Theoretical Models {Lecture 24}

* A theoretical model can aid in achieving a fool proof security system.

Multi-level security

* A structure where information or assets are defined or classified in multiple categories e.g Top secret, secret, confidential, restricted, unclassified in military organizations.

Bell LaPadula (BLP) Model

* Keeps data confidential (main goal)
* designed for multi-level security environments
* The simple security property probibits people from reading information above their clearance level. (No read up)

Date: _____

* The * security property prohibits people from writing information below their clearance level. (NO write down)

Biba integrity Model

* keeps data integrity safe (main goal)
* designed for multi-level security environments.
* The simple integrity property prohibits people from reading information below their clearance level
  ↳ (NO read down)
* The * integrity property prohibits people from writing information above their clearance level
  ↳ (No write up)

In slides:

Simple integrity: modify only if: $I(S) \geq I(O)$

Integrity confinement: read only if: $I(S) \leq I(O)$

Invocation property: invoke only if: $I(S_1) \geq I(S_2)$

Clark-Wilson Integrity model

* built upon principles of change control rather than integrity levels.
* No changes by unauthorized subjects.
* No unauthorized changes by authorized subjects.

Date: _____

* maintain internal and external consistency
* well-formed transactions: a user can modify data only in constrained ways
* seperation of duty: one can create a transaction but not execute it.
* Main Components:
  → USERS → CDI (constrained Data Items) → whose integrity should be preserved
  → UDI (un-constrained Items) → IVPs (Integrity verification procedures) → TPs (transaction Procedures) → that change CDIs
* Certification & Enforcement of Rules
  These rules ensure integrity of data items
  → Certification is performed by a security officer
  → Enforcement is done by the system

C1 : IVPs must ensure that all CDIs are in valid state
C2: All TPs must be certified (all CDIs involved must be valid)
E1: The system must maintain a list of relations in C2.
E2: The system must maintain a list of allowed (users, TP_i, CDIs) combinations. i.e access tuples.
(more on slides)

Date: _____

* The Chinese Wall Model (Brewer & Nash Model)

→ Addresses the **Conflict of Interest** problem

→ **Model Elements** : * **subjects** : active entities interested in accessing protected objects

* **information** : objects, datasets, CI class

* **access rules** : rules for reading/writing data

→ **Rules** : S = subject, O = object, CI = conflict of Interest (DS = dataset)

* **simple Security Rule** : S can read O if O is in same DS as an object already accessed by S OR O belongs to new CI

* ***-property rule** : S can write O only if S can read O AND all objects that S can read are in same DS as O.

Difference blw CW & BLP

* CW is based on access history

* BLP is history-less

Date: _____

Intrusion Detection (Lec 23)

* intrusion: break into a system
* intruders may be outside or inside system
* every intrusion is called an incident

Types of Intruders

* Masquerader: unauthorized outsider gaining access to authorized user account
* Misfeasor: inside legitimate user who exploit access or accesses unauthorized information
* Clandestine user: a user who invades supervisory control & uses it to evade auditing and access controls.

Intrusion Detection System (IDS)

* A security service that monitor & analyzes system events in real-time to warn for intrusions.
* IDS look for attack signatures
* IDS components: * Sensors * Analysers * User Interface

IDS Analysis Approaches

* Anomaly Based Detection
* Signature Based Detection

Anomaly Based Detection

* train models on large data collected of

Date: _____

legitimate user's behaviour, to detect otherwise.

* primary strength: detects novel attacks
* but could generate many false alarms and thus reduce their effectiveness. ~~* signature etc~~

Signature Based Detection

* it looks at sensor data to detect already known intruder attack patterns (signatures)
* new attack patterns must continually be added
* simply matches patterns with signature database i.e rule-based heuristic identification.
  → ① analyze historical audit records and define rules
  ② observe current data & match rules
* rules/signature database

Host-based IDS

* monitors activities on a single host
* watch host OS or application logs
* audit includes info like identification & authentication mechanisms, file opens & program executions, admin.
* Drawbacks: → info needed to log comes from (past) experience.
  → unselective logging: store everything (normal & sus logs) uses too much storage
  → selective logging: store only sus logs (risk of undetected attack)

Date: _____

* strengths: → detects internal & external intrusions
→ works even when network traffic is encrypted
→ monitors key components → system specific activity
→ near-real-time detection → no extra hardware.

Network Based Detection

* Monitors traffic at certain points in network
* examines each packet to detect intrusion patterns
* a filter is applied to discard or pass packets on attack recognition module.
* strengths: → less cost of ownership → packet analysis
→ real-time → mal-intent detection → OS independence

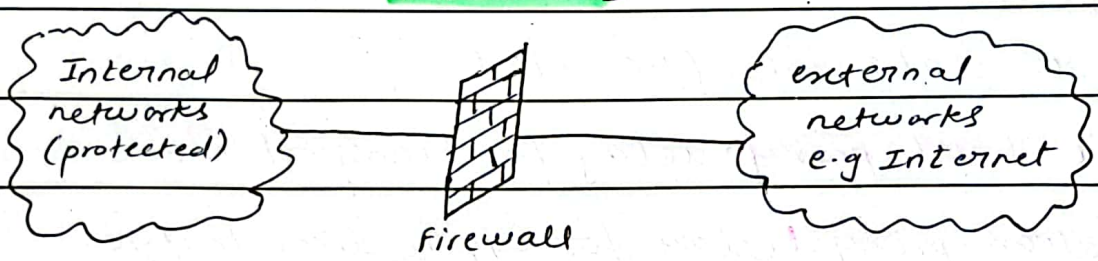
Honeypots

* Decoy system designed to lure attackers away from actual critical systems.
* purpose: → divert attacker away → collect signatures
→ detect new threats → engage attacker on system untill admin responds.
* Decoy Files: a marker, on read/write sends alert, used to give wrong info
* Honey Net: collection of 2 or more decoys
* Interaction level: capability to mimic a real asset
→ High → Low → Medium

Date: _____

* Deception Technology: proactive cyber defense system using decoys. → uses AI generated traps
→ immediate alerts

Firewalls



* insulates internal networks
* single point of protection for LANs
* Goals:
  → all traffic must pass through firewall (both directions)
  → only authorized traffic wrt Local policy allowed to pass
  → firewall is immune to penetration
* Policies:
  → service control e.g filters for IP & ports
  → direction control e.g internal LAN or to external internet
  → user control e.g student vs faculty
  → behaviour control e.g filter frequent requests, spams etc.
* can act as NAT, VPN endpoint
* implemented on a router

Date: _____

* Types of Firewalls :

* Packet Filtering: accepts/rejects packet based on Layer 3/4 packet headers

* Stateful packet inspection: like packet filtering but considers state info (i.e what happend previously)

* Circuit level proxy: relay for transport connections

* Application proxy: relay for application traffic

Packet Filtering

* rule sets

* default policy : Allow, Reject ← recommended

default policy applies to those packets that donot match.

* packet info includes : IP, port, protocol, direction etc.

* Rules: conditions to match packet info, wildcards, accept/drop.

* Advantages: simple, speedy, transparent

* Disadvantages: cannot prevent app specific attacks, limited logging, doesn't support advanced user authentication, can't prevent IP spoofing

Stateful Packet Inspection

* considers past packets as well.

* same as packet filtering besides state

* packets arriving that belong to an existing

Date: _____

approved connection are accepted.

* connections are accepted by packet filtering firewall
* records connection info : src/dest IP, src/dest port, seq #, connection state (new, estab, close)

Circuit-level Proxy

* circuit-level gateway
* acts as a relay (intermediary server)
* sets up 2 TCP connections: 1 with internal host and 1 with external host
  → For incomming data : acts as server
  → For outgoing data : acts as client
* relays TCP segments without examining contents
* security function : determine which connection to allow
* any external data that is requested by internal users is allowed else if no requested, connection blocked.

Application-level Proxy

* application level gateway
* inspects app-level operation (HTTP response content, email content) & allows/denies based of predefined rules.
* logs attempted access & allowed access events

Date: _____

* maintains separate connections with internal and external hosts. (same as circuit-level proxy)
* mostly used as proxy

Firewall Location

* Located on host or network devices e.g end-user computers & or routers etc.
* separate network into 2 zones:
  ① public-facing zone e.g web, email, DNS etc
  ② End-user computers & internal servers e.g DBs
* public-facing is de-militarized zone (DMZ)

Security in TCP/IP (Lec 21-22)

* implementation options: Channel Security, Message Security

Channel Security

* transport layer security - TLS/SSL
* channel security assures that the communication channel between two devices is secure.
* Commonly used protocol for channel security are:
  → Secure Sockets Layer (SSL) (predecessor of TLS)
  → Transport Layer Security (TLS)
  → key features: Encryption, Data Integrity, Authentication,

Date: _____

Forward Secrecy, secure hand-shakes.

message Security

* end-to-end security
* secures the content of messages or data packets sent over a network
* ensures confidentiality, integrity and authenticity.
* key features: Encryption, Data Integrity, Authentication

Security Internal to Applications

* focuses on safeguarding softwares themselves i.e code, data etc.
* implement security features within the app design

Security External to applications

* focuses on securing the environment in which the softweres / apps execute.
* protects systems, networks & resources

Date: _____

SSL / TLS

* **SSL**: secure sockets layer
* implemented between Layer 4 & Layer 5
* above Transport Layer
* SSL / TLS Protocol Stack:

SSL	SSL handshake protocol	SSL change cipher spec protocol	SSL alert protocol	application protocol HTTP
	SSL record protocol			
TL	reliable transport protocol (TCP)			
NL	network protocol (IP)			

* **Handshake**: exchange cipher algo and secret keys.
* **change cipher spec**: indicates usage of secret key
* **Alert**: signal problem with SSL connection, give status
* **Record**: securely carries data to higher layers.

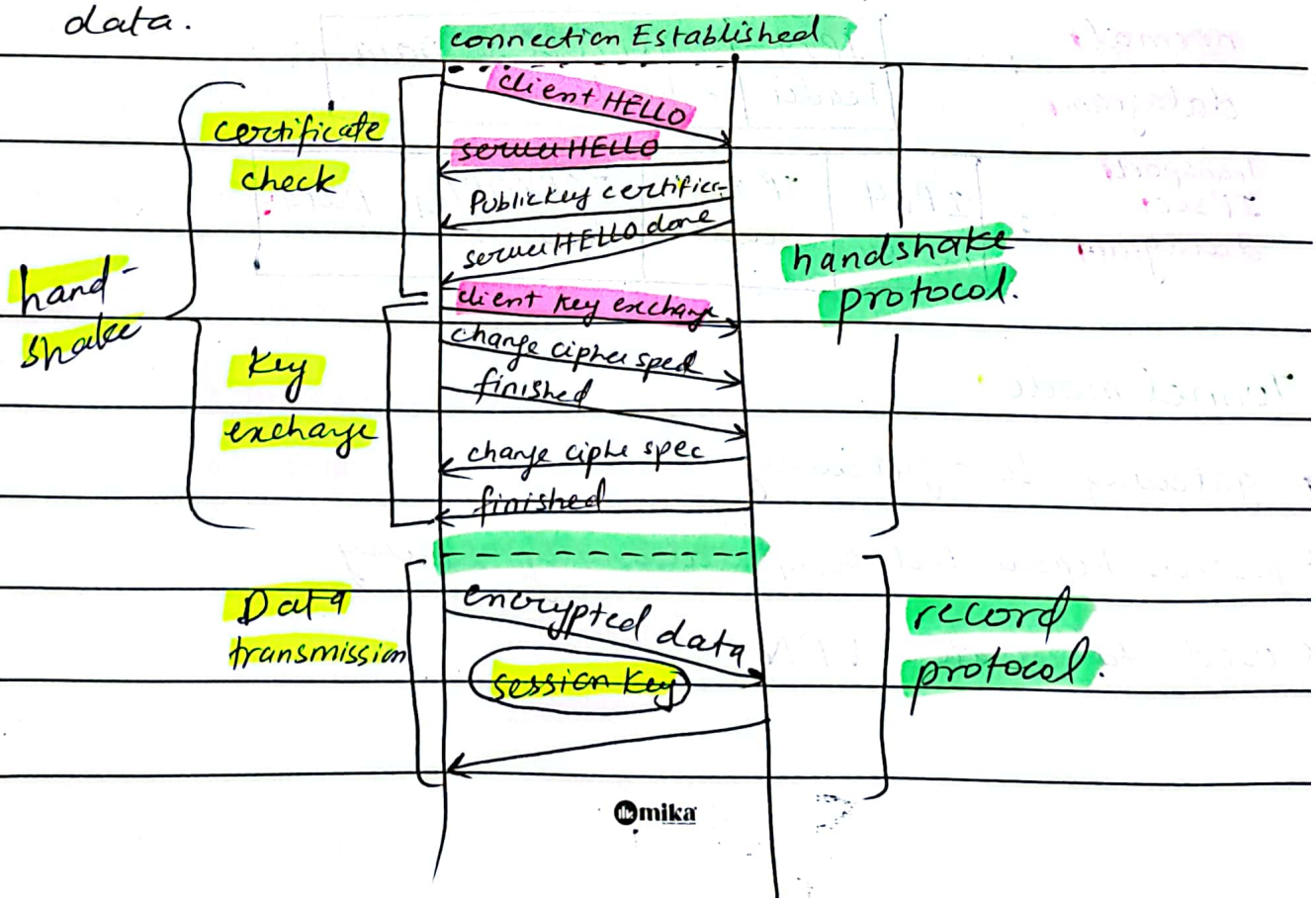
Handshake:

* after TCP ESTAB
* **client Hello**: ① TLS version client supports } sent options by client
  ② what cyphers client supports
* **server Hello**: ① choose one TLS version } selected options by server.
  ② chooses cypher algo
* server sends its **certificate & public key**
* client verifies the certificate authenticity

Date: _____

* Lastly server sends Hello Done ~~which marks the end of TLS/SSL handshake~~.

* Now, Key exchange takes place
* client sends a session key (symmetric key) by encrypting it using public key of server.
* after both server & client have generated/ received the same symmetric key the cipher-spec exchange takes place.
* the client sends its cipher spec
* the server sends its cipher spec
* both send finished message.
* now record protocol is used to exchange data.



Date: _____

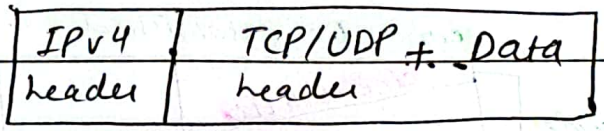
IP sec : Internet Protocol Security

* security at layer 3
* IPsec ensures CIA
* network layer security
* with in OS
* above link layer.
* IPsec operating modes :
  1. secure virtual channel (tunnel-mode SA)
  2. secure virtual channel (transport-mode SA)

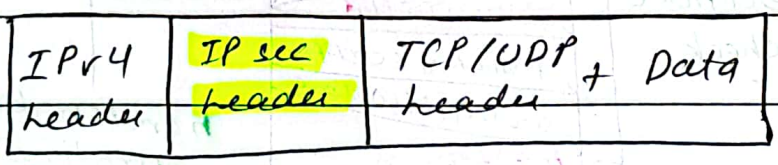
Transport mode :

* end-to-end security, used by hosts
* computationally light but no protection of headers

normal datagram :



Transport IPsec datagram :



Tunnel mode :

* gateway-to-gateway
* protects header but computationally heavy
* used to create VPN.

Date: _____

normal datagram :

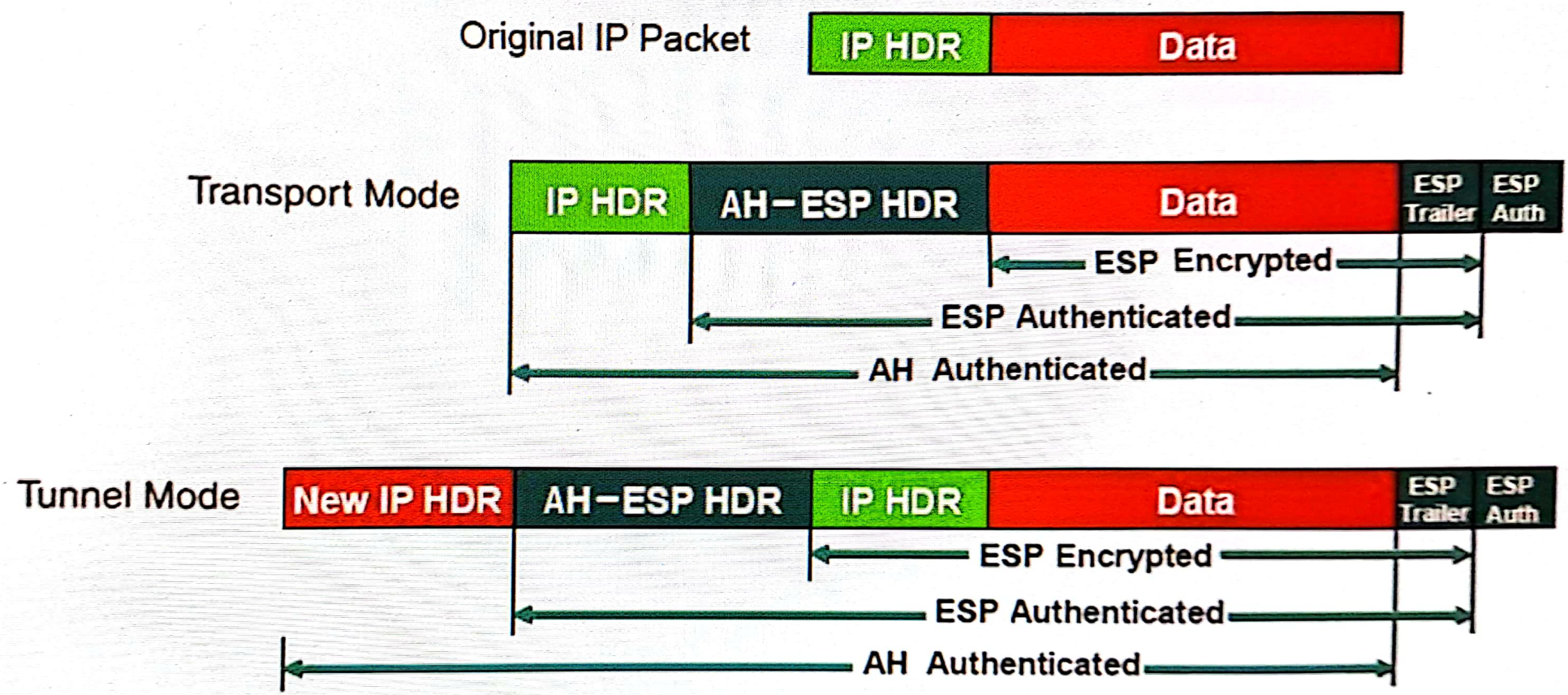
IPv4 header (end-to-end)	TCP/UDP header + data

Tunnel IPsec datagram :

IPv4 header (tunnel)	IPv4 header (end-to-end)	TCP/UDP header + data

IPv4 header (tunnel)	IPsec header	IPv4 header (e2e)	TCP/UDP header + data

* packet types
  1. AH (authentication header) ← protects the headers
  2. ESP (encapsulating security payload) ← protects the payload
* protocol for key exchange:
  → IKE (Internet Key Exchange)
* IPsec local databases
  → SAD (security associations database)
  → SPD (security policies database)
* check last slide of lec 21-22 for ESP, AH diagram


Original IP Packet
IP HDR
Data
Transport Mode
IP HDR
AH–ESP HDR
Data
ESP Trailer
ESP Auth
ESP Encrypted
ESP Authenticated
AH Authenticated
Tunnel Mode
New IP HDR
AH–ESP HDR
IP HDR
Data
ESP Trailer
ESP Auth
ESP Encrypted
ESP Authenticated
AH Authenticated