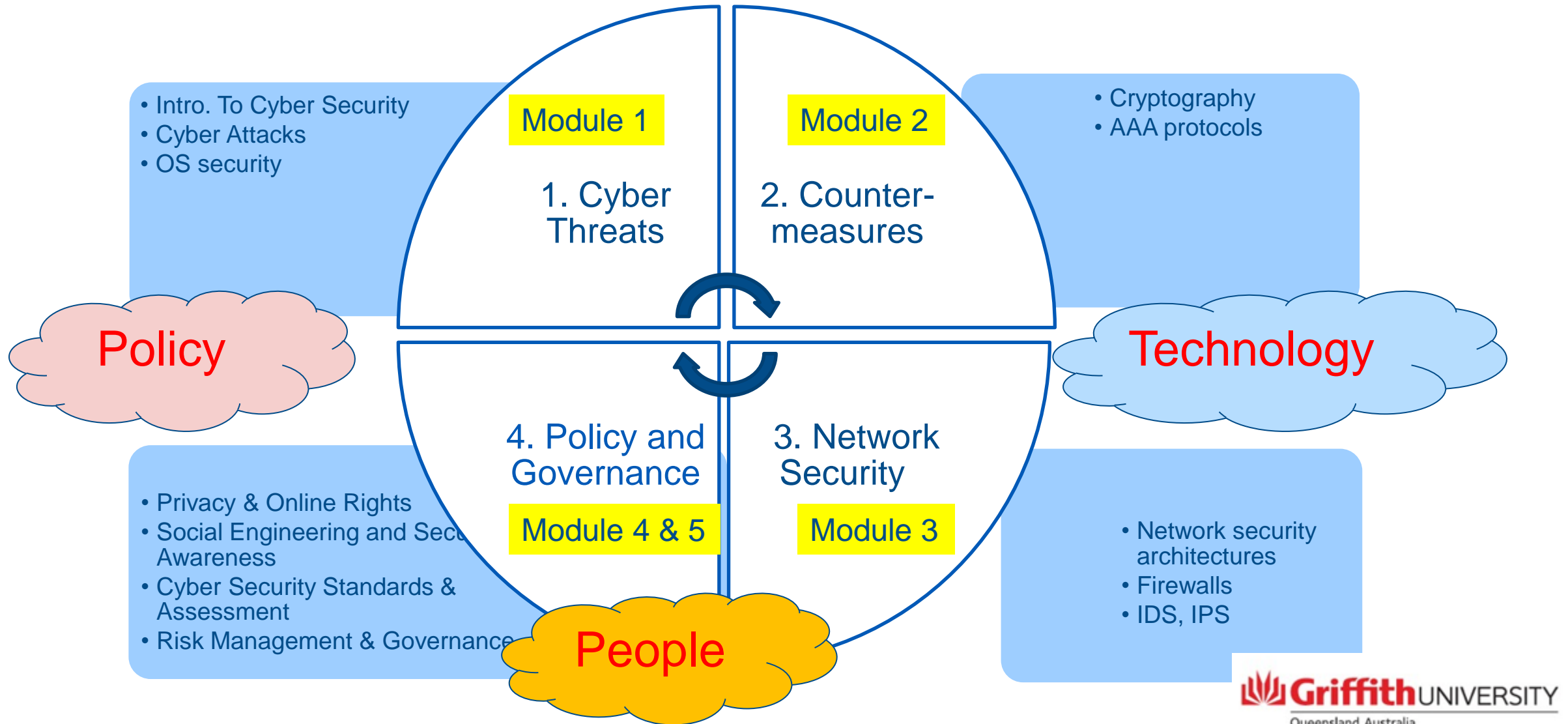


Fundamentals of Cyber Security

Hui Tian

Griffith University

Course Contents



Mod 3-1: Network Security I

- Physical Layer
- DLL
- Network Layer

Mod 3-2: Network Security II

- Transport Layer security issues
- Realtime cyber threat detection and mitigation
 - Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
 - Firewall
- SSL/TLS
- HTTPS

Reference:

Chapter 8, 9, 22, 23 Computer Security: Principles and Practice, William Stallings
TCP/IP Illustrated Volume 1 (2nd Edition), Kevin Fall and W. Richard Stevens



Network Security

Objectives

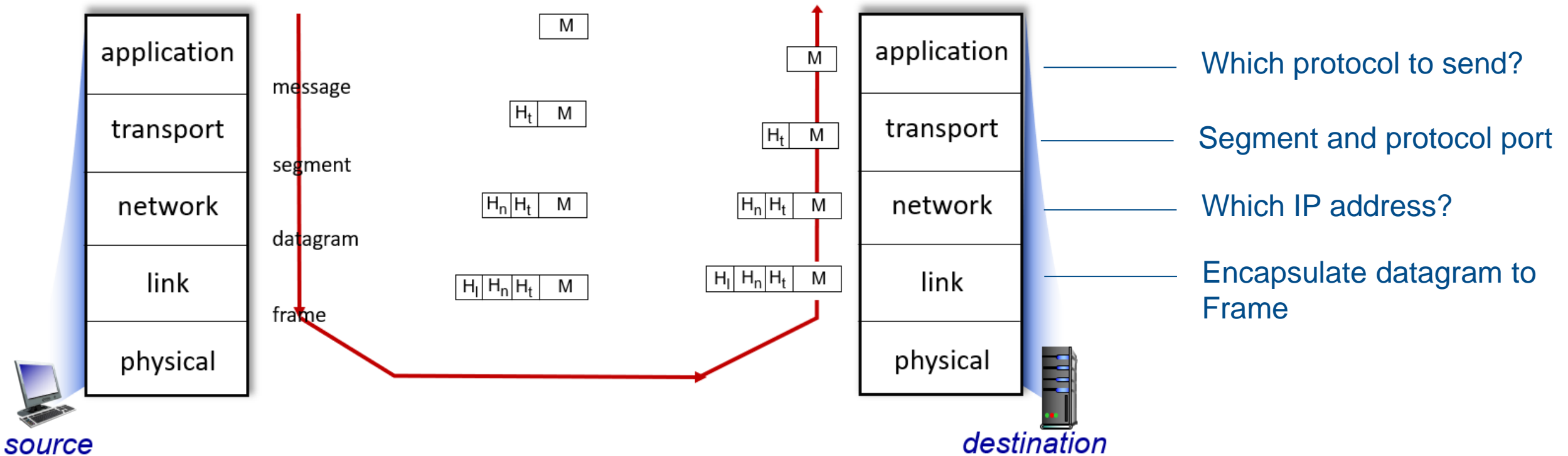
- Understand basic TCP/IP hacks including spoofs and flooding
- Combine all knowledge in cryptography, authentication and access control and understand how IPSec works towards a secure networking
- Understand Firewall and basic operation
- Identify where and how to apply IDS and IPS



Network Security

Internet service

Postal service: Envelope → Destination with successively smaller hops
State → City → Street → Address → Apartment number
⇒ Australia Post never knows contents of envelope



src-port src-IP dst-port dst-IP STMP/HTTPS

Post port, src address, dst port, dst address, post office/DHL/EMS.

Network Security

Application

- BitTorrent, DNS, FTP, HTTP, NFS, NTP, SMTP, DHCP, Telnet etc.
- **Message** at this level
 - **URL** in web services (e.g. <http://www.tempurl.org/myservice>)

Transport

- TCP, UDP etc.
- **Segment (packet)** at this level
 - **TCP** port number (e.g. **80** , **Seq number**)

Internet/Network


- IP (IPv4, IPv6), ICMP, IPsec etc.
- **Datagram** at this level
 - **IP address** in the network layer (e.g. **157.58.56.101**)

Link/Network Access

- ARP, NDP, Tunnels (L2TP), PPP, Media Access Control (Ethernet, DSL, ISDN, FDDI) etc.
- **Frame** at this level
 - **Ethernet** (MAC) addresses in the link layer (e.g. **00-B0-D0-05-04-7E**)

Physical

- Ethernet physical layer Including 10BASE-T, 10BASE2, etc
- ISDN, DSL
- Bluetooth



ARP spoof, IP
address, routing
issues, sniffs

List of TCP/UDP port number: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers



Network Security

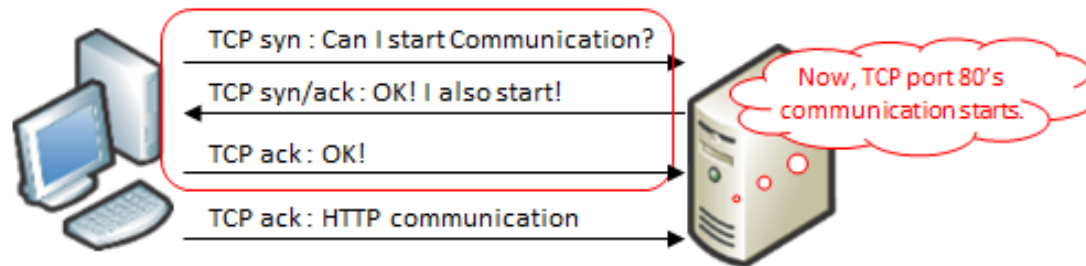
Transport Layer

- UDP/TCP
- Segment and add sequence number, receivers repack in order

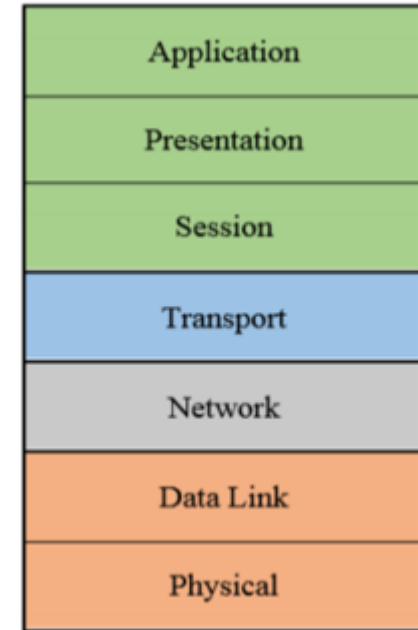
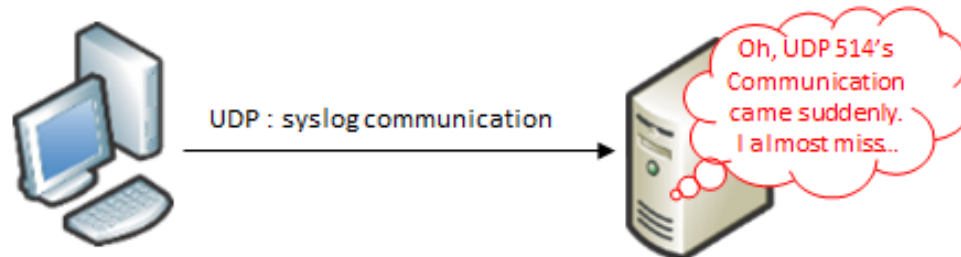
TCP/UDP

How to start TCP communication

3way Handshake



How to start UDP communication





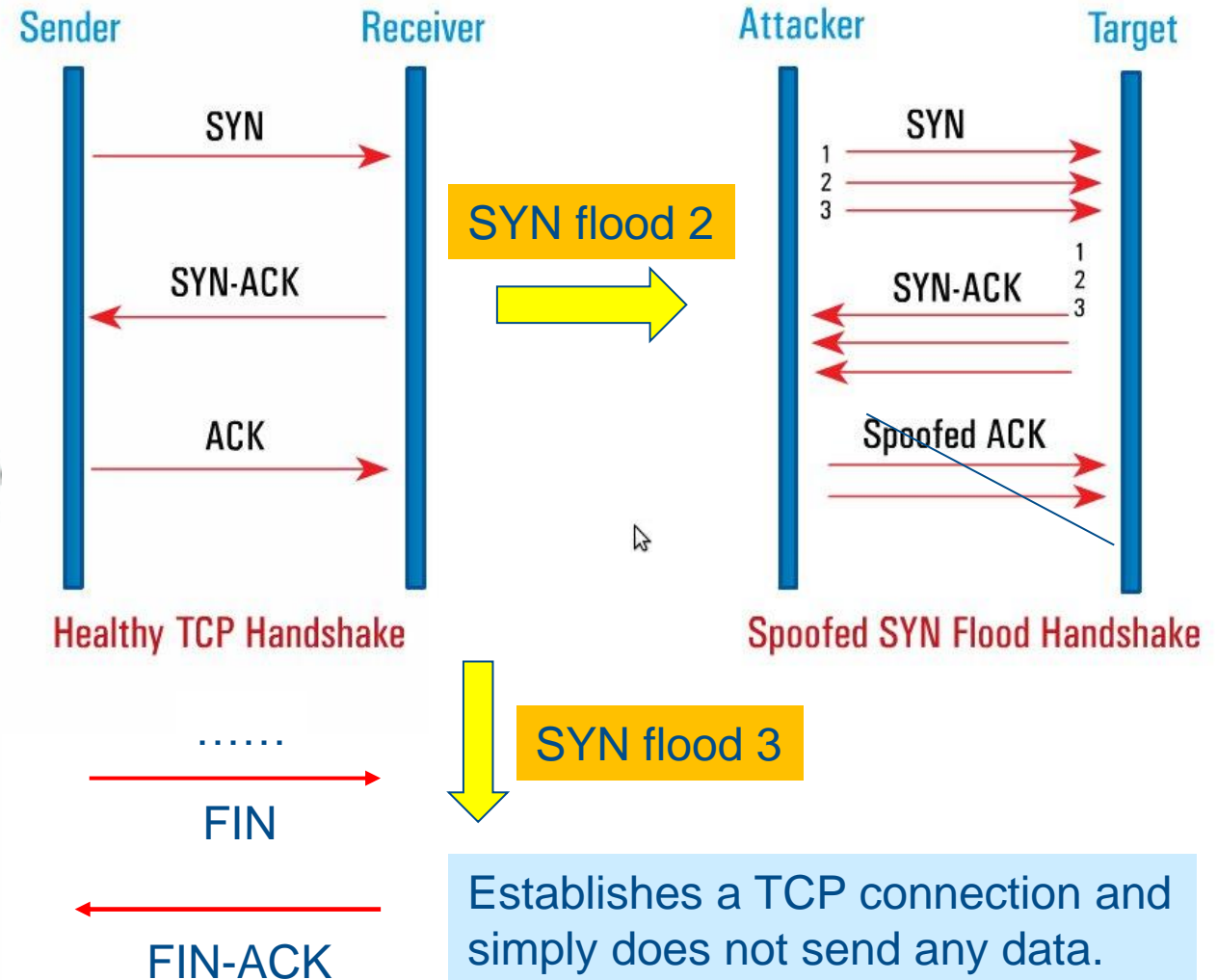
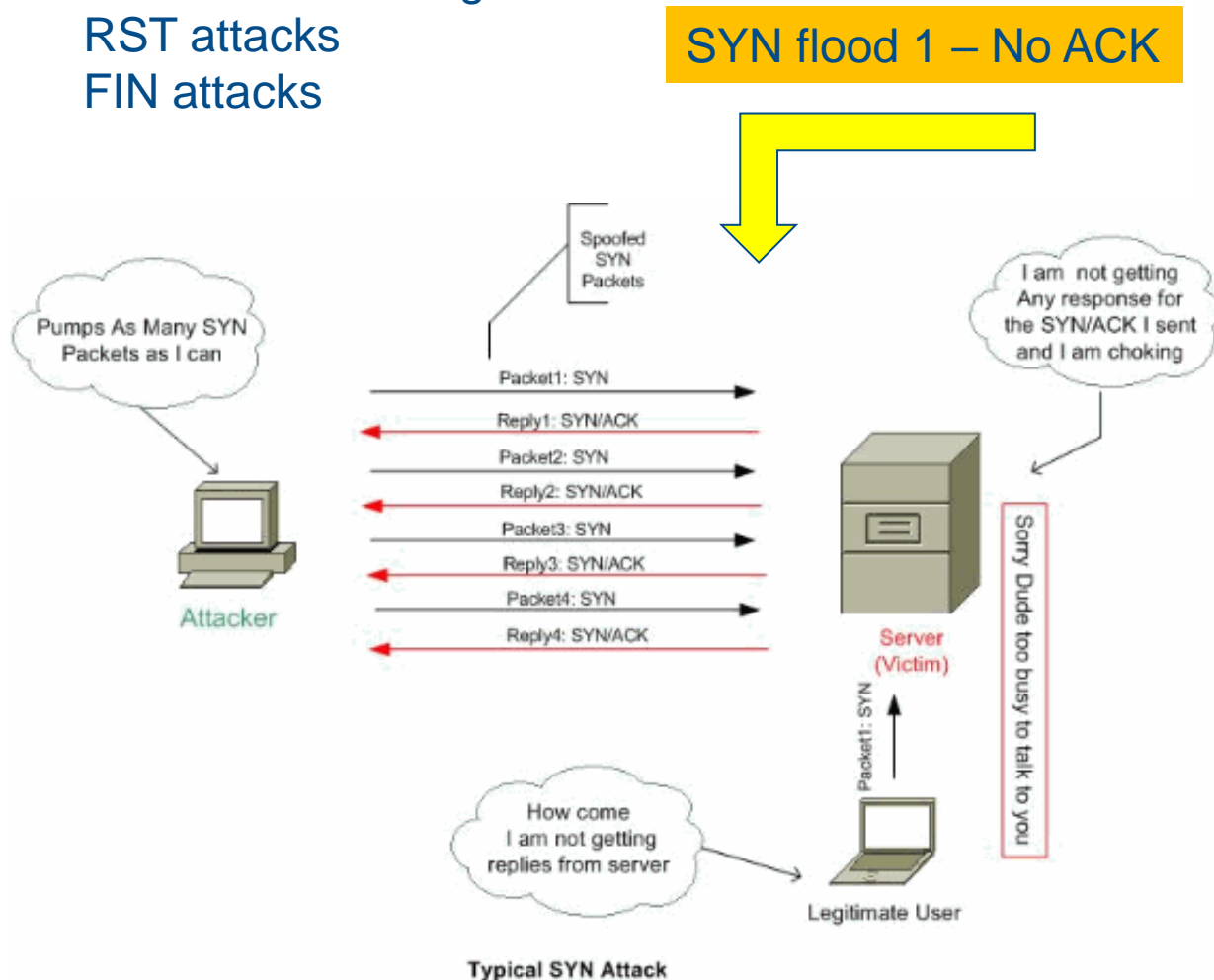
Network Security

TCP security issues:

SYN flood-Causing DoS

RST attacks

FIN attacks





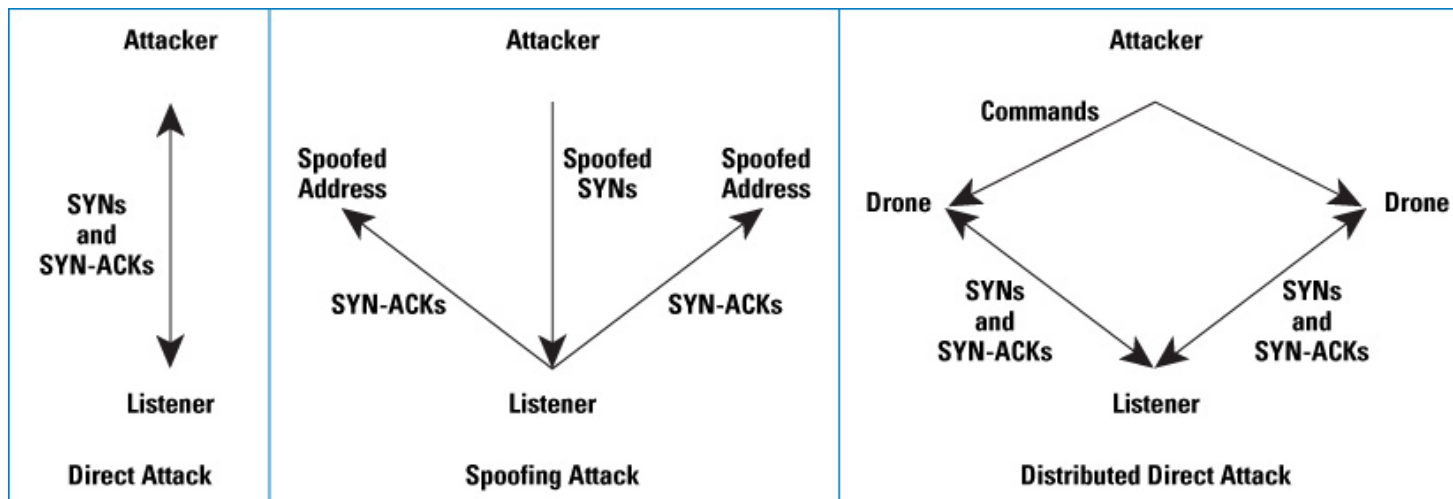
Network Security

Denial of Service

prevent authorized users from accessing a resource, or to **reduce the quality of service** that they receive, can happen in Network, Transport & Application Layer

Distributed DoS attacks (DDoS)

- More than one attacker sends SYN packets by changing or without changing the source IP Address.
- Difficult to stop compared to direct attack and spoofing attack.
- Difficult to conduct compared to direct attack and Spoofing attack.





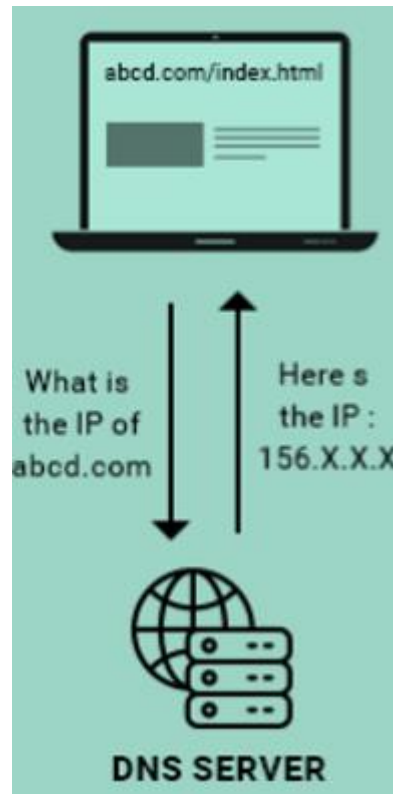
Network Security

UDP security issues

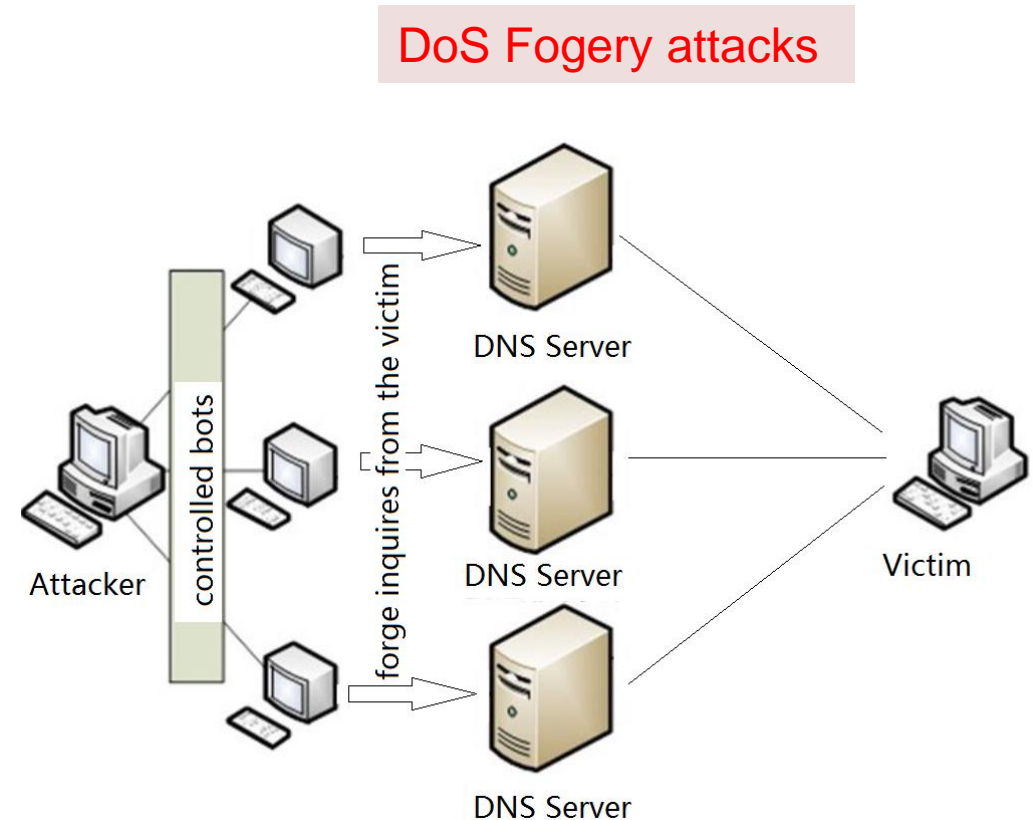
- Illegal connection, no handshake protocol, no authentication
- Easy to be blocked or replaced for UDP data

Ex: DNS

- Based on UDP, no authentication
- Cache poisoning
- DoS forgery attacks
Set the target as the source and send queries



Cache poisoning





Network Security

TCP/UDP mitigation

1. Firewall to block suspicious traffic
2. IDS
3. IPS
4. SSL/TLS



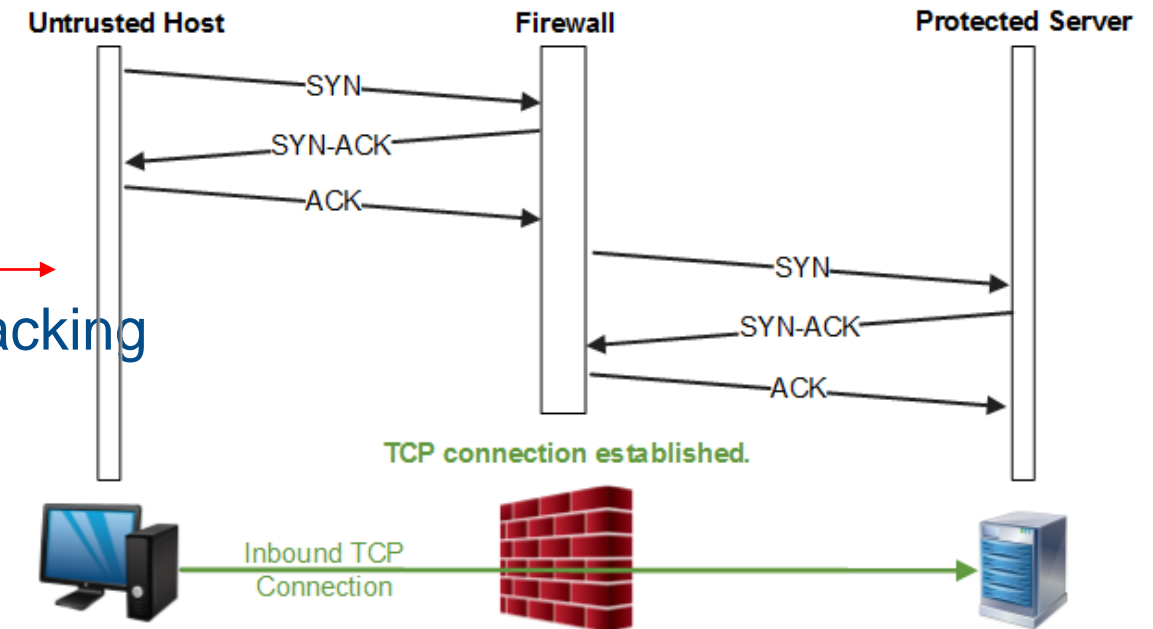
Network Security

Firewall

- Connection first, security with best effort
- Can be hardware, software
- **Support**
 - ✓ Access control
 - ✓ Log management
 - ✓ Traffic control
 - ✓ NAT
 - ✓ VPN

- **Techniques:**
 - ✓ Packet filter
 - ✓ **Proxy** →
 - ✓ Stateful firewall tracking

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Mailserver	TCP	>1023	25	Any	Permit
B	Outbound	Mailserver	External	TCP	25	>1023	Yes	Permit
C	Outbound	Internal	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Internal	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

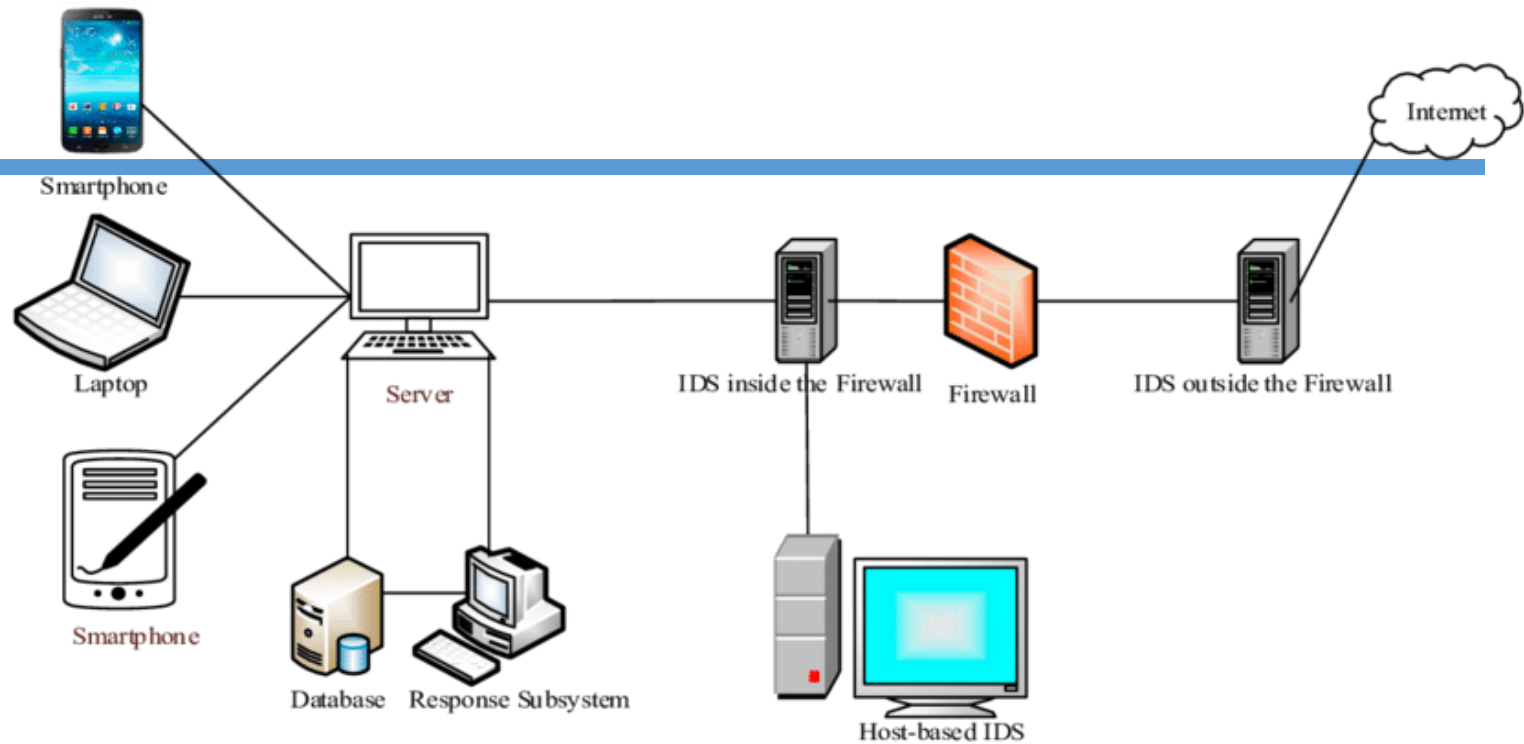




Network Security

Intrusion Detection System

- Detect inappropriate, incorrect or anomalous activities
- can learn and creates rules



- **Host-based ID system:** installs the IDS on a host and monitor activities on it.
- **Network-based ID system:** can be put before/behind a firewall. Detects, classify and proactively stop malicious actions from the attackers who managed to pass the firewall based on predefined set of signatures and rules.
- **Honeypot system:** designed to lure attackers. Any attacks against the honeypot are made to seem successful, giving admin time to mobilize, log and possibly track and apprehend the attacker without exposing the production systems.



Network Security

Intrusion Detection System

- Compare data to known threats
- Compare data to baseline of normal activity
- Must be “trained” for your specific environment
- Configure specific rules
- Tweak to eliminate false positive

What about encrypted data?

- Cannot examine encrypted data
- Some solutions allow the configuration of decryption keys
 - ✓ Enter symmetric key
 - ✓ Import PKI certificate

NIDS tools:

- Snort (free and open source)
- Alien Vault Unified Security Management(USM)
- Symantec NetProwler

IDS looks for hints of:

Reconnaissance

- Ping sweeps
- Port scan
- SNMP scanning

Network exploits

- Testing discovered targets for weaknesses

DoS

- Excessive traffic or activity on a specific host beyond normal usage



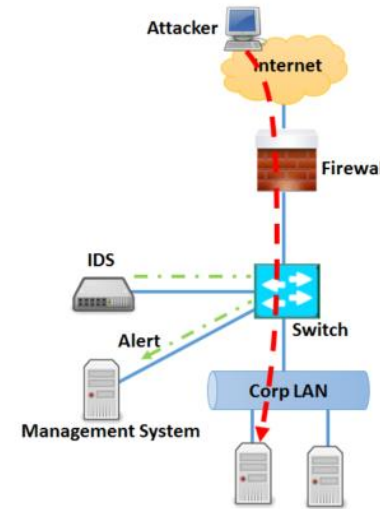
Network Security

Intrusion Prevention System

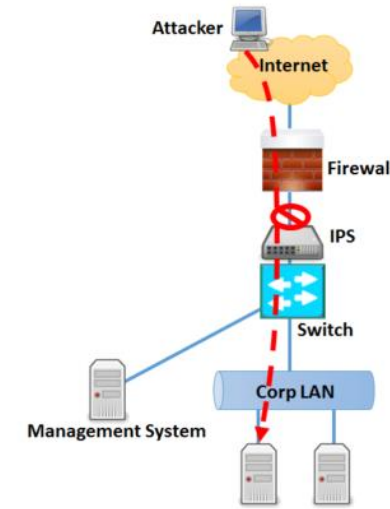
- Can respond to an incident in real-time
- Detect misuse and abuse of network resources
- In-band response (NIDS out-of-band)

<https://www.itprc.com/intrusion-prevention-detection-tools/>

Intrusion Detection System



Intrusion Prevention System



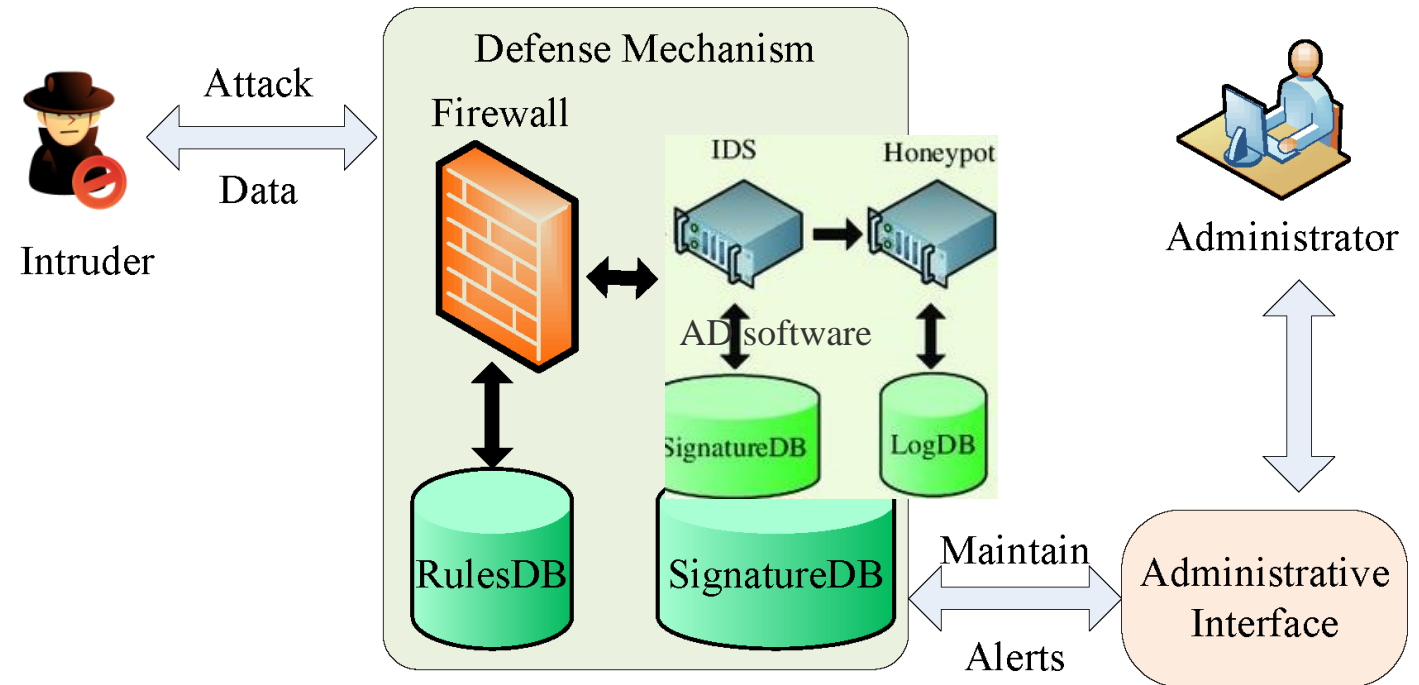
IDS	IPS
Detection mode only	Active traffic control
Traffic replication required	Original traffic required
Decoupling detection and reaction functionalities	Detection and reaction support
IDS as a good assistant for network admin	No admin assistance needed
Usually used for testing rules	Requires strict configuration



Network Security

Honeypot System

- Security mechanism set to detect attacks or deflect them from a legitimate target
- Used to gain information about how cybercriminals operate
- Honeypots lure attackers, so ensure isolation from production environments
- Extract signature for IDS and IPS





Network Security

SSL/TLS protocol

- Authenticity
 - Server and Client need to exchange certificate to authenticate each other
- Confidentiality
 - Encryption
- Integrity
 - Apply encryption and Hash
- Two layer
 - Handshake protocol
 - Record protocol, define data format for transmission
- Built above TLL

TCP/IP

Application Layer (DNS, SMTP, IMAP, FTP, HTTP, Telnet, SNMP)

Transport Layer (UDP, TCP)

Internet Layer (IP, ARP, NAT, ICMP, OSPF)

Network Access Layer (Token Ring, PPP, Ethernet)

TCP/IP

Application Layer (DNS, SMTP, IMAP, FTP, HTTP, Telnet, SNMP)

SSL Handshake

SSL Record Layer

Transport Layer (UDP, TCP)

Internet Layer (IP, ARP, NAT, ICMP, OSPF)

Network Access Layer (Token Ring, PPP, Ethernet)



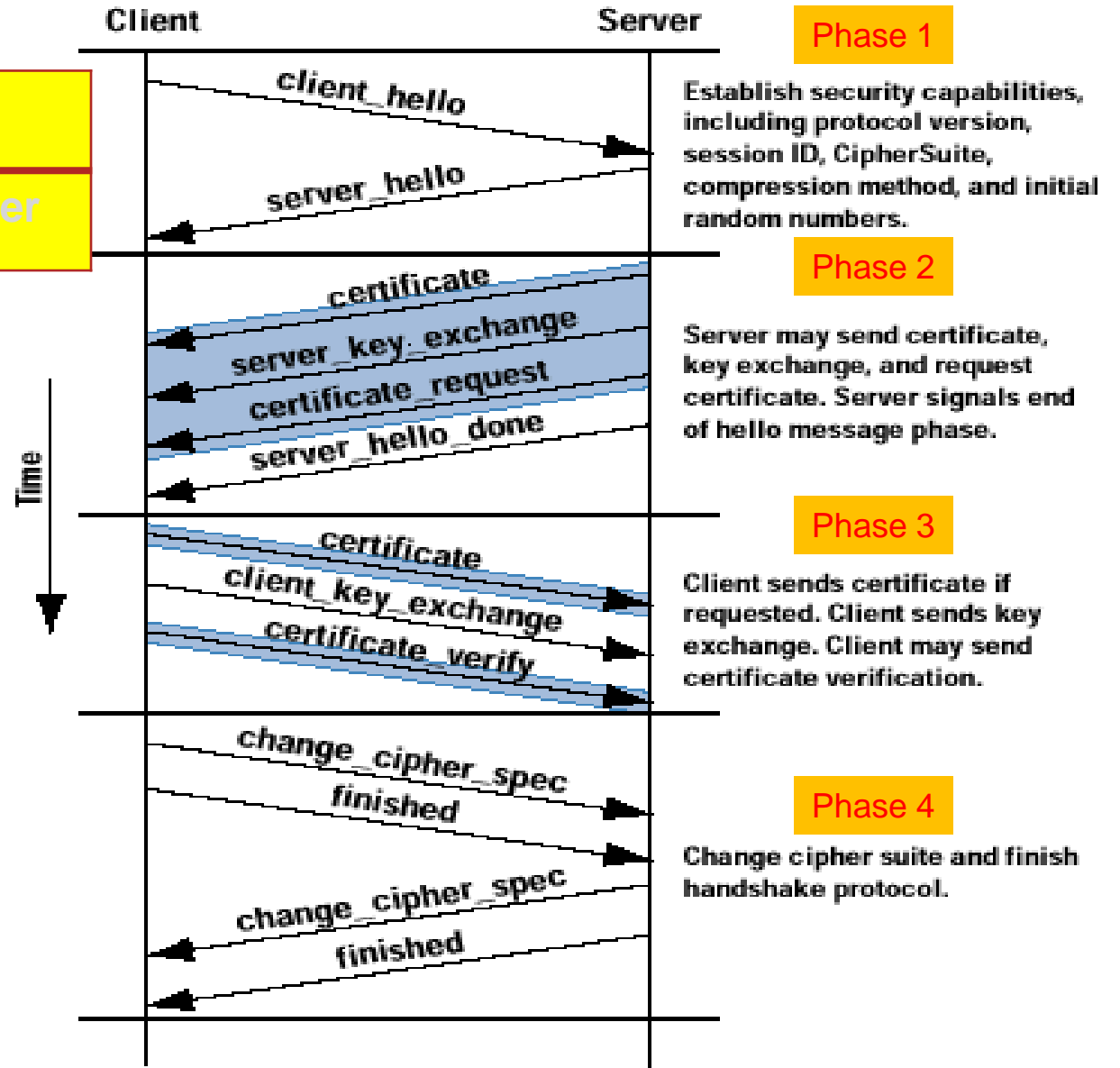
Network Security

SSL handshake protocol

SSL Handshake

SSL Record Layer

- Authentication using public key certificates
- Encryption algorithm discussion
- Derivation of encryption and authentication keys
- Key confirmation
- Before any data transmission



Note: Shaded transfers are optional or situation-dependent messages that are not always sent



Network Security

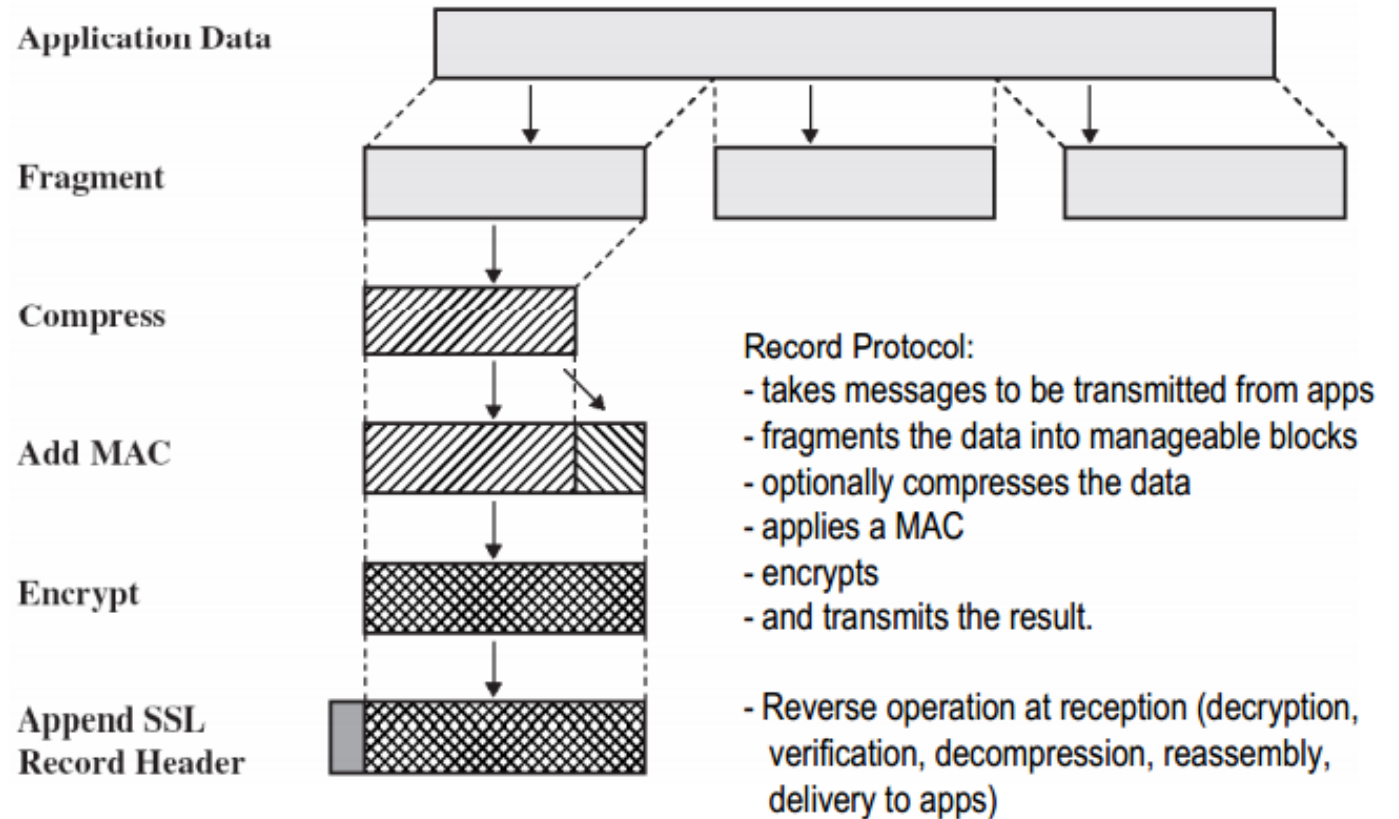
SSL Handshake

SSL/TLS record protocol

SSL Record Layer

- Provide capsulation, compression, encryption for high-level protocols such as HTTP, FTP etc.
- Message Authentication Code is to provide msg integrity
- Encryption by symmetric algorithms

Record Protocol Operation

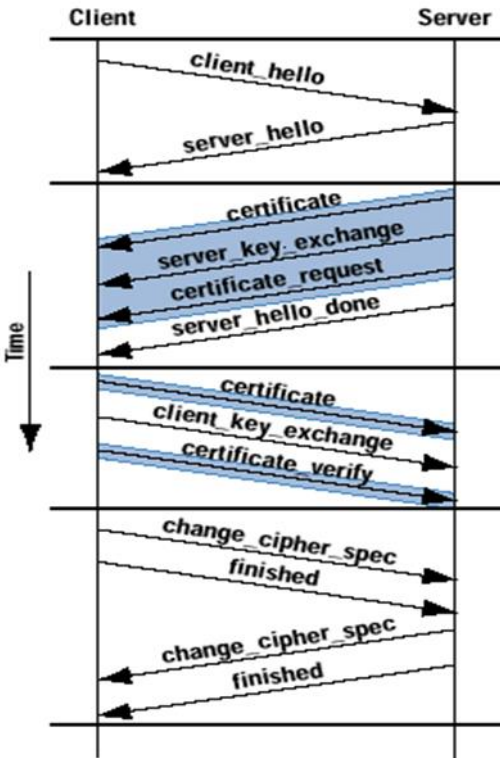




Network Security

Case Study 1 - TLS1.2

CA: Certificate Authority



Hello let's do TLS

OK Here is my Certificate,
containing my public key

Certificate verified with **CA!**

Let's use this session key (encrypted
using server public key)

Encrypted key



Server's
Public key



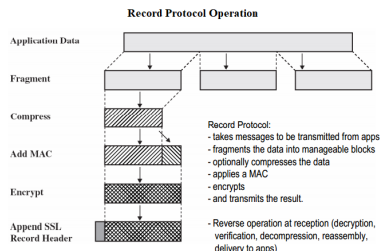
Server's
Private key

Decrypted Key

Symmetric Encrypt / Decrypt

Decrypted Data

Encrypted Data

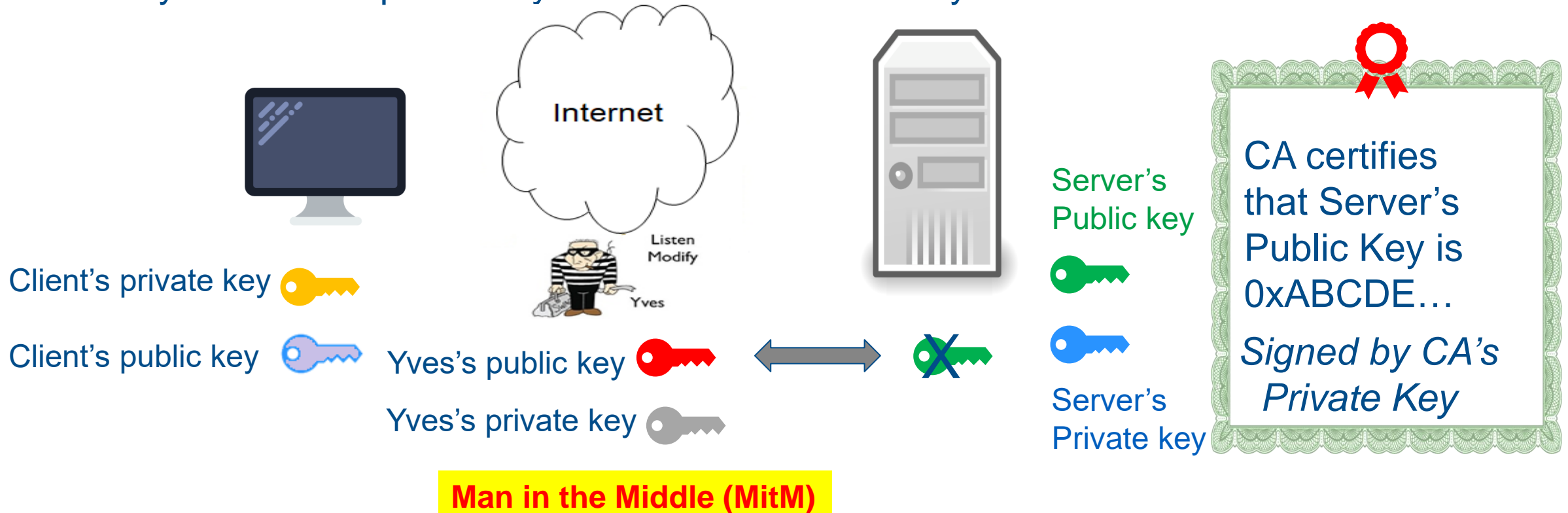


Network Security

Case study 1: TLS 1.2

Authentication for a server:

How can you trust the public key of the server? Is it really from the true Server?





Network Security

TLS (Transport layer security)

- Internet standard version of SSL
- **Handshake protocol** provides: Authentication (Server to Client, X.509 certificate), establishment of keys for record protocol
- **Record protocol** provides: Msg confidentiality (symmetric algorithms) & Integrity (MAC)

SSL Handshake

SSL Record Layer

SSL/TLS Attacks

- Attacks on handshake protocol, exploit format and implementation of RSA, 1998, 2012
- Attacks on the record and application data protocols, BEAST'11, chosen plain-text attack; CRIME'12, recover content of web cookies with compressed data in TLS
- Attacks on PKI, validity of X.509 certificates is vulnerable, 2012
- Other attacks, DoS with SSL/TLS server, 2011
- Heartbleed, 2014



Network Security

Case Study - TLS1.2



Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128

Key Exchange + Authentication + Block Cipher (Session) + Message Digest

DH

RSA

AES

SHA256



Network Security

Case study 2: HTTP over SSL – HTTPS

- A secure communication between a web browser and a web server
- HTTPS capability is built into all modern Web browsers and server support HTTPS.
- Normal HTTP uses port 80, HTTPS uses 443 which invokes SSL. – refer to RFC2818
- Provide a solution for Web transaction security.
A message from HTTP (regarding web transaction) is passed down to SSL, which then wraps this message into an SSL record.

What are encrypted?

URL of the requested doc

Contents of the doc

Contents of browser forms

Cookies sent from browser to server and from
server to browser

Contents of HTTP header



Network Security

Conclusion

- Transport layer security
- Firewall
- IDS & IPS
- SSL/TLS
- HTTPS

Next Topic

- Privacy Preserving Computing and Data Compliance