Web Security — Security Architecture / Part 2

(1)

Confidentiality : Make sure that IT services and resources are only available to accredited entities.
ex : transport level encryption, disk encryption

Integrity : Make sure that the information as well as information processing is exact, reliable, trusted, provable. ex : MAC (Message Authentication Code), Signature

Availability : Make sure that IT services and resources are available for accredited users.
ex : Redundancy, Load balancing

Traceability : garantir que les accès ou tentative d'accès aux éléments considérés sont tracés (conservée ↑ exploitable)
Non repudiation : keeping track of events for auditing.
Authorization : def & enforcement of access control to ressources and informat°
Authentication : process of verifying the identity of an entity.
Identification : process of determining the identity of an entity.

→ = **Authenticity** = Authentication + integrity
simple authentication : 1 factor
strong authentication : 2 factors or more
single authentication : one factor ← the one we prefer
Application layer : HTTP, FTP, RDP
Transport Layer : TLS, SSH
Network Layer : IPSec
Link Layer : PAP, CHAP, PPPoE

(2) principles → other paper

(3) / threat Landscape

Vulnerability : failure or Deviation of the information systems weakness that could be used to endanger or cause Harm to an informational asset.
→ eventually known and documented
→ can eventually be exploited
Main reasons or root cause : Design / Implementation / Operation

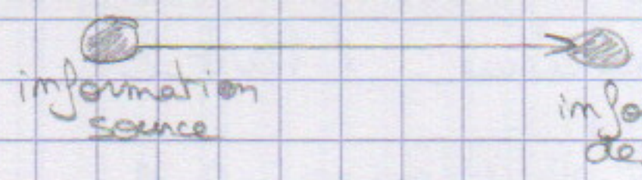
▽ ↑ more vulnerabilities on applications layer.

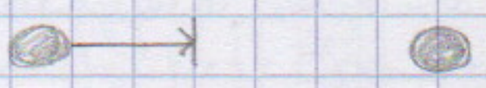
OWASP TOP 10 — Open Web Application Security Project

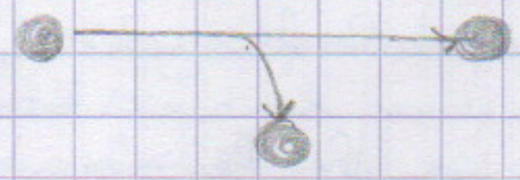
Broken Access Control : utilisateurs non autorisés peuvent accéder à des données ou à des fonctions qu'ils ne devraient pas pouvoir atteindre
Cryptographic failure : problèmes liés à la protection des données sensibles → chiffrement inadéquat ou inexistant
Injection flaws : attaquants insèrent du code malveillant dans une appli° (via champs utilisateur) SQL, NoSQL, LDAP
Insecure design : failles dans l'architecture ou la conception d'une application.
Security Misconfiguration : configurations mal sécurisées → permissions incorrectes / fonction inutile/active
Vulnerable & Outdated Components : utilisation de library, framework avec des vulnérabilités connues.
Identification and Authentication failures : Mauvaise gestion des sessions / authentification utilisateur
Software & data integrity failures : manipulation non securisée des mise à jour
Security Logging and monitoring failures : absence de surveillance des logs
Server-side request forgery : appli envoie des requetes non securisées

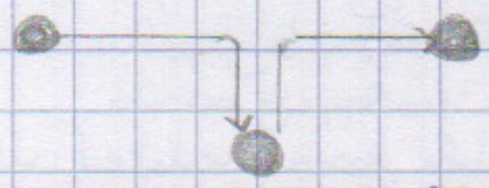
Vulnerability impact classification.
spoofing : usurpation of a legitimate user credential
tampering : alteration (modification or destruction) of data or system
repudiation : unability to prove that an action has been performed
information disclosure : leak of information (data, or system configuration)
denial of service : inability of the system to serve legitimate users
elevation of privilege : gain of additionnal rights allowing the attacker to perform add° action

Taxonomy : Interruption (ex : DoS) - compromises availibility
Interception (ex. MitM) - compromises confidentiality
Modification - compromises integrity
Forging - compromises authenticity

normal flow: 

Interruption: 

Interception: 

Modificat°: 

Fabrication: 

TCP/IP design goals: Interconnection / Interoperability
Fault tolerance and resilience to network outages
Various services (mail, file exchange, terminal access).
Various network technologies
Resource management
Cost / Accountability / Security ? Not really

Vulnerabilities:

ARP Spoofing: Manipulating ARP tables to associate an attacker's MAC address with a legitimate IP, enabling packet interception
IP Spoofing: Forging the source IP address in packets to impersonate another device.

Routing attacks:
Distance Vector Routing: Routing protocol that calculates route based on distance (hop count). Vulnerable to routing table poisoning.
Link state Routing: Routing protocol that builds a full network map to determine the best path. Vulnerable to falsified state updates.
BGP:

ICMP attacks
No authentication: Exploiting the lack of authentication on ICMP to flood or mislead systems
ICMP redirect message: Used to redirect the traffic to another route, exploitable by MitM attack.
ICMP destinat° unreachable: Indicates that a destination is unreachable, can be spoofed to disrupt communication.
ICMP echo request/reply: Used in ping operations to check availibility - abused in ping flood.

TCP layer attacks:
TCP SYN flooding: Overhelms a server by sending numerous SYN requests without completing the handshake.
TCP session hijack. Taking over an active TCP session by injecting packets.
TCP session poisoning: Corrupting TCP session data to disrupt or take control.

Application Layer attacks
Applications don't authenticate properly: Transmitting credentials unencrypted, exposing them to interception.
Authentication information in clear: ↙

DNS insecurity: **DNS poisoning:** Corrupting DNS entries to redirect users to malicious site
DNS zone transfer: extracting DNS record during a misconfigured transfer, revealing internal data.

DoS
TCP SYN floods
ICMP echo (ping) floods: Overhelming a system with ICMP echo request
UDP floods: Sending massive UDP packets
ICMP floods: general flooding of ICMP messages
"Ping of Death": Sending oversized ping packets to crash or destabilize systems.

(4) Cryptography

Symmetric : DES, 3DES, AES, BlowFish
Asymmetric : DH, RSA, El Gamal, ECC
Hashing : MD5, SHA1, SHA-256

Kerckhoff's principle : The only secret involved with a cryptosystem should be the key.

Cryptanalysis attacks:

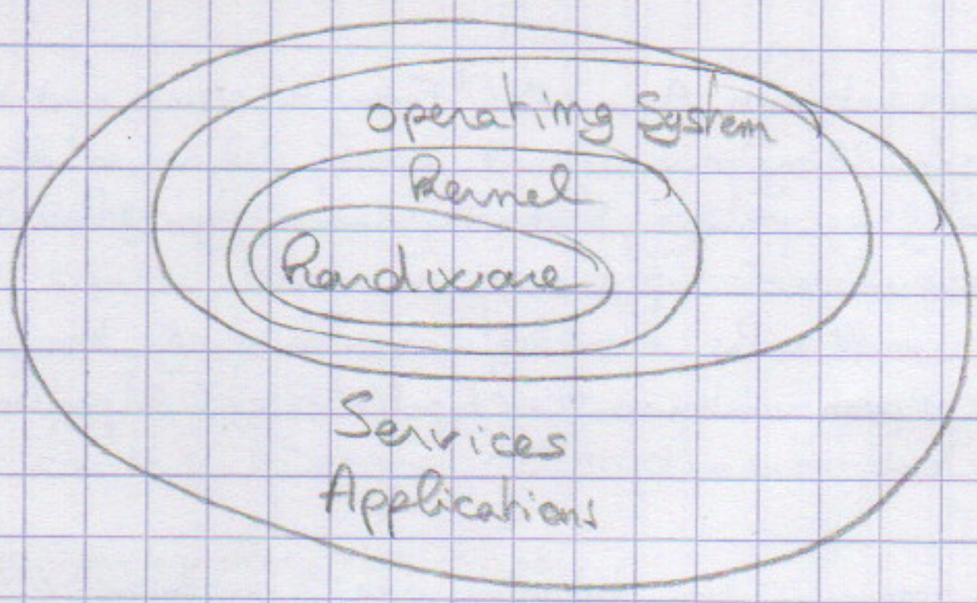
Brute force : Trying all key values in the keyspace
Frequency Analysis : Guess values based on frequency of occurence
Dictionary Attack : find plaintext based on common words.
Replay attack : Repeating previous known values
Factoring attacks : Find keys through prime factorization
Chosen plaintext : Attack can encrypt chosen plaintext.
Chosen ciphertext : Decrypt known ciphertext to discover the key
DFA → side channel attack
Social Engineering : Humans are the weakest link
RNG attack : Predict IV used by an algorithm
Temporary files : may contain plaintext

(5) SDN

(6) OSI : Layer 1 to 7

OSI : Open Systems Interconnection

The onion model



7. Application : Ce avec quoi l'utilisateur interagit — DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, FTP, TELNET
Network process to application
6. Presentation : operating system layer — Recognize data : HTML, DOC, JPEG, MP3, AVI, Sockets
Data representation and encryption
5. Session : Put in place a session between Hosts. — Session establishment in TCP, SIP, RTP
InterHost communication
4. Transport : How much information we communicate — TCP, UDP, SCTP, SSL, TLS
End to end connections and reliability
3. Network : Router (IP Range) — IP, ARP, IPSec, ICMP, IGMP
Path determination and logical addressing
2. Data Link : Switch — Ethernet, 802.11, MAC/LLC, VLAN, ATM
Physical addressing
1. Physical : physical wire — RS-232, RJ45, V.34, 802.11
Media, signal, and binary transmission

Zero Trust Architecture : Security model based on the principle that no entity nor activity should be trusted by default.
Implicit trust is remplaced by strict authN and autorization
→ Any activity and traffic is a threat // Enforce least privileged access // Monitor and log.

OSI

Layer 8 : User / Human

Application Layer

The computers programs which actually do things with the network / "→ deliver the mail, browse the web..."

7 Vulnerabilities : Open design issues allow free use of application resources by unintended parties / Back door and application design flaw bypass standard security controls / Inadequate security controls force "all-or-nothing" approach, resulting in either excessive or insufficient access.

Controls : Application level access controls to define and enforce access to appliadion / Standards, testing and review of applicat° code & functionality : A baseline ← measure & recommend improvements / monitor inquiries

Presentation Layer

Provides commonly used functions for applications / "→ meet I18N standards"

6 Vulnerabilities : Poor handling of unexpected input can lead to application crashes or surrender of control to execute arbitrary instructions / Unintentional or ill-advised use of externally supplied input in control contexts may allow remote manipulation or informat° leakage / Cryptographic flaw may be exploited

Controls : Careful specification and checking of received input (into application or library functions) / Separation of user input and program control function - input should be sanitized

Session Layer

Provides a single connection for one application / "→ am in charge of the entire message"

5 Vulnerabilities : Weak or non-existent authentication mechanisms / Passing of session credentials such as user ID and password in clear / Session identification may be subject to spoofing and hijack / Leakage of information based on failed authentication attempts

Controls : Encrypted password exchange and storage / Accounts have specific expirations for credentials and authorization / Protect session identification information via random/crypto means

Transport Layer

Ensure that data gets between A and B / "From the source and destination, → make sure that the data gets there"

4 Vulnerabilities : Mishandling or undefined, poorly defined, or "illegal" conditions / Diff in transport protocol impl° allow "fingerprinting" and other enumeration of host informat° / Overloading of transport-layer mecanisms such as port numbers

Controls : Strict firewall rules limiting access to specific transmission protocols and sub-protocol informat° such as TCP/UDP port number or ICMP type / Stateful inspection at firewall layer

Network Layer

Provide end-to-end communication between any 2 machines / "→ tried to get a packet to its destination"

3 Vulnerabilities : Route spoofing - propagation of false network topology / IP address spoofing - false source adressing on malicious packets. / Identity & Resource ID vulnerability

Controls : Route policy controls - Use strict anti-spoofing and route filters at network edges / Firewall with strong filter & anti-spoof / ARP / Broadcast monitoring software / Implementations that minimize the ability to abuse protocol features such as broadcast.

Data Link Layer

Provide basic connection between 2 logically connected machines / "→ stuff packets down a wire to my neighbour"

2 Vulnerabilities : MAC address spoofing / VLAN circumvention / Switches may be forced to flood traffic to all VLAN ports.

Controls : MAC address filtering (identifying stations by address and cross referencing physical port or logical port / Do not use VLANs to enforce secure designs.
Tools : anti-arpspoof / Arpon / Antidote / Arpwatch

Physical Layer

Necessary infrastructure // "wires in the ground and connectors" // physical hardware of the network

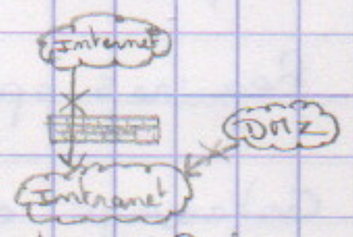
1 Vulnerabilities : Loss of power / Loss of environmental control / Physical Theft of data and Hardware / Physical damage or destruction of Data and Hardware / Unauthorized changes to the functional environment / Disconnection of physical data links / Keystroke / Interference & jamming

Controls : Locked perimeter and enclosures / Electronic lock mecanisms for logging / video & audio surveillance / PIN & password secured locks / Biometric authentication systems / Data Storage cryptography / Electroma. shield

(7) Firewall

Firewall :- System or combinaison of systems that supports an access control policy between 2 networks.
- All network packets entering firewall are filtered, to determine whether or not the network flow or the emitting/receiving Hosts have authority to cross boundaries.
- Firewall can limit types of transactions that enter system/network, as well as types of transactions that leave system/network.
- Can be configured to block certain types or ranges of IP addresses, as well as certain types of TCP port numbers (applications).

DMZ : demilitarized zone ← sous réseau séparé du réseau local et isolé de celui-ci ainsi que d'internet par un pare-feu. Ce sous réseau contient les machines étant susceptibles d'être accedées depuis internet et qui n'ont pas besoin d'accéder au réseau local.



Internal Hosts can access DMZ and internet.
External Hosts can access DMZ only, not intranet.
DMZ Hosts can access internet only
Advantages → if a service gets compromised in DMZ it cannot effect internal Hosts.

Packet filter firewall - essentially router that has been programmed to filter out or allow in certain IP addresses or TCP port numbers.

Proxy server - more advanced firewall that acts as doorman into corporate network. Any external transaction that requests something from corporate network must enter through proxy server
→ more advanced but make external accesses slower.

Packet filtering:
- filter = program that examines source address and destination address of incoming packet to firewall user
- filter tables = lists of addresses whose data packets and embedded messages are either allowed or prohibited from proceeding through the firewall.

Filter tables can limit access of certain IP addresses to certain destination

Packet filter: a set of rules is applied to each incoming IP packets to decide whether it will be forwarded or discarded. The TCP/IP packet is parsed and filtered based on infor° that is usually found in packets Headers:
→ Protocol number / Source & destination IP addresses / Source & destination port numbers / TCP connection flags

Most of packet filters are stateless:
- each TCP/IP connection must be examined independently from what happened in the past.

At the packet level, there is some statefulness: an outgoing connection with source port x opens the port x for incoming packets for the duration of the connection.

Rule: How to know a packet is for SSH ? - inbound: src-port > 1023, dst-port = 22
- outbound: src-port = 22, dst-port > 1023
- Protocol = TCP

Default firewall rules:
- Egress Filtering → Outbound traffic from external addresses → Drop
- Ingress Filtering → Inbound traffic from internal addresses → Drop
- Default Deny

Advantages: transparent to application, user / Simple packet filters can be efficient
Disadvantages: Usually fail open / Very hard to configure the rules / Doesn't have enough info to take action

Alternatives: Stateful packet filters
→ keep the connection states
→ easier to specify rules
→ more popular

packet fragmentation attack:

Pro firewall: Centralized management of security / Can even be stealth / Scalability / Providing auditing, monitoring and recording capabilities / Records // Logs that can ease forensic or incident analysis / Mutualize administration and configuration on PoE rather than the entire network

Con firewall: Network bottleneck / SPOF (Single Point of Failure) / Critical element of security architecture / Complexity: deep knowledge of filtered protocols / Require understanding of firewall feature (interface with other filtering components, address translation ...)

Alternatives: Proxy firewalls: 2 connections instead of one / either at transport level (SOCKS proxy) or at application level (HTTP proxy).
Requires applications (or dynamically linked libraries) to be modified to use the proxy.

Application Gateways ⇔ application level filters
→ port level filter determine legitimacy of party asking for information, applicat° level filters assures validity of what they are asking for.
→ application level filters examine entire request for data rather than source and destination addresses
→ Once legitimacy of request has been established, only proxy clients and severs actually communicate with each other.

Application proxies: enforce policy for specific protocols (ex: virus scanning for SMTP)
→ need to understand MIME, encoding, Zip archives
flexible approach but may introduce network delays
SMTP (E-Mail), DNS (domain name system, NTP (Network Time Protocol), HTTP, ...
Must protect host running protocol stack
→ disable all non-required services ← keep it simple / install // modify services you want / Run Security audit to establish baseline

Proxy server:

Proxy firewall: Data available (application level information / User information)
Advantages (Better policy enforcement / better logging / failed closed)
DisAdvantages (Doesn't perform as well / One proxy for each application / client modification)

A firewall consisting of 2 packet filters and an application gateway.

8) - Hardening

System Hardening: installing kernel / software patches and configuring a system in order to prevent attacker from exploiting and attacking your system.
→ obj: make it difficult to RE and tamper.
Patches / Security tools / System rules and policies
↳ SELinux / AppArmor / grsecurity

Minimize the size of the target: removal of unneeded software packages
define or use predefined qualified profile.

Correct known problems: apply patches to remaining software.

Configure kernel parameters: disable IP forwarding, drop source routed / Protect against SYN floods, Smurf attacks / Drop ICMP redirects, reduce ARP timeouts / Help stop remote network mapping efforts.

other kernel parameters: enable stack protection / Prevent core dump / Set limits on processes.

(8) + Hardening (suite)

Secure the boot process : update the BIOS / configure password protection in BIOS / prevent boot from untrusted sources / Set Boot Loader Password / Enable Authentication for single-User Mode (in etc/inittab) / Disable Interactive HotKey Startup.

DNS Hardening tips : enable bind chroot support or use container / Apply port restrictions in firewall / customize logging as desired / Disable recursive queries on authoritative servers.

Mail Server Hardening tips : chroot postfix (manual process) or container / Ensure unauthorized parties can't relay / establish port restrictions and access control / Anti-virus Anti-spam

Apache Hardening tips : Hide the Apache Version number.

Log Management : detach logs from their device and systems origins / Log at different points / take cover in the cloud.

AutRN considerations : Enable 2-factor authentication when available / check your login history, the list of authorized devices and / or sources.

(9) VPN : ipsec, ssh, tls ← last lecture.

VPN = Virtual Private Networks

3 ≠ modes of use : - Remote access client connections / LAN to LAN interconnecting / controlled access within an intranet.

Several different protocols : PPTP - Point to Point tunneling Protocol
L2TP - Layer 2 tunneling protocol
IPSec - Layer 3 : network

Layer 2 : L2TP and PPTP
Layer 3 : IPSec

Layer 3 : MPLS-Based VPNs
Non-MPLS-Based VPNs (Virtual Routers)
Layer 2 : MPLS VPNs

PPTP : tunneling protocol that allows managers to choose whatever encryption or authentication technology they wish to hang off either end of the established tunnel.

MPLS : forwarding scheme designed to speed up IP packets forwarding.
→ use a fixed length label in the packet header to decide packet forwarding

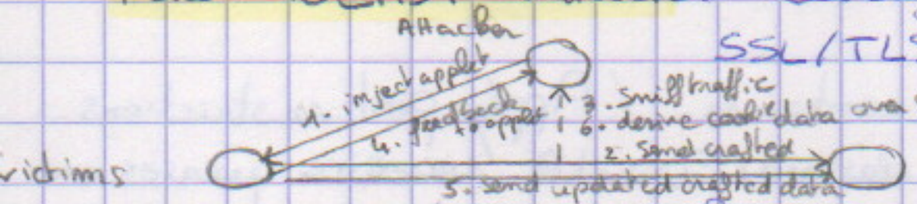
IPSec : IP Security protocol ← Authentication, confidentiality and integrity
use several protocols:
AH : Authentication Header ← authentifie les messages
ESP : Encapsulating Security Payload ← authentifie et crypte les messages.
IKE : Internet Key Exchange
SA : Security Associations

mode transport : les machines source et destination sont les extrémités de la connexion sécurisée.

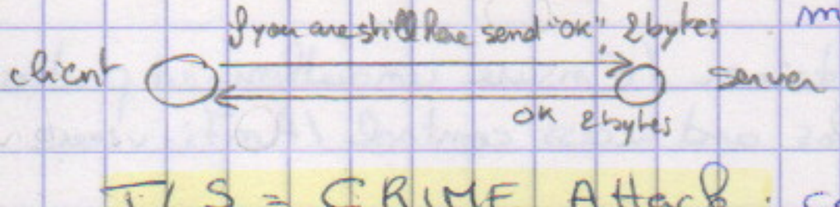
mode tunnel : les extremités de la connexion sécurisée sont des passerelles, les comm° sont encapsulées dans les entêtes de protocole de tunnel.

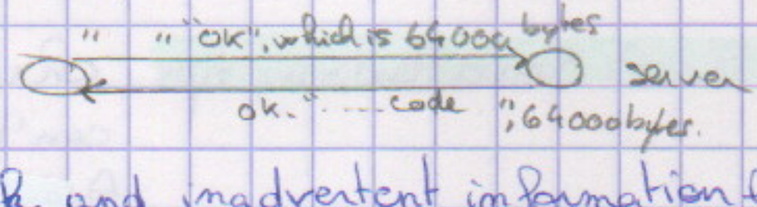
SSL / TLS (by Netscape) (standardized by IETF)
Secure Socket Layer (SSL) / Transport Layer Security (TLS).
SSL v3.1 ~ TLS v1.0 Latest release : TLS v1.3
Repose sur le protocole TCP avec des numéros de ports spécifiques : HTTPS (443), NNTPS (563), LDAPS (636), FTPS (989 ou 990), telnet (992), IMAPS (993) POP3S (995) → principale utilisation = HTTPS
HTTPS = HTTP + SSL

TLS - BEAST attack : Leverages weakness in cipher block chaining (CBC) to exploit SSL/TLS and allow MitM attacks against SSL.

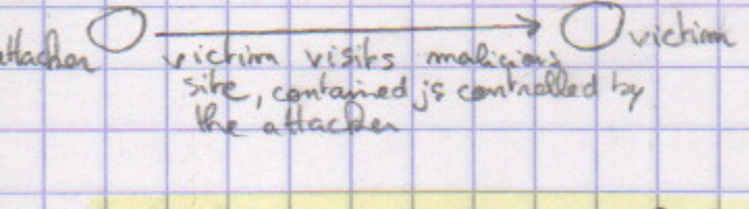


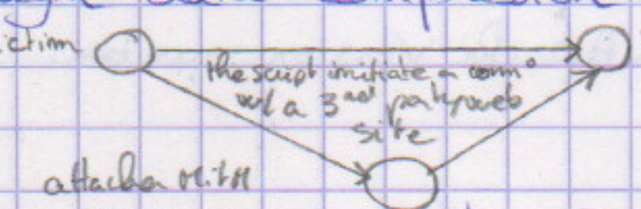
TLS - Heartbleed Attack : Abuse the Reart beat feature in OpenSSL to retrieve chucks of memory for the server

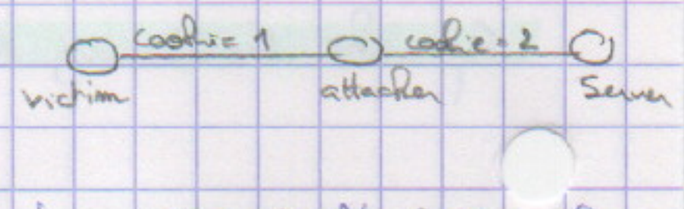




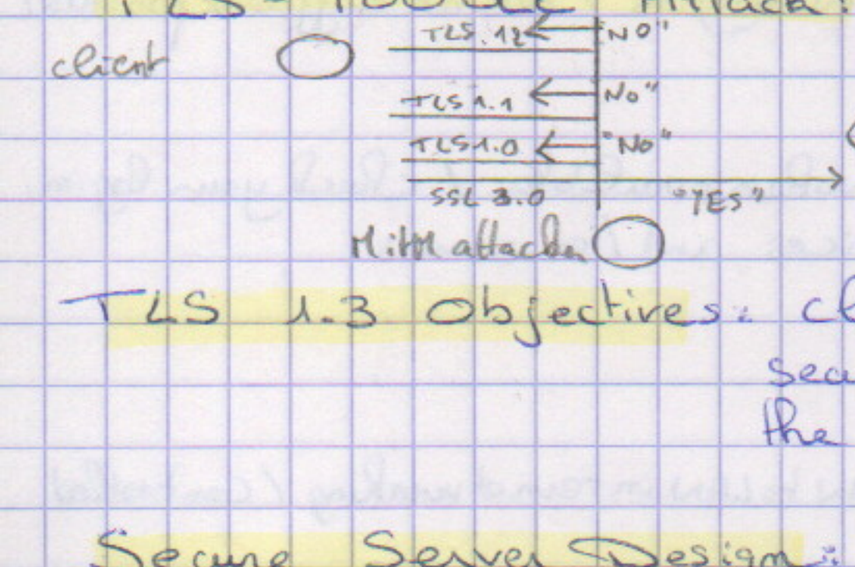
TLS - CRIME Attack : combines chosen plaintext attack and inadvertent information leakage through data compression







TLS - POODLE Attack : a MitM exploit which takes advantage of default fallback to SSL 3.0



TLS 1.3 Objectives : clean up (remove unsafe or unused features) / Security (improve security with up-to-date techniques / Privacy (Encrypt more of the protocol) / Performance / Continuity (backward compatibility)

Secure Server Design : - Use TLS or Other Strong Transport Everywhere / Do not provide Non-TLS pages for secure content / Do not mix TLS and non-TLS content.

Secure Certificate : Use strong Keys & protect them / Use fully qualified names in certificates / Do not use wildcard certificates.

Server protocol and cipher configuration : Only support strong protocols / Prefer Ephemeral Key Exchanges / Only support strong cryptographic ciphers.

+ exercice 2
+ exercice 4
+ protocole pcap TP ?