M1
Sécurité des systèmes d'informations
2023-2024

SESSION 4
Partie 2

UNIVERSITE PARIS 8 VINCENNES-SAINT-DENIS

Christophe Villeneuve

@hellosct1

@hellosct1@mamot.fr

Aujourd’hui : Session 4 : Les aspects réseaux et applicatifs

- ~~Correction TP3~~
- ~~La sécurité du protocole IP~~
- ~~Sécurisation d’un réseau~~
- Les bases de la cryptographie
- Serveurs applicatifs
- Les usurpations

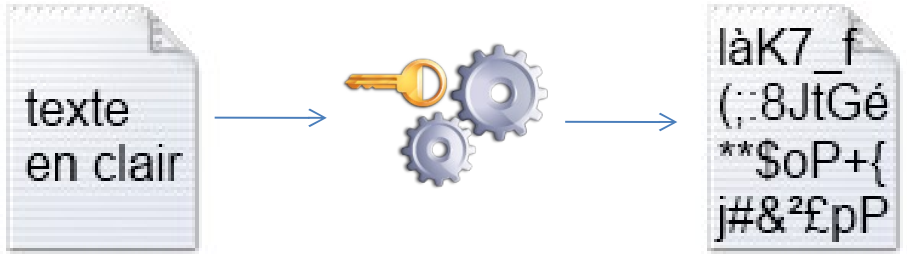
- La sécurité du protocole IP
- Sécurisation d’un réseau
- Les bases de la cryptographie
- Serveurs applicatifs
- Les usurpations

Vocabulaire : Cryptographie

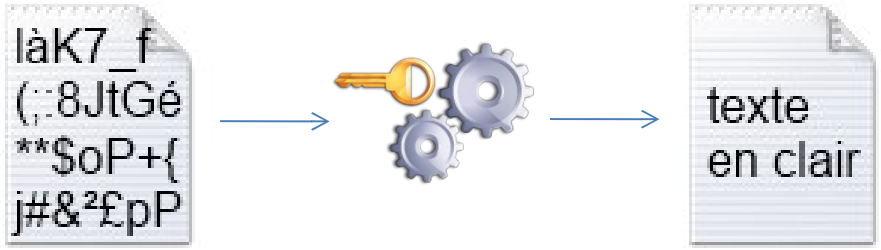
- Discipline consistant à manipuler des données de telle façon que les services suivants puissent être fournis :
  - Intégrité
    - Objectif : s'assurer que les données n'ont pas été modifiées sans autorisation.
      - Remarque : dans les faits, la cryptographie ne s'attache pas vraiment à empêcher une modification de données, mais plutôt à fournir un moyen sûr de détecter une modification malveillante.
  - Confidentialité
    - Objectif : ne permettre l'accès aux données qu'aux seules personnes autorisées.
  - Preuve (authentification et non-répudiation)
    - Objectif : fournir un moyen de preuve garantissant la véritable identité des entités ainsi que l'imputation de leurs actions.

Vocabulaire : Chiffrer / Déchiffrer

- Chiffrer
  - Transformer une donnée de telle façon qu'elle devienne incompréhensible.
  - Seules les entités autorisées pourront comprendre cette donnée chiffrée.



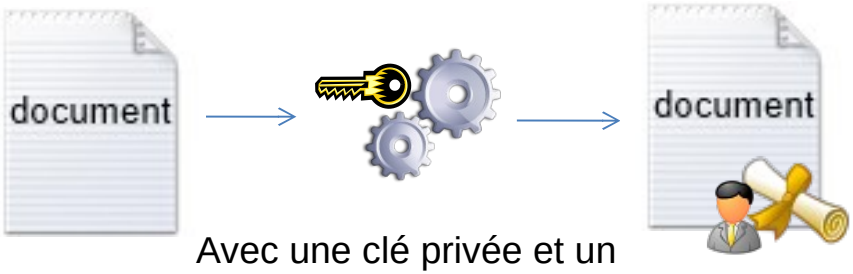
- Déchiffrer
  - Transformer une donnée précédemment chiffrée pour reconstituer la donnée d'origine.
  - Seules les entités autorisées ont la capacité de procéder à cette action



Recours à un algorithme et à une clé cryptographique.

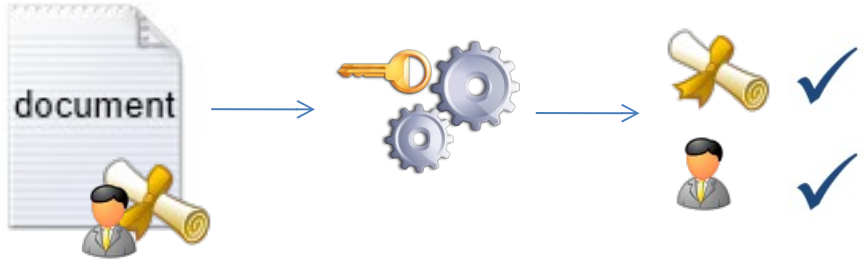
Vocabulaire : Signer / Vérifier la signature

- Signer
  - Créer une signature électronique unique à la donnée et à son auteur. La signature lie donc la donnée d'origine et son auteur.



Avec une clé privée et un message en entrée, on obtient une signature en sortie

- Vérifier la signature
  - S'assurer que la donnée d'origine n'a pas été modifiée et que son auteur est authentifié. Si la signature n'est pas valide, alors il ne faut pas faire confiance au document.

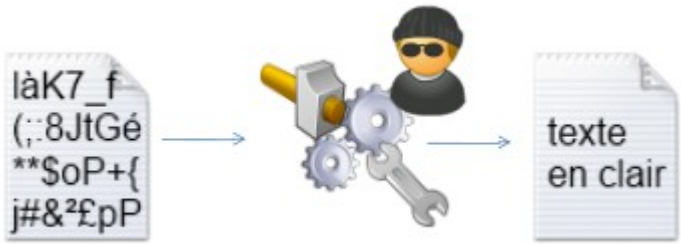


Avec la clé publique, la signature et le message en entrée,
on obtient un verdict OK/NOK en sortie

Vocabulaire : Crypter / Décrypter

- Crypter
  - La notion de crypter n’existe pas. Il s’agit d’un abus de langage.

- Décrypter
  - Reconstituer la donnée d’origine en tentant de « casser » la donnée chiffrée ou l’algorithme cryptographique.



Chiffrement de César

Un peu d'histoire…

- Algorithme cryptographiques historique.
- Les algorithmes sont maintenant basés sur des fonctions mathématiques.

Méthode :

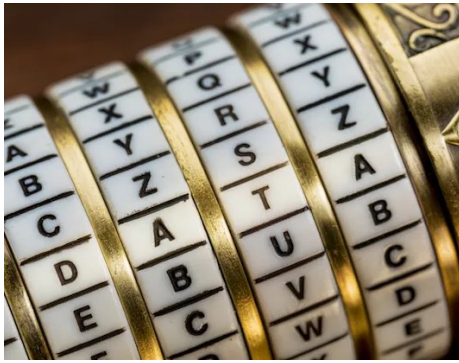
il s'agit ici de
« décaler »
chaque caractère par un
nombre déterminé.

Exemple : clé = 3

A B C D E F G H U J I K …

A B C D E F G H U J I K …

Exercice



- Message chiffrée : ELHQYHQXH
- Avec
  - Lettre Alphabétique
  - Clé = 3
- Quelle est le message en clair ?

Réponse :

BIENVENUE

Détails de la réponse

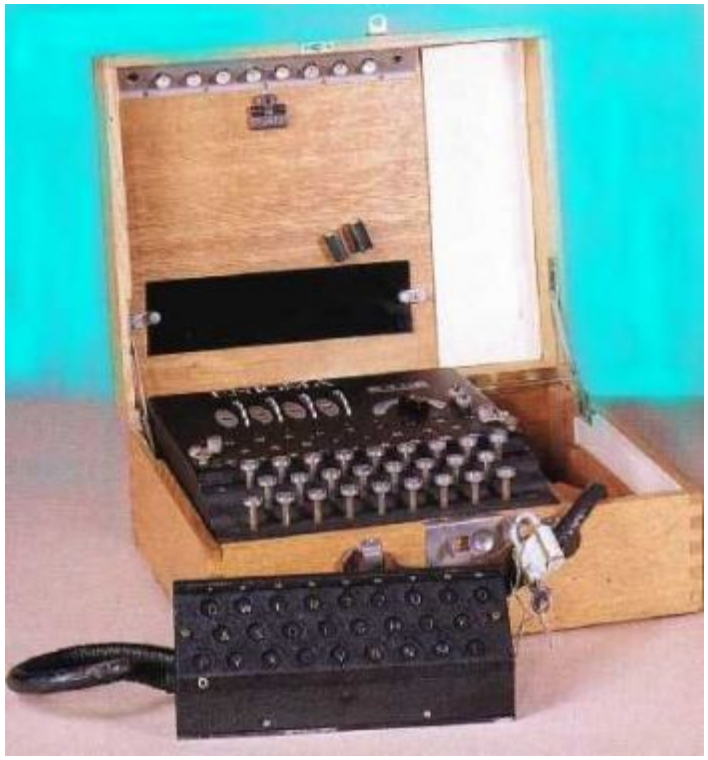
d	e	f	g	h	i	j	k	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

E	L	H	Q	Y	H	Q	X	H
b	i	e	n	v	e	n	u	e

Machine Enigma : Présentation

- Machine initiale conçue au début du XXè siècle.
- Ressemble à des machines à écrire
  - Avec un clavier destiné à un opérateur
  - Un tableau de sortie (panneau lumineux)
  - Plusieurs rotors
  - Un réflecteur
  - Un tableau de connexion
- A bénéficié de plusieurs évolutions et versions.

  → Utilisée par les Allemands pendant la seconde guerre mondiale



Méthode de chiffrement

- Basée sur de la substitution :
  - L’opérateur tape le message en clair.
  - Chaque lettre du message en clair est remplacée par une autre lettre dans le message chiffré

    → Les lettres chiffrées s’allument sur le tableau de sortie au fur et à mesure de la frappe en clair de l’opérateur
- L’utilisation des rotors a pour conséquence
  - Une lettre en clair sera être substituée
  - Par des lettres différentes tout au long du message chiffré.

Machine Enigma : Fonctionnalités

Un peu d'histoire…

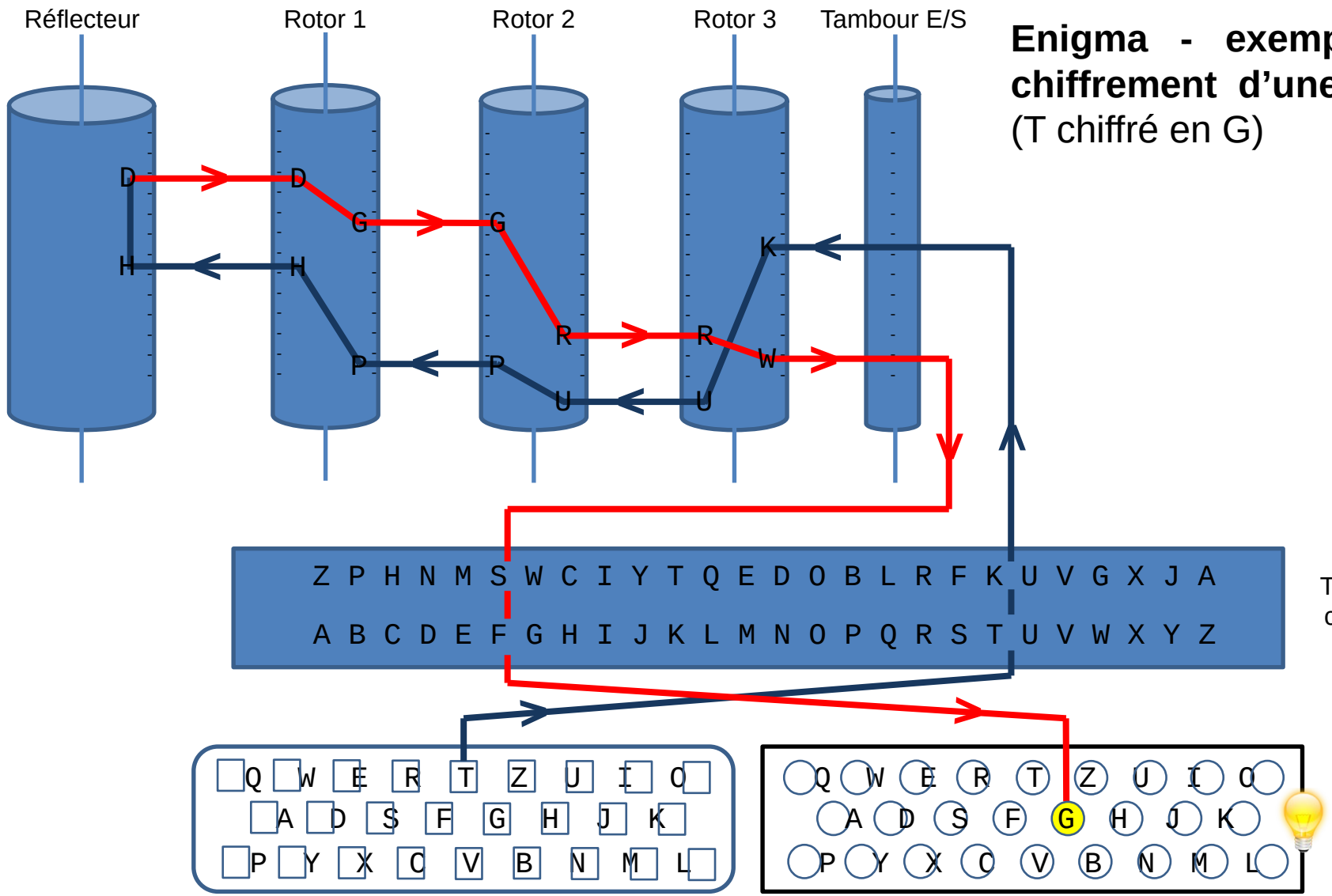
- Tableau de connexion
  - Se situe avant l'entrée sur le brouilleur
  - Effectue des permutations simples.

- De 3 à 6 rotors (selon le modèle)
  - Permutations aléatoires des lettres de l'alphabet ;
  - Le rotor tourne à chaque lettre tapée ;
  - Lorsque le premier rotor a fait un tour (26 positions), le second rotor tourne d'un cran, et ainsi de suite.

- Le réflecteur
  - Dernière permutation 2 à 2 des lettres avant de les faire
  - Retraverser les retors et le tableau de connexion.

Machine Enigma : Exemple

Un peu d'histoire…



Enigma - exemple de chiffrement d'une lettre (T chiffré en G)

Tableau de connexion

Chiffrement symétrique

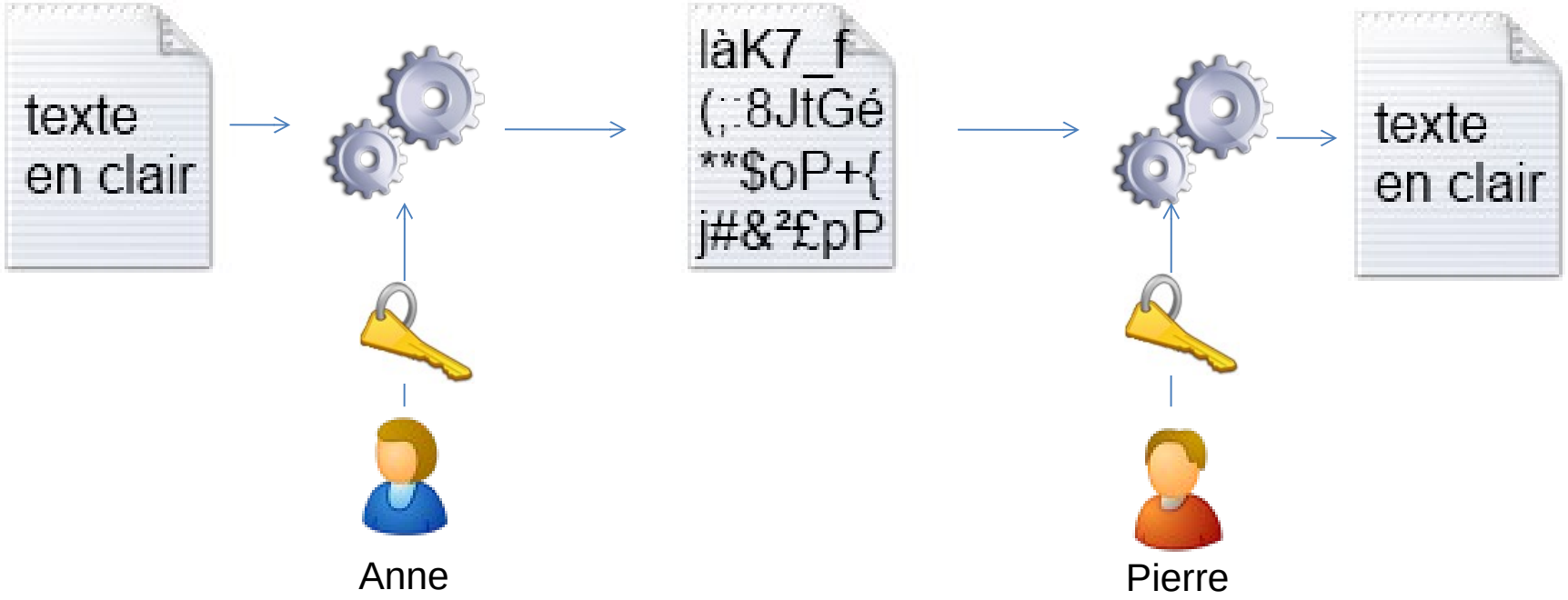
- La clé utilisée pour le chiffrement
  - Identique que celle utilisée pour le déchiffrement
- Cette clé doit être secrète :
  - Seules les personnes habilitées doivent posséder cette clé,

    /!\ sinon la confidentialité du message n’est plus assurée !

Exemple : chiffrement symétrique

- Anne souhaite

  envoyer un message confidentiel à Pierre



Clé secrète partagée entre Alice et Pierre

Chiffrement asymétrique (1/2)

- La clé utilisée
  - pour le chiffrement est différente

    de celle utilisée pour le déchiffrement.
- Il est nécessaire d'utiliser 2 clés :
  - Clé publique :
    - comme son nom l'indique, cette clé est publique et peut être donnée à tout le monde
  - Clé privée :
    - cette clé doit être personnelle et connue de son seul propriétaire.
    - Elle ne doit jamais être divulguée !

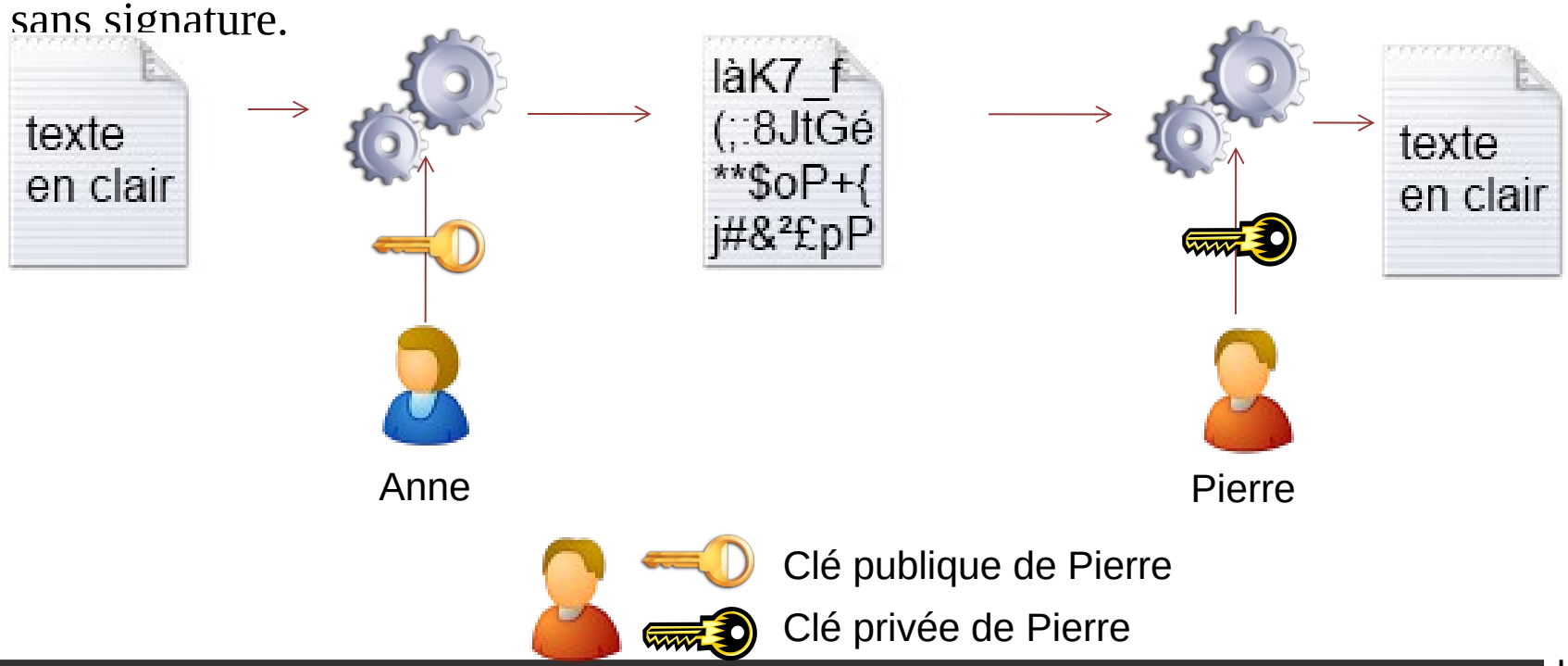
Chiffrement asymétrique (2/2)

- Ces deux clés sont mathématiquement liées
  - La connaissance de la clé publique
    - ne permet pas de calculer de manière efficace la clé privée

      /!\ attention à la taille de la clé, qui doit être suffisamment longue
  - Chaque personne doit donc posséder 2 clés :
    - Une clé privée (confidentielle)
    - Une clé publique qu'il peut divulguer à tout le monde.

Exemple : Chiffrement asymétrique

- Anne souhaite envoyer un message confidentiel à Pierre
- Anne chiffre le message avec la clé publique de Pierre
- Pierre déchiffre le message grâce à sa privée ;
- Notes :
  - Anne ne pourra jamais (et n'aura jamais besoin de) utiliser la clé privée de Pierre puisque celle-ci est confidentielle à Pierre !
  - Anne n'a pas besoin d'utiliser ses clés personnelles dans cet exemple de chiffrement sans signature.



Chiffrement symétrique vs Chiffrement asymétrique

Chiffrement symétrique	Chiffrement asymétrique
Avantages	
• Rapidité des opérations (adapté à du trafic en temps réel) ; • Clés courtes (256 bits suffisent actuellement) ;	• Facilité d'échange des clés : les seules clés qui ont besoin d'être échangées sont des clés publiques (dont il faut assurer la protection en intégrité) ;
Inconvénients	
• Difficulté d'échange sécurisé des clés secrètes : comment le faire en protégeant ce secret ?	• Lenteur des opérations (peu adapté à du trafic en temps réel) ; • Grande taille des clés (2048 bits minimum actuellement) ;
Exemples d'algorithmes sûrs (janvier 2015)	
• AES.	• RSA.

Signature électronique

- Rappel de l’objectif :
  - s’assurer de la non-modification d’une donnée,
  - s’assurer de l’identité de son auteur.
- Si la signature n’est pas valide,
  - C’est que l’auteur « n’est pas le bon »
  - Ou que la donnée reçue n’est pas celle que son auteur avait signé.
- Notes :
  - La signature électronique n’assure pas la confidentialité des données, mais leur intégrité et la notion de preuve ;
  - Lorsque l’on chiffre un message, il est fortement recommandé de le signer également afin d’assurer l’intégrité du message.

Principe (1/2)

- Le signataire d'un message génère

  → grâce à un algorithme cryptographique spécifique ←

  - Une valeur unique calculée à partir du message que l'on souhaite signer : un condensat (un haché) ;
    - Les algorithmes de calcul de condensat sont publics et ne gèrent pas de secret, donc tout le monde peut les utiliser et calculer les mêmes condensats à partir d'un même message ;
    - Deux messages différents ne peuvent pas donner lieu au même condensat.
- Le signataire utilise l'algorithme de signature :
  - Prend en entrée sa clé privée et le condensat précédent,
  - pour produire une signature électronique
- Le signataire envoie (ou stocke)
  - le message et la signature électronique,
  - permettant ainsi à un lecteur d'en prendre connaissance

Principe (2/2)

- Le lecteur calcule lui-même
  - le condensat du message en clair
- Le lecteur utilise
  - l’algorithme de vérification de signature,
    - Qui prend en entrée la clé publique du signataire,
    - Le condensat et la signature, pour rendre un verdict.
  - Si le verdict est négatif,
    - Alors il ne faut pas faire confiance au message reçu

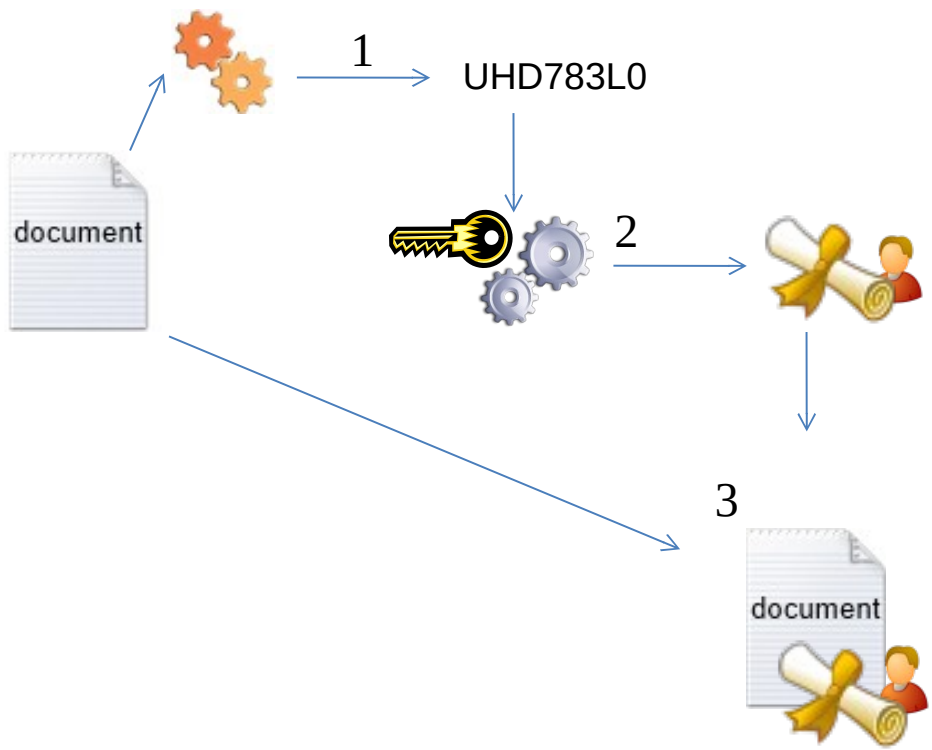
      → celui-ci ne correspond pas

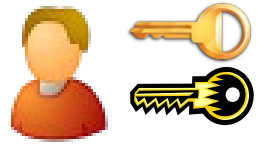
      — pour une raison que l’on ignore —

      au message du signataire

Déroulement : Etapes de la signature

- Le signataire génère le condensat unique associé au message ;
- Le signataire utilise l'algorithme de signature, qui prend en entrée sa clé privée et le condensat précédent, pour produire une signature électronique ;
- Le signataire envoie (ou stocke) le message et la signature électronique, permettant ainsi à un lecteur d'en prendre connaissance ;
- La vérification par le destinataire/lecteur est décrite sur la diapositive suivante.





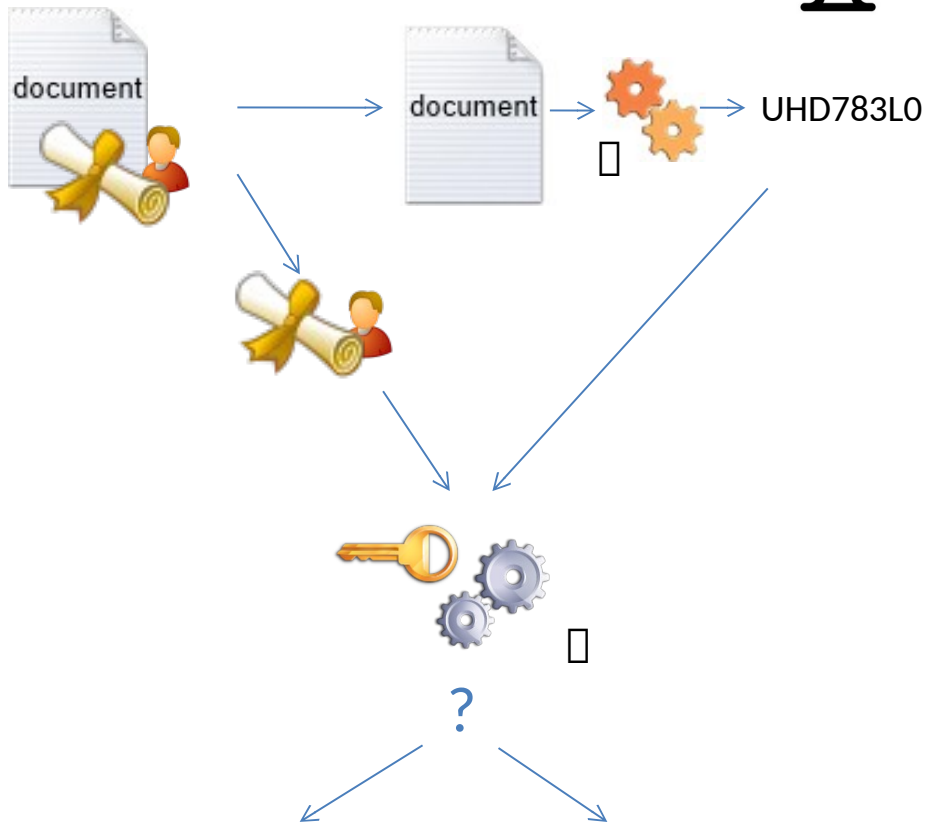
Clé publique du signataire

Clé privée du signataire

Déroulement : Etapes de Vérification signature

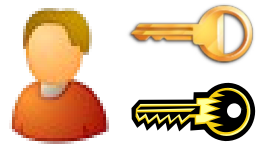
Vérification de la signature par un lecteur/destinataire :

- Le lecteur calcule le condensat du message en clair ;
- Le lecteur utilise l'algorithme de vérification de signature,
  - qui prend en entrée la clé publique du signataire,
  - le condensat et la signature,
  - pour rendre un verdict.
- Si le verdict est négatif, alors il ne faut pas faire confiance au message reçu (celui-ci ne correspond pas — pour une raison que l'on ignore — au message du signataire).



 La signature est valide. Le message est intègre.

✘ La signature est invalide. Le message n'est pas intègre.

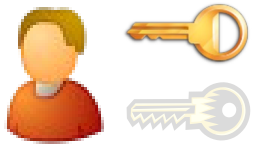


Clé publique du signataire

Clé privée du signataire

Certificats électroniques

- Un aspect important n’a pas été traité jusqu’à maintenant :



Clé publique de Pierre

Clé privée de Pierre

Les interlocuteurs de Pierre ont besoin d’utiliser sa clé publique.

Exemple 1 :

Comment peuvent-ils être certains que la « clé publique de Pierre » appartient effectivement à Pierre et qu’elle n’a pas été générée frauduleusement en son nom ?

Exemple 2 :

Comment les visiteurs d’un site web bancaire peuvent être certains que le site web est légitime et qu’il ne s’agit pas d’un site frauduleux imitant celui d’une banque ?

Solution :

Utilisation de certificats électroniques.

Certificats électroniques (1/2)

- Un certificat est un fichier électronique qui comprend notamment :
  - La clé publique d'un individu
    - ou d'une entité ou d'un nom de domaine
  - Les détails de cet individu (ou de cette entité)
    - nom, prénom, nom de domaine, etc.
  - La signature par un tiers de confiance,
    - chargé de garantir que le propriétaire de la clé publique a été vérifié

      – par conséquent –

      - l'authenticité de la clé publique vis-à-vis de son propriétaire.
    - La signature porte sur l'identité du détenteur et la clé publique afin d'assurer l'intégrité de l'ensemble ;
  - D'autres informations telles que l'usage
    - de la clé, les dates de validité
    - des informations concernant la révocation, etc.

Certificats électroniques (2/2)

- Le tiers de confiance,

  Une autorité de certification, en charge de :

  - Vérifier l'identité de la personne demandant à créer le certificat ;
  - Créer le certificat après vérification, puis le signer
    - Avec la clé privée de l'autorité de certification
  - Tenir à jour une liste des certificats qui ont été révoqués
    - Exemple si la clé a été compromise

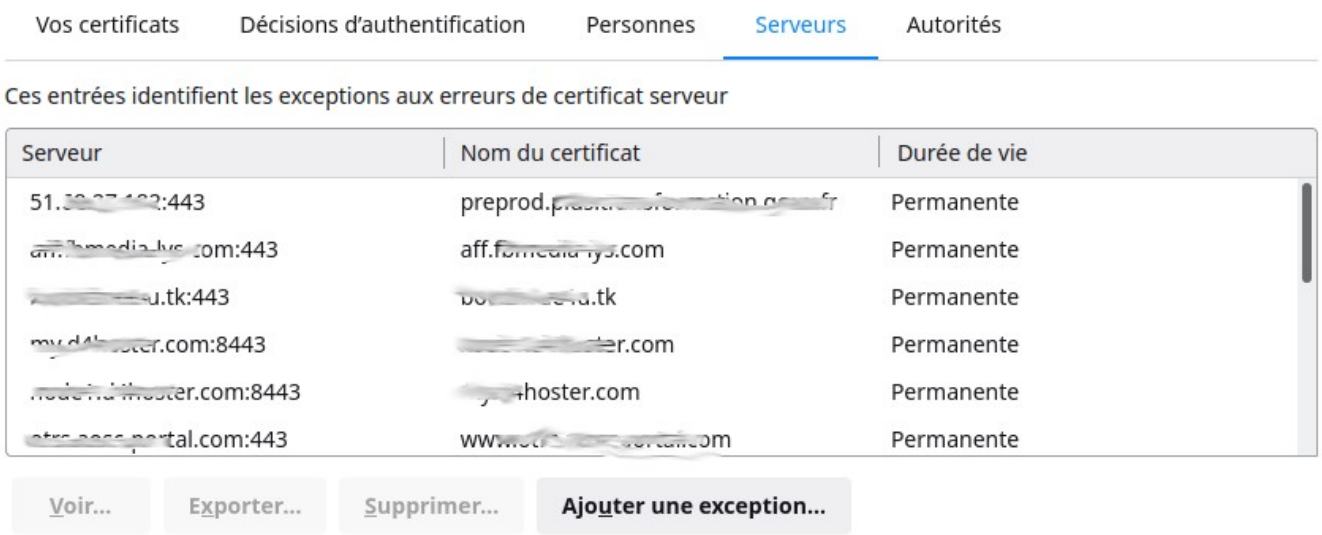
Comment connaître les autorités de certification ?

- Elles sont directement intégrées
  - par les éditeurs dans les systèmes d'exploitation
  - et/ou les navigateurs ;
- L'utilisateur est également libre
  - de rajouter l'autorité de certification de son choix
    - s'il choisit de faire confiance à des certificats signés
    - par une autorité non-intégrée dans son navigateur

Dans Firefox :

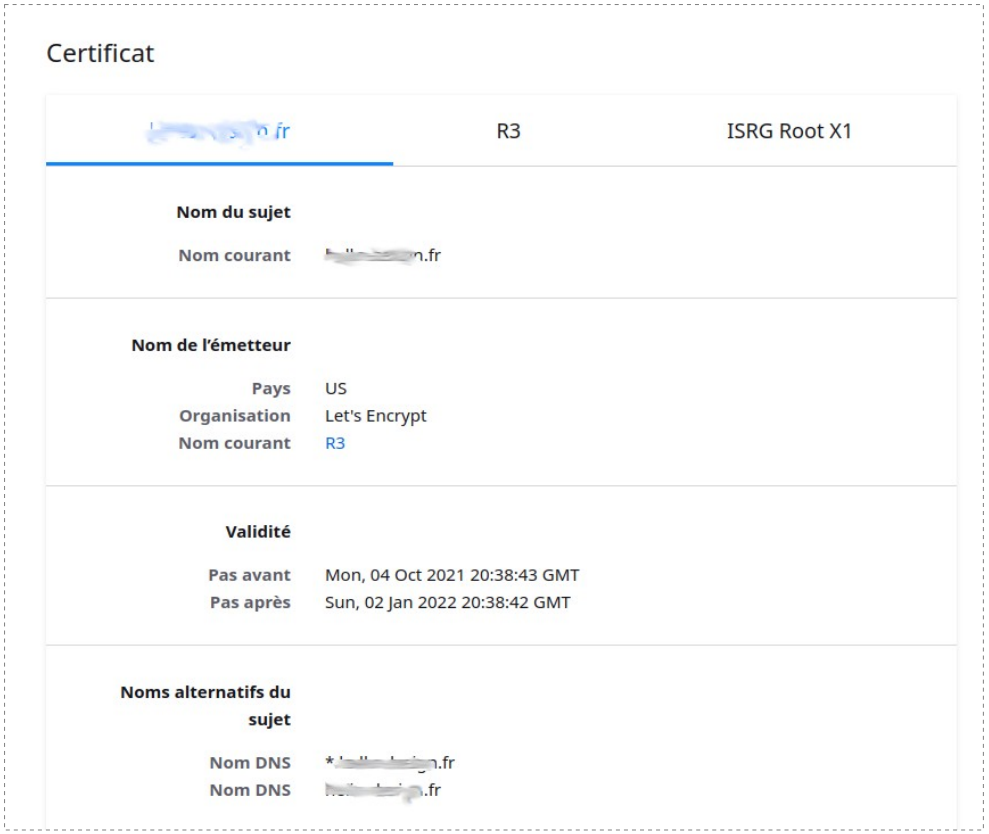
Tapez URL
about:preferences#privacy

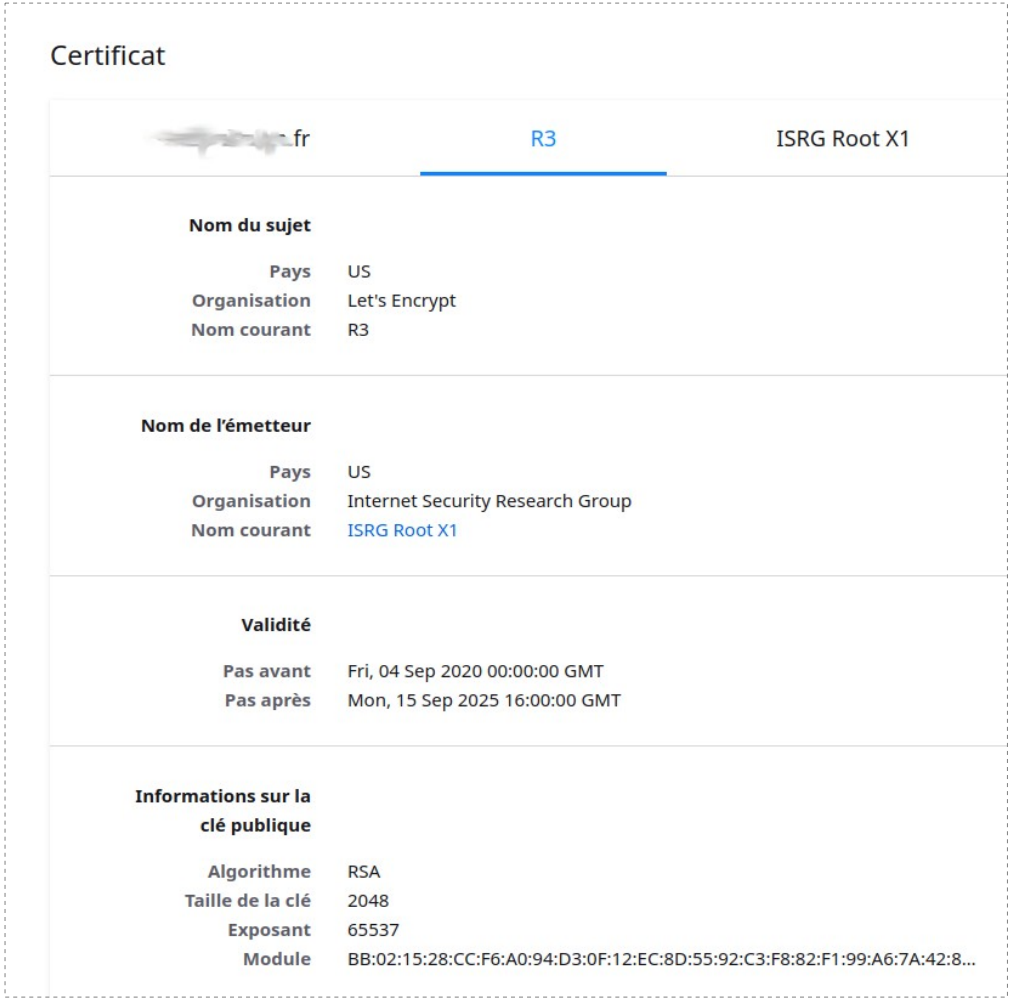
Onglets Certificats



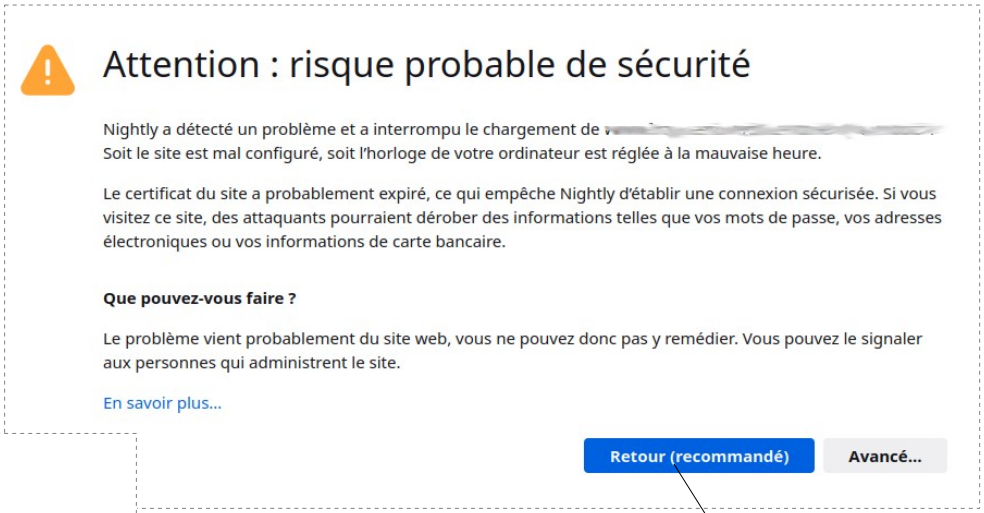
Modèles : Certificats électroniques

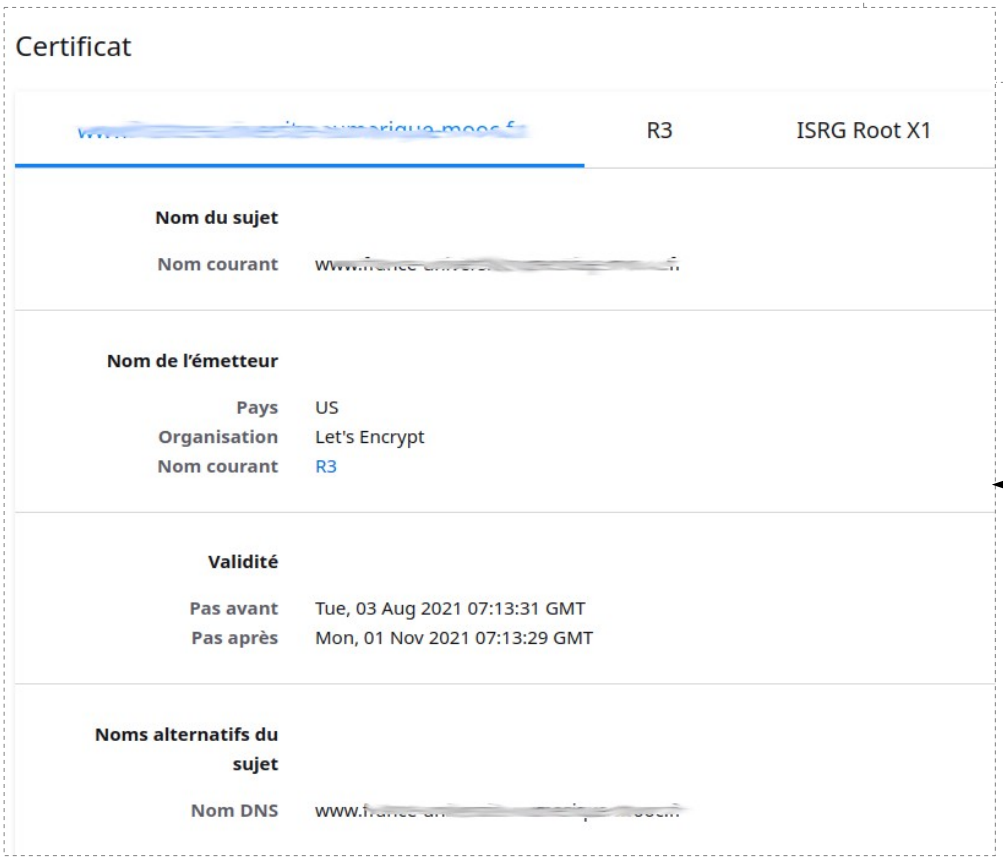
Les détails techniques du certificat, la clé et la signature se trouvent dans Détails

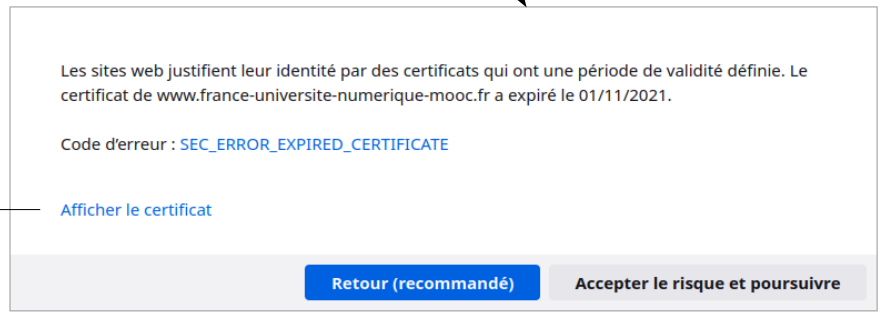




Certificat non valide

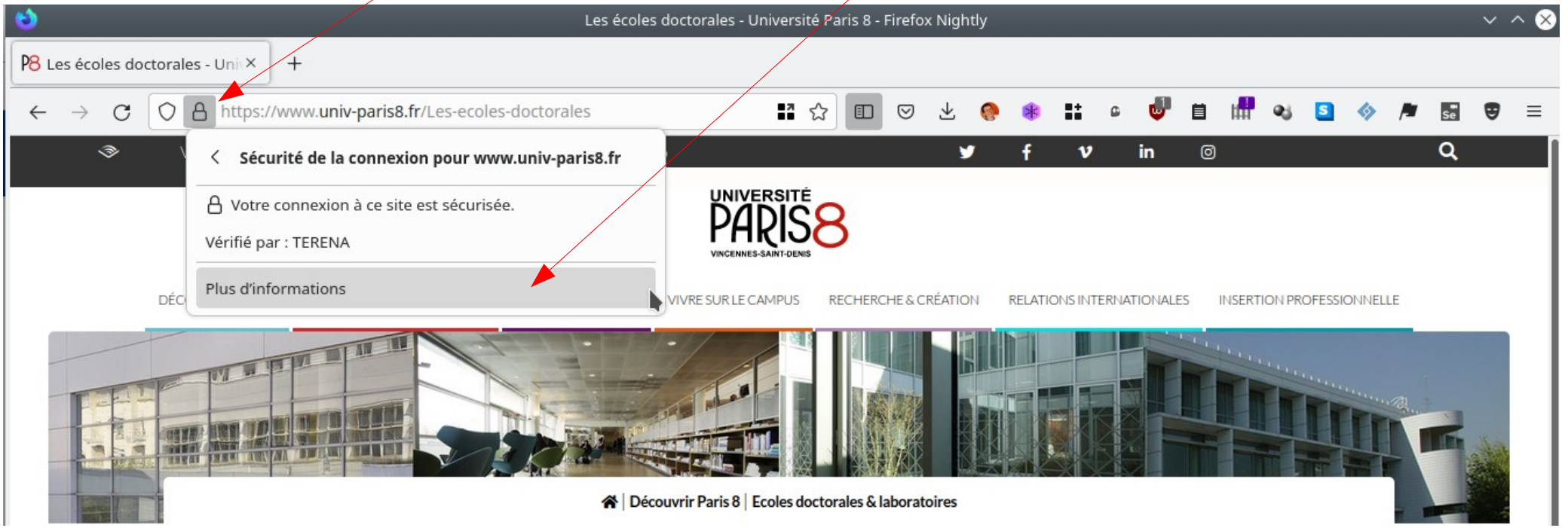






Où trouver les certificats dans un navigateur ? (1/2)

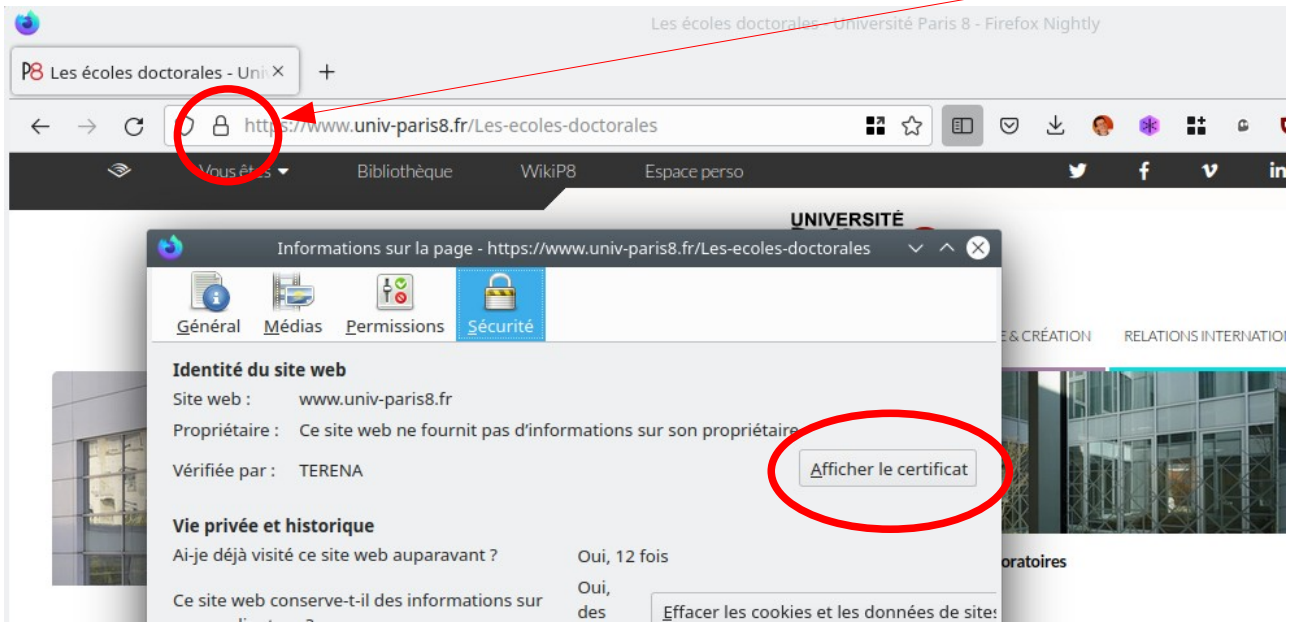
- Navigateur Firefox
  - Ouvrir le certificat d'un site WEB



Où trouver les certificats dans un navigateur ? (2/2)

Le certificat du site WEB est disponible et valide,
cela amène donc
deux avantages à l'utilisateur,

- caractéristiques du HTTPS



Confiants que le site WEB est légitime

→ Le certificat a été vérifié et signé par une autorité de certification de confiance

Le certificat contient la clé publique du site WEB, nous pouvons donc chiffrer nos connexions vers ce site

Méthode : chiffrement avec la clé publique du destinataire (vu dans le cours)

Jetons cryptographiques (tokens)

- Les jetons sont utilisés pour stocker
  - Clés privées (cryptographie asymétrique)
  - Clés secrètes (cryptographie symétrique)

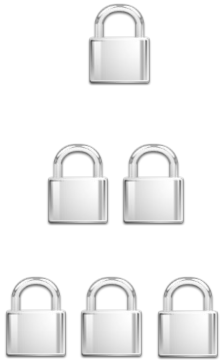
- Un jeton contient une information sensible

  (une clé privée ou secrète)

  - Protéger ce jeton pour que seules les personnes habilitées puissent l'utiliser

Exemples de jetons

- Leurs moyens de protection (ainsi que leur niveau de sécurité) :
  - Fichier sur disque,
    - Associé à un mot de passe connu de l'utilisateur seulement
      - Exemple avec l'application libre GPG
  - Jeton USB
    - Associé à un mot de passe
      - Exemple de nombreux produits commerciaux qui utilisent un jeton physique pour authentifier un utilisateur sur un poste de travail
  - Carte à puce
    - Associée à un mot de passe simple
      - Exemple des cartes bancaires avec un code PIN permettant d'authentifier le propriétaire de la carte avant d'autoriser la transaction.



Pour éviter qu'une personne malveillante
ne découvre facilement le mot de passe simple,

on impose un verrouillage de la carte à puce
après 3 tentatives infructueuses.

A retenir

- La cryptographie est
  - Une des disciplines de la cryptologie
  - But : Protéger des messages

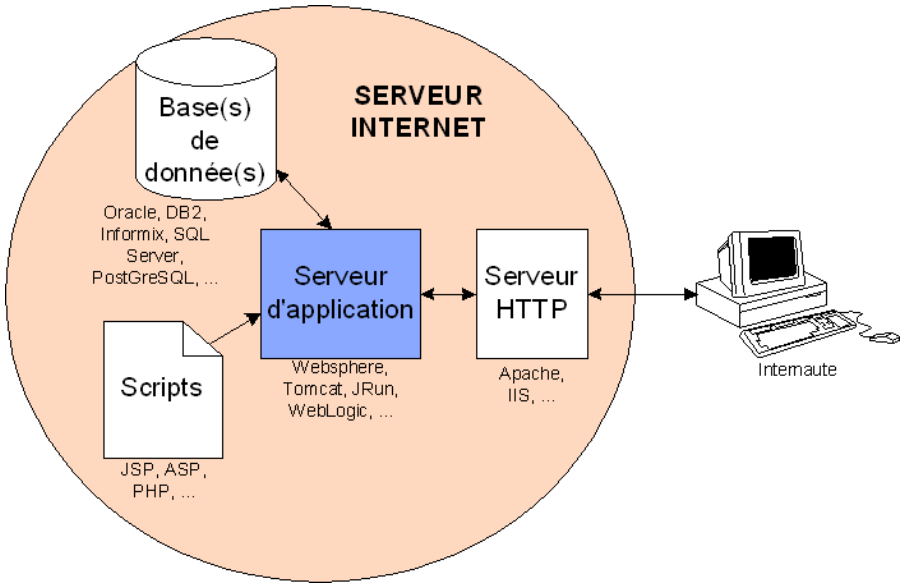
https://school.hello-design.fr

4C

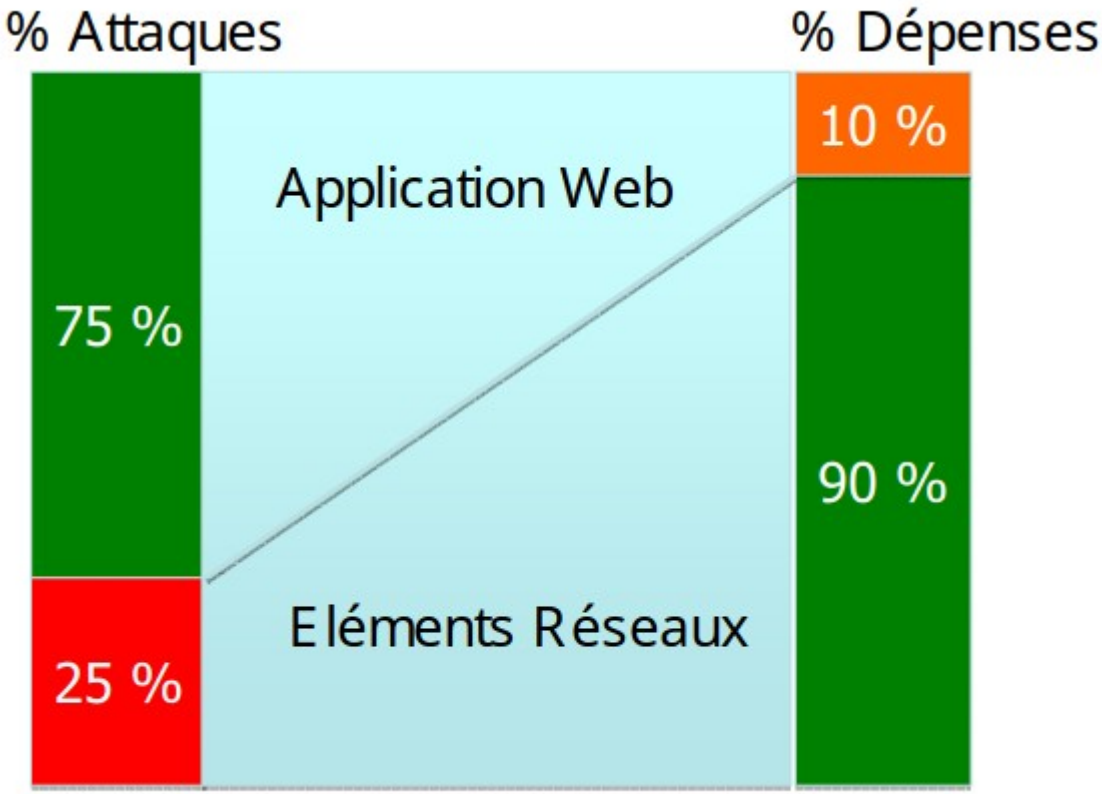
- La sécurité du protocole IP
- Sécurisation d’un réseau
- Les bases de la cryptographie
- Serveurs applicatifs
- Les usurpations

Serveur applicatif

- Un serveur d'applications c'est un logiciel d'infrastructure offrant
  - un contexte d'exécution pour des composants applicatifs
- L'objectif
  - Permettre à partir d'un client aussi léger que possible d'effectuer des traitements distants sur une machine puissante, en mode transactionnel.
- Les utilisateurs y accèdent par le biais d'un navigateur.
- De l'autre côté, le serveur séparent les niveaux : accès aux données, traitement métier et présentation.
- Ces composants peuvent assurer de manière plus ou moins cachée :
  - les fonctions de moniteur transactionnel,
  - la persistance des données,
  - la gestion de la montée en charge
  - ...
- Principaux Serveurs d'applications
  - Apache
  - Nginx
  - ...



Faiblesses des applications Web

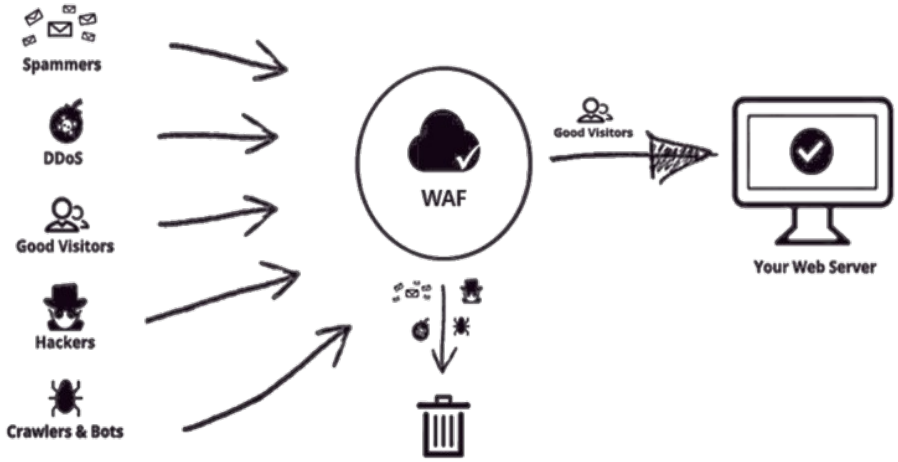


Etude Gartner
75 % des attaques ciblent le niveau applicatif
33 % des applications web sont vulnérables

WAF (1/2)

- Web Applicatif Firewall
  - En FR → Pare-feu pour Applications Web
- Protège le serveur d'applications Web
  - dans le backend des multiples attaques
    - Phishing, ransomware, attaque DDOS, malware...
- But :
  - Surveille
  - Analyser
    - les paquets de requête HTTP / HTTPS
    - les modèles de trafic
  - Bloque les paquets
- Chaque paquet envoyé au serveur

  → Vérification de la demande de la requête

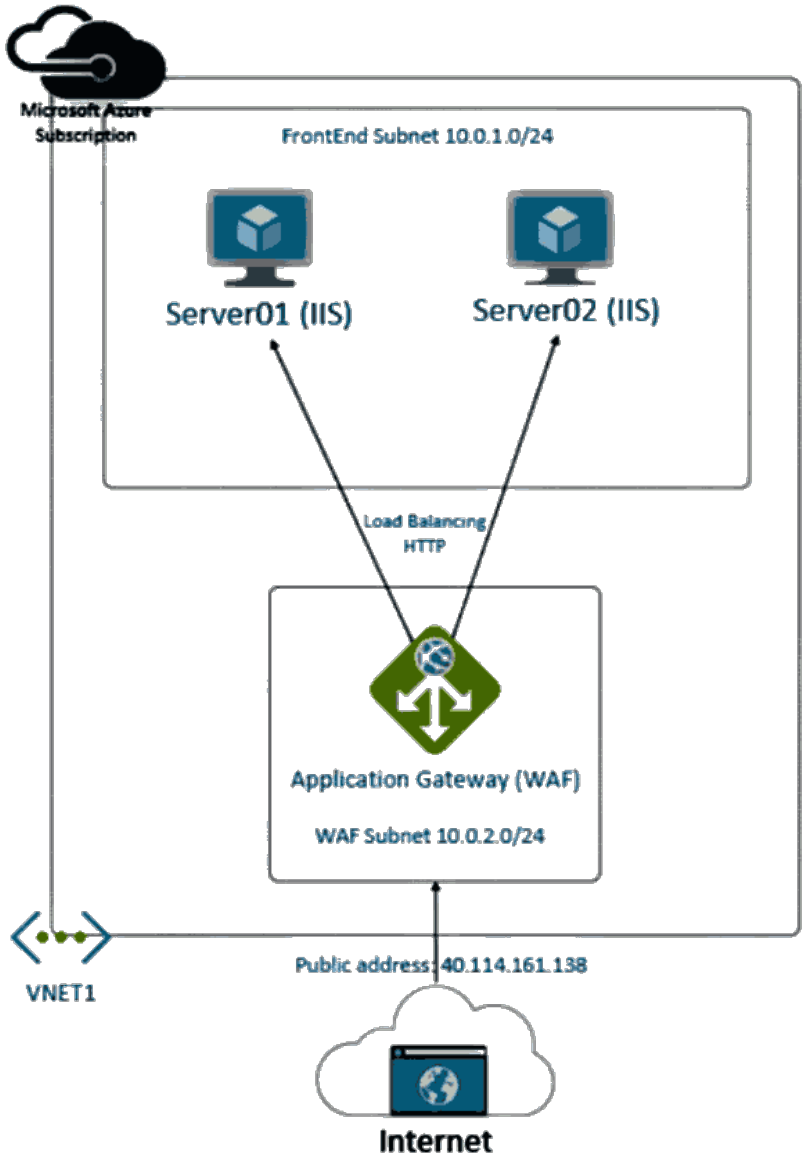


WAF (2/2)

- Les fonctionnalités du WAF peuvent être implémentées
  - En software

    Une application est installée sur le système d'exploitation
  - En hardware

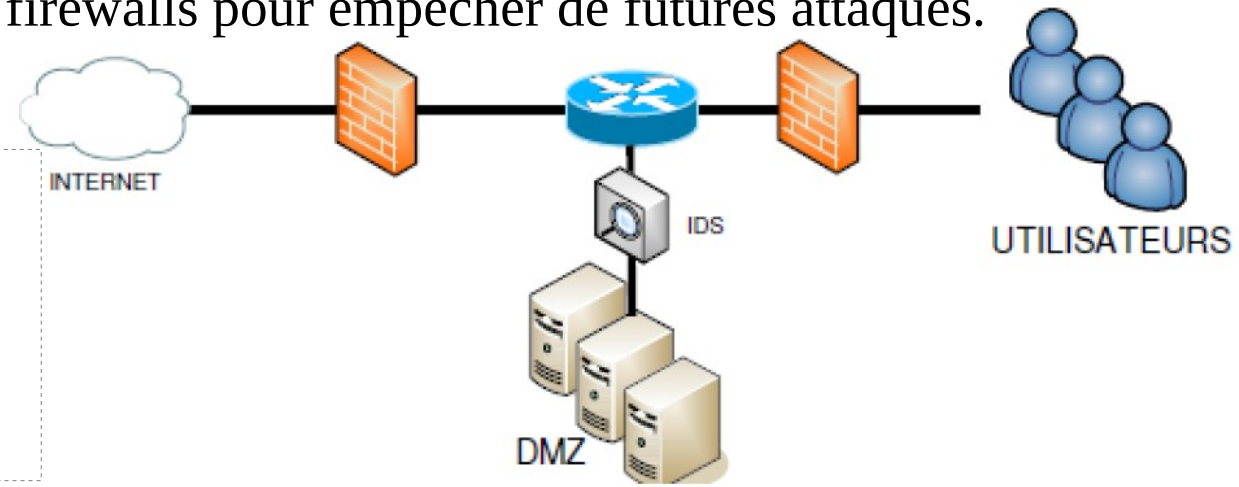
    Les fonctionnalités sont intégrées dans une solution d'appliance.
- Différents types de WAF
  - Les WAF en réseau
  - Les WAF basés sur l'hôte
  - Les WAF hébergés dans le cloud



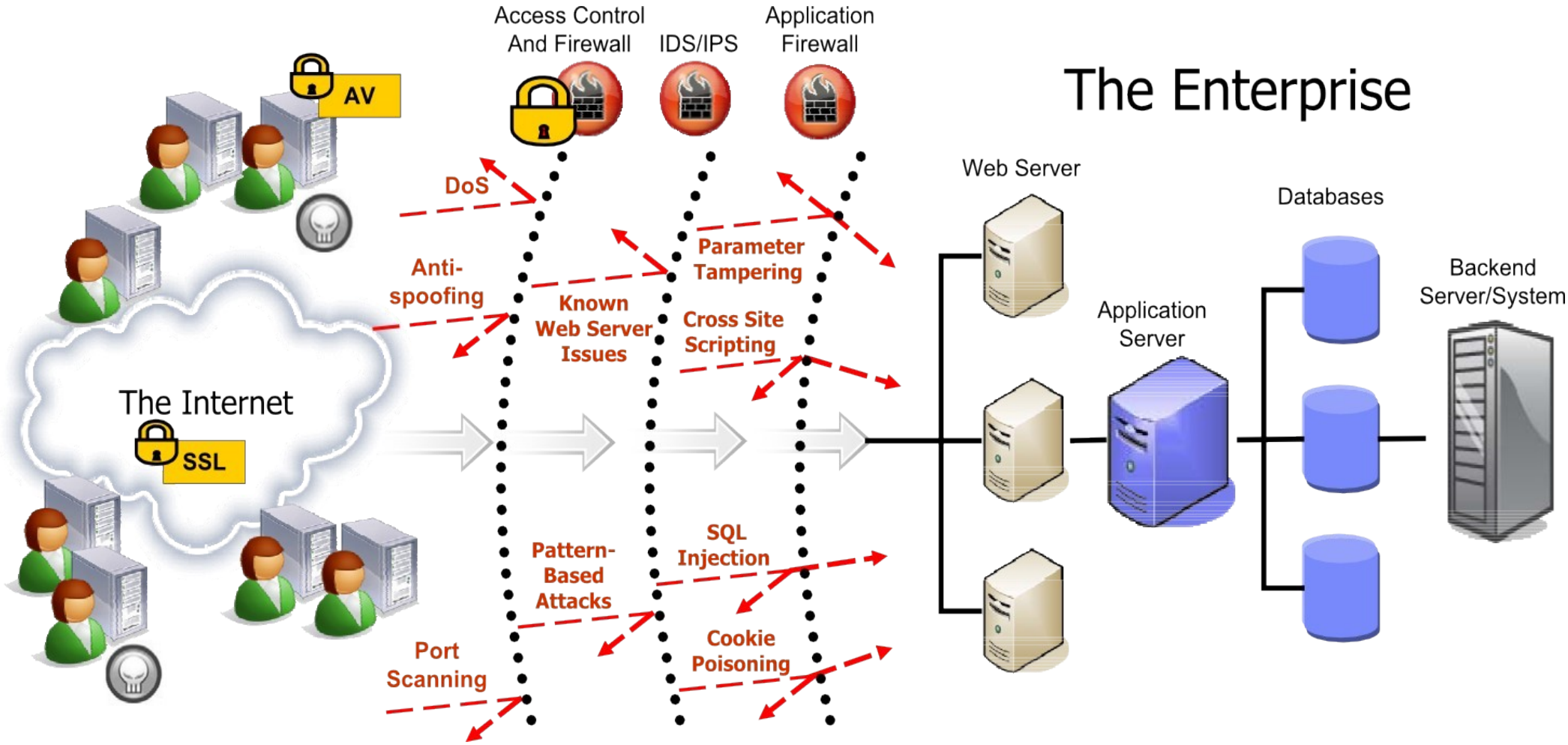
IPS

- Système de prévention des intrusions
- C’est une forme de sécurité de réseau
- Sert à détecter et prévenir les menaces identifiées.
- Rôle :
  - Signaler des événements aux administrateurs du système et prend des mesures préventives comme :
    - La fermeture des points d’accès
    - La reconfiguration des firewalls pour empêcher de futures attaques.

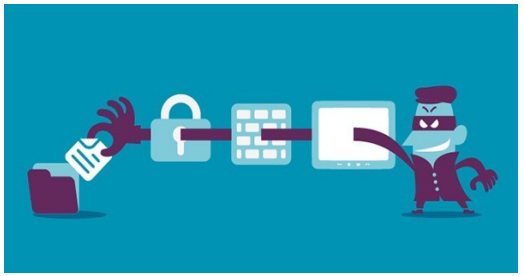
Exemple :
Un réseau d’entreprise typique ayant une multitude de points d’accès
- Avoir un moyen de surveiller les signes d’effraction potentielle, d’incidents et de menaces imminentes.

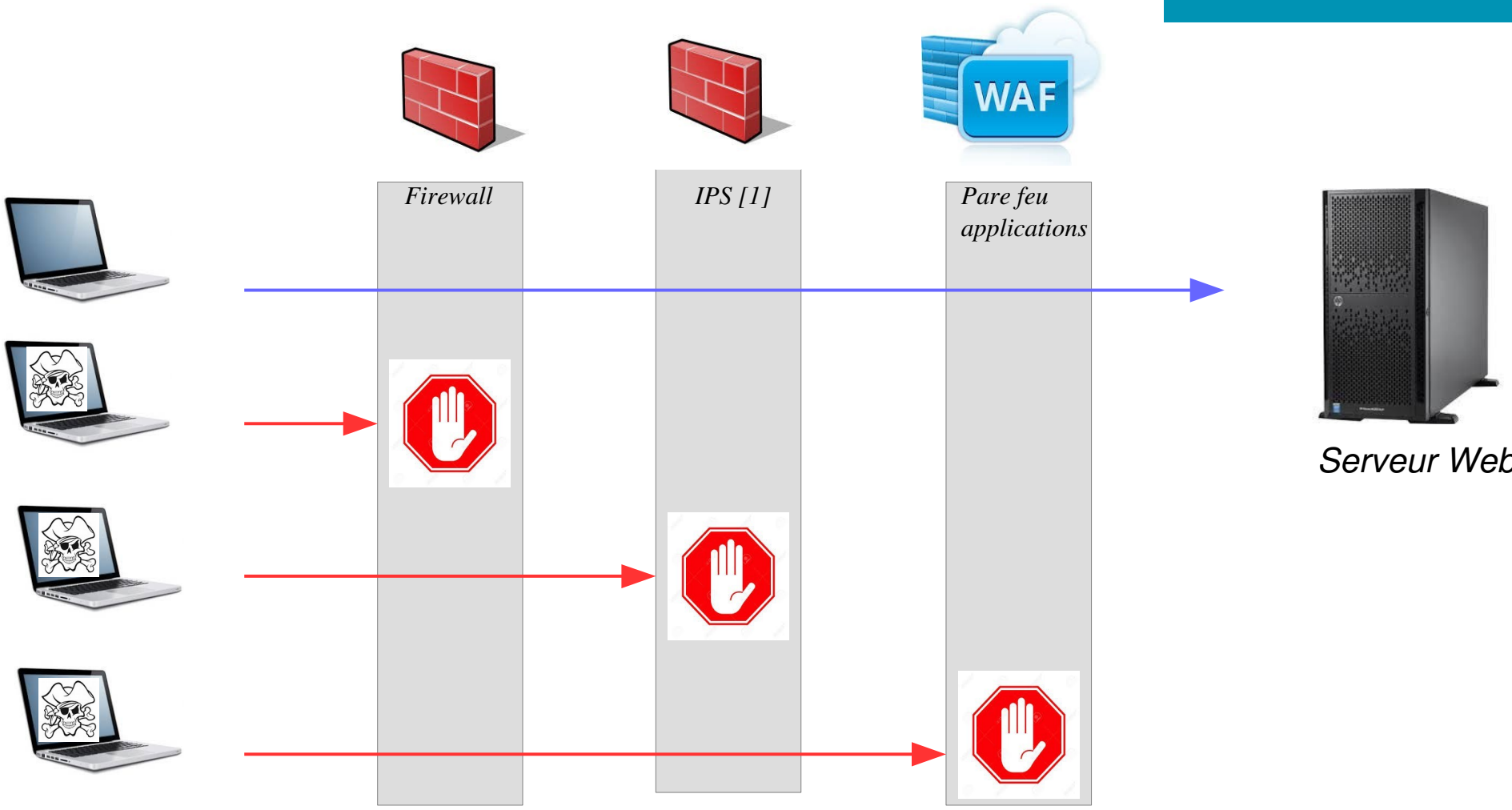


Les attaques sur internet



Niveau de protection





[1] Systeme prévention intrusion

Configuration

- Apache
  - Plugin :

    $ a2ensite default-ssl
  - Config :

```
# Virtualhost du HTTPS (port 443)
<VirtualHost *:443>
  ServerName urlSite.net
  ServerAlias www.urlSite.net
  DocumentRoot /var/www/urlSite

  SSLEngine on
  SSLCertificateFile /etc/apache2/ssl/server.crt
  SSLCertificateKeyFile /etc/apache2/ssl/server.key
</VirtualHost>
```

- Nginx

```
server {
        listen 443 ssl default_server;
        listen [::]:443 ssl default_server;
        ssl_certificate /etc/nginx/certificate/nginx-
certificate.crt;
        ssl_certificate_key /etc/nginx/certificate/nginx.key;
        root /var/www/urlSitel;
        index index.html index.htm;
        server_name _;
        location / {
                try_files $uri $uri/ =404;
        }
}
```

Sécurisé son serveur Web

- Beaucoup de moyens disponible
  - pour sécuriser son serveur Web
- Tâche rigoureuse
- Système est connecté au réseau Internet

Protection simple

- Changer le port d’écoute du SSH
- Utiliser exclusivement le TLS en administration
- Ne pas administrer n’importe où
- Nettoyer les logiciels malveillants sur votre PC
- Mise à jour du serveur
- Maintenir vos propres applications
- Les paramètres de votre langage
- Les règles Apache ModSecurity
- Désactiver les services inutiles

Protection avancée

- Désactiver le suivi des requêtes HTTP
- Exécuter en tant qu'utilisateur et groupe séparés
- Désactiver la signature
- Désactiver la bannière
- Restreindre l'accès à un réseau ou une IP spécifique
- Utiliser uniquement TLS 1.2 ou +
- Désactiver la liste de l'annuaire
- Supprimer les modules inutiles
- Rester à jour

A retenir

- Un serveur d’applications est aussi
  - un élément à sécuriser

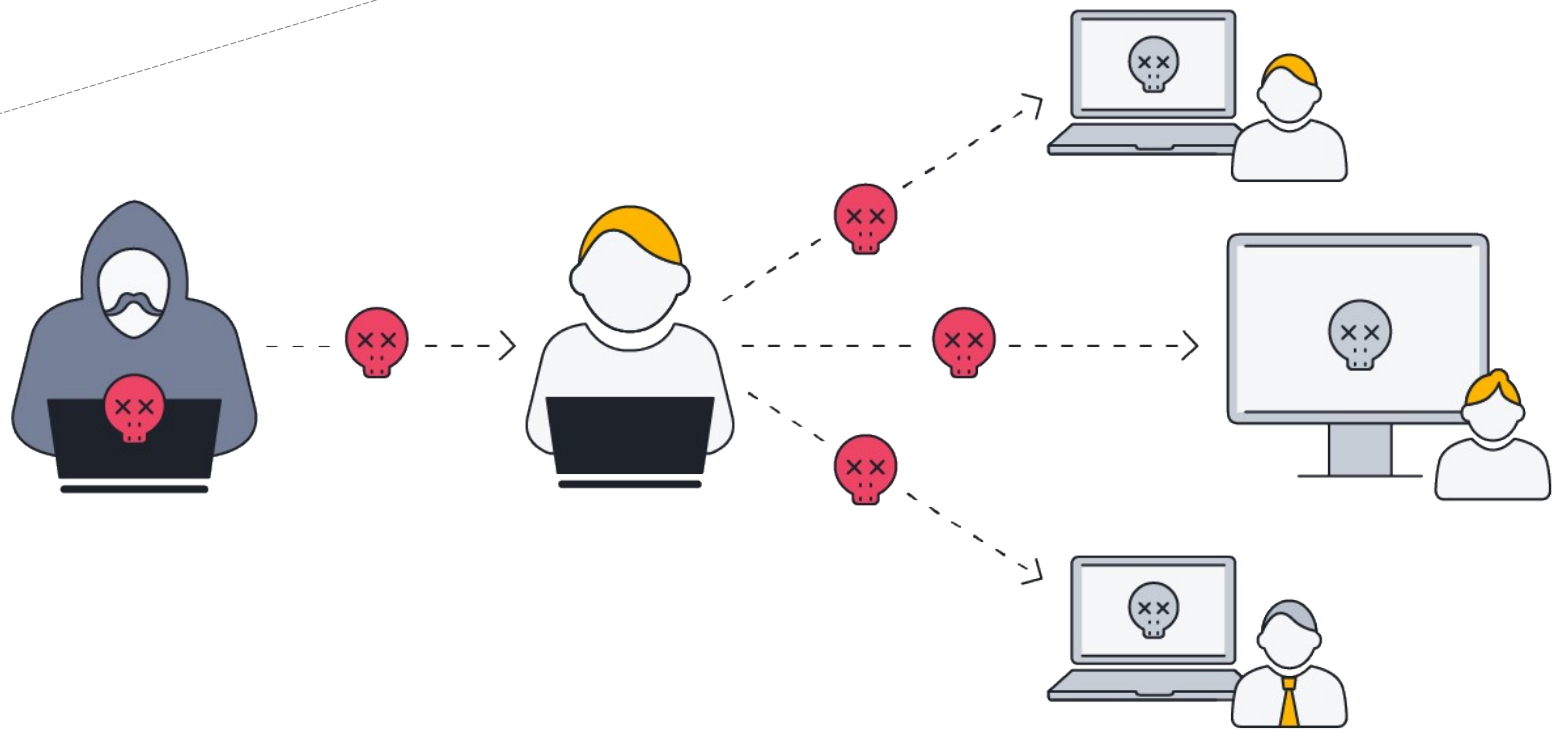
https://school.hello-design.fr

4E

- La sécurité du protocole IP
- Sécurisation d’un réseau
- Les bases de la cryptographie
- Serveurs applicatifs
- Les usurpations

Serveur proxy : Piratage d’un réseau

Quels sont les signes révélateurs ?
d'un piratage d'un réseau



Signe révélateur : → Rançongiciels

- Affichent en home page des sites
- Restreignent l’accès au contenu
  - tant que les victimes n’ont pas transféré le montant de la rançon aux pirates.

- Comment réagir :
  - Mettre en place un plan d’action
  - Sauvegarder leurs données et mettre en œuvre une solution de récupération

Signe révélateur : → l'ordinateur fonctionne tout seul

- Le curseur de la souris commence à se déplacer tout seul
- prise de contrôle par un élément extérieur
  - Ex : piratage de bureau à distance

- Comment réagir :
  - Déconnexion du réseau de tous les ordinateurs touchés
    - Actions :
      - Déterminer le point d'entrée
      - Surveiller le trafic réseau pour détecter toute activité suspecte
      - Exécuter un antivirus, de se déconnecter de tous les programmes ou services sur une machine infectée
      - Configurer de nouveaux mots de passe pour tout.

Signe révélateur : → messages étranges

- Proviennent pas du véritable titulaire du compte
- E-mails contiennent généralement des liens ou des pièces jointes infectés
- Plateformes de communication collaborative
  - Slack, Skype, Teams, Matrix,...
- Comment réagir :
  - Sensibilisés les collaborateurs
  - Identifié les techniques d’hameçonnage

Signe révélateur : → Fichiers subitement cryptés

- Les pirates chiffrent les fichiers pour en bloquer l'accès jusqu'à ce que les victimes paient les sommes demandées
- Peut de chance de pouvoir repérer des fichiers chiffrés
  - tant qu'il n'a pas cliqué dessus pour essayer de les ouvrir.
- Des mesures proactives doivent impérativement être prises pour se protéger des malwares.

- Comment réagir :
  - Restaurer les choses dans l'état préalable à leur chiffrement et à l'attaque,
  - Si absence de sauvegardes de fichiers
    - Appeler à des professionnels afin de déterminer si les données peuvent être déchiffrées
    - sans céder aux exigences des pirates.

Signe révélateur : → Etranges redirections

- Internaute est redirigé ailleurs que sur la page d'accueil habituelle
  - configurée dans les préférences de son navigateur
  - Atterrit sur des sites étranges lorsqu'il essaie de surfer, il est possible qu'un hacker se soit infiltré.
- Problèmes
  - Virus de redirection.
  - Placent les contenus demandés par des publicités

- Comment réagir :
  - Ne pas essayer de résoudre le problème sans avoir sauvegardé l'intégralité de ses données
  - Utiliser un logiciel de détection de redirection peut ensuite être utilisé

Actions pour assurer la pérennité de vos affaires

- Ayez une politique de sécurité en place
  - qui sera rigoureusement suivie par vos employés
- Faites régulièrement
  - la mise à jour de vos logiciels
- Ayez un excellent plan de sauvegarde
- Si vous doutez d'un lien/courriel
  - ne l'ouvrez pas
- Sécurisez tous les appareils qui sont connectés à Internet
- Vérifiez chaque support externe que vous branchez à votre réseau
  - clé USB...
- Chiffrez vos données les plus sensibles
- Ne déléguez pas seulement la sécurité à votre département IT
  - impliquez tous les employés
- Révisez votre plan de continuité d'affaires
  - Vous saurez quoi faire si vos systèmes sont compromis

Plus loin… Dans les applications

Usurpation d'identité via les cookies

- Comme toutes les applications
  - les applications web sont sujettes à des vulnérabilités.
- Faiblesse basée :
  - Sur les cookies
    - Un attaquant peut
      - contourner un mécanisme d'authentification.
  - Sur un code source mal développé
    - Un attaquant peut
      - contourner un mécanisme d'authentification
      - accéder à des données pour les divulguer ou les corrompre

Les cookies : Qu’est ce ?

- Fichiers gérés par les navigateurs web afin de stocker (et réutiliser)

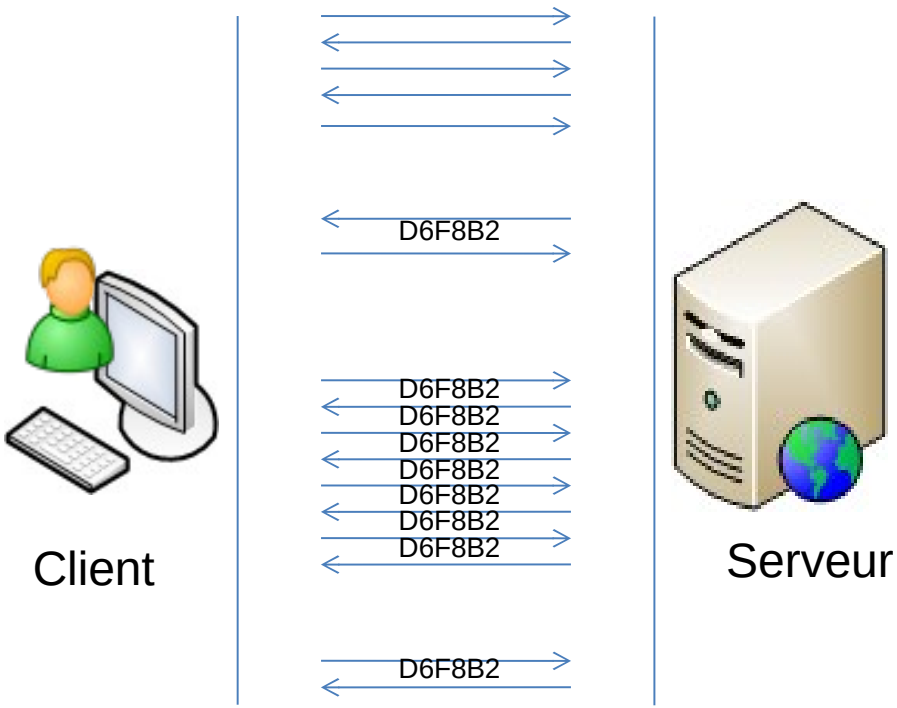
  des informations concernant l’utilisateur

  - par exemple :
    - son identifiant
    - ses préférences d’affichage et de disposition de la page web
- Sont nécessaires pour toutes les pages web dynamiques
  - qui nécessitent d’identifier ou d’authentifier l’utilisateur
  - Permet la mise en œuvre de sessions
    - les sites marchand
    - les sites bancaires
    - les sites « en général »

- Usurper l’identité d’un utilisateur sur un site web
  - Si récupération du cookie d’identification

Cookies : Fonctionnement

- Fonctionnement habituel d'une connexion sur un site web nécessitant une authentification
  - ex : site marchand, site bancaire...



1 - Phase d'authentification :
via un mot de passe en général

2 - Phase de génération du cookie d'identification [1]
L'utilisateur est maintenant connecté
→ A son compte

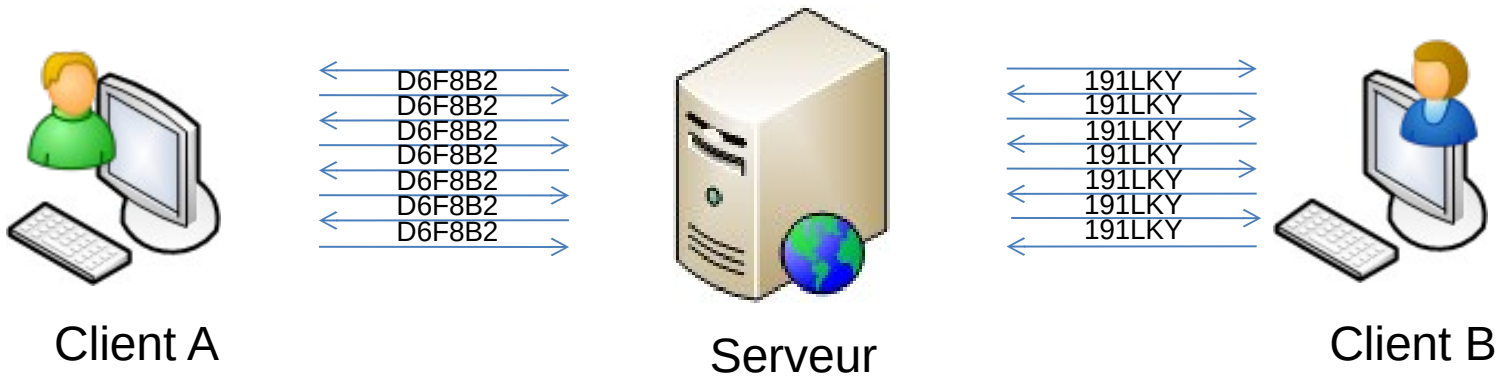
3 - Phase de « navigation »
Le cookie est inclus dans tous les échanges
afin que le serveur puisse identifier
la connexion de l'utilisateur

4 - Phase de déconnexion
la session de l'utilisateur est maintenant clôturée
Le cookie est invalidé

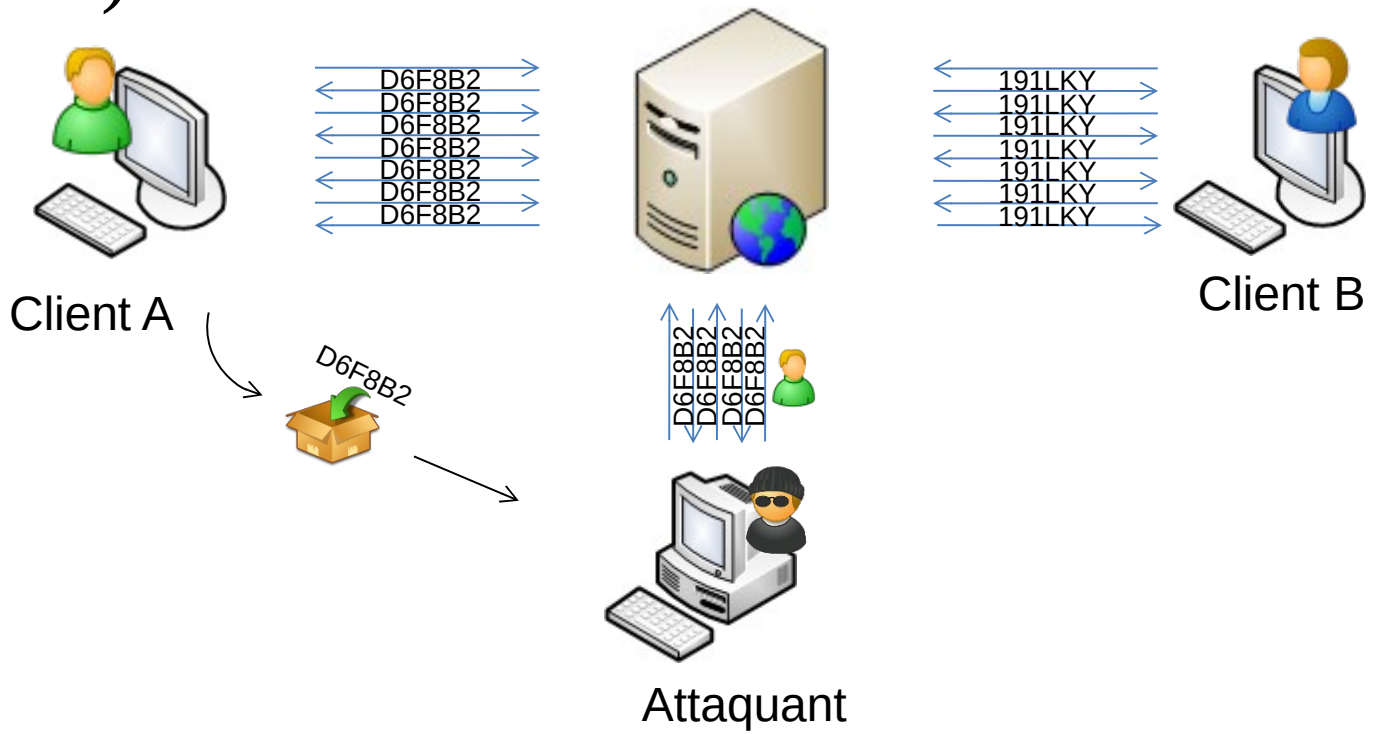
[1] Un cookie d'identification est en fait une chaîne de caractères aléatoire et unique suffisamment longue pour qu'elle ne puisse pas être générée deux fois par erreur.
Ex cookie d'identification : D6F8B2BE3ED3040D9A3C10-D6F8B2A305D048B9

Cookies : Vol (1/2)

- Pour chaque connexion
  - Un utilisateur du site web possède
    - son propre cookie, unique à lui.
  - Le serveur identifie à qui appartient chaque connexion
    - Affiche les pages web qui lui sont propre



Cookies : Vol (2/2)



- Hypothèse :
  - Un attaquant arrive à dérober le cookie d'un utilisateur et se connecte au même serveur ?
- Résultat :
  - Il se fait passer pour l'utilisateur
    - il a dérobé le cookie au près du serveur applicatif !
    - Il usurpe donc l'identité de la victime et accède à son compte

Cookie : Dérobé

- Différents moyens pour dérober un cookie d'identification :
  - Soit en écoutant le trafic réseau HTTP et en interceptant les données applicatives, dont le cookie

    - Moyen de protection : l'utilisateur doit **s'assurer que le site auquel il est connecté utilise du HTTPS** (le cookie est donc chiffré pendant le transport).
  - Soit en dérobant le cookie sur le poste de travail en utilisant une vulnérabilité du système

    - Moyen de protection : l'utilisateur doit **sécuriser son système d'exploitation et ses logiciels** correctement (services inutiles désactivés, installation des mises à jours de sécurité, anti-virus, etc. voir le module 2 pour plus d'informations).
  - Soit en dérobant le cookie sur le poste de travail via des méthodes d'ingénierie sociale ciblées sur l'utilisateur

    - Moyen de protection : l'utilisateur doit **être sensibilisé aux méthodes d'ingénierie sociale** (phishing, spam, etc.) afin de « ne pas tomber dans le panneau »
  - Soit en dérobant le cookie via une faille sur le serveur

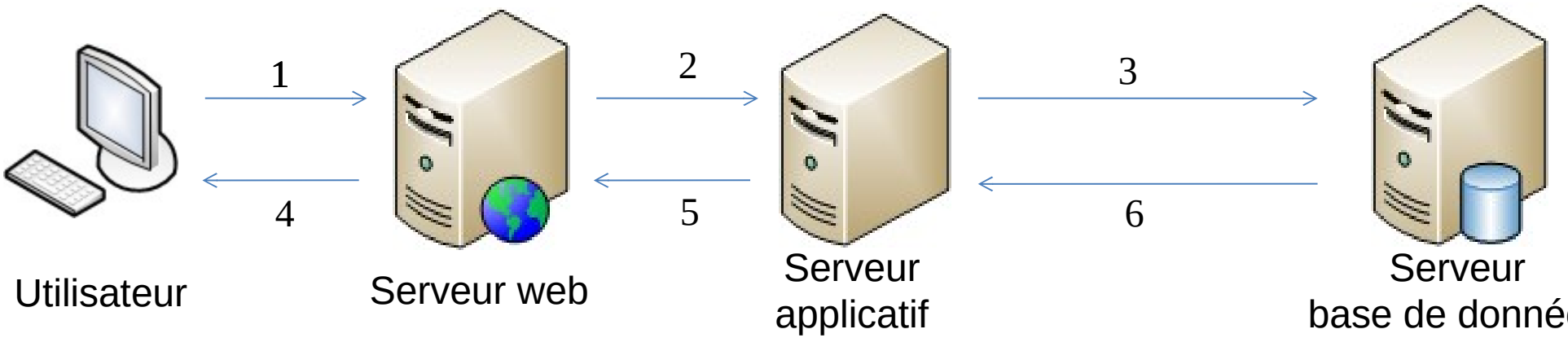
    - Moyen de protection : l'exploitant du serveur **doit suivre les bonnes pratiques de sécurisation et du maintien en condition de sécurité** du serveur, ainsi que les **bonnes pratiques de développement applicatif**

Injection SQL : Qu'est ce ?

- Permet à un attaquant d'interagir
  - directement avec la base de données d'un site web
- Objectif :
  - Contourner le mécanisme d'authentification
  - Accéder ou de modifier frauduleusement les données confidentielles de la base
    - Ex : mots de passe, téléphones, numéro de carte bancaire, etc.
- Multiples variantes possibles

Injection SQL : Exemple (1/4)

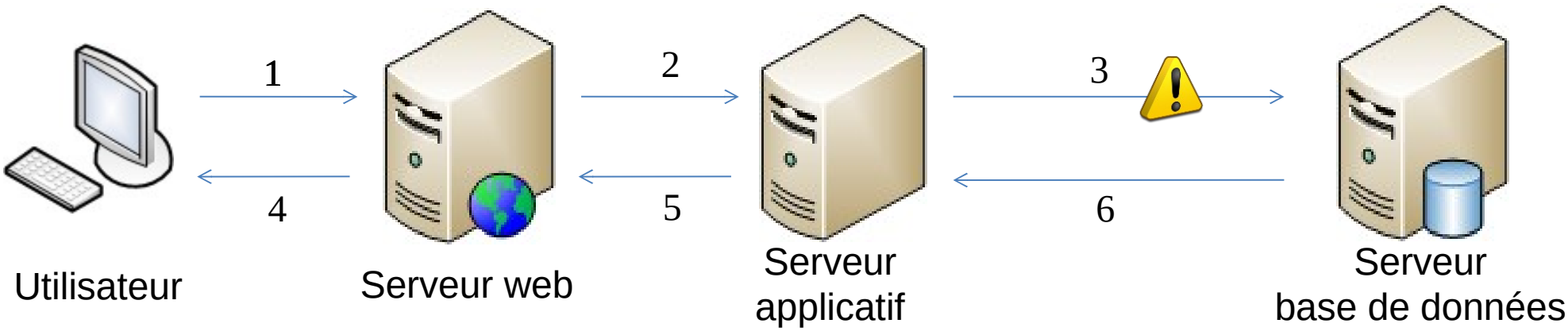
- Contournement d'authentification d'une page web
  - Architecture standard logicielle d'un site web faisant appel à une base de données



Légende :
1 - Le navigateur client demande l'affichage d'une page
2 - Le serveur web transfère la demande au serveur applicatif
3 - Le serveur applicatif génère une requête SQL afin de récupérer les informations nécessaires
4 - Le serveur base de données retourne le résultat de la requête au serveur applicatif
5 - Le serveur applicatif transmet au serveur web les informations nécessaires à la création de la page à afficher
6 - Le serveur web envoie les pages HTML au navigateur client

Injection SQL : Exemple (2/4)

- L'objectif d'une attaque de type injection SQL
  - Détourner la requête SQL de l'étape 3
  - But : créer sa propre requête SQL malveillante



Injection SQL : Exemple (3/4)

- Formulaire

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion :

$user contient le login renseigné dans le formulaire par l'utilisateur.
$mdp contient le mot de passe.

La requête SQL permettant de vérifier le login et le mot est la suivante :

```
select count(*) from user where user='$user' and mdp='$mdp'
```

Ainsi, une requête légitime serait la suivante :

```
select count(*) from user where user='thomas' and mdp='cykUfl9an'
```

Injection SQL : Exemple (4/4)

- Formulaire

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion :

Mais que se passe-t-il si un attaquant rentre précisément les chaines de caractères suivantes ?
Login : azerty
Mot de passe : abcd' or 1=1/*

La requête SQL select count(*) from user where user='$user' and mdp='$mdp'

devient donc :

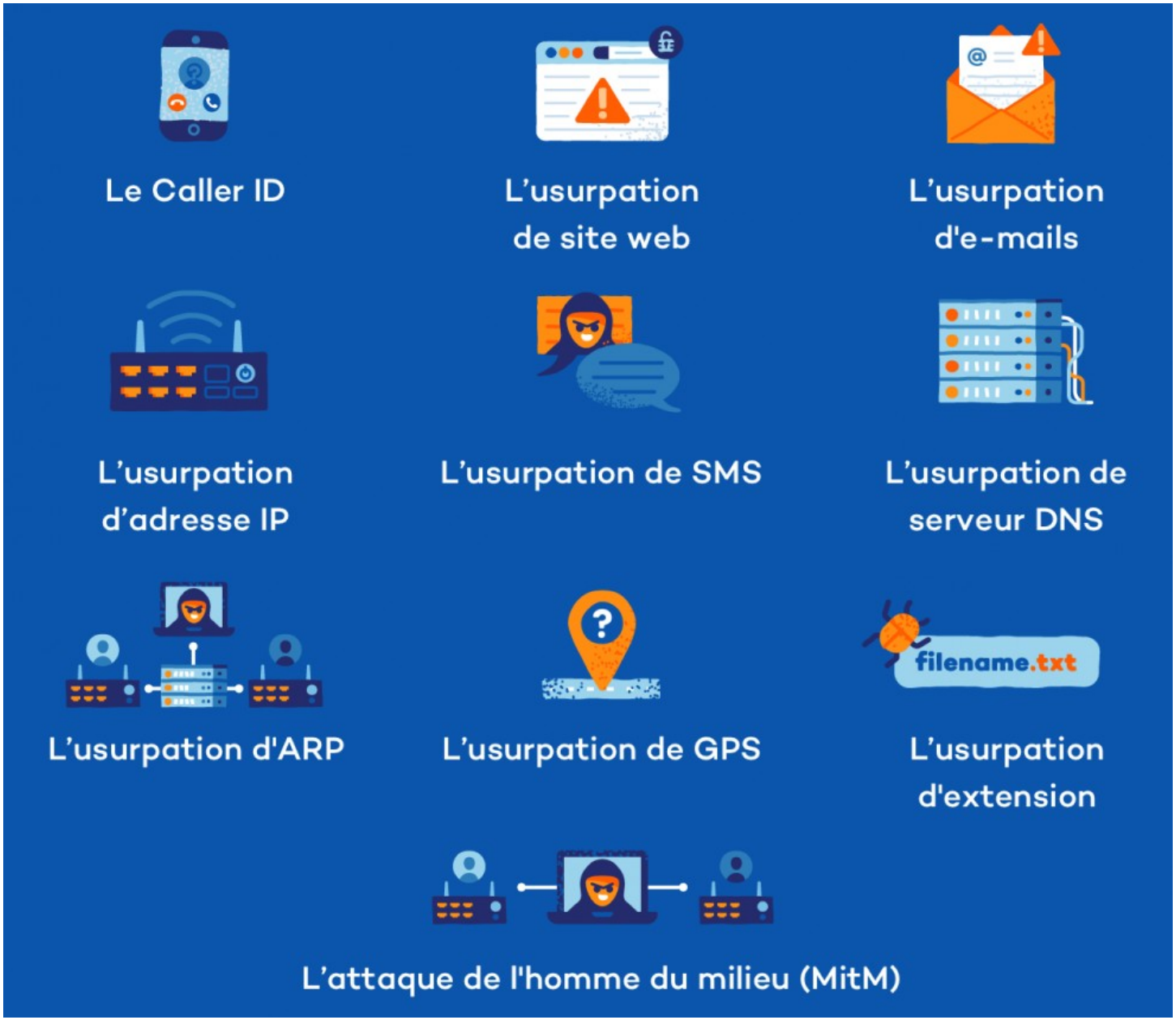
select count(*) from user where user='azerty' and mdp='abcd' or 1=1/*'

Cette condition est toujours vraie !

Injection SQL : Explication

- La condition étant toujours vraie
  - la requête est donc toujours valide
    - → quel que soit le mot de passe renseigné par l'attaquant !
      - Les caractères /* sont utilisés pour ignorer la fin de la requête légitime.
- La faiblesse réside ici dans le code applicatif
  - Les données renseignées par l'utilisateur ne sont pas vérifiées/validées
- Comment s'en protéger ?
  - Valider systématiquement chaque donnée extérieure avant de l'utiliser
  - Utiliser les requêtes préparées
    - Sous le nom de « prepared statements »
  - Respecter les bonnes pratiques de développement recommandées
    - par l'industrie concernant le code PHP, Java, etc.

Les différents types d’attaques d’usurpation d’identité



Usurpation d’identité via …!!… (1/2)

- Présentation du numéro (Caller ID)
  - Création de numéro de Tel/Nom par VoIP
- Usurpation de site web
  - Un faux site qui ressemble au vrai
- Usurpation d’e-mails
  - Envoie d’email avec de fausses adresses
- Usurpation d’adresse IP
  - Masquer l’emplacement
  - Faire croire à un ordinateur réel
- Usurpation de serveur DNS
  - Appelé empoisonnement de cache
  - Rediriger le trafic vers des adresses IP différentes

Usurpation d’identité via …!!… (2/2)

- Usurpation d’ARP (address Resolution Protocol)
  - Modifier/voler des données ou détournement de session
  - Accès Multimédia
- Usurpation de SMS
  - Envoie d’un SMS en utilisant un numéro de téléphone d’une autre personne
  - Généralement Phishing ou logiciels malveillants
- Usurpation de GPS
  - Diffusion de faux signaux GPS qui ressemblent à de vrais
  - Attaque sur les mobiles
- L’attaque de l’homme du milieu (MitM)
  - Un escroc pirate un réseau Wifi ou intercepter le trafic web
- Usurpation d’extension
  - Masquer les dossiers d’extension de logiciels malveillants
  - Cache les logiciels malveillants à l’intérieur de l’extension

Usurpation d’identité : Que faire ? (1/2)

- Ne communiquez jamais d’informations personnelles sensibles
- Marquez les copies des documents d’identité que vous transmettez
- Ne donnez que le minimum d’informations personnelles indispensables
- Faites attention à qui vous parlez sur Internet ou par téléphone
- Vérifiez les paramètres de confidentialité de vos informations personnelles
- Vérifiez régulièrement vos relevés de compte bancaire

Usurpation d’identité : Que faire ? (2/2)

- Conservez vos informations personnelles et bancaires ainsi que vos documents d’identité en lieu sûr
- Détruisez tous les documents qui contiennent des informations personnelles avant de les jeter
- Utilisez des mots de passe différents et complexes pour chaque site et application
- Activez la double authentification
- N’ouvrez pas les messages suspects et leurs pièces jointes, et ne cliquez jamais sur les liens
- Mettez régulièrement à jour vos appareils et leurs logiciels ou applications

A retenir

- L’usurpation n’est pas
  - un phénomène occasionnel
- Les techniques des escrocs sont toujours
  - A la recherche d’une nouvelle technique

https://school.hello-design.fr

4D

TP 4

- Deadline
  - Le 22 mars 2023 23:59
- Énumération structurée (avec détails)
  - Tous les formats acceptés
    - ODT, Docx, PDF, Markdown…
- Sujet :
    - Identifier les piliers techniques et non techniques de la sécurité de réseau ?

Rendez-vous au prochain cours

- Merci de votre attention