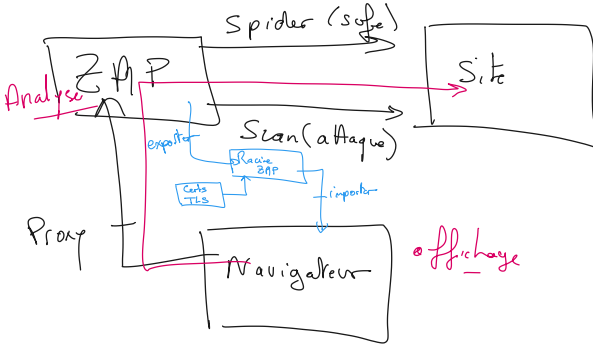
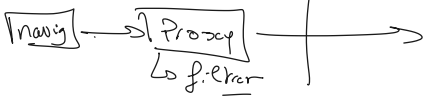
Bonjour Tout le Monde



internet



attaque "Man in the Middle"

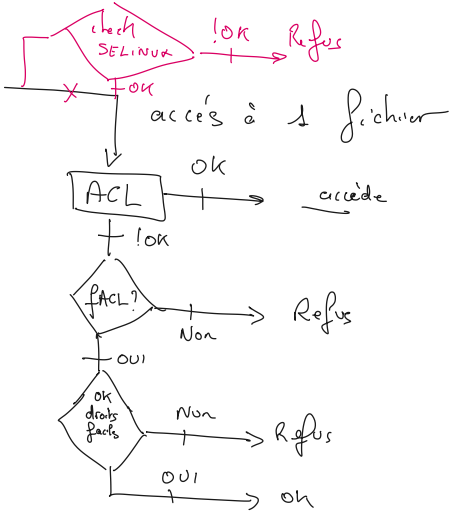
sécure, ok.

http → non detectable

https → detectable

Certificat → Rôle → attester
authentifier
crypter

https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing



/etc → confs

lecture pour tout le monde ? → OUI

→ installe apache

→ Process user | apache apache

/var/www/html

site (php)

→ Bug, faille

→ exploit = remonter le contenu d'un fichier de /etc/...

Collision de Hashage

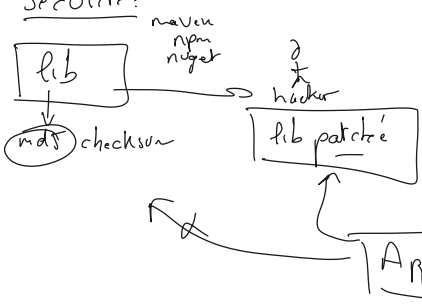
CRC AB

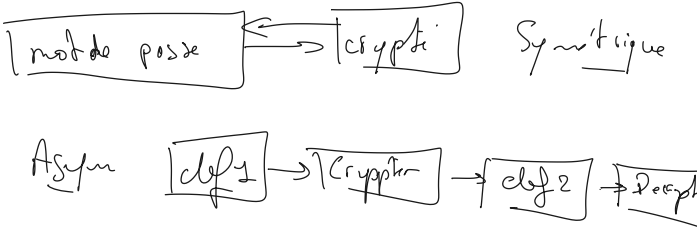
65 66 = CRC = 131

lecture AC = CRC = 132

BA = CRC = 131

Sécurité :





mot de passe = alphanum mémorisable

a-z A-Z 0-9 $ @ / \ - + ...

é

Clef (jeton): Contenu alphanum complexe non mémorisable / copiable / collable

Certificats → clef (de certificats)

→ flux (mémoire, fichiers, dans des "magasins")

→ Contenu binaire (non mémorisable)

- Pas compatible copier / coller
- doit passer par des magasin (Keystore)

ex chaine alpha de 10 caractères: 10^{62} possib.

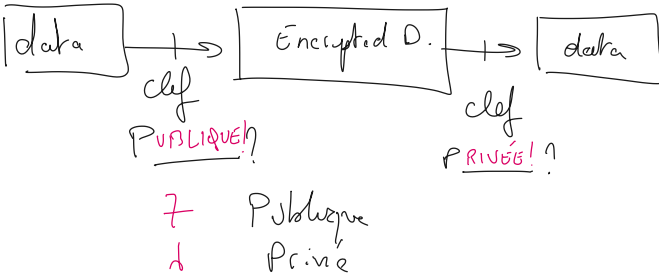
binaire de " " : 10^{256} possib.

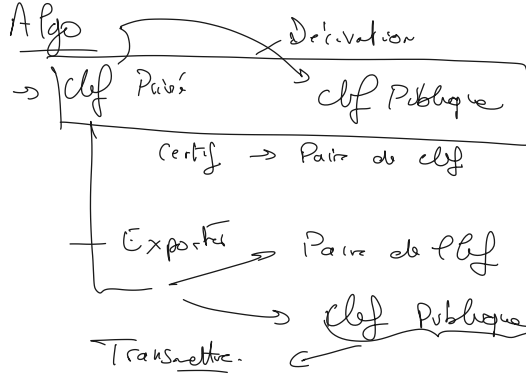
W11 → TPM → Crypto → Pas commun

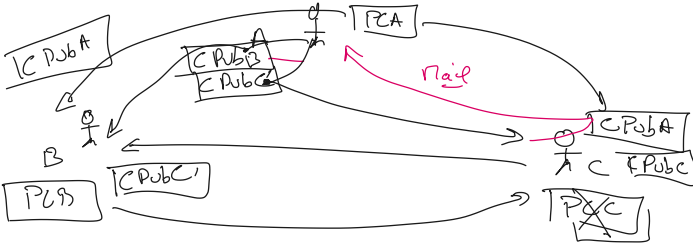
données sensible = crypter!

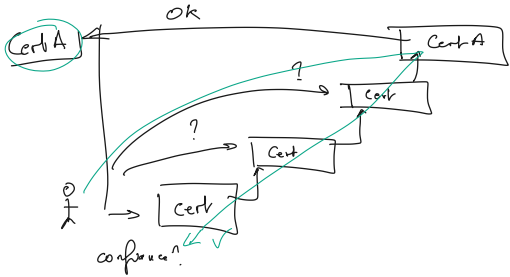
↳ sur disque = crypter le contenu

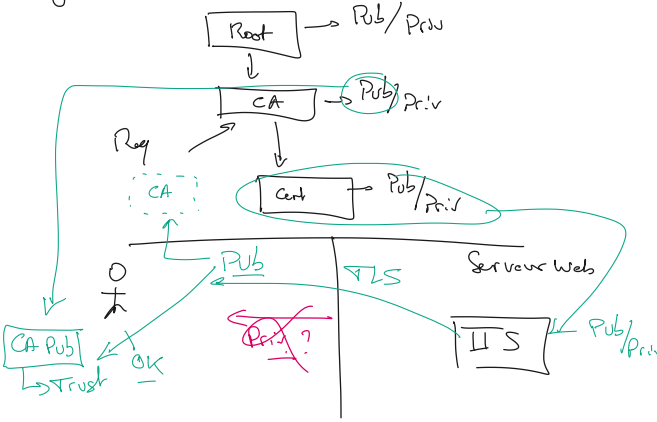
- niveau filesystème = NTFS → EFS
- " bloc disque = bitlocker (encrypté) → partition de boot C:\

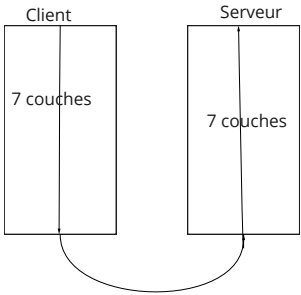

data
clef
PUBLIQUE ?
Encrypted D.
clef
PRIVÉE !
data
7 Publique
d Privé

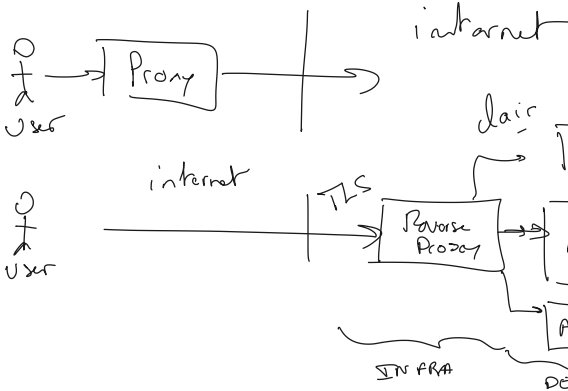

Algo
Dérivation
clef Privé
clef Publique
Certif → Paire de clef
Exporter
Paire de clef
clef Publique
Transmettre.

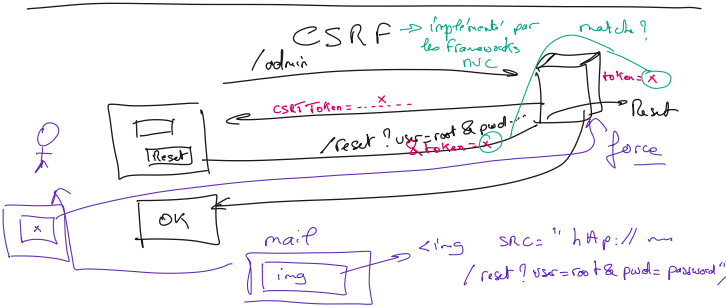

CA
CPubA
CPubB
CPubC
Mail
B
CPubA
C
CPubC
PCB
CPubC'
PCC


ok
Cert A
Cert A
?
Cert
?
Cert
Cert
confiance ?


génère une PKI (admin)
Root
Pub/Priv
CA
Pub
Priv
Req
CA
Cert
Pub/Priv
Pub
TLS
Serveur Web
CA Pub
Trust
OK
Priv ?
IIS
Pub/Priv


Client
Serveur
7 couches
7 couches


Proxy
User
internet
dair
App
internet
TLS
User
Reverse Proxy
App
App
INFRA
DEV


CSRF
implémenté par les Frameworks MVC
/admin
match ?
token = X
CSRF Token = ...X...
Reset
/reset ? user=root & pwd=...
& token = X
force
Reset
OK
mail
img
<img
SRC= " http://
/reset ? user=root & pwd= password ">