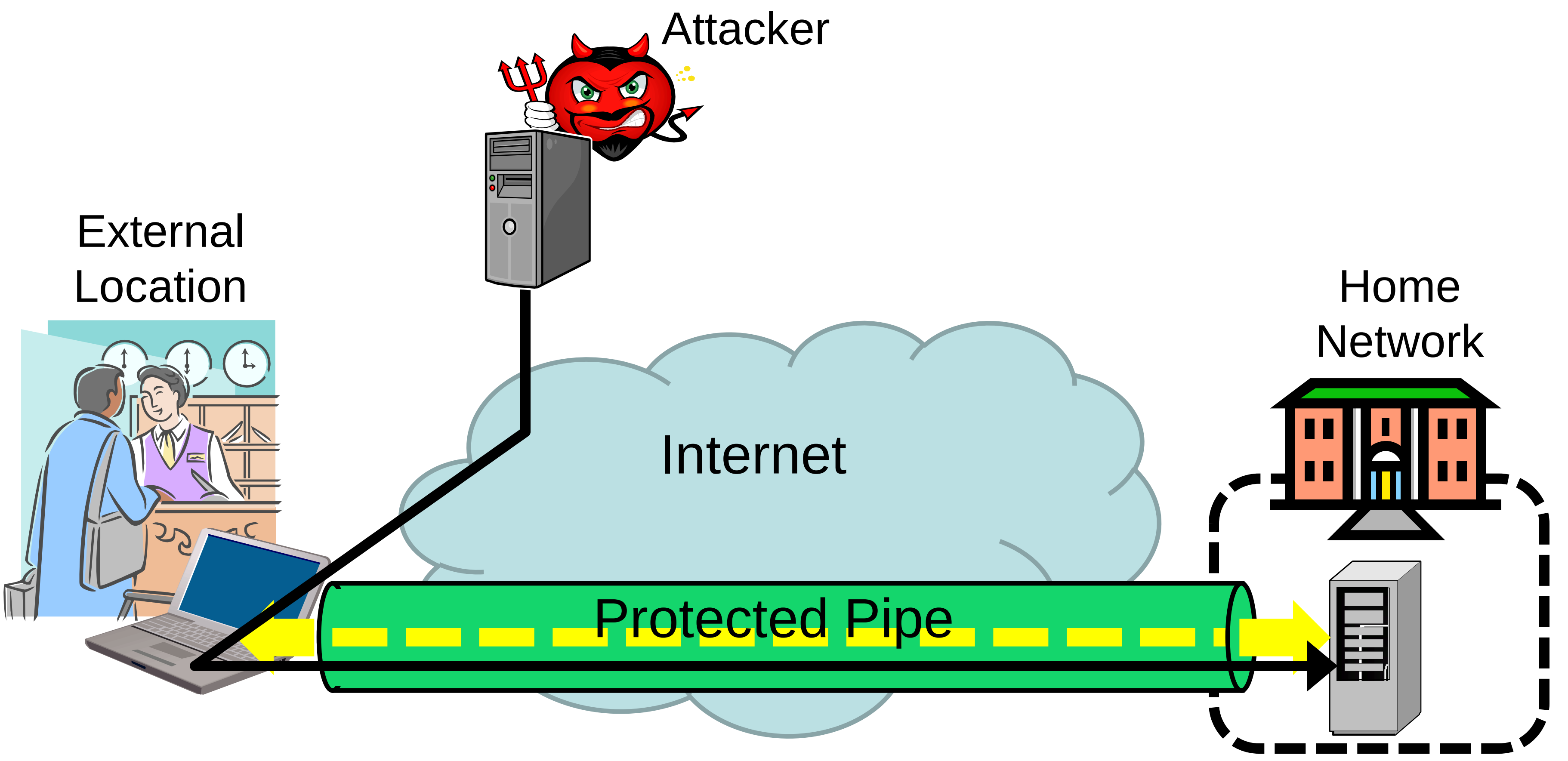
Security Associations

- A security association (SA) contains info needed by an IPSec endpoint to support one end of an IPSec connection.
- Can include cryptographic keys and algorithms, key lifetimes, security parameter index (SPI), and security protocol identifier (ESP or AH).
- The SPI is included in the IPSec header to associate a packet with the appropriate SA.
- Security Associations are simplex
  - need one for each direction of connection
  - stored in a security association database (SAD).
- Key exchange is largely automated after initial manual configuration by administrator prior to connection setup.
- (See ISAKMP, IKE, Oakley, Skeme and SAs)

Risks of using IPSec for VPN

- IPSec typically used for VPN (Virtual Private Networks)
- A VPN client at external location may be connected to the Internet (e.g. from hotel room or café) while at the same time being connected to home network via VPN.
  - VPN gives direct access to resources in home network.
- Internet access from external location may give high exposure to cyber threats
  - No network firewall, no network IDS
- Attacks against the VPN client at external location can directly access the home network through VPN tunnel

Risk of using VPN



Secure pipe can be attack channel to home network !

End of lecture