Ecole de Management Strasbourg

UNIVERSITÉ DE STRASBOURG

www.em-strasbourg.eu

Module 3: Sécurité logique du S.I.

(Parties 1 et 2)

Novembre 2019

Sommaire

(Partie 1/2)

I) Introduction – panorama et évolution des menaces

- la sophistication des menaces

II) Les principes clé assurant la sécurité logique du S.I.

- “need-to-know” / “least privilege”
- ségrégation des tâches
- défense en profondeur

III) Authentification et Cryptographie

- les bases techniques
- applications pratiques:

TLS / HTTPS, signature électronique, authentification forte, non-répudiation, horodatage sécurité, SSH, hachage…

IV) Mesures techniques pour sécuriser le S.I.

- Applications Métier
- Systèmes d’exploitation et postes de travail
- Réseaux
- Bases de données
- Plateformes virtualisées

© 2019 Jean-Claude Héritier

Sommaire

(Partie 2/2)

V) Cas pratique : protection contre les fuites de données

VI) Sécurité des applications Web

VII) Sécurité et technologies émergentes

- BYOD
- Cloud computing
- Réseaux sociaux

VIII) L'investigation numérique légale (« Digital forensics »)

IX) Sécurité physique du S.I.

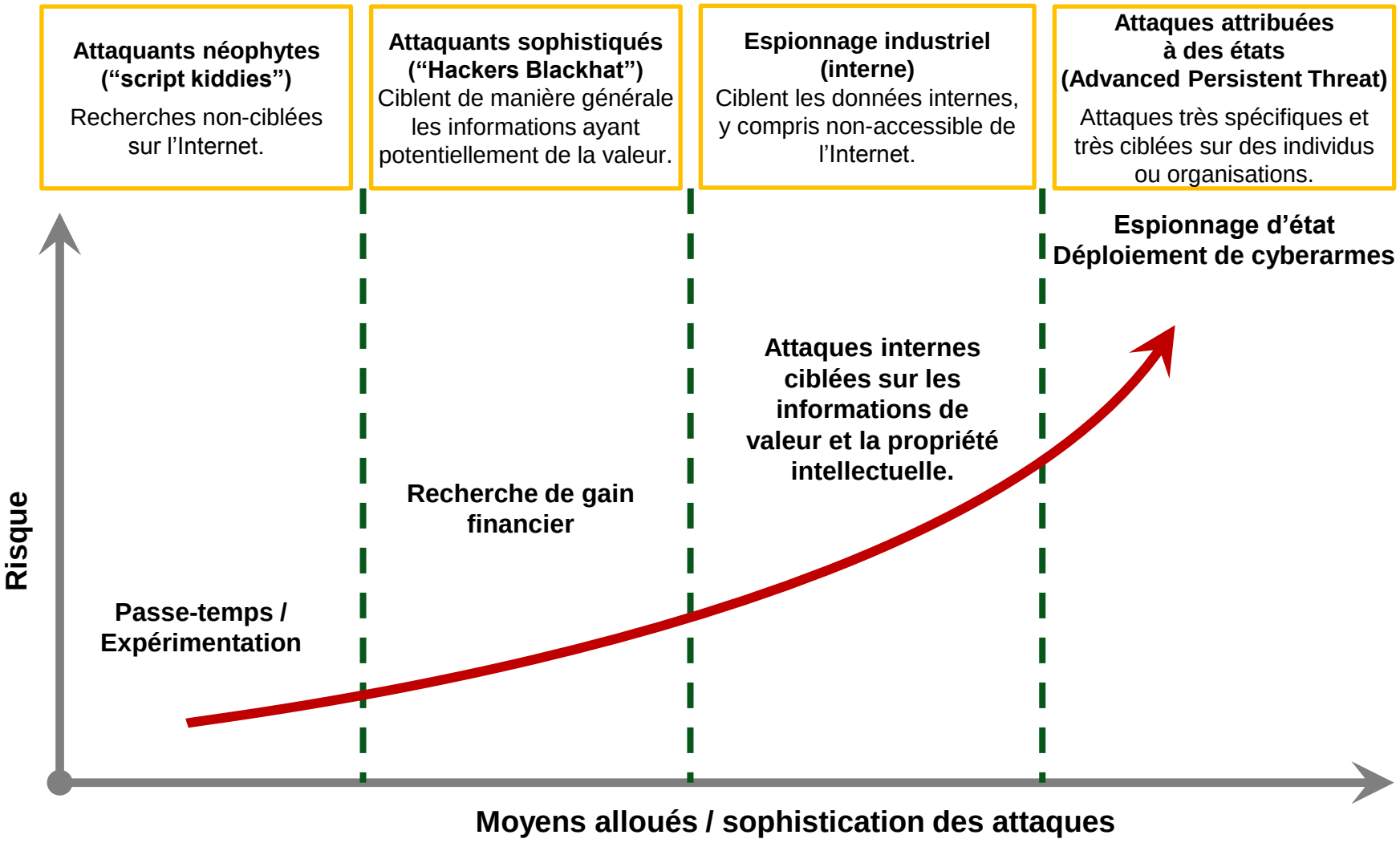
© 2019 Jean-Claude Héritier

I) Introduction – panorama et évolution des menaces

- La sophistication des menaces

© 2019 Jean-Claude Héritier

La sophistication des attaques



© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

La sophistication des attaques (« Advanced Persistent Threats »)

Vulnérabilité	Solution de sécurité initiale	Adaptation des vecteurs d'attaque
Faiblesses liés à une authentification à simple facteur (ex: identifiant + mot de passe). Fiabilité relative des mots de passe (peuvent être compromis ou devinés).	Authentification forte (multi-facteurs). Ex: identifiant + mot de passe + mot de passe à usage unique (OTP)	Attaque ciblée par phishing du fournisseurs de solution OTP (RSA, mars 2011) et vol des clés de chiffrement utilisées par la cible réelle de l'attaque (Lockheed Martin, attaqué en mai 2011)
Code malveillant masqué sous une apparence de code reconnu (ex: Adobe)	Certificats numériques pour "signer" le code et vérification des certificats par les systèmes d'exploitation ou les navigateurs web avant exécution.	Attaque d'un vendeur dont les applications sont exécutées sur un grand nombre de machines (ex: Adobe) et utilisation de son infrastructure de signature pour signer du code malveillant (sept. 2012).
Bases de signatures antivirus ne pouvant plus suivre le rythme des nouveaux malware (plus de 200.000 nouvelles signatures par jour).	"Liste blanches" des applications autorisées, rejet de toutes les autres. (ex: "software restriction policies" dans Windows Server 2003 & 2008)	Attaque de la solutions de signature d'un vendeur (Bit9) et utilisation pour signer du code sur la liste blanche des clients de la société (inclus Agences Gouvernementales U.S.) (fev. 2013).

© 2019 Jean-Claude Héritier

Introduction - Panorama et évolution des menaces

• Liens et références

- **ANSSI – rapport annuel 2018**
  - https://www.ssi.gouv.fr/uploads/2019/04/anssi_rapport_annuel_2018.pdf

- **Verizon –** *2018 Data Breach Investigations Report*
  - https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Heartbleed – *Faille de sécurité OpenSSL*
- http://www.heartbleed.fr/

Shellshock – *Faille de sécurité dans le Shell Bash*
- https://linuxfr.org/news/une-faille-nommee-shellshock

Tyupkin – *Manipulation des distributeurs de billets par un malware*
- https://securelist.com/blog/research/66988/tyupkin-manipulating-atm-machines-with-malware/

Kaspersky - *Cyberthreat real-time map*
- https://cybermap.kaspersky.com/

© 2019 Jean-Claude Héritier

II) Les principes clé assurant la sécurité logique du S.I.

- “need-to-know ” / “least privilege”
- ségrégation des tâches
- défense en profondeur

© 2019 Jean-Claude Héritier

Principe #1 – “need-to-know ” / “least privilege”

- **Principe de base :**
  - **Tout accès à l’information doit être justifié par un besoin raisonnable (« selon les besoins »)**
    - En ligne avec la Classification de l’Information (notion d’habilitation).
    - En ligne avec les besoins Métier.
  - **Par défaut, l’accès doit être restreint, supervisé ou non-autorisé.**
    - Mesures organisationnelles
    - Restrictions techniques (« principe du moindre privilège »)

Exemples

© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

Principe #1 – “need-to-know ” / “least privilege”

Exemples	Y a-t-il un risque de sécurité logique?	Amélioration possible ?
1) Lors d’un transfert interne, la procédure consiste à supprimer manuellement les accès de l’individu transféré aux répertoires partagés sur le réseau interne qui ne sont plus nécessaires, sur base de l’inventaire tenu par l’équipe en charge de la gestion des accès.	Facteurs de risque: - Inventaire manuel. - Suppression manuelle. *-> Risque d’erreurs humaines et pour conséquence des accès inappropriés qui persistent,*	Gestion des accès aux répertoires partagés par groupes plutôt que par individus. Définition d’un propriétaire pour chaque répertoire partagé. Re-certification périodique des accès par les propriétaires. Contrôle par le RSSI des suppressions d’accès .
2 a) L’ancien responsable de l’équipe gérant les accès aux répertoires partagés de toute l’entreprise est désormais employé à plein temps par le service Ressources Humaines. Ses anciens accès ont été révoqués. Afin d’alléger la charge de travail de son ancienne équipe, il a toutefois conservé des privilèges lui permettant de gérer les droits d’accès sur le partage réseau des Ressources Humaines (par exemple lors de l’arrivée de stagiaires ou d’intérimaires).	Semble a-priori aligné avec les besoins… mais il faut creuser pour confirmer que des accès supplémentaires ne persistent pas…	Confirmer que des accès supplémentaires ne persistent pas ici ou là, en particulier sur les répertoires réseau de son ancienne équipe… *Vérifier de quels groupes il fait partie.* *Vérifier les accès de ces groupes.*
2 b) Ses anciens accès ont été révoqués, excepté un accès en lecture aux répertoires réseau de son ancienne équipe afin de pouvoir consulter les demandes d’accès à venir.	Présence de données sensibles sur els répertoires réseau de son ancienne équipe? *(par ex. fichier de mots de passe, gestionnaire de mots de passe, etc.)*	Réduire les accès aux répertoires réseau non-requis. Re-certification des accès,

© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

Principe #1 – “need-to-know ” / “least privilege”

Exemples	Y a-t-il un risque de sécurité logique?	Amélioration possible ?
3) Afin de pouvoir passer certaines écritures comptables en fin d’année, les trois responsables du service disposent d’un menu de « dépannage » autorisant les mouvements sur tous les types de comptes.	Besoin temporaire <-> Accès permanent? Accès restreint uniquement aux personnes appropriées?	Utilisation de comptes dédiés activés en cas de besoin et suivis en terme d’utilisation. Contrôle a-posteriori des activités de ce compte (ex: journal d’audit)
4) Des consultants externes sont fréquemment amenés à travailler pour divers services et ont besoin de consulter les informations relatives à de nombreux projets. Pour simplifier la gestion des accès trop lourde, le service informatique leur a attribué un accès en lecture seule au serveur SharePoint sur lequel les informations relatives à tous les projets en cours sont présentes.	Besoin limité <-> Accès complet? Lecture seule -> n’empêche pas la perte de confidentialité. Présence de données sensibles?	Préférer un répertoire dédié dans lequel l’information demandée est déposée en fonction des besoins. Valider la mise à disposition avec le propriétaire de l’information. Considérer la mise à disposition via des postes de travail sécurisés si documents sensibles (ex: pas d’impression, filtrage des accès Internet, etc.
5) Plusieurs employés en congé de longue durée disposent toujours d’un profil utilisateur actif sur le réseau interne.	Possibilité d’accès au S.I.	Désactivation des accès automatique si aucune activité au-delà de x jours (par exemple par script). **Ou** Contrôle détectif périodique par le RSSI (requête PowerShell qui retourne les utilisateurs actifs mais non-utilisés depuis x jours)

© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

Principe #1 – “need-to-know ” / “least privilege”

Exemples	Y a-t-il un risque de sécurité logique?	Amélioration possible ?
6.a) Découvrant une fraude interne potentielle, la Direction décide de limiter les risques d’accès aux données de l’entreprise en révoquant immédiatement les accès physiques des employés concernés au site de l’entreprise.	Quid des accès à distance?	Désactivation des accès logiques / Désactivation des accès distants (VPN). *(combinaison de mesures techniques et organisationnelles)*
6.b) Elle décide aussi de faire désactiver les comptes utilisateurs de tous les employés concernés sur le contrôleur de Domaine.	Quid des accès applicatifs?	Désactivation des accès logiques également au niveau des applications (les plus sensibles en premier).

Quels challenges?

Trouver le juste équilibre
-> le plus complexe

Maintenir le « need to know » dans le temps

Accès des administrateurs (inventaire à jour)

Personnel externe / sous-traitant

Besoins d’accès « temporaires »
(ex: remplacement / dépannage, etc.)

Etc.

© 2019 Jean-Claude Héritier

Sécurité logique - Introduction
Principe #2 – « Ségrégation des tâches »

- **Principe de base :**
  - **Impliquer au moins deux personnes sur les opérations présentant un risque important (« maker / checker »)**
    - Limiter les risques d'erreurs humaines
    - Limiter le risque de fraude

Deux personnes

- Employé A et Employé B -> ségrégation au niveau individuel.
- Département 1 et Département 2 -> ségrégation au niveau processus.

Ségrégation opérationnelle
-> exemple: signature obligatoire pour valider une opération.

⟺

Ségrégation technique (contrôle « hardcodé »)
-> ex: principe des 4 yeux dans une application Métier.

Doit être supportée par…

opérations présentant un risque important

Exemples:

- Opérations de paiements **+** Gestion des accès aux applications de paiement
- Rôles au sein de la fonction informatique: gestion des bases de données, développement, mise en production, etc.
- Banque: Front Office // Middle Office // Back Office (cf pages suivantes)
- **SAP:** Création d'un nouveau fournisseur (ex: SAP SR01) // Insertion de facture dans le batch de paiement (SAP SR03)
- Gestion du paramétrage VS Exécution du contrôle (ex: gestion des limites, gestion des règles de réconciliation, etc.

A retenir: Constitue un contrôle opérationnel clé.

Peut entraîner des contraintes organisationnelles -> nécessité d'une approche basée sur les risques

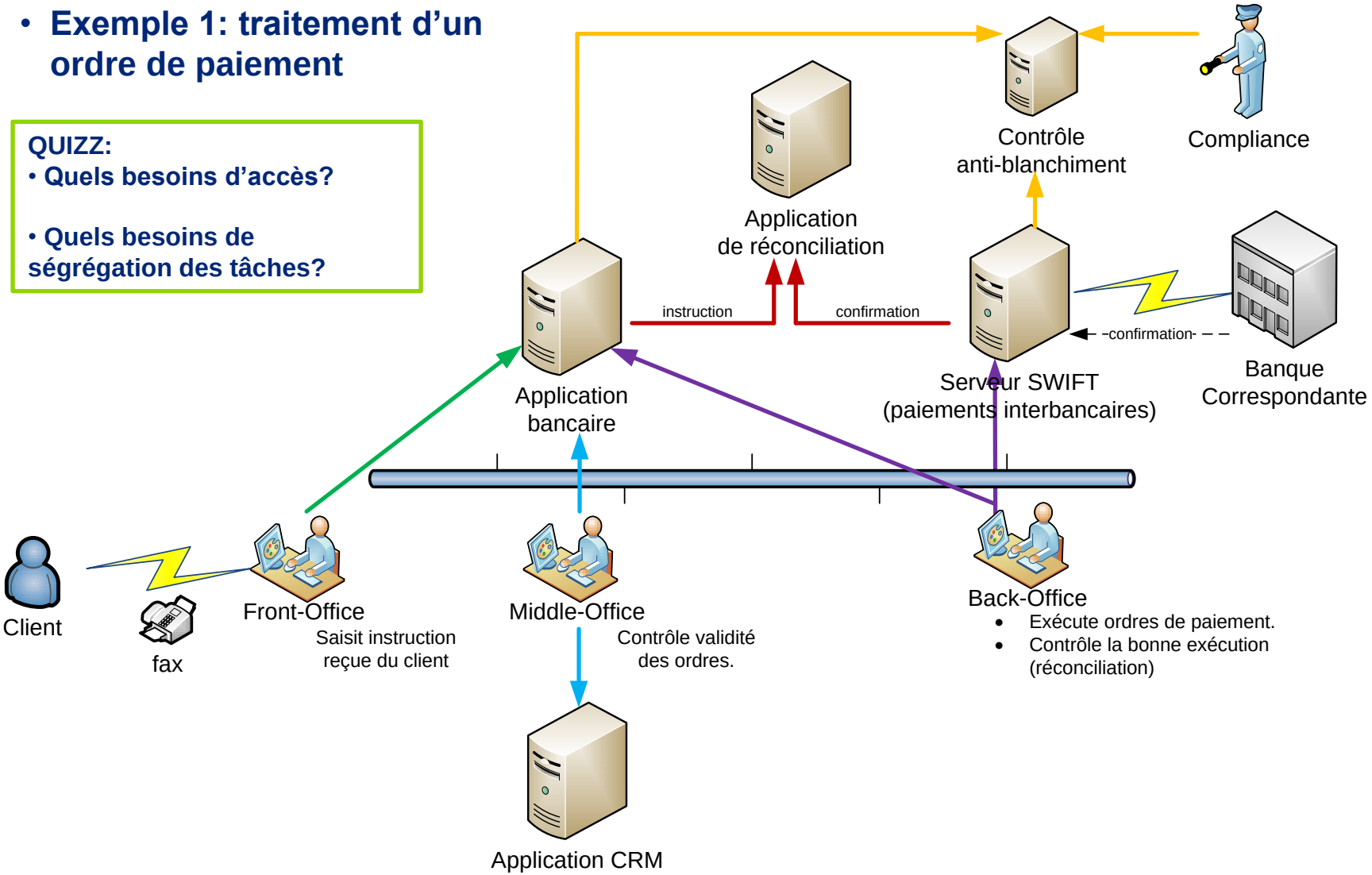
© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

Principe #2 – « Ségrégation des tâches »

- **Exemple 1: traitement d'un ordre de paiement**

QUIZZ:
- **Quels besoins d'accès?**
- **Quels besoins de ségrégation des tâches?**



© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

Principe #2 – « Ségrégation des tâches »

A nuancer au cas par cas.

- **Exemple 1 (suite): traitement d'un ordre de paiement et ségrégation des rôles**

	Application bancaire	Application CRM	Serveur SWIFT (paiements interbancaires)	Application de réconciliation	Contrôle anti-blanchiment
Front-Office	Saisie des ordres ✓ Validation des ordres ✗	Lecture seule ✗ Accès restreint à ses clients.	Pas d'accès ✗	Pas d'accès ✗	Pas d'accès ✗
Middle-Office	Saisie des ordres ✗ Validation des ordres ✓	Accès complet (lecture / écriture)	Pas d'accès ✗	Lecture seule ✗	Lecture seule ✗
Back-Office	Saisie des ordres ✗ Validation des ordres ✓	Lecture seule ✗	Accès complet **(modification des paiements sous 4-yeux)** ✓	Accès complet **(modification du paramétrage restreinte)**	Lecture seule ✗
Compliance	Saisie des ordres ✗ Validation des ordres ✗	Lecture seule ✗	Pas d'accès ✗	Pas d'accès ✗	Accès complet (lecture / écriture)

© 2019 Jean-Claude Héritier

Principe #2 – « Ségrégation des tâches »

- **Exemple 2 - ségrégation au sein de la fonction informatique**

1. Ségrégation du service informatique vis-à-vis des autres services:

Exemples:
- Maintenance
- Gestion de la sécurité
- Administration système
- Développement
- Mises en production
- Etc.

Service Informatique

Tous les autres services

Exemples
- Responsabilités opérationnelles.
- Validation des changements.
- Définition du paramétrage des applications
- Etc,

Ségrégation entre services
(ex: droits d'accès distincts entre les services pour éviter les combinaisons «toxiques»)

2. Ségrégations attendues au sein du service informatique:
(en fonction de l'analyse des risques)

Responsable du Service Informatique (CIO)

Equipe Développement

Administration des bases de données (DBA)

Sécurité de l'information

Equipe Exploitation

Développement initial des applications

Maintenance des applications existantes

Gestion de l'infrastructure

Support Utilisateur

Traitement des données

La ségrégation doit se retrouver au niveau de l'organisation du service IT.

QUIZZ: quelles limites?

© 2019 Jean-Claude Héritier

Principe #3 - Défense en profondeur

- **Objectif: présenter des lignes de défense multiples et indépendantes face aux menaces**

La sécurité ne doit pas reposer sur un élément (« single point of failure ») mais sur un ensemble cohérent de mesures de sécurité.

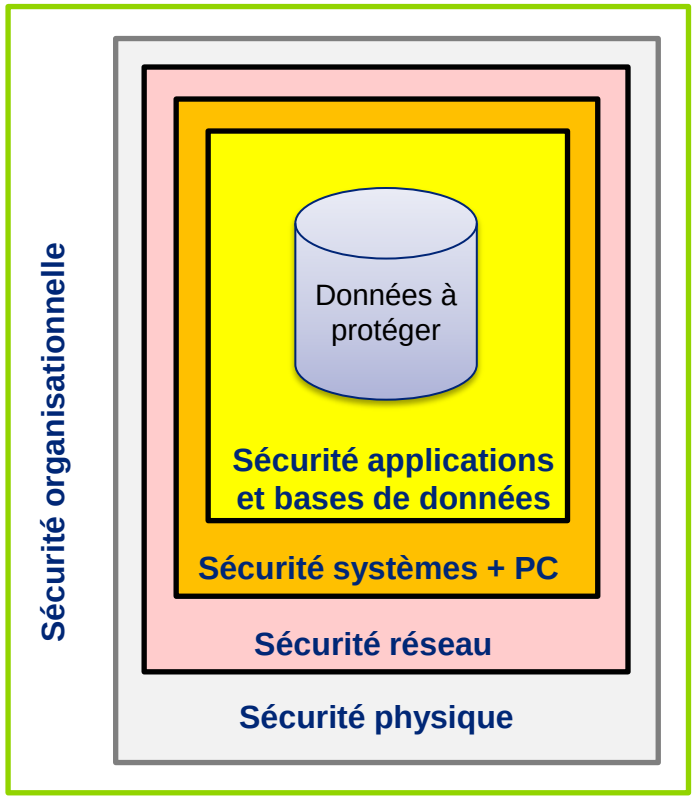
Eléments requis:

• Existence de **plusieurs lignes de défense indépendantes autour des ressources critiques** (la sécurité d'une ligne n'a pas pour pré-requis la sécurité de la ligne précédente)

• Mise en place supportée par une **analyse des risques** , qui fixe des objectifs de sécurité (prise en compte de scénarios).

• Combinaison de mesures **préventives** (mécanismes d'alerte) et **correctives** (procédures de réaction).

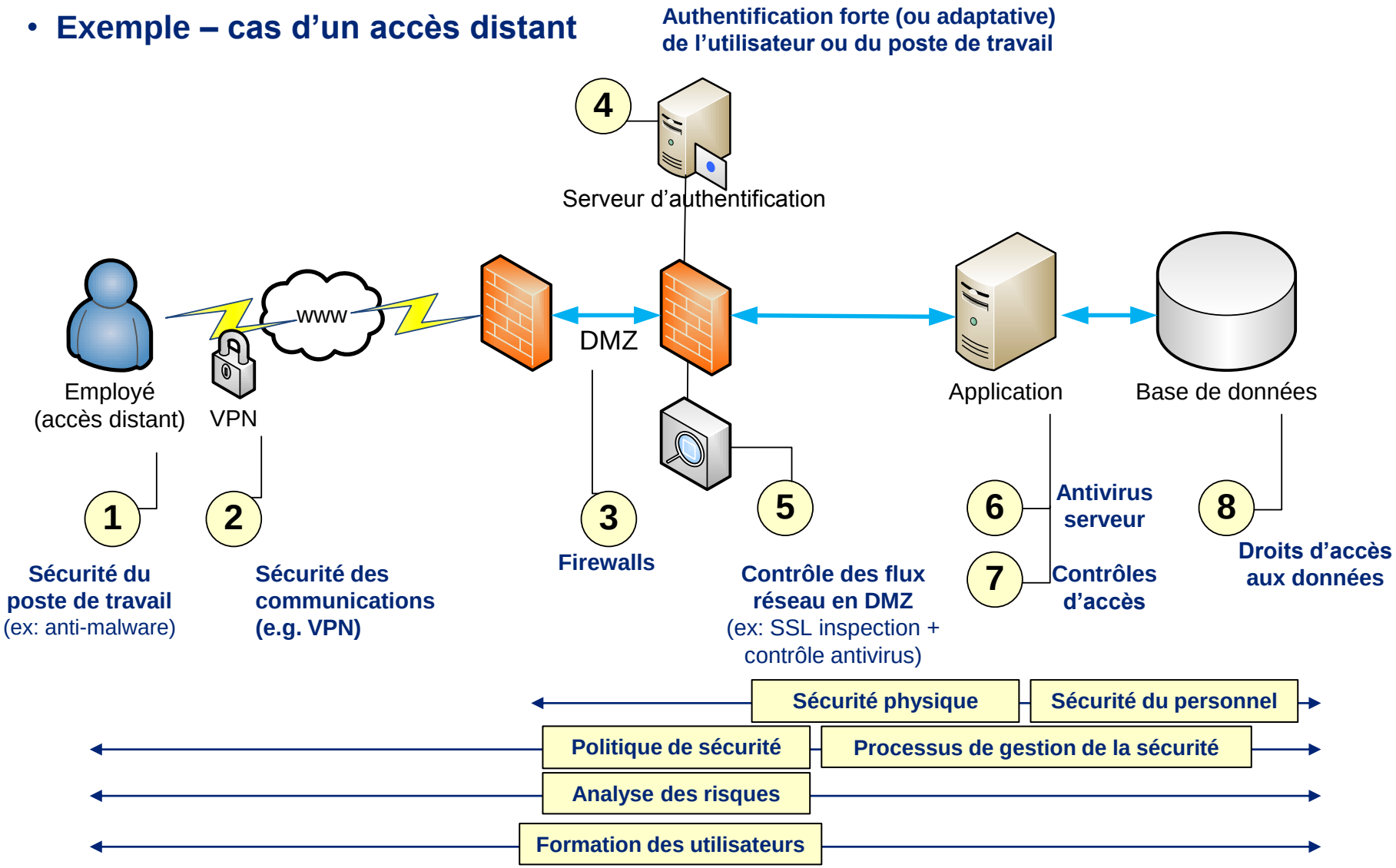
• Englobe toutes les dimensions de la sécurité du S.I.
- Aspects techniques
- Aspects organisationnels
- Aspects humains



© 2019 Jean-Claude Héritier

Principe #3 - Défense en profondeur

- **Exemple – cas d'un accès distant**



© 2019 Jean-Claude Héritier

Sécurité logique – Introduction
Illustration: quelques exemples d'attaques récentes

1. NSA / Edward Snowden

- Sous-traitant et administrateur système de la NSA , disposant d'un accès distant (Honolulu).
- Habilitation « Top-secret » (comme 1.4 millions de personnes en Octobre 2012*)

Vulnérabilité possible:
Elévation de privilèges par la création de clés numériques (SSH? Certificats auto-signés?), puis accès à des documents classifiés et copie non-autorisée.

Contre-mesures prises par la NSA après la publication de documents classifiés:**
- Licenciement potentiel de 90% des administrateurs systèmes de la NSA (de ~1000 personnes à ~100).

-Surveillance renforcée sur les administrateurs système: **« two-man rule »** (voire **« three-man rule »** selon certaines sources).

- Automatisation des flux de travail – remplacement accéléré des administrateurs systèmes par des machines.

Sources: * Office of the Director of National Intelligence - 2012 Report on Security Clearance Determinations
** http://www.reuters.com/article/2013/08/09/us-usa-security-nsa-leaks-idUSBRE97801020130809

2. OVH (juillet 2013):

- un hacker a réussi à obtenir les accès sur un compte e-mail d'un des administrateurs système.
- grâce à cet accès email, il a obtenu l'accès sur le VPN interne d'un autre employé.
- Puis grâce à cet accès VPN, il a fini par compromettre les accès de l'un des administrateurs système qui s'occupe du backoffice interne.

Objectifs du hackeur selon OVH:
- récupérer la base de données des clients Europe.
- gagner l'accès sur le système d'installation de serveurs au Canada.

Vulnérabilités:
- Authentification VPN uniquement basée sur mot de passe.
- Accès aux e-mails internes sans passer par le VPN (?)

Contre-mesures prises par OVH après l'attaque:
- Re-génération des mots de passe de tous les employés.

- Nouvelle solution VPN et sécurité physique renforcée.

- Restrictions d'accès aux e-mails internes (uniquement depuis Bureau ou via VPN).

- Authentification VPN **2-facteurs** via mot de passe et token hardware personnel (Yubikey).

Source: OVH http://travaux.ovh.net/?do=details&id=8998

© 2019 Jean-Claude Héritier

Sécurité logique - Introduction

- **Liens et références**

Ségrégation des tâches

– **BDO Consulting –** *Segregation of duties checklist*
  - http://www.covesys.com/docs/appnotes/segdutieschecklist-%20sod.pdf

– *Segregation of Duties conflicts in SAP environment*
  - em-strasbourg.duckdns.org/cours/r%C3%A9f%C3%A9rentiels/SOD/SAP%20GRC%20SOD%20Conflicts%20High%20Risk.xlsx

Défense en profondeur

– **ANSSI -** *Mémento sur le concept de la défense en profondeur appliqué aux S.I.*
  - http://www.ssi.gouv.fr/IMG/pdf/mementodep-v1-1.pdf
    (inclus une méthode de défense en profondeur et un exemple d'application de la méthode proposée)

© 2019 Jean-Claude Héritier

III) Authentification et Cryptographie

- les bases techniques pour la sécurité logique
- applications pratiques

© 2019 Jean-Claude Héritier

Cryptographie

–

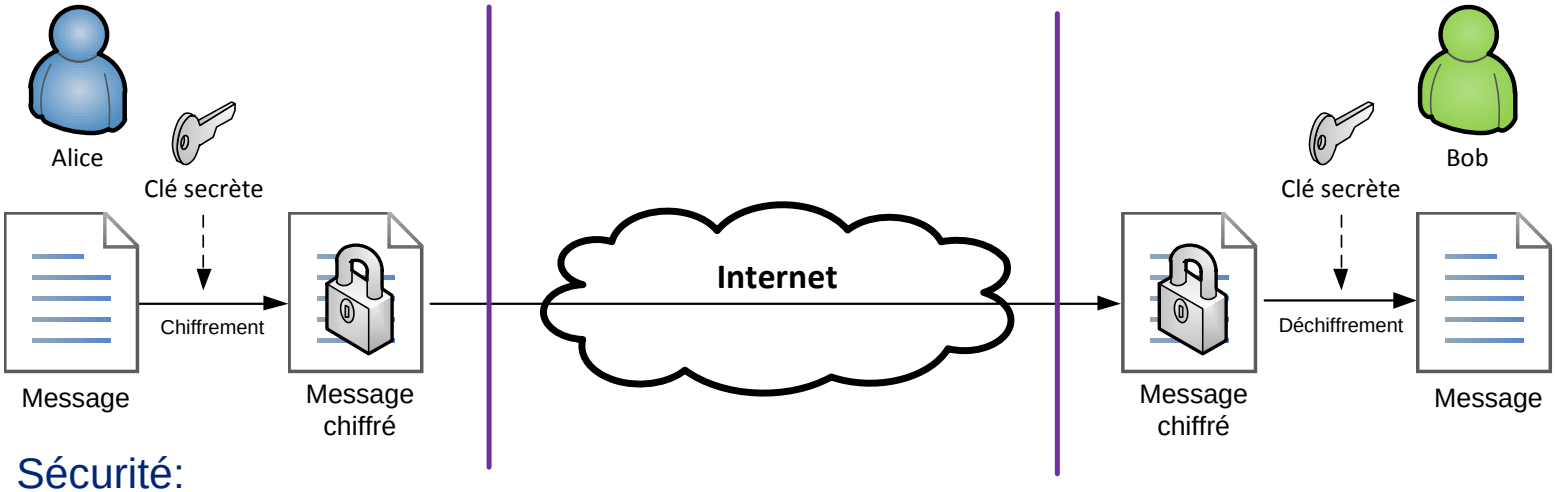
les bases techniques

© 2019 Jean-Claude Héritier

Introduction à la cryptographie

Chiffrement symétrique (« chiffrement à clé secrète ») (1/2)

Principe: algorithmes utilisant une clé identique pour le chiffrement et le déchiffrement.



Sécurité:

- **Confidentialité** ✓
- **Intégrité*** ✗
- **Authentification** ✗
- **Non-répudiation** ✗

* Propagation d'erreurs, mais des manipulations ciblées peuvent passer inaperçues.

Avantages:

- Simplicité du processus
- Sécurité (selon longueur de la clé)
- Haute performance

Problèmes:

- Gestion des clés secrètes:
  - Echange de la clé secrète.
  - Nombre de clés requises peut devenir problématique:

Partenaires / Nombre de clés

- 2 -> 1 clé
- 3 -> 3 clés
- 4 -> 6 clés
- 10 -> 45 clés
- 100 -> 4950 clés
- 1000 -> 495500 clés
- etc.

Exemples d'algorithmes de chiffrement symétriques:

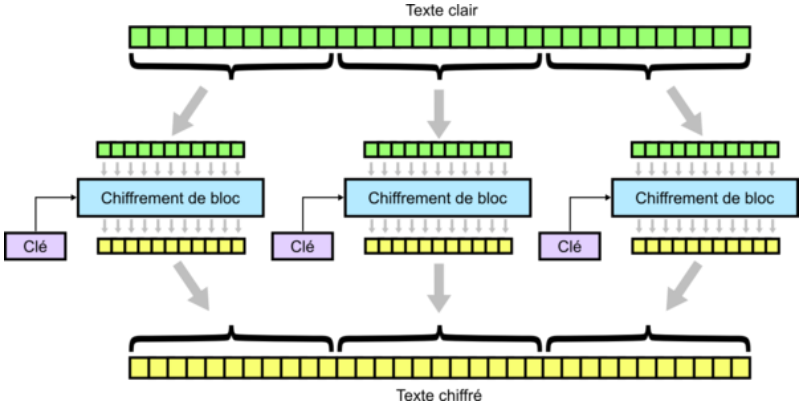
- par blocs (block ciphers) -> Twofish, Blowfish, DES & 3DES, **AES**, IDEA, RC5, etc.
- par flux (stream ciphers) -> **RC4** (utilisé par exemple par le protocole WEP du wi-fi)

© 2019 Jean-Claude Héritier

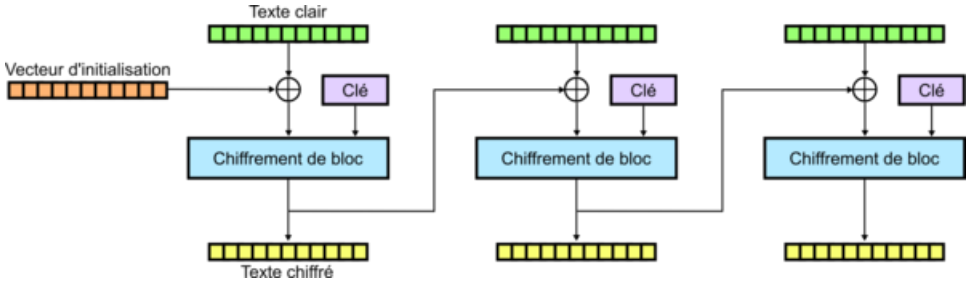
Chiffrement symétrique (« chiffrement à clé secrète ») (2/2)

A savoir: Impact du mode d'opération en cryptographie symétrique.

Certains modes de chiffrement sont plus vulnérables que d'autres:



Chiffrement en mode ECB Fortement déconseillé



Enchaînement des blocs : « Cipher Block Chaining » (CBC)

Exemple:

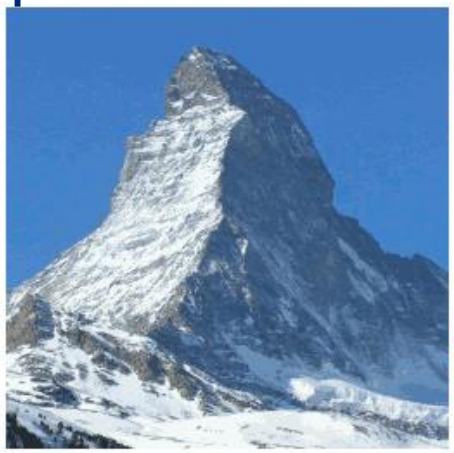
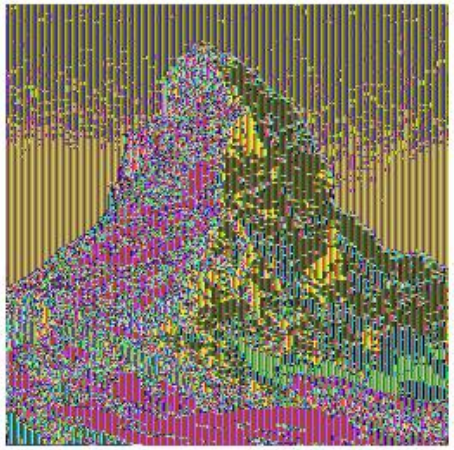
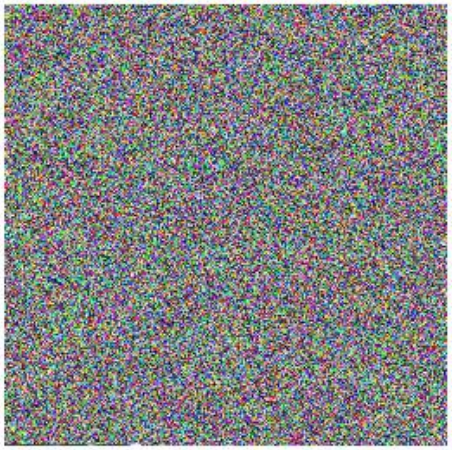


Image originale



Chiffrement en mode ECB



Chiffrement avec un mode sûr (autre que ECB)

© 2019 Jean-Claude Héritier

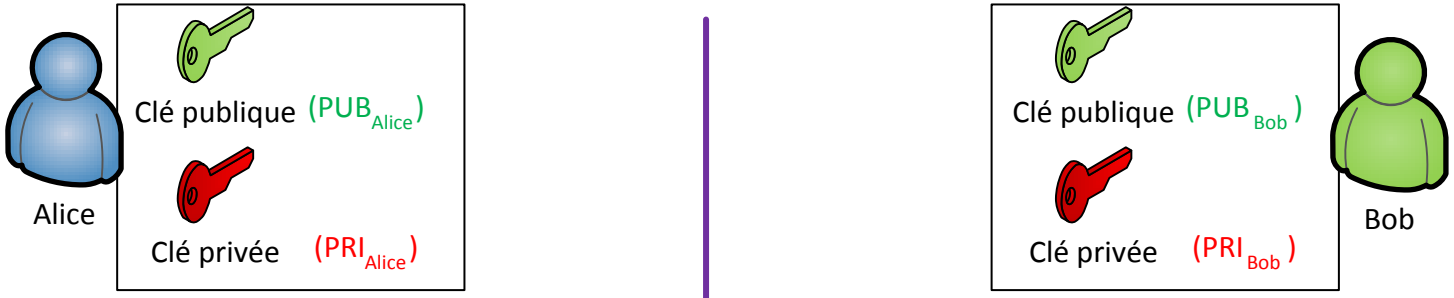
Chiffrement asymétrique (« chiffrement à clé publique ») (1/4)

Principe: chaque utilisateur dispose d'une paire de clés (1 clé publique et 1 clé privée).

> Ce que chiffre la clé publique ne peut être déchiffré que par la clé privée.

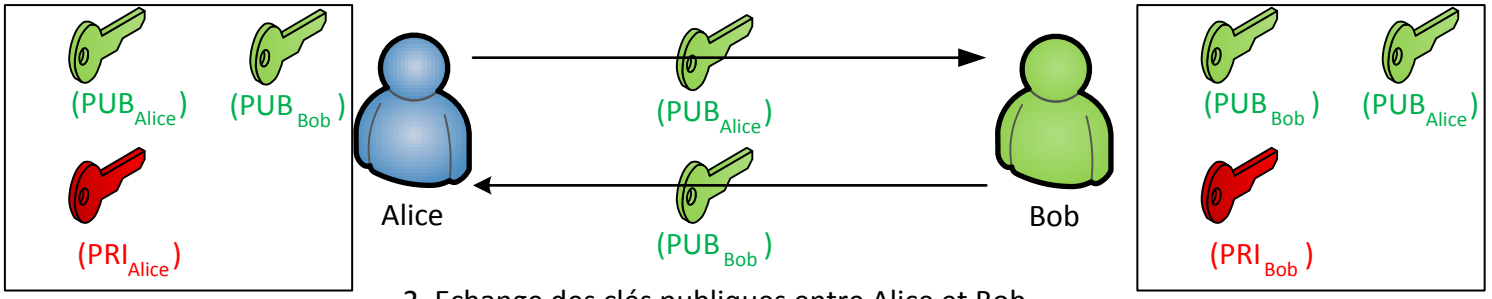
> Ce que chiffre la clé privée ne peut être déchiffré que par la clé publique.

Etape 1: chaque utilisateur génère sa paire de clés individuelle



1A. Création d'une paire de clés par Alice

Etape 2: les utilisateurs échangent leurs clés publiques



2. Echange des clés publiques entre Alice et Bob

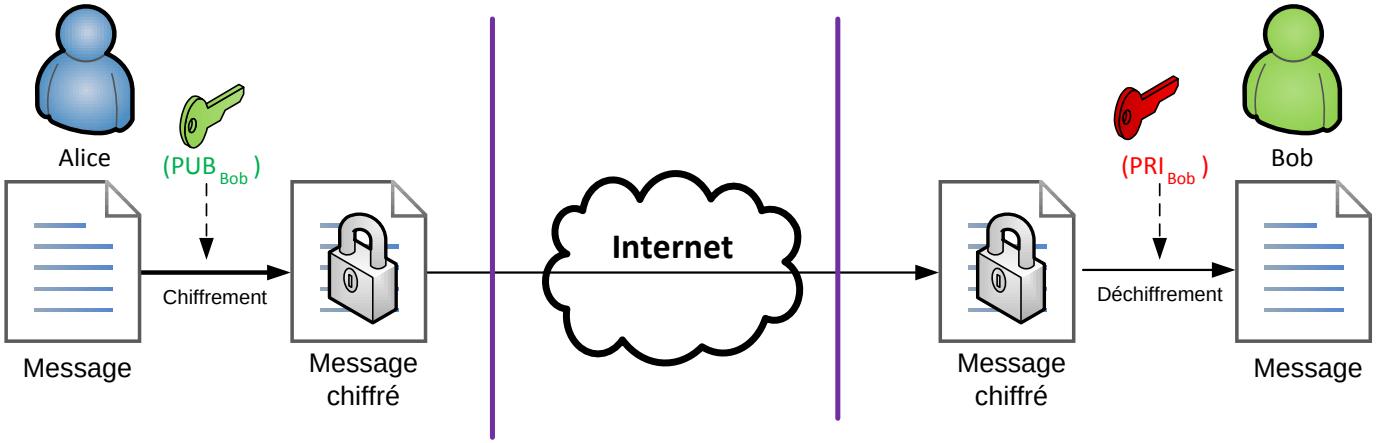
© 2019 Jean-Claude Héritier

Chiffrement asymétrique (« chiffrement à clé publique ») (2/4)

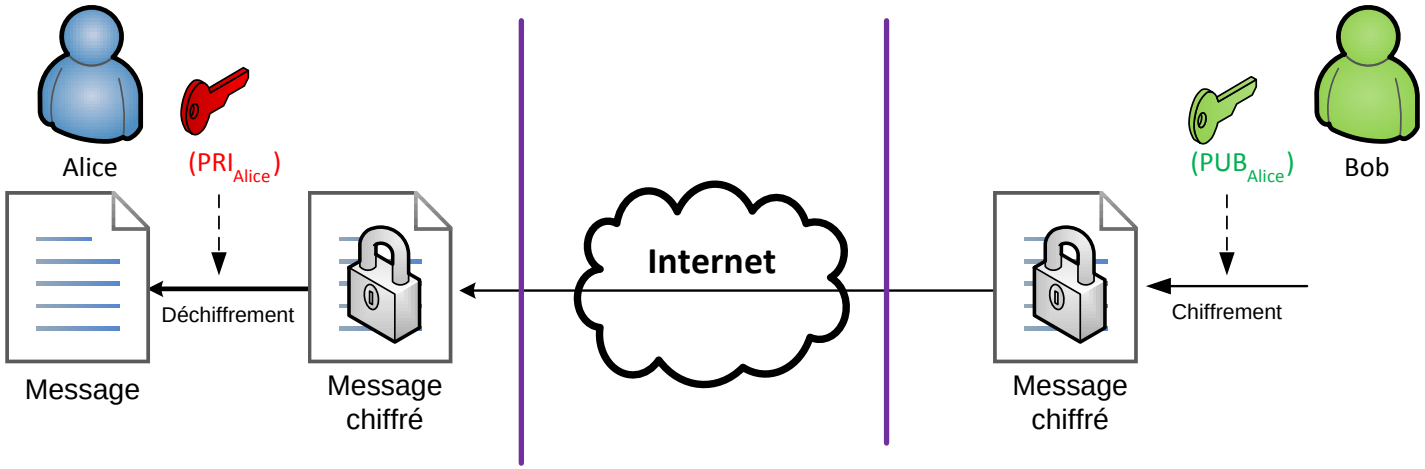
A) Confidentialité par chiffrement asymétrique:

> chiffrement avec la clé publique du destinataire.

Etape 3: envoi de données par chiffrement asymétrique



Etape 4: réponse par chiffrement asymétrique



- **Confidentialité** ✓
- **Intégrité** ✗
- **Authentification*** ✓
  - du destinataire
  - ~~de l'expéditeur~~

*** = sous réserve de confiance en la clé publique.**

Seul Bob peut lire le message envoyé par Alice.

Seule Alice peut lire la réponse envoyée par Bob.

Quelles limites?

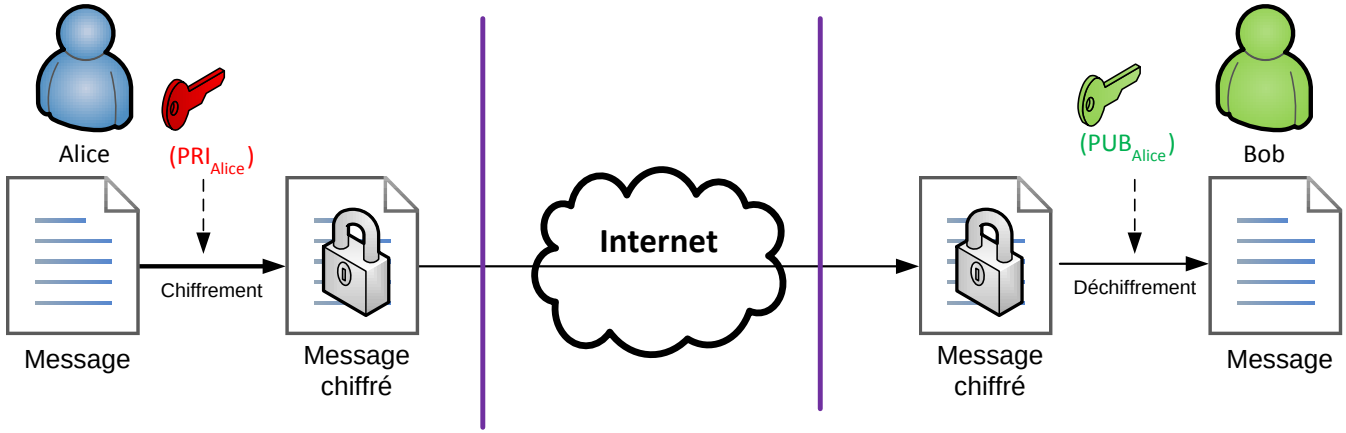
© 2019 Jean-Claude Héritier

Chiffrement asymétrique (« chiffrement à clé publique ») (3/4)

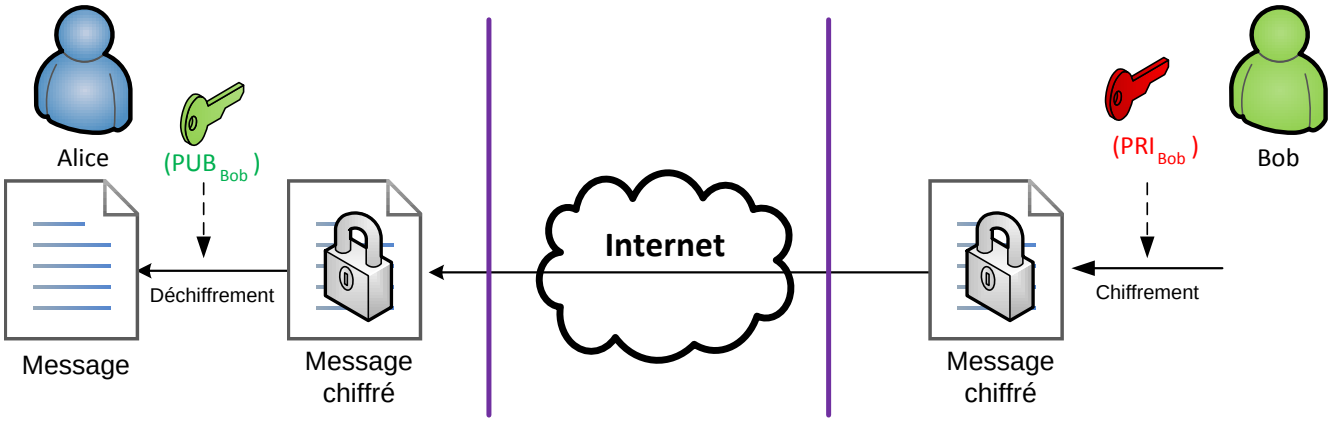
B) Authentification de l'expéditeur par chiffrement asymétrique:

> chiffrement avec la clé privée de l'expéditeur.

Etape 3bis: envoi de données par chiffrement asymétrique (avec authentification de l'expéditeur)



Etape 4bis: réponse par chiffrement asymétrique (avec authentification de l'expéditeur)



- **Confidentialité** ✓
- **Intégrité** ✗
- **Authentification*** ✓
  - ~~du destinataire~~
  - de l'expéditeur

*** = sous réserve de confiance en la clé publique.**

Bob a l'assurance que le message provient d'Alice.

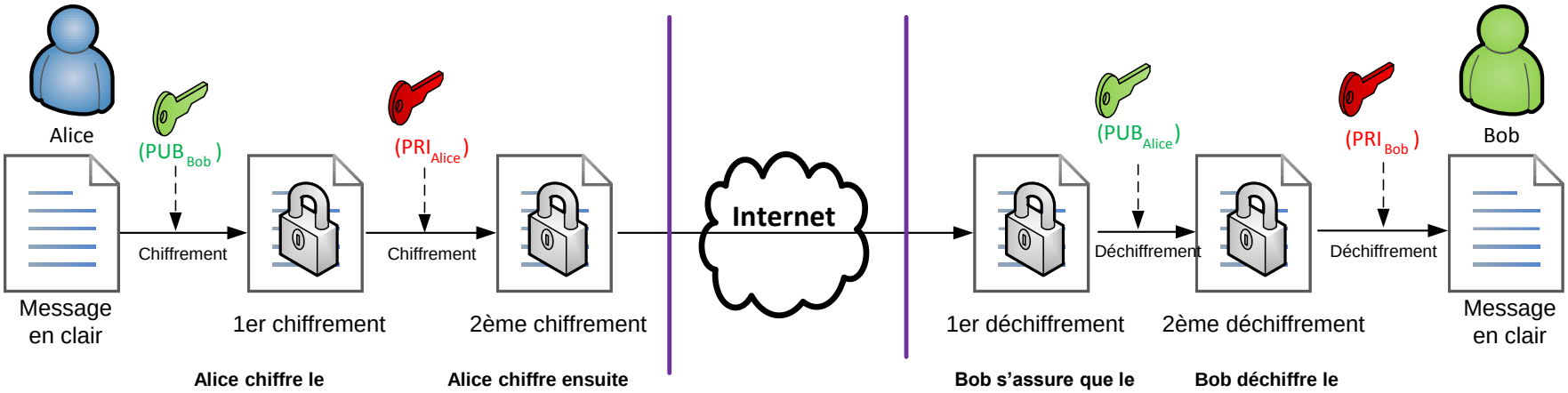
Alice a l'assurance que la réponse provient de Bob.

Quelles autres limites?

© 2019 Jean-Claude Héritier

Chiffrement asymétrique (« chiffrement à clé publique ») (4/4)

En combinant les deux approches, le chiffrement asymétrique permet d'authentifier expéditeur et destinataire, tout en assurant confidentialité et intégrité:



Alice chiffre le message avec la clé publique de Bob pour s'assurer que le message ne pourra être lu que par Bob.

Alice chiffre ensuite le message avec sa clé privée pour prouver à Bob qu'elle en est bien l'expéditeur.

Bob s'assure que le message vient bien d'Alice.

Bob déchiffre le message avec sa clé privée.

- **Confidentialité** ✓
- **Intégrité** ✗
- **Authentification*** ✓
  - du destinataire
  - de l'expéditeur
- **Non-répudiation*** ✓

*** = sous réserve de confiance en la clé publique (la clé privée ne soit pas être compromise).**

Limites

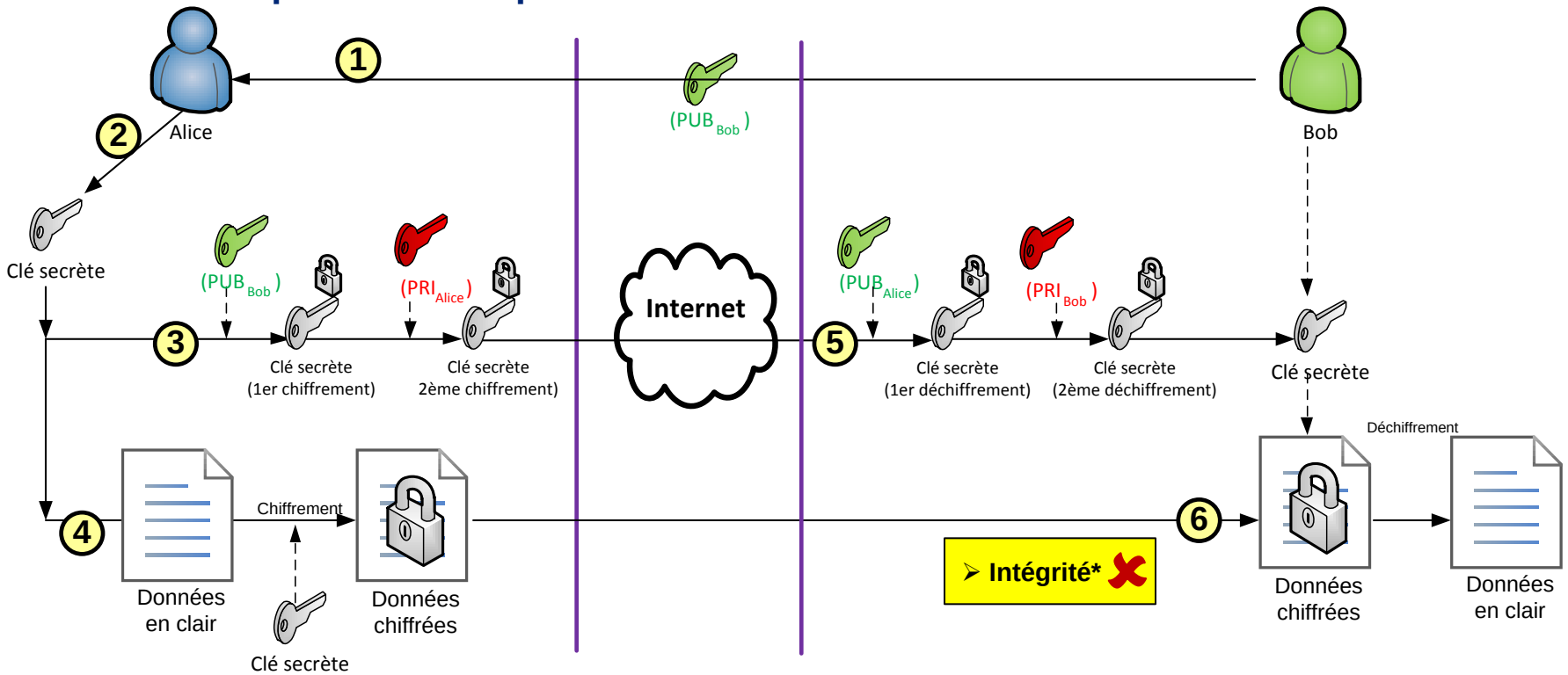
- **Problème #1:** Contraintes de performance des algorithmes à clé publique -> rarement utilisés pour la confidentialité des données.
  - Les algorithmes à clé publique sont typiquement utilisés pour supporter l'échange de clés symétriques / secrètes: un **mode hybride** combinant chiffrement à clé publique et échange de clé secrète (=symétrique) est le plus souvent utilisé.
- **Problème #2:** Assurance limitée sur l'intégrité des données (Propagation d'erreurs, mais des manipulations ciblées peuvent passer inaperçues).
- **Problème #3**: Comment s'assurer que la clé privée n'est pas compromise et appartient bien à son propriétaire?

© 2019 Jean-Claude Héritier

Introduction à la cryptographie

Chiffrement hybride (association du chiffrement à clé publique et du chiffrement symétrique)

Solution au problème #1: performance du chiffrement des données



1. Alice obtient la clé publique de Bob.

2. Alice génère une clé secrète utilisant un algorithme de chiffrement symétrique (« clé de session »): la même clé permettra de chiffrer et déchiffrer.

3. Alice chiffre la clé symétrique avec la clé publique de Bob, puis avec sa clé privée pour prouver à Bob qu'elle en est l'expéditeur, puis envoie la clé secrète chiffrée à Bob..

4. Alice chiffre les données avec la clé symétrique, puis envoie les données ainsi chiffrées à Bob.

5. Bob vérifie que la clé provient d'Alice (en utilisant la clé publique d'Alice), puis déchiffre la clé secrète au moyen de sa clé privée.

6. Bob dispose de la clé secrète partagée avec Alice et peut ainsi déchiffrer les données. Seule la clé secrète fournie par Alice peut déchiffrer ces données.

Limites?

Problème #2: comment s'assurer de l'INTEGRITE des données reçues? A-t-on reçu toutes les données, rien que les données, et dans le bon ordre?

Problème #3: comment Bob s'assure t'il que la clé publique d'Alice est fiable?

© 2019 Jean-Claude Héritier

Garantir l'intégrité des données: les fonctions de hachage

Solution au problème #2: création d'une empreinte cryptographique (« hash », « digest » ou « condensat ») unique, de taille fixe, par une fonction à sens unique ayant pour but de garantir l'authenticité d'un fichier ou d'un message.

Caractéristiques des algorithmes de hachage:

- Facilité et rapidité: tout fichier doit pouvoir être « haché » en un temps informatique court.
- Intégrité: il est *impossible* de modifier le fichier sans que son empreinte ne soit également modifiée **(à nuancer*).**
- Unicité: il ne doit *jamais* arriver que deux fichiers différents aient une même empreinte.
- Non-réversibilité: il doit être impossible de générer un fichier ayant une empreinte donnée.

Exemples:

Fichier ------ ------> Message digest

It is computationally infeasible to produce two messages having the same message digest. -> `385ef39262a26e211969b752dad2f914`

It is computationally infeasible to produce two messages having the same message digEst. ->`16fa5d7f432f06fdcf464bffe96ac80c`

Md5sum (128 bit)	385ef39262a26e211969b752dad2f914 (sujet à collisions => non-recommandé)
Sha1sum (160 bit)	3ba8dbe9bc09e6ad309d44cd2ca760bca12e0c61
Sha256sum (256 bit)	939b498047ff2baa631dc26a549e274f939ba3d66ae1c6d3f5f373edd547e7c9
Sha512sum (512 bit)	cdab4420839ace33ff217334884dade7f91febd779115e9b1874401c00adcc8816c3827832f6a5fa0b2ead0f0db15af9bdb60331a42fa9cd3d192bc684a28b66

***A savoir:** attaques par collision => durée de vie « utile » relative des algorithmes de hachage.

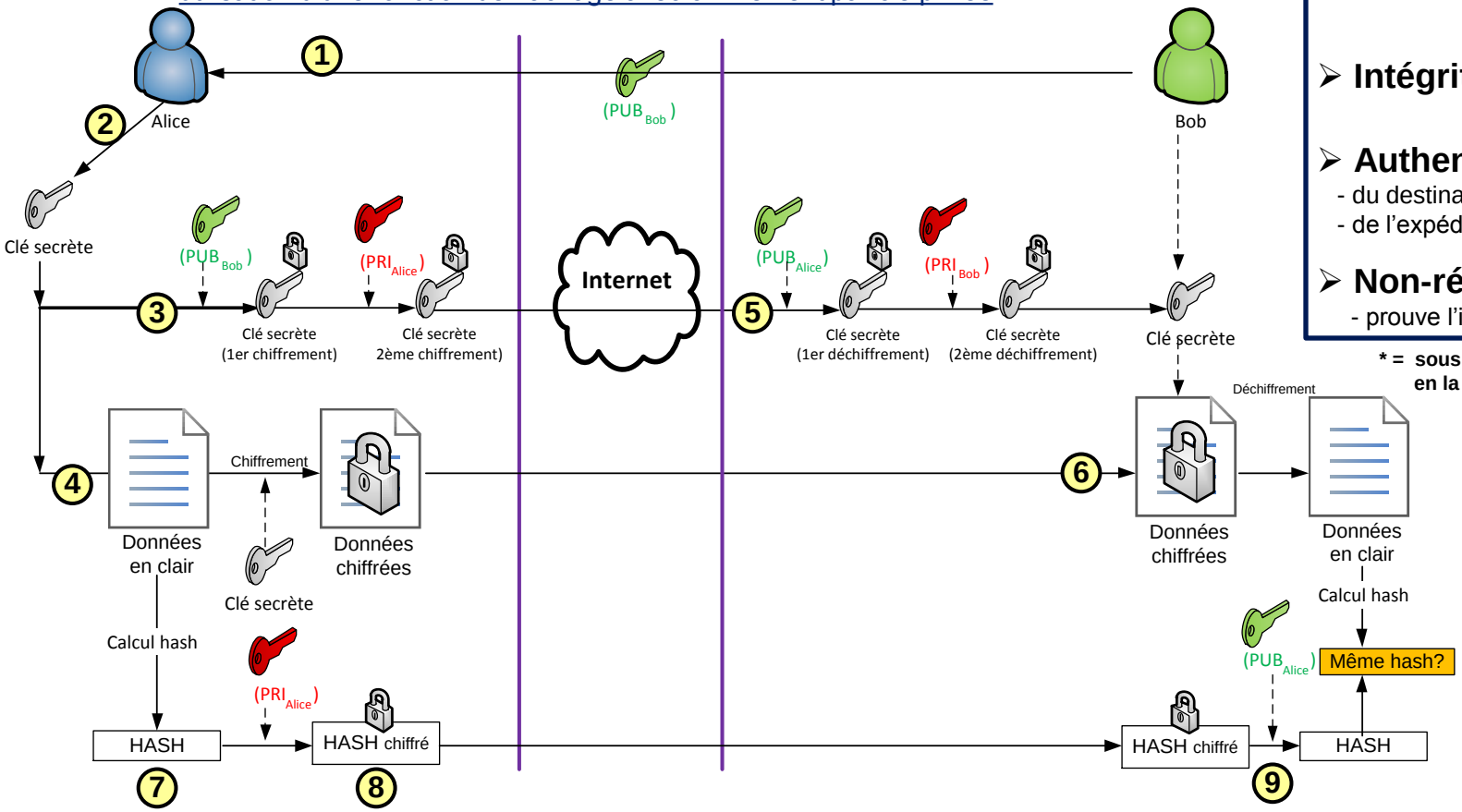
© 2019 Jean-Claude Héritier

Introduction à la cryptographie

Chiffrement hybride (association du chiffrement à clé publique et du chiffrement symétrique)

Suite: comment garantir l'intégrité du fichier échangé?

> utilisation d'une fonction de hachage avec chiffrement par clé privée



- **Confidentialité** ✓
- **Intégrité** ✓
- **Authentification*** ✓
  - du destinataire
  - de l'expéditeur
- **Non-répudiation*** ✓
  - prouve l'identité de l'auteur

*** = sous réserve de confiance en la clé publique.**

7. Alice calcule une empreinte cryptographique des données au moyen d'une fonction de hachage;

8. Alice chiffre ensuite le hash au moyen de sa clé privée pour prouver qu'elle en est à l'origine.

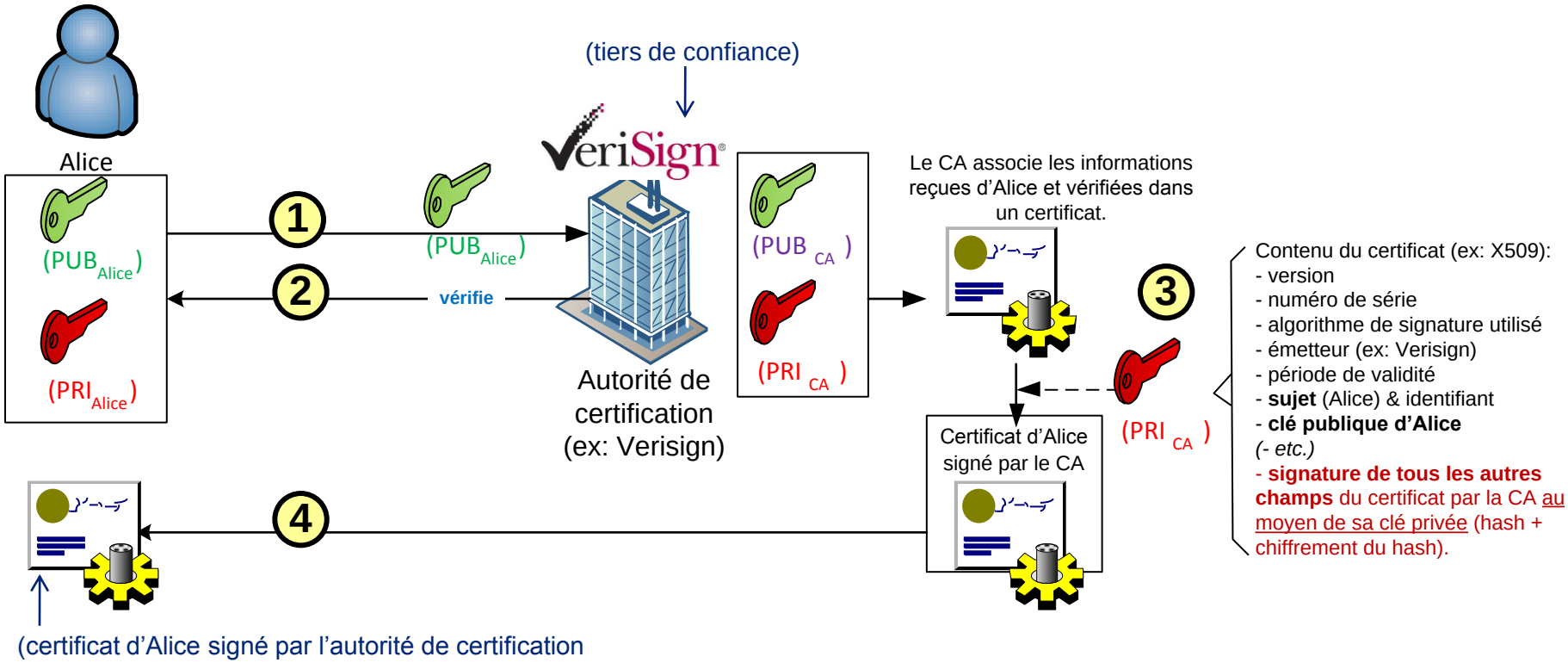
8. Bob vérifie que le hash provient d'Alice en le déchiffrant avec la clé publique d'Alice, puis compare le hash reçu avec le hash du fichier.

*** Reste encore le problème #3: comment Bob s'assure t'il que la clé publique d'Alice n'a pas été compromise?**

© 2019 Jean-Claude Héritier

Solution au problème #3: les autorités de certification

> Obtention d'un **certificat** par Alice auprès d'une Autorité de Certification (« CA »)



1. Alice demande un certificat à l'autorité de certification et communique son identité ainsi que sa clé publique.

2. L'autorité de certification vérifie les données d'Alice en fonction de différents standards (ex: ETSI TS 102 042).

3. Après avoir établi l'identité de Alice, l'autorité de certification génère un certificat pour Alice (contenant l'identification d'Alice, la clé publique d'Alice et l'identifiant de l'autorité**), puis signe le certificat avec sa clé privée et ajoute la signature dans le certificat.**

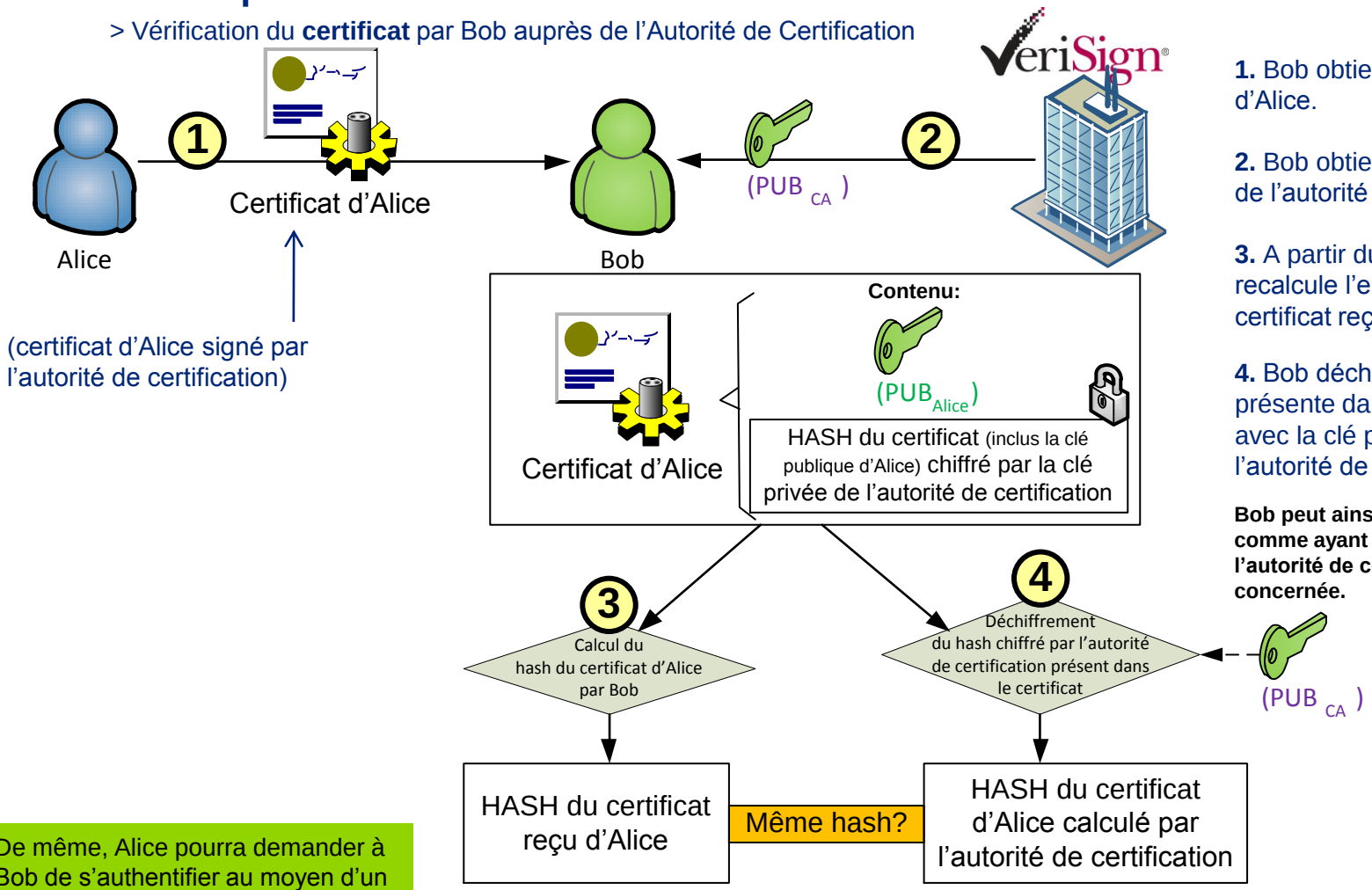
4. L'autorité de certification remet le certificat signé à Alice.

© 2019 Jean-Claude Héritier

Chiffrement hybride (association du chiffrement à clé publique et du chiffrement symétrique)

Solution au problème #3: les autorités de certification

> Vérification du **certificat** par Bob auprès de l'Autorité de Certification



1. Bob obtient le certificat d'Alice.

2. Bob obtient la clé publique de l'autorité de certification.

3. A partir du certificat, Bob recalcule l'empreinte du certificat reçu d'Alice (hash).

4. Bob déchiffre l'empreinte présente dans le certificat avec la clé publique de l'autorité de certification.

Bob peut ainsi authentifier le hash comme ayant été fourni par l'autorité de certification concernée.

De même, Alice pourra demander à Bob de s'authentifier au moyen d'un certificat remis par une autorité de certification

Bob est ainsi certain de disposer de la clé publique d'Alice, en se basant sur la validation du certificat par une autorité de certification.

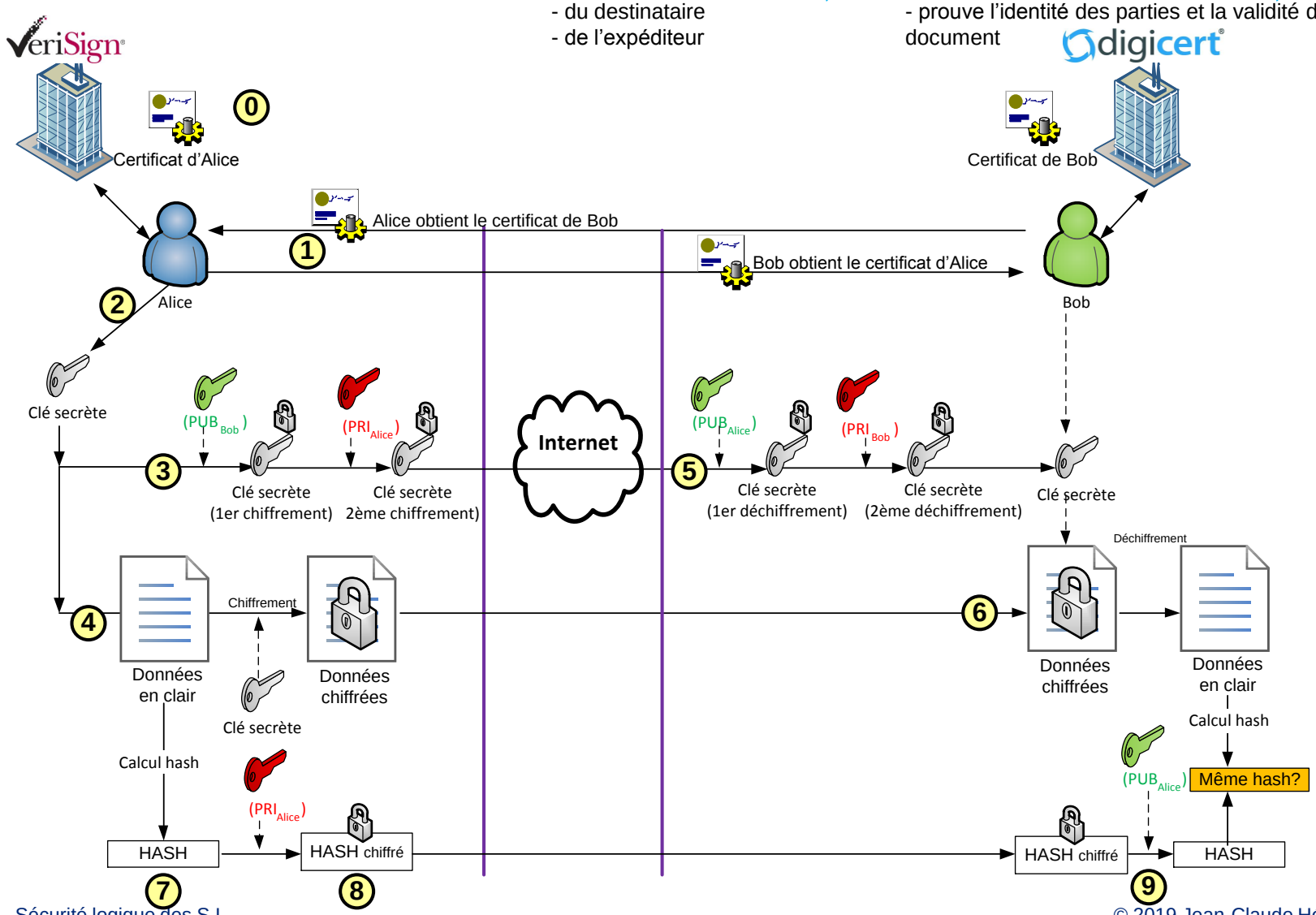
© 2019 Jean-Claude Héritier

Introduction à la cryptographie

Résumé: vue d'ensemble d'un échange sécurisé et authentifié

La confiance en la clé publique de Alice et Bob est garantie par les autorités de certification.

- **Confidentialité** ✓
- **Intégrité** ✓
- **Authentification** ✓
  - du destinataire
  - de l'expéditeur
- **Non-répudiation** ✓
  - prouve l'identité des parties et la validité du document



© 2019 Jean-Claude Héritier

Cryptographie

–

applications pratiques

© 2019 Jean-Claude Héritier

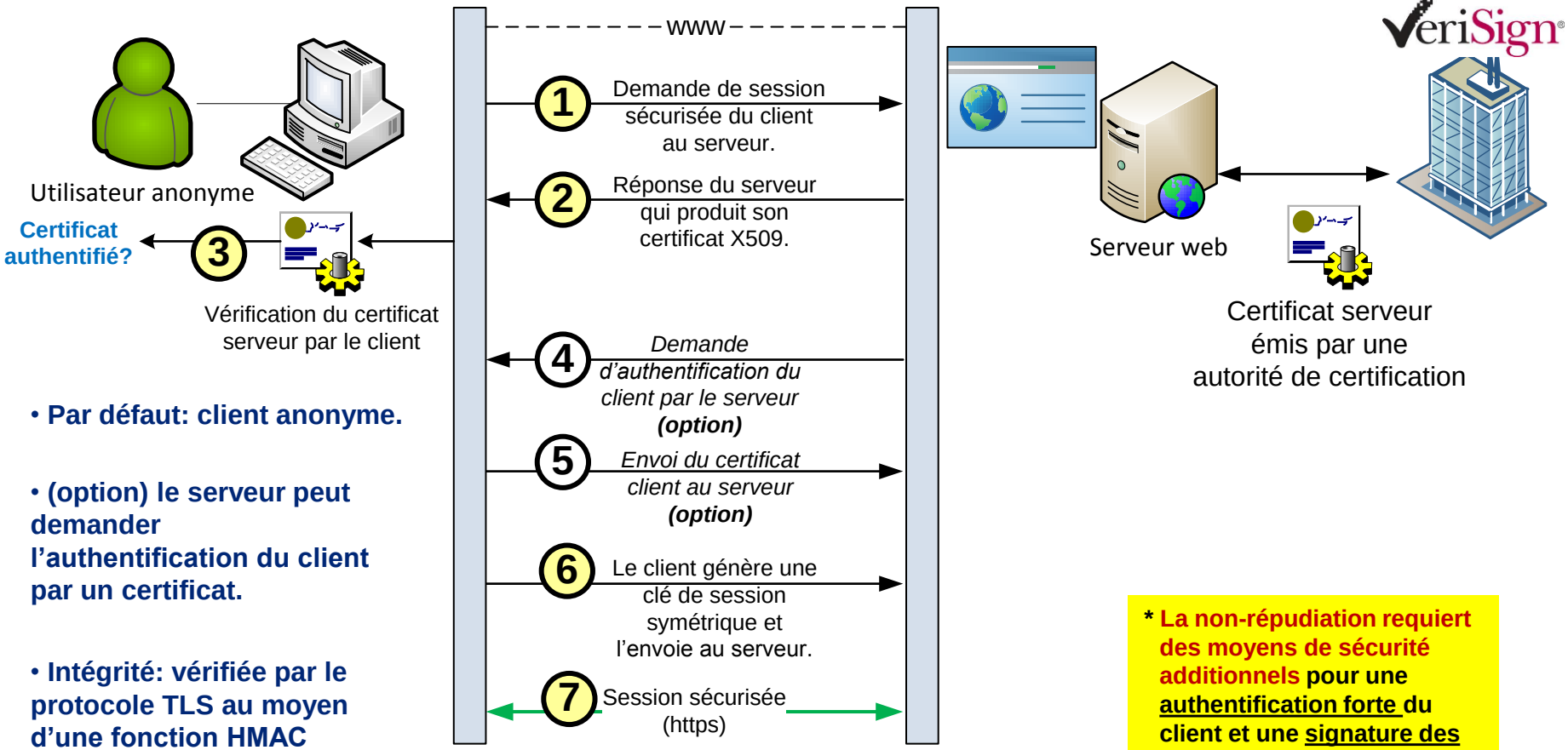
1. SSL / TLS (https)

© 2019 Jean-Claude Héritier

Cryptographie – applications pratiques

1) SSL / TLS (transport layer security) (ex: https, ftps)

Etablissement d'une session TLS:



- **Par défaut: client anonyme.**
- **(option) le serveur peut demander l'authentification du client par un certificat.**
- **Intégrité: vérifiée par le protocole TLS au moyen d'une fonction HMAC** (HMAC-SHA-1).

*** La non-répudiation requiert des moyens de sécurité additionnels pour une authentification forte du client et une signature des transactions.**

- **Confidentialité** ✓
- **Intégrité** ✓
- **Authentification** ✓
  - du serveur
  - du client **(option)**
- **Non-répudiation***
  - possible mais requiert des mesures complémentaires

© 2019 Jean-Claude Héritier

Cryptographie – applications pratiques
1) SSL / TLS (transport layer security)

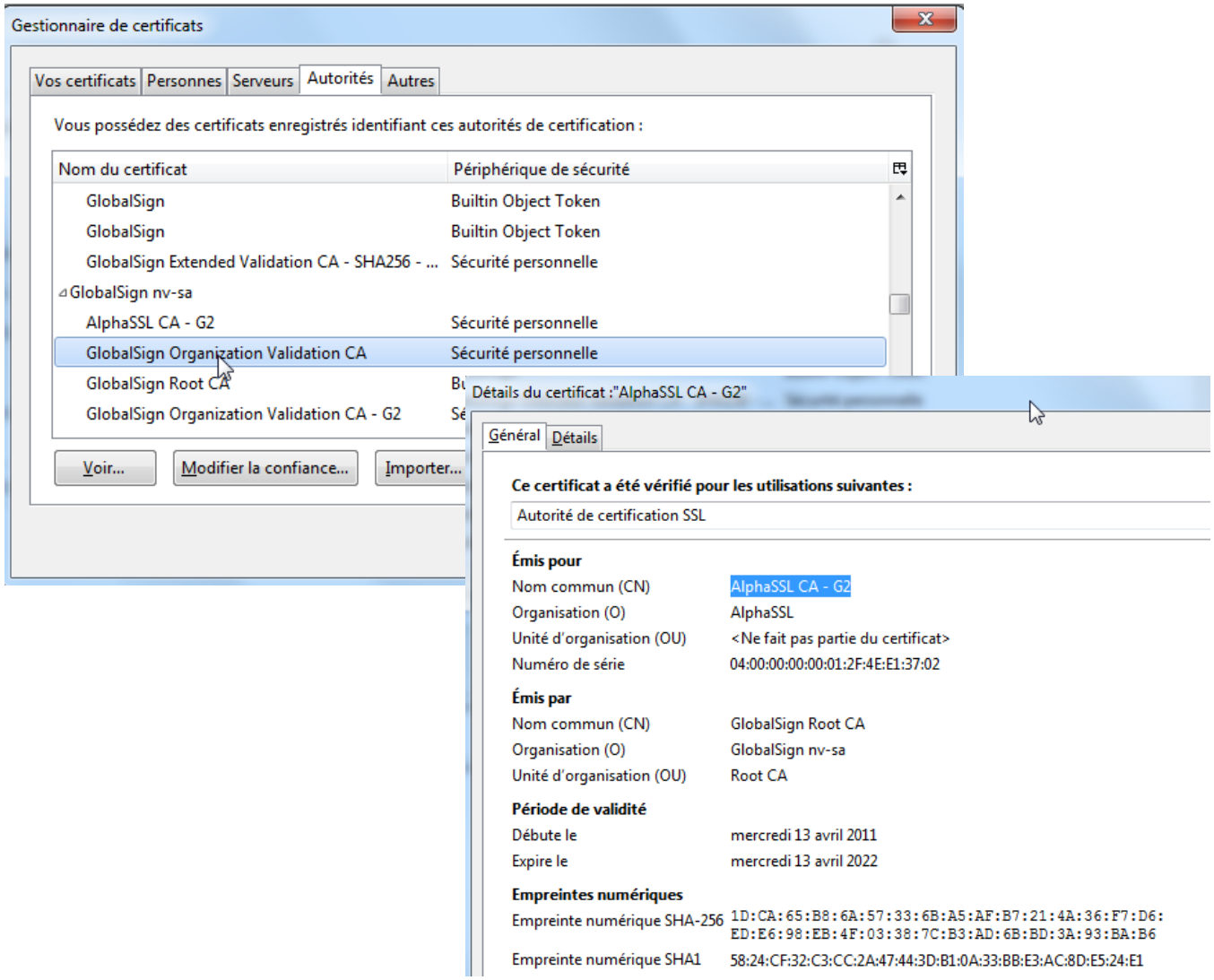
Certificats SSL et navigateurs web:

Certificat d'autorités de certification installés dans un navigateur web (ex: Firefox) (« liste de certificats racines »)

Ces certificats sont implicitement considérés comme étant dignes de confiance.

A chaque connexion HTTPS sur un site, le navigateur vérifie que le certificat du site est signé par une des autorités de certification pré-installées («root CA»).

Si le certificat est bien signé par une de ces autorités, aucune alerte n'est affichée.



© 2019 Jean-Claude Héritier

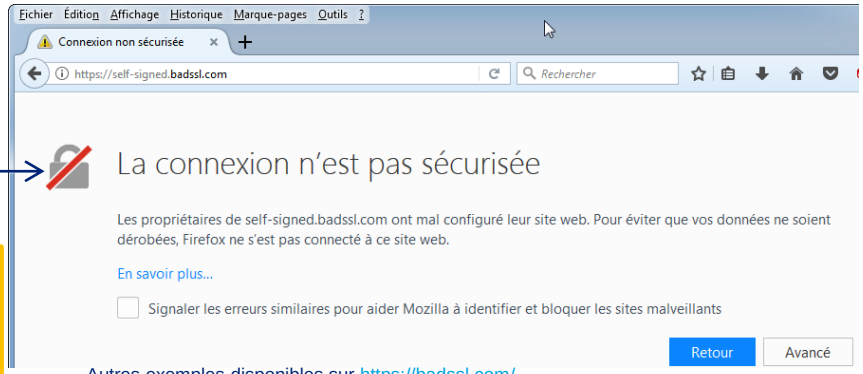
Cryptographie – applications pratiques
1) SSL / TLS (transport layer security)

Certificats SSL:

Certificat non-signé par une autorité de certification. Par exemple:

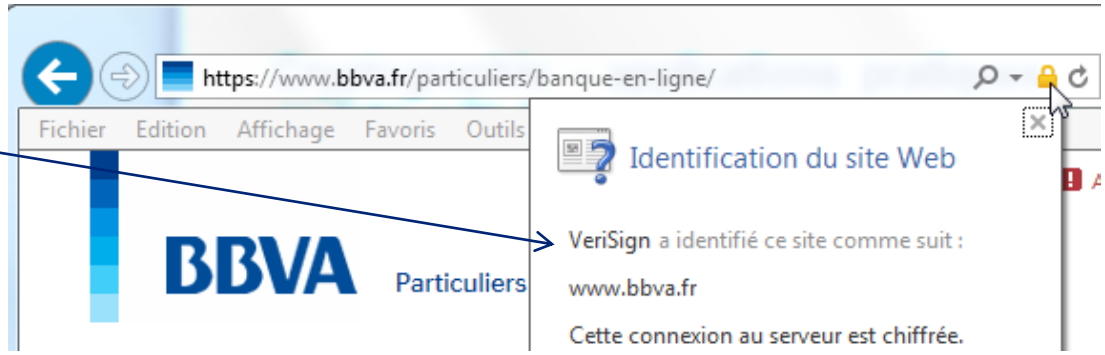
- CA interne (p.ex. Intranet d'entreprise) -> message d'erreur si le navigateur n'est pas autorisé à faire confiance à cette autorité de certification
- site web public mal configuré (cas présenté ici)

Toute la sécurité repose sur la confiance dans les autorités de certification « racines » qui sont définies dans le navigateur.



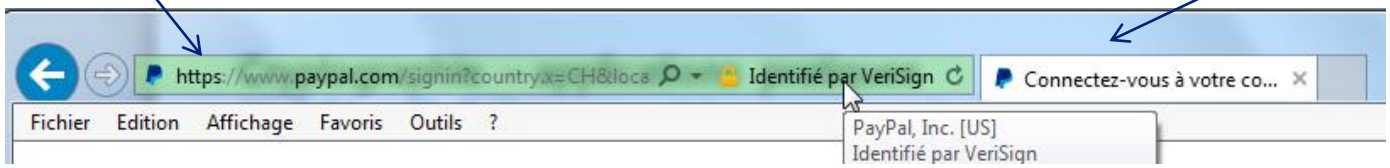
Autres exemples disponibles sur https://badssl.com/

Certificat signé par une autorité de certification



Certificat signé par une autorité de certification avec validation étendue (extended validation », EV)

EV: Nom de l'autorité de certification visible dans le navigateur.



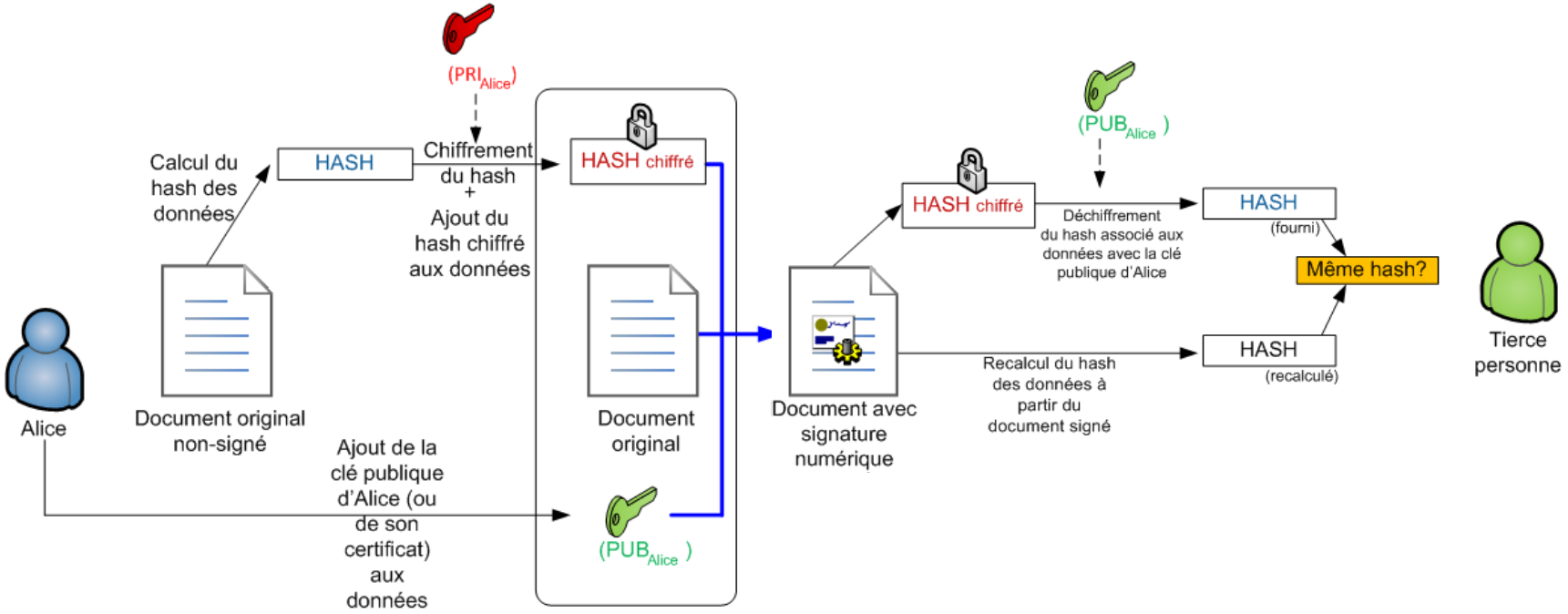
© 2019 Jean-Claude Héritier

2. Signature électronique

© 2019 Jean-Claude Héritier

Cryptographie – applications pratiques
2) Signature électronique

Principe: utilisation de la cryptographie asymétrique pour garantir l'intégrité d'un document et en identifier l'auteur.



Signature numérique du document ⟷ **Vérification de la signature numérique**

Valeur légale de la signature électronique:
- **UE**: cadre communautaire défini par la Directive européenne 1999/93/CE
- **En France:**
  - Même valeur légale qu'une signature manuscrite depuis 2000.
  - Requiert l'utilisation de **certificats qualifiés** (émis par un fournisseur de certificats accrédité - *Art. 6.1 et 6.2 du décret 2001-272 du 30 mars 2001*).

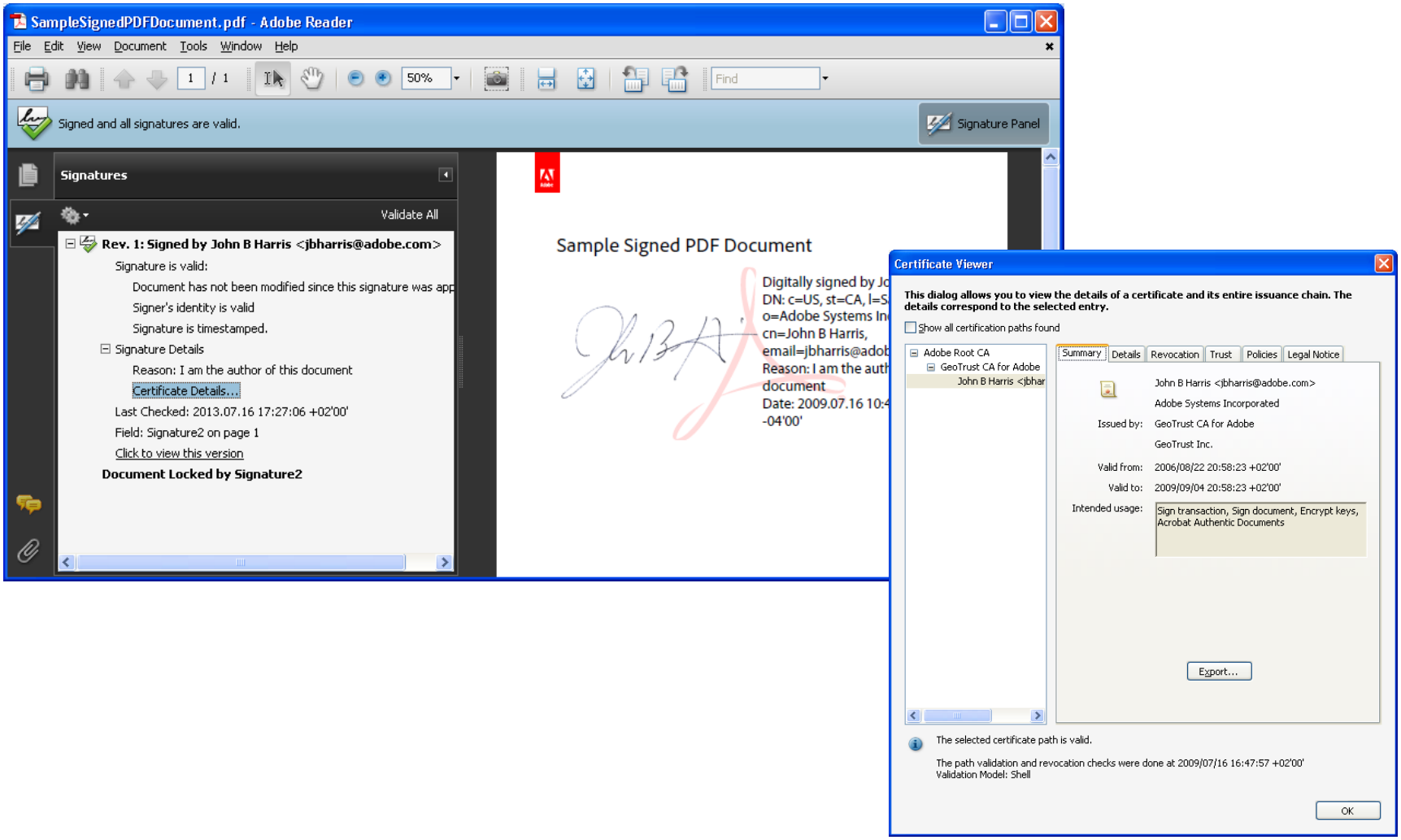
- **Intégrité** ✓
- **Authentification*** ✓
  - du signataire
- **Non-répudiation*** ✓
  - prouve l'identité de l'auteur

*** = sous réserve de confiance en la clé publique.**

© 2019 Jean-Claude Héritier

2) Signature électronique

Exemple de document signé numériquement:



© 2019 Jean-Claude Héritier

3. Authentification forte

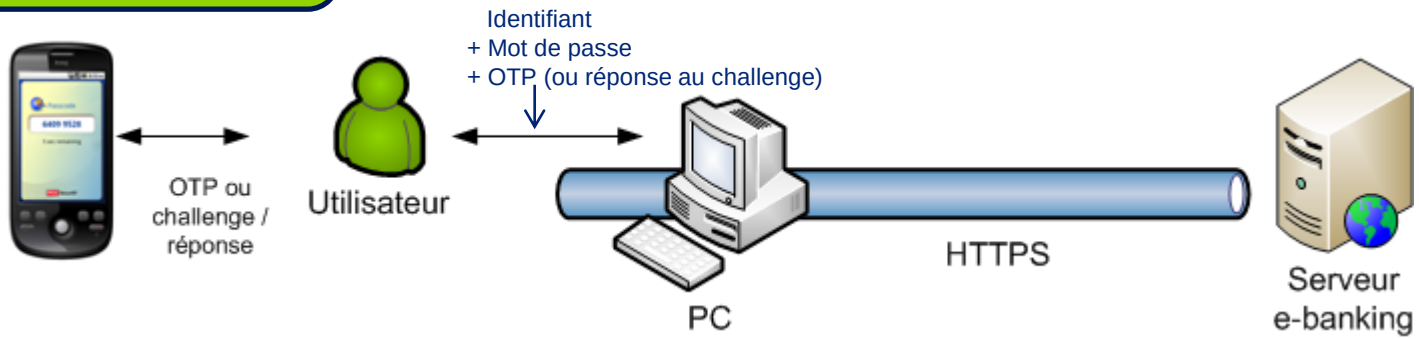
© 2019 Jean-Claude Héritier

3) Authentification forte

Principe: pallier aux faiblesses inhérentes à l'authentification par mot de passe par l'utilisation de plusieurs facteurs:

Quelque chose que l'utilisateur connait.	« something you know »	• Mot de passe • PIN • Schéma de déverrouillage (e.g. Android)
Quelque chose que l'utilisateur possède.	« something you have »	• Tokens - connectés / non-connectés - synchrones / asynchrones - matériels / logiciels • Smartcards
Quelque chose que l'utilisateur est.	« something you are »	• Biométrie

Exemple:



© 2019 Jean-Claude Héritier

3) Authentification forte

Exemples:

RSA SecurID

RSA SecurID
Software Token
(Android)

Yubikey (solution asynchrone)

LuxTrust
'Signing Stick'

RSA SecurID Software Token
(Microsoft Windows)

RSA SecurID Toolbar

QUIZZ: Quels challenges?

© 2019 Jean-Claude Héritier

3) Authentification forte

QUIZZ

Authentification	Remplit les critères d'une authentification forte?	Points d'attention / limites?
1. Mot de passe défini par l'utilisateur + OTP reçu par SMS	✓	OTP limité dans le temps?
2. Mot de passe défini par l'utilisateur + OTP généré par une application dédiée sur smartphone	✓	Vol, perte, malware, absence de mot de passe sur le smartphone ?
3. Mot de passe défini par l'utilisateur + code à usage unique sur carte à biffer (« scratchcard »)	✓	OTP non dynamique?
4. OTP (ex: Yubikey) + Captcha	✗	1 seul facteur
5. Mot de passe défini par l'utilisateur + phrase secrète identifiant le site marchand	✗	1 seul facteur
6. Mot de passe défini par l'utilisateur + OTP envoyé par e-mail	✗	Pas multi-facteur
7. Mot de passe défini par l'utilisateur + OTP dynamique à trois chiffres	✓	Une chance sur 1000 pour un attaquant?

© 2019 Jean-Claude Héritier

3) Authentification forte

QUIZZ

Authentification	Remplit les critères d'une authentification forte?	Points d'attention / limites?
8. Mot de passe défini par l'utilisateur + OTP communiqué par téléphone par le Support	✗	Quelle valeur de l'authentification ? (erreur humaine, social engineering…)
9. Mot de passe défini par l'utilisateur + empreinte vocale	✓	Probablement assez facile à contrefaire (« replay attack »).
10. Mot de passe défini par l'utilisateur + Challenge / Réponse	✓	A priori sûr. A voir au cas par cas.
11. Mot de passe défini par l'utilisateur + notification « push » vers smartphone (iPhone APN, Android C2DM/GCM)	✓	Sécurité du smartphone : vol, perte, malware?

Exemple de notification « push »

© 2019 Jean-Claude Héritier

3) Authentification forte

Challenges et solutions possibles:

Sécurité	• Attaques « MITM*» ou « MITB** » • Accès non-autorisé au token	• Analyse des risques • Audit de sécurité (But: prévenir toute interception de l'OTP)
Intégration	• Tokens connectés: drivers / middleware devant être compatibles (-> plutôt réservés à un environnement d'entreprise pour ne pas limiter l'utilisation)	• Choix de solution(s) adaptée(s) au contexte d'utilisation.
Conformité	• Utilisation d'une solution d'authentification « véritablement multi-facteurs »?	• Les facteurs doivent être de différentes catégories (FFIEC) (ex: OTP non-dynamiques à proscrire)
Coûts	• Achat (~50 EUR / token / an) + licences • Déploiement / Distribution • Support (soft tokens)	• Analyse coûts / bénéfices
Continuité	• Serveur d'authentification peut devenir un composant critique (impact en cas d'indisponibilité?)	• Intégration au plan de continuité • Authentification adaptative (ex: authentification forte ou standard selon des scénarios et risques prédéfinis)
Non-standardisation	• Multiplication des tokens pour les utilisateurs? • Dépendance envers un fournisseur?	• Soft-tokens • Initiatives de standardisation (ex: OATH) - solutions compatibles à privilégier de manière générale.

etc…

* MITM: « man-in-the-middle »
** MITB: « man-in-the-browser »

© 2019 Jean-Claude Héritier

4. Non-répudiation

© 2019 Jean-Claude Héritier

4) Non-répudiation (1/4)

Principe: prouver de manière irréfutable l'origine et l'intégrité des données, d'une manière vérifiable par toute tierce-partie et à tout moment.

Propriétés fondamentales de la non-répudiation:

1. Les transactions doivent être liées à un envoyeur dont l'identité est confirmée. (-> authentification forte avant soumission d'une transaction)	Non-répudiation de l'origine -> prouve que les données ont été envoyées
2. Les transactions ne doivent pas pouvoir être contrefaites. (-> intégrité des données envoyées pour permettre une vérification ultérieure)	
3. Les transactions ne doivent pas pouvoir être altérées une fois reçues.	Non-répudiation de l'arrivée -> prouve que les données ont été reçues
4. Les transactions doivent rester vérifiables dans le temps.	

© 2019 Jean-Claude Héritier

4) Non-répudiation (2/4)

Cas #1 - Mise en œuvre de la non-répudiation via une solution de type OTP

Certificat authentifié?

3 Vérification du certificat serveur par le client

Session sécurisée (https)

1 Demande de session sécurisée du client au serveur (SSL)

2 Réponse du serveur qui produit son certificat X509.

Serveur web

Serveur d'authentification

Serveur d'application

4 L'expéditeur envoie son identifiant

5 Le serveur renvoie un challenge

6 L'expéditeur envoie la réponse au challenge qu'il a générée avec sa solution OTP

7 Authentification réussie.
L'utilisateur est autorisé à soumettre des transactions

Le serveur vérifie la réponse au challenge et génère la connection dans un log.

8 Envoi de la transaction (numéro de série du token OTP, date & heure, réponse du token (basée sur le temps), référence de la transaction, identifiant utilisateur, détails de la transaction, hash de toutes les informations soumises).

Le serveur vérifie le hash soumis par l'expéditeur.

9 Le serveur envoie une confirmation de la transaction signée numériquement. (ex: PDF)

Enregistrement d'une trace d'audit de la transaction et du hash

(1) (2) & (3) Authentification forte du client et du serveur web.

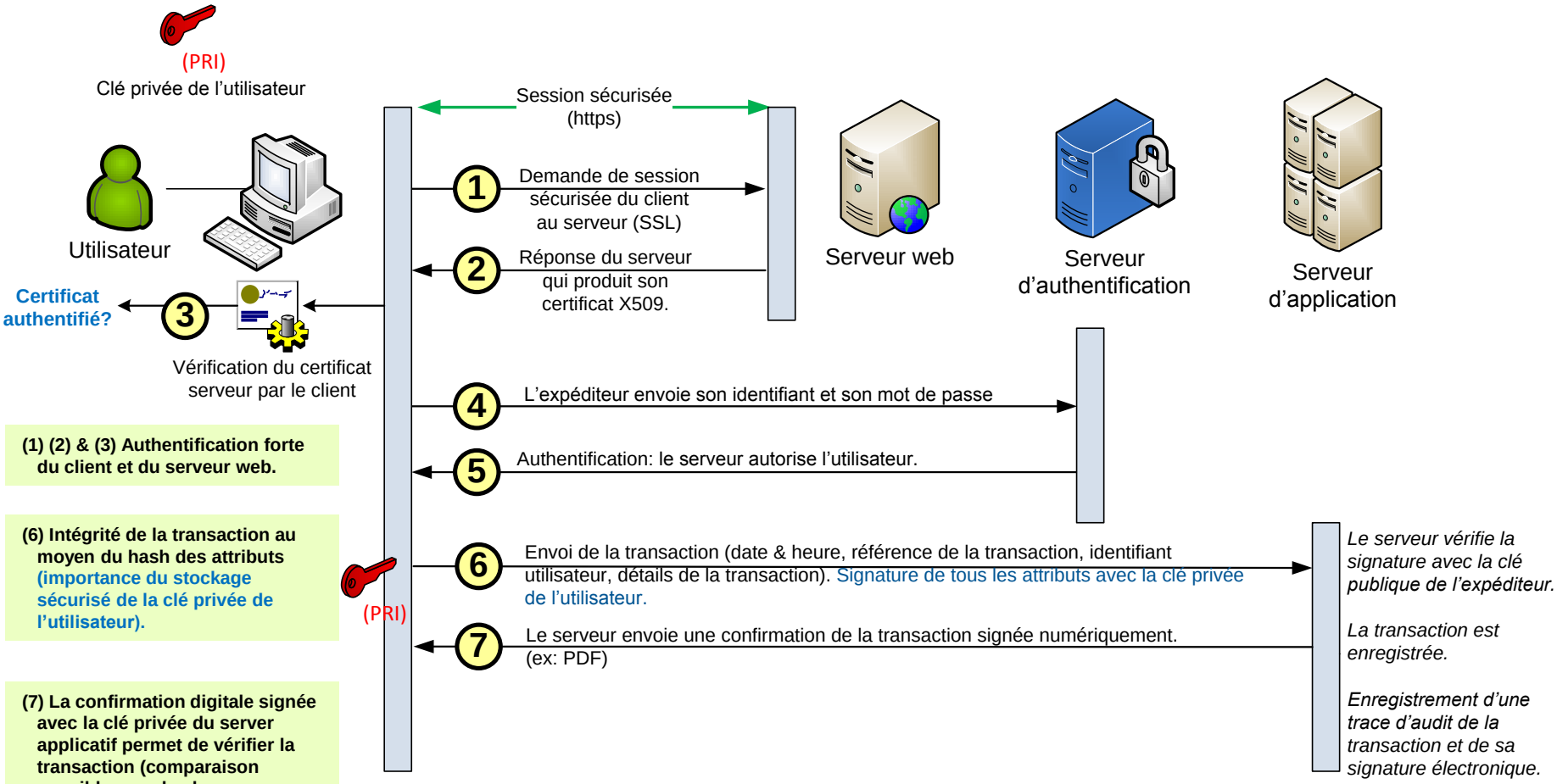
(8) Intégrité de la transaction au moyen du hash (inclure la réponse du token basée sur le temps rend une falsification très complexe)

(9) La confirmation digitale signée avec la clé privée du server applicatif permet de vérifier la transaction (comparaison possible avec les logs enregistrés en cas de contestation).

© 2019 Jean-Claude Héritier

4) Non-répudiation (3/4)

Cas #2 - Mise en œuvre de la non-répudiation via signatures électroniques



© 2019 Jean-Claude Héritier

Cryptographie – applications pratiques
4) Non-répudiation (4/4)

Comparaison des différents concepts de non-répudiation:

1	• **Certificats numériques émis par un tiers de confiance qualifié (« Qualified CA »)** • **Certificats conservés sur des dispositifs matériels (ex: smartcards).**	**Etat de l'art de la non-répudiation**
2	• **Certificats numériques émis par un tiers de confiance qualifié (« Qualified CA »)** • **Certificats conservés sur des dispositifs logiciels (ex: système d'exploitation)**	**Suffisant pour la non-répudiation comme mesure de sécurité*** (élément de résolution de litiges mais à valeur limitée d'un point de vue légal)
3	• **Certificats numériques émis par un tiers de confiance non-qualifié (« non-Qualified CA »)** • **Certificats conservés sur des dispositifs matériels (ex: smartcards).**	
4	• **Certificats numériques émis par un tiers de confiance non-qualifié (« non-Qualified CA »)** • **Certificats conservés sur des dispositifs logiciels (ex: système d'exploitation)**	
5	• **Solution OTP avec challenge / réponse**	
6	• **Solution OTP sans challenge / réponse**	**Apporte des éléments de non-répudiation, mais non-suffisant.**

Valeur en terme de non-répudiation

Elevée

Moyenne

© 2019 Jean-Claude Héritier

5. Horodatage sécurisé

© 2019 Jean-Claude Héritier

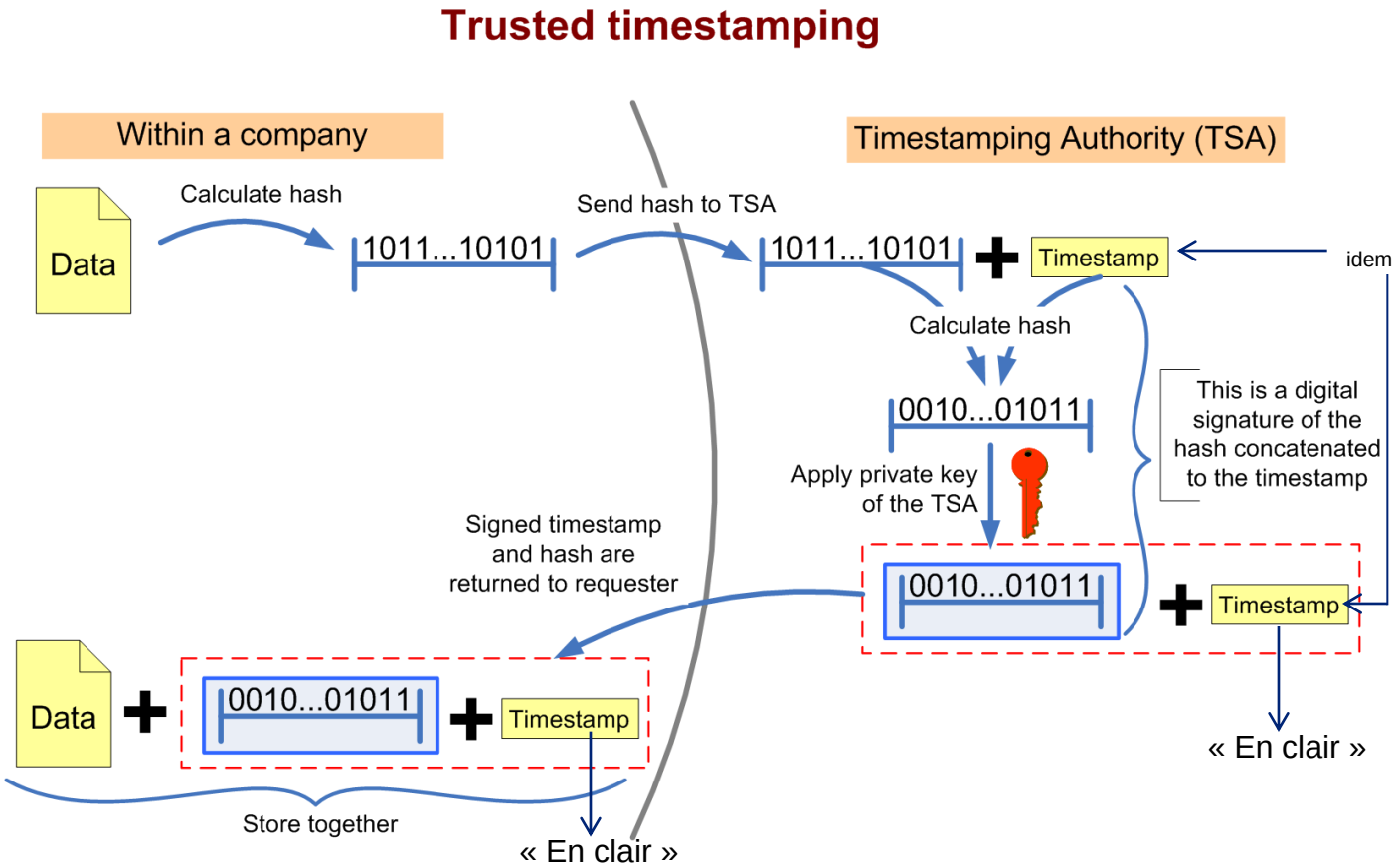
5) L'horodatage sécurisé (1/2)

Principe: utilisation de la cryptographie asymétrique (signatures numériques & fonctions de hachage) pour associer de manière fiable un document à une date & heure et prouver l'existence de données à un instant donné..

Mise en œuvre:

Etape 1 : Génération d'un « timestamp » sécurisé par une autorité neutre d'horodatage.

- Intégrité
- Authenticité
- Confidentialité



© 2019 Jean-Claude Héritier

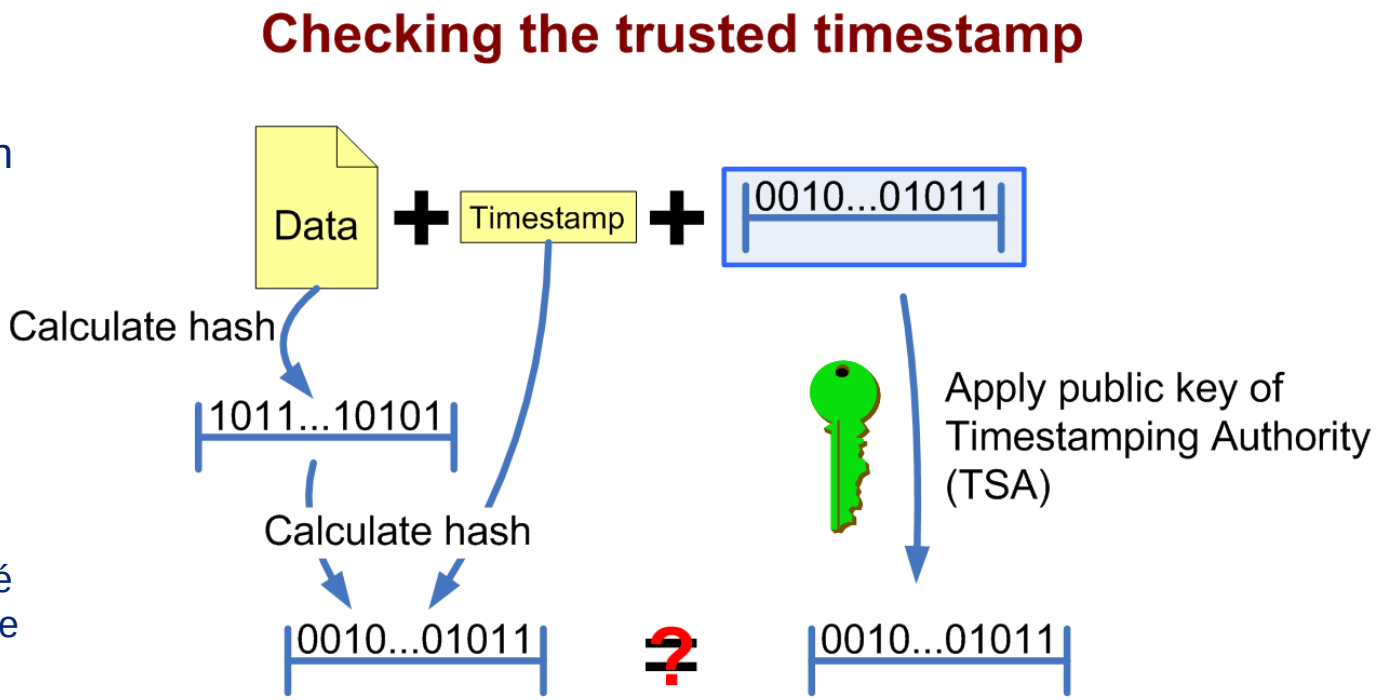
5) L'horodatage sécurisé (2/2)

Mise en œuvre:

Etape 2 : Vérification du « timestamp » sécurisé à tout moment:

1. - Hash(fichier)
   - Ajout du timestamp reçu

2. Déchiffrement du timestamp sécurisé avec la clé publique du TSA.



=> COMPARAISON If the calculated hashcode equals the result of the decrypted signature, neither the document or the timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.

Challenges:
- Archivage sécurisé des Timestamps (-> support de type ''WORM'')
- Assurer une non-répudiation sur le long terme (-> algorithmes & supports de stockage)
- Confiance en un seul tiers? (-> multiples TSA, arbres de Merkel, etc.)

© 2019 Jean-Claude Héritier

6. SSH

© 2019 Jean-Claude Héritier

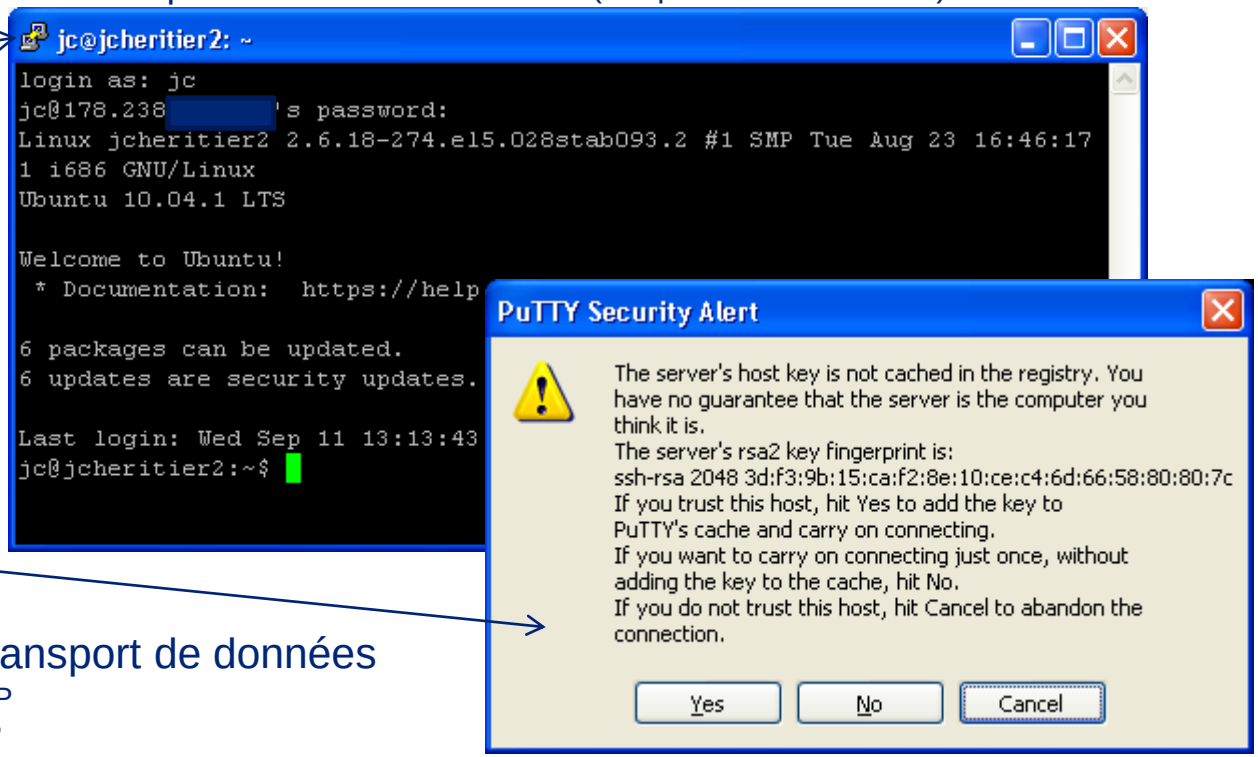
6) SSH / OpenSSH

Fonctions:

1) protocole sécurisé d'administration à distance (ligne de commande) (**S**ecure **SH**ell)

> standard pour l'administration des plateformes UNIX / Linux (remplacement de telnet)

Exemple de session SSH:
- **serveur SSH**: openssh-server (Linux)
- **client SSH**: Putty (Windows)



Cas 1

Authentification du client par identifiant + mot de passe.

Authentification du serveur par empreinte cryptographique (« host key »)

Cas 2

Authentification du client et du serveur par certificats.
(recommandé sur machines sensibles)

2) protocole sécurisé de transport de données

> Remplacement de FTP par SFTP
> Remplacement de RCP par SCP

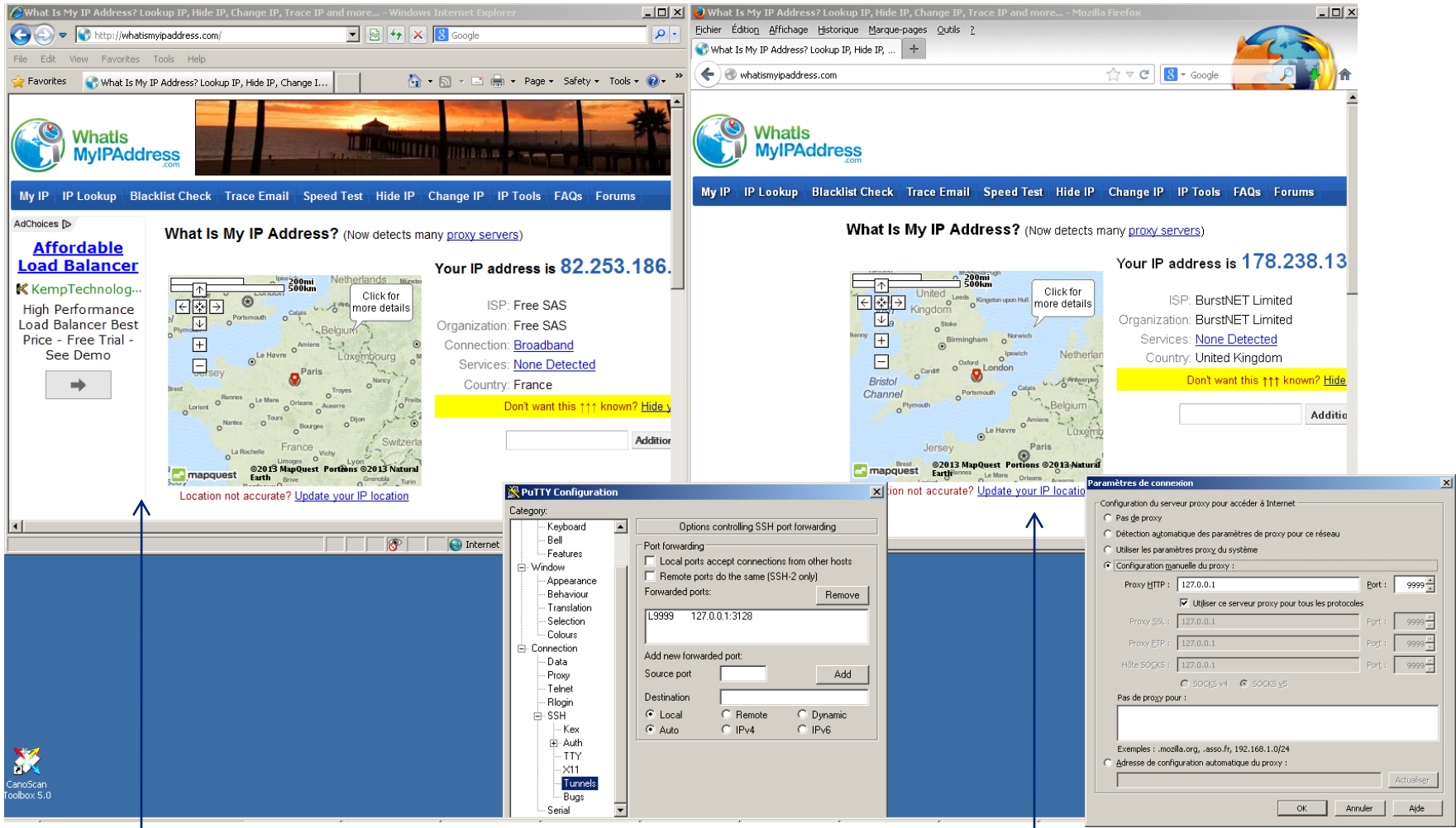
3) protocole de tunneling:

> Permet de transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel.

> Couramment utilisé afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole de récupérations de courrier électronique POP3 – port 110 par défaut) en la faisant transférer sur un autre port (ex: 443) par le biais du tunnel chiffré SSH.

© 2019 Jean-Claude Héritier

Exemple de tunnel SSH:



Internet Explorer: pas de proxy configuré. Le traffic a pour source une IP française.

Client SSH (Putty): tunnelling du port source 9999 vers le port 3128 du serveur distant (port d'écoute du proxy HTTP distant)

Firefox: configuration du navigateur pour utiliser un proxy local sur le port 9999. Le traffic est encapsulé dans le tunnel SSH et ressort sur la machine distante (U.K.)

© 2019 Jean-Claude Héritier

7. Hachage des mots de passe

© 2019 Jean-Claude Héritier

7) Hachage des mots de passe

Applications des fonctions de hachage:

- **Contrôle d'intégrité & authenticité:** **Fichiers, messages**
- **Signature de fichiers:** **Outils de gestion de codes sources (ex: Git), P2P, etc.**
- **Sécurisation de mots de passe:** **Stockage de mots de passe sous forme hachée (= exigence minimum de sécurité)**

Quelles vulnérabilités pour les mots de passe stockés sous forme de hash?

- Attaques par dictionnaire
- Attaques par force brute
- Attaques par «rainbow tables»
- Collisions

Mot de passe sous forme hachée: si deux mots de passe identiques produisent le même hash -> vulnérabilité.

Quelles contre-mesures?

- **Mots de passe « salés » (ajout d'une composante fixe ou variable au mot de passe avant calcul du hash pour augmenter artificiellement la complexité du mot de passe) (« salted hashes »)**

© 2019 Jean-Claude Héritier

Récap

© 2019 Jean-Claude Héritier

Liens et références

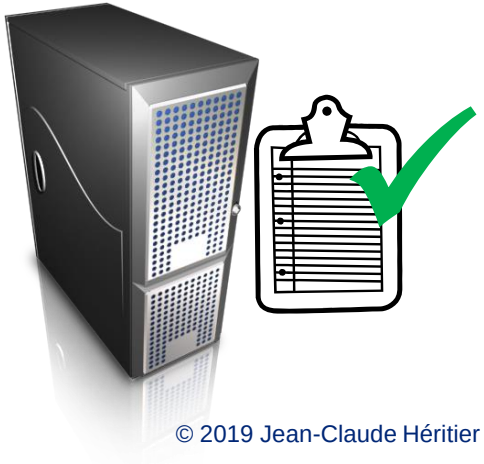
- **ANSSI** - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

- A propos du stockage des mots de passe sous forme hachée et de la sécurité par « sels »: http://www.rhyous.com/2012/06/18/how-to-effectively-salt-a-password-stored-as-a-hash-in-a-database

© 2019 Jean-Claude Héritier

IV) Mesures techniques pour sécuriser le S.I.

- Applications Métier
- Systèmes d’exploitation et postes de travail
- Réseaux
- Bases de données
- Plateformes virtualisées



© 2019 Jean-Claude Héritier

Applications métier

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

- **Objectif sécurité:**
  - **S'assurer de la fiabilité des traitements réalisés par l'application (ou chaine d'applications) supportant le processus Métier.**

Lien avec analyse des risques

→ **Risques génériques** (ex: accès…)

→ **Risques spécifiques à l'environnement Métier** (au cas par cas)

1) Contrôles généraux informatiques liés à une application:

- **Contrôles d'accès applicatifs**

Authentification des utilisateurs

- Authentification basée sur le système d'exploitation ? / gérée par l'application? / single-sign-on?
- Authentification alignée sur la politique de sécurité? (ex: paramétrage des mots de passe)

Autorisations des utilisateurs

- Identification des fonctions sensibles?
- Définition des **accès incompatibles**?
- Gestion des accès par groupes?
- Existence de profils génériques?
- Existence de comptes spéciaux (ex: profils de dépannage)?
- **Etc.**

Exemples de fonctions incompatibles?
(combinaisons « toxiques »)

Exemple de matrice des rôles par processus (SAP, ou autre ERP)

Roles / Function/ Processes	Create Vendor	Change Vendor	Post Goods Receipt	Post Payment	Process Inventory	Goods Issue	Maintain PO
Create Vendor		X	X	X			X
Change Vendor	X		X	X			X
Post Goods Receipt	X	X		X	X	X	X
Post Payment	X	X	X			X	X
Process Inventory			X				X
Goods Issue			X	X			
Maintain PO	X	X	X	X	X		

© 2007 SAP A.G. - lien

X - Existence of Conflict

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

1) Contrôles généraux informatiques liés à une application (suite):

Gestion des accès

- Accès restreints aux fonctions de gestion des accès / gestion des utilisateurs / gestion des menus.
- Contrôles des 4-yeux sur la gestion des accès (si application sensible, ex: paiements)

Gestion du paramétrage

- **Accès restreints à la gestion du paramétrage applicatif** (ex: limites, indicateurs, configuration des alertes, etc.). La logique applicative ne doit pas pouvoir être modifiée par les utilisateurs ayant un rôle dans l'exécution du processus opérationnel (ex: règles de réconciliation || utilisateurs en charge de la réconciliation)

Configuration des menus

- Les menus peuvent renvoyer à des programmes ayant un niveau de sécurité différent.

Ex: menu **« Saisie Comptable »**
- → Programme appelé: `Pgm_Saisie1` (pas d'auto-validation possible)
- → Programme appelé: `Pgm_Saisie2` (auto-validation possible)

Ligne de commande applicative

- Suivant les applications, existence de « lignes de commande » permettant d'appeler directement un programme, indépendamment de tout menu.

Ex: menu **« Saisie Comptable »** → Programme appelé: `Pgm_Saisie1` (pas d'auto-validation possible)

Ex: via ligne de commande (alternative) → Appel possible du programme: `Pgm_Saisie2` (auto-validation possible)

Logs

- Paramétrage des journaux d'évènement (logs) applicatifs:
  - types d'évènements applicatifs enregistrés?
  - traçabilité des actions utilisateurs? (basée sur les besoin métier et sur les risques)
  - intégrité des logs? (quid d'une interruption / interruption de séquence)?
  - **etc.**

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

1) **Contrôles généraux informatiques liés à une application** (suite):

Gestion des changements

Etc.

- Accès aux environnements de Test et Pré-production? (Confidentialité des données?)
- Sécurité des Transports en Production (SAP) / intégrité des changements?
(existence d'un processus standard et formel de gestion des changements au niveau applicatif)

Pré-requis: environnement de contrôle fiable (accès logiques / changements / sécurité système / sécurité physique, etc.)

Il est important de couvrir en premier lieu les risques liés à l'environnement informatique via les contrôles généraux informatiques.

2) **Contrôles applicatifs** (spécifiques à chaque application):

Contrôles sur saisies manuelles

Contrôles programmés -> analyse au cas par cas <u>en fonction des besoins métier</u> et des risques d'erreur:

exemples:
- valeurs négatives ou nulles dans champ Montant, Taux d'intérêt, etc.?
- limites (ex: contrôle VISA si débit > cash disponible sur compte client)
- **etc.**

Qualité / fiabilité des traitements

- Dans quelle mesure les contrôles applicatifs sont-ils alignés avec les besoins métier?
- De quels éléments spécifiques dépend la fiabilité des traitements informatiques de l'application?

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

- **Exemple 1: Processus de paiement - sécurité d'une application bancaire**

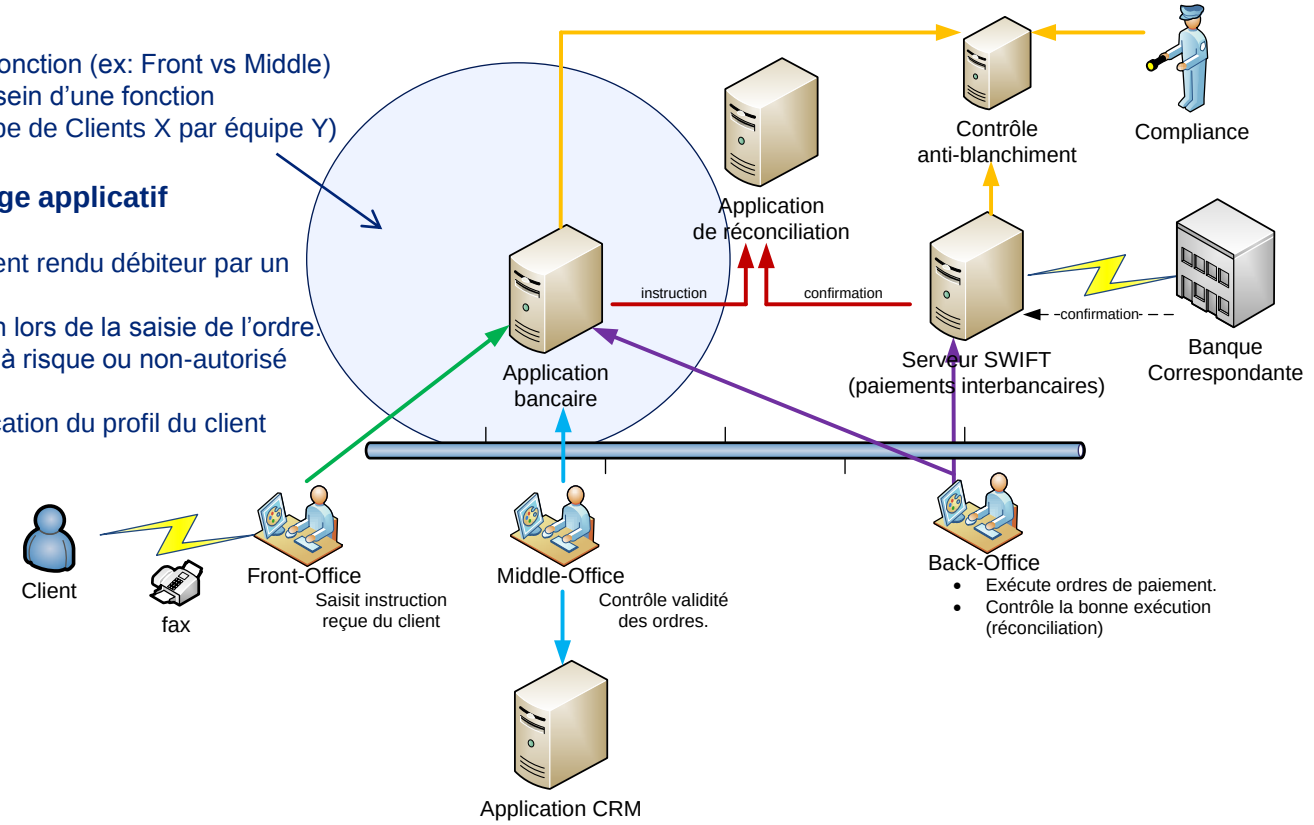
Besoin Métier:

- **Contrôles d'accès et ségrégation des tâches**
entre Front-Office / Middle Office / Back-Office / Compliance, etc.
exemples:
  - Restriction d'accès par fonction (ex: Front vs Middle)
  - Restrictions d'accès au sein d'une fonction (ex: Front: accès au groupe de Clients X par équipe Y)

- **Intégrité du paramétrage applicatif**
exemples:
  - contrôle VISA si compte client rendu débiteur par un ordre.
  - message d'alerte si doublon lors de la saisie de l'ordre.
  - message d'alerte si produit à risque ou non-autorisé (selon profil du client).
  - validation requise si modification du profil du client
  - **etc.**

Auto-matique

Manuel



© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

- **Exemple 2: Processus de paiement - sécurité d'une application CRM**

Besoin Métier:

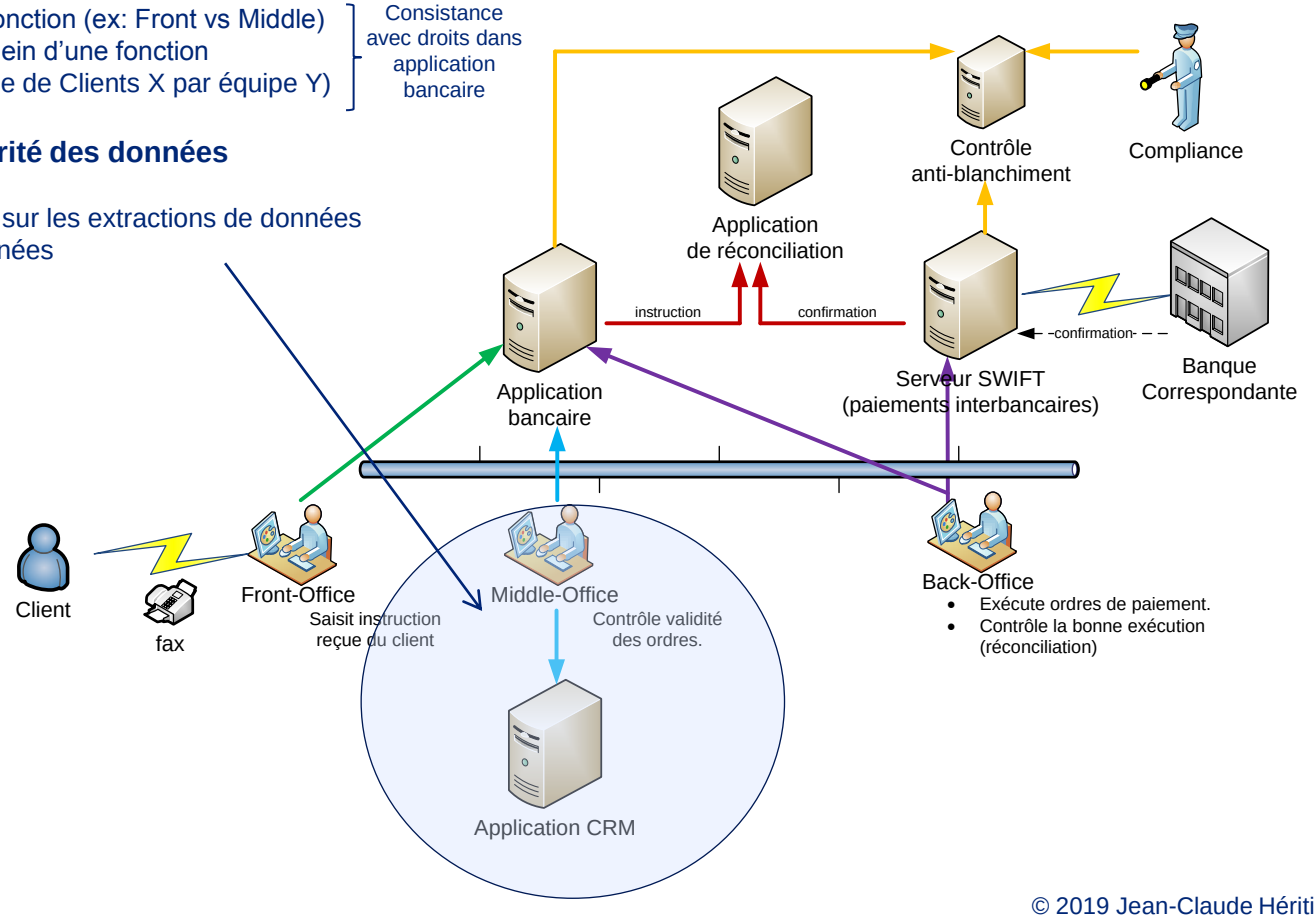
- **Contrôles d'accès aux données client**

exemples:
- Restriction d'accès par fonction (ex: Front vs Middle)
- Restrictions d'accès au sein d'une fonction (ex: Front: accès au groupe de Clients X par équipe Y)

Consistance avec droits dans application bancaire

- **Confidentialité et intégrité des données**

exemples:
- contrôles préventif / détectif sur les extractions de données
- traçabilité des MAJ des données
- **etc.**



© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

- **Exemple 3: Processus de paiement - sécurité d'une application anti-blanchiment**

Besoin Métier:

- **Contrôles d'accès**
  exemples:
  - Accès au paramétrage de la logique de détection AML.
  - Accès à la gestion des alertes.
  - Etc.

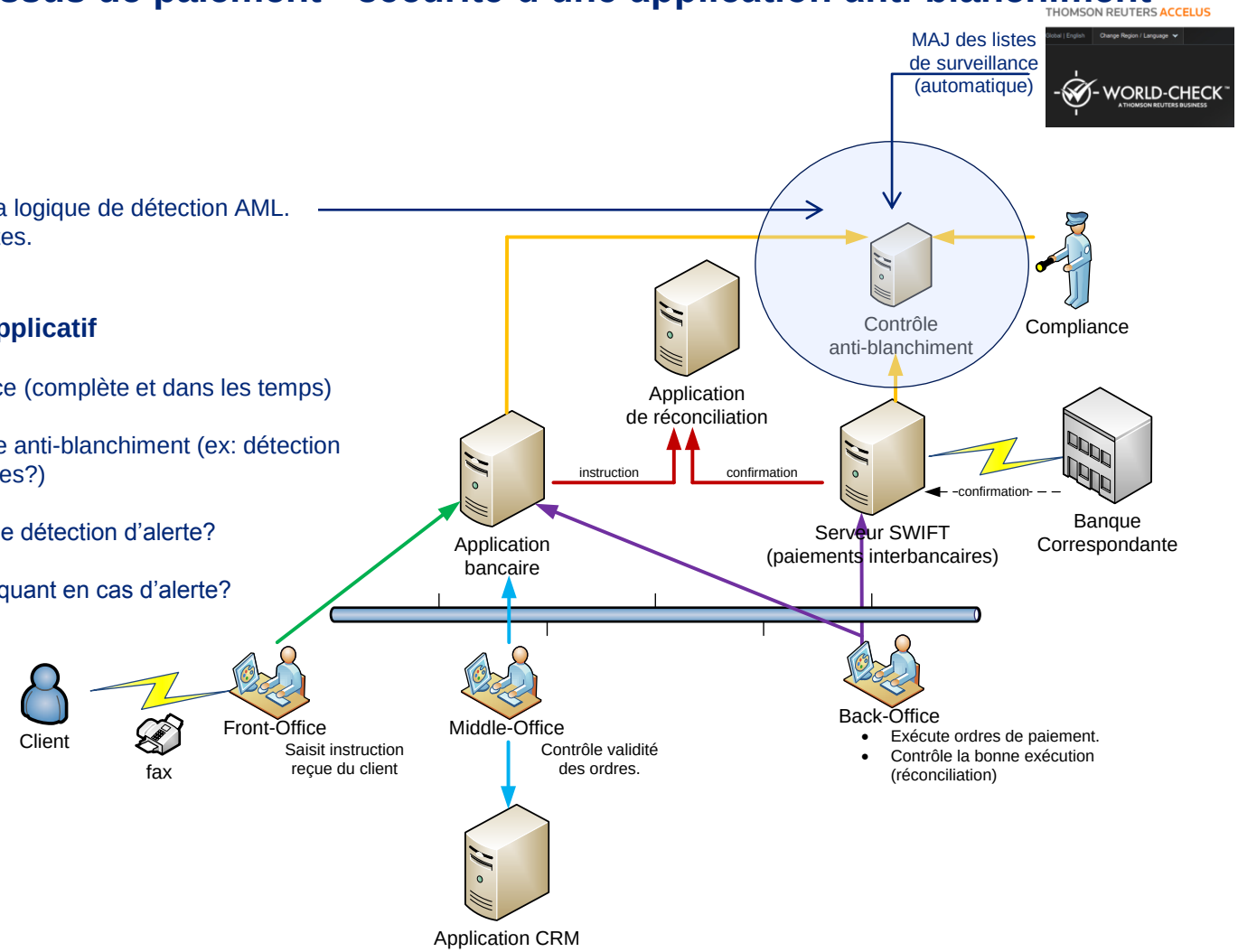
- **Intégrité du contrôle applicatif**
  exemples:
  - MAJ des liste de surveillance (complète et dans les temps)

  - Qualité / Validité du contrôle anti-blanchiment (ex: détection des correspondances partielles?)

  - Remontée d'alerte en cas de détection d'alerte?

  - Contrôle bloquant / non-bloquant en cas d'alerte?

  - **etc.**



© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Applications Métier

- **A retenir:**
  - **La nécessité d'une <u>approche basée sur les risques</u> pour évaluer les contrôles applicatifs:**
    (pré-requis: compréhension générale de l'environnement et du processus Métier)

    A) Risques génériques (ex: accès…) ➡ Approche standard pour toutes les applications

    B) Risques spécifiques à l'environnement Métier ➡ Approche au cas par cas.

    - Gestion des accès
    - Gestion du paramétrage
    - Gestion des changements
    - Contrôle des administrateurs
    - etc.

  - **Contrôles programmés VS contrôles manuels:**
    (contrôles manuels: un compromis en terme de fiabilité et un indicateur de risque potentiel)

  - **Contrôles programmés:** une fiabilité a priori meilleure mais qui n'est pas absolue.
    (ex: bug, régression après un changement, etc. => importance du processus de gestion des changements)

  - **De possibles limites fonctionnelles des applications:**
    - Exemple: application Métier qui ne supporte pas une ségrégation des tâches sur la gestion des accès.

  - **La possibilités de contrôles compensatifs pour réduire les risques de manière valable:**
    Exemples:
    - pas de ségrégation des tâches sur les entrées comptables, mais une revue manuelle du listing de toutes les entrées est effectuée par le responsable Comptabilité en fin de semaine.
    - pas de ségrégation des tâches sur la gestion des accès dans l'application de paiement, mais les mots de passe d'administration sont partagés entre deux équipes (chacune connait une partie du mot de passe).

    ➡ **Fiabilité des contrôles compensatifs à évaluer au cas par cas** (peuvent introduire de nouveaux risques).

© 2019 Jean-Claude Héritier

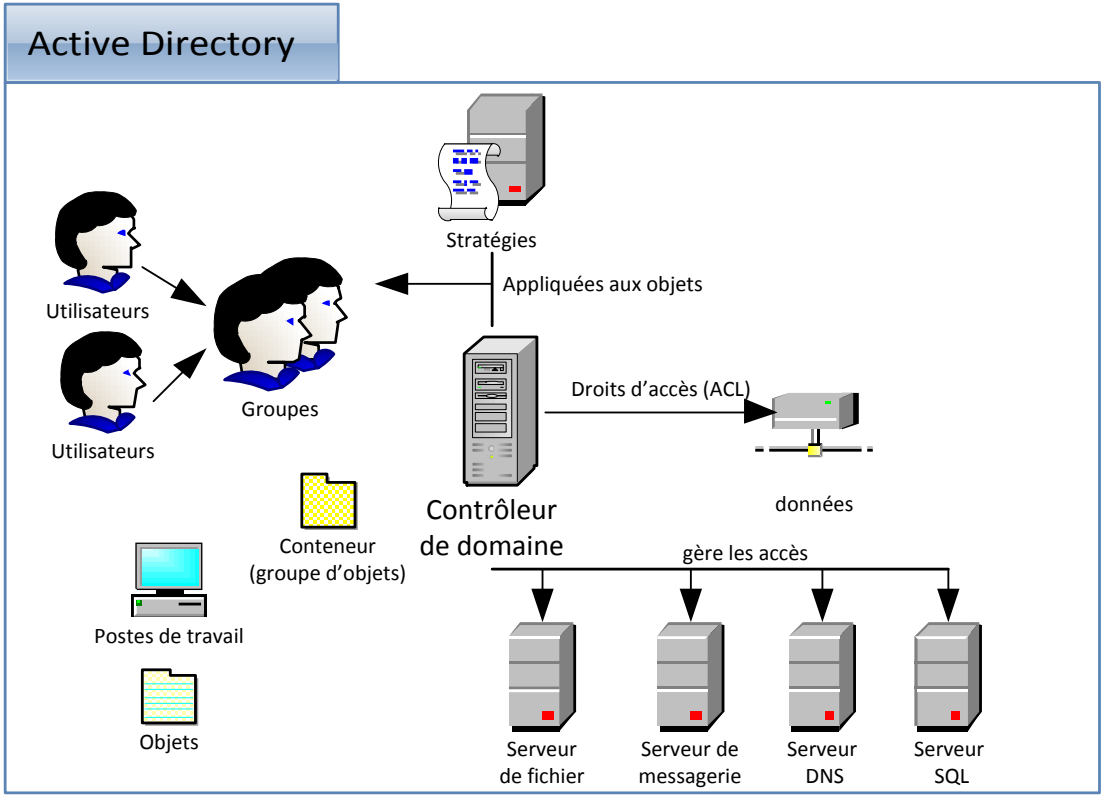
Systèmes d’exploitation et postes de travail

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Principe**
  - **Système d'exploitation serveur**
    - Gestion des accès aux ressources partagées
    - Gestion des accès aux ressources locales
  - **Fonctions**
    - Gestion du matériel (CPU, disques, mémoire, threads, I/O, etc.)
    - Gestion des processus système (synchronisation, tâches de fond, tâches planifiées)
    - Support des protocoles réseau
    - Gestion de la sécurité: utilisateurs, groupes, accès aux ressources,
    - Permet l'interaction entre les applications et le matériel.

Exemples:
- Microsoft Windows Server 2003, 2008, 2012
- GNU/Linux, *BSD
- IBM AIX
- IBM i operating System
- IBM z/OS (Mainframe)
- Apple OS X Server



© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Moyens de contrôles d'accès (Contrôleur de Domaine AD)**

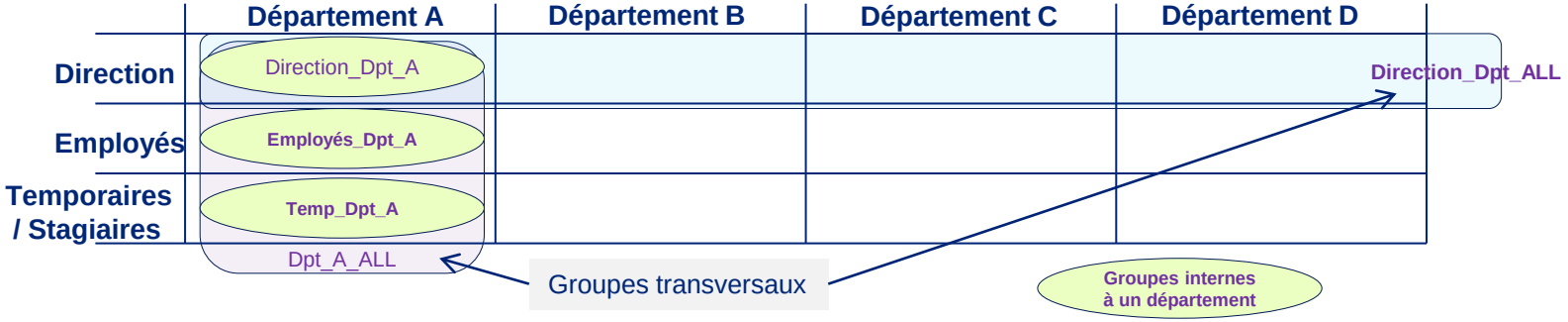
Risque: accès non-autorisé aux ressources partagées sur un Domaine

Postes de travail
- Applications
- Intranet / Internet
- Disque dur local
- Etc.

Partages réseau:
- Fichiers partagés par Service

– **Processus**
  - Gestion des accès – définition de **groupes** AD d'utilisateurs correspondants au niveau de granularité requis.

Exemple: matrice à 2 dimensions



  - Définitions de Groupes d'utilisateurs **avec Privilèges**:
    - **« Domain Admins »**
    - **« Enterprise Admins »**

    Administration du Domaine (Super-Utilisateurs) → **Réservés au personnel IT habilité**

    - **Support_IT** (exemple)

    Droits restreints (par exemple: réinitialiser un mot de passe, mais pas de création d'utilisateur)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Les permissions sur un répertoire partagé:**
  - Les permissions définissent les autorisations au niveau des objets (ex: sur un fichier ou un répertoire)
  - Les permissions sont attribuées par les propriétaires des objets (« owners ») et définies par utilisateur ou par groupe.

Quelques bonnes pratiques pour la gestion des listes de contrôle d'accès (ACLs):

• Gestion des accès par Groupes plutôt que par individus.

• Permissions simples sont préférables.

• Eviter les répertoires partagés accessibles à tous les utilisateurs du Domaine.

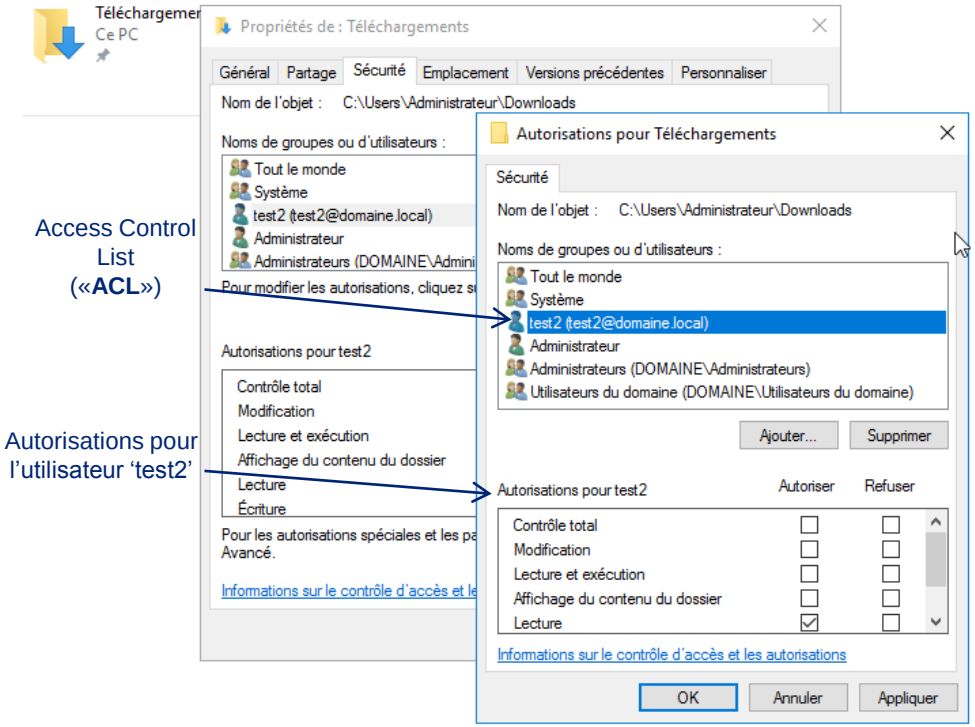
Processus:

• Processus de gestion des accès aux répertoires partagés:

- Propriétaire -> approuve les demandes d'accès

• Maintien d'un inventaire des répertoires partagés et re-certification périodique des accès (ex: annuellement).

Exemple: droits d'accès sur un répertoire (Windows Server 2016)



Points d'attention:

- présence d'utilisateurs nominatifs (au lieu de groupes) dans les ACLs?
- présence du groupe 'Tout le monde' ou 'everyone'? Présence du groupe 'Utilisateurs du Domaine' avec des droits particuliers?
- permission «Contrôle total» accessible à certains utilisateurs ne faisant pas partie de l'équipe IT?
- etc.

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Gestion des Groupes AD**

Exemple: Utilisateurs et ordinateurs (Windows Server 2016)

Utilisateurs et Groupes d'un Domaine AD

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory [WIN-QVMI
- Requêtes enregistrées
- domaine.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LABO STRASBOURG
  - Managed Service Accounts
  - SIEGE PARIS
  - Users
  - USINE LYON

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Administrateurs clés	Groupe de sécurité - Global	Les membres de ce groupe peuvent effectuer des actions administratives sur des objets c
Administrateurs clés Enterprise	Groupe de sécurité - Universel	Les membres de ce groupe peuvent effectuer des actions administratives sur des objets c
Administrateurs de l'entreprise	Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
Administrateurs du schéma	Groupe de sécurité - Universel	Administrateurs désignés du schéma
Admins du domaine	Groupe de sécurité - Global	Administrateurs désignés du domaine
Contrôleurs de domaine	Groupe de sécurité - Global	Tous les contrôleurs de domaine du domaine
Contrôleurs de domaine clonables	Groupe de sécurité - Global	Les membres de ce groupe qui sont des contrôleurs de domaine peuvent être clonés.
Contrôleurs de domaine d'entreprise en lecture seule	Groupe de sécurité - Universel	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans l'entre
Contrôleurs de domaine en lecture seule	Groupe de sécurité - Global	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans le dom
DefaultAccount	Utilisateur	Compte utilisateur géré par le système.
DnsAdmins	Groupe de sécurité - Domaine ...	Groupe des administrateurs DNS
DnsUpdateProxy	Groupe de sécurité - Global	Les clients DNS qui sont autorisés à effectuer des mises à jour dynamiques en tant que cli
Éditeurs de certificats	Groupe de sécurité - Domaine ...	Les membres de ce groupe ont l'autorisation de publier des certificats dans le répertoire
Groupe de réplication dont le mot de passe RODC est autorisé	Groupe de sécurité - Domaine ...	Les mots de passe des membres de ce groupe peuvent être répliqués sur tous les contrôle
Groupe de réplication dont le mot de passe RODC est refusé	Groupe de sécurité - Domaine ...	Les mots de passe des membres de ce groupe ne peuvent pas être répliqués sur des contr
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe de sécurité - Global	Tous les invités du domaine
lucile	Utilisateur	
Ordinateurs du domaine	Groupe de sécurité - Global	Toutes les stations de travail et les serveurs joints au domaine
Propriétaires créateurs de la stratégie de groupe	Groupe de sécurité - Global	Les membres de ce groupe peuvent modifier la stratégie de groupe pour le domaine
Protected Users	Groupe de sécurité - Global	Les membres de ce groupe bénéficient de protections supplémentaires contre les atteinte
Serveurs RAS et IAS	Groupe de sécurité - Domaine ...	Les serveurs de ce groupe peuvent accéder aux propriétés d'accès distant des utilisateurs
test2	Utilisateur	
Utilisateurs du domaine	Groupe de sécurité - Global	Tous les utilisateurs du domaine

Propriétés de : Utilisateurs du domaine

Général | Membres | Membre de | Géré par

Membres :

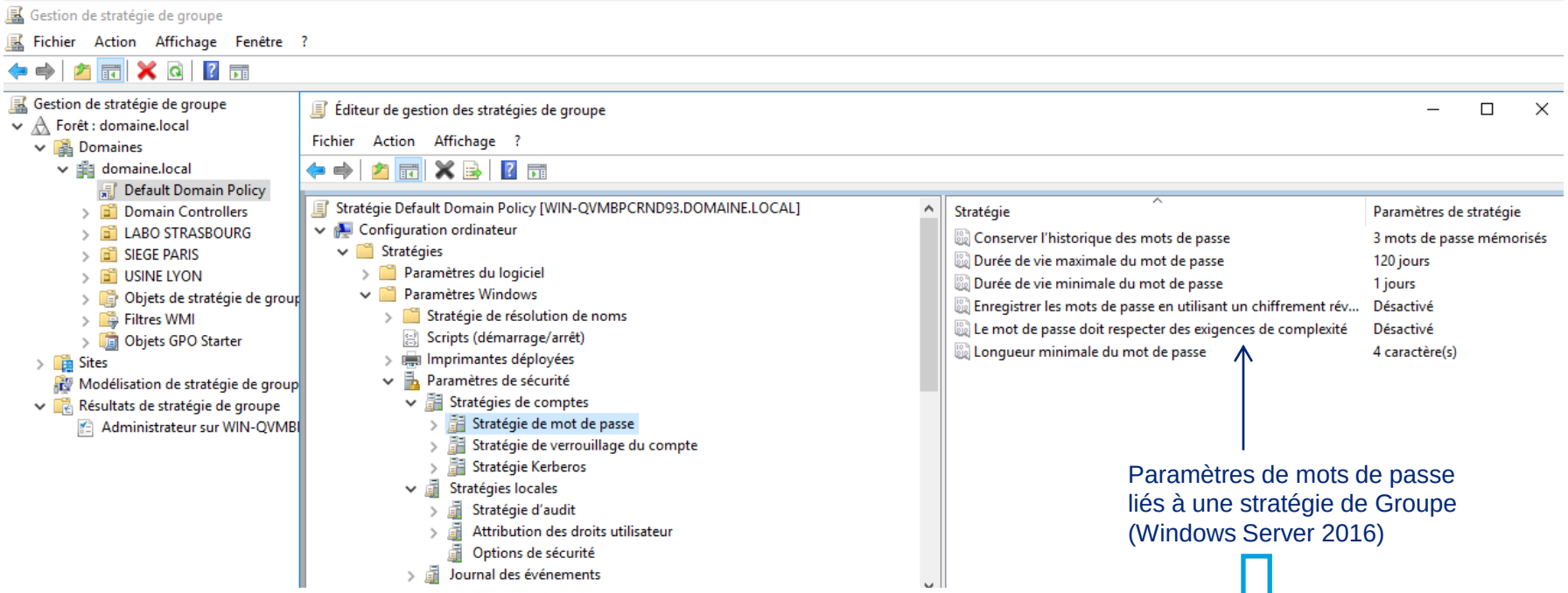
Nom	Dossier Services de domaine Active Directory
Administrateur	domaine.local/Users
DefaultAccount	domaine.local/Users
krbtgt	domaine.local/Users
lucile	domaine.local/Users
test	domaine.local
test2	domaine.local/Users

Ici: membres du groupe Utilisateurs du domaine

© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Gestion des stratégies de Groupes (« Group Policies »)**



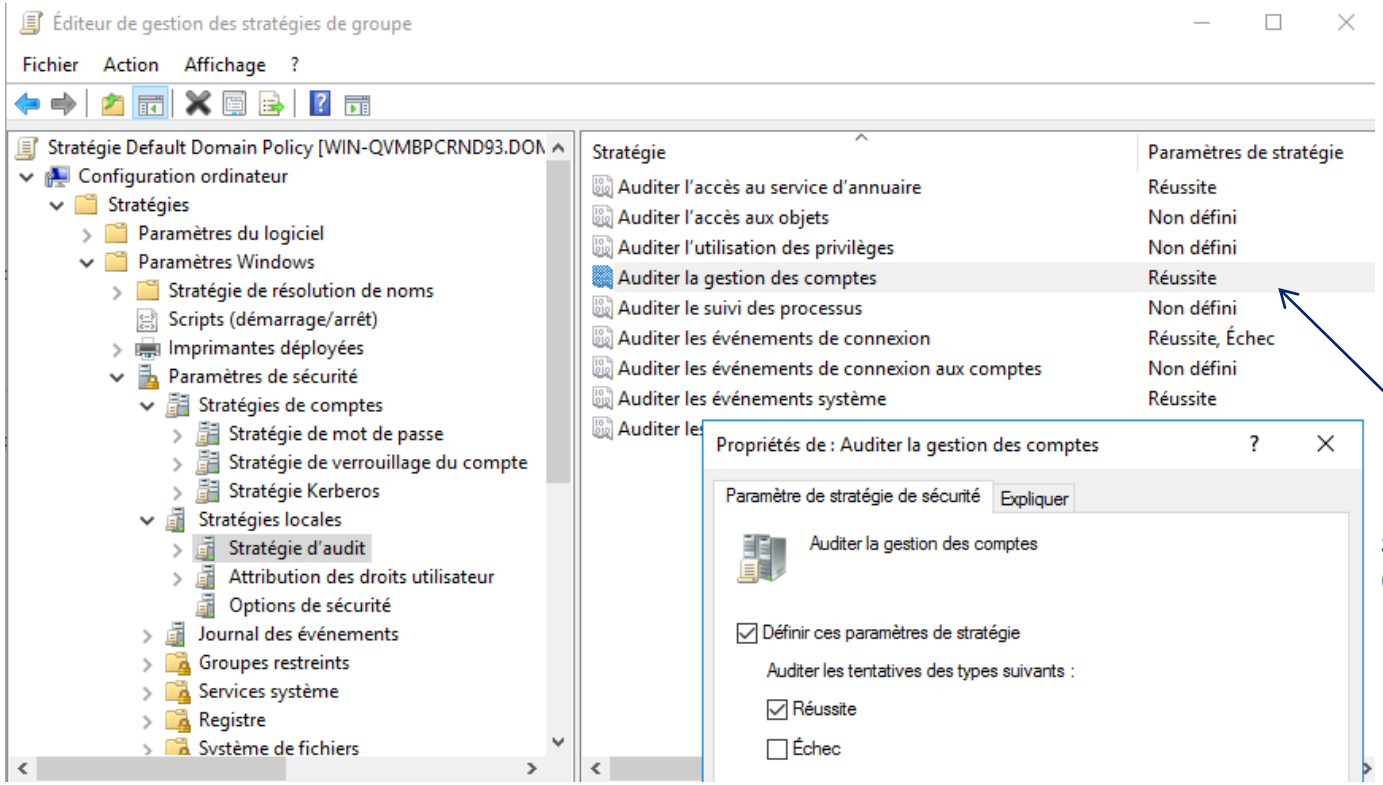
Paramètres de mots de passe liés à une stratégie de Groupe (Windows Server 2016)

Chaque stratégie de Groupe s'applique à un ou plusieurs Groupes d'utilisateurs.
(ici: « Default Domain Policy » -> s'applique généralement à tous les utilisateurs d'un Domaine)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Gestion des stratégies de Groupes (« Group Policies »)**



Stratégie d'Audit
(Windows Server 2016)

(ici: stratégie « Default Domain Policy » -> s'applique généralement à tous les utilisateurs d'un Domaine)

© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Gestion des stratégies de Groupes (« Group Policies »)**

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

- Gestion de stratégie de groupe
  - Forêt : domaine.local
    - Domaines
      - domaine.local
        - Default Domain Policy
        - Domain Controllers
        - LABO STRASBOURG
        - SIEGE PARIS
        - USINE LYON
        - Objets de stratégie de groupe
        - Filtres WMI
        - Objets GPO Starter
    - Sites
    - Modélisation de stratégie de groupe
    - Résultats de stratégie de groupe

Default Domain Policy

Étendue | Détails | Paramètres | Délégation

Default Domain Policy

Données recueillies le : 12/ 11/ 2018 22:11:02

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies de comptes/ Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	120 jours
Antériorité minimale du mot de passe	1 jours
Appliquer l'historique des mots de passe	3 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	4 caractères

Stratégies de comptes/ Stratégie de verrouillage du compte

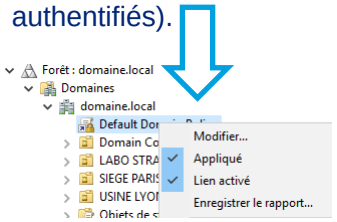
Stratégie	Paramètre
Durée de verrouillage de comptes	60 minutes
Réinitialiser le compteur de verrouillages du compte après	60 minutes
Seuil de verrouillage de comptes	30 tentative d'ouverture de session non valides

Stratégies de comptes/ Stratégie Kerberos

Stratégie locale/ Stratégie d'audit

Stratégie	Paramètre
Auditer l'accès au service d'annuaire	Opération réussie
Auditer la gestion des comptes	Opération réussie
Auditer les événements de connexion	Succès, Échec

Il est possible d'extraire tous les paramètres définis par une stratégie de compte au format HTML.
(ici la « default domain policy » qui s'applique à tous les utilisateurs authentifiés).



Astuce:
la commande `gpresult /h output.html` permet à tout utilisateur d'extraire au format html les paramètres de sécurité qui lui sont appliqués par la combinaison de toutes les stratégies de groupe (« Resultant Set Of Policies »)

```
PS C:\Users\Administrateur\Desktop> gpresult.exe /H output.html
```
(avec PowerShell)

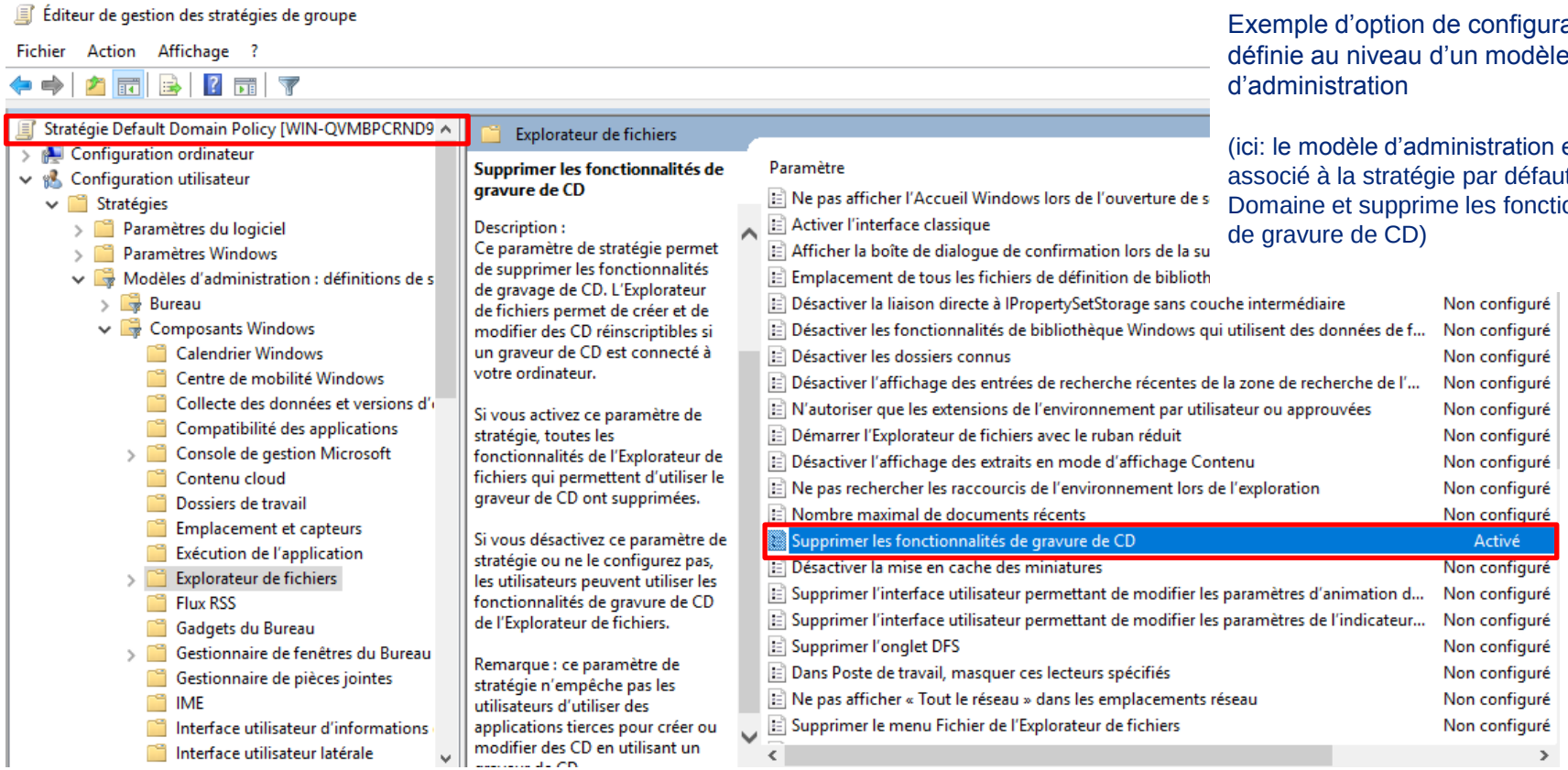
```
C:\Users\Administrateur\Desktop>gpresult /h output1.html
```
(avec cmd.exe)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Systèmes d'exploitation et postes de travail

- **Gestion des stratégies de Groupes –** Modèles d'administration (**Administrative Templates**)

Les modèles d'administration permettent de définir des options de sécurité avancées au niveau des GPO:
=> Option simple pour personnaliser la configuration de sécurité



Exemple d'option de configuration définie au niveau d'un modèle d'administration

(ici: le modèle d'administration est associé à la stratégie par défaut du Domaine et supprime les fonctionnalités de gravure de CD)

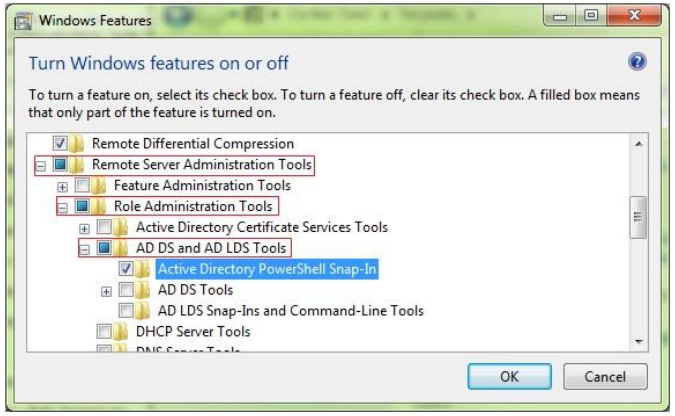
© 2019 Jean-Claude Héritier

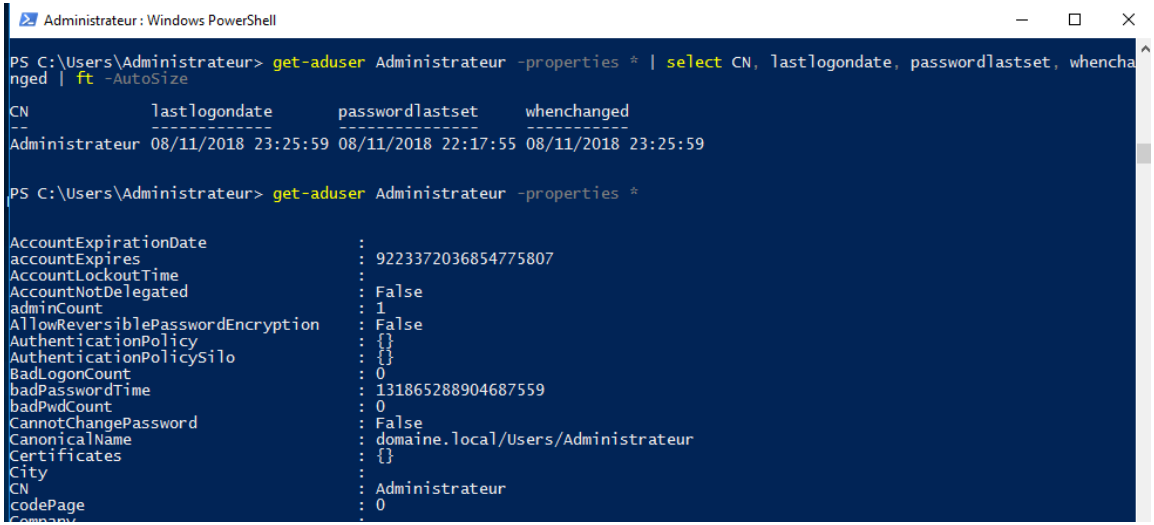
Systèmes d'exploitation et postes de travail

- **Quelques commandes utiles:**

`net users /domain`	-> liste tous les utilisateurs d'un domaine
`net users toto /domain`	-> affiche les propriétés de l'utilisateur toto sur le contrôleur de Domaine
`net groups /domain`	-> liste tous les groupes définis sur un domaine
`net group "Domain Admins" / domain`	-> liste les membres du groupe 'Domain Admins' définis sur le contrôleur de Domaine

- **PowerShell snap-in**

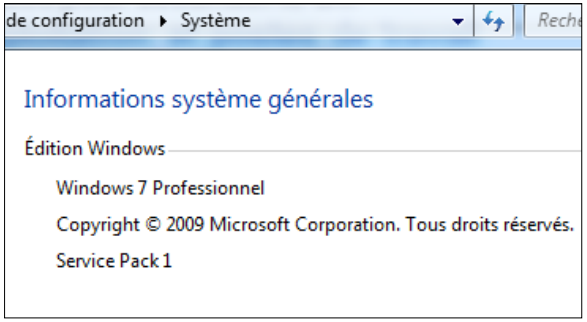




Etc.

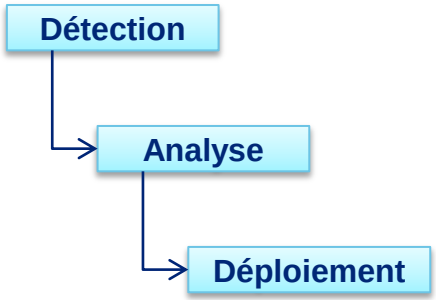
© 2019 Jean-Claude Héritier

- **Gestion des vulnérabilités et des correctifs logiciels (*patch management*)**
  - **Contexte:**
    - Existence de vulnérabilités plus ou moins critiques dans les systèmes d'exploitation (publiques et non-publiques).
    - Publication de correctifs par les éditeurs durant le cycle de vie du produit.
      - Exemples de correctifs publiés par Microsoft:
        - Service Packs,
        - Correctifs en cycle mensuel
        - Correctifs publiés hors-cycle (correction de failles critiques)



Risques: incompatibilités logicielles ou matérielles avec un correctif de sécurité. **Tous les patchs ne sont pas pertinents.**

  - **Enjeux:**
    - Gérer de manière optimale (« industrialiser ») les processus de détection, d'analyse et de déploiement des mises à jours de sécurité logicielles.



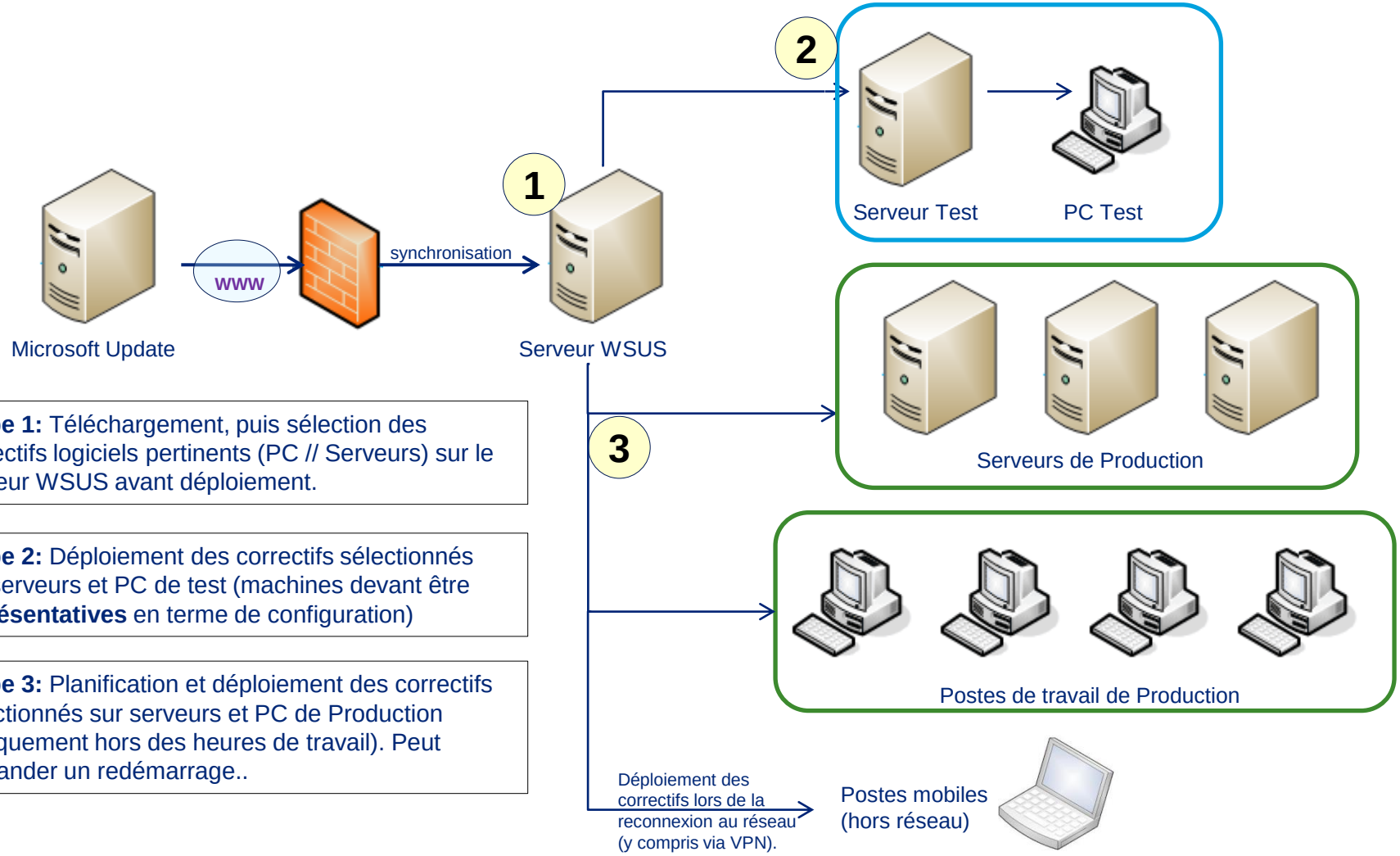
- **Processus de veille sécurité.**
- **Outils de gestion** des correctifs couvrant l'ensemble du parc informatique:
  - référence tous les composants (systèmes, bases de données, applications…)
  - maintien un historique des mises à jours installées.
- .Définition de stratégies de déploiement des correctifs:
  - **tests avant déploiement** (permettent de prévenir les effets de bord / régressions).

Exemples de solutions:
- Microsoft Software Update Services
- Altiris, Shavlik, Patchlink, etc.

© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Gestion des vulnérabilités et des correctifs logiciels (*patch management*)**



Etape 1: Téléchargement, puis sélection des correctifs logiciels pertinents (PC // Serveurs) sur le serveur WSUS avant déploiement.

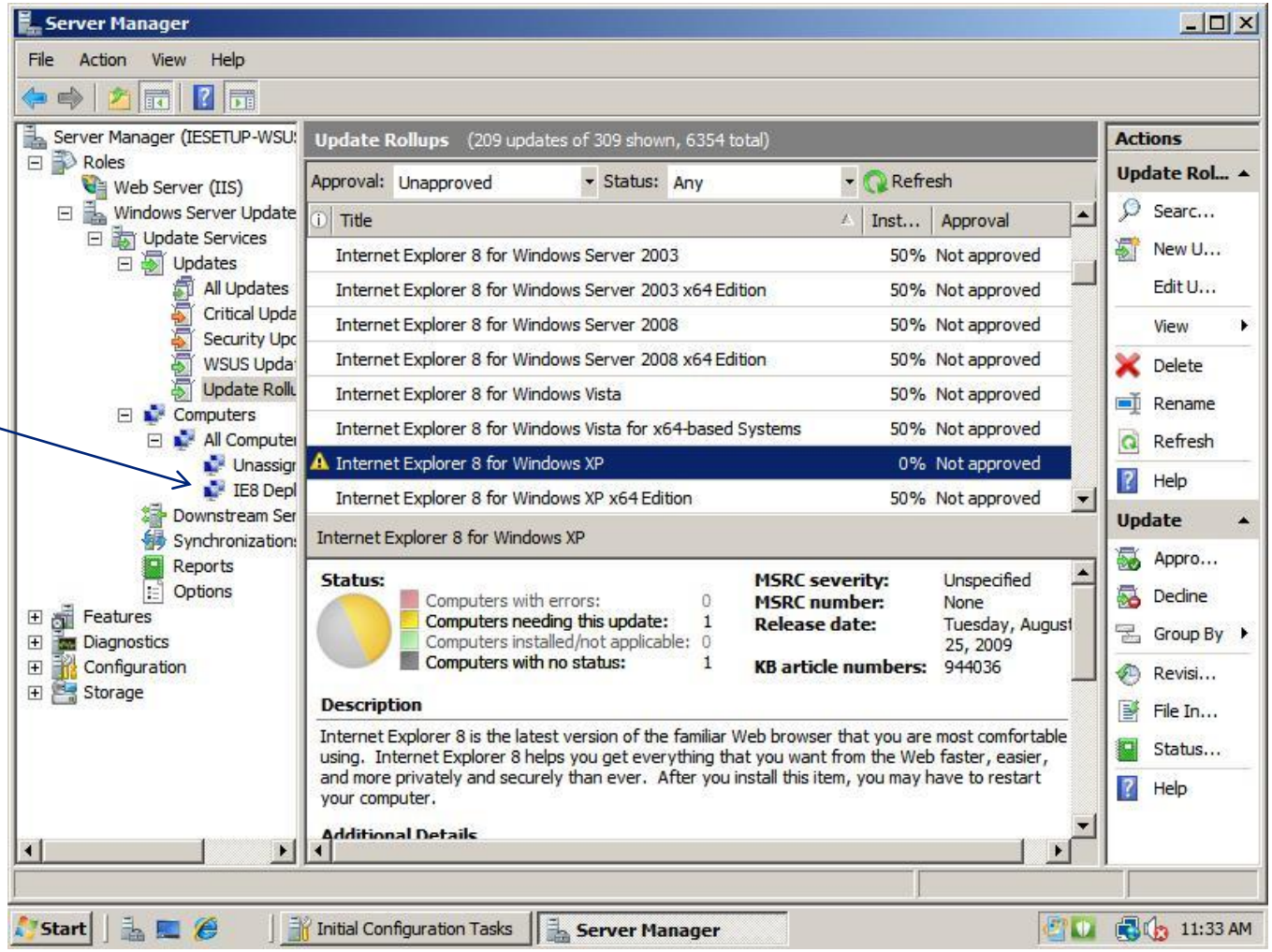
Etape 2: Déploiement des correctifs sélectionnés sur serveurs et PC de test (machines devant être **représentatives** en terme de configuration)

Etape 3: Planification et déploiement des correctifs sélectionnés sur serveurs et PC de Production (typiquement hors des heures de travail). Peut demander un redémarrage..

© 2019 Jean-Claude Héritier

- **Gestion des vulnérabilités et des correctifs logiciels (*patch management*)**
  - **Exemple: console d'administration de Microsoft Windows Update Services (WUS)**

Groupe de machine cible pour le déploiement d'Internet Explorer 8



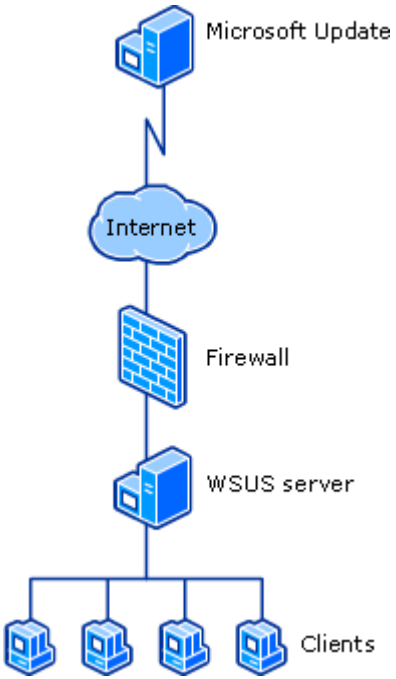
Source: http://blogs.msdn.com

© 2019 Jean-Claude Héritier

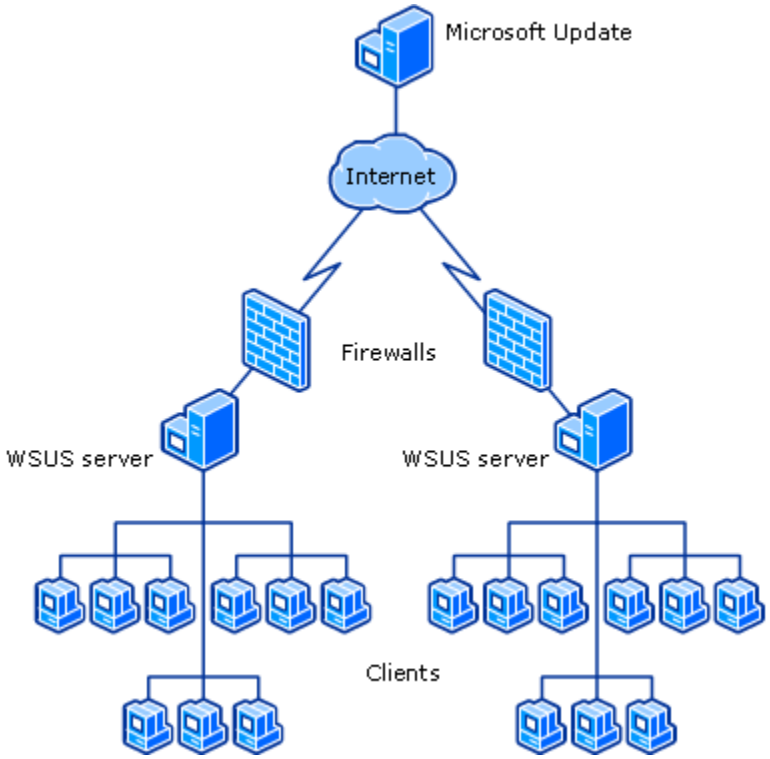
Systèmes d'exploitation et postes de travail

- **Gestion des vulnérabilités et des correctifs logiciels (*patch management*)**
  - **Exemple: Windows Update Services (WUS)**

Cas #1: Un seul serveur WSUS



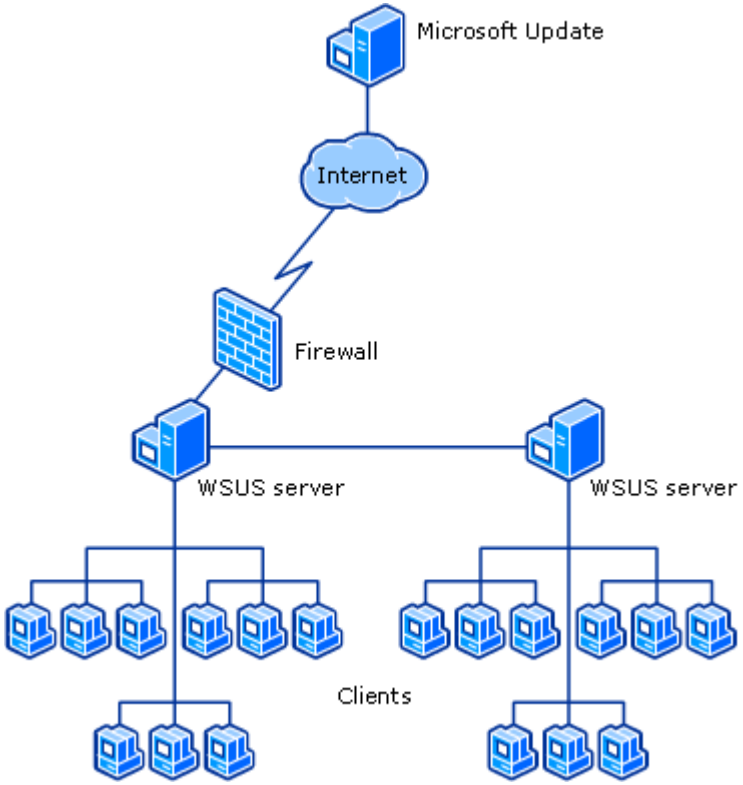
Cas #2: Multiples serveurs WSUS indépendants
(ex: cas de filiales gérant leurs correctifs de manière indépendante)



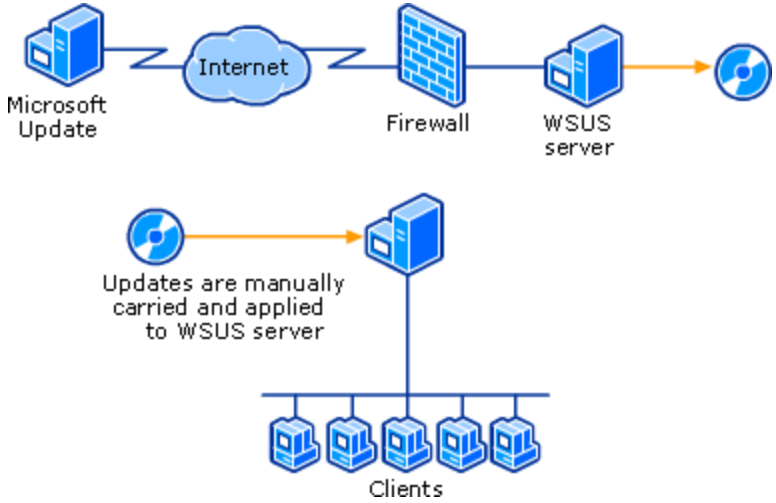
© 2019 Jean-Claude Héritier

- **Gestion des vulnérabilités et des correctifs logiciels (*patch management*)**
  - **Exemple: Windows Update Services (WUS)**

Cas #3: Multiples serveurs WSUS avec synchronisation interne
(un seul serveur WSUS est exposé à l'Internet)



Cas #4: Serveurs WSUS non-connectés (ou connectivité limitée)
Une synchronisation hors ligne est possible.



© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Protection antivirus / anti-malware:**
  - Elément de sécurité incontournable sur les postes de travail **et** sur les serveurs.
  - Fonctionnement basé sur des fichiers de signature (à jour) et sur une analyse heuristique (basé sur le comportement).

Tendance: Sophistication des menaces: virus « polymorphes » et « métamorphes », rootkits, etc..

Quelques bonnes pratiques pour la gestion des contrôles anti-virus / anti-malware:

• Protection homogène du parc informatique:
- tous les serveurs
- tous les postes de travail
- cas des utilisateurs nomades / hors ligne -> mise à jour avant reconnexion au réseau interne.

• Antivirus maintenus à jour (version et bases de signatures).

•**Défense en profondeur** par plusieurs niveaux de contrôle anti-virus:
- **DMZ:** passerelles e-mail et web (idéalement inspection du trafic SSL).
- Antivirus sur serveurs (y compris Linux / Unix)
- Antivirus sur postes de travail et équipements mobiles.

} Assurer au minimum deux niveaux de contrôle pour les fichiers en provenance de l'Internet.

• **Principe de moindre privilège**: pas de droits Administrateurs locaux par défaut pour les utilisateurs standards.

Processus:
• Processus de surveillance des alertes (contrôles détectifs en cas de non-mise à jour).

• Remontée des alertes.

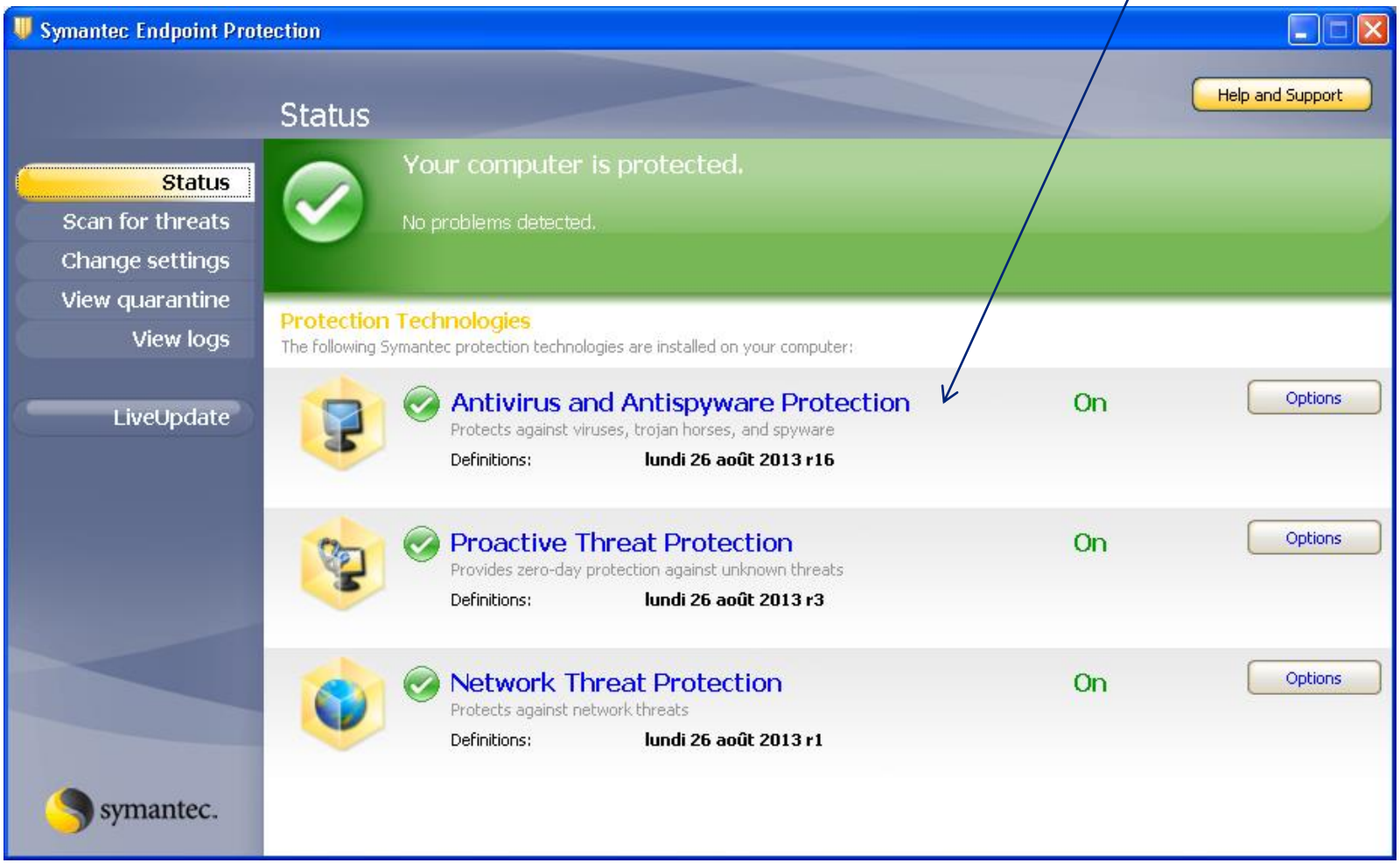
• Politique de sécurité et sensibilisation des utilisateurs.

© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Protection antivirus / anti-malware:**

Exemple de **protection à jour** sur un poste de travail.

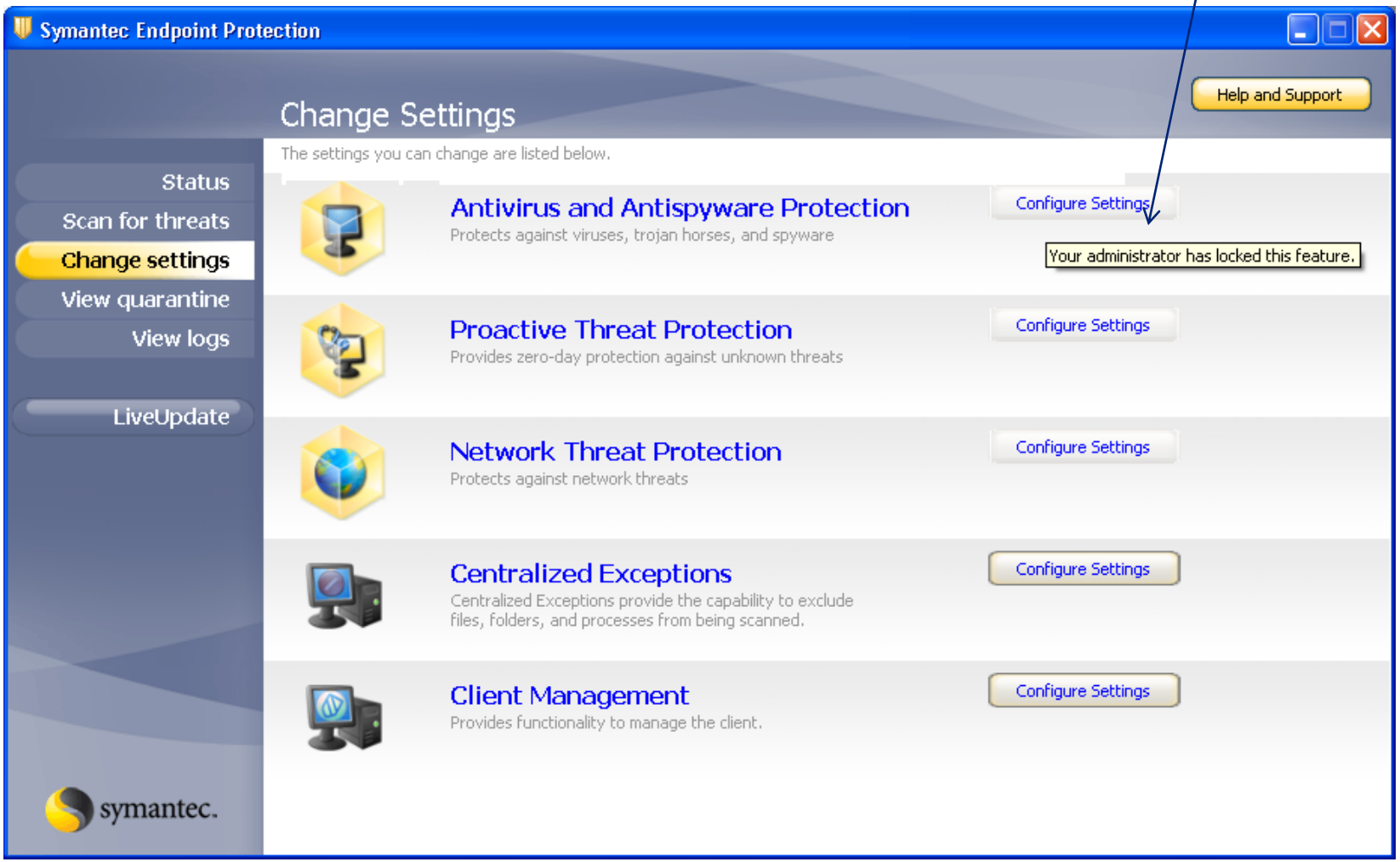


© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Protection antivirus / anti-malware:**

Droits d'accès limités pour un utilisateur standard.



© 2019 Jean-Claude Héritier

Systèmes d'exploitation et postes de travail

- **Contrôles des médias amovibles:**

Quizz: quels périphériques locaux de sortie de données sur un poste de travail ou PC portable standard?

- **Ports USB**
- **Ports Firewire**
- **Lecteurs de cartes SD**
- **Graveur DVD**
- **Wifi**

Mesures de contrôle:

Exemple: Blocage des périphériques par Stratégie de Groupe (Windows 7)

System/Removable Storage Access

Policy	Setting
All Removable Storage classes: Deny all access	Enabled
CD and DVD: Deny read access	Enabled
CD and DVD: Deny write access	Enabled
Floppy Drives: Deny read access	Enabled
Floppy Drives: Deny write access	Enabled
Removable Disks: Deny read access	Enabled
Removable Disks: Deny write access	Enabled
Tape Drives: Deny read access	Enabled
Tape Drives: Deny write access	Enabled
WPD Devices: Deny read access	Enabled
WPD Devices: Deny write access	Enabled

Clés USB sécurisées (ici:Ironkey et Kingston DataTraveller)

© 2019 Jean-Claude Héritier

Réseaux

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Fonctions clé d'un réseau informatique:**
  - **Partage des ressources (sur un mode généralement client-serveur):**
    - Partage d'infrastructure (ex: imprimantes, systèmes de sauvegarde, etc.)
    - Partage d'informations (ex: fichiers clients, état des stocks, rapports financiers, etc.)
  - **Moyen de communication** (ex: messagerie électronique)
  - **Commerce électronique** / activités en ligne

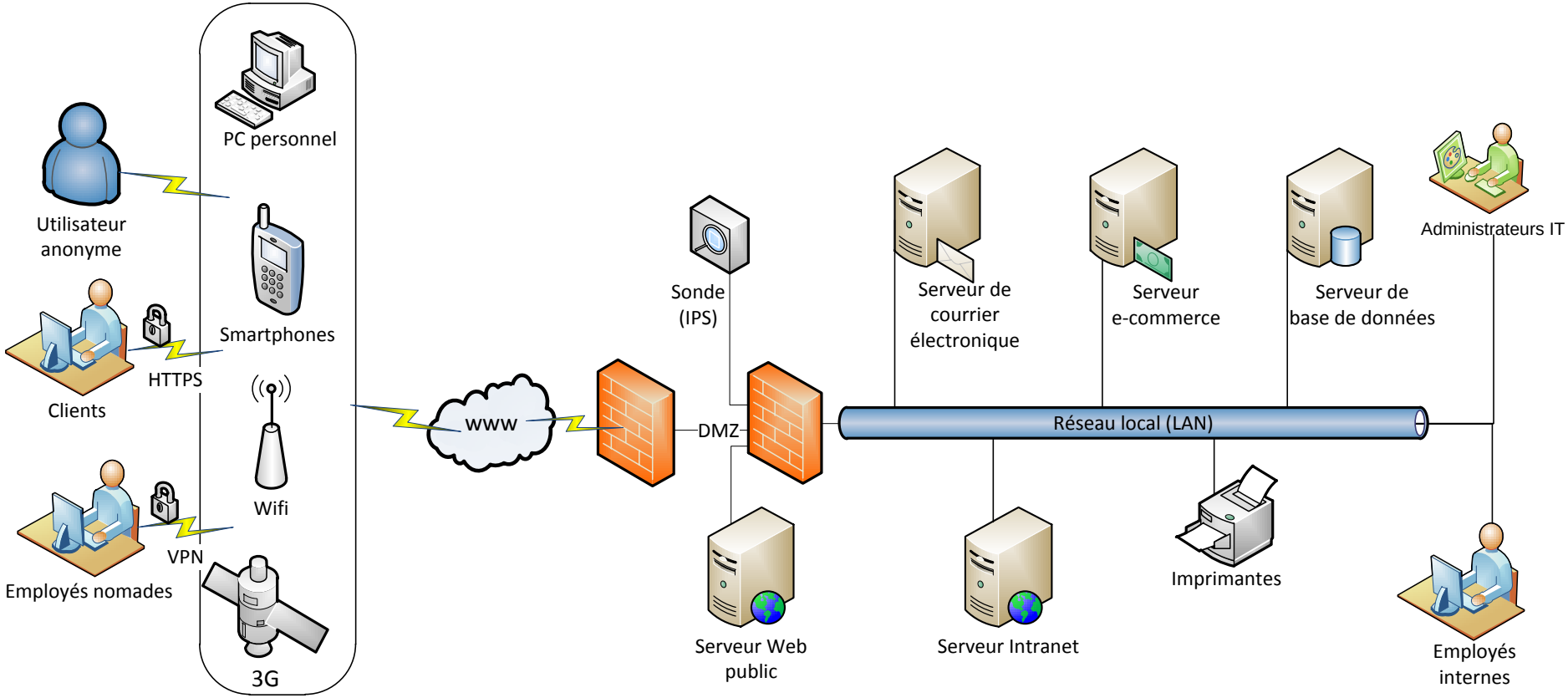
Importance vitale du réseau informatique – 1ère ligne de défense logique

- **Challenges en terme de sécurité:**
  - **Dissémination des utilisateurs** (internes, employés nomades, clients, publics)
  - **Interconnexion des réseaux ayant différents niveaux de sécurité**
    ex: réseaux privés accédés depuis des réseaux publics
  - **Multiplication des utilisations et des protocoles** (sans fil, 3G, réseaux privés virtuels, NFC, etc.)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Exemple de réseau informatique:**



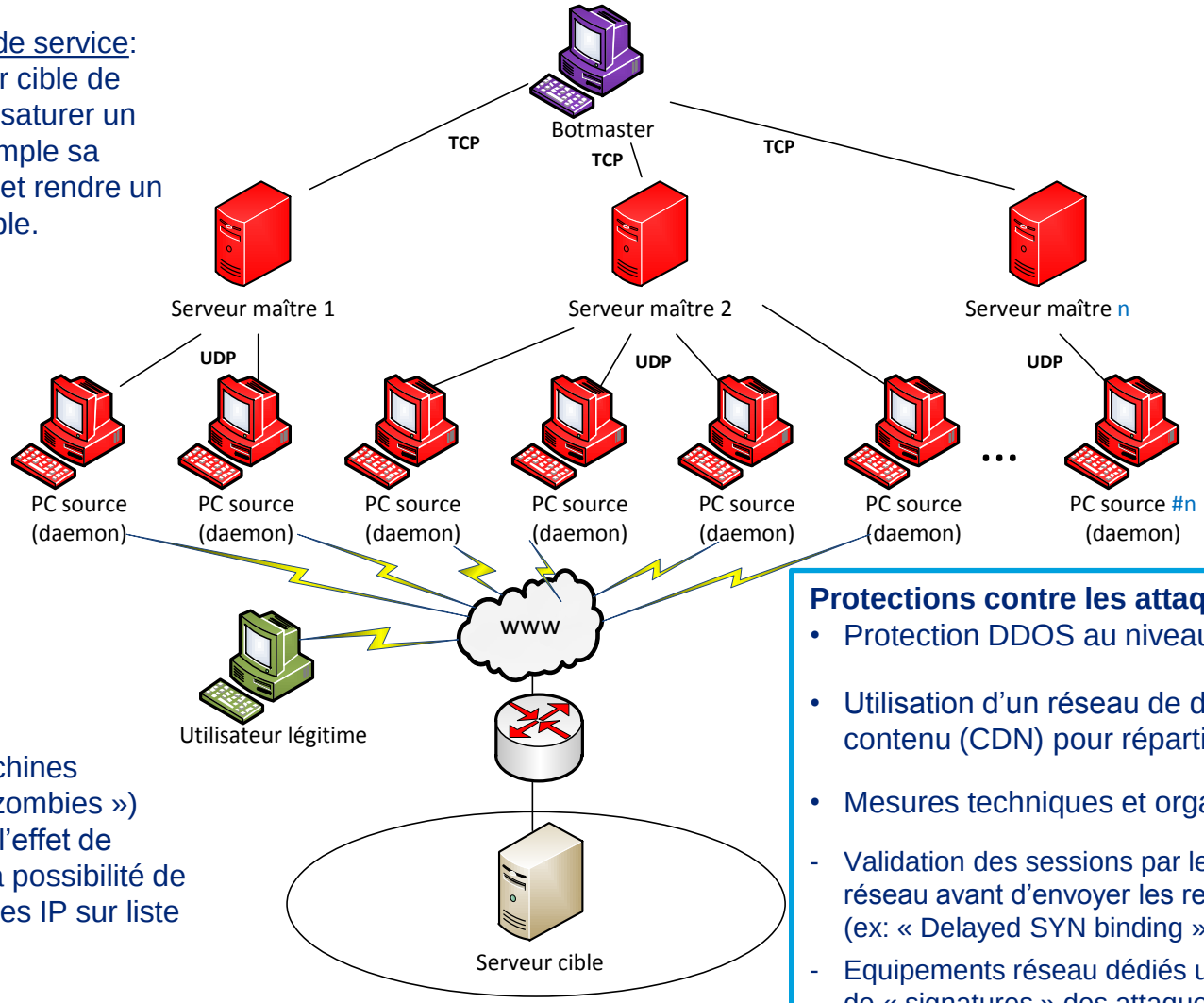
QUIZZ: Quels risques et quels contrôles d'accès?

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Exemple de menace: attaque par déni de service distribué (DDOS)**

Principe du déni de service: inonder le serveur cible de requêtes, afin de saturer un élément (par exemple sa bande passante) et rendre un service indisponible.



DDOS:
Utilisation de machines compromises (« zombies ») pour démultiplier l'effet de levier (et limiter la possibilité de mettre les adresses IP sur liste noire).

Protections contre les attaques DDOS:

- Protection DDOS au niveau des FAI (option)
- Utilisation d'un réseau de diffusion de contenu (CDN) pour répartir la charge DDOS
- Mesures techniques et organisationnelles:
  - Validation des sessions par les équipements réseau avant d'envoyer les requêtes au serveur (ex: « Delayed SYN binding »)
  - Equipements réseau dédiés utilisant des bases de « signatures » des attaques. Etc.

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Classification des réseaux:**

Distance entre processeurs	Classification
1 m	**Réseau personnel**
10 m -> 1 km	**LAN** (ex: salle, immeuble, campus)
1 km -> 10 km	**MAN** (réseau métropolitain)
10 km -> 1000 km	**WAN** (wide area network)
Planète entière	**Internet**

→ Exemple: filiales à Paris, Londres, Sydney (interconnectées par un VLAN)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

A retenir:
- Chaque couche correspond à un niveau d'abstraction,
- Chaque couche assure une fonction bien définie.
- Chaque couche rend des services à la couche supérieure.
- Chaque couche peut utiliser les protocoles qu'elle veut sans que cela affecte le fonctionnement des couches supérieures.

- **Hiérarchie des protocoles réseaux:**

- Couches hautes, orientées application
- Fonctions assurées par les **protocoles applicatifs**

- Couches basses, orientées communications.
- Fonctions assurées en général par le **système d'exploitation**

Modèle OSI	Modèle TCP/IP
7. Application	**Application**
6. Présentation	*Absent de ce modèle*
5. Session	*Absent de ce modèle*
4. Transport	**Transport**
3. Réseau	**Internet**
2. Liaison de données	**Liaison**
1. Physique	*Absent de ce modèle*

Application: contient les protocoles utilisés par les applications (**ex: HTTP, FTP, SSH, SMTP, POP3; Telnet, etc**).

Transport: gère la segmentation des flux applicatifs en plus petits paquets et assure le contrôle des messages en réception (renforce les garanties de livraison) (**ex: TCP, UDP**). **Notion de port.**

Réseau: gère l'acheminement de paquets, indépendamment les uns des autres, vers leur destination (**ex: IP**). **Notion d'adresse IP.**
(analogie avec le courrier postal qui ne se préoccupe pas des timbres, formats d'enveloppes, etc)

Liaison: gère l'envoi de messages de longueur finie entre deux machines directement connectées (**ex: Ethernet**).

Physique: gère la transmission de bits sous forme de signaux électriques.

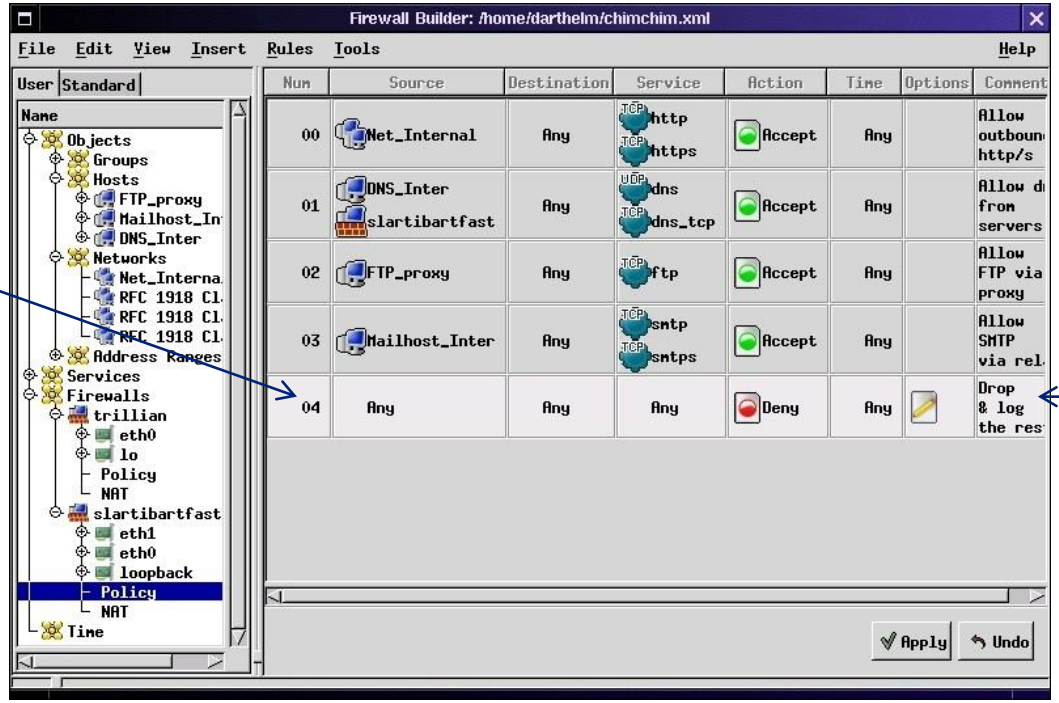
Les 5 couches à retenir

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Les Firewalls**
  - **Permettent de contrôler quels types de communications sont autorisées sur un réseau informatique:**
    - Au niveau de la **couche réseau**: origine ou destination des paquets (IP).
    - Au niveau de la **couche transport**: ports TCP ou UDP utilisés.
    - Au niveau de la **couche applicative**: vérifient la complète conformité du paquet à un protocole attendu (ex: vérifient que seul du trafic HTTP circule sur le port 80)
      - Permet de contrôler l'utilisation de tunnels TCP (peuvent être utilisés pour contourner le filtrage par port).
  - **Principe de base: tout ce qui n'est pas autorisé doit être bloqué (« need-to-know »):**

Exemple de liste de contrôle d'accès (ACL)
(ici Firewall Builder pour iptables):



Règle de blocage par défaut
(le trafic qui n'est pas autorisé est bloqué)

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Quelques règles de bonne gestion des firewalls**

QUIZZ: quels contrôles (préventifs & détectifs)?

Aspects organisationnels:

– Utilisation de règles simples, explicites et documentées pour limiter les risques d'erreurs.

– **Gestion des accès**, qui doivent être restreints aux seuls administrateurs réseau autorisés - idéalement depuis un réseau dédié (VLAN) ou des machines spécifiques. Aucune interface d'administration ne doit être accessible depuis l'Internet.

– **Gestion des changements** : autorisation des modifications / visa par le RSSI avant toute modification.

– **Mise à jour régulière des correctifs de sécurité** sur les firewalls.

– **Contrôle des alertes** en temps réel (par exemple, toute modification de la configuration doit générer une alerte)

– **Tests intrusifs périodiques** (scanners de ports, scanners de vulnérabilités, tests intrusifs manuels, etc.)

Aspects techniques:

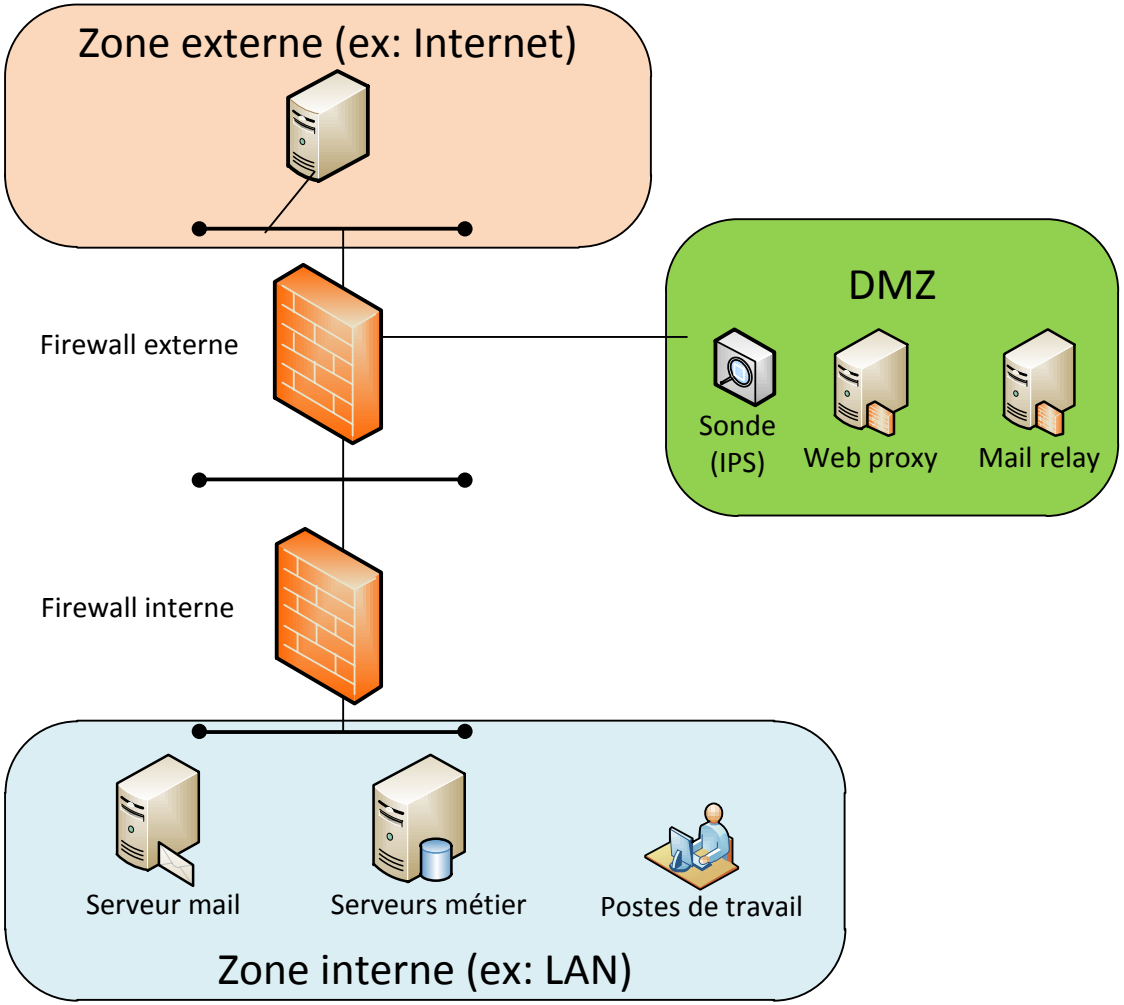
– **Capacité à détecter** les attaques, les inconsistances de session (« stateful inspection »), l'usurpation d'adresse, etc.

– **Défense en profondeur**: Utilisation de **deux niveaux de firewalls** formant une **DMZ**, idéalement de technologies complémentaires:

  - Exemple: CISCO ASA comme firewall externe et Juniper Netscreen comme firewall interne.

© 2019 Jean-Claude Héritier

- **DMZ – quelques exemples de conceptions**

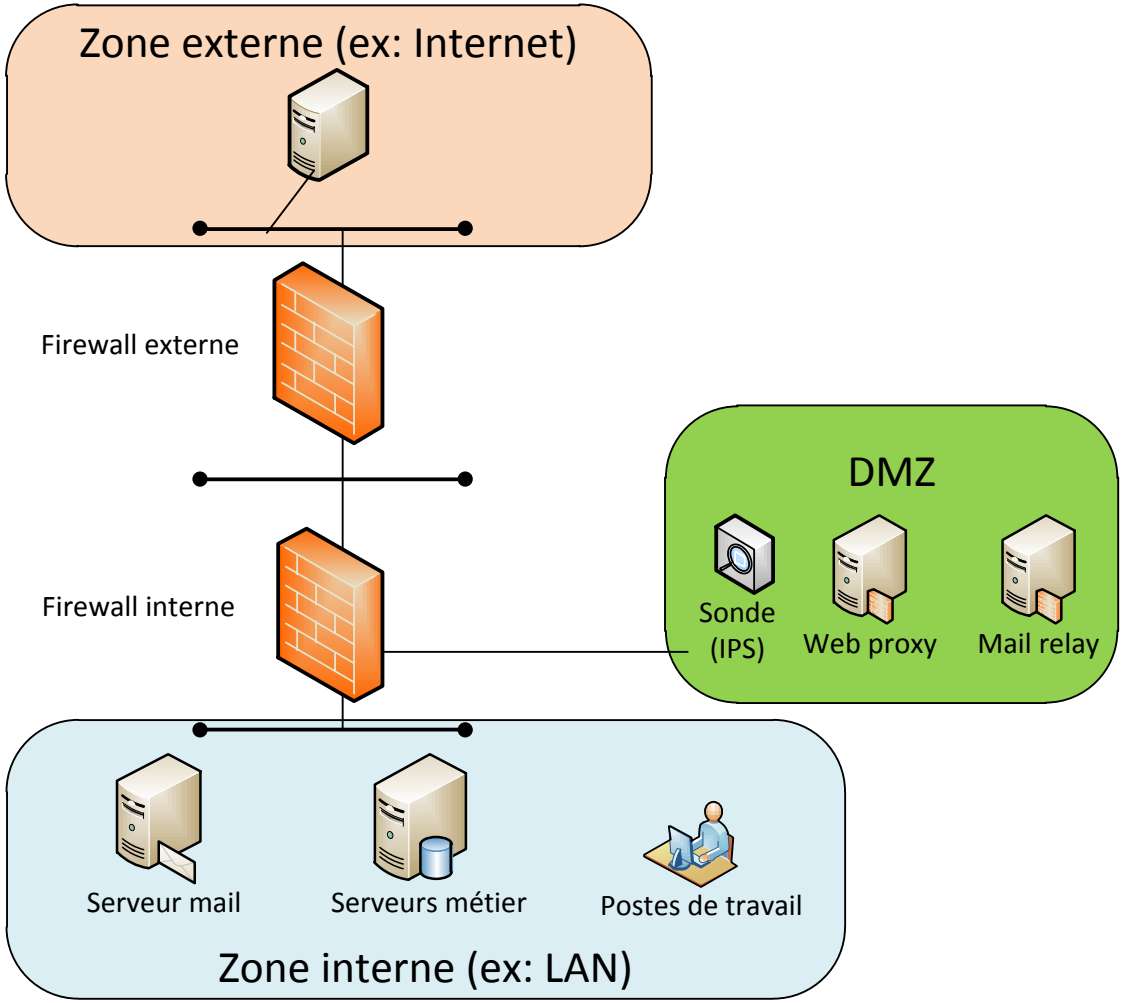


Cas #1 : DMZ sur le firewall externe

Les services en DMZ ne sont protégés que par un seul niveau de Firewall
-> non-recommandé

© 2019 Jean-Claude Héritier

- **DMZ – quelques exemples de conceptions**



Cas #2 : DMZ sur le firewall interne

- Le trafic externe passe par deux firewalls avant d'atteindre la DMZ.
- Le trafic de la DMZ vers le réseau interne (généralement plus complexe) ne passe que par un seul niveau de firewall, ce qui réduit la complexité et les coûts d'administration.
- Plus facile à comprendre car seuls les flux externes passent par le firewall externe.

Conception généralement recommandée.

© 2019 Jean-Claude Héritier

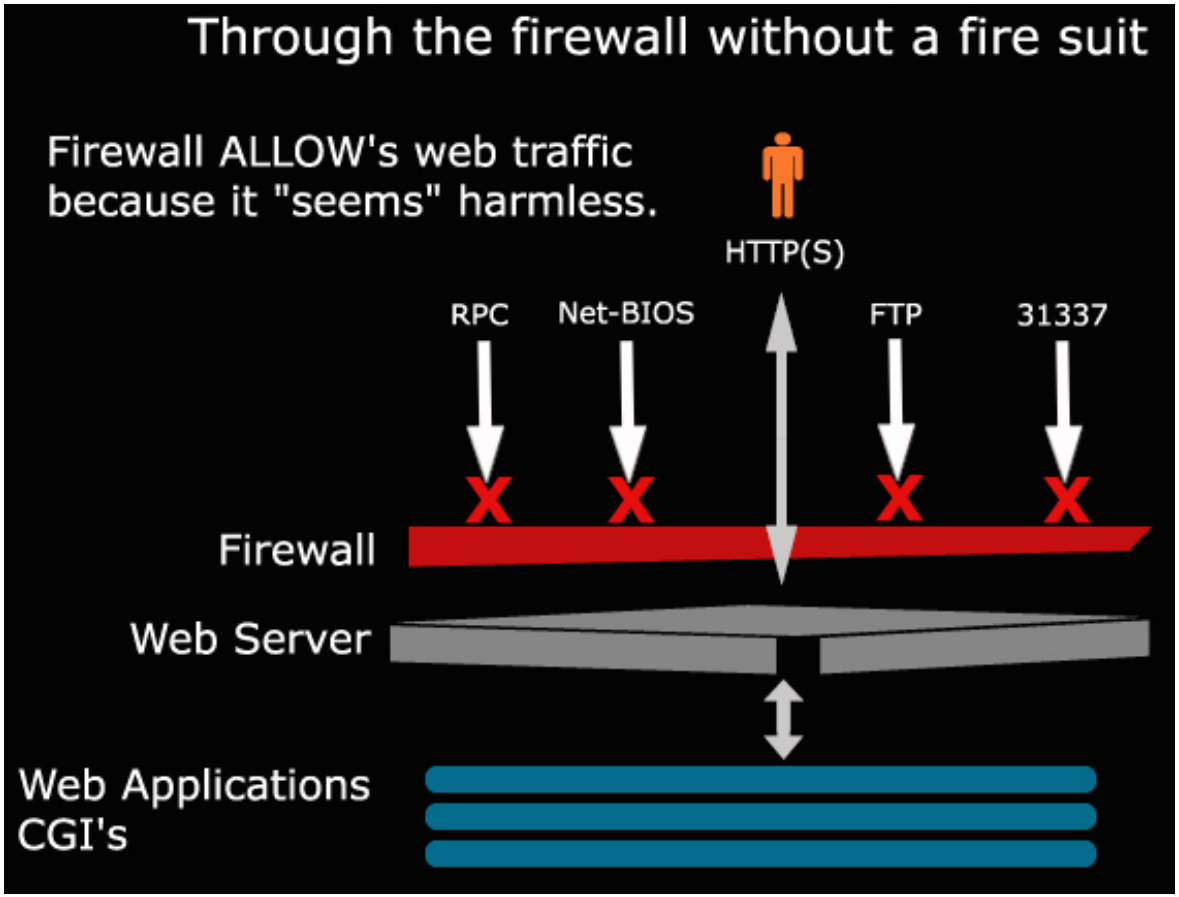
Réseaux

- **Firewalls – une erreur fréquente:**

But, I have a firewall . . .

L'utilisation d'un firewall ne garantit pas le blocage du code dangereux en provenance de l'extérieur.

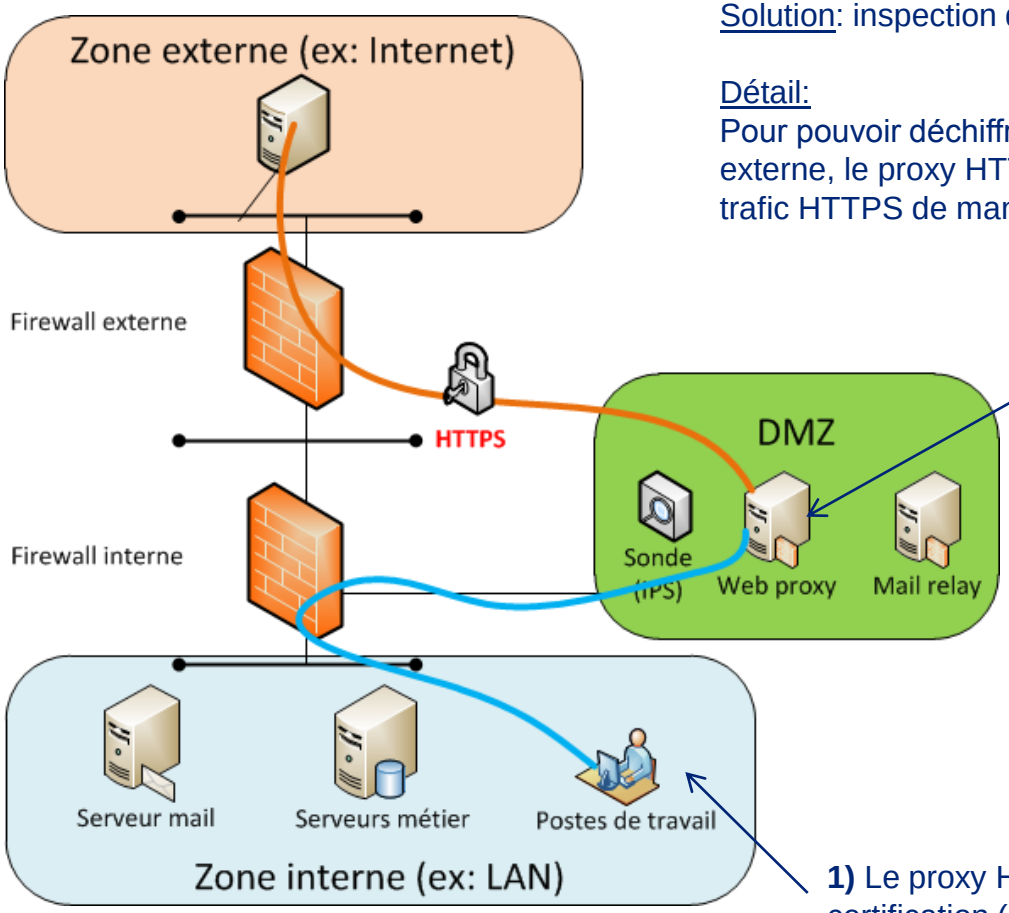
Par exemple, le firewall ne bloquera pas nécessairement le téléchargement d'un malware par un utilisateur interne s'il a lieu via une connexion chiffrée (ex: HTTPS)



Source: Jeremiah Grossman, BlackHat 2001

© 2019 Jean-Claude Héritier

- **Firewalls – solution: l'inspection du trafic SSL par un proxy HTTPS**



Solution: inspection du trafic SSL par un proxy web compatible.

Détail:
Pour pouvoir déchiffrer le trafic SSL entre l'utilisateur et le site web externe, le proxy HTTPS est configuré pour pouvoir déchiffrer le trafic HTTPS de manière transparente (invisible) pour le client:

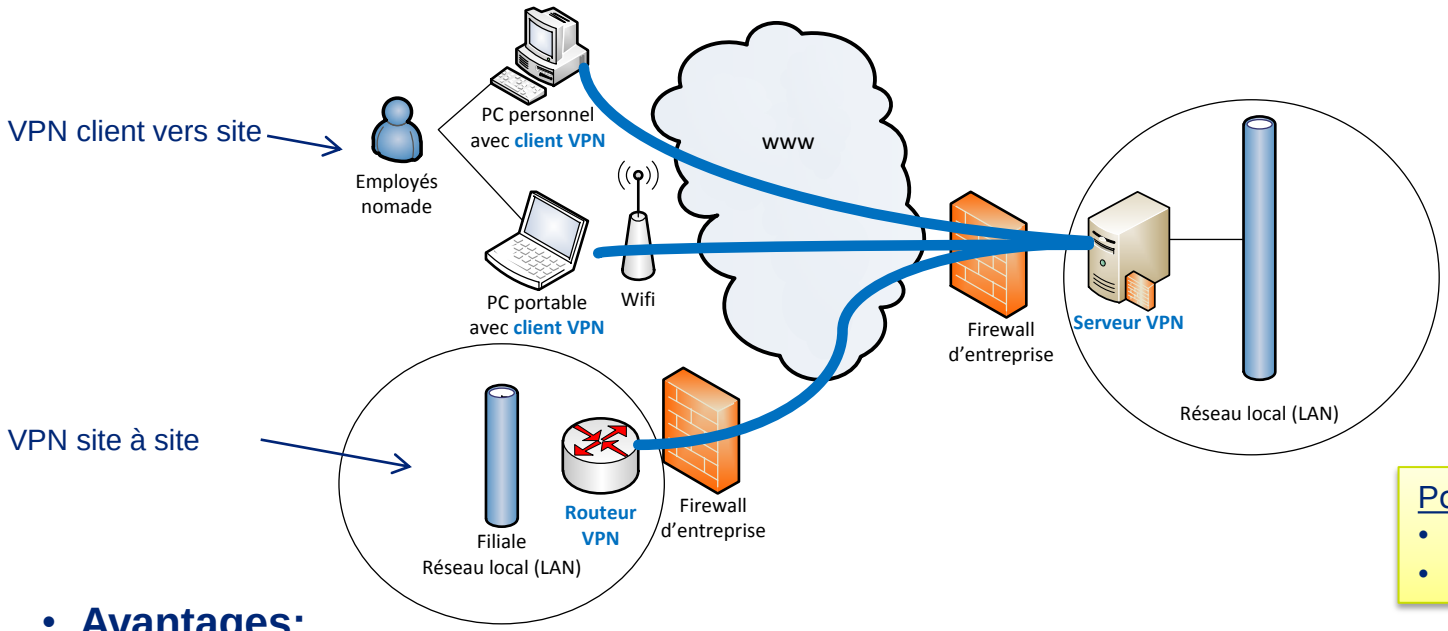
2) Le proxy HTTPS est ensuite en mesure
- d'intercepter les requêtes utilisateur et d'établir lui-même la session HTTPS avec le site web externe.
- A réception de réponse chiffrée du site externe le proxy déchiffre le trafic HTTPS avec la clé de session établie entre lui et le site web externe.
- Le trafic est alors inspecté, puis – si ne contenant pas de code malicieux - chiffré à nouveau avec un certificat (auto-signé) qui sera accepté par le poste client (bien que non-émis par le site externe).

1) Le proxy HTTPS doit être défini comme autorité de certification (CA) de confiance dans la liste des CA incorporées au navigateur web du PC client. Ainsi le proxy HTTPS peut générer des certificats que le client considérera comme émis par le site externe.

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Réseaux

- **Les réseaux privés virtuels (VPN - Virtual Private Network)**
  - **Principe: extension logique du réseau local (i.e. privé) au travers d'un réseau public (ex: Internet) via un protocole de tunnelisation** (ex: SSL, IPSEC):
    - Authentification mutuelle du client et du serveur VPN.
    - Chiffrement des paquets de données par le **client VPN.**
    - Transport des paquets chiffrés par Internet (réseau transporteur).
    - Réception et déchiffrement des paquets par le **serveur VPN.**



Points d'attention:
- Sécurité du poste client.
- Authentification suffisante?

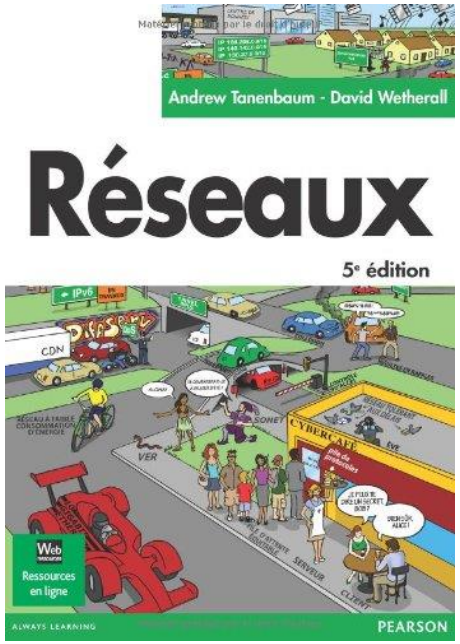
- **Avantages:**
  - **Coût** - largement inférieur à celui d'une ligne louée (NB: bande passante cependant non-garantie).
  - **Confidentialité – Intégrité – Authentification** (standard: mot de passe seul ⚠ Non-recommandé, option: authentification forte)

© 2019 Jean-Claude Héritier

Sécurité logique - Réseaux

- **Liens et références**

  – **Réseaux (édition 5) -** Andrew Tanenbaum & David J.Wetherall
    - **ISBN-13:** 978-2744075216



  – **Distribution Linux et outils d'analyse sécurité:**
    - **Kali Linux (ex. BackTrack) :** http://www.kali.org/

© 2019 Jean-Claude Héritier

Bases de données

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Bases de données

Exemples:

Dans la mesure du possible, définir une **fonction DBA indépendante** des administrateurs système et des administrateurs applicatifs.

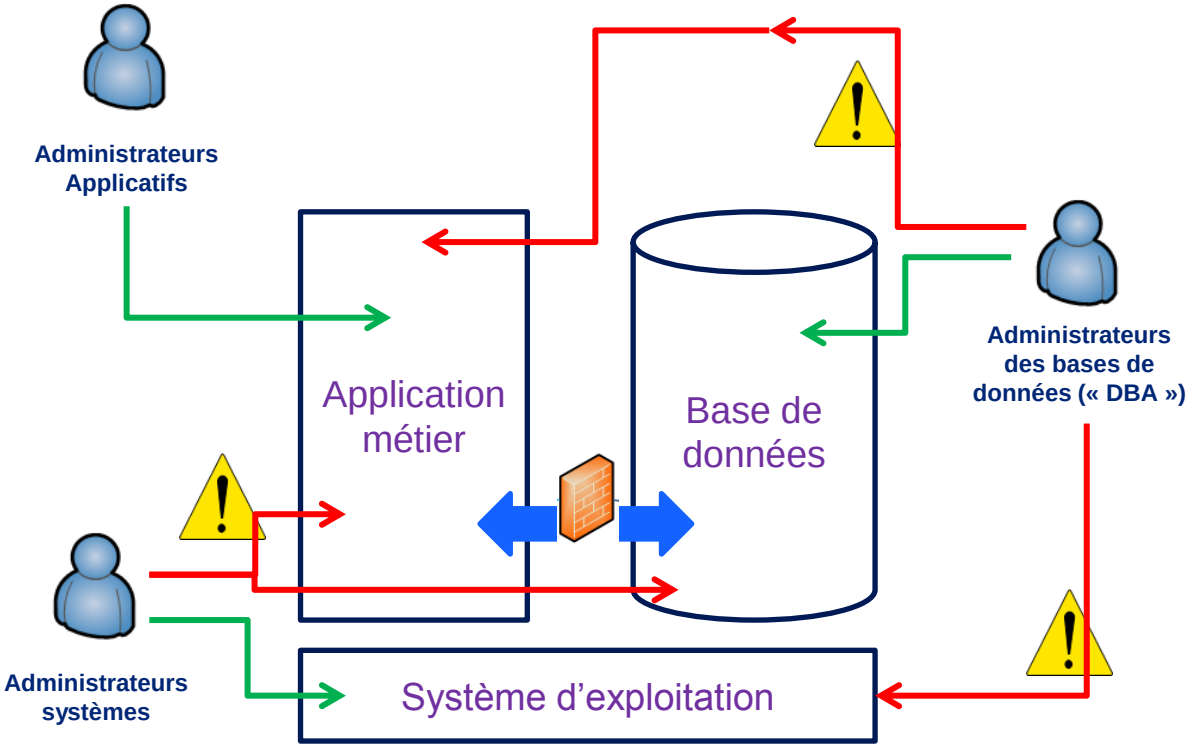
Considérer la possibilité de **chiffrer les champs sensibles** de la base de données.

Contrôles d'accès contre connexions directes ODBC (ex: firewalls)

Selon la sensibilité des données, considérer des contrôles préventifs et détectifs sur les accès aux bases de données.

Exemples:
- solutions natives (ex: Oracle)
- solutions dédiées (ex: Imperva)
- contrôles opérationnels,

Etc.



Référence: http://www.sans.edu/research/security-laboratory/article/it-separation-duties

© 2019 Jean-Claude Héritier

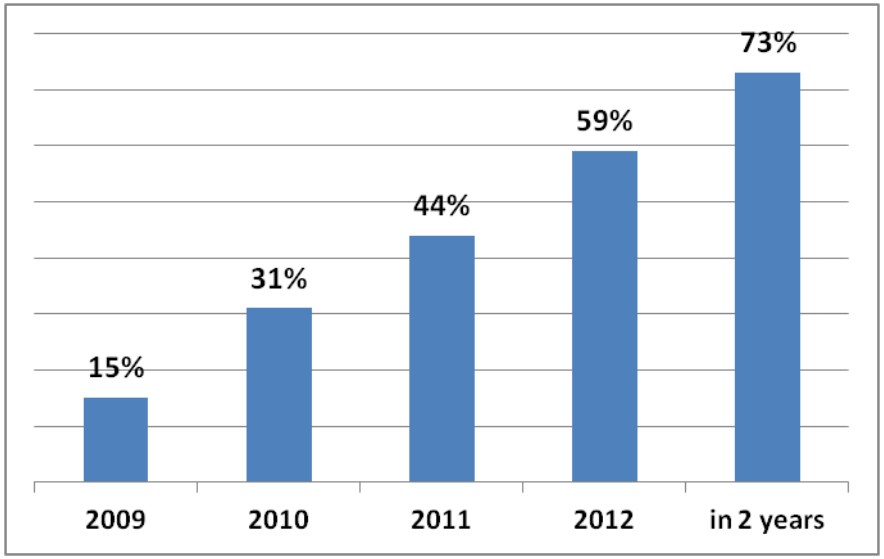
Plateformes virtualisées

© 2019 Jean-Claude Héritier

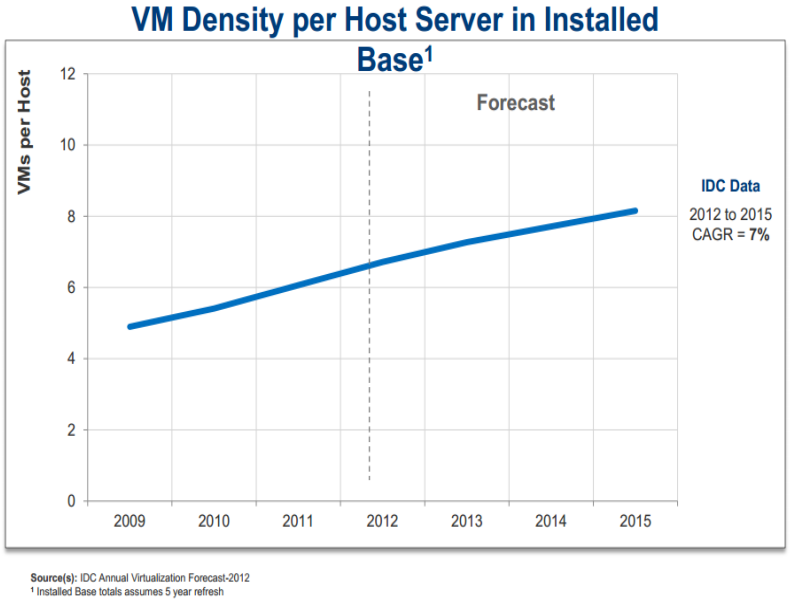
Mesures techniques pour sécuriser le S.I.
Plateformes virtualisées

- **Statistiques**

Pourcentage de systèmes serveur x86 (ex: Windows, Linux) exécutés dans des machines virtuelles:



Source: VMware Customer Survey – Janv. 2010, Juin 2011, Mars 2012



Source: IDC Annual virtualisation forecast 2012

- **Principe:**

- dissocie le système d'exploitation et les applications du matériel physique: plusieurs systèmes d'exploitation peuvent être exécutés sur un seul serveur physique en tant que machines virtuelles.

- **Bénéfices:**

- 80 % d'utilisation en plus des ressources des serveurs.
- Jusqu'à 50 % d'économies en coûts d'investissement et d'exploitation.

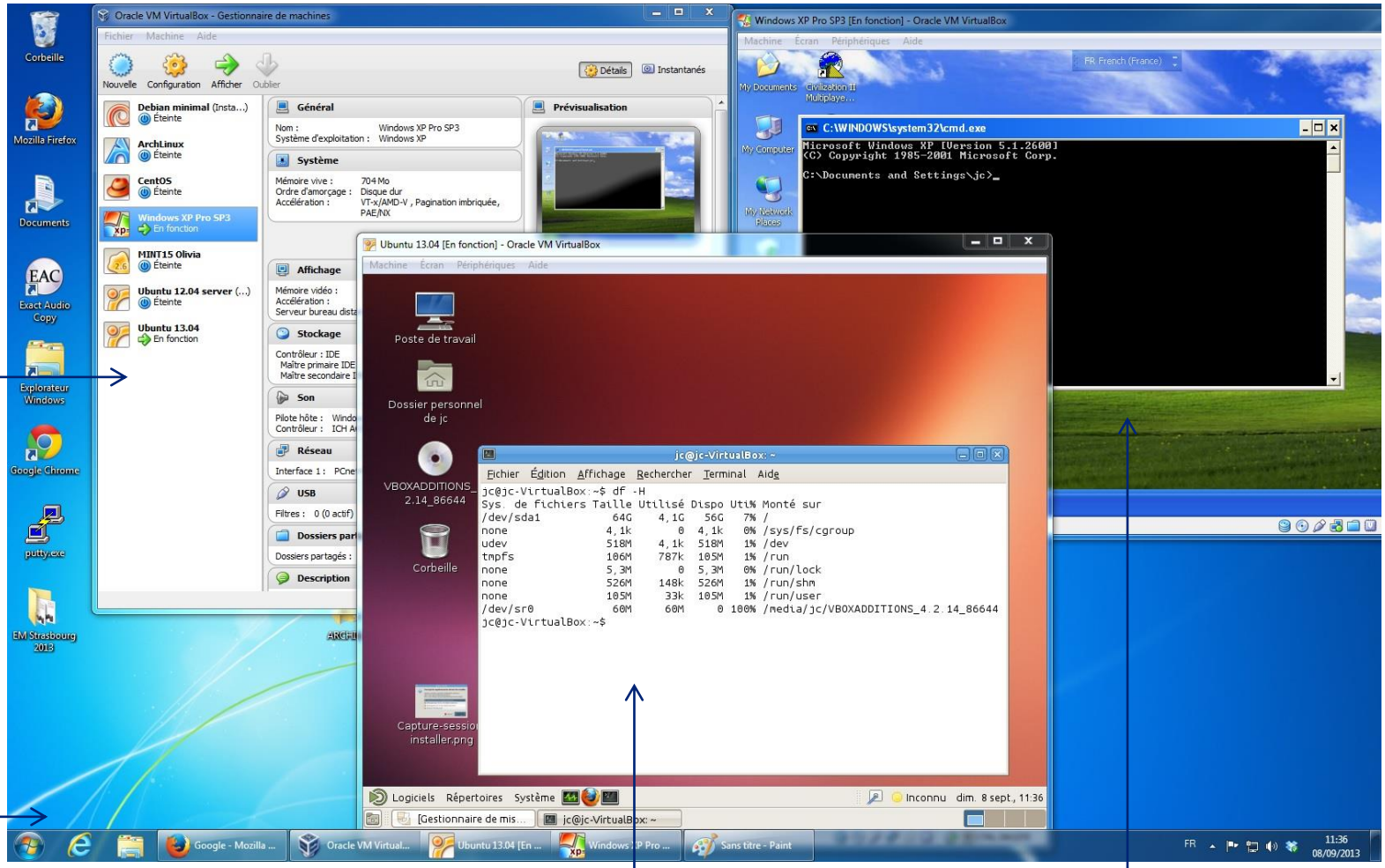
Source: VMware : http://www.vmware.com/fr/virtualization/

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.

Plateformes virtualisées

- **Exemple d'exécution de machines virtuelles**



Machine hôte:
Logiciel de virtualisation (Oracle VM VirtualBox)

Machine hôte:
Windows Seven

Machine virtuelle 1:
Ubuntu 13.04

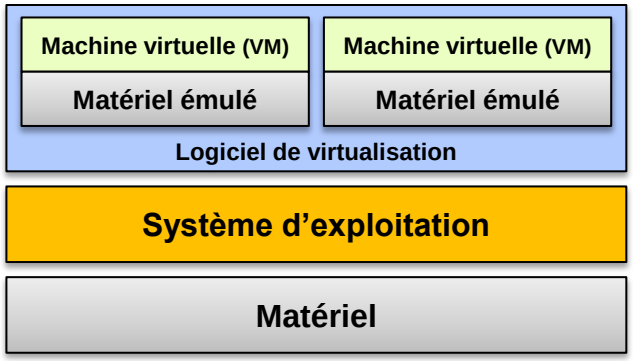
Machine virtuelle 2:
Windows XP

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.
Plateformes virtualisées

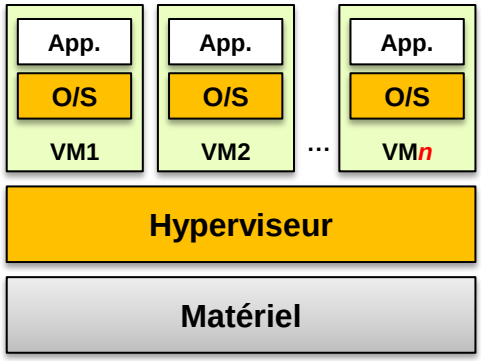
- **Les différents types de virtualisation**

Virtualisation de serveurs



Application de virtualisation: une application installée sur le serveur hôte va virtualiser les systèmes d'exploitation invités. Les systèmes invités sont complètement indépendants du système hôte.

Exemples: VMware server, VMware Workstation, VMPlayer, VirtualBox, VirtualPC, QEMU, etc.



Hyperviseur: une légère couche logicielle est insérée entre le matériel et le système d'exploitation invité. Cela permet au système invité de communiquer directement avec le matériel.

Exemples: VMware ESX/ESXi, Citrix Xen Server, Microsoft Hyper-V.

Avantages

- Permet d'utiliser les ressources matérielles (parc informatique) de manière optimale:
  - Economies: électricité, locaux, compatibilité du matériel, etc.)
  - Répartition des machines virtuelles sur les machines physiques suivant la charge (y compris sans interruption de service avec des outils comme VMware vMotion).
- Permet de facilement redimensionner les serveurs (ajout de puissance, mémoire, matériel, etc.)
- Simplifie les opérations d'installation / déploiement / maintenance.
- Possibilités de prendre des instantanés (« snapshots ») et de clôner les machines virtuelles.
- Améliore la sécurité des données: pas de données sauvegardées en local sur le poste de travail utilisateur.

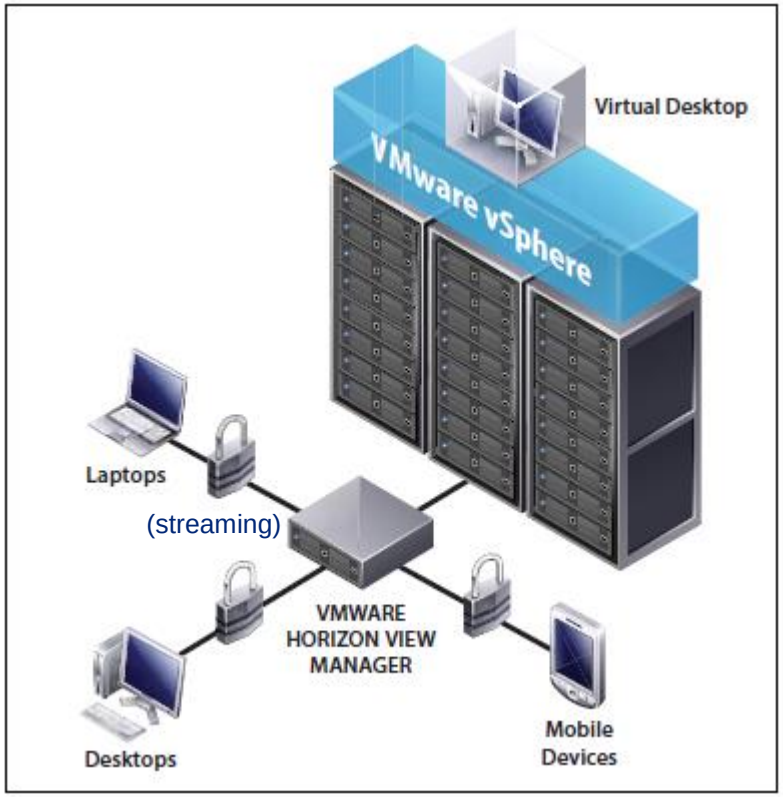
© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.

Plateformes virtualisées

- **Les différents types de virtualisation**

Virtualisation de postes de travail



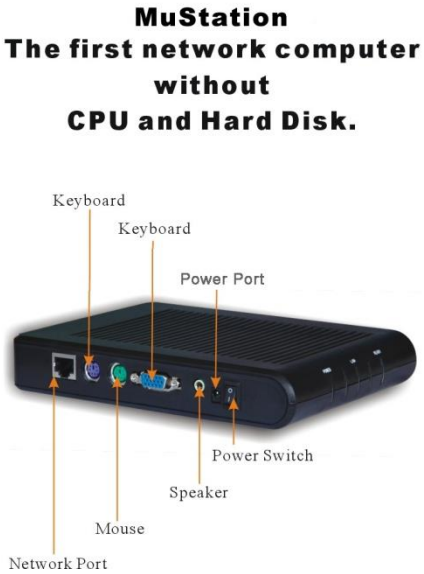
Avantages

- Simplifie le déploiement des postes de travail utilisateurs et des applications.
- Possibilité de **clients légers**.
- Améliore les capacités de reprise en cas de sinistre (**DRP**): tous les composants et applications sont disponibles lors de la connexion depuis un autre périphérique.
- Améliore la sécurité des données: pas de données sauvegardées en local sur le poste de travail utilisateur.

Exemples de solutions:

- Citrix XenDesktop
- Microsoft Windows Thin PC
- VMware Horizon View (VMware VDI)

Exemple de client léger:

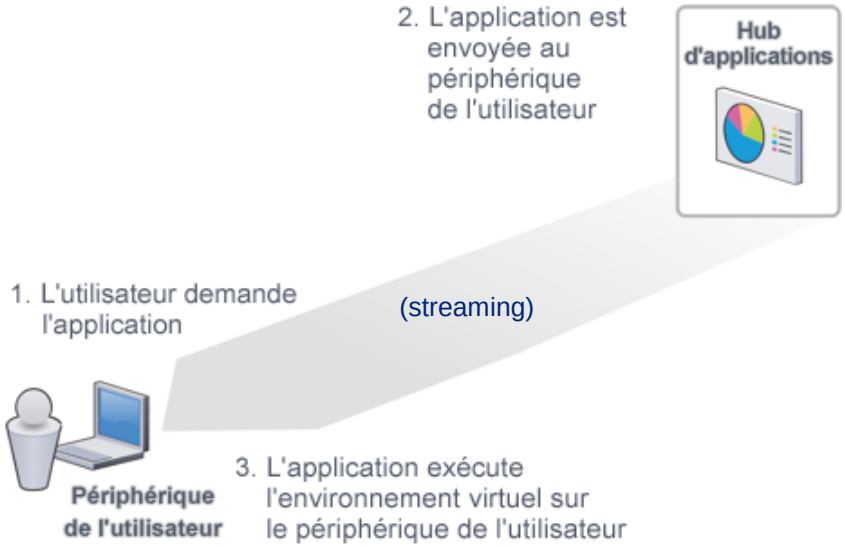


© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.

Plateformes virtualisées

- **Les différents types de virtualisation** **Virtualisation d'applications**



• Requiert un système d'exploitation compatible et un logiciel client.
• L'application est exécutée dans un environnement isolé sur le périphérique de l'utilisateur.

Exemples de solutions:
- Citrix XenApp
- Microsoft Application Virtualization
- VMware ThinApp

Avantages
- Accessibilité des applications qui sont disponibles sur n'importe quel appareil autorisé, sans nécessiter d'installation.
- Accélère le déploiement des applications (simplifie les tests de compatibilité).
- Simplifie la gestion des systèmes d'exploitation et postes de travail (réduit les incompatibilités et la dépendance envers le matériel et les systèmes d'exploitation).
- Réduit les besoins en ressources par rapport à une machine virtuelle (seule l'application est virtualisée).
- Améliore la sécurité en dissociant applications et système d'exploitation (une application est moins affectée par un système vulnérable, et une application vulnérable.
- Certaines solutions rendent possibles des accès hors-ligne à des applications.

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.

Plateformes virtualisées

- **Sécurité des plateformes virtualisées**

1. Vulnérabilités des machines virtuelles

- Les machines virtuelles sont fondamentalement soumises aux mêmes risques de sécurité logique que des machines physiques (virus, vulnérabilités système, etc.)

→

- Protection antivirus (VMs)
- Correctifs de sécurité (VMs).
- Segmentation réseau des VMs

Etc.

---

2. Vulnérabilités de l'hyperviseur

- Une défaillance de l'hyperviseur - ou du système hôte - peut affecter toutes les machines virtuelles.

→

- Protection antivirus (host)
- Correctifs de sécurité (host)
- Mises à jour sécurité sur l'hyperviseur

Etc.

---

3. Vulnérabilités de configuration

- Une défaillance de l'hyperviseur - ou du système hôte - peut affecter toutes les machines virtuelles.
- La facilité de cloner et déployer des machines introduit de nouvelles vulnérabilités.

→

- Revues de configuration et standards de paramétrage.
  (ex: référentiels DISA, SANS, etc.)
- Gestion des changements (hôte / hyperviseur et VMs)
- Surveillance / gestion des évènements de sécurité

Etc.

En résumé:

- **Des risques standards: l'environnement de contrôle doit être étendu aux plateformes virtualisées.**
- **Et des risques spécifiques liés à la Virtualisation qui doivent être intégrés dans l'environnement de contrôle.**

© 2019 Jean-Claude Héritier

Mesures techniques pour sécuriser le S.I.

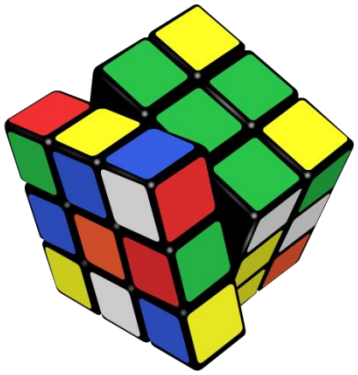
Liens et références

Microsoft – Technet – Guides techniques sur la sécurité
http://technet.microsoft.com/fr-fr/library/bb977553.aspx

ANSSI - guide d'hygiène informatique:
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

© 2019 Jean-Claude Héritier

V) Cas pratique : protection contre les fuites de données



© 2019 Jean-Claude Héritier

Cas pratique : protection contre les fuites de données

Points clés

- **Analyse des risques:** quelles données protéger?
- Quelles menaces?

Classification de l'information

Analyse des risques

Contrôles d'accès

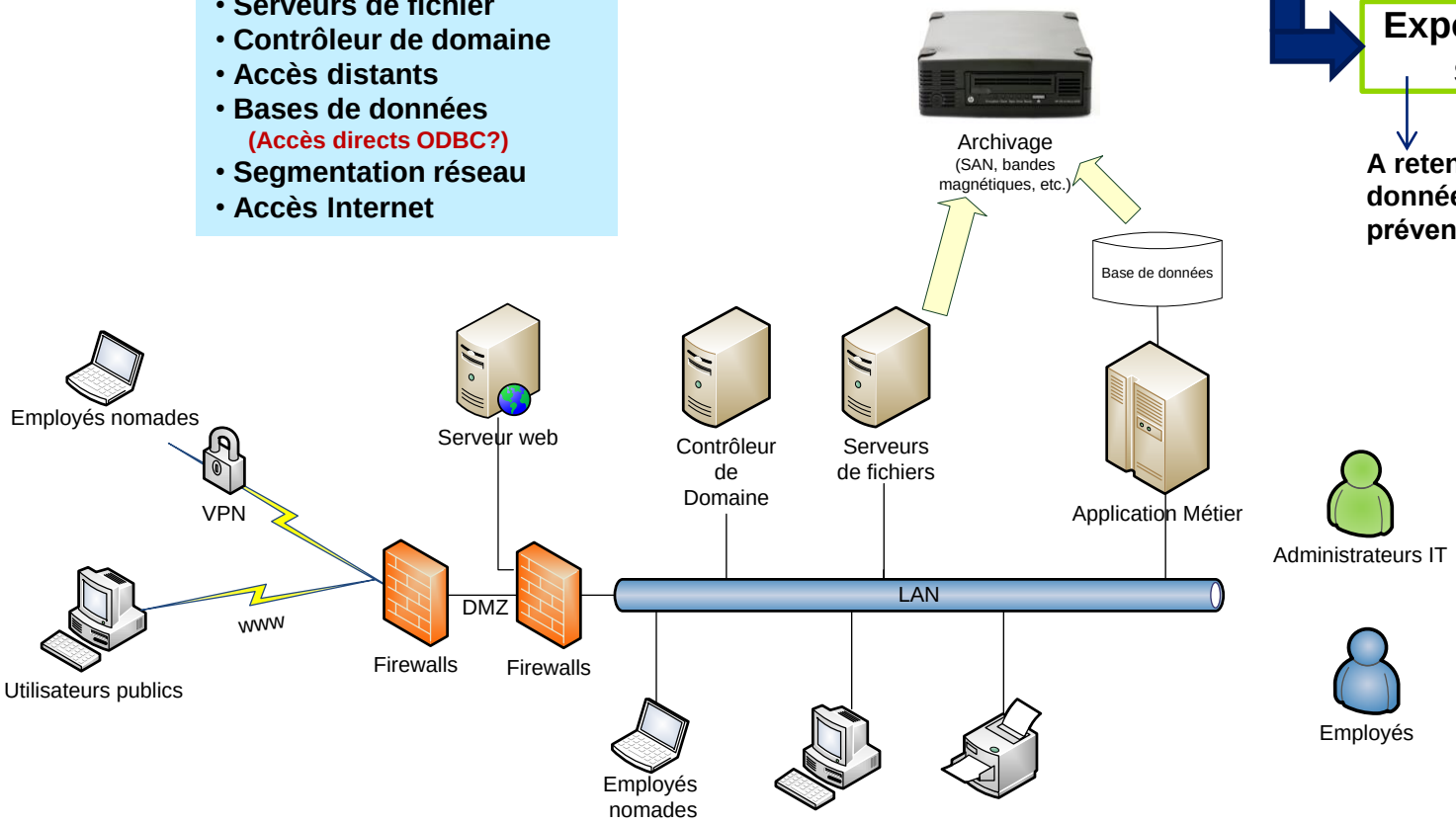
- **Applications**
- **Serveurs de fichier**
- **Contrôleur de domaine**
- **Accès distants**
- **Bases de données**
  (Accès directs ODBC?)
- **Segmentation réseau**
- **Accès Internet**

Extraction de données sensibles?

(export ''en masse''?)

Export de données sensibles?

A retenir: si accès aux données, il est très difficile de prévenir l'export.

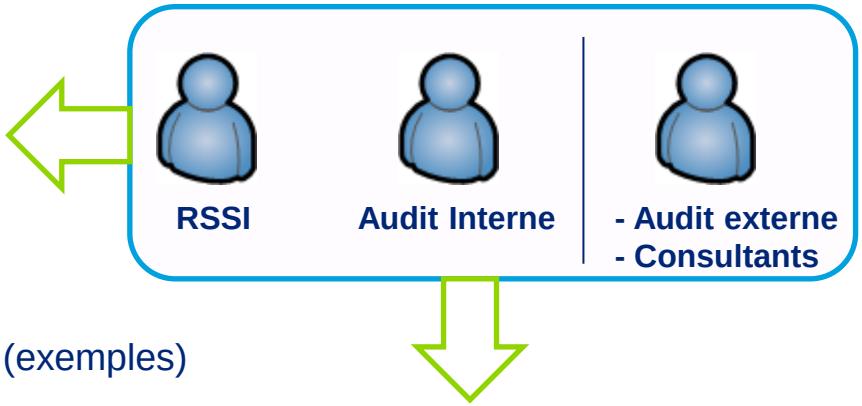


© 2019 Jean-Claude Héritier

Cas pratique : protection contre les fuites de données

Contrôles clés

- **Contrôles organisationnels**
  - **Classification de l'information**
  - **Politique de sécurité et procédures**
  - **Sensibilisation des employés**
  - **Re-certification périodique des accès**



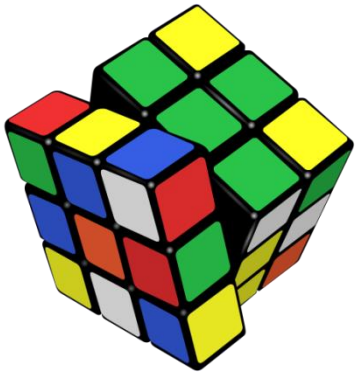
- **Mesures techniques: contrôles d'accès** (exemples)

Contrôleur de Domaine	Postes de travail	Applications	Réseau	Bases de données	Supports de sauvegarde
• Droits d'accès sur fichiers / répertoires sensibles: - ségrégation par département - re-certification des accès aux répertoires partagés. • Présence de fichiers sensibles sur les partages réseau existant?	• Contrôle des médias amovibles (clés USB, graveurs, etc.) • Chiffrement des disques durs. • Applications autorisées (contrôles des applications portables?)	• Droits d'accès aux données (lecture) • Contrôle des fonctions d'export « en masse » (ex: logs, mécanismes d'alerte, 4-yeux, etc.)	• Accès Internet: - upload de fichiers - webmail - partage de fichiers (Dropbox, etc.) • Possibilités de contourner les contrôles d'accès réseau? (tunneling, désactiver proxy du navigateur web, connexion wifi, etc.) • Risques d'écoute réseau? (réponse: utilisation de TLS et de certificats)	• Contrôles contre les accès directs (ex: ODBC). • Contrôles des outils de requête / rapports personnalisés (ex: gestion des changements, visa du RSSI pour exécuter des requêtes sensibles, etc.)	• Chiffrement des supports? • Droits de restauration? • Destruction sécurisée en fin de vie? • Sécurité physique des medias?
• **Contrôle des profils avec privilèges** (Administrateurs du Domaine, Administrateurs de bases de données, gestionnaires des sauvegardes, etc.). **Mise en œuvre de contrôles préventifs ou détectifs** (techniques / organisationnels), en fonction des risques.					

A évaluer au cas par cas.

© 2019 Jean-Claude Héritier

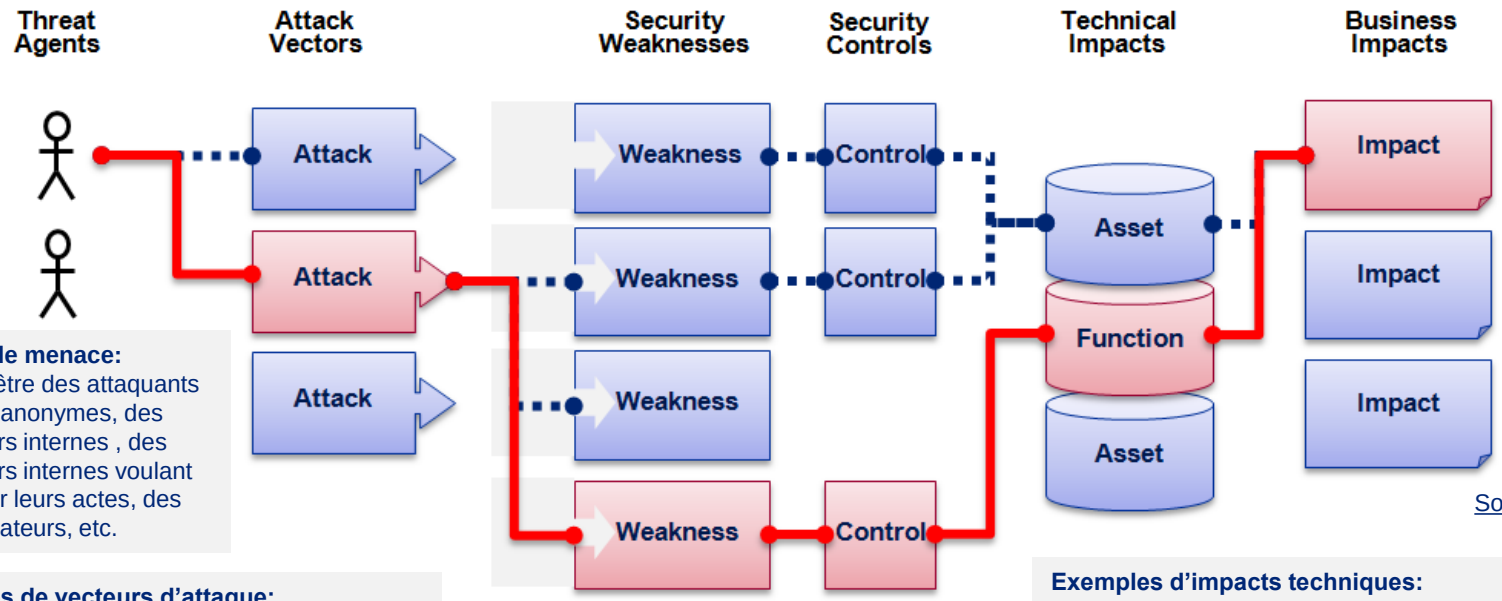
VI) Sécurité des applications Web



© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Divers chemins d'attaque:**



Source: OWASP

Agents de menace:
peuvent être des attaquants externes anonymes, des utilisateurs internes , des utilisateurs internes voulant camoufler leurs actes, des administrateurs, etc.

Exemples de vecteurs d'attaque:
- Scripts qui exploitent la syntaxe d'un interpréteur cible (injection)
- Attaquant accédant à des comptes par défaut,
- Modification d'URL,
- Vulnérabilités non corrigées,
- Fichiers et répertoires non protégés,
- etc.

Exemple de vulnérabilité:
- envoi de données non-fiables par une application à un interpréteur (de type injection SQL)

Exemples d'impacts techniques:
- perte ou une corruption de données,
- perte de droits, ou un refus d'accès.
- détournement de sessions
- défigurer des sites web
- rediriger l'utilisateur vers un site malveillant
- parfois prise de contrôle totale du serveur.
- etc.

- **La nécessité de déterminer le risque global**

Risque global = **probabilité** relative à chaque agent de menace, vecteur d'attaque, et vulnérabilité **X** Estimation d'**impact** technique et financier pour l'entreprise

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Le top 10 des risques de sécurité:**

A1 – Injection	**A2 – Violation de Gestion d'Authentification et de Session**	**A3 – Cross-Site Scripting (XSS)**	**A4 – Références directes non sécurisées à un objet**
A5 – Mauvaise configuration Sécurité	**A6 – Exposition de données sensibles**	**A7 – Manque de contrôle d'accès au niveau fonctionnel**	**A8 - Falsification de requête intersite (CSRF)**
	A9 - Utilisation de composants avec des vulnérabilités connues	**A10 - Redirections et renvois non validés**	

Référence: OWASP Top 10

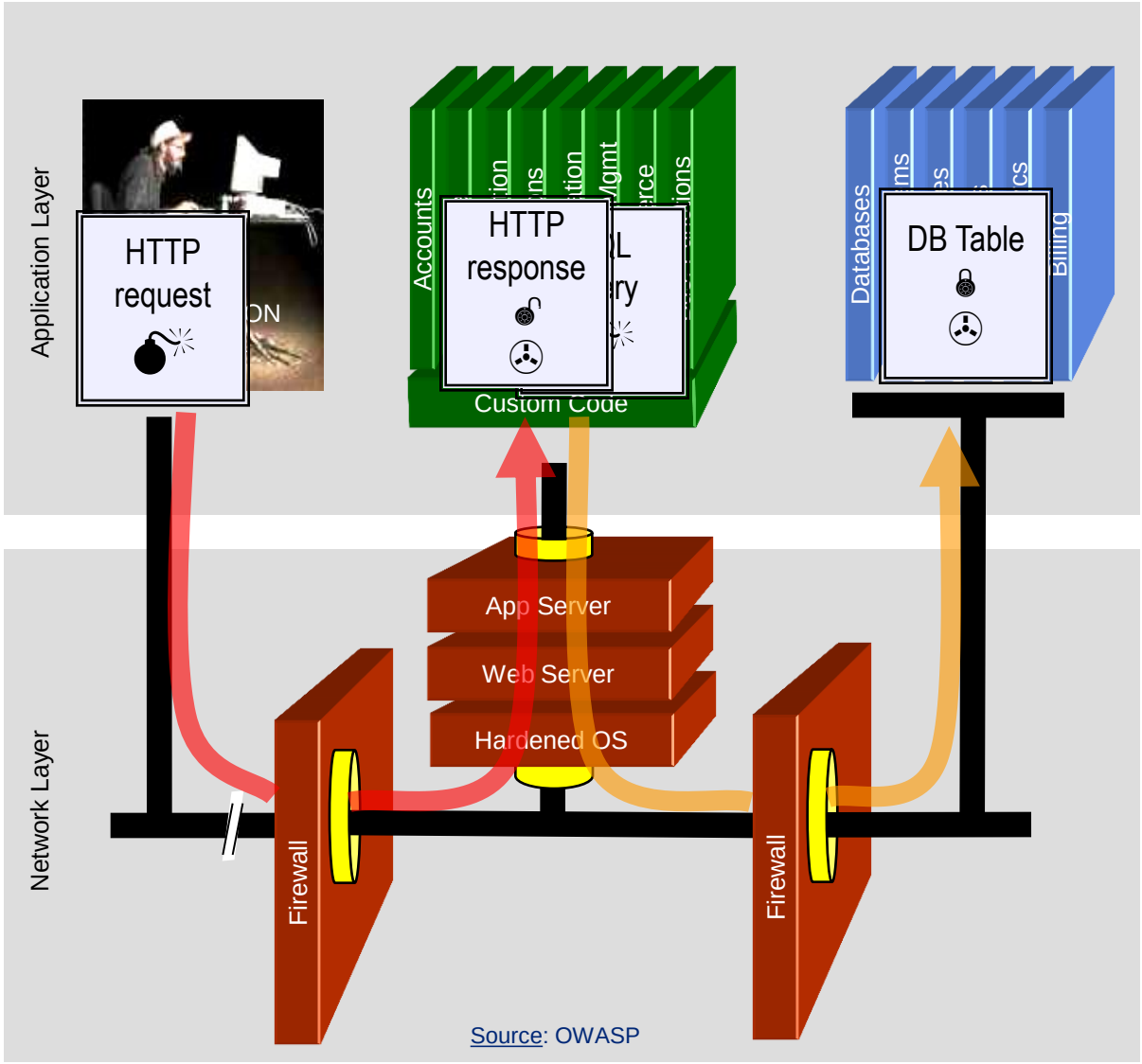
Quelques exemples

© 2019 Jean-Claude Héritier

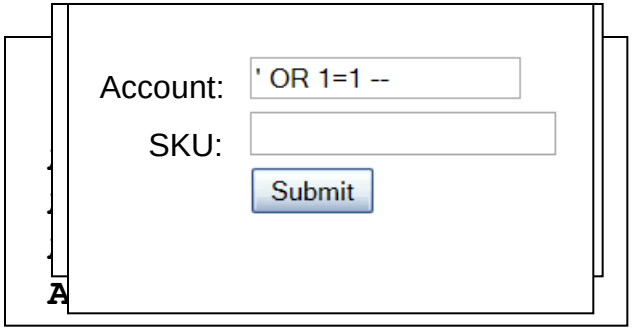
Sécurité des applications Web

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A1 - Injection SQL**



Source: OWASP



1. L'application présente un formulaire pour l'entrée de données

2. L'attaquant envoie une attaque via le formulaire

3. L'application fait suivre l'attaque vers la base de données sous forme de requête SQL.

4. La base de données exécute la requête contenant l'attaque et renvoie les résultats sous forme chiffrée à l'application.

5. L'application déchiffre les données et retourne le résultat de la requête à l'utilisateur.

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Le top 10 des risques de sécurité:**

A1 – Injection

A2 – Violation de Gestion d'Authentification et de Session

A3 – Cross-Site Scripting (XSS)

A4 – Références directes non sécurisées à un objet

A5 – Mauvaise configuration Sécurité

A6 – Exposition de données sensibles

A7 – Manque de contrôle d'accès au niveau fonctionnel

A8 - Falsification de requête intersite (CSRF)

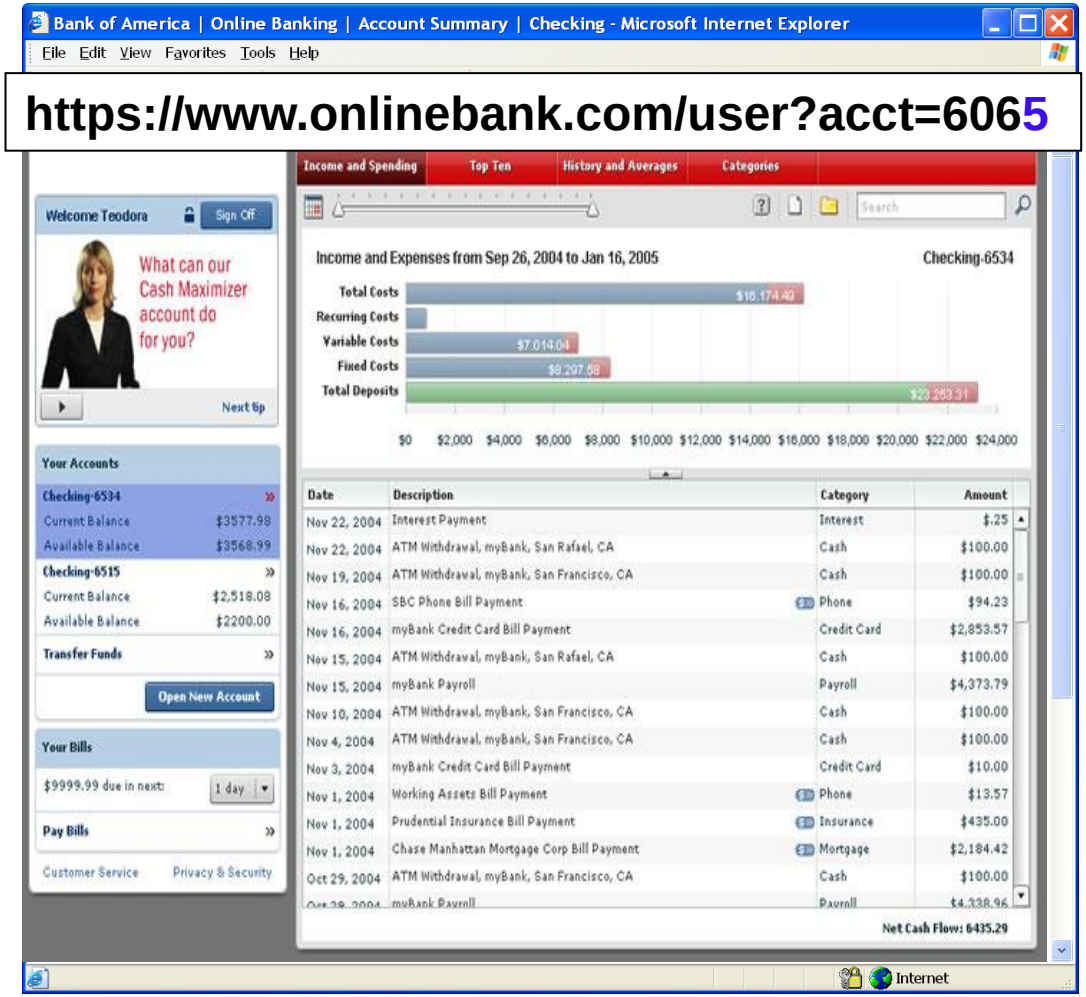
A9 - Utilisation de composants avec des vulnérabilités connues

A10 - Redirections et renvois non validés

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A4 - Références directes non sécurisées à un objet**



Source: OWASP

1. L'attaquant remarque que le paramètre de son compte est 6065
   ?acct=6065

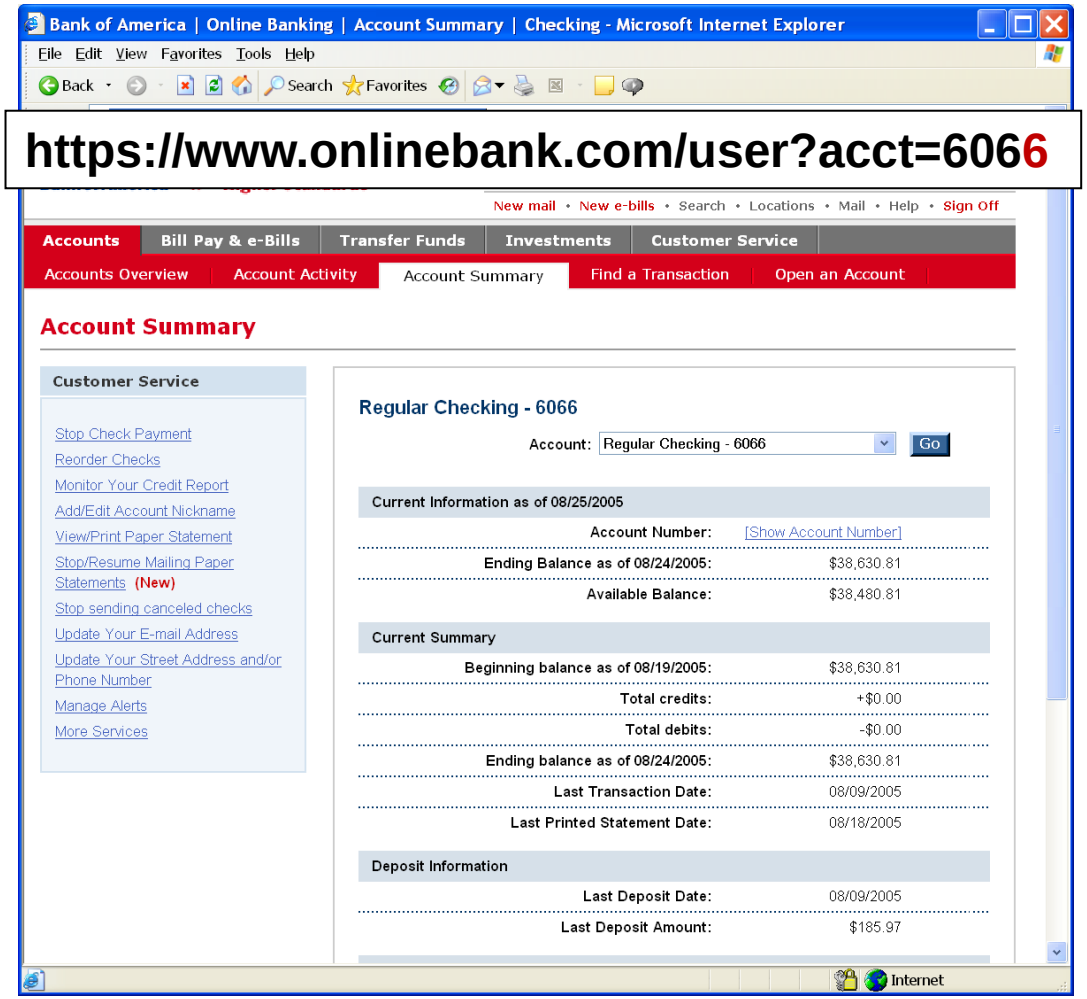
2. Il modifie la valeur du paramètre à une valeur proche (ex: 6066)
   ?acct=6066

3. L'attaquant peut voir les informations du compte de la victime.

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A4 - Références directes non sécurisées à un objet**



Source: OWASP

1. L'attaquant remarque que le paramètre de son compte est 6065
?acct=6065

2. Il modifie la valeur du paramètre à une valeur proche (ex: 6066)
?acct=6066

3. L'attaquant peut voir les informations du compte de la victime.

Contre-mesures:
-Remplacer les références directes par des références temporaires (RandomAccessReferenceMap)

http://app?file=Report123.xls
http://app?file=1

http://app?id=9182374
http://app?id=7d3J93

Report123.xls

Acct:9182374

- Valider les références directes (format, droits d'accès, etc.)

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Le top 10 des risques de sécurité:**

A1 – Injection

A2 – Violation de Gestion d'Authentification et de Session

A3 – Cross-Site Scripting (XSS)

A4 – Références directes non sécurisées à un objet

A5 – Mauvaise configuration Sécurité

A6 – Exposition de données sensibles

A7 – Manque de contrôle d'accès au niveau fonctionnel

A8 - Falsification de requête intersite (CSRF)

A9 - Utilisation de composants avec des vulnérabilités connues

A10 - Redirections et renvois non validés

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A5 – Mauvaise configuration Sécurité**

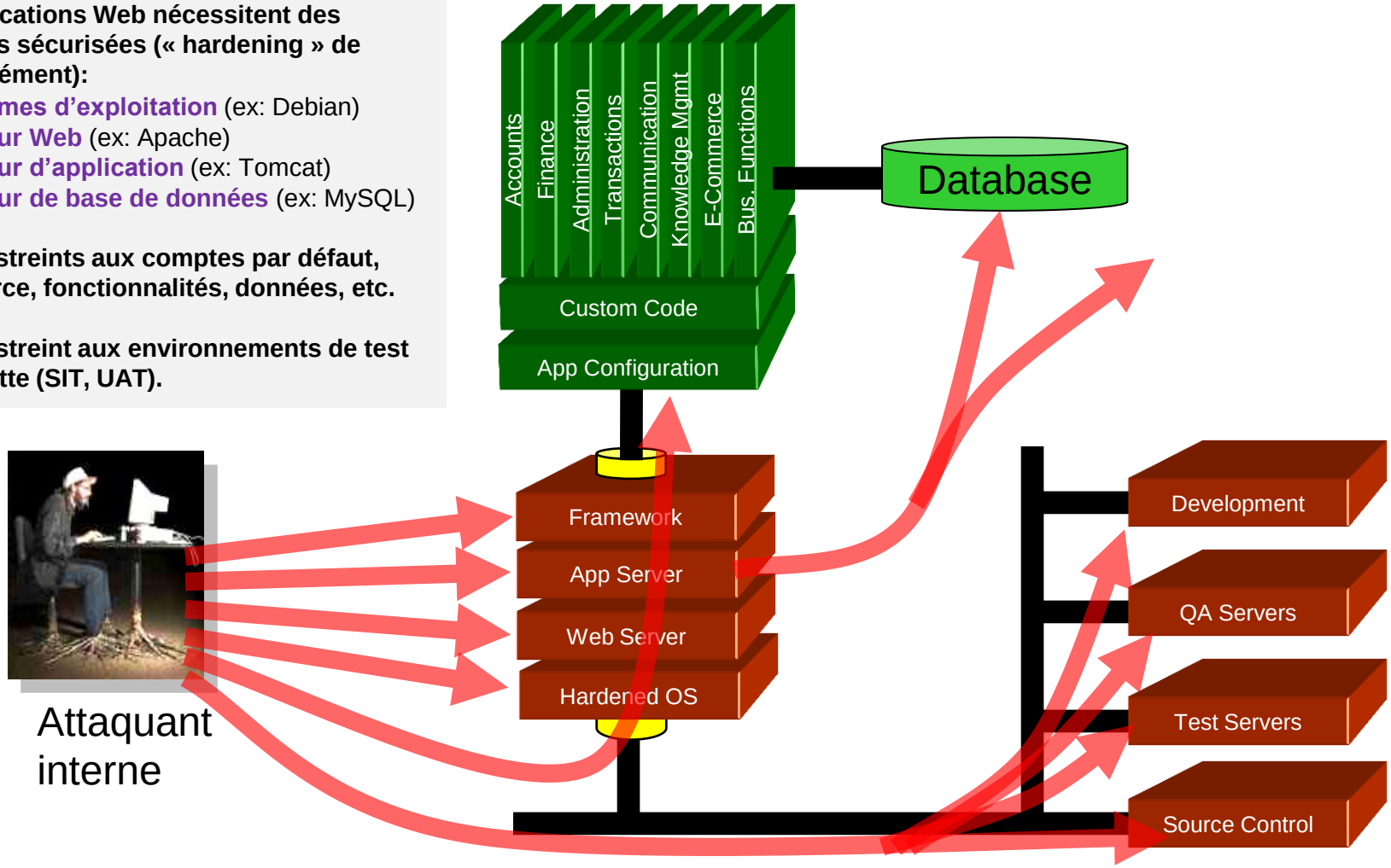
Contre-mesures:

-Les applications Web nécessitent des fondations sécurisées (« hardening » de chaque élément):

- **Systèmes d'exploitation** (ex: Debian)
- **Serveur Web** (ex: Apache)
- **Serveur d'application** (ex: Tomcat)
- **Serveur de base de données** (ex: MySQL)

-Accès restreints aux comptes par défaut, code source, fonctionnalités, données, etc.

-Accès restreint aux environnements de test et de recette (SIT, UAT).



Source: OWASP

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Le top 10 des risques de sécurité:**

A1 – Injection

A2 – Violation de Gestion d'Authentification et de Session

A3 – Cross-Site Scripting (XSS)

A4 – Références directes non sécurisées à un objet

A5 – Mauvaise configuration Sécurité

A6 – Exposition de données sensibles

A7 – Manque de contrôle d'accès au niveau fonctionnel

A8 - Falsification de requête intersite (CSRF)

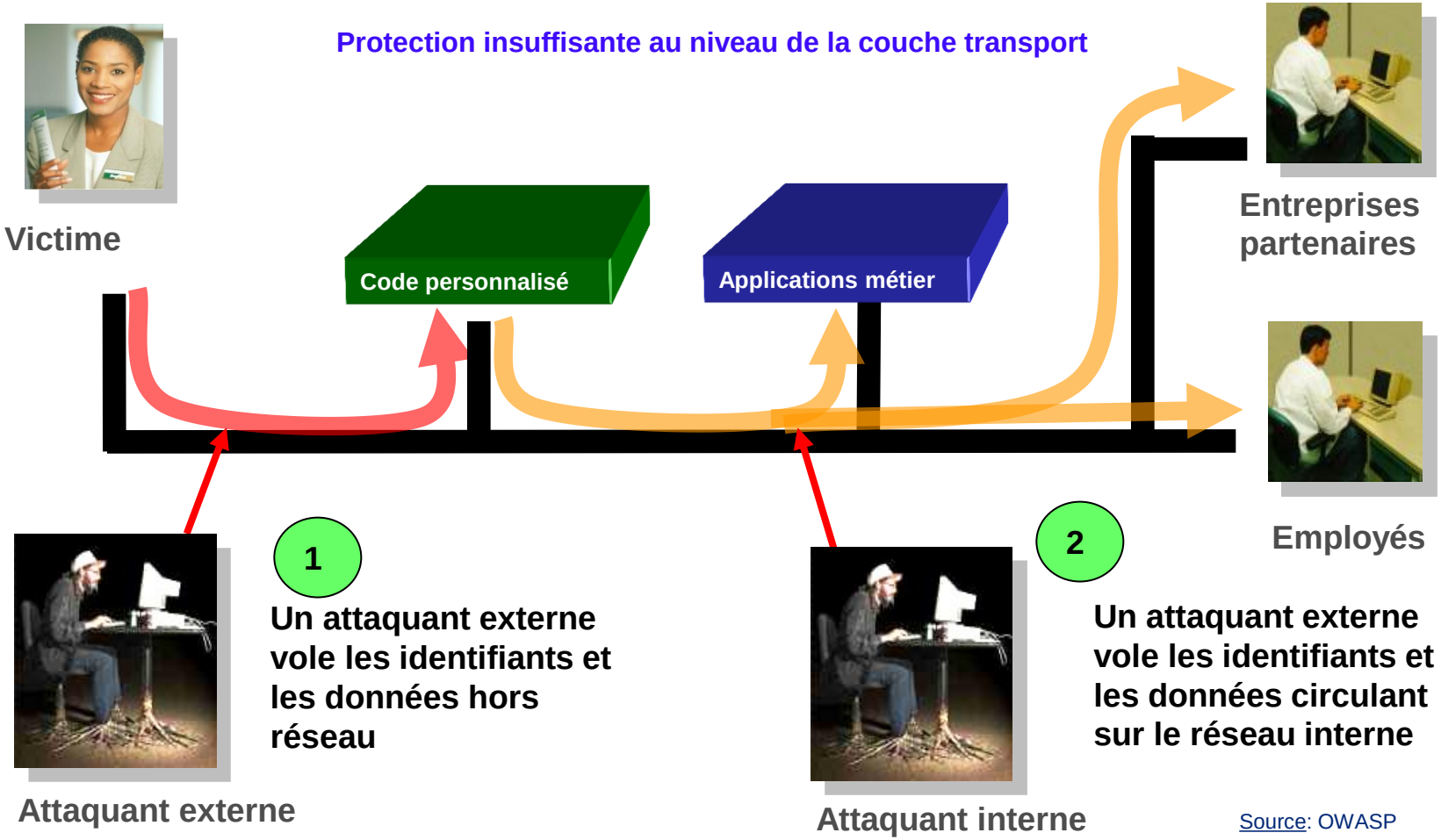
A9 - Utilisation de composants avec des vulnérabilités connues

A10 - Redirections et renvois non validés

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A6 - Exposition de données sensibles**



Source: OWASP

Contre-mesures:
-Chiffrement des données (si données sensibles) en utilisant les solutions possibles de manière appropriée (algorithmes standard, gestion des clés, validation des certificats, etc.)

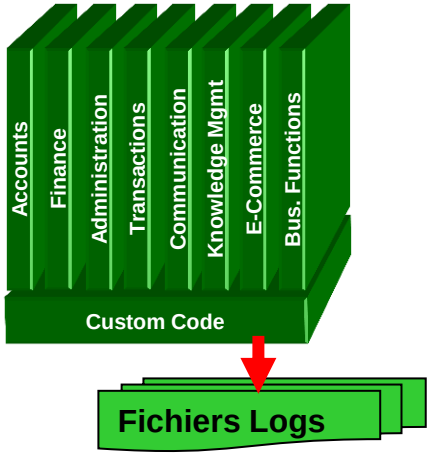
© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A6 - Exposition de données sensibles**

Protection insuffisante des données sensibles statiques

1 La victime saisit son numéro de carte de crédit dans un formulaire



2 Le gestionnaire d'erreur enregistre les détails du numéro de carte de crédit (par exemple si le serveur e-commerce du vendeur n'est pas disponible)

3 Les logs sont accessibles à tous les membres du service informatique pour l'analyse des erreurs (debugging)

4 Un attaquant interne exploite les logs pour voler 4 millions de numéros de carte de crédit.

Source: OWASP

Contre-mesures:
-Identifier les données sensibles et leur lieu de stockage, appliquer correctement des mécanismes de chiffrement appropriés, en fonction des menaces.

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Le top 10 des risques de sécurité:**

A1 – Injection

A2 – Violation de Gestion d'Authentification et de Session

A3 – Cross-Site Scripting (XSS)

A4 – Références directes non sécurisées à un objet

A5 – Mauvaise configuration Sécurité

A6 – Exposition de données sensibles

A7 – Manque de contrôle d'accès au niveau fonctionnel

A8 - Falsification de requête intersite (CSRF)

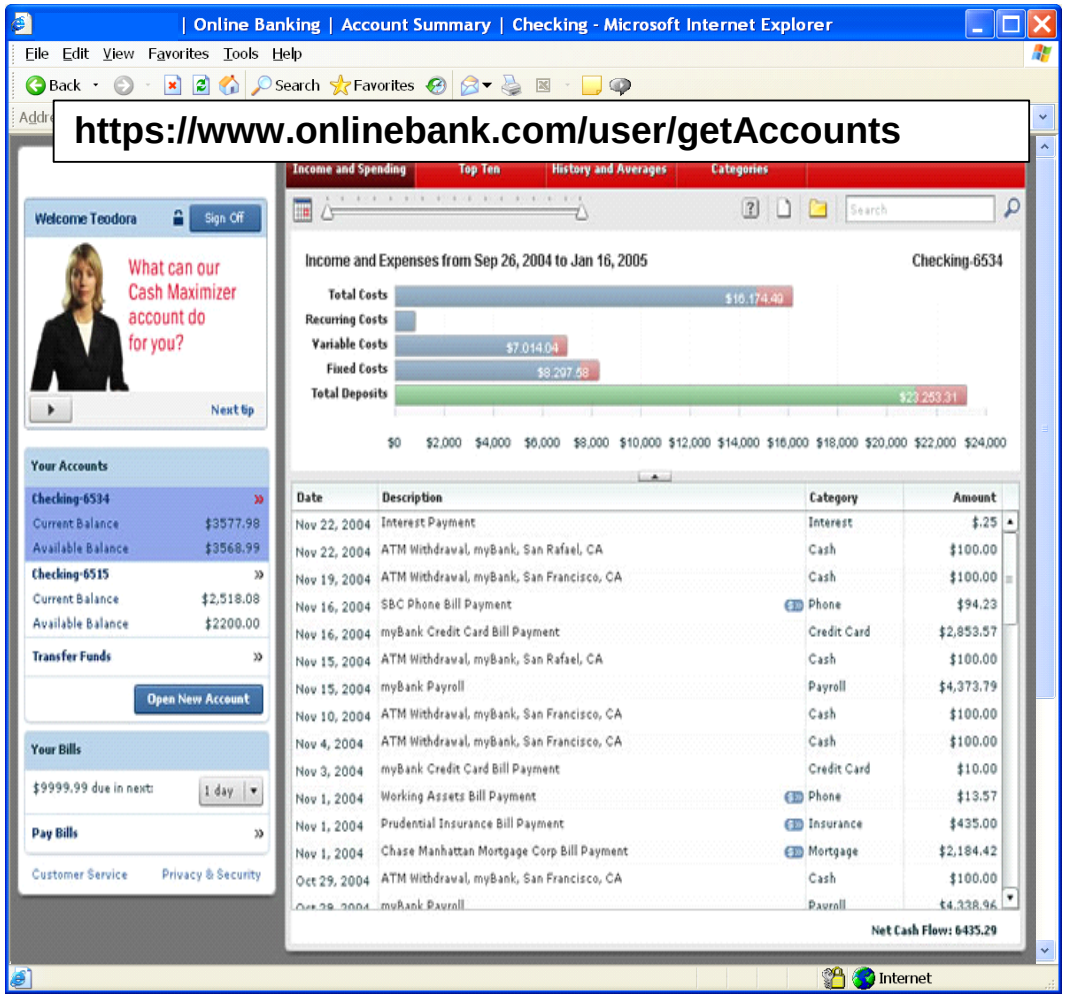
A9 - Utilisation de composants avec des vulnérabilités connues

A10 - Redirections et renvois non validés

© 2019 Jean-Claude Héritier

Quels sont les Risques de Sécurité des Applications Web?

- **Exemple: A7 - Manque de contrôle d'accès au niveau fonctionnel**



1. L'attaquant remarque que l'URL indique son rôle
/user/getAccounts

2. Il modifie la valeur du paramètre à un autre rôle (ex: 606)
/admin/getAccounts, ou
/manager/getAccounts

3. L'attaquant peut voir plus d'informations que celles de son propre compte.

Contre-mesures:
-**Restreindre les accès aux utilisateurs autorisés en fonction de leurs rôles ou permissions.**
- **Interdire toute requête vers des pages non-autorisées** (fichiers de configuration, fichier de logs, fichiers source, etc.)
-**Valider l'architecture**
-**Valider la mise en place** (ex: désactiver au niveau du serveur web l'accès à certains types de fichiers non-autorisés).

Source: OWASP

© 2019 Jean-Claude Héritier

Sécurité des applications web

- **Liens et références**

OWASP *- communauté travaillant sur la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous.*

– **OWASP Top 10 / Testing guide / code review guide**

- https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf

  Les 10 failles de sécurité Web les plus courantes, régulièrement MAJ.
  (détaille les techniques de base pour se protéger contre les faiblesses les plus importantes inhérentes à la sécurité des applications web).

- https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
  (guide de référence pour tester la sécurité des applications web)

- https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project (livre)

Ethical hacking

– **Offensive Security –** *formations en ligne (payantes) et certifications professionnelles*
https://www.offensive-security.com/information-security-training/

© 2019 Jean-Claude Héritier

Exemples:
Quelques défis de sécurité
(et solutions)

source: http://www.securite-info.org/defis-simples.php

© 2019 Jean-Claude Héritier

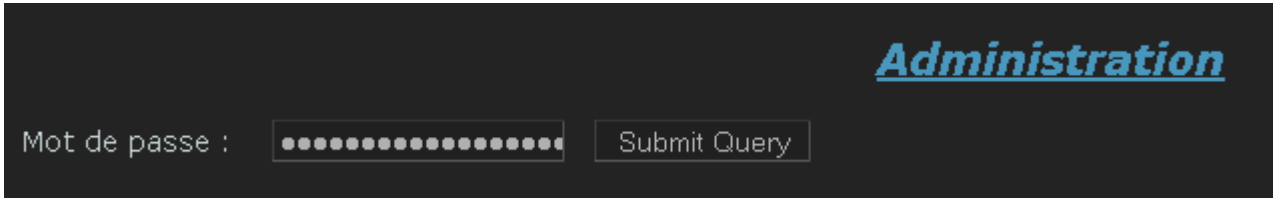
Sécurité des applications Web

Quelques défis de sécurité (simples mais éducatifs ;-))

- **Défi #1:**

  Un webmaster débutant décide de protéger la page d'administration de son site par un mot de passe.
  Étant très pressé, et n'ayant pas le temps de noter le mot de passe, il décide d'utiliser une solution rapide, et imagine qu'aucun de ses visiteurs n'ira chercher le mot de passe...
  Votre objectif est donc de trouver le mot de passe pour pouvoir accéder au niveau suivant.

  http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/1/



Solution: commencer par inspecter le code source de la page…

- **Défi #2:**

  Cette fois-ci, notre webmaster à stocké le mot de passe dans un fichier...

  http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/2/admin.php

Solution: commencer par inspecter la racine du répertoire web…

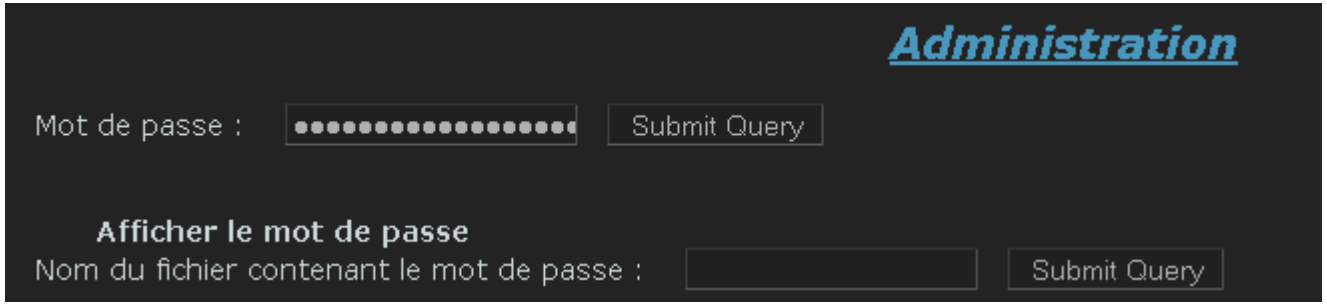
© 2019 Jean-Claude Héritier

Quelques défis de sécurité

- **Défi #3:**

Le webmaster a corrigé la faille, et a choisi de mettre un mot de passe très compliqué.
Le mot de passe est tellement compliqué qu'il n'arrive pas à s'en souvenir.
Donc, il ajoute un formulaire pour afficher le fichier contenant le mot de passe...

http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/3/admin.php



Solution: le serveur attend un nom de fichier précis. Commencer par essayer de contourner le mécanisme de sécurité en soumettant le nom d'un fichier qui existe réellement sur le serveur…

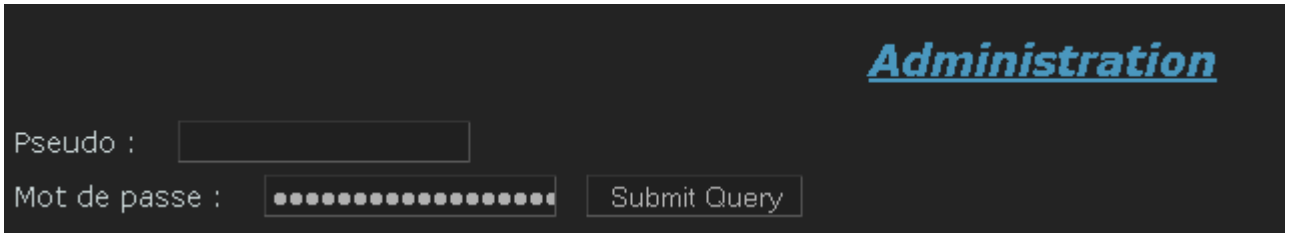
© 2019 Jean-Claude Héritier

Quelques défis de sécurité

- **Défi #4:**

Son système n'étant pas sécurisé, le webmaster a donc décidé d'en faire un plus perfectionné :
Désormais, il faut un pseudo et un mot de passe : le script va chercher le mot de passe correspondant au pseudo, puis le compare avec mot de passe envoyé.
Mais il y a un cas que le webmaster n'a pas prévu...

http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/4/



Solution: commencer par essayer de voir si la page gère les pseudos non existants (i.e. comportement face à un cas non-prévu par le code)…

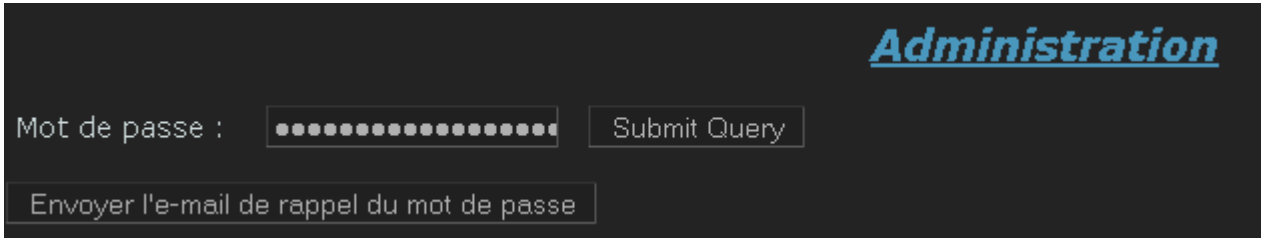
© 2019 Jean-Claude Héritier

Quelques défis de sécurité

- **Défi #5:**

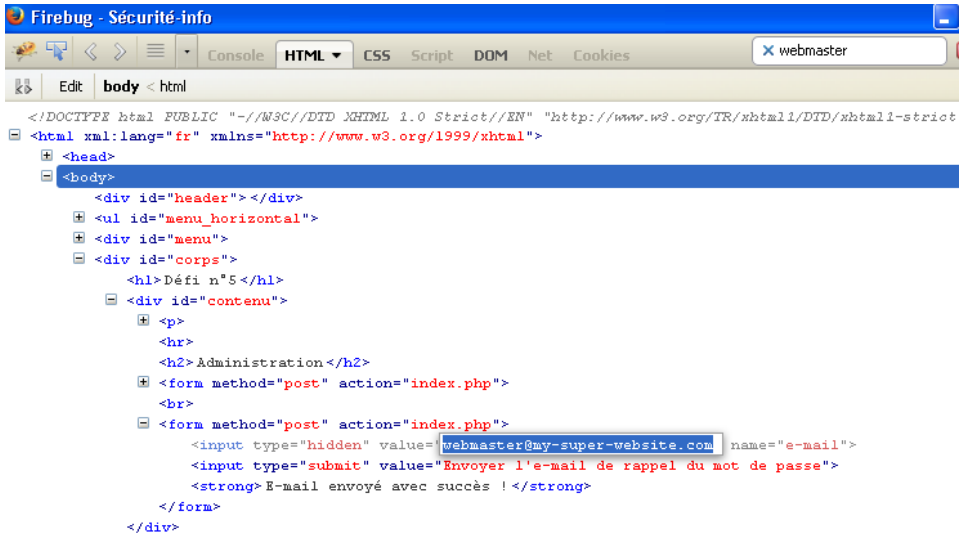
  Après plusieurs aspirines, le webmaster décide de garder un mot de passe très complexe, mais il ajoute une fonction pour s'envoyer le mot de passe par e-mail, afin de ne pas le perdre.

  http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/5/



Solution: essayer de changer l'adresse e-mail vers laquelle est envoyé le mot de passe de rappel…

(possibilité d'utiliser des outils d'édition de code source comme le plug-in Firebug)



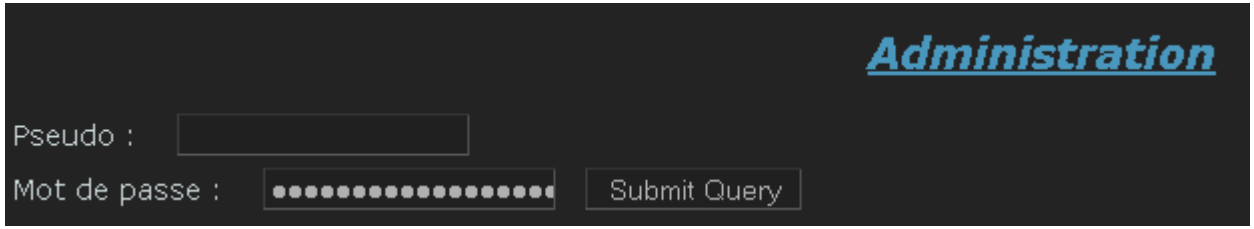
© 2019 Jean-Claude Héritier

Quelques défis de sécurité

- **Défi #6:**

  Notre fameux webmaster découvre qu'il est possible d'utiliser des bases de données en PHP.
  Il installe donc MySQL, puis créé un système de login fonctionnant avec une base de données MySQL...

  http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/6/



Solution: dans le cas de bases de données, essayer de voir si la base de données est vulnérable à l'injection de code SQL…

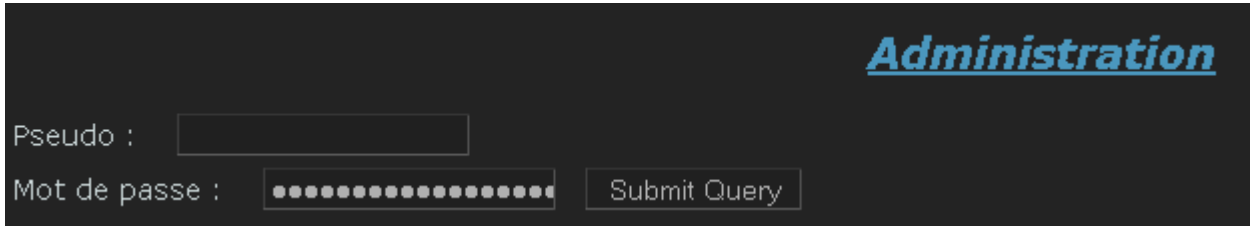
© 2019 Jean-Claude Héritier

Quelques défis de sécurité

- **Défi #7:**

  Après plusieurs mois de déprime, le webmaster décide de faire un système très particulier, dans lequel un mot de passe différent est généré à chaque fois.

  http://www.securite-info.org/defis-simples.php - http://www.securite-info.org/defis-s/7/



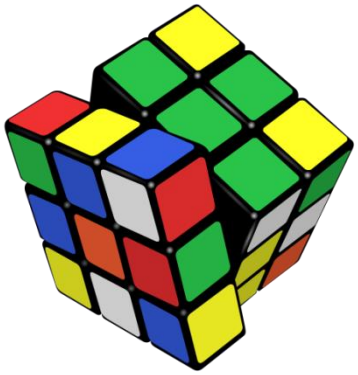
Solutions: Inspecter le code de la page qui montre le hash MD5 du mot de passe attendu.

• option 1: essayer de trouver le mot de passe à l'origine du hash attendu (attaque par force brute) – **LONG!**
• option 2: Peut-on essayer de soumettre à la fois un mot de passe et la valeur du hash attendu pour ce mot de passe ?

© 2019 Jean-Claude Héritier

VII) Sécurité et technologies émergentes

- BYOD
- Cloud computing

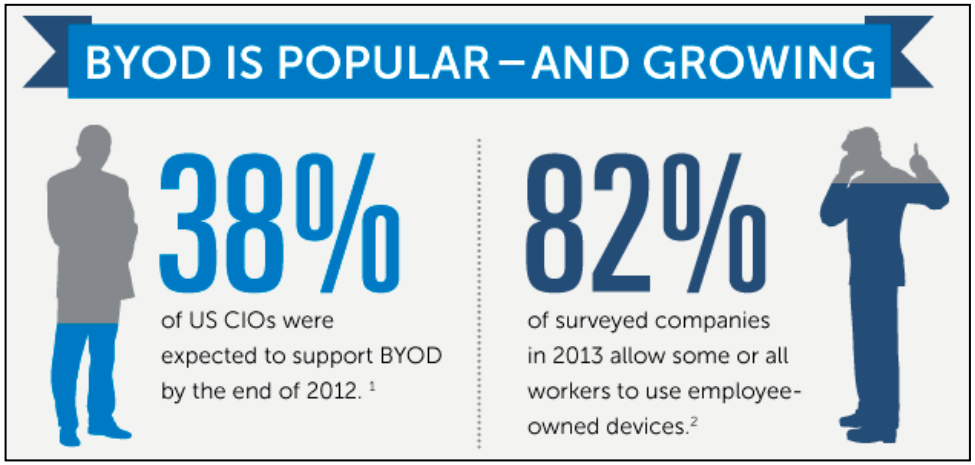


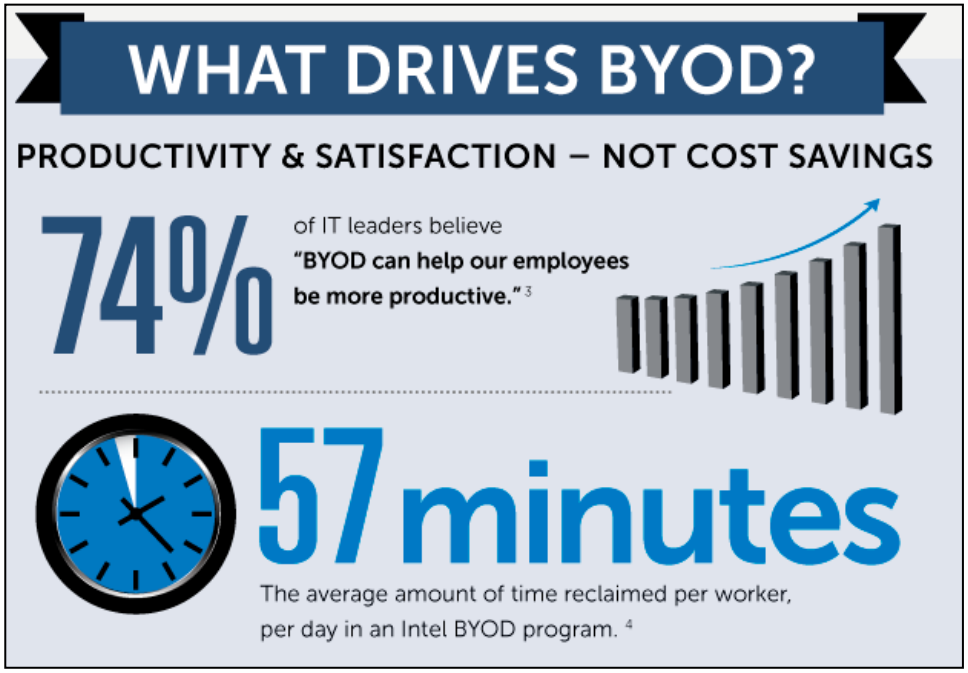
© 2019 Jean-Claude Héritier

Bring Your Own Device

© 2019 Jean-Claude Héritier

Bring Your Own Device
Quelques chiffres





Source: http://www.govtech.com/infographics/BYOD-By-the-Numbers-Infographic.html

© 2019 Jean-Claude Héritier

Bring Your Own Device
Contexte

- **BYOD - Une tendance de fond qui ne peut être ignorée:**
  - Démocratisation de l'équipement privé en *Smartphones*, tablettes et ordinateurs, parfois plus récents et performants que l'équipement mis à disposition en entreprise.
  - Des employés de plus en plus en situation de mobilité et de travail à distance.
  - Une certaine redondance entre outils et applications utilisés dans la sphère professionnelle et privée (ex: messagerie électronique, ordinateurs portables, smartphone, services / stockage en ligne, etc.)
  - Attente de certains employés de pouvoir utiliser le matériel de leur choix (ex: Direction, cadres, jeunes embauchés) -> facteur de différentiation à l'embauche et de productivité.

De plus en plus de salariés apportent leurs équipements personnels au travail (Smartphone, tablettes, PC, etc.) et les utilisent pour accéder au S.I. de l'entreprise:

Exemples: 75% des employés au Brésil et en Russie utilisent leurs propres technologies au travail, ~80% au Moyen-Orient, etc.

- **Exemples et cas d'utilisation:**
  - Accès à la messagerie d'entreprise (webmail) depuis un ordinateur personnel ou Smartphone privé.
  - Connexion à l'Intranet d'entreprise au moyen d'un client VPN sur PC personnel.
  - Accès à des applications métier via une interface web depuis un PC personnel.
  - Etc.

Avantages:
- satisfaction des employés
- productivité améliorée sur des équipements familiers
- réduction des coûts (**à confirmer sur la durée**)

Challenges:
- **sécurité de l'information**
- **problématiques juridiques**

© 2019 Jean-Claude Héritier

Bring Your Own Device
Challenges

De multiples facteurs de risque:

- **Accès à des données d'entreprise depuis des terminaux privés**, qui augmentent la surface d'attaque et le nombre de possibilités de sortir de l'information.
- **Extension des risques du milieu « Consumer » au milieu « Corporate »**
  - vulnérabilités Android et iOS, jailbraking, etc.
  - cohabitation d'applications privées et professionnelles
  - etc.
- **Flotte de terminaux hétérogènes**, complexe à gérer.
- **Sécurité du poste de travail**, qui dépend de l'utilisateur
- **Matériel privé pouvant être partagé** (enfants, famille des employés…), **volé ou perdu.**
- Etc.

Des problématiques juridiques:

- propriété des données lors du départ d'un employé.
- temps de travail.
- limite entre sphère privée et professionnelle.
- cyber-surveillance / traçabilité des employés (GPS).
- effacement à distance d'un terminal personnel par l'entreprise.
- etc.

Challenge pour les DSI:
Comment exercer un contrôle sur ces appareils personnels puisqu'elles restent responsables de la sécurité du réseau de leur entreprise?

A noter: position de l'ANSSI sur les terminaux mobiles

- **«** il est illusoire d'espérer atteindre un haut niveau de sécurité avec un ordiphone ou une tablette ordinaire, quel que soit le soin consacré à son paramétrage.**»**
- **«** Sauf à utiliser des solutions de cloisonnement dont il a été vérifié qu'elles répondent aux besoins de sécurité de l'entreprise, il est préférable d'utiliser des ordiphones professionnels dédiés à cet usage.**»**

© 2019 Jean-Claude Héritier

Bring Your Own Device
Sécurisation

- **Eléments de sécurisation**
  - Solutions de gestion centralisées de terminaux mobiles (« **MDM** »).
  - Si possible, ne rien stocker sur le terminal mobile -> utilisation de solutions de déport d'écran (ex: publication d'applications en mode web): adapté aux ordinateurs, mais moins aux smartphones.
  - Sécuriser les terminaux (smartphones et postes de travail privés) au moyen d'un container professionnel chiffré.
    - Permet de cibler l'effacement à distance.
    - Données vulnérables au jailbraking / existence d'utilitaires de déchiffrement (ex: Elcomsoft Phone Password Breaker).
  - Contrôles d'accès et authentification des terminaux
    - Mot de passe / mot de passe à usage unique / challenge-réponse / certificats, agents, etc.
  - Chiffrement de la carte mémoire (Blackberry, iOS, Android)
    - Attention: la clé de chiffrement est stockée sur le terminal lui-même.
  - Effacement des données à distance
    - Risques: perte de données légitimes en cas d'erreur / effacement massifs en cas de bug, etc.
  - Mesures organisationnelles
    - Charte informatique doit intégrer les aspects BYOD: droits et devoirs des salariés, propriété des terminaux, protection des données personnelles, droit d'effacement à distance, support des terminaux personnels par le personnel de Support Informatique, etc.

© 2019 Jean-Claude Héritier

Cloud computing

© 2019 Jean-Claude Héritier

Cloud Computing
Contexte

- **Pas une technologie nouvelle, mais un nouveau modèle d'affaire.**

- **Technologie désormais mature -** adoption croissante et en accélération du Cloud pour supporter des processus métier de plus en plus nombreux, et parfois critiques.

- **Acceptation du phénomène et feu vert des régulateurs.**
  – Exemple : accord du régulateur bancaire néerlandais (DNB) pour l'utilisation de services « Cloud », au cas par cas (ex: Amazon Web Services (AWS) agréé depuis Juillet 2013 - supporte des plateformes de banque de détail).

Cloud: permet de transférer certains risques vers le fournisseur.

Tous les risques ne peuvent être transférés:
- la gestion peut-être déléguée à un fournisseur de Cloud.
- la responsabilité reste celle de l'Organisation.

En pratique, une majorité des entreprises ont déjà adopté certaines formes de cloud computing:
- 82% utilisent des solutions « Software as a service » (SaaS)
- 51% utilisent des solutions « Infrastructure as a service » (IaaS)
- 40% utilisent des solutions « Platform as a service » (PaaS)

Source: The Global State of Information Security Survey 2013 – PwC

Les entreprises doivent donc adapter leur gouvernance sécurité pour intégrer la gestion des fournisseurs de solutions "cloud" et s'assurer d'une assurance suffisante sur les contrôles sécurité de leurs fournisseurs de solutions Cloud.

© 2019 Jean-Claude Héritier

Cloud Computing
Challenges et sécurité

Avantages en terme de sécurité	Risques / challenges
Economies d'échelle Mutualisation des coûts qui permet de bénéficier de solutions de sécurité avancées et garanties, à moindre prix. Evite aussi pour le client toute maintenance des machines, source d'incidents.	Perte de contrôle Certains contrôles de sécurité peuvent disparaitre lors du mouvement vers le Cloud Computing. Un contrat de service n'assure pas forcément une couverture complète des risques de sécurité,
Interfaces standardisées pour utiliser des fournisseurs de services d'infogérance en sécurité (MSSP): Les fournisseurs de solutions Cloud proposent souvent une interface standardisée et ouverte vers des MSSP.	Enfermement Le Cloud Computing peut introduire une dépendance envers un fournisseur de Cloud particulier, en particulier si la portabilité des données n'est pas assurée.
Continuité et résilience des ressources cloud Les fournisseurs de solutions Cloud peuvent réallouer dynamiquement des ressources, y compris pour assurer la sécurité (filtrage, défense contre le déni de service distribué (DDOS), etc.)	Isolation insuffisante Les solutions externalisées de Cloud Computing reposent fréquemment sur la mutualisation et le partage de ressources entre plusieurs clients. Une isolation insuffisante du stockage, de la mémoire, du routage (ou même les risques de réputation liés à d'autres clients) peuvent avoir des effets désastreux.
Audit et collecte d'évidences Les solutions Cloud permettent une gestion optimisées des journaux d'évènements et permettent ainsi un meilleur suivi des évènement de sécurité sans compromettre trop la performance.	Risques de conformité Dans certains cas, l'utilisation de services Cloud publics peut compromettre la conformité réglementaire (ex: PCI DSS).
Configurations par défaut sécurisées et mises à jour de sécurité régulières Le fournisseurs de Cloud peut utiliser des images et logiciels dont la sécurité aura été renforcée et régulièrement mis à jour en terme de correctifs, du fait de processus optimisés,	Accès aux interfaces de gestion du Cloud Les interfaces de gestion des fournisseurs Cloud publics sont accessibles via l'Internet et donnent potentiellement l'accès à de grandes quantités de données (= cibles privilégiées).

© 2019 Jean-Claude Héritier

Liens et références

- **BYOD**
  - **ANSSI** - Recommandations de sécurité relatives aux ordiphones
    - https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-ordiphones/
      (21 recommandations pour sécuriser au mieux l'emploi de tablettes et smartphones en environnement professionnel).

- **Cloud Computing**
  - **Cloud Security Alliance** - Security Guidance for Critical Areas of Focus in Cloud Computing V3.0
    https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
    (document de référence et actualisé sur la sécurisation du Cloud)

  - **ENISA** - Cloud Computing Risk Assessment
    http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
    (inventaire des risques liés au Cloud et mesures de sécurité associées)

© 2019 Jean-Claude Héritier

VIII) L’investigation numérique légale (« Digital forensics »)

© 2019 Jean-Claude Héritier

L'investigation numérique légale (« Digital forensics »)

Objectifs et défis actuels

- **Objectif:**

  Collecter, conserver et analyser des preuves issues de supports numériques en vue de les produire dans le cadre d'une investigation interne et / ou d'une action en justice.

- **Exemples d'informations analysées lors d'investigations:**
  - E-mails, historique de navigation Internet, messagerie instantanée.
  - Fichiers Word, Excel, etc. et métadonnées (ex: date de dernière modification)
  - Images
  - Logiciels installés
  - Logs d'activité (applications, réseau, etc.

Fichiers non-structurés

Fichiers structurés

QUIZZ: Quels challenges pour l'investigation numérique?

- **Assurer la validité des preuves / éviter toute distorsion**
  - Ne rien faire qui puisse modifier les données (ex: le simple démarrage d'une machine peut rendre les preuves irrecevables)
- **Support multiples et mouvement vers la dématérialisation**
  - Explosion des solutions de stockage et de communication ces 5 dernières années.
  - Démocratisation du stockage dans le « Cloud » (Dropbox, Google drive, iCloud, etc.)
- **Volumes de données à analyser** (croissance exponentielle)
- **Nouveaux défis liés aux technologies** (ex: effacement à distance des terminaux mobiles, solutions anti-investigation: Linux Portable, chiffrement, modification des timestamps, etc.)
- **« Culture de l'impatience »** qui se développe face à la technologie et aux investigations numériques, malgré les défis.

© 2019 Jean-Claude Héritier

L'investigation numérique légale (« Digital forensics »)

Principes clé

Pré-requis: protocole d'autorisation avant investigation interne

- **Approche traditionnelle:**
  1. Débrancher la machine cible (machine « morte »).
  2. Extraire physiquement le disque dur.
  3. Connecter le disque dur à une solution de **copie bit à bit intégrale** du support.
     -> Réalisation d'une copie «parfaite » des données, y compris espace disque non-utilisé.
  4. Prise d'une empreinte numérique (« hash ») du disque source et du disque « image ».
     -> Validation des images
  5. Mettre le disque source sous scellés (si investigation légale)
  6. Analyser les données, typiquement via un expert neutre.
  7. Rapport d'analyse et archivage des preuves.

Exemple de solution matérielle de duplication de disque (Atola Insight)

- **Approche « Live »:** Extraire les données « volatiles » avant déconnection.
- **Exemples de solutions:**

Propriétaires:

- **EnCase Forensic**
- **Forensic Toolkit Imager (FTK Imager)**
- **Nuix eDiscovery** Fonctions avancées: recherche par mots clés, dé-duplication, etc.)
- Live: **Windows Forensic Toolchest (WFT)**

Open-source:

- **CAINE (Computer Aided INvestigative Environment)**
- **BackTrack Linux:** compilation d'outils forensics:
  - dd, Autopsy, Sleuthkit, etc.

Etc.

© 2019 Jean-Claude Héritier

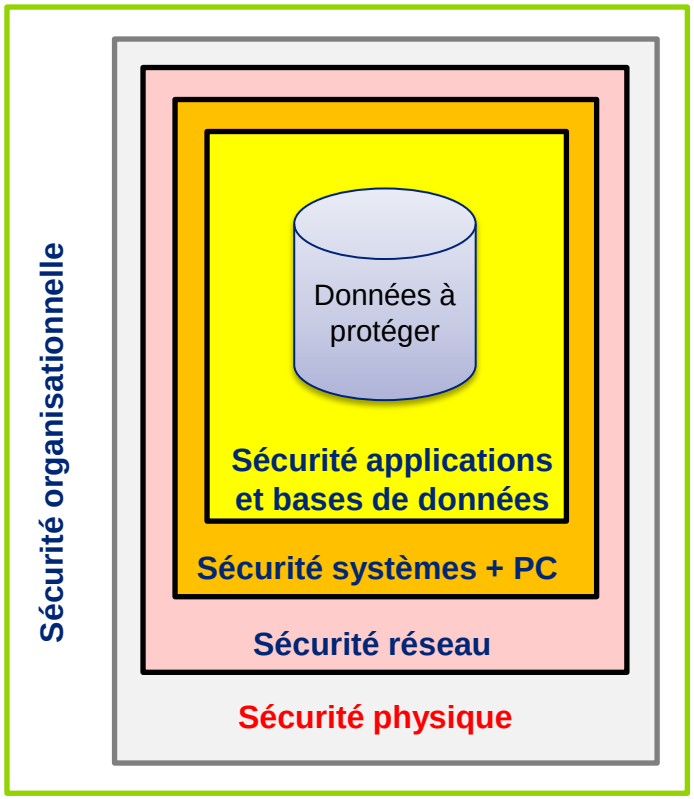
IX) Sécurité physique du système d’information

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information
Introduction

- **La sécurité physique: un élément fondamental de toute démarche de sécurisation de l'information.**

- **Comprend la protection:**
  - **Des bâtiments**
  - **Des équipements matériels:**
    - infrastructure: réseau, serveurs, supports de stockage, postes de travail, etc.
  - **Des informations et logiciels présents sur le matériel:**
    - Applications, bases de données, systèmes d'exploitation.



La sécurité physique constitue la 1ère ligne de défense assurant la sécurité de l'information contre les menaces liées à l'environnement.

Fréquemment soumise à des contraintes liées à l'existant (ex: bâtiments anciens)

Mise en œuvre requiert une analyse des risques et une identification des vulnérabilités.

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information
Menaces

QUIZZ: Quelles menaces ?

- **Menaces liées à l'environnement**
  - Sinistres d'origine naturelle (inondation, tremblement de terre, etc.)

- **Déficience de l'environnement physique**
  - Alimentation électrique (exemple de menaces: Coupures électriques, surtensions)
  - Humidité (ex: fuite d'eau)
  - Température (ex: panne de climatisation)

- **Menaces d'origine humaine**
  - Accès non-autorisés / non-supervisés (ex: accès de tiers non-supervisés aux salles informatiques, équipements mutualisés, etc.)
  - Vol d'information / vol de matériel (fuites d'informations suite à la consultation d'information mise au rebus par l'entreprise)
  - Espionnage (ex: pose de keyloggers matériels sur les postes de travail ou équipements réseau)
  - Equipements hors-site (utilisateurs mobiles, équipements en cours de maintenance, etc.)
  - Pandémie
  - Etc.

A savoir: dans la majorité des cas, l'accès physique à une machine permet de compromettre la sécurité des données.

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information

Quels objectifs?

- **Objectif numéro 1 de la sécurité physique:**

Protéger la vie des employés avant tout

Ex: - agent d'extinction d'incendies potentiellement dangereux (gaz halon)
- ne pas compromettre l'évacuation du personnel

- **Objectif général:** **Protéger les actifs de l'entreprise**
  - Prévenir les menaces
  - Retarder
  - Détecter
  - Evaluer
  - Répondre

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information

Contrôles environnementaux

- **Environnement de contrôle associant contrôles préventifs, détectifs et correctifs.**

Exemples de contrôles environnementaux:

Menace	Prévention	Détection	Correction
FEU			
EAU			
Electricité			
Chaleur			
AUTRES			

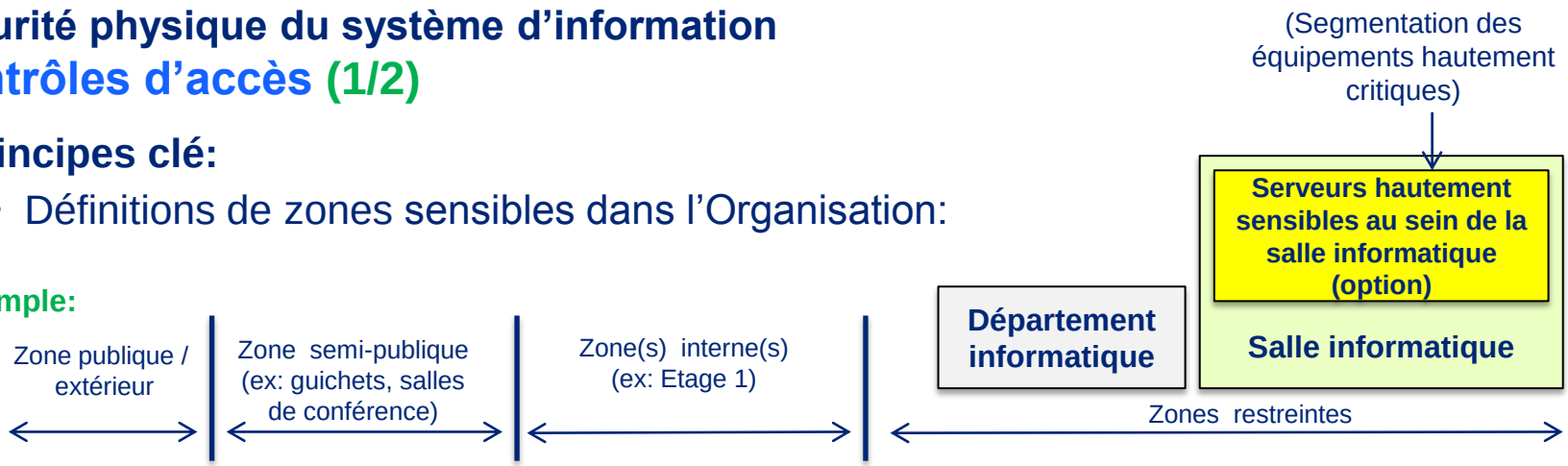
QUIZZ: Quels exemples de défaillances possibles?

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information
Contrôles d'accès (1/2)

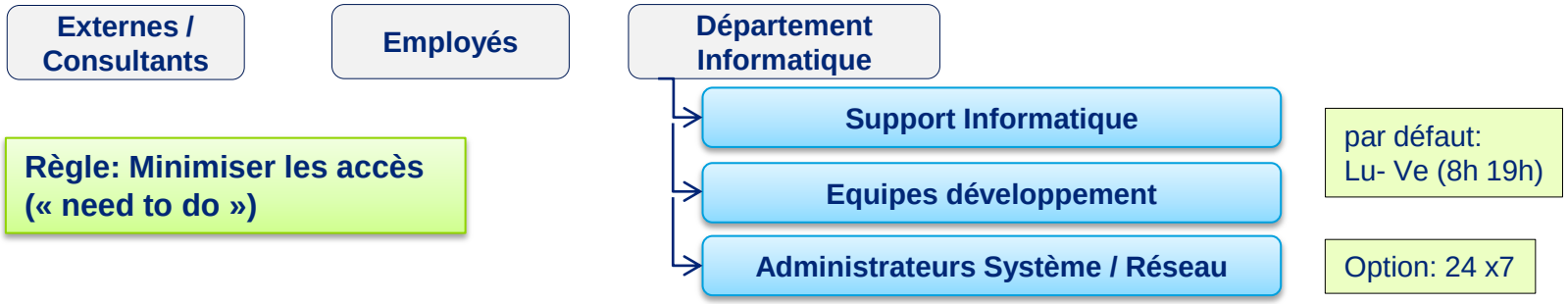
- **Principes clé:**
  - Définitions de zones sensibles dans l'Organisation:

Exemple:



- Prise en compte de la valeur de l'information et du cycle de vie de l'information.

  - Définition de groupes d'accès et plages horaires pour chaque zone:



© 2019 Jean-Claude Héritier

Sécurité physique du système d'information
Contrôles d'accès (2/2)

- **Principes clé:**
  - Dispositifs de contrôle d'accès
    - Identification (ex: réception, badges…)
    - 1 ou 2 facteurs (e.g. badge + code PIN)
    - Assurer une traçabilité via des journaux d'accès.
  - Processus de gestion des accès physiques
    - Processus standard de Création / Modification / Suppression de tout accès physique.
    - Processus initié par les Ressources Humaines ou par le Responsable de service.
    - Contrôle des badges non-attribués.
    - Contrôle des accès au système de gestion des badges.
  - Revues périodiques des contrôles d'accès.
    - Recertification
    - Audit

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information

Exemples de risques et contrôles

Exemples de situations à risque	Exemples de contre-mesures:
• Perte / vol de badge	• Sensibilisation des employés. • Accès restreints (heures / zones) • Authentification (garde / PIN, etc.)
• Archives des données sur cassettes sont conservées hors de la salle informatique	• Externalisation des supports de sauvegarde. • Chiffrement des supports externalisés • Transport par une société spécialisée
• Récupération de documents classifiés par le personnel de nettoyage	• « Clean-desk and clean printer policy » • Sensibilisation des employés. • Classification des documents / poubelles sécurisées
• Consultants externes en mission longue durée sur site.	• Sensibilisation / accord de confidentialité • Accès restreints à certaines zones (ex: étage x) • Identification par badge • Supervision lors d'accès à des zones sensibles.
• Le personnel utilise une entrée de service et arrive en général par groupes le matin.	• Caméras de surveillance. • Double SAS • Tourniquet individuel. • Port de badge

© 2019 Jean-Claude Héritier

Sécurité physique du système d'information

Exemples de risques et contrôles

Exemples de situations à risque	Exemples de contre-mesures:
• La salle informatique dispose d'un système d'extinction par gaz (Argonite). Pour pallier à une faible climatisation, les fenêtres restent entre-ouvertes en été.	• Revoir le système de refroidissement afin d'éviter toute perte d'étanchéité qui peut compromettre l'extinction.
• Les serveurs sensibles de la société sont hébergés au sein d'un centre de traitement mutualisé.	• Assurer une séparation physique des serveurs sensibles au sein du centre mutualisé (option: reprendre les machines sensibles en interne)
• Le serveurs de Test sont hébergés dans la cave de l'établissement car leur disponibilité n'est pas une priorité.	• Evaluer si cette situation est acceptable en fonction de la confidentialité des données présente sur les machines de test (y compris mots de passe).
• En fin de vie, les postes de travail sont recyclés par don à une association.	• S'assurer que les données sur disque sont systématiquement effacées ou détruites de manière sécurisée.
• En cas d'alarme, la procédure est que tout le monde sorte le plus vite possible.	• S'assurer qu'un recomptage a lieu. • S'assurer que ceci ne peut-être exploité pour le vol de documents sensibles (ex: les safety managers vérifient l'évacuation des locaux avant de sortir à leur tour)

© 2019 Jean-Claude Héritier

Questions?

© 2019 Jean-Claude Héritier