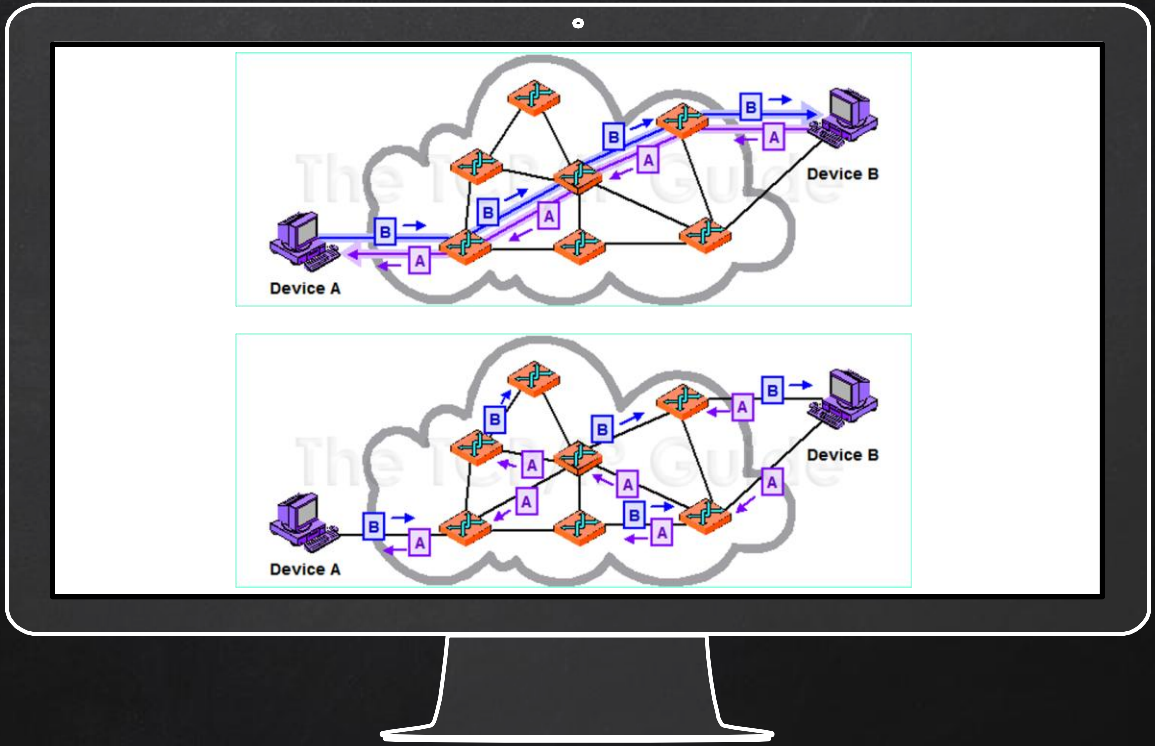
اونيۏرسيتي تيکنولوݢي مارا
UNIVERSITI TEKNOLOGI MARA

CSC662 – COMPUTER SECURITY

061 – NETWORK SECURITY

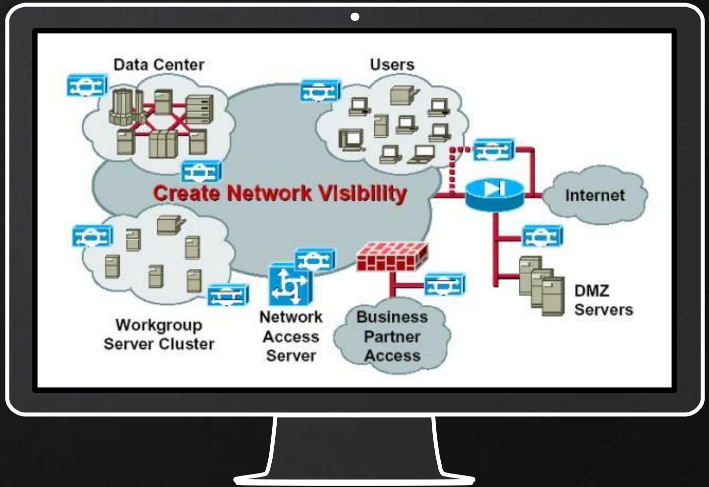
Circuit Switching vs Packet Switching



- ✗ Connection-Oriented: Circuit switching establishes a dedicated communication path between the source and destination before the data transmission starts. This path remains active for the entire duration of the communication session.
- ✗ Connectionless: Packet switching does not establish a dedicated connection before transmitting data. Each packet is individually addressed and routed independently.
- ✗ Overall, circuit switching provides a dedicated and continuous communication path, while packet switching allows for more efficient use of network resources and supports various types of traffic.

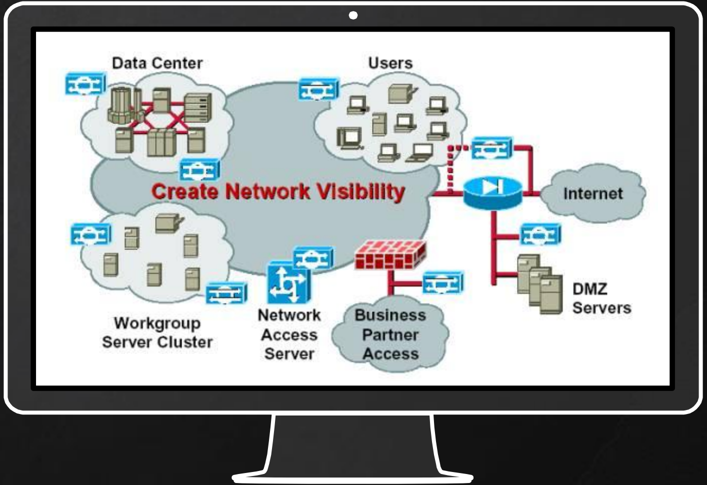
Preventive Network Security Mechanisms 1/2

- ✓ Firewall
  - ✗ Control incoming and outgoing traffic on network with predetermined security policies.
- ✓ Proxy Server
  - ✗ To have a better data security and network performance. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests.
- ✓ Network Segmentation
  - ✗ Boundaries between network segments where computing assets within the segment have a common function, risk or role within an organization.

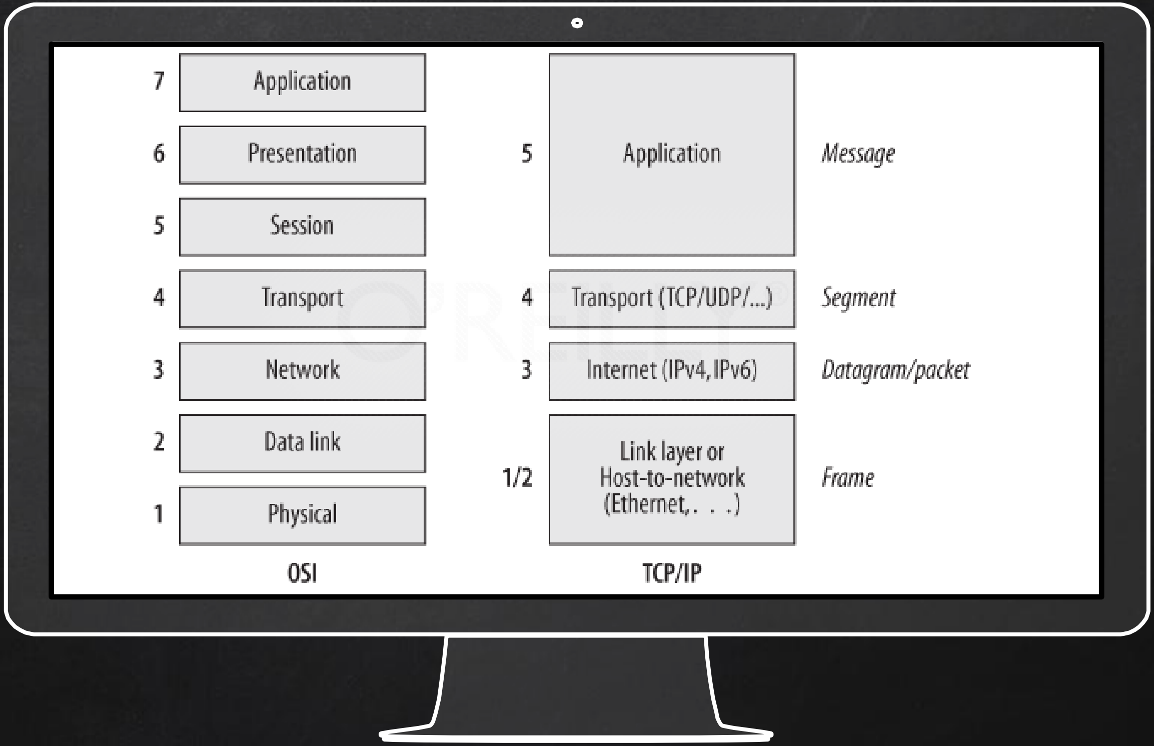


Preventive Network Security Mechanisms 2/2

- ✓ Remote Access VPN
  - ✕ Provides remote and secure access to an organization network to individual hosts or clients
  - ✕ Zero Trust Network Access (ZTNA) - A user should only has access and permission that required to fulfill the role
- ✓ Intrusion Detection/Prevention Systems (IDS/IPS)
  - ✕ To detect or prevent the network security attacks such as brute force attacks, Denial-of-Service attacks and exploits of network vulnerabilities.

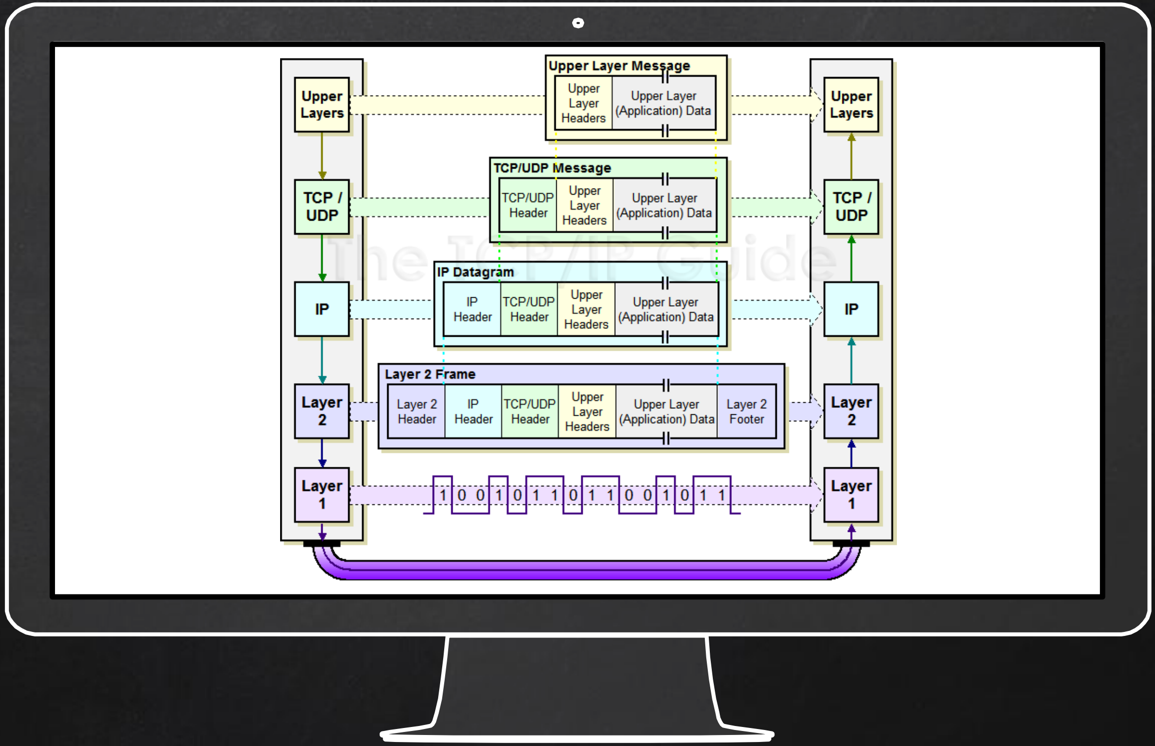


OSI And TCP/IP Layered Models

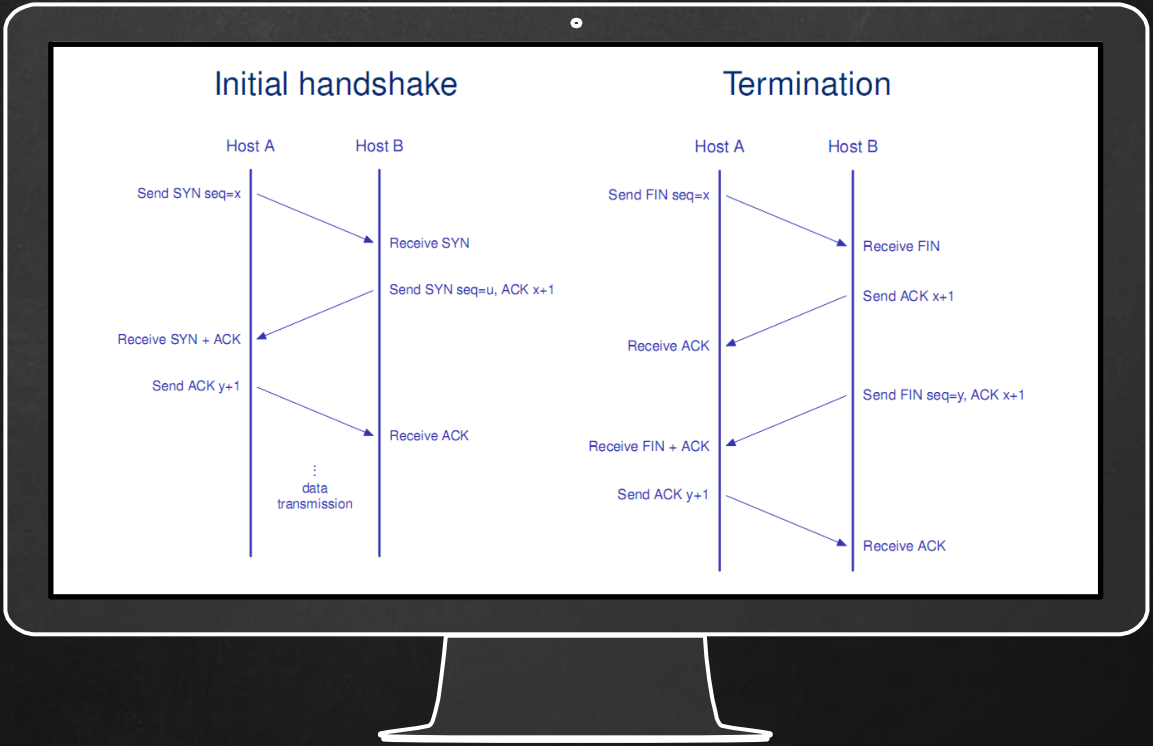


	OSI		TCP/IP	
7	Application	5	Application	*Message*
6	Presentation			
5	Session			
4	Transport	4	Transport (TCP/UDP/...)	*Segment*
3	Network	3	Internet (IPv4, IPv6)	*Datagram/packet*
2	Data link	1/2	Link layer or Host-to-network (Ethernet, . . .)	*Frame*
1	Physical			

TCP/IP Encapsulation



TCP Connection Synchronization



Initial handshake

Host A

Host B

Send SYN seq=x

Receive SYN

Send SYN seq=u, ACK x+1

Receive SYN + ACK

Send ACK y+1

Receive ACK

⋮
data
transmission

Termination

Host A

Host B

Send FIN seq=x

Receive FIN

Send ACK x+1

Receive ACK

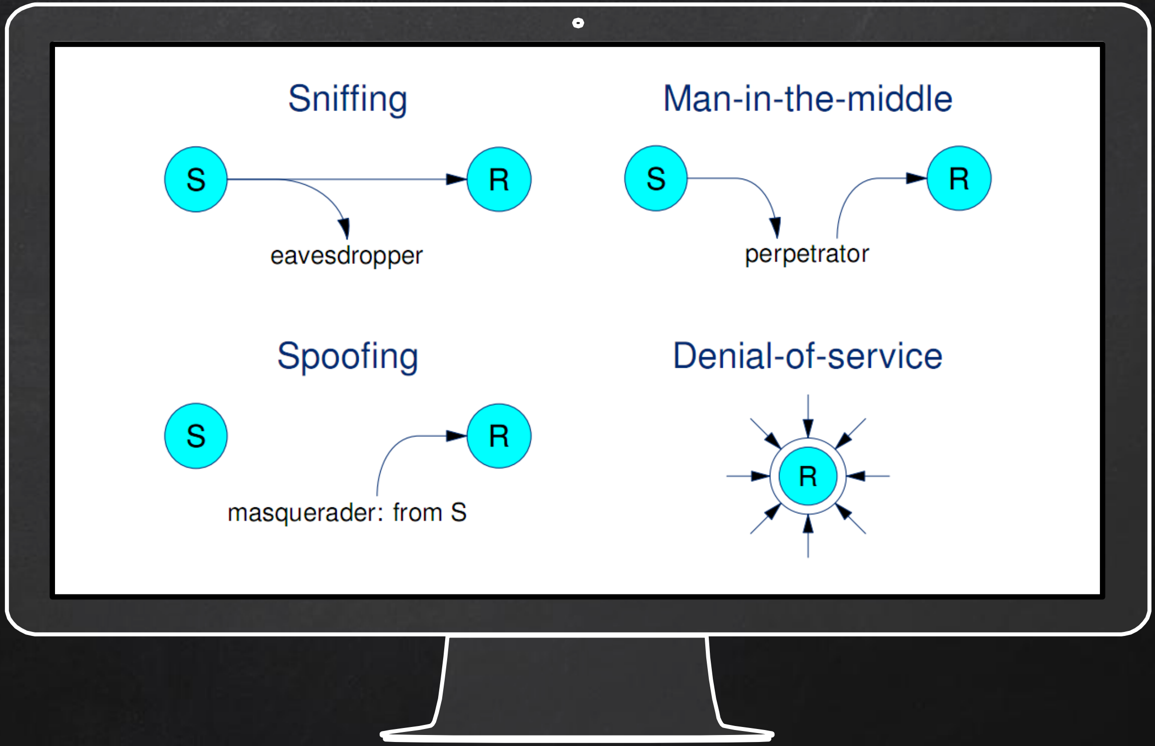
Send FIN seq=y, ACK x+1

Receive FIN + ACK

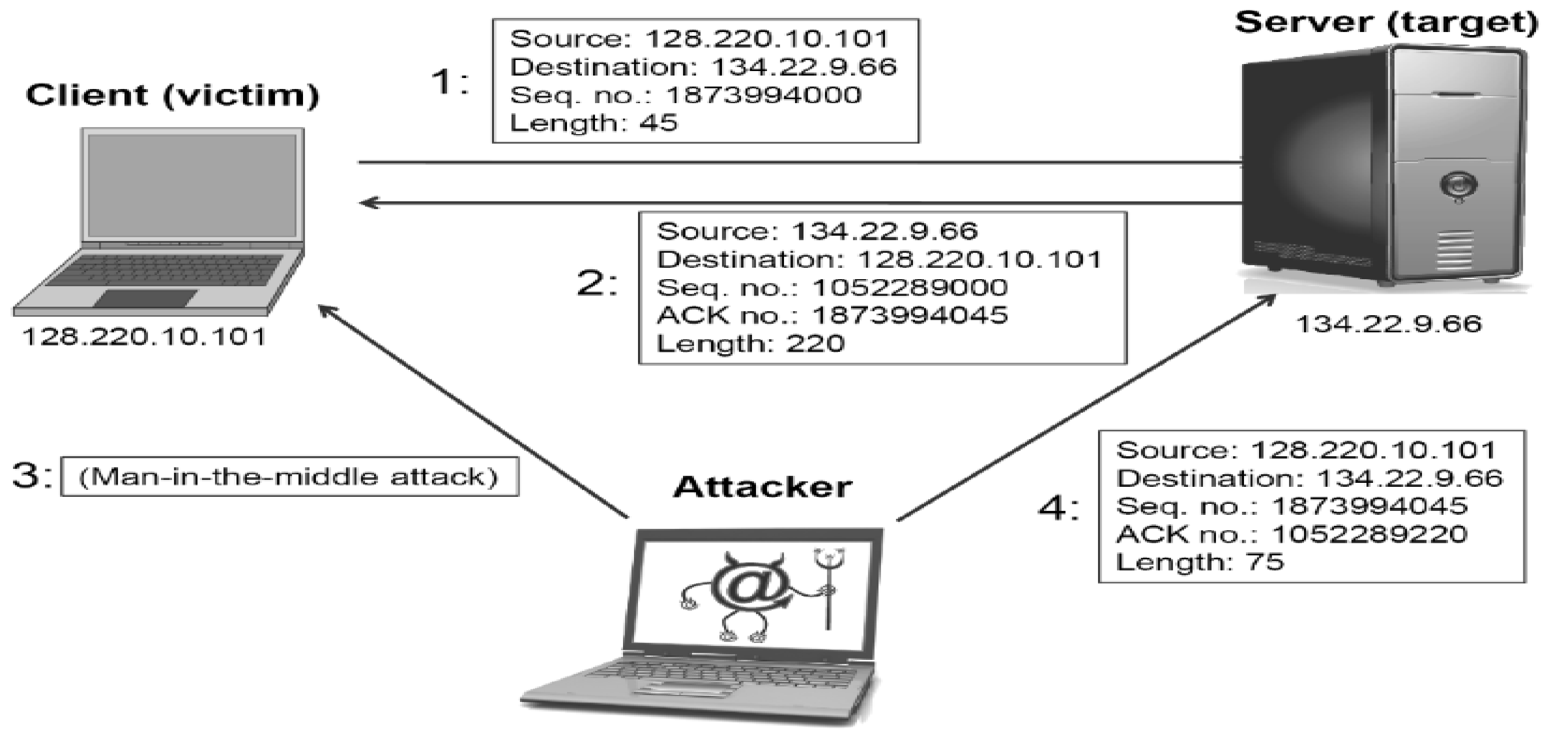
Send ACK y+1

Receive ACK

What Can Go Wrong?



What Can Go Wrong?: TCP Session Hijacking



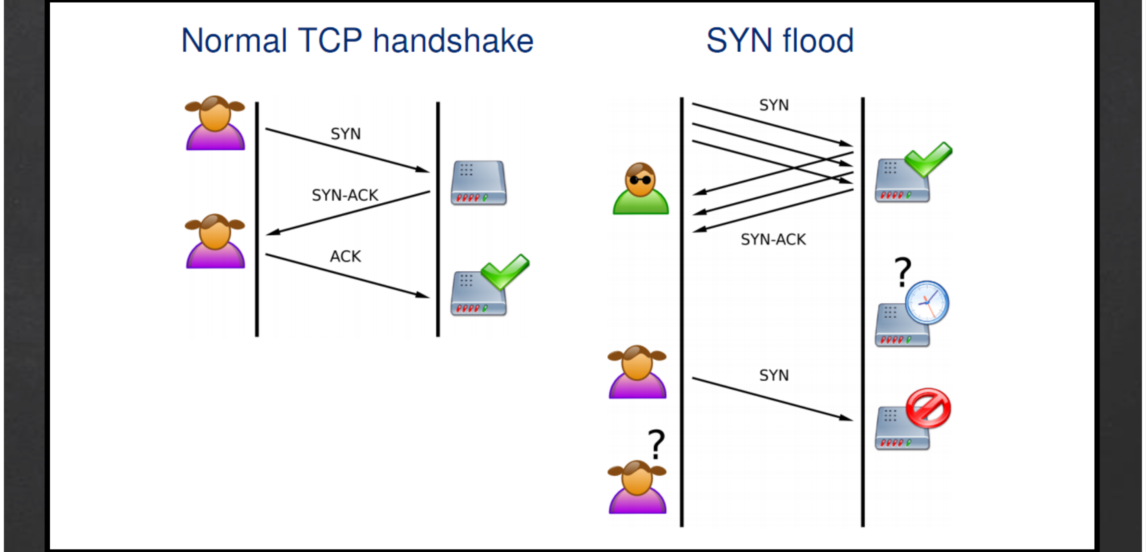
1: Source: 128.220.10.101
Destination: 134.22.9.66
Seq. no.: 1873994000
Length: 45

2: Source: 134.22.9.66
Destination: 128.220.10.101
Seq. no.: 1052289000
ACK no.: 1873994045
Length: 220

3: (Man-in-the-middle attack)

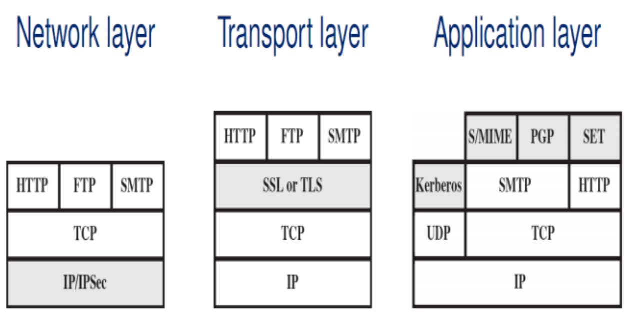
4: Source: 128.220.10.101
Destination: 134.22.9.66
Seq. no.: 1873994045
ACK no.: 1052289220
Length: 75

What Can Go Wrong?: Denial-of-Service



IP Layer Security: IPSec

- Operates at network layer of the OSI model and can be used to authenticate and encrypt IP packets.
- Objective:
  - Secure connectivity of branch offices - ensuring the confidentiality and integrity of data transmitted over the network
  - Secure remote access
- Advantages:
  - Bypass resistance - eavesdropping or tampering with the data during transmission
  - Transparency to end users and applications
- Disadvantages:
  - Infrastructure support needed - policies, key management, and potentially the use of additional hardware or software components.
  - Performance degradation - encryption and authentication processes involved in IPsec can introduce some performance degradation.



Network layer

HTTP | FTP | SMTP

TCP

IP/IPSec

Transport layer

HTTP | FTP | SMTP

SSL or TLS

TCP

IP

Application layer

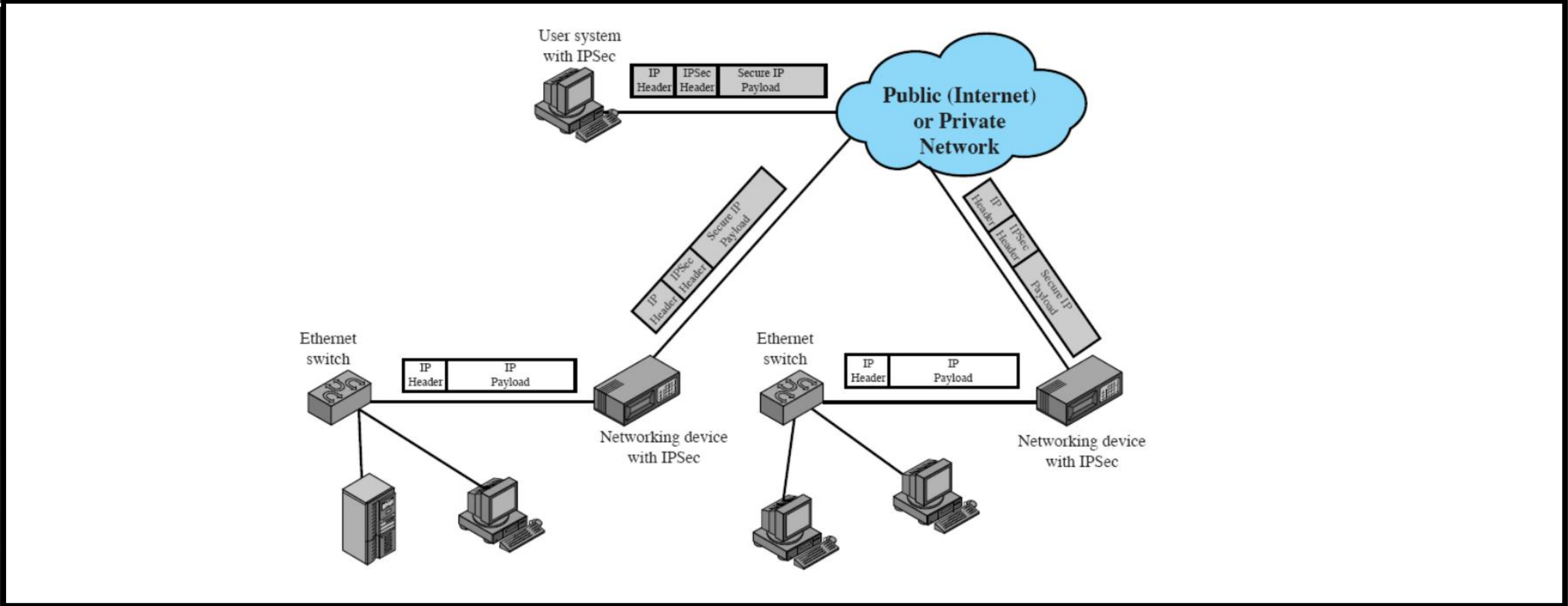
S/MIME | PGP | SET

Kerberos | SMTP | HTTP

UDP | TCP

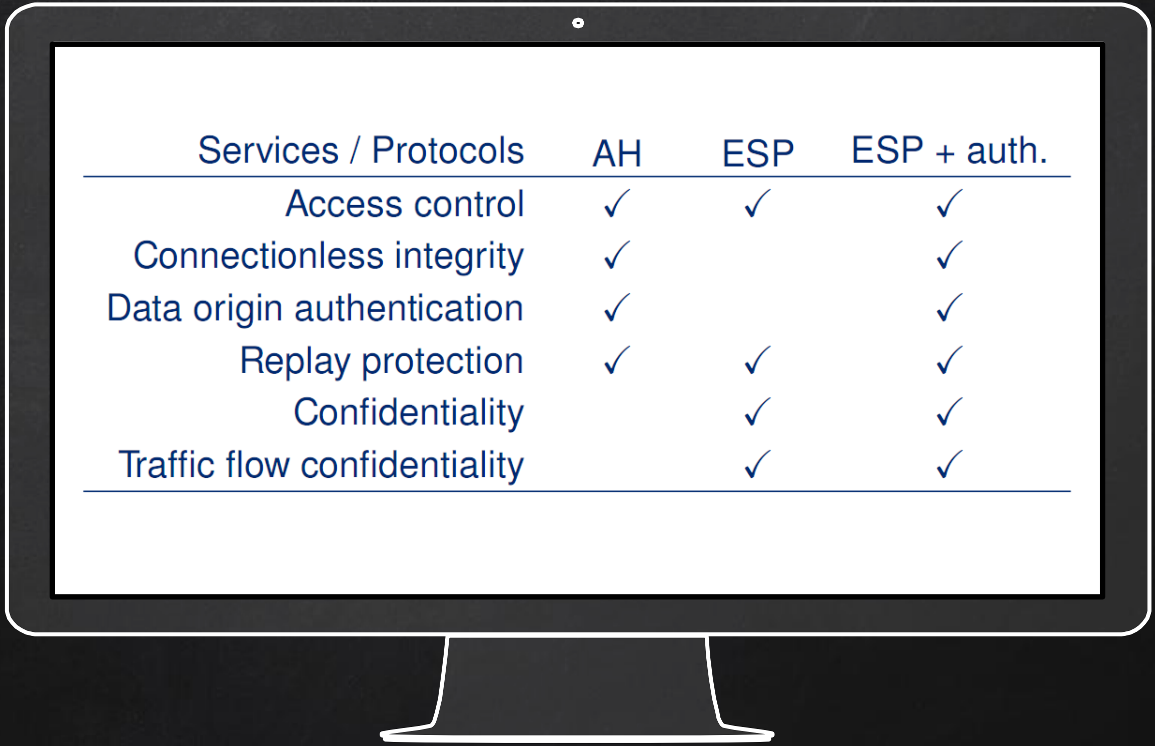
IP

IP Layer Security: Example



routers, firewalls, and VPN gateways.

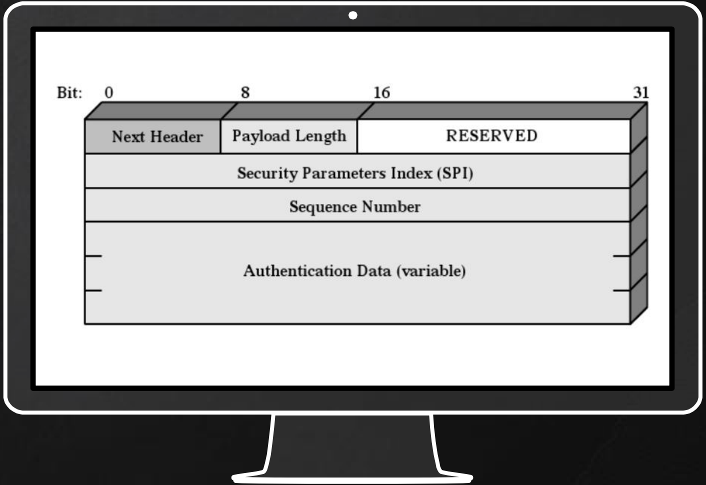
IP Layer Security: Services And Protocols (Authentication Header (AH), Encapsulating Security Payload (ESP) ESP with Authentication (ESP+Auth)



Services / Protocols	AH	ESP	ESP + auth.
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Replay protection	✓	✓	✓
Confidentiality		✓	✓
Traffic flow confidentiality		✓	✓

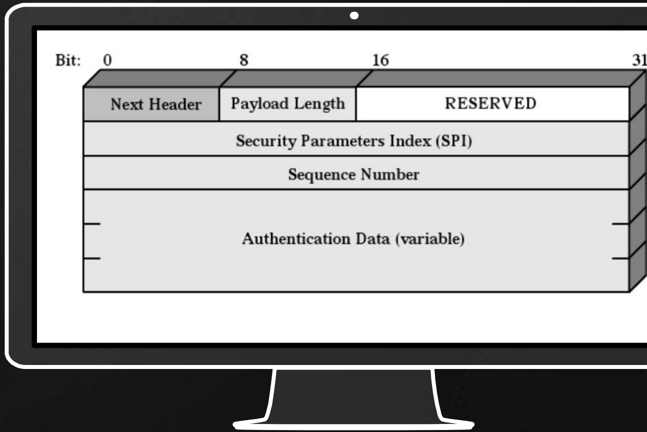
IP Layer Security: Authentication Header (AH)

- ✓ Authentications of immutable (unchangeable) packet fields to ensure integrity
- ✓ Replay attack prevention (via a separate sequence number) - Each packet is assigned a unique sequence number, and the recipient can use this information to detect and discard duplicate or out-of-order packets
- ✓ Uses MAC(Message Authentication Code); shared secret needed – a cryptographic technique used to ensure the integrity and authenticity of a message.


Bit: 0
8
16
31
Next Header
Payload Length
RESERVED
Security Parameters Index (SPI)
Sequence Number
Authentication Data (variable)

IP Layer Security: Encapsulated Security Payload (ESP)

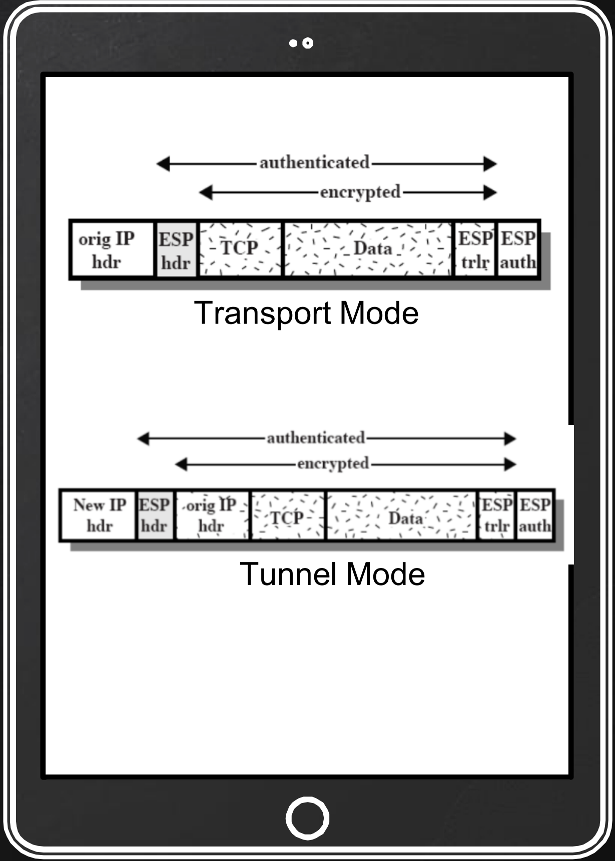
- ✓ Encryption of full packet payload (data) of the original IP packet, as well as any higher-layer protocol data (e.g., TCP or UDP).
- ✓ To ensure the confidentiality of the transmitted data, making it unreadable to unauthorized parties.
- ✓ Optional authentication of packet payload - the sender can include authentication data that allows the recipient to verify the integrity and authenticity of the payload.



Bit: 0	8	16	31
Next Header	Payload Length	RESERVED	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

IP Layer Security: Modes

- ✓ Transport mode
  - ✗ Simple mechanism for end-to-end security between two hosts.
  - ✗ It encrypts and/or authenticates the payload of the IP packet, ensuring the confidentiality, integrity, and authenticity of the data being transmitted.
- ✓ Tunnel mode
  - ✗ Transparent intermediate tunneling - to create a secure "tunnel" between two networks.
  - ✗ Bundling of TCP streams: prevention of traffic analysis by eavesdropper.
  - ✗ bundling of multiple TCP streams or multiple communications between different hosts into a single IPsec-protected tunnel.



Transport Mode

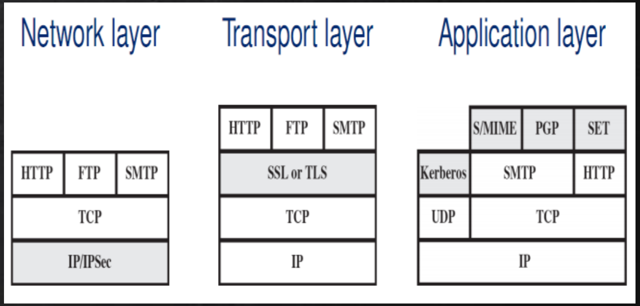
Tunnel Mode

IP Layer Security: Security Association (SA)

- ✓ Uniquely identifies an IPsec flow - distinguish flow of traffic between two network entities that are secured using IPsec
- ✓ SA components consists of
  - ✗ Security Parameters Index (SPI) - distinguish between different SAs
  - ✗ Destination IP address - destination entity for which the SA is established
  - ✗ Security Protocol Identifier – specifies destination entity for which the SA is established (AH or ESP)
- ✓ SA is unidirectional, two SA’s are needed if both directions are to be under IPsec
- ✓ SA is reset if a sequence number overflows to prevent replay attack
- ✓ Multiple SA’s may be assigned to a flow

Transport Layer Security: SSL/TLS

- Objectives:
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over a computer network (data exchange between client and server.) Secure information transmission in Internet applications (establishing trust)
  - Mutual authentication in Internet applications
- Advantages:
  - Secure end-to-end communication over TCP (not limited to HTTP but SMTP, FTP, IMAP, POP etc)
- Disadvantages:
  - PKI support needed to manage digital cert for authentication & establishing the identity of the communicating parties
  - Potential use of weak cryptographic algorithms (e.g.RC4)



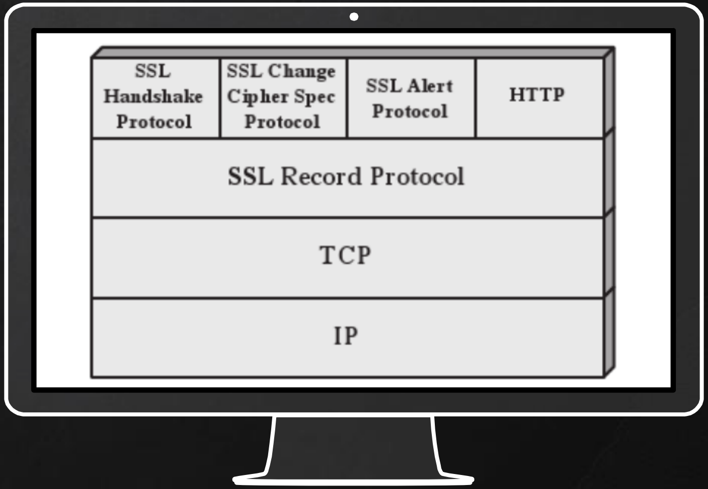
Network layer
HTTP FTP SMTP
TCP
IP/IPSec

Transport layer
HTTP FTP SMTP
SSL or TLS
TCP
IP

Application layer
S/MIME PGP SET
Kerberos SMTP HTTP
UDP TCP
IP

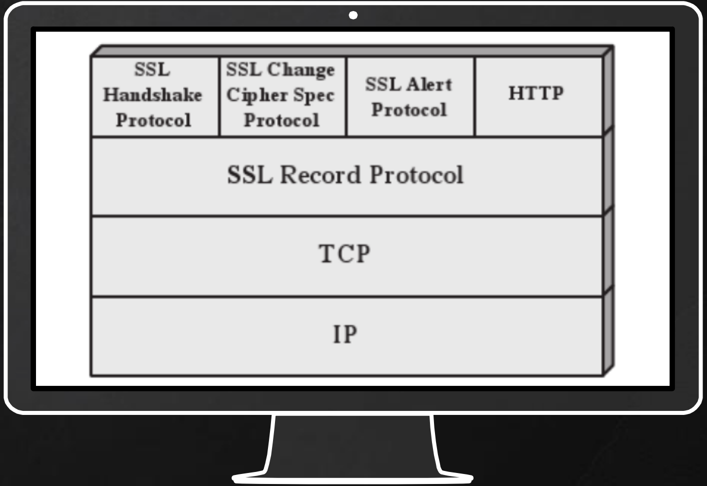
Transport Layer Security: SSL Architecture

- ✓ SSL connection is established on top of a TCP connection.
- ✓ SSL operates as a protocol layer above TCP, providing a secure and encrypted communication channel.
- ✓ When a client and server wish to establish a secure connection, they begin with a TCP connection and then initiate the SSL handshake to set up the secure communication layer.
- ✓ SSL sessions represent an association between a client and a server. Sessions define parameters that can be share between connections. - During the SSL handshake, cryptographic parameters, such as encryption keys, are negotiated and established.

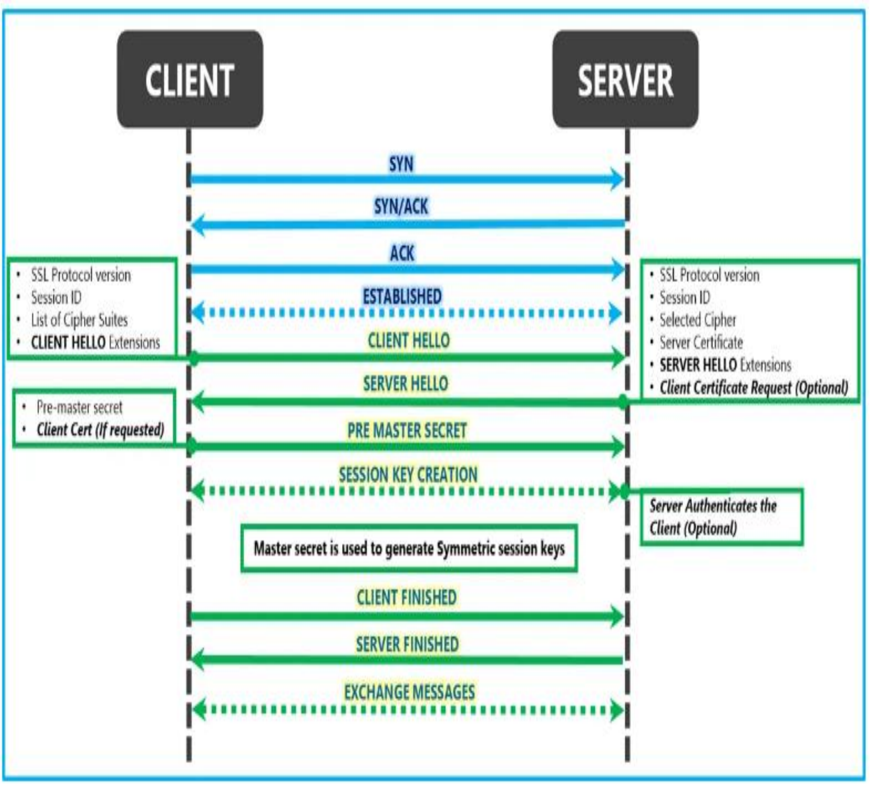


Transport Layer Security: SSL Record Protocol

- ✓ Carries out information transfer
- ✓ Provides confidentiality and message integrity services.
- ✓ Information Transfer: - responsible for framing and encapsulating higher-layer protocol data (such as application data) into SSL/TLS records. These records are then transmitted over the network.
- ✓ Confidentiality: One of the primary goals of the SSL Record Protocol is to provide confidentiality for the transmitted data. Encrypting the payload of SSL records using encryption algorithms negotiated during the SSL/TLS handshake. Common encryption algorithms include those using symmetric key ciphers like AES (Advanced Encryption Standard).
- ✓ Message Integrity: - The SSL Record Protocol ensures the integrity of the transmitted data through the use of cryptographic hash functions, such as HMAC (Hash-based Message Authentication Code). This helps verify that the data has not been tampered with during transmission



Transport Layer Security: SSL Handshake Protocol



CLIENT

SERVER

SYN

SYN/ACK

ACK

ESTABLISHED

CLIENT HELLO

SERVER HELLO

PRE MASTER SECRET

SESSION KEY CREATION

CLIENT FINISHED

SERVER FINISHED

EXCHANGE MESSAGES

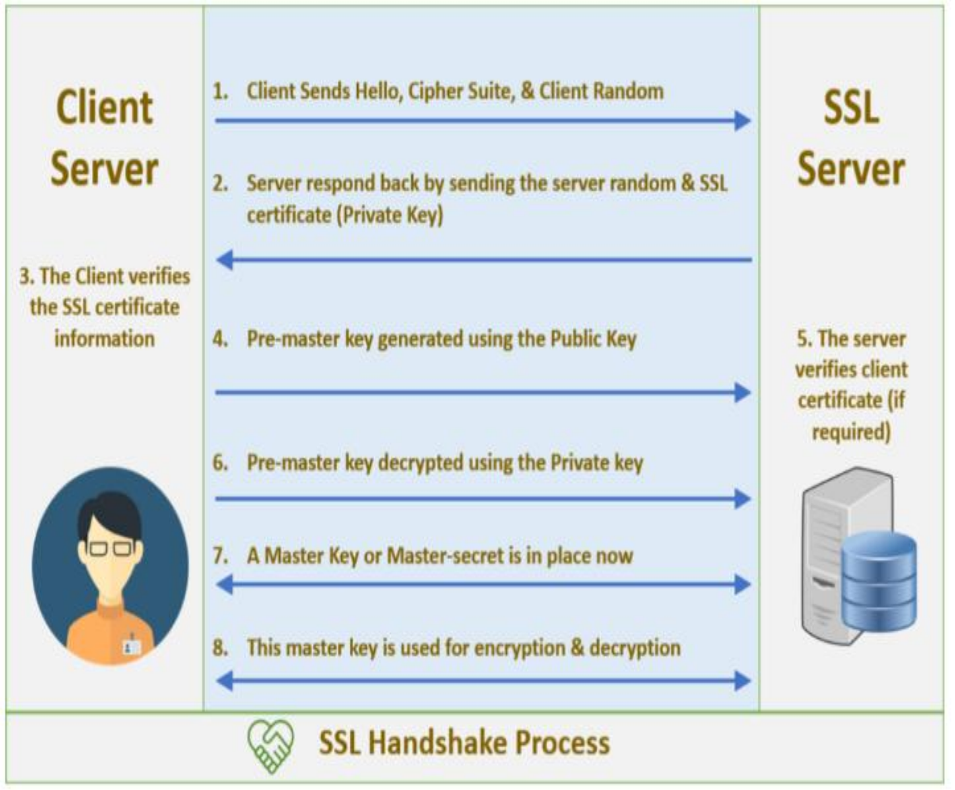
- SSL Protocol version
- Session ID
- List of Cipher Suites
- **CLIENT HELLO** Extensions

- SSL Protocol version
- Session ID
- Selected Cipher
- Server Certificate
- **SERVER HELLO** Extensions
- *Client Certificate Request (Optional)*

- Pre-master secret
- *Client Cert (If requested)*

Server Authenticates the Client (Optional)

Master secret is used to generate Symmetric session keys



Client Server

SSL Server

1. Client Sends Hello, Cipher Suite, & Client Random
2. Server respond back by sending the server random & SSL certificate (Private Key)

3. The Client verifies the SSL certificate information

4. Pre-master key generated using the Public Key

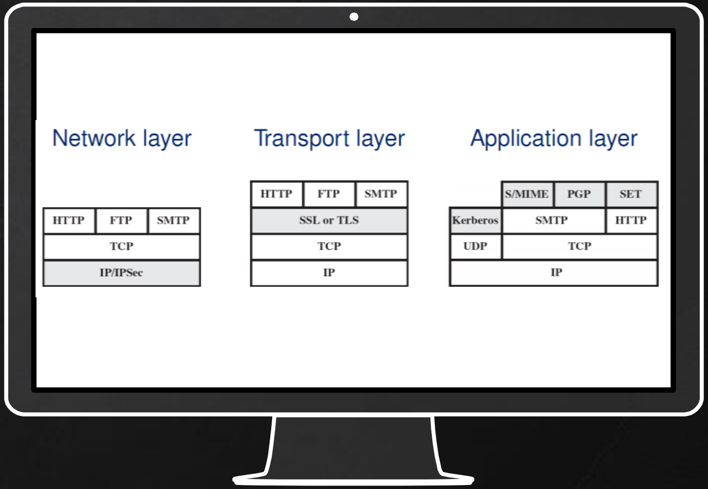
5. The server verifies client certificate (if required)

6. Pre-master key decrypted using the Private key
7. A Master Key or Master-secret is in place now
8. This master key is used for encryption & decryption

SSL Handshake Process

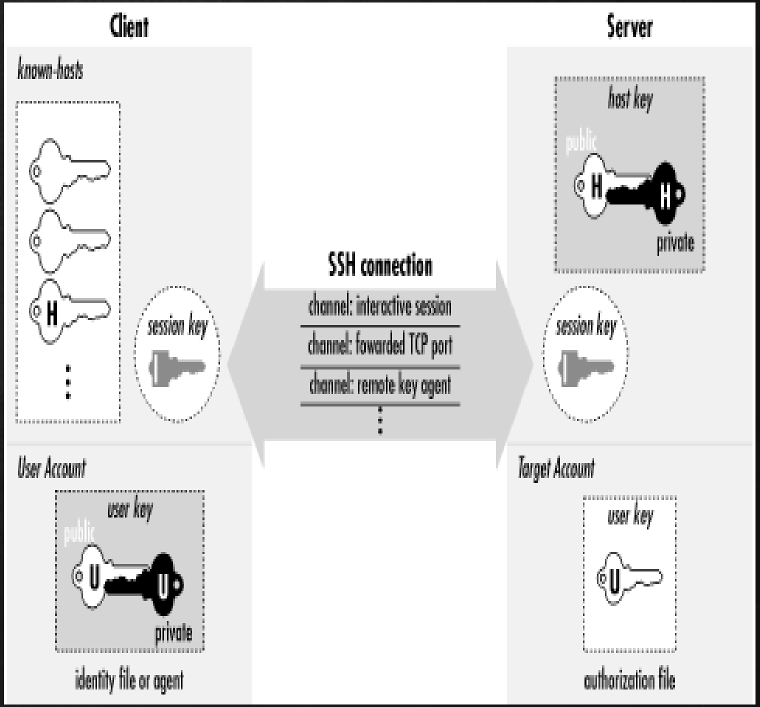
Application Layer Security: SSH

- SSH (Secure Shell) is a cryptographic network protocol that provides secure remote login, command execution, and file transfer capabilities over an insecure network.
- Objectives
  - Secure remote login
  - Secure services (e.g.FTP, copy (scp)) over an insecure network
  - Secure port forwarding
- Advantages
  - Various authentication methods - password-based authentication, public-key authentication, and two-factor authentication.
  - A neat way to bypass firewalls - SSH tunneling (encrypted tunnel) or port forwarding.
- Disadvantages
  - point-to-point only - client and a server. not suitable for broadcasting or multicasting data.
  - Some security vulnerabilities



Application Layer Security: SSH Architecture

- ✓ Server - A program that allows incoming SSH connections to a machine, handling authentication, authorization, and so forth.
- ✓ Client - A program that connects to SSH servers and makes request.
- ✓ Session - An ongoing connection between a client and a server. It begins after the client successfully authenticates to a server and ends when the connection terminates.
- ✓ Key – Provide encryption, to ensure that only person holding that key can decrypt the message; in authentication, it allows you to later verify that the key holder actually signed the message.

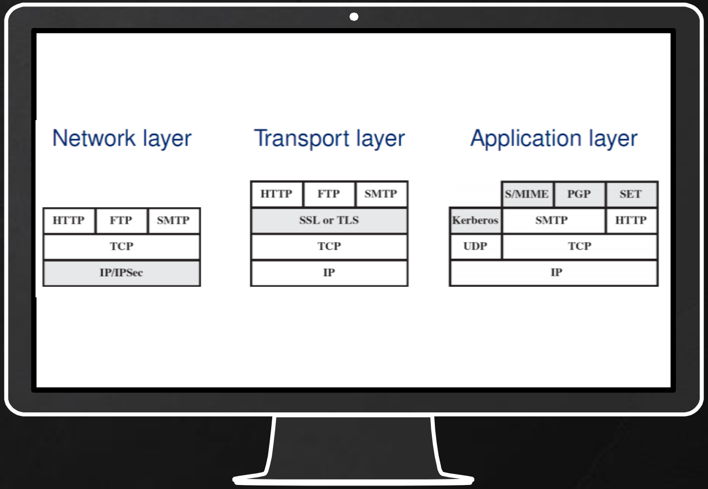


Application Layer Security: Preventable Attacks

✓ Eavesdropping – encryption

✓ TCP session hijacking - Implement Strong Authentication eg: secure login methods, multi-factor authentication (MFA), and strong password policies.

✓ Man-in-the-midle attacks – use secure communication protocols, certificate pinning

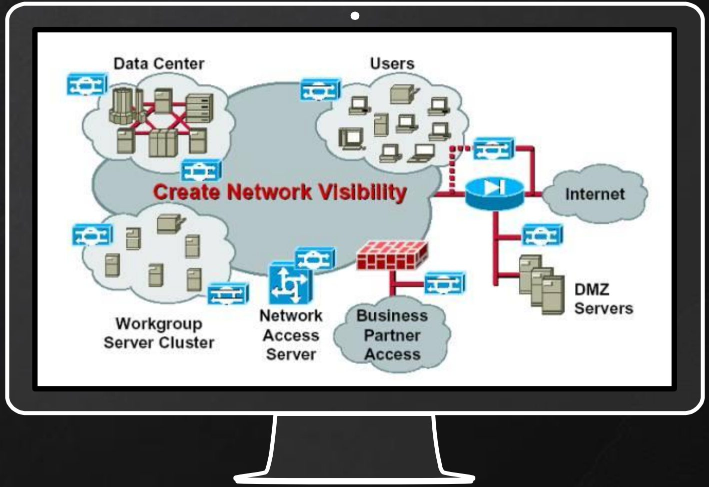


Application Layer Security: Non-Preventable Attacks

- ✓ Password cracking - Implement Strong Password Policies, MFA, Password Hashing and Salting
- ✓ TCP/IP attacks: SYN flood, desynchronization - Firewall, IDS, IPS, TCP/IP Stack Hardening
- ✓ Traffic analysis - Encryption
- ✓ Covert channels - Regular Audits and Monitoring, Network Segmentation, Access Controls

Other Network Security Protection Mechanisms

- ✓ Data Loss Prevention (DLP)
  - ✗ Combination of technology and best practices to prevent the exposure of sensitive information outside of an organization.
  - ✗ Regularly monitor and inspect data leaving organization network
  - ✗ Implement encryption for sensitive data
- ✓ Email Security
  - ✗ Any processes, products and services designed to protect email accounts and email contents from external threats.
  - ✗ Implement anti-phishing solutions, Email Filtering, Enforce strong authentication for email accounts (prevent email spoofing)
- ✓ Sandboxing
  - ✗ A safe, protected and isolated environment in computer system to run or open suspected insecure programs or files.



Key Points

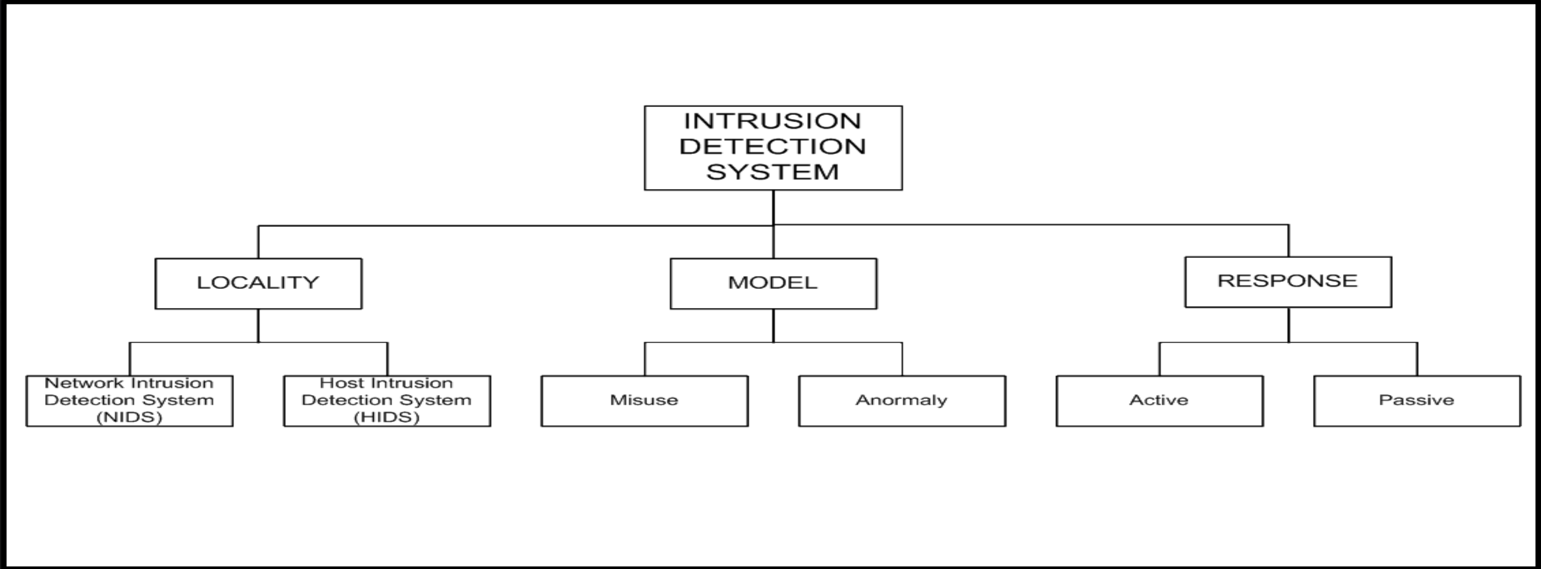
- ✓ Network security technologies can be deployed at all layers of network protocols
- ✓ IP layer security provides a transparent security service; needs, however, infrastructure support
- ✓ Trasport layer security provides a reliable end-to-end security services
- ✓ Application layer security mechanisms can be tailored to specific application needs

CSC662 – COMPUTER SECURITY

062 – INTRUSION DETECTION SYSTEM

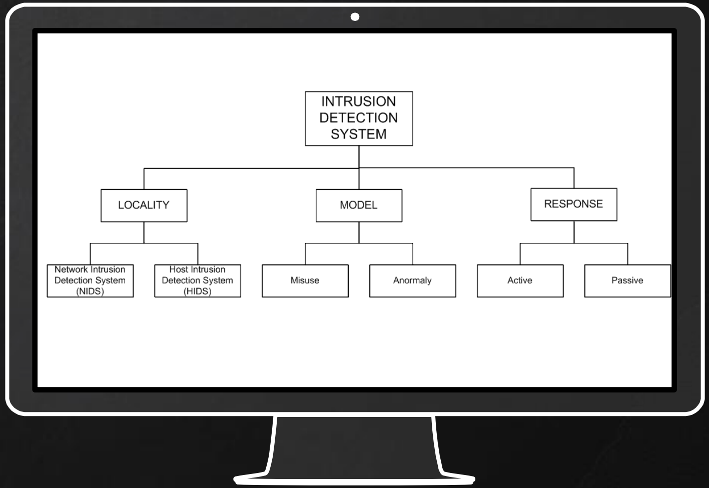
Intrusion Detection System (IDS)

- ✓ Detects malicious activity in computer systems
  - × Identifies and stops attacks in progress
  - × Conducts forensic analysis once attack is over


INTRUSION DETECTION SYSTEM
LOCALITY
MODEL
RESPONSE
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)
Misuse
Anormaly
Active
Passive

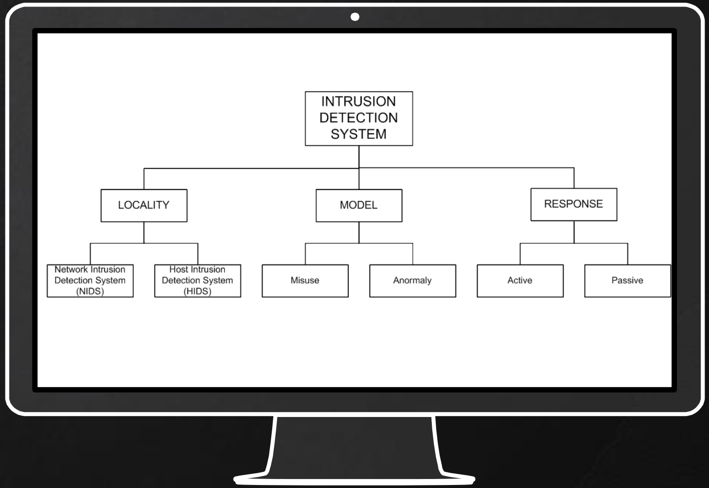
Intrusion Detection System: Values

- ✓ Monitors network resources to detect intrusions and attacks that were not stopped by preventative techniques (firewalls, proxy servers, packet-filtering routers, network segmentations)
- ✓ Expands available options to manage risk from threats and vulnerabilities


INTRUSION DETECTION SYSTEM
LOCALITY
MODEL
RESPONSE
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)
Misuse
Anormaly
Active
Passive

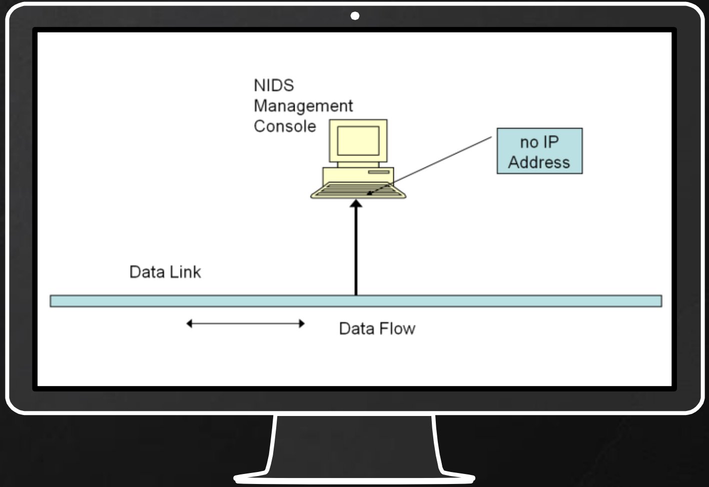
Intrusion Detection System: Types

- Network-based (NIDS)
  - Monitors network traffic
  - Provides early warning system for attacks
  - Uses passive detection
- Host-based (HIDS)
  - Monitors activity on host machine
  - Able to stop compromises while they are in progress
  - Uses active detection


INTRUSION DETECTION SYSTEM
LOCALITY
MODEL
RESPONSE
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)
Misuse
Anormaly
Active
Passive

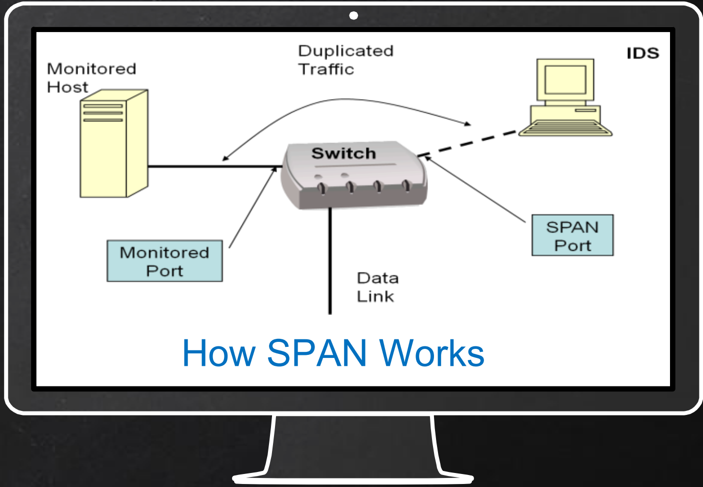
Intrusion Detection System: Network-Based IDS

- ✓ Uses a dedicated platform for purpose of monitoring network activity
- ✓ Analyzes all passing traffic
  - ✕ Sensors have two network connections
  - ✕ One operates in promiscuous mode to sniff passing traffic
  - ✕ An administrative NIC sends data such as alerts to a centralized management system
- ✓ Most commonly employed form of IDS



Network-Based IDS: Monitoring Interface Connection

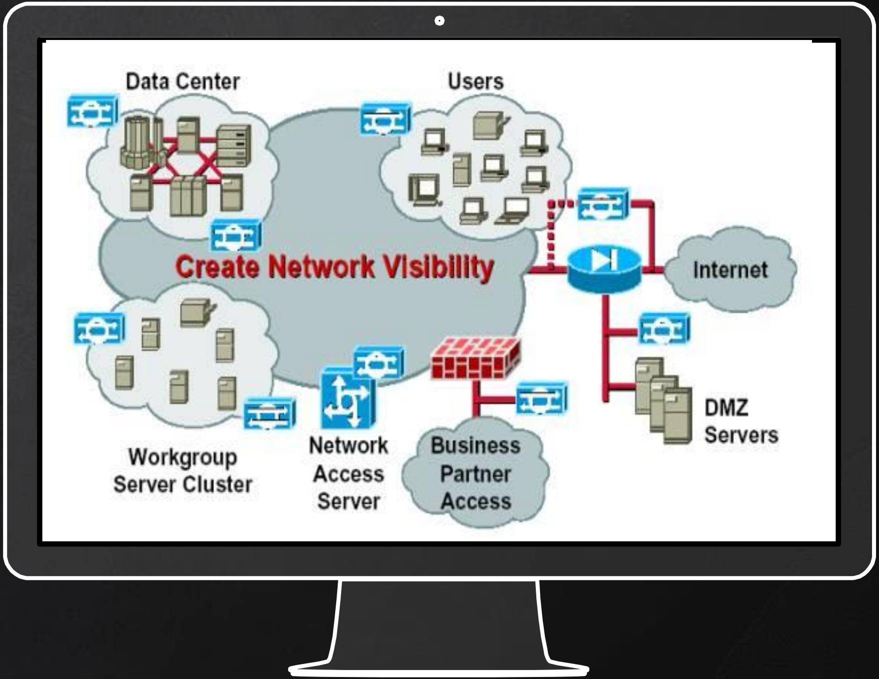
- ✓ Using Switch Port Analyzer (SPAN) configurations – allows the mirroring of traffic from one or more ports to another designated port
  - ✓ NIDS is connected to the port designated for monitoring (SPAN port), where it receives a copy of the traffic passing through the specified ports.
  - ✓ a non-intrusive way to monitor network traffic without requiring additional hardware.
- ✓ Using hubs in conjunction with switches
  - ✓ connecting a hub to a switch port, then connecting the NIDS to the hub, the NIDS can capture a copy of all traffic passing through the connected switch port (passive).
  - ✓ Simple iplementation and cost-effective.
- ✓ Using taps(device) in conjunction with switches
  - ✓ inserted into a network link, and it duplicates the traffic to send a copy to the NIDS for analysis.
  - ✓ non-intrusive way to capture network traffic, passive devices, do not have risk of disruption to the network.



How SPAN Works

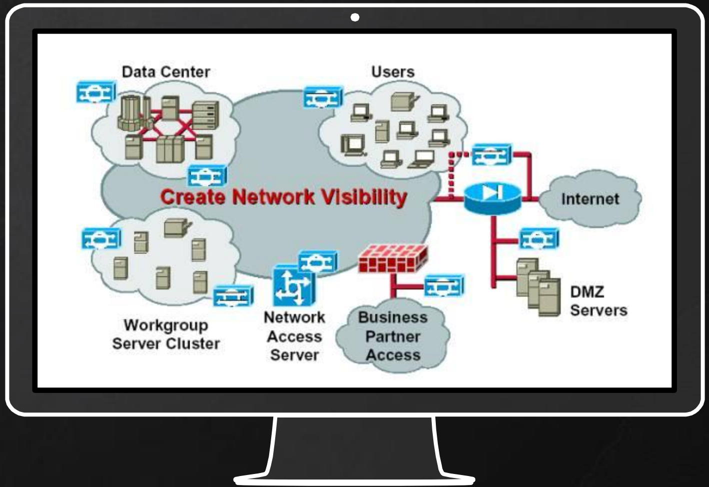
Network-Based IDS: Architecture

- ✓ Place IDS sensors strategically to defend most valuable assets
- ✓ Typical locations of IDS sensors
  - ✓ Just inside the firewall – 1st line of defense
  - ✓ On the DMZ
  - ✓ On the server farm segment
  - ✓ On network segments connecting mainframe or midrange hosts



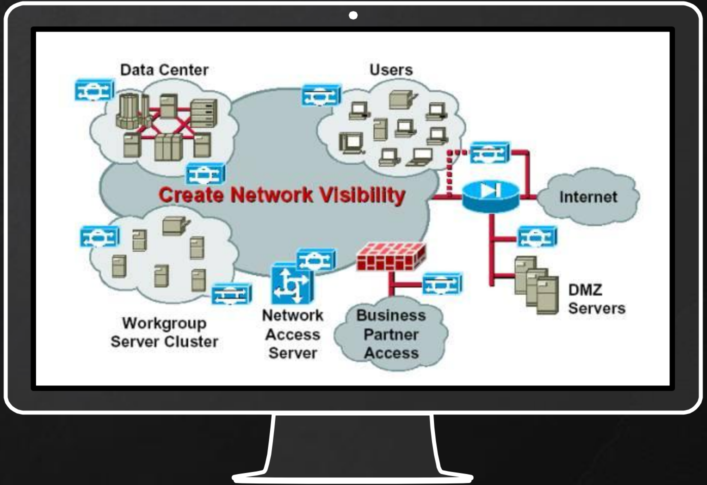
Network-Based IDS: Strengths

- ✓ Cost of Ownership
  - ✗ Lower because IDS is shared
- ✓ Packet Analysis
  - ✗ Can look at all network traffic
- ✓ Evidence Removal (Integrity)
  - ✗ Packets are captured in a separate machine
  - ✗ Prevent tampering or alteration of evidence in the event of a security incident.
- ✓ Real-Time Detection and Response
  - ✗ Can detect (and block) DDoS attacks
- ✓ Operating System Independence
  - ✓ to monitor and analyze traffic regardless of the operating systems used on the network.



Network-Based IDS: Limitations

- ✓ Traffic between hosts on the same segment is not monitored; only traffic entering or leaving the segment crosses the monitored link.
  - ✓ Communication that stays within the segment might not be visible to the NIDS, potentially leading to blind spots in monitoring.
- ✓ Switch may offer limited number of SPAN ports or none at all.
  - ✓ it limits the ability to monitor multiple segments simultaneously



Intrusion Detection System: Host-Based IDS

- ✓ Primarily used to protect only critical servers
- ✓ Software agent resides on the protected system
- ✓ Detects intrusions by analyzing logs of operating systems and applications, resource utilization, and other system activity
- ✓ Use of resources can have impact on system performance

Intrusion Detection System: Types Of Software

- ✓ Host wrappers
  - × Inexpensive and deployable on all machines
  - × Do not provide in-depth, active monitoring measures of agent-based HIDS products
  - × Suitable for environments where a basic level of intrusion detection is needed, and budget constraints are a consideration.
- ✓ Agent-based software
  - × More suited for single purpose servers such as web servers or database servers, where targeted monitoring and protection are critical.
  - × These agents can provide more detailed insights into the security status and activities on the host.

Intrusion Detection System: Methods Of Operation

- ✓ Auditing logs (system logs, event logs, security logs, system log) - to identify patterns or anomalies indicative of security incidents.
- ✓ Monitoring file checksums to identify changes - to monitor the integrity of files. Changes in file checksums can indicate alterations or unauthorized modifications.
- ✓ Elementary network-based signature techniques including port activity - analyzes network traffic and looks for patterns or signatures associated with known attacks.
- ✓ Intercepting and evaluating requests by applications for system resources before they are processed - IDS may intercept and analyze application requests for system resources before they are executed or processed.
- ✓ Monitoring of system processes for suspicious activity - o identify patterns or activities indicative of security threats.

Intrusion Detection System: Active Capabilities

- ✓ Log the event - provides a record of the incident for forensic analysis, compliance, and auditing purposes.
- ✓ Alert the administrator - generates an alert to notify administrators in real-time, allowing for immediate investigation and response to the security incident.
- ✓ Terminate the user login - Halting a potentially malicious user's activities in real-time to prevent further unauthorized access or actions on the system.
- ✓ Disable the user account - Disabling the user account prevents the user from accessing the system entirely and contains the potential threat.

Intrusion Detection System: Strengths

- ✓ Verifies success or failure of attack by reviewing HIDS log entries
- ✓ Monitors use and system specific activities; useful in forensic analysis of the attack
- ✓ Can monitor network encrypted traffic
- ✓ Near real-time detection and response
  - × Analysis is log based, but good design mitigates much of the delay.
- ✓ Can focus on key system components
- ✓ No additional hardware

Intrusion Detection System: Limitation

- ✓ Host’s performance might downgrade as HIDS uses its computing resources such as CPU rsources, memory, and disk I/O.

IDS Detection Models

- ✓ Misuse/Signature detection - recognize known attacks
  - ✗ Define a set of attack signatures
  - ✗ Detect actions that match a signature
  - ✗ Add new signatures often
  - ✗ Examples: ARMD, ASIM, Bro, CSM, Cyber Cop, GRIDS, Stalker, Tripwire
- ✓ Anomaly detection - recognize atypical behavior
  - ✗ Define a set of metrics for the system
  - ✗ Build a statistical model for those metrics during “normal” operation
  - ✗ Detect when metrics differ significantly from normal
  - ✗ Examples: AAFID, MIDAS, NADIR, UNICORN

IDS Detection Models: Misuse

- ✓ The concept behind the Misuse Detection Systems (MDSs) is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected.
- ✓ They can detect many or all known attack patterns, but they are of little use for unknown attack methods.
- ✓ MDSs try to recognize known “bad” behavior.

Misuse Detection System: Expert Systems

- ✓ Designed to mimic the decision-making abilities of a human expert in a particular field. In the context of intrusion detection, expert systems can be used to encode knowledge about known attack scenarios and patterns.
- ✓ These are modelled in such a way as to separate the rule matching phase from the action phase. Ex: NIDES developed by SRI.
- ✓ NIDES follows a hybrid ID technique.
- ✓ It builds user profiles based on many different criteria.
- ✓ The expert system misused detection component encodes known scenarios and attack patterns

Misuse Detection System: Key Stroke Monitoring

- ✓ Key Stroke Monitoring: This is a very simple technique that monitors keystrokes for attack patterns.
- ✓ Features of shells in which user definable aliases are present, certain features can defeat the technique unless alias expansion and semantic analysis of commands is taken up.
- ✓ Operating systems do not offer much support for keystroke capturing, so the keystroke monitor should have a hook that analyses keystrokes before sending them to their intended receiver.
- ✓ An improvement would be to monitor system calls by application programs as well.

Misuse Detection System: Model Based

- ✓ This states that certain scenarios are derived by certain other observable activities.
- ✓ The model-based scheme consists of three important modules
- ✓ The **anticipator** uses the active models and the scenario models to try to predict the next step in the scenario that is expected to occur (prediction).
- ✓ The **planner** then translates this hypothesis into a format that shows the behaviour as it would occur in the audit trail (record of system activities and events.
- ✓ The **interpreter** then searches for this data in the audit trail. It compares the expected behavior, generated by the planner, with the actual recorded activities in the audit trail.
- ✓ The system proceeds in this way, accumulating more and more evidence for an intrusion attempt until a threshold is crossed.

Misuse Detection System: State Transition Analysis

- ✓ The monitored system is presented as a state transition diagram.
- ✓ As data is analyzed, the system makes transitions from one state to another.
- ✓ A transition takes place on some Boolean condition being true.
- ✓ Drawbacks
  - ✕ Attack patterns can specify only a sequence of events, rather than more complex forms.
  - ✕ There are no general-purpose methods to prune(eliminate) the search except through the assertion primitives.
  - ✕ They can't detect denial of service attacks.

Misuse Detection System: Pattern Matching

- ✓ This model encodes known intrusion signatures as patterns that are then matched against the audit data.
- ✓ The implementation makes transitions on certain events called labels, and Boolean variables called guards can be placed at each transition.
- ✓ Advantages
  - ✕ Declarative Specification - expressing what needs to be achieved rather than prescribing how to achieve it.
  - ✕ Multiple event streams - Handling multiple event streams allows for a more comprehensive analysis of system activities.
  - ✕ Portability - can be applied across various types of systems without major modifications.
  - ✕ Real-time capabilities - it can analyze and respond to events in near real-time.

IDS Detection Models: Anomaly

- ✓ Anomaly detection systems (ADSs) assume that all intrusive activities are necessarily anomalous.
- ✓ Anomalous activities that are not intrusive are flagged as intrusive.
- ✓ Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are)
- ✓ ADSs are also **computationally expensive** because of the overhead of keeping track of, and possibly updating several system profile metrics.

Anomaly Detection System: Statistical

- ✓ Behaviour profiles for subjects are generated.
- ✓ The anomaly detector constantly generates the variance of the present profile from the original one.
- ✓ They adaptively learn the behaviour of users.
- ✓ Potentially more sensitive than humans.
- ✓ Disadvantages
  - ✗ They can gradually be trained by intruders so that eventually, intrusive events are considered normal.
  - ✗ It is not known exactly what the subset of all possible measures that accurately predicts intrusive activities is.

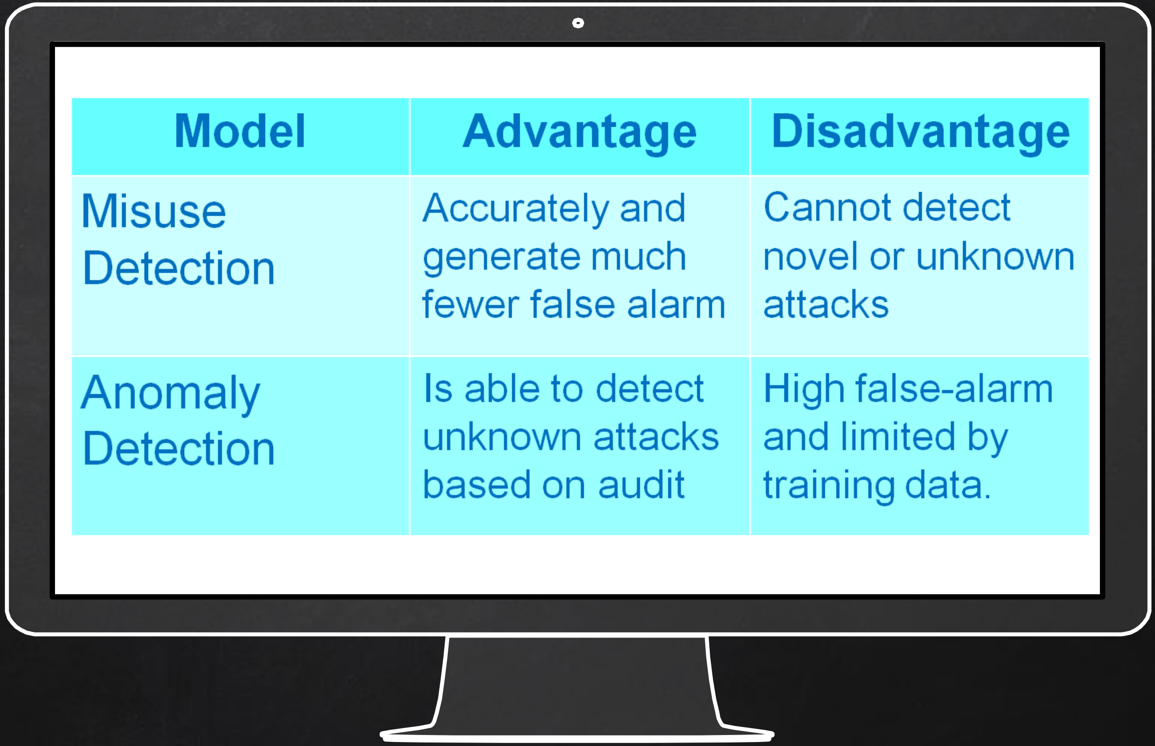
Anomaly Detection System: Predictive Pattern

- ✓ This method tries to predict future events based on the events that have already occurred. We could have a rule
  - ✗ E1 → E2 → (E3 = 80%, E4 =15%, E5 = 5%)
- ✓ The problem is that some intrusion scenarios that are not described by the rules will not be flagged intrusive.
- ✓ Advantages:
  - ✗ Rule based sequential patterns can detect anomalous activities that were difficult with traditional methods.
  - ✗ Systems built using this model are highly adaptive to changes.
  - ✗ It is easier to detect users who try to train the system during its learning period.
  - ✗ Anomalous activities can be detected and reported within seconds of receive audit events.

Anomaly Detection System: Neural Networks

- ✓ The ideas here is to train neural network to predict a user’s next action or command, given the window of *n* previous actions.
- ✓ Advantages
  - ✕ They cope with noisy data (errors, inconsistencies, or irrelevant information)
  - ✕ Their success does not depend on any statistical assumption about the nature of the underlying data
  - ✕ They are easier to modify for new user communities
- ✓ Disadvantages
  - ✕ A small window will result in false positives, a large window will result in irrelevant data as well as increase the chance of false negatives.
  - ✕ The net topology is only determined after considerable trail and error.
  - ✕ The intruder can train the net during its learning phase.

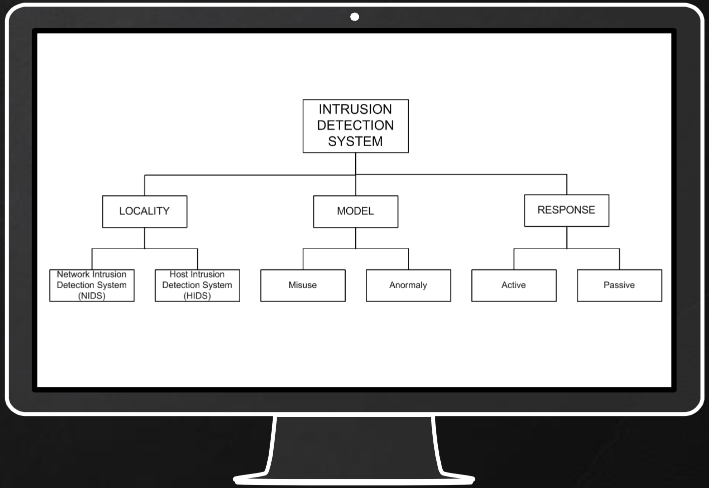
Misuse Detection vs Anomaly Detection



Model	Advantage	Disadvantage
Misuse Detection	Accurately and generate much fewer false alarm	Cannot detect novel or unknown attacks
Anomaly Detection	Is able to detect unknown attacks based on audit	High false-alarm and limited by training data.

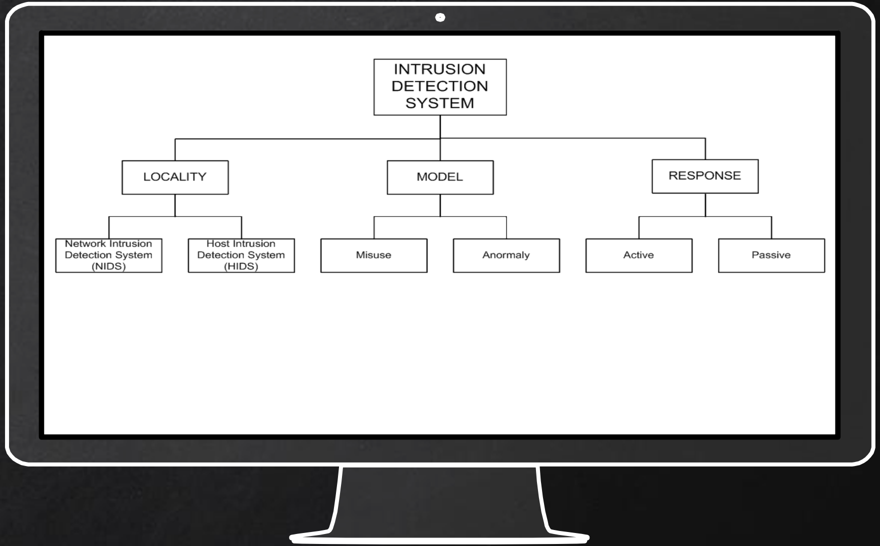
Active Detection Systems

- Have logging, alerting, and recording features of passive IDS, with additional ability to take action against offending traffic
- Options
  - IDS shunning or blocking
  - TCP reset
- Used in networks where IDS administrator has carefully tuned the sensor’s behaviour to minimize number of false positive alarms

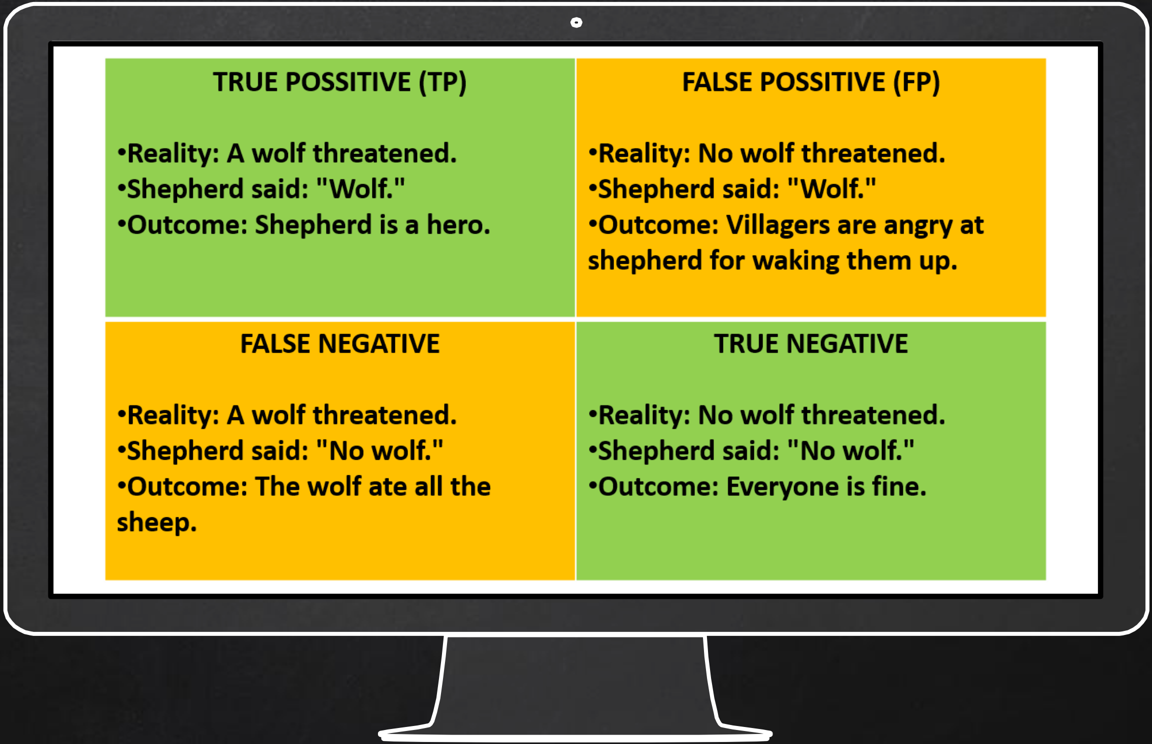

INTRUSION DETECTION SYSTEM
LOCALITY
MODEL
RESPONSE
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)
Misuse
Anormaly
Active
Passive

Passive Detection Systems

- ✓ Can take passive action (logging and alerting) when an attack is identified
- ✓ Cannot take active actions to stop an attack in progress


INTRUSION DETECTION SYSTEM
LOCALITY
MODEL
RESPONSE
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)
Misuse
Anormaly
Active
Passive

Detection Classifications



TRUE POSSITIVE (TP) •Reality: A wolf threatened. •Shepherd said: "Wolf." •Outcome: Shepherd is a hero.	**FALSE POSSITIVE (FP)** •Reality: No wolf threatened. •Shepherd said: "Wolf." •Outcome: Villagers are angry at shepherd for waking them up.
FALSE NEGATIVE •Reality: A wolf threatened. •Shepherd said: "No wolf." •Outcome: The wolf ate all the sheep.	**TRUE NEGATIVE** •Reality: No wolf threatened. •Shepherd said: "No wolf." •Outcome: Everyone is fine.

Detection Results

- ✓ IDS **correctly** identify intrusions and attacks
  - × True positives
  - × True negatives
- ✓ IDS **incorrectly** identify intrusions and attacks
  - × False positives
    - Legitimate activity reported as malicious
  - × False negatives
    - IDS missed an attack

Dealing With False Detection Results

- ✓ False positives
  - × Reduce number using the tuning process
- ✓ False negatives
  - × Obtain more coverage by using a combination of network-based and host-based IDS
  - × Deploy NIDS at multiple strategic locations in the network
  - × Update intrusion pattern/signature of the HIDS

thanks!

Any questions?

You can find me at
wanya@uitm.edu.my