Numérique et sciences de l'information

Tous niveaux
Module No 11

Un enjeu majeur, la cybersécurité. Seconde partie

Agenda

- ***A. Les principes et les enjeux***
  - ***C01 Aspects et enjeux de la sécurité***
  - ***C02 Enjeux économiques et modes d'action***
  - ***C03 Plan de secours et plan de continuité des activités***
  - ***C04 Sécurité et commerce électronique. Sécurité et banqueSécurité et banque***
- ***B. Les méthodes et les outils***
  - ***C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse.***
  - ***C06 Architectures de sécurité***
  - ***C07 Renforcer la sécurité des réseaux et des systèmes***
  - ***C08 Renforcer la sécurité des accès et des contrôle d'identités***
  - ***C09 Renforcer la sécurité des applications et des services***
  - ***C10 Renforcer la sécurité des dispositifs mobiles***
  - ***C11 Evaluer la sécurité***
  - ***C12 Manager les risques dans les projets SI***
- ***C. Bilan et perspectives***

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des données. Cryptographie et cryptanalyse.***
    - ***Définitions, théorie et pratique.***
    - *Evolution des législations.*

Définitions

- **Chiffrer**, c'est transformer la teneur d'un message avec une clef pour que seul le destinataire qui possède la même clef puisse comprendre le sens du message.
- Le **chiffrement** est une des techniques de la cryptologie, science qui regroupe la cryptographie et la cryptanalyse.
- La **cryptographie** (du grec kruptos (caché) et graphein (écrire)) peut être assimilée à « l'étude des écritures secrètes" et consiste en l'art de dissimuler ses instructions à ses ennemis tout en étant capable de les transmettre à ses amis au moyen d'un texte chiffré.
- En face, chez l'adversaire, il s'agit de briser le code, de trouver le système qui préside à son élaboration : c'est la **cryptanalyse**.

Définitions

- Les logiciels de chiffrement ont pour vocation de rendre illisibles le contenu de documents confidentiels pour tous ceux qui ne possèdent pas la clef de déchiffrement.
- Ceux qui possèdent cette clef **déchiffrent** le document.
- Ceux qui ne la possèdent pas et désirent –le plus souvent pour de mauvais motifs- en lire le contenu tentent de **décrypter** le document.
- On peut distinguer deux principaux types de chiffrement : le **chiffrement à clef privée** et le **chiffrement à clef publique**.

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des données. Cryptographie et cryptanalyse.***
    - *Définitions, théorie et pratique.*
    - ***Evolution des législations.***

Evolution des législations

- Les systèmes de cryptage sont d'autant plus efficaces que la clef de chiffrement est plus longue.
- Les USA ont longtemps limité l'exportation des produits de chiffrement aux versions incluant des clefs de 40 bits alors qu 'ils utilisaient en interne des clefs de 128 bits.
- Deux lois de 97 ont libéralisé l'exportation des matériels et logiciels de cryptographie.
- Le problème légal en France : la loi du 29/12/90 imposait de faire la demande d'autorisation d'un logiciel de cryptage auprès du Service Central de la Sécurité des Systèmes d'Information.
- Le SCSSI vérifiait que l'algorithme utilisé n'est pas trop efficace pour être en mesure de décrypter lui-même l'information.
- Ainsi *Netscape* a du ainsi demander l'autorisation d'employer SSL dans son navigateur importé en France.

Evolution des législations

- Des lois récentes ont libéralisé l'usage des dispositifs de cryptage et ont prévu la création des tiers de confiance.
- En France, depuis les décrets du 19 mars 1999, il était possible d'utiliser :
  - Une clef de 40 bits, en totale liberté quelque soit l'usage.
  - Une clef de 128 bits en totale liberté pour un usage privé, et soumise à déclaration dans les autres cas.
- La **loi sur l'économie numérique** de février 2003 a modifié ces dispositions libéralisant le recours et l'usage aux logiciels de chiffrement, et ce sans limitation de puissance.
- Il n'y a donc plus de "verrou" des 128 bits, taille de clef au-delà de laquelle un simple usage devait être déclaré.
- En revanche, la fourniture de moyen de chiffrement reste sujette à déclaration : un simple usager d'un système libre *GNU/Linux* doté d'un module de chiffrement et voulant le partager pourra être assimilé à un "fournisseur".

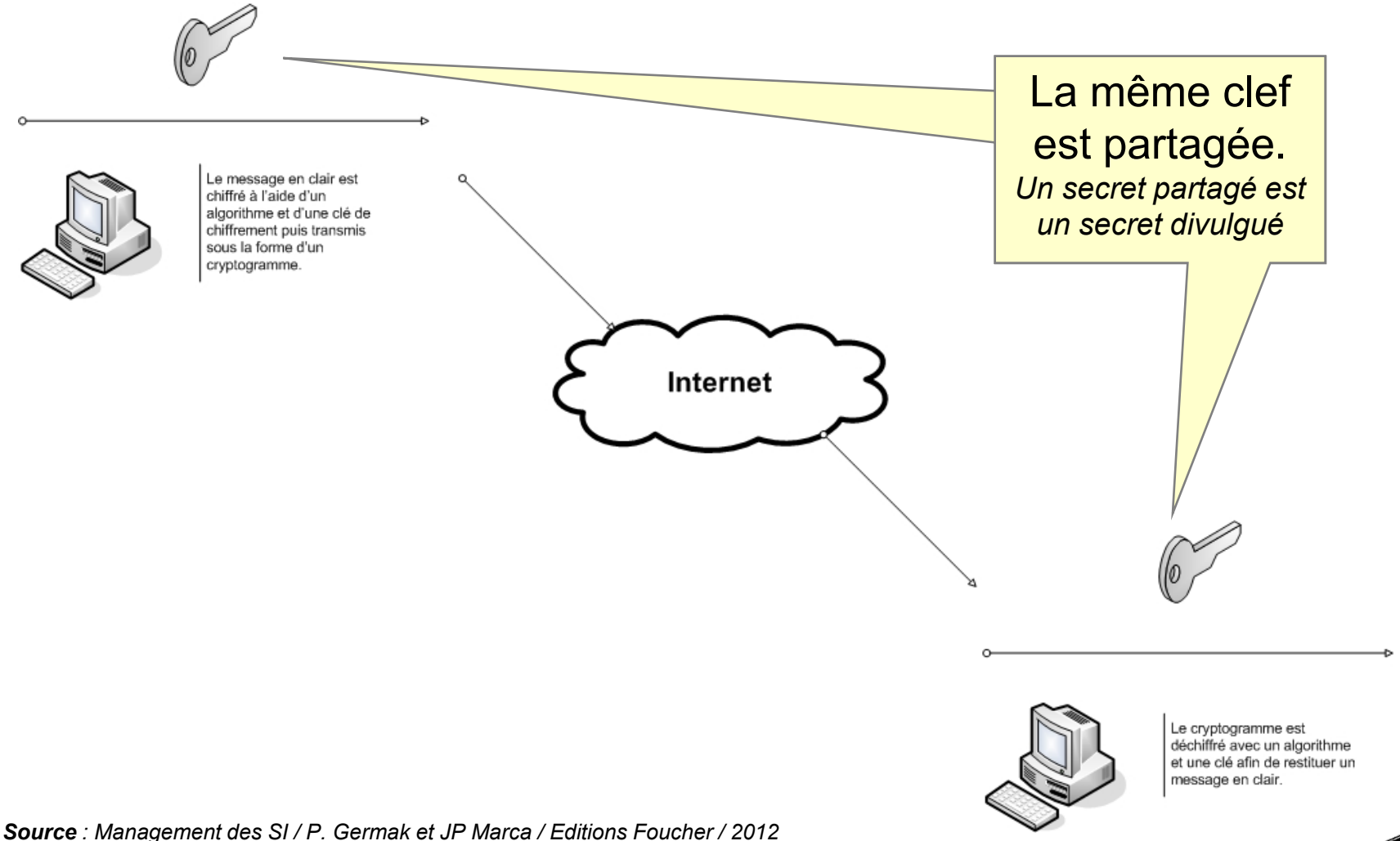
Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - ***Chiffrement à clef privée.***
    - *Chiffrement à clef publique.*
    - *Algorithmes de chiffrage.*
    - *PGP et GnuPG*
    - *Mise en place d'une architecture PKI. Certification et enregistrement.*

Chiffrement à clef privée

- Les algorithmes **à clef privée sont** aussi appelés algorithmes symétriques.
- En effet, lorsque l'on chiffre une information à l'aide d'un algorithme symétrique avec une clef secrète, le destinataire utilisera la même clef secrète pour déchiffrer.
- Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clef privée auparavant, par courrier, par téléphone ou lors d'un entretien privé.
- Les deux utilisateurs utilisent cette même clef pour chiffrer et déchiffrer un message.

Chiffrement à clef privée



***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

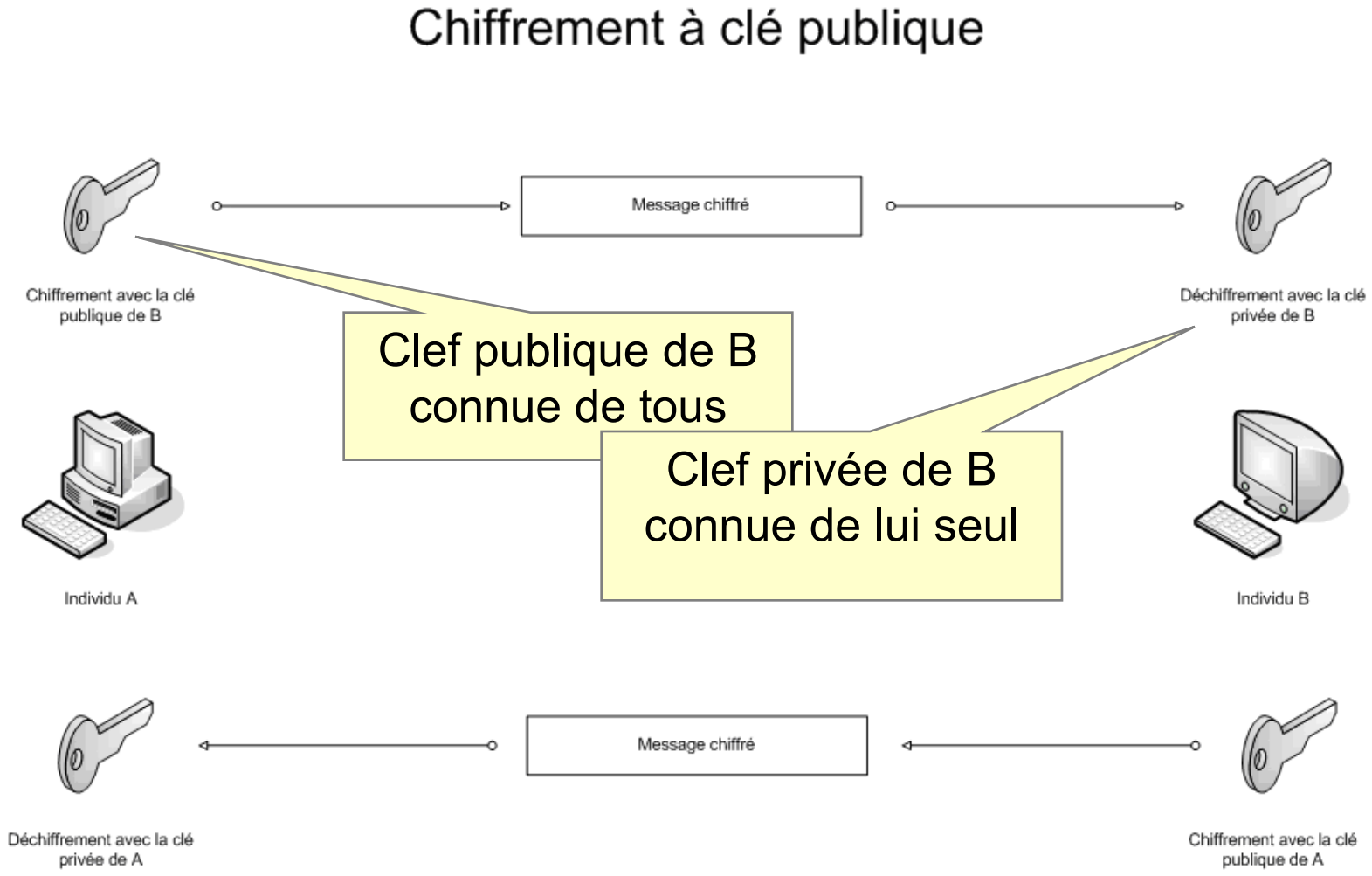
Plan

- **B. Les méthodes et les outils**
  - **Architectures de sécurité**
    - Chiffrement à clef privée.
    - **Chiffrement à clef publique.**
    - Algorithmes de chiffrage.
    - PGP et GnuPG
    - Mise en place d'une architecture PKI. Certification et enregistrement.

Chiffrement à clef publique

- La cryptographie **à clef publique** a été inventée par Whitfield Diffie et Martin Hetlman en 1976 pour éviter ce problème d'échange de clef secrète préalable.
- Les algorithmes à clef publique, appelés algorithmes asymétriques, utilisent la clef publique (connue de tous) du destinataire, qui sera à priori le seul à pouvoir le déchiffrer à l'aide de sa clef privée (connue de lui seul).
- Une fois un message envoyé chiffré avec la clef publique du destinataire, nul autre que lui ne peut le déchiffrer, pas même l'expéditeur.

Chiffrement à clef publique



***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

Chiffrement à clef publique

- Outre la confidentialité, ce système assure aussi le principe de non-répudiation.
- La non-répudiation doit reposer dans une preuve de la signature, détenue par le destinataire du document signé, vérifiable par un tiers, inaltérable par l'émetteur signataire.
- Pour conférer cette qualité à sa signature, il suffit que l'émetteur la chiffre avec sa clef privée.
- Le destinataire la déchiffre avec la clef publique du signataire.
- La réussite du déchiffrement apporte la preuve que la signature est authentique.
- Si la signature est constituée par un ***condensat*** du message (résumé numérique obtenu par un algorithme de condensation type *MD5* ou *SHA*), on garantit en plus l'intégrité du message.

Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - *Chiffrement à clef privée.*
    - *Chiffrement à clef publique.*
    - ***Algorithmes de chiffrage.***
    - *PGP et GnuPG*
    - *Mise en place d'une architecture PKI. Certification et enregistrement.*

Algorithmes de chiffrage

$A(C)$
M → C

$B(D)$
C → M

- Le message M est transformé en C via un algorithme *A* utilisant une clef de chiffrage C.
- Le message chiffré C est retransformé en M via un algorithme *B* utilisant une clef de déchiffrage D.
- La sécurité ne doit pas dépendre du secret des algorithmes, *A* et *B* mais uniquement du secret des clefs C et D.
- Le code doit être très difficile à casser en partant uniquement des messages cryptés
- Le code doit être très difficile à casser même si l'on dispose d'un échantillon de messages et des messages cryptés correspondants .

RSA

- Le plus célèbre des algorithmes à clef publique, ***RSA***, est dû à Ron ***R***ivest, Adi ***S***hamir et Leonard ***A***dleman du MIT.
- Les clefs sont constituées de la façon suivante :
  1. Choisir deux (grands) nombres premiers p et q.
  2. Calculer $n=p*q$: les opérations s'effectueront modulo n.
  3. Calculer $\varphi(n)=(p-1)(q-1)$.
  4. Choisir un entier e inférieur à $\varphi(n)$ et premier avec $\varphi(n)$: c'est l'exposant de la clef publique.
  5. Calculer l'inverse d de e pour la multiplication modulo $\varphi(n)$ (il existe et est unique puisque e et $\varphi(n)$ sont premiers entre eux : calcul par l'algorithme d'Euclide). L'entier d est l'exposant de la clef privée.
- La clef publique se compose de l'entier n et de l'exposant e, connus de tous.
- La clef privée est l'exposant d qui doit être tenu secret.

RSA

- Voici comment fonctionnent le codage et le décodage :
  - Le message à transmettre est d'abord transformé en un entier (par exemple par concaténation des codes ascii des caractères qui le composent).
  - On note *m* cet entier qui est censé être inférieur à *n*.
  - Le codage le transforme en $c=m^e \text{ modulo } n$.
  - Pour décoder, il faut connaître *d* et calculer $c^d \text{ modulo } n$.
  - On retrouve *m*.
- Évidemment, quelqu'un qui connaît *n* peut théoriquement retrouver ses deux facteurs premiers *p* et *q* et donc recalculer les éléments de la clef privée.
- La sécurité du système repose sur le fait que la décomposition d'un nombre en produit de facteurs premiers est très coûteuse en temps de calcul : il est virtuellement impossible de décomposer un nombre produit de deux très grands facteurs premiers.
- Cela n'empêche pas les utilisateurs de changer assez souvent de clef par mesure de sécurité.

AES

- ***Advanced Encryption Standard*** ou ***AES*** (soit « standard de chiffrement avancé »), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique.
- Rappelons que *RSA* est un algorithme de chiffrement asymétrique (ou à clef publique).
- Chiffrement déchiffrement se font avec une seule clef AES, alors qu'on doit utiliser 2 clefs séparées (une clef publique et une clef privée) en RSA.
- La force d'une clef 128-bits AES est approximativement equivalente à une clef 2600-bits RSA mais les deux algorithmes ont une finalité différente :
  - Pour chiffrer ses propres sauvegardes : AES.
  - Pour chiffrer des échanges avec des tiers : RSA
- AES est devenu le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis.
- Il a été également approuvé par la NSA (*National Security Agency*) pour les informations top secrètes.

Algorithmes de chiffrage

- Le chiffre de Vigenere, considéré comme incassable au milieu du XIX siècle, a été a été cassé par le major prussien Friedrich Kasiski en 1863.
- L'algorithme du sac à dos (algorithme de Hellman, Merkle et Diffie) proposé comme une solution à clef publique a été rejeté en quelques années.
- Le DES, algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clefs de 56 bits a été déclassifié en 1999.
- RSA doit utiliser des produits de deux nombres premiers de plus en plus grands, pour garder toujours une longueur d' avance face à la puissance de calcul croissante des ordinateurs qui permet d'explorer toutes les combinaisons dans un temps raisonnable.
- Si un mathématicien découvrait une technique permettant de factoriser sans effort un nombre de n'importe quelle longueur, RSA serait facilement « cassable ».
- L'architecture et la longueur des clefs de AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ».
- Le niveau « TOP SECRET » nécessite des clefs de 192 ou 256 bits.
- L'AES n'a pour l'instant pas été cassé et la recherche exhaustive (« force brute ») demeure la seule solution (2^{128} opérations pour une clef de 128 bits)
- **Mais le chiffrement absolu n'existe pas.**

Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - *Chiffrement à clef privée.*
    - *Chiffrement à clef publique.*
    - *Algorithmes de chiffrage.*
    - ***PGP et GnuPG***
    - *Mise en place d'une architecture PKI. Certification et enregistrement.*

PGP et GnuPG

PGP

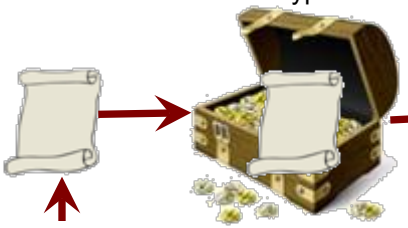
- "***Pretty Good Privacy***" (en anglais : "Plutôt bonne intimité") est un logiciel de cryptographie renforcée qui est bien adapté à l'utilisation sur Internet.
- PGP est gratuit, facile d'utilisation, et disponible en français.
- PGP a été créé en 1991 par Philip Zimmermann, un informaticien américain.
- Ayant diffusé son logiciel sur Internet, il a été poursuivi par le gouvernement américain pour trafic d'armes (car la cryptographie est considérée là-bas comme une "arme" interdite d'exportation).
- PGP, utilise à la fois les clefs symétriques ("clef de session" de 128 bits) et les clefs asymétriques ("clef publique" de 512 à 2048 ou 4096 bits qui permet de crypter la clef de session).

PGP

- Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées.
- Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.
- La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement.
- La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.
- Ensuite, l'opération de chiffrement se fait principalement en deux étapes :
  - PGP crée une clef secrète IDEA de manière aléatoire, et chiffre les données avec cette clef
  - PGP crypte la clef secrète IDEA et la transmet au moyen de la clef RSA publique du destinataire.
- L'opération de déchiffrement se fait également en deux étapes :
  - PGP déchiffre la clef secrète IDEA au moyen de la clef RSA privée.
  - PGP déchiffre les données avec la clef secrète IDEA précédemment obtenue.

PGP

Le texte en clair est crypté avec la clef de session



Texte chiffré

La clef de session est cryptée avec la clef publique de B

Emetteur A

Message crypté = texte chiffré + clef de session cryptée

Récepteur B

Envoi via réseau

Réseau

Clef de session à durée de vie limitée

Clef publique de B

Clef privée de B

Clef privée de B utilisée pour déchiffrer la clef de session

Clef de session utilisée pour déchiffrer le texte transmis

Texte chiffré

Texte en clair d'origine

PGP

- Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clef publique à la vitesse du cryptage conventionnel.
- Le chiffrement conventionnel symétrique est environ 1000 fois plus rapide que les algorithmes de chiffrement asymétriques à clef publique, mais n'est pas adapté aux échanges.
- Le chiffrement à clef publique résoud le problème de la distribution des clefs.
- Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clefs, sans pour autant compromettre la sécurité.

GnuPG

- ***GnuPG*** (ou *GPG*, de l'anglais ***GNU Privacy Guard***) est l'implémentation *GNU* du standard OpenPGP défini dans la RFC 48802.
- Le projet est initié à la fin des années 1990 dans le but de remplacer la suite PGP par une alternative en logiciel libre.
- Il est distribué selon les termes de la *GNU GPL.*
- Le risque principal de *GnuPG*, comme pour tous les procédés de chiffrement à clef publique, est que la clef privée doit être enregistrée quelque part.
- Si c'est sur une clef *USB* que l'on garde avec soi, les risques de perte, de vol ou de copie existent. Si elle se trouve sur le disque dur d'un ordinateur, on est alors exposé aux risques classiques du piratage. Notons qu'une phrase (ou mot) de passe, optionnelle mais pouvant protéger la clef privée, limite alors les risques.
- Depuis sa version 2.0, *GnuPG* peut être installé sur une carte à puce. La clef privée est alors protégée par le code *PIN* de la carte, ce qui permet d'en améliorer sensiblement la confidentialité.

Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - *Chiffrement à clef privée.*
    - *Chiffrement à clef publique.*
    - *Algorithmes de chiffrage.*
    - *PGP et GnuPG*
    - ***Mise en place d'une architecture PKI. Certification et enregistrement.***

Retour sur le chiffrement à clef publique

- Le chiffrement des données est complexe à mettre en œuvre.
- Il nécessite des boîtiers spécialisés et/ou des logiciels de chiffrement à toutes les extrémités du réseau, ainsi que des échanges de clefs.
- Ces échanges reposent sur une infrastructure technique et des procédures d'exploitation et d'administration qui permettent de délivrer et de stocker des certificats numériques de manière sécurisée (Infrastructure à clef publique ou **PKI – Public Key Infrastructure**).
- Un certificat électronique est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.
- Ces certificats permettent d'accéder aux clefs publiques.
- Problème : Peut-on faire confiance à l'organisme qui distribue les clefs ?

Certificats numériques

- Comment Juliette peut-elle être certaine que la clé publique qu'elle reçoit est bien celle de Roméo et vice-versa ?
- La solution est de passer par un **tiers de confiance** reconnu par tous deux, et qui va leur fournir des **certificats**.
- Un certificat est un document électronique (un fichier) qui atteste qu'une clé publique est bien liée à une organisation ou une personne.
- Il ne contient que des éléments publics.
- Sa diffusion ne pose donc évidemment aucun problème de sécurité.
- Le tiers de confiance est un organisme indépendant qui atteste de la véracité, via sa signature électronique, des informations contenues dans le certificat.
- Un tel organisme est désigné sous le nom d'**Autorité de Certification** (**AC**).

Certificats numériques

- Un certificat contient généralement :
  - la clé publique de l'entité (utilisateur, serveur);
  - un nom et d'autres champs permettant d'identifier cette entité (société, service) ;
  - les dates de début et de fin de validité du certificat ;
  - un numéro de série ;
  - le nom de l'organisation qui contresigne le certificat ;
  - la signature des données du certificat par l'Autorité de Certification (AC).

Certificats numériques

- Le Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique le définit ainsi : « ***Certificat électronique*** *: un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire* » ;

- Avec cette autre précision : « *les données de vérification de signature électronique sont les éléments, tels que des clefs cryptographiques publiques, utilisés pour vérifier la signature électronique*. »

- On le voit au travers de ces définitions, le **certificat numérique** est l'instrument qui va remplir un double rôle : permettre le chiffrement avec des clefs et attester l'identité du signataire.

- Un autre point à noter est l'indication de « clefs cryptographiques publiques », ce qui veut dire que système de chiffrement doit impérativement être asymétrique.

Certificats numériques

- L'usage du certificat électronique de signature permet :
  - l'authentification de l'émetteur : confirmation que le document est bien envoyé par la personne identifiée ;
  - l'intégrité des données transmises : cohérence entre les données envoyées et celles reçues ;
  - la non-répudiation des messages : ('ensemble de ces fonctionnalités offre l'assurance que ni la transaction elle-même, ni les informations transmises lors de cette transaction ne pourront être contestées ultérieurement par l'émetteur.
- L'usage du certificat électronique de chiffrement permet :
  - la confidentialité : protection contre toute tentation de piratage et préservation de la confidentialité des échanges.

Certificats numériques

- Lors d'une authentification à clef publique, le récepteur du message doit connaître la clef publique de son interlocuteur.
- Mais il doit pouvoir en vérifier la validité auprès d'un tiers de confiance, dans la mesure où une usurpation d'identité serait possible.
- Le vérificateur doit s'adresser à une autorité de certification, une instance fiable et indépendante chargée de gérer les clefs publiques des interlocuteurs de confiance.
- L'autorité de certification procure un certificat numérique contenant le nom de l'interlocuteur et la clef publique de confiance.
- La norme gérant les certificats numériques est appelée X.509 de l'Union Internationale des Télécommunications.

Fonctionnement d'une architecture PKI

- **L'entité finale** ou entité d'extrémité (EE : End Entity) : l'utilisateur ou le système qui est le sujet du certificat
- **L'autorité d'enregistrement** (AE/RA) : exécute les vérifications d'usage sur l'identité de l'utilisateur. Fait la demande de certificat et donne le certificat signé à l'utilisateur.
- **L'autorité de certification** (AC/CA) : signe les demandes de certificat (CSR) et les listes de révocation (CRL)
- **L'autorité de dépôt** (AD/Repository) : stocke les certificats numériques et les listes de révocation (CRL).
- **L'autorité de séquestre** (AS/Key Escrow) : stocke de façon sécurisées les clefs de chiffrement qui ont été engendrées par l'IGC, pour pouvoir les restaurer le cas échéant.

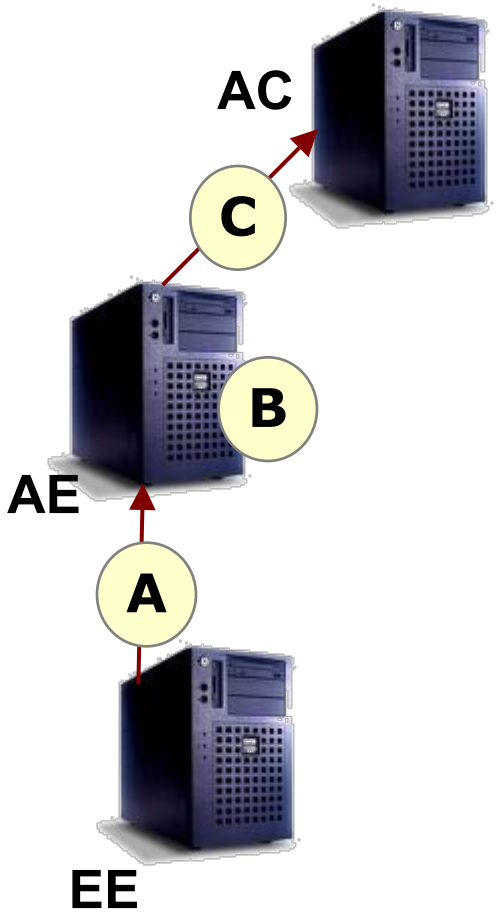
Fonctionnement d'une architecture PKI

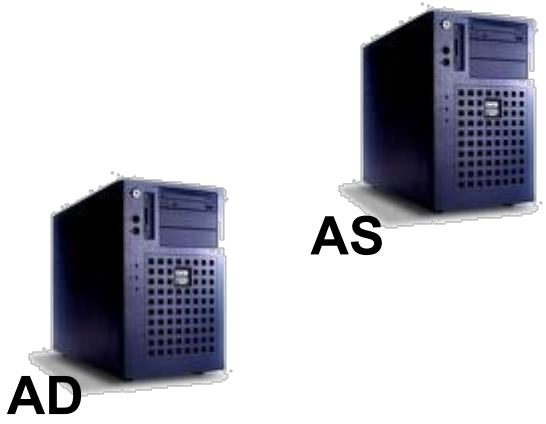
A. Le serveur EE a fait une demande de certificat à AE en remplissant un formulaire et en fournissant les justificatifs.

B. EE ne requiert pas directement son certificat auprès de l'AC, de même qu'un citoyen s'adresse à la mairie pour obtenir un passeport qui sera délivré par la Préfecture.
L'AE d'une PKI vérifie le lien entre le sujet et sa clé publique.
L'AE peut être :

- une agence commerciale d'une banque ou d'un opérateur ;
- le correspondant RH d'un employé d'une entreprise ;
- un simple site web, à condition que l'AE dispose de moyens complémentaires pour vérifier l'identité du sujet : adresse e-mail, authentifiant et mots de passe transmis par une voie tierce telle que le courrier postal…

C. AE transmet la demande (CSR) à AC.





Fonctionnement d'une architecture PKI

D. L'AC est l'entité morale qui signera et délivrera les certificats en son nom,
Par exemple :

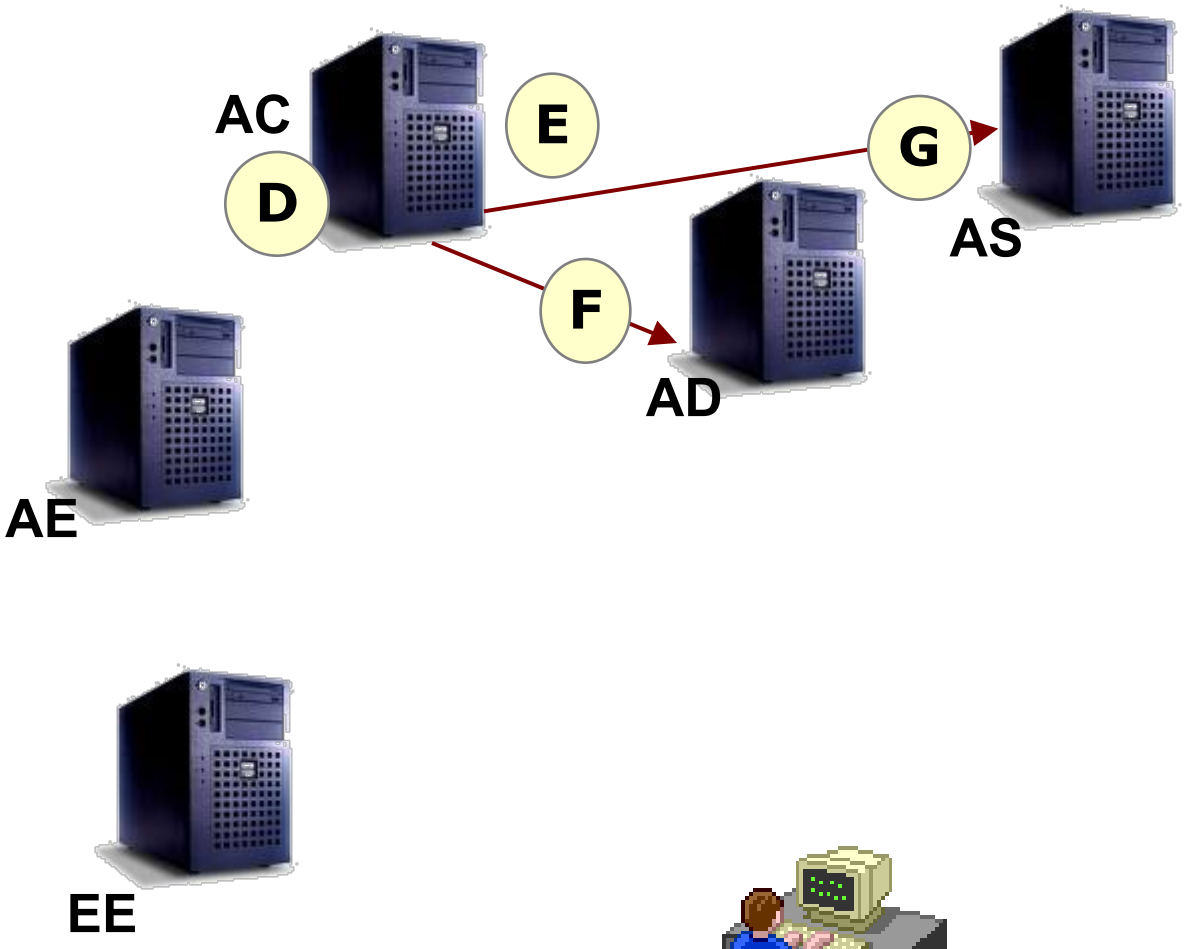
- une grande entreprise pour délivrer des certificats à ses employés ;
- un opérateur de services (Globalsign, Symante0verisign) pour ses clients ;
- une banque pour ses clients particuliers ou entreprises ;
- une administration.

L'AC veille à l'application de la politique de certification adoptée pour la PKI.
La paire de clefs peut être générée en divers lieux (EE, AE ou AC selon le cas).
Considérons le cas le plus sécurisé (AC).

E. AC crée une clef privée et le certificat (qui contient la clef publique)

F. AC transmet le certificat à AD

G AC transmet la clef privée à AS

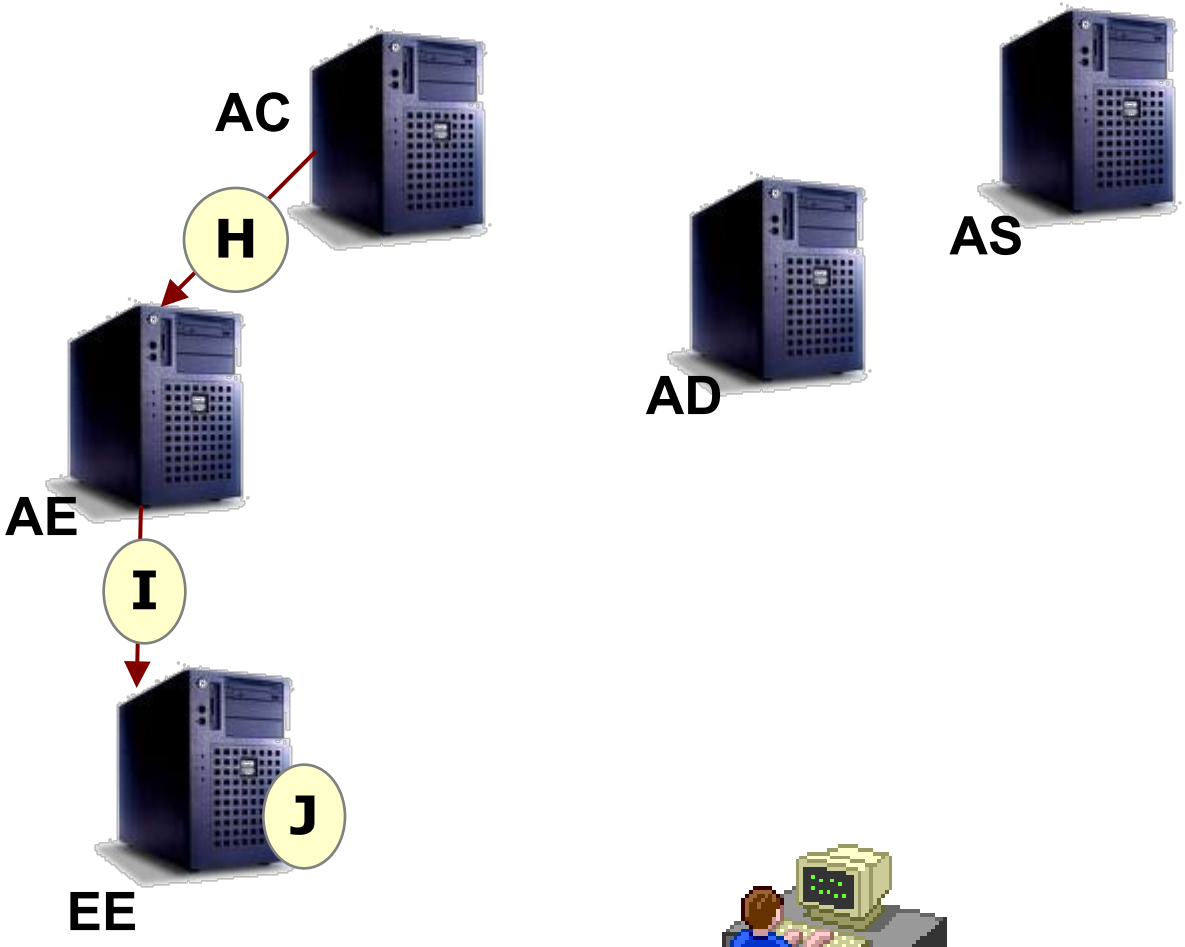


Fonctionnement d'une architecture PKI

H. AC transmet le certificat signé (CRT) ainsi que la clef privée à AE.

I. AE retransmet le certificat signé (CRT) ainsi que la clef privée à AEE

J. EE est en mesure de communiquer ce certificat (et la clef publique associée) à toute entité utilisatrice qui en fait la demande.



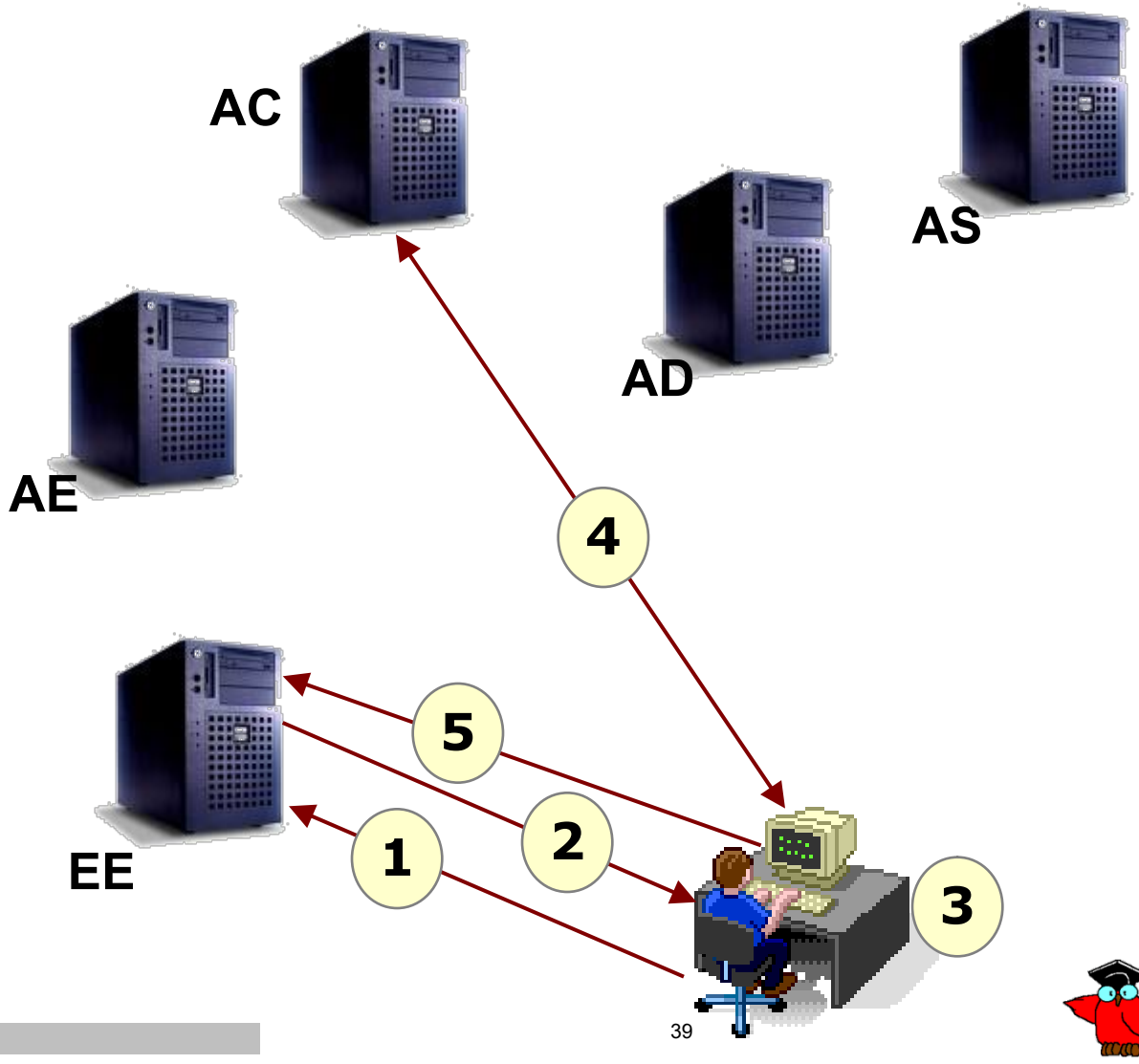
Fonctionnement d'une architecture PKI

1. L'utilisateur demande au serveur de prouver son identité

2. Le serveur EE montre un certificat signé

3. L'utilisateur vérifie le certificat du site :
   - il regarde la date de validité du certificat;
   - Il vérifie que l'adresse du serveur correspond bien à l'adresse indiquée par le certificat;
   - Il fait confiance à l'AC (4) concernée quant à la vérification des informations associées au site lors de la création du certificat;
   - Il vérifie que le certificat a bien été scellé par cette AC :
     - Il utilise la clef publique de l'AC pour déchiffrer l'empreinte cryptée du certificat,
     - Il calcule l'empreinte du certificat,
     - Il compare les empreintes.

5. Il accède au serveur EE



Fonctionnement d'une architecture PKI

Signature d'un certificat par une Autorité de certification

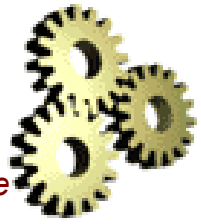
Certificat

Nom : J. Surfe

Clef publique :

Autorité de certification : BP

Signature de l'autorité de certification :



Signature

Clef privée de l'autorité de certification

Vérification de la validité du certificat par l'utilisateur

Certificat

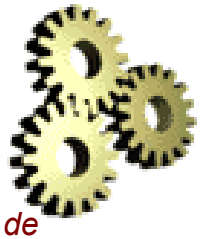
Nom : J. Surfe

Clef publique :

Autorité de certification : BP

Signature de l'autorité de certification :

Clef publique de l'autorité de certification



Vérification de signature

OK ?

But d'une architecture PKI

- Les infrastructures à clefs publiques (ICP ou PKI) assurent une prise en charge intégrale de la gestion des clefs.
- Objectif : Conformément à ce que nous avons dit dans les diapositives précédentes, délivrer des certificat numériques qui offrent les garanties suivantes lors des transactions électroniques :
  - Confidentialité : seul le destinataire légitime du message pourra le lire
  - Authentification : l'identité de l 'émetteur est garantie
  - Intégrité : Garantie qu'un message expédié n'a pas altéré accidentellement ou intentionnellement ;
  - Non-répudiation : l'auteur du message ne peut pas renier son message.

But d'une architecture PKI

- **Sécurisation des échanges Web**
- Aujourd'hui, les certificats les plus couramment utilisés sont les certificats serveurs, c'est-à-dire des certificats garantissant le lien entre un nom de serveur (www.ma-banque.fr) et sa clé publique.
- Un tel certificat est utilisé pour que des utilisateurs puissent authentifier le serveur avant de lui envoyer des informations confidentielles.
- Ils permettent en outre de mettre en place, via un protocole adéquat (SSLv3, TLS) une connexion sécurisée (chiffrée) permettant de sécuriser les échanges.
- Ce type de certificat est largement utilisé par les sites d'achat en ligne.
- Des serveurs peuvent également utiliser des certificats pour s'authentifier mutuellement et échanger des données de manière sécurisée.
- Quand des certificats utilisateurs sont déployés, d'autres usages sont possibles.

But d'une architecture PKI

- **Authentification forte des utilisateurs**
- Les certificats utilisateurs permettent l'authentification des utilisateurs, aussi bien en local, que pour un accès distant ou nomade en faisant appel aux techniques de RPV.
- Ils peuvent être utilisés pour autoriser l'accès à un réseau filaire ou Wi-Fi (802.1X).
- La sécurité de l'authentification ainsi obtenue est largement supérieure au couple classique identifiant / mot de passe, procédé très répandu mais qui n'offre qu'une faible sécurité.
- L'usage de la PKI permet une authentification multi-facteurs :
  - quelque chose que l'utilisateur possède : la carte à puce dans laquelle est stockée la clé privée ;
  - quelque chose que l'utilisateur connaît : le code PIN nécessaire pour débloquer l'usage de la clé secrète par la carte.
- A noter que l'authentification est la plupart du temps mutuelle puisque le serveur fournit également un certificat qui permet au client de l'authentifier.

But d'une architecture PKI

- **Messagerie sécurisée**
- **Horodatage**
- **Télé-procédures administratives**
- Au-delà de ces utilisations classiques, l'apparition en France des télé-procédures administratives a offert aux PKI une nouvelle occasion de montrer leur intérêt.
- Les télé-procédures les plus connues étaient TéléTVA pour la déclaration de la TVA et TéléIR pour la déclaration des revenus, regroupées aujourd'hui dans le portail fiscal www.impots.gouv.fr (12 millions de déclarations IR et 85% des impôts pour les professionnels)
- Le certificat avait alors deux fonctions :
  - d'une part permettre au serveur de l'administration d'authentifier le télédéclarant, comme si le déclarant présentait sa pièce d'identité avant d'accéder à son dossier fiscal ;
  - d'autre part permettre au déclarant de signer électroniquement sa déclaration, comme il le faisait auparavant avec une signature manuscrite.

Architecture PKI

- les infrastructures à clefs publiques nécessitent une approche organisationnelle très attentive à la formation des utilisateurs et à leur appropriation des mécanismes de protection de la confidentialité des échanges.
- Ce type d'infrastructure peut servir de base robuste à un déploiement de la signature électronique dans une organisation ou un réseau.
- Malheureusement, du fait de l'absence de normes, ce sont des solutions propriétaires, incomplètes et peu compatibles entre elles, ce qui limite leur adoption.

Quelques offres commerciales d'infrastructure à clef publique

Editeur	Offre
Baltimore Technologies	Unicert
Entrust Technologies	Entrust/PKI
Keynectis	PKI/offre initiale
TrustyCom	TrustyKey
Sagem	Xelios

Offre open source openPKI

Editeur	Offre
www.openssl.org	openssl

Agenda

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - ***C06 Renforcer la sécurité des réseaux et des systèmes***
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - ***Analyse de la vulnérabilité des réseaux et des systèmes.***
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions.*
    - *Procédures types pour un réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Sécurité des réseaux

- Dans la partie consacré aux risques, nous avons évoqué une typologie des principales attaques qui visent les systèmes d'information.
- Nombre de ces offensives utilisent le réseau comme support pour leurs attaques.
- Chaque jour, les pirates représentent une menace croissante.
- Avec les millions de stations connectées à l'Internet, ils ont un champ d'action quasi illimité.
- Par ailleurs ils utilisent le réseau pour partager les connaissances.
- Une simple requête avec un moteur de recherche sur les mots "*crack*", "*hack*" ou "*phreak*" fait référence des milliers de sites, dont beaucoup contiennent des programmes rédigés dans l'intention de nuire.

Importance de la sécurité des réseaux

- Comme tous les progrès technologiques, depuis l'aube de l'humanité, les réseaux informatiques ouverts en général et l'Internet en particulier représentent à la fois des opportunités et des menaces.
- Ce sont des opportunités pour s'ouvrir sur le monde, pour trouver l'information pertinente ou le partenaire attendu, pour présenter les produits et les services proposés par l'entreprise, pour acheter au meilleur prix.
- Ce sont aussi des menaces directement liées à l'ouverture.
- La progression des attaques est en croissance exponentielle et celles-ci sont de plus en plus virulentes.

Importance de la sécurité des réseaux

- Le nombre de machines infectées par le ver "*slammer*" en janvier 2003 doublait tous les 8,5 secondes pendant sa période de propagation.
- 200 000 serveurs ont été infectés et les activités de nombreuses sociétés ont été fortement perturbées.
- Nous avons vu avec *Conflicker* que ce sont peut-être 9 millions de machines qui ont été contaminées.
- La protection des réseaux est plus que jamais à l'ordre du jour

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des réseaux et des systèmes**
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - ***Modes d'attaque. Nouvelles menaces.***
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions.*
    - *Procédures types pour un réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Modes d'attaque

- Les "**sniffer de paquets**" sont des applications logicielles qui utilisent une carte réseau dans un mode de fonctionnement qui envoie tous les paquets reçus sur la ligne physique vers une application chargée de leur analyse.
- Comme certains protocoles de réseau envoient leurs données en clair, un "sniffer de paquets" peut y découvrir des informations comme des identifiants d'utilisateurs et des mots de passe.
- Les applications supportées par ces protocoles ne sont généralement pas critiques mais les pirates s'appuient sur le fait les utilisateurs n'ont généralement qu'un mot de passe pour tous leurs accès et que celui qui est ainsi capturé peut aussi servir pour accéder à des données beaucoup plus critiques.
- Cette approche des pirates est curieusement nommée "**ingénierie sociale**" car elle repose sur l'exploitation des faiblesses humaines.

Modes d'attaque

- L'attaque par **usurpation d'adresse Internet** ou ***spoofing*** consiste à imiter les conversations d'un ordinateur connu, crédité d'un bon capital de confiance.
- Le pirate cherche à se faire passer pour cet interlocuteur habituel en utilisant une adresse IP appartenant au réseau ou connue de lui en tant que correspondante régulière.
- Ce mode est souvent un point de départ pour d'autres types d'attaque.

Modes d’attaque

- Les attaques par déni de service sont les plus médiatisées et font partie des plus difficiles à contrer.
- Elles ne cherchent ni à obtenir un accès au réseau ni à récupérer les informations contenues sur les stations qui s'y rattachent.
- Elles ont pour seul objectif de rendre un service inaccessible en saturant une ressource et en paralysant le fonctionnement de l'infrastructure.
- En raison de leur facilité de mise en oeuvre et des dégâts potentiels importants qu'elles peuvent provoquer, ces attaques méritent une attention particulière.

Modes d'attaque

- Le réseau sert aussi de médium pour infecter les postes des utilisateurs finaux avec des virus et les attaques par cheval de Troie.
- Un virus est un logiciel conçu pour exécuter une fonction indésirable le poste de travail.
- Un cheval de Troie est conçu pour apparaître comme autre chose que ce qu'il est réellement.
- Il peut par exemple se présenter sous l'aspect d'un jeu.
- Il se transmet à tous les correspondants identifiés dans le carnet d'adresse de la victime.
- Lorsque ceux-ci reçoivent le jeu et le lancent, le phénomène se reproduit, entraînant ainsi une propagation exponentielle de la menace.
- La parade à ces attaques est le logiciel anti-virus.

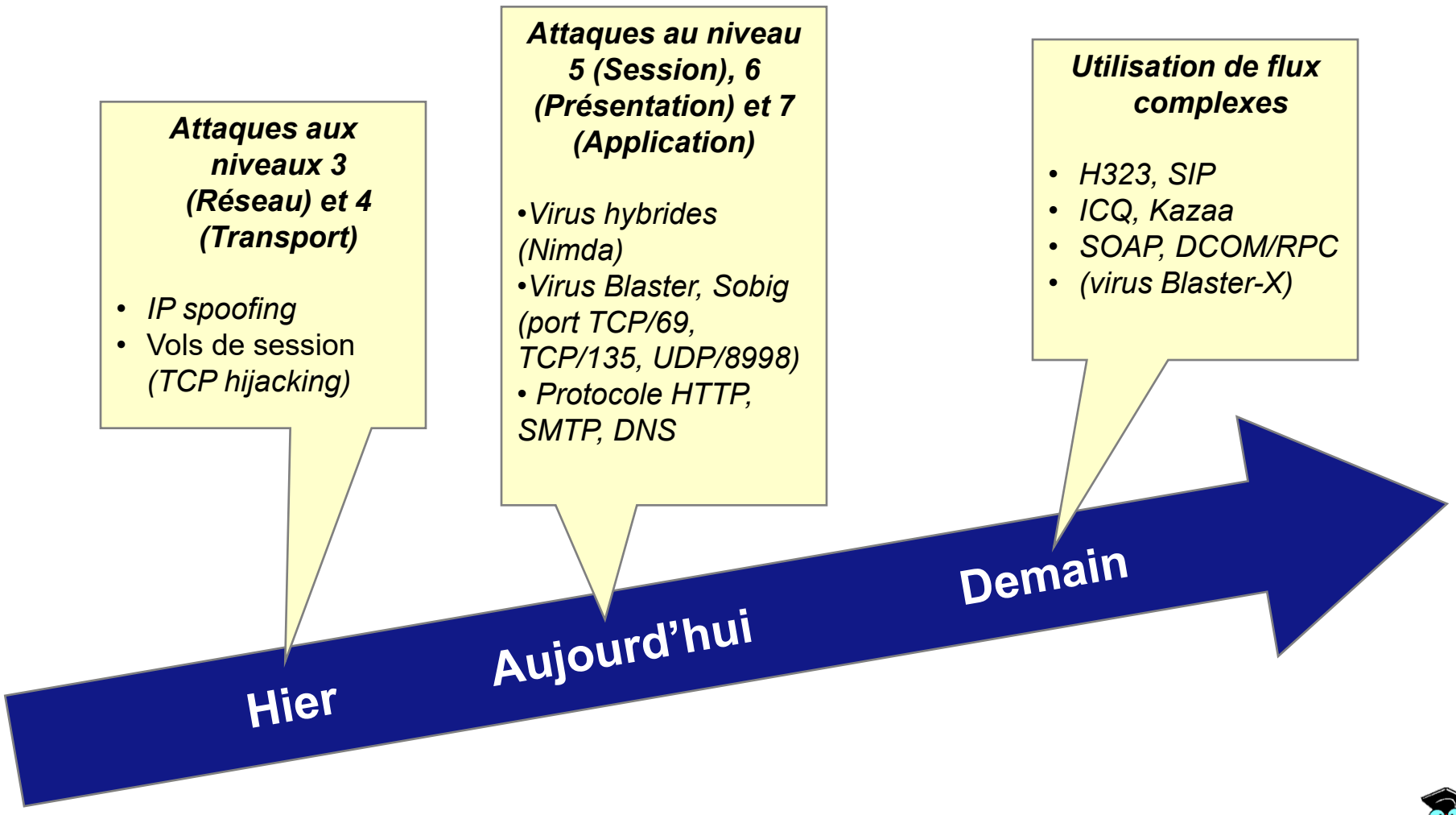
Modes d'attaque

- Cette liste n'est pas limitative.
- Les pirates sont des individus très imaginatifs et il existe d'autres types d'attaque qu'il serait trop long de décrire ici mais que nous retrouverons ultérieurement :
  - Attaques sur les mots de passe,
  - Attaques par le milieu (*Man in the middle*),
  - Attaques sur la couche applicative,
  - Reconnaissance du réseau,
  - Exploitation de la confiance par hameçonnage (*phishing*)
  - Redirection des ports, etc.

Nouvelles menaces

- Aux menaces « traditionnelles » qui se situent au niveau des couches réseau / transport du modèle OSI (vol de session, usurpation d'adresse, déni de service…) viennent s'ajouter d'autres menaces :
  - Celles qui sont liées aux vulnérabilités des très nombreux logiciels de communication (Navigateur Internet, Serveur Web, Serveur DNS, etc.…) qui utilisent des protocoles dits applicatifs au dessus du couple des protocoles réseau/transport pour communiquer. Par exemple :
    - le protocole HTTP permettant de faire communiquer le navigateur Internet avec le serveur Web,
    - le protocole SMTP permettant aux serveurs de messagerie de s'échanger les mails;
  - Celles liées aux contenus qu'il s'agisse des nouveaux virus, vers informatique ou chevaux de Troie.

Nouvelles menaces



Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - ***Face à ces menaces, le sécurité périmétrique multi-niveaux.***
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions.*
    - *Procédures types pour un réseau réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

La sécurité périmétrique multi-niveaux

- Face à cette menace que l'on peut qualifier de « multi-niveaux » en se référant aux différentes couches d'un réseau de communication il est indispensable de mettre en place une **protection « multi-niveaux »** :
  - Protection contre les attaques de niveau réseau/transport (pour simplifier, ce que nous appellerons « niveau réseau » dans ce document regroupe les équivalents des couches OSI/3 – réseau – et OSI/4 – transport -)
  - Protection contre les attaques qui touchent les protocoles applicatifs (« attaques applicatives »)
  - Protection contre les attaques de contenu

La sécurité périmétrique multi-niveaux

- Assurer la **disponibilité des flux de données** implique de disposer de capacités d'émission, de réception et de transfert. La disponibilité repose généralement sur une redondance des équipements, sur la mise en œuvre de fonctions de sauvegarde et de reprise.
- Assurer **l'intégrité des flux de données** implique de s'assurer que les données reçues sont bien celles qui ont été transmises. Le contrôle peut être réalisé pendant l'échange, par la mise en œuvre de mécanismes prévus dans certains protocoles de transfert.
- Il convient aussi de s'assurer de **l'intégrité des données reçues, stockées et utilisées**. Des mécanismes de condensat (*hash coding*) sont alors nécessaires. Ils permettent de mémoriser un état donné et de vérifier que l'état actuel est toujours identique à l'état enregistré lors de la réception.
- Assurer la **confidentialité des flux de données** implique de protéger les échanges d'information dont le détournement par des tiers porterait préjudice.

La sécurité périmétrique multi-niveaux

- Le **premier niveau** consiste à installer des pare-feux aux frontières du réseau interne (intranet) avec les réseaux externes voisins (l'Internet, les extranets construits avec les partenaires). Au même niveau interviennent les sondes de détection d'intrusion qui sont permettent d'écouter un réseau en vue de détecter des tentatives d'intrusions. Les serveurs proxys peuvent aussi participer à cette construction.
- Un **second niveau** repose sur l'utilisation de réseaux privés virtuels (RPV/VPN) qui offrent des solutions de cloisonnement grâce à l'utilisation de protocoles comme IPSec.
- Le **troisième niveau** est celui du chiffrement des données.

La sécurité périmétrique multi-niveaux

- La **protection de la confidentialité** implique la détermination des droits et privilèges qui elle-même passe par un mécanisme d'identification et d'authentification des systèmes ou des individus placés aux extrémités de la ligne de communication.
- Le mécanisme peut être simple (identifiant et mot de passe) ou fort (par exemple idem + jeton – cf plus loin).
- Un enjeu lié à l'authentification est celui de son unicité.
- L'utilisateur rejettera les règles de la politique de sécurité si elle le contraint en plus à mémoriser autant de procédures, de numéros de compte et de mots de passe qu'il y a d'applications.
- Une solution d'authentification unique (***SSO*** pour **Single Sign-On**) est indispensable.

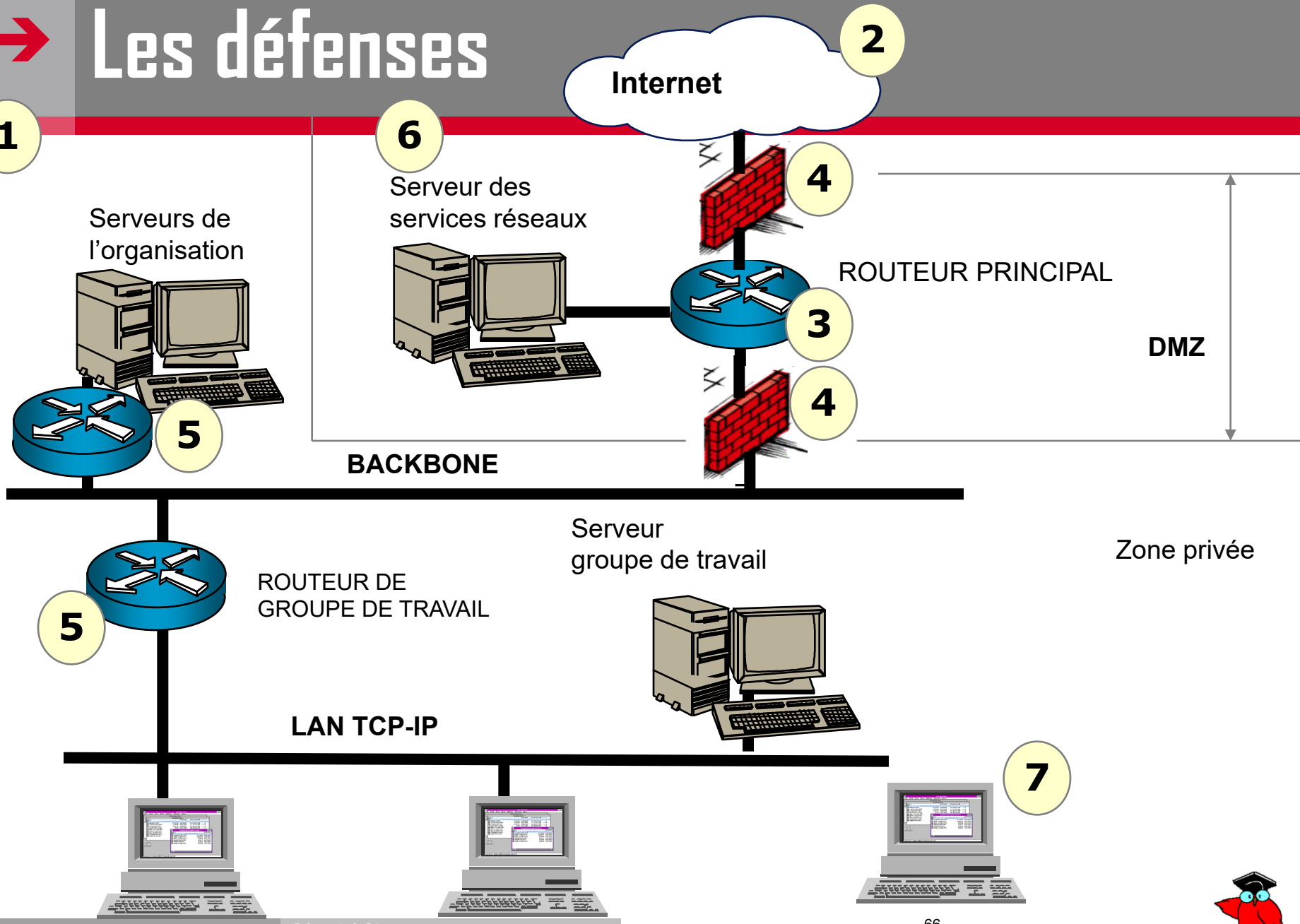
La sécurité périmétrique multi-niveaux

- **Garantir la preuve** implique ne pouvoir nier avoir émis ou reçu un flux effectivement transmis.
- Cette garantie repose sur des journaux, des accusés de réception, des mécanismes d'authentification et de signature (données chiffrées ajoutées à une information numérique pour authentifier son auteur) ainsi que sur des mécanismes d'horodatage (association d'un événement et d'une information sur l'instant de cet évènement).
- Elle introduit aussi la notion de **tiers de confiance**, version numérique du notaire qui enregistre et authentifie les actes.

La sécurité périmétrique multi-niveaux

- La protection du réseau apparaît donc comme une composante essentielle de la stratégie de sécurité du système d'information.
- A chacun de ces objectifs, face aux menaces recensées, sont associées diverses solutions techniques.
- Nous allons décrire quelques-unes de ces solutions, mais il ne faut pas oublier l'aspect humain (sensibilisation, information, formation, accompagnement) propre à toute politique de sécurité que nous avons évoqué dans la première partie

Les défenses



Les défenses

1. Arriver à une architecture qui prenne en compte la sécurité :
   - En construisant plusieurs réseaux physiques (différents câbles) et logiques (différents numéros IP)
   - En installant des routeurs avec des filtres, un serveur dédié réseau et éventuellement un garde-barrière (filtre) applicatif
2. Rendre inaccessibles depuis l'Internet (routage IP) certains réseaux internes :
   - Annoncer sur l'Internet uniquement les réseaux qui doivent communiquer avec l'extérieur
   - Et pas systématiquement l'ensemble des réseaux internes

Les défenses

3 Installer des filtres sur le routeur d'entrée de site

4 Installer des pares-feux (firewall) pour délimiter la zone publique (DMZ) et la zone privée

5 Interdire certains trafics venant des différents réseaux (gestion, ...), entre eux et avec l'Internet

- En ne mettant pas systématiquement une route par défaut
- En installant des filtres dans les routeurs

6 Installer dans la DMZ une machine dédiée pour les services réseaux avec de bons outils serveur de messagerie, serveur HTTP, serveur FTP, serveur DNS, proxy, . . .

7 Si une machine est vraiment sensible :

- La déconnecter du réseau physiquement ou
- Logiquement en ne configurant pas le coupleur (pas de commande "ipconfig")

Les pare-feux

- Les **pare-feux** (de l'anglais **firewall**) sont des dispositifs –logiciels le plus souvent- qui permettent de limiter, de filtrer, de séparer et d'analyser les entrées/sorties d'un réseau.
- Ils ont pour objectif de bloquer l'entrée sur un réseau interne lors d' une tentative d'attaque ou d'intrusion.
- La fonction première d'un pare-feu est de faire appliquer les règles d'état de connexion et de réaliser un filtrage détaillé des sessions qui sont appelées à travers lui.
- Il utilise des filtres qui contrôlent les données qui transitent et peuvent agir au niveau de l'identité de l'émetteur ou du protocole concerné.

Les pare-feux

- Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocole	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

- Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web).
- La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue qui peut être celle du privilège minimum).
- Le port 23 est par exemple souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance.

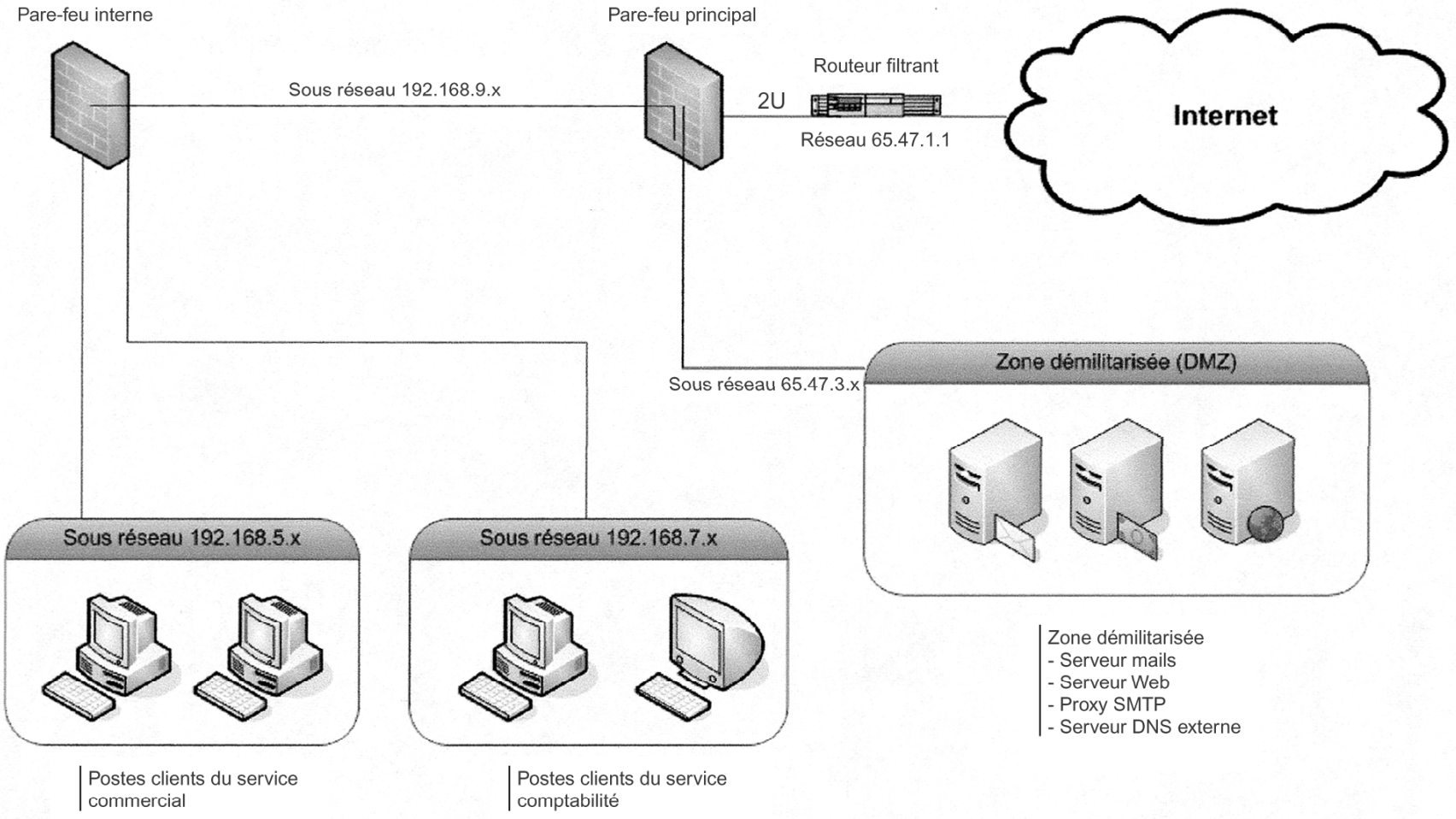
Les pare-feux

- Illustrons par un exemple le fonctionnement d'un pare-feu.
  - Dans un petit réseau Poste à Poste (P2P) qui utilise un partage de connexion Internet, configuration courante dans les TPE, le pare-feu est activé sur le poste passerelle qui est connecté à l'Internet (via ADSL ou RNIS).
  - Lorsqu'un utilisateur du réseau envoie une requête vers un serveur web, celle-ci transite par la passerelle, donc par le pare-feu qui en garde trace en enregistrant 4 valeurs : l'adresse IP du demandeur, le port d'où provient la requête, l'adresse IP et le port de destination.
  - Les données entrantes sont identifiées de la même manière.
  - Si les caractéristiques de la donnée entrante ne correspondent pas à celles d'une réponse attendue à une requête dont le pare-feu a gardé la trace, elle est bloquée.
  - Le pare-feu peut enregistrer dans un journal toutes les entrées non sollicitées.
  - Si le petit réseau considéré contient une machine qui doit pouvoir jouer le rôle d'un serveur FTP ouvert au public, il faut que l'administrateur paramètre l'inhibition du blocage pour cette machine et ce protocole (adresse IP et No de port)

Les pare-feux

- L'action d'un pare-feu se définit donc sur différents points :
  - Restriction des accès sur une entrée précise ;
  - Restriction des sorties afin de limiter les émissions de données ;
  - Arrêt des agressions destinées à affaiblir les défenses.
- Un pare-feu est indispensable mais il ne constitue pas une protection sans faille.
- Lorsqu'un cambrioleur fracture une porte blindée, il a tout loisir de visiter tranquillement le local si le propriétaire n'a pas prévu d'autres dispositifs de protection.
- Il en est de même pour les pare-feux qui deviennent plus perméables du fait de l'évolution des protocoles réseaux qui visent plus de souplesse mais de ce fait offrent plus facilement une porte d'accès aux trafics malveillants.

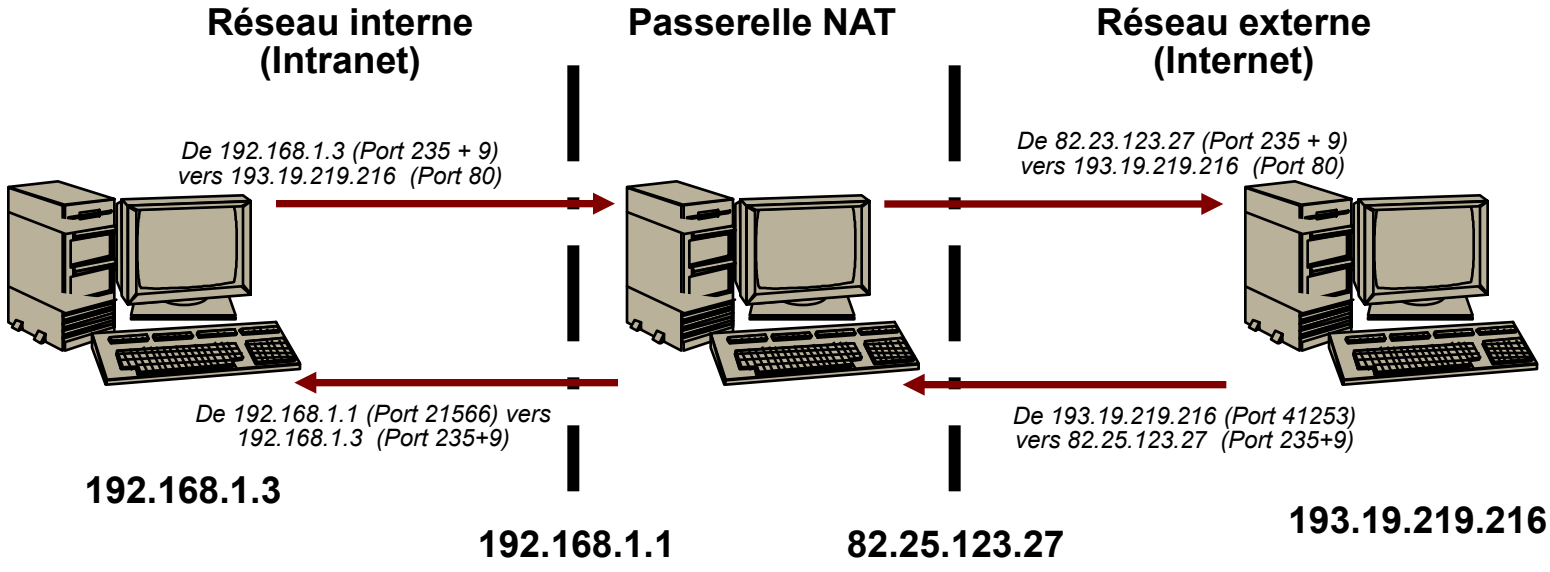
Les pare-feux



***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

Les pare-feux

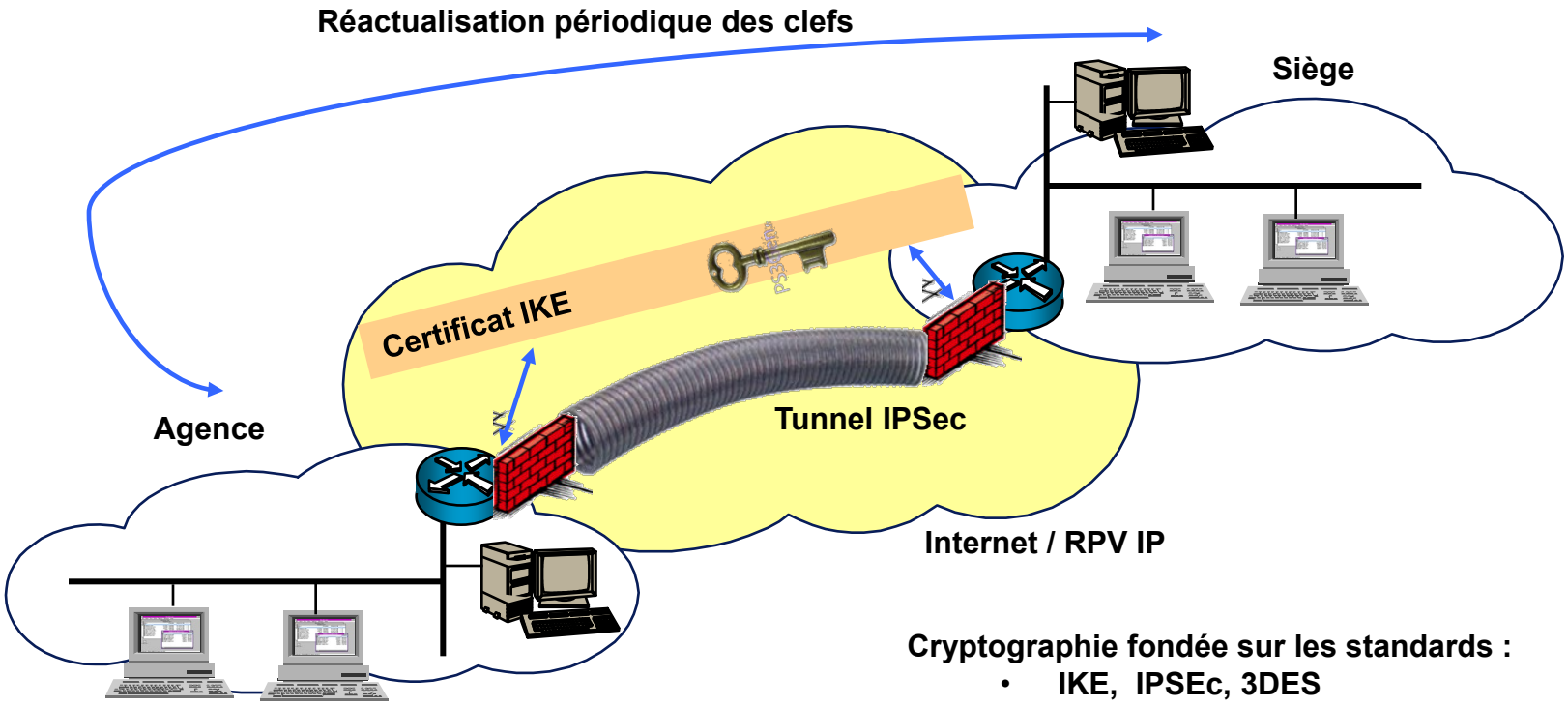
- Les pare-feux assurent souvent un type de protection par translation d'adresse (*Network Address Translation*).
- Le principe est de masquer les adresses internes du réseau vis-à-vis de l'extérieur.
- Le diagramme suivant explique le fonctionnement de la translation d'adresses :



RPV et IPSec

- Les réseaux privés virtuels (**RPV**) et le protocole ***IPSec***, qui assure à la fois confidentialité, authentification et intégrité, fournissent un niveau de sécurité suffisant pour la plupart des transferts et des entreprises.
- Le RPV associe des algorithmes de cryptage à une technologie baptisée « *tunneling* » de manière à établir une connexion sécurisée entre deux sites.
- Une fois les deux interlocuteurs identifiés, il faut créer un « tunnel », ce qui consiste à créer un chemin logique entre les deux points à relier au sein du réseau.
- Les services *IPSec* s'appuient sur les modules *Authentification Header* pour garantir l'authenticité des trames IP, *Encapsulation Security Payload* pour la confidentialité des données en cryptant une trame source et *Internet Key Exchange* pour la gestion des protocoles de chiffrements retenus et le partage de la clef de chiffrement entre émetteur et destinataire.

Mécanismes de sécurité des RPV



Cryptographie fondée sur les standards :

- **IKE, IPSEc, 3DES**
- **Interopérabilité des équipements**

MZ et DMZ

- Une architecture de sécurité à base de pare-feux conduit à dissocier les notions de **zone militarisée** et de **zone démilitarisée** (***MZ*** et ***DMZ***).
  - La *DMZ* est une zone tampon, sorte de no man's land construit autour des systèmes clefs du système d'information.
  - Ceux-ci, par opposition, forment la *MZ*.
- Les zones sont séparées les unes des autres par des systèmes de pare-feux.
- La *DMZ* va contenir les serveurs qui communiquent avec les zones de niveau de confiance inférieur, par exemple Internet.
- Aucune donnée et aucun applicatif sensible ne sont stockés ou exécutés dans cette zone.

Sécurisation des serveurs

- Le contrôle d'accès système doit être le point de contention central du système d'information.
- L'idée générale est de mutualiser un maximum de fonctionnalités en un point unique qui va constituer le point de passage obligé entre les différentes zones du système d'information, y compris l'extérieur.
- Le NAC (cf. chapitre suivant) répond à cet objectif.
- Sécuriser implique aussi de pérenniser pour assurer disponibilité et intégrité.
- La technique des « disques miroir », où l'information est écrite deux fois, augmente la sécurité, mais aussi le prix.
- La recherche de la sécurité à moindre coût a conduit à la technologie RAID (*Redundant Array of Independant Disks*).
- Il s'agit de répartir l'information sur un réseau de petits disques plutôt que sur une grosse unité, pour assurer une fiabilité complète et pour accélérer le processus en répartissant le travail entre plusieurs canaux et plusieurs têtes de lecture.

Proxys

- Un **serveur Proxy** (mandataire) est un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges.
- Le proxy peut protéger : il permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur. Si personne à l'extérieur ne peut voir ces machines internes, l'attaque est beaucoup plus difficile, car l'attaquant est aveugle. N'oublions cependant pas que 80% des attaques proviennent de l'intérieur du réseau et non de l'extérieur.
- Le proxy peut masquer les informations concernant un ordinateur: En effet, quand l'utilisateur de celui-ci surfe, tous les sites Web peuvent savoir de quel site il vient, quel navigateur il utilise, quel est son système d'exploitation, son adresse IP... Certains proxys masquent ces informations. Ces proxys sont dits proxy anonymes.
- Le proxy peut mémoriser les pages les plus demandées. C'est un proxy-cache.

Procédures

- Outre ces dispositifs techniques, la sécurité implique de disposer de procédures clairement établies :
  - Validation et contrôle du modèle de sécurité
  - Désactivation des services superflus
  - Administration des comptes utilisateurs
  - Administration des droits d'accès
  - Journalisation
  - Sauvegardes
  - Vérification d'intégrité de fichiers
  - Plan pour la continuité de l'exploitation (dans le cadre du PCA vu dans la première partie)
  - Procédures de reprise après panne
  - Formation et sensibilisation des utilisateurs

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - ***Concept de Network Access Control.***
    - *Détection (IDS) et prévention (IPS) des intrusions.*
    - *Procédures types pour un réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Network Access Control

- Un Contrôleur d'accès au réseau (***Network Access Control*** ou ***NAC***) est une solution informatique permettant de soumettre l'accès à un réseau d'entreprise à un protocole d'identification de l'utilisateur et au respect par la machine de cet utilisateur des restrictions d'usage définies pour ce réseau.

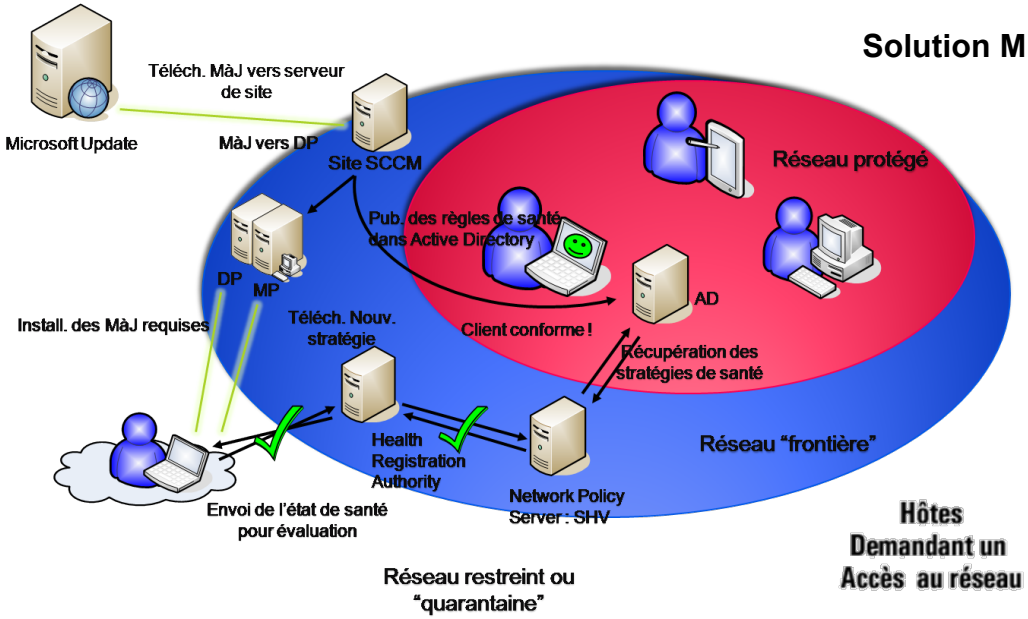
- Plusieurs sociétés comme *Cisco Systems*, *Microsoft* , *Juniper Networks, Symantec*, ont développé des solutions *(frameworks)* permettant d'implémenter des mécanismes de protection d'accès au réseau d'entreprise et de vérifier le respect par les postes clients, des règles de sécurité imposées par l'entreprise : état de la protection antivirus, mises à jour de sécurité, présence d'un certificat, et bien d'autres.

- Ces *frameworks* ont donné naissance à bon nombre d'"*appliances*", matériels spécialisés dans le contrôle d'accès au réseau.

Network Access Control

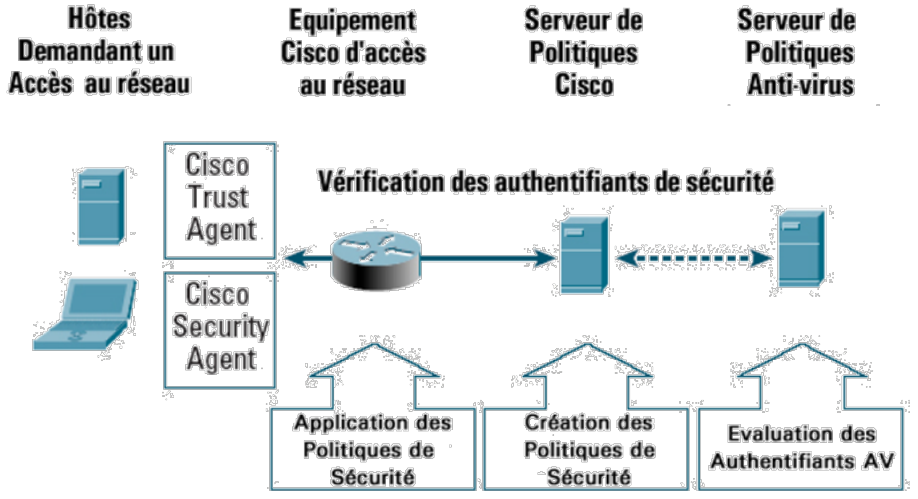
- Par exemple *Cisco* utilise ses pare-feux PIX, ses *appliances* ASA, ses routeurs et ses commutateurs pour constituer son NAC.
- *NAP (Network Access Protection)* est la solution *NAC* de *Microsoft*.
- Les solutions NAC :
  - Déterminent le niveau de sécurité du réseau.
  - Ouvrent l'accès aux différentes parties du réseau, en fonction des résultats de la première étape.
  - Remédient aux défauts de conformité et diffusent les composants de la politique de sécurité jusqu'aux points terminaux.
- Par exemple, si la politique dit de refuser l'accès aux points terminaux dont le niveau de téléchargement des mises à jour est supérieur à 30 jours, alors le NAC restreint l'accès de ces clients non conformes à la politique et, éventuellement, entame un processus d'assainissement en téléchargeant et en installant les correctifs requis.
- Les trois mots-clefs dans le processus du NAC sont les suivantes: Identifier, évaluer et assainir.

NACs Cisco et Microsoft



Réseau restreint ou "quarantaine"

Solution Microsoft (via System Center)



Cisco NAC

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - ***Détection (IDS) et prévention (IPS) des intrusions. Scan des vulnérabilités et déploiement des pare-feux.***
    - *Procédures types pour un réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Face à ces menaces, le sécurité périmétrique multi-niveaux

Détection (IDS) des intrusions

- On appelle *IDS* (*Intrusion Detection System*) un mécanisme écoutant le trafic réseau de manière furtive en vue de repérer des activités suspectes et permettant ainsi de lancer une action de prévention sur les risques d'intrusion.
- Il existe deux grandes familles distinctes d'IDS :
  - Les *N-IDS* (*Network Based Intrusion Detection System*), ils assurent la sécurité au niveau du réseau.
  - Les *H-IDS* (*Host Based Intrusion Detection System*), ils assurent la sécurité au niveau des hôtes.
- Un *N-IDS* nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur le réseau.
- Il est courant de trouver plusieurs *IDS* sur les différents segments du réseau :
  - On place une sonde à l'extérieur du réseau afin d'étudier les tentatives d'attaques
  - On place une sonde en interne pour analyser les requêtes ayant traversé le pare-feu ou bien menée depuis l'intérieur.

Détection (IDS) des intrusions

- Le trafic d'un réseau IP est constitué de datagrammes IP.
- Un *N-IDS* est capable de capturer les paquets lorsqu'ils circulent sur les liaisons physiques sur lesquelles il est connecté.
- Un *N-IDS* consiste en une pile TCP/IP qui réassemble les datagrammes IP et les connexions TCP.
- Il peut appliquer les techniques suivantes pour reconnaître les intrusions :
  - Vérification de la pile protocolaire : Une simple vérification protocolaire peut mettre en évidence les paquets invalides qui traduisent souvent une intention de nuire.
  - Vérification des protocoles applicatifs : nombre d'intrusions utilisent des comportements protocolaires invalides, comme par exemple "WinNuke", qui utilise des données NetBIOS invalides

Prévention (IPS) des intrusions

- On parle de plus en plus d'*IPS* (*Intrusion Prevention System*) en remplacement des *IDS*.
- L'*IPS* est un Système de Prévention/Protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions comme la plupart des IDS le sont.
- La principale différence entre un *IDS* (réseau) et un *IPS* (réseau) tient principalement en 2 caractéristiques :
  - le positionnement en coupure sur le réseau de l'*IPS* et non plus seulement en écoute sur le réseau pour l'*IDS* (traditionnellement positionné comme un sniffer sur le réseau).
  - la possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que l'*IPS* est constitué en natif d'une technique de filtrage de paquets et de moyens de bloquages (*drop connection, drop offending packets, block intruder*, …).

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des réseaux et des systèmes**
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions. Scan des vulnérabilités et déploiement des pare-feux.*
    - ***Procédures types pour un réseau Win2K.***
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Procédures types pour un réseau type Windows 200x

- **Règle No 1 :** Utiliser de préférence le système de fichiers *NTFS*. Il fournit des dispositifs de sécurité (mise en place de droits et de permissions selon les utilisateurs) alors que l'autre système (FAT) n'en n'offre pas.
- **Règle No 2 :** Dans l'hypothèse la plus courante d'un réseau TCP/IP, invalider *Netbios* pour ne plus utiliser d'applications relatives à ce protocole.
- **Règle No 3 :** Bloquer tous les ports non essentiels au protocole TCP/IP en entrée et en sortie. En particulier, les entrées et sorties UDP à ports 137, 138, et le port 139 de TCP. Ceci peut empêcher plusieurs types d'attaques.
- **Règle No 4 :** Le compte administrateur ayant les droits les plus élevés, c'est lui qui est systématiquement visé par les attaques. Diminuer les droits associés à ce compte et cacher le véritable

Procédures types pour un réseau type Windows 200x

- **Règle No 5 :** S'assurer que tous les dispositifs de sécurité ont été activés au plus haut niveau. Les utilisateurs doivent respecter des règles et définir des mots de passe de plus de 8 caractères.
- **Règle No 6 :** Examiner périodiquement les systèmes pour s'assurer de la fiabilité des comptes utilisateurs. Effacer ou invalider les comptes inutilisés. Utiliser des comptes provisoires pour être sûr de fixer une date d'échéance pour chaque compte.
- **Règle No 7 :** Définir les droits d'accès des utilisateurs selon un plan et des normes précises et configurer le système de sorte qu'il audite régulièrement les utilisateurs.

Procédures types pour un réseau type Windows 200x

- **Règle No 8** : Le compte d'invité est créé par défaut à chaque installation du système. Si le choix est fait de le conserver, vérifier régulièrement le nombre d'invités et contrôler les droits attribués (en cas de changement par un tiers indésirable). La meilleure solution consiste à désactiver ce compte et à créer soigneusement des comptes temporaires types.
- **Règle No 9 :** S'assurer que les utilisateurs ne laissent pas leurs postes de travail allumés et sans surveillance. Edicter que les économiseurs d'écran doivent être verrouillés en cas d'absence momentanée. Les utilisateurs doivent fermer leur session quand ils ne reviennent pas sur leur poste de travail.

Procédures types pour un réseau type Windows 200x

- **Règle No 10 :** Préférer, pour les tâches simples et basiques, l'utilisation de scripts développés maison à l'installation d'outils sur les serveurs. On est au moins sûr de ce que l'on a créé. La fiabilité est inversement proportionnelle au nombre d'outils installés. Mais ne pas omettre d'installer certains outils incontournables qui vont faciliter le diagnostic et la maintenance du système. Un réseau sécurisé n'est pas seulement un réseau bien configuré, mais aussi un réseau bien entretenu.
- **Règle No 11 :** Eliminer les services inutiles. Il est fréquent de laisser des services inutiles sur un serveur alors que c'est souvent par le biais d'un service inactif que les attaques se faufilent.

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions. Scan des vulnérabilités et déploiement des pare-feux.*
    - *Procédures types pour un réseau réseau Win2K.*
    - ***Evolution. Exemple des architectures Cisco : de SAFE à SecureX.***
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - *Serveurs et réseaux de haute disponibilité.*

Renforcer la sécurité des réseaux et des systèmes

Sécurité : Qui utilise quoi ?

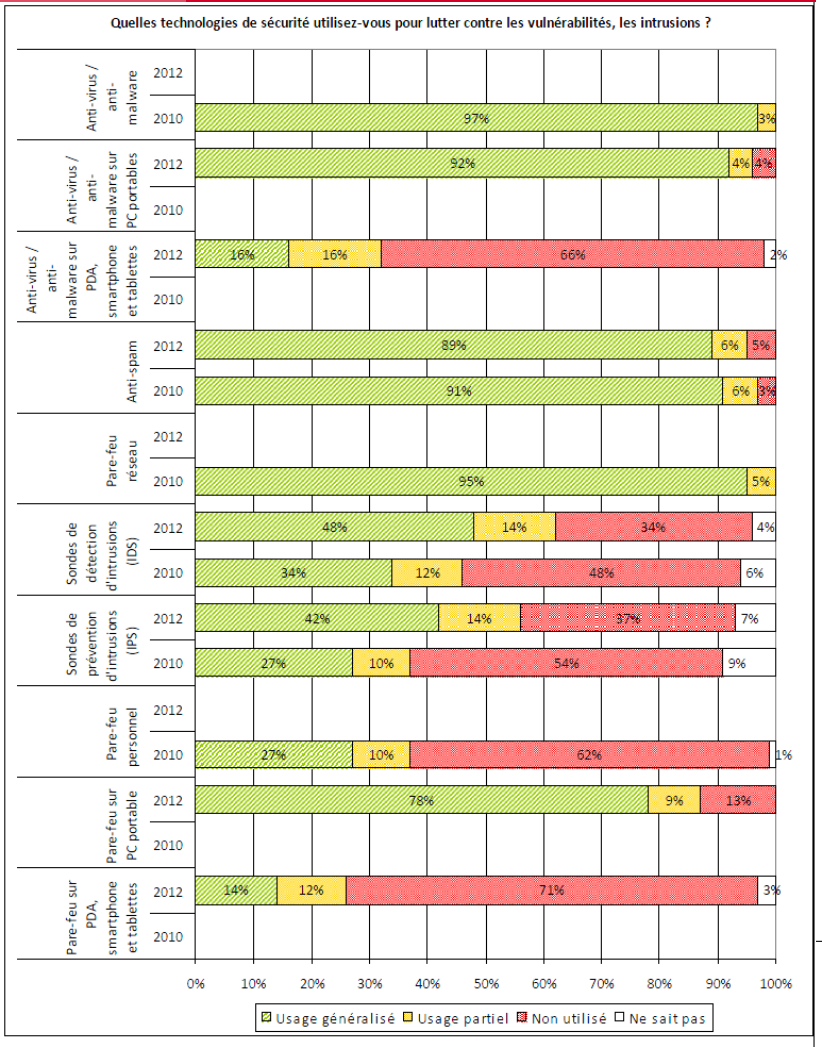


Figure 20 - Technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités (1/2)

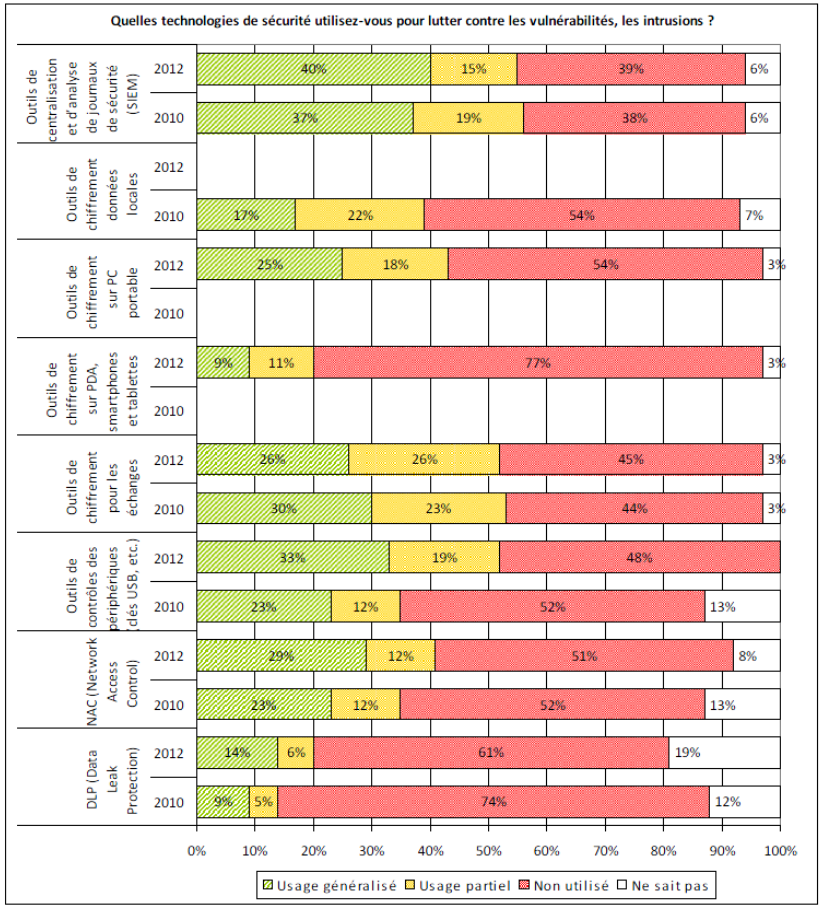


Figure 21 - Technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités (2/2)

Source : Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Evolution

- En matière de défense des réseaux, l'évolution est guidée par trois facteurs :
  - Le souci de réduire la vulnérabilité des réseaux actuels,
  - La réponse réactive à l'apparition de nouvelles menaces,
  - La prise en compte de nouvelles technologies réseaux;
- En ce qui concerne le premier point, l'évolution va vers plus d'intelligence dédiée à la sécurité dans les équipements, en particulier dans les routeurs et les pare-feux ;
- Les routeurs ne jouent pas nominalement un rôle dans la sécurité, mais ils sont vulnérables et peuvent, à leur insu, devenir les meilleurs amis des pirates.

Evolution

- Il faut les protéger plus efficacement pour réduire la probabilité que leur sécurité puisse être directement compromise en mettant en œuvre des fonctionnalités souvent sous-exploitées :
  - Verrouillage de l'accès *Telnet* ;
  - Verrouillage de l'accès *SNMP* (*Simple Network Management Protocol*) ;
  - Contrôle de l'accès grâce à l'utilisation de certaines procédures;
  - Désactivation des services inutiles;
  - Ouverture de sessions avec des droits appropriés;
  - Authentification des updates de routage.
- Des pare-feux intelligents, jouant le rôle de point de raccordement des tunnels IPSec des RPV de site à site, en combinaison avec des solutions d'intégration de type EAI voire des architectures PKI peuvent conduire à des architectures plus sécurisées, mais il est vrai plus complexes à gérer.

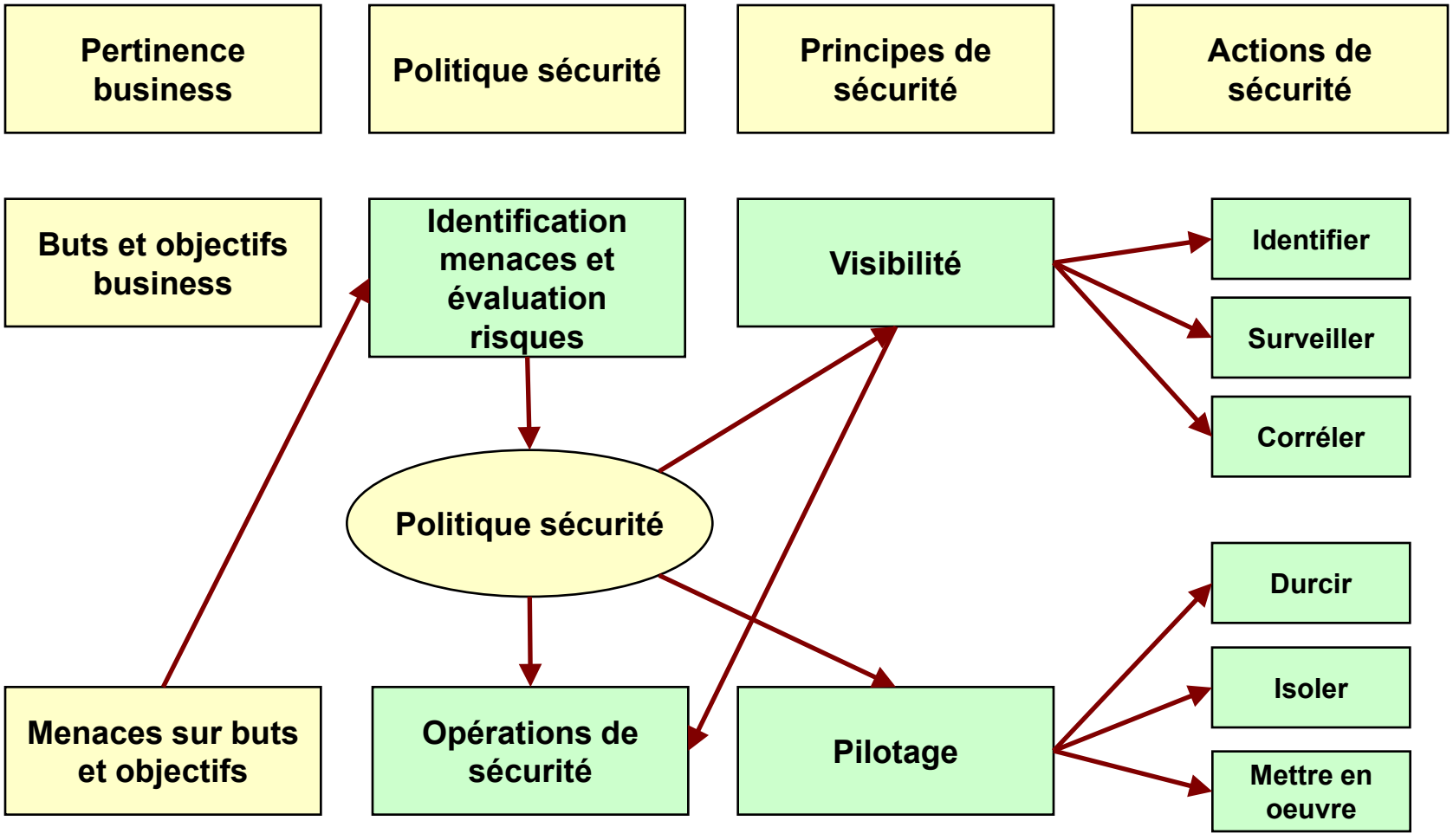
Evolution

- Dans le contexte de l'évolution des technologies réseaux, du fait de la prépondérance du protocole IP, le fait le plus marquant est la passage d'IPV4 à IPV6.
- Alors que la sécurité est optionnelle dans IPv4, elle est prévue de façon native dans IPv6.
- En effet, les systèmes de sécurité d'IPv4 sont essentiellement des couches supplémentaires rapportées sur protocole de base comme *Application Layer Security* (*PGP, Web of Trust*) ou *Transport Layer Security* (*SSH/SSL*).
- Sur IPv6, le souci de sécurisation est intégré dans le protocole qui autorise, grâce à son immense espace d'adressage, des adresses globales.
- Celles-ci permettent d'éviter le transit des informations par des niveaux intermédiaires qui présentent des failles : les transmissions de données sont sécurisées de bout en bout sans avoir nécessairement recours à des couches supplémentaires.

Cisco Safe

- Les constructeurs et les intégrateurs proposent la mise en place d'architecture globale de sécurité atténuant les risques face à une menace nouvelle et favorisant la réactivité pour construire rapidement une défense.
- Ces architectures globales proposent (exemple de l'architecture *SAFE* de *Cisco*) :
  - Sécurité et atténuation des attaques basées sur une politique,
  - Mise en œuvre de la sécurité sur l'ensemble de l'infrastructure (et pas seulement sur des périphériques de sécurité spécialisés),
  - Déploiement rentable,
  - Gestion et *reporting* sécurisés,
  - Accès des utilisateurs et des administrateurs aux ressources critiques du réseau soumis à authentification et à autorisation,
  - Détection des intrusions pour les ressources critiques et les sous-réseaux.

Cisco Safe



Source Cisco

Cisco SecureX

- L'Architecture NG *SecureX* de *Cisco* met en œuvre des politiques de sécurité fondées sur la connaissance du contexte d'accès au réseau.
- Avec ses fonctions de sécurité intégrées sensibles au contexte, cette architecture a pour ambition de :
  - Faire respecter les règles de sécurité basées sur une politique qui prend en compte le contexte global - qui, quoi, où, quand et comment on accède au réseau.
  - Fournir un accès hautement sécurisé à l'environnement virtuel, physique, sur site et *cloud* pour garantir l'application cohérente des règles de sécurité.
  - Simplifier les règles de sécurité pour faire coïncider les besoins IT et les pratiques de l'entreprise.
  - Offrir une protection dès l'apparition d'une menace et ce, grâce à l'ensemble (réseau surveillance + BdD + experts + dispositif de d mise à jour) *Cisco Security Operation Intelligence* (*SIO*) qui permet corrélation et protection en temps réel.
  - Prendre en charge tout type de terminaux, des ordinateurs portables aux appareils mobiles de nouvelle génération tels que le *Cius* de *Cisco*, les *iPads*, les *iPhones* et les autres smartphones.

Plan

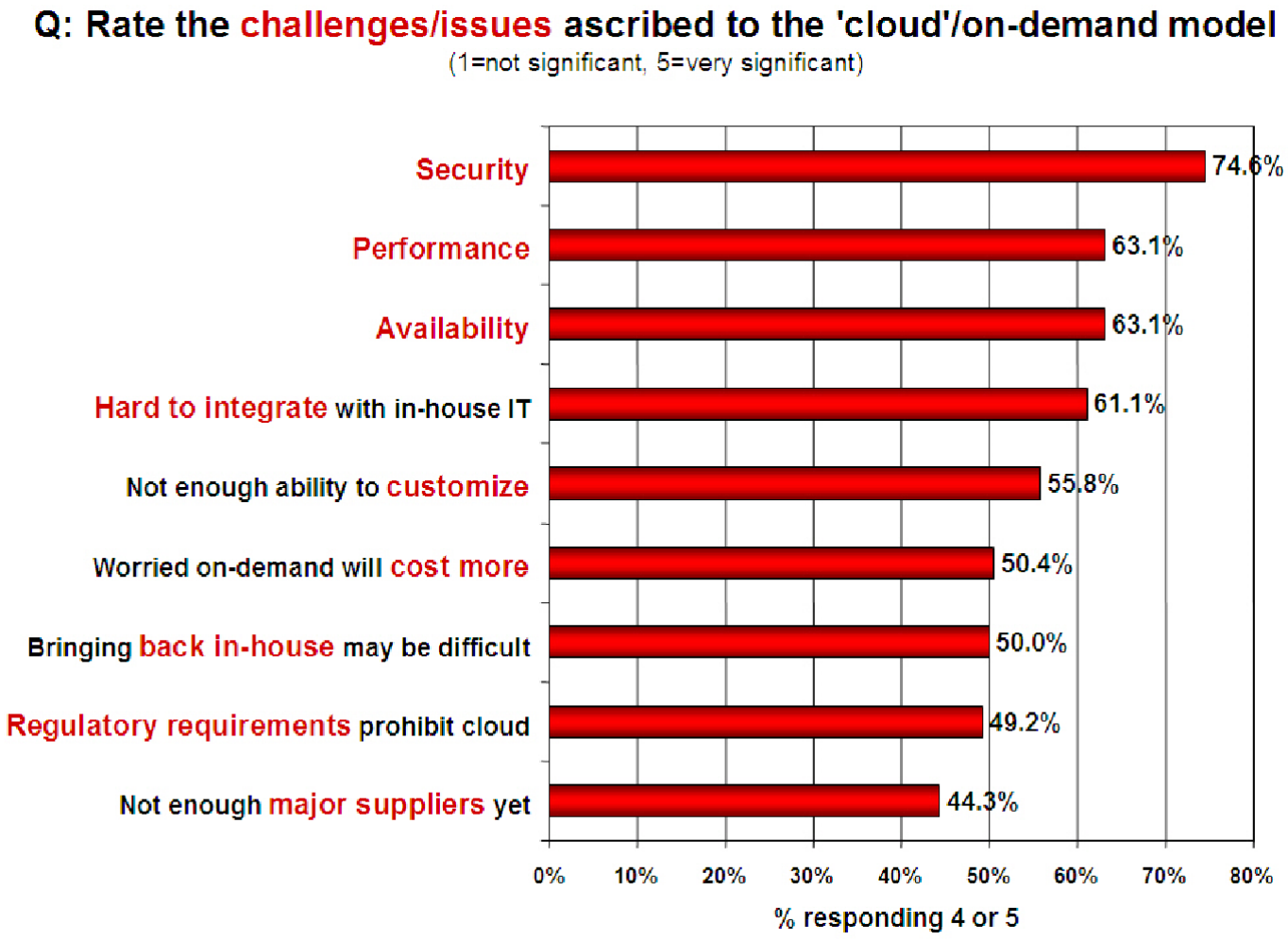
- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions. Scan des vulnérabilités et déploiement des pare-feux.*
    - *Procédures types pour un réseau réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - ***Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides***
    - *Serveurs et réseaux de haute disponibilité.*

Cloud and security

«[Cloud Computing] is a security nightmare and it can't be handled in traditional ways.»

John Chambers, CISCO CEO

Nouvelle problématique de sécurité avec le cloud



Source: IDC Enterprise Panel, August 2008 n=244

Nouvelle problématique de sécurité avec le cloud

- Jusqu'à aujourd'hui, chacun était maître de sa sécurité (et le reste s'il peut échapper au *cloud*).
- Avec les tablettes et les smartphones est venu l'avènement d'une nouvelle ère, le post-PC, où un ordinateur classique et unique n'est plus le centre de l'activité numérique de chacun et où une grande partie des données va se trouver déportée pour pouvoir être accessible en tous lieux, en tout instant, par le terminal qui sera le plus pertinent en ce lieu, en cet instant.
- Avec le *cloud*, avec les solutions *d'Amazon*, d'*Apple*, de *Google*, d'*IBM*, de *Microsoft*, de *Salesforce* ou de *SAP*, la donnée est dans le nuage; or tous les pilotes savent qu'il est plus difficile de piloter dans un nuage (*IFR*) que par un ciel clair (*VFR*).
- Cette évolution pose un changement de paradigme : on peut se retrouver brutalement dépossédé des données dont croyait légitimentn le propriétaire (Affaire *Megaupload* et réponse de la justice à la requête de Kyle Goodwin, soutenu par l'*Electronic Frontier Foundation* (EFF) .
- Dès lors la problématique de sécurité est double.
- Il faut d'abord s'assurer que les serveurs dans le *cloud* soient sécurisés, chiffrés, et qu'en cas de fuite de données, les utilisateurs soient avertis. Une problématique classique censée être résolue par les SLA.
- La deuxième problématique est d'ordre juridique : A qui appartient véritablement une donnée ?

Nouvelle problématique de sécurité avec le cloud

- Au plan technique, le Cloud pose deux difficultés majeures.
  - D'une part, en permettant des déploiements d'applications sur différents réseaux privés, publics ou sur une combinaison des deux, il provoque une banalisation des accès qui doit s'accompagner d'une authentification (gestion d'identité) renforcée.
    De plus, ce type d'architecture implique par nature que l'on ne sait plus réellement où sont les applications et où sont stockées les données confidentielles.
  - D'autre part, avec la virtualisation et l'externalisation des serveurs et des équipements de stockage, les systèmes informatiques ne sont plus cloisonnés comme autrefois.
    Sur le LAN cloisonné, les applications étaient protégées grâce aux firewalls et IPS.
    Avec le Cloud, le LAN explose, ressources et applications se dispersent, et ne sont plus protégées directement.
    Les entreprises vont avoir de plus en plus de mal à localiser les équipements et applications, et ne pourront plus avoir une entière confiance dans l'infrastructure.
    Elles auront par ailleurs plus de difficultés à savoir qui accède aux applications et comment.

Nouvelle problématique de sécurité avec le cloud

- Il devient dès lors impératif de repenser la sécurité, et de rajouter des protections.
- On peut donc identifier cinq mesures pour améliorer la sécurité du *cloud* :

1. Repenser la sécurité périmétrique pour tenir compte de l'architecture en place dans l'entreprise et chez ses prestataires éventuels
2. Concentrer les efforts de sécurité sur des périmètres réduits et multipliés, au plus près des équipements hébergeant les applications les plus stratégiques et stockant les données les plus sensibles pour l'entreprise et ses clients.
3. Associer une *appliance* de sécurité virtualisée aux applications stratégiques, les données sensibles de l'entreprise restant ainsi protégées, où que soient les plate-formes physiques les supportant.
4. Renforcer l'administration de la sécurité qui devra savoir gérer l'ensemble des ressources, en privé et en externe.
5. Mettre en place un dispositif de surveillance pour être alerté en cas de vulnérabilité, d'attaque ou d'incident sur une ressource exploitée par un tiers, ce que les prestataires *cloud*, que ce soit en mode *IaaS, PaaS ou SaaS*, proposent encore rarement.

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des réseaux et des systèmes***
    - *Analyse de la vulnérabilité des réseaux et des systèmes.*
    - *Modes d'attaque. Nouvelles menaces.*
    - *Face à ces menaces, le sécurité périmétrique multi-niveaux.*
    - *Concept de Network Access Control.*
    - *Détection (IDS) et prévention (IPS) des intrusions. Scan des vulnérabilités et déploiement des pare-feux.*
    - *Procédures types pour un réseau Win2K.*
    - *Evolution. Exemple des architectures Cisco : de SAFE à SecureX.*
    - *Nouvelle problématique de sécurité avec le cloud. Sécurité dans les clouds publics, privés et hybrides*
    - ***Serveurs et réseaux de haute disponibilité.***

Serveurs et réseaux de haute disponibilité

- La **haute disponibilité** (*HA*), également connue sous l'appellation plus technique de *LDR+Switch* (réplication logique des données plus basculement), permet de déplacer rapidement des utilisateurs et des processus vers un serveur secondaire entièrement répliqué et, par conséquent, capable de prendre en charge tout ou partie des fonctions du serveur de production.
- Les éléments qui interviennent dans une solution dehaute disponibilité sont les suivants :
  - **Matériel** : Un second serveur dont la capacité sera suffisante pour stocker les données répliquées et répondre à d'éventuels besoins de production.
  - **Bande passante** : Si le second serveur est situé sur un autre site (ce qui est plus que souhaitable), il faut pouvoir compter sur une bande passante capable de prendre en charge le volume de données envoyé par le serveur de production, la capacité de traitement en entrée/sortie du serveur de secours et les liaisons de communication entre les différents sites.
  - **Logiciel de haute disponibilité** : Ce composant exécute, gère et surveille la réplication (*mirroring*) des données critiques envoyées vers le serveur de secours. Ce logiciel permet également de déplacer efficacement les utilisateurs et les processus vers le serveur de secours en cas d'interruption de l'activité.

Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - ***C07 Renforcer la sécurité des accès et des contrôle d'identités***
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des accès et des contrôle d'identités***
    - ***Identification et authentification des utilisateurs. Mots de passe. Sécurité du poste de travail.***
    - *Authentifications fortes. Systèmes biométriques.*
    - *Authentification LDAP et SSO*
    - *Nouvel enjeu pour la fédération d'identités : intégrer le SaaS. SAML comme norme d'échange*

Identification et authentification

« S'identifier, c'est communiquer son identité.

S'authentifier, c'est apporter la preuve de son identité.. »

Philippe Wolf
Ecole polytechnique. CNRS.

Identifier et authentifier

- La protection de la confidentialité implique la détermination des droits et privilèges qui elle-même passe par un **mécanisme d'identification** et **d'authentification** des systèmes ou des individus placés aux extrémités de la ligne de communication.
- Le mécanisme peut être simple (identifiant et mot de passe) ou fort (idem + jeton).
- Un autre enjeu lié à l'authentification est celui de son unicité.
- L'utilisateur rejettera les règles de la stratégie de sécurité si elle le contraint en plus à mémoriser autant de procédures, de numéros de compte et de mots de passe qu'il y a d'applications.
- Une solution d'authentification unique (**SSO pour Single Sign-On**) est indispensable.

Sécurité du poste de travail

- Le piratage de serveurs devient de plus en plus difficile, les attaquants se dirigent donc vers des proies plus faciles : les postes clients.
- De plus en plus de postes clients, contenant les identifiants et mots de passe de leurs utilisateurs, se connectent à distance à des réseaux d'entreprise.
- La prise de contrôle d'un tel poste permet l'accès à l'ensemble des applications et des fichiers utilisés par le titulaire de l'ordinateur.
- Un seul poste client piraté suffit à court-circuiter toutes les barrières de protection d'un réseau d'entreprise (les pare-feu acceptent les connexions de ces postes).

Sécurité du poste de travail

- Les dernières versions de Windows permettent l'enregistrement automatique de mots de passe.
- Cette pratique dangereuse permet à n'importe quelle personne ayant un accès physique à un ordinateur d'utiliser les ressources qu'il renferme.
- La sécurité des postes de travail passe donc souvent par la restriction des fonctionnalités, que ce soit au niveau des lecteurs de supports amovibles, sources d'infection (postes « *diskless* ») ou au niveau des systèmes d'exploitation.
- Sous Windows par exemple, si l'exécution des scripts n'est pas utile, il vaut mieux retirer le *Windows Scripting Host*. Les postes deviendront ainsi immunisés aux vers les plus courants. De même avec les navigateurs Internet : en neutralisant l'exécution de code (même signé), il est possible d'éviter bon nombre d'attaques communes. Même approche avec les macros commandes des outils bureautiques.

Sécurité du poste de travail

- Les mises à jour de sécurité disponibles, tant pour le système d'exploitation que pour les applications utilisées (Internet Explorer, Outlook, Office ...), doivent être installées par les administrateurs.
- De même, l'installation d'un **antivirus** est indispensable, sa mise à jour, l'analyse régulière du système ainsi que de l'ensemble des documents téléchargés (courriels, fichiers, pages Web).
- La limitation des logiciels clients à une liste de logiciels autorisés contribue aussi à l'amélioration de la sécurité.

Antivirus

- Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier.
- On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur.
- Il existe plusieurs méthodes d'éradication :
  - La suppression du code correspondant au virus dans le fichier infecté ;
  - La suppression du fichier infecté ;
  - La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

Antivirus

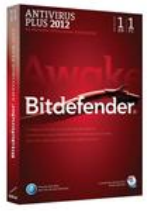
- Les virus se reproduisent en infectant des « applications hôtes », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant.
- Pour ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier.
- Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale**.
- Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter.
- Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus.
- Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus.

Antivirus

- Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus.
- De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "**virus polymorphes**".
- Certains antivirus utilisent un contrôleur d'intégrité pour vérifier si les fichiers ont été modifiés.
- Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.
- La **méthode heuristique** consiste à analyser le comportement des applications afin de détecter une activité proche de celle d'un virus connu.
- Ce type d'antivirus peut ainsi détecter des virus même lorsque la base antivirale n'a pas été mise à jour. En contrepartie, ils sont susceptibles de déclencher de fausses alertes.

Antivirus : une offre large

Les antivirus payants



BitDefender Antivirus 2012

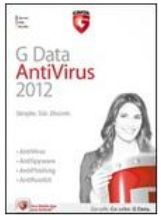
Télécharger la version d'essai

ESET NOD32 Antivirus 5

Télécharger la version d'essai

F-Secure Antivirus 2012

Télécharger la version d'essai



GDATA Antivirus 2012

Télécharger la version d'essai

PC Tools Spyware Doctor avec Antivirus

Télécharger la version d'essai

Kaspersky Antivirus 2012

Télécharger la version d'essai

McAfee Antivirus Plus 2012

Télécharger la version d'essai

Norton Antivirus 2012

Télécharger la version d'essai

Trend Micro Titanium

Les antivirus gratuits

Avira Free Antivirus 12

Télécharger gratuitement

Avast Antivirus Gratuit 6

Télécharger gratuitement

AVG Antivirus 2012

Télécharger gratuitement

Microsoft Security Essentials 2.1

Télécharger gratuitement

Panda Cloud Antivirus 1.5

Télécharger gratuitement

***Source** : www.clubic.com*

Do We Really Need a Security Industry?

« La raison principale de l'existence de l'industrie de la sécurité informatique est que les produits et services informatiques ne sont pas naturellement sûrs. Si les ordinateurs étaient protégés des virus, il n'y aurait pas besoin de produits antivirus. Si le mauvais trafic réseau ne pouvait être utilisé pour attaquer les ordinateurs, personne ne s'inquiéterait d'acheter un pare-feu. S'il n'y avait plus de débordement de tampon, personne n'aurait besoin d'acheter des produits pour se protéger contre leurs effets. Si les produits informatiques que nous achetons étaient sûrs par défaut, nous n'aurions pas besoin de dépenser des milliards chaque année pour les rendre plus sûrs. »

Bruce Schneier, cryptologue

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des accès et des contrôle d'identités**
    - *Identification et authentification des utilisateurs. Mots de passe. Sécurité du poste de travail.*
    - **Authentifications fortes. Systèmes biométriques.**
    - *Authentification LDAP et SSO*
    - *Nouvel enjeu pour la fédération d'identités : intégrer le SaaS. SAML comme norme d'échange*

Authentification forte

- On appelle **authentification forte** tout système permettant un accès informatique après une double vérification.
- L'objectif est de pallier les faiblesses de l'authentification unique par mot de passe.
- En effet, les mots de passe peuvent être volés, forcés et posent un problème de mémorisation à l'utilisateur et de renouvellement à l'entreprise.
- S'ils restent en usage dans les environnements où l'impératif de sécurité est faible, grâce à leur rapport qualité / prix imbattable, ils montrent certaines limites dans des contextes à sécurité élevée.
- En raison du coût de l'authentification forte, son usage reste aujourd'hui réservé aux grands comptes ou, plus généralement, aux secteurs critiques de l'industrie et des services (banque, énergie, défense, aéronautique, automobile, recherche scientifique).
- Elle se retrouve toutefois de plus en plus fréquemment utilisée par des entreprises de taille modeste qui souhaitent ouvrir leur système d'information à l'extérieur.

Authentification forte

- L'authentification forte consiste donc à mixer différentes stratégies d'authentification :
  - une carte magnétique et une identification biométrique par exemple,
  - un certificat électronique et un code alphanumérique affiché à l'écran.
- Ces informations sont ensuite mises en relation avec une solution de gestion des identités et des accès, elle-même en relation avec un annuaire ou un méta-annuaire de l'entreprise qui référence tous les utilisateurs du parc informatique ainsi que leurs droits.

Authentification forte

- L'authentification forte s'appuie sur d'autres concepts que celui des mots de passe.
- Le premier d'entre eux étant celui du **jeton unique**.
- Le principe est simple : il s'agit d'un algorithme de génération de mots de passe unique, à durée de vie courte, qui se synchronise avec une application cliente installée sur le poste de travail.
- Cet algorithme peut être installé sur une calculette se contentant alors d'afficher le code généré, sur une clef USB, qu'il faudra brancher à l'appareil, ou sur une carte à puces qui transmet le code par contact avec un appareil de lecture.
- Le mot de passe ainsi généré n'est valable que pour une période de temps de 1 à 2 minutes.

Authentification forte

- Deuxième solution d'authentification forte mise en place, cette fois-ci pour sécuriser les accès aux services Internet : les **certificats électroniques**, qui appliquent en partie le principe du jeton sur le Web.
- Les certificats électroniques sont des fichiers attestant de l'identité de l'auteur en liant par exemple son mot de passe à des renseignements personnels (code INSEE).
- Le certificat électronique envoie ensuite ces informations à un serveur central qui vérifie que ce fichier est bien représenté dans sa base de données avant de lui autoriser l'accès aux services Web.
- Contrairement au principe du jeton, les certificats électroniques disposent d'une durée de vie plus longue, en moyenne de quelques semaines.
- Autre différence, le jeton n'est pas émis par une carte que possède l'utilisateur mais par le serveur, après saisie des données personnelles de l'utilisateur.
- Aussi, si l'utilisateur perd son certificat électronique, il peut en redemander un autre et s'authentifier rapidement.

Systèmes biométriques

- Sans doute la méthode la plus prometteuse, mais aussi la plus délicate à mettre en œuvre, la **biométrie**.
- Elle repose sur des systèmes de capture d'images couplés à une base de données centrale stockant les informations personnelles.
- On distingue 4 catégories d'applications à la biométrie :
  - la reconnaissance digitale,
  - la reconnaissance d'iris,
  - la reconnaissance faciale,
  - la reconnaissance vocale.
- L'avantage de ces méthodes est clair : l'utilisateur a toujours sur lui ses "codes d'authentification" et ne peut les perdre ou les oublier.

Systèmes biométriques

- Il existe toutefois - outre son coût - plusieurs limites à la biométrie.
- Tout d'abord l'aspect juridique, les droits des personnes étant fichés, leurs caractéristiques morphologiques aussi.
- Ces bases de données sont à rapprocher de celles utilisées par la police et donc soumises à des lois très strictes.
- D'autre part, les données peuvent être falsifiées dans le cas de la reconnaissance digitale ou de la reconnaissance vocale.
- Enfin, la biométrie pose le problème de la qualité de l'authentification.
- Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système.
- L'un des axes de recherche de la biométrie porte donc sur la multimodalité, c'est-à-dire la combinaison de plusieurs méthodes d'identification par voie biométrique.

Systèmes biométriques

Lecteur Handkey d'Abiova

Détection de l'iris IRISPASS-M de Oki

Biovein de Easydentic reconnaissance du réseau veineux

Authentifications fortes.

Algorithmes et protocoles

- Les solutions d'authentification forte s'appuient sur les nombreux protocoles de sécurité que nous avons rencontrés (ou que nous verrons prochainement), de manière à acheminer l'information personnelle de l'utilisateur de la manière la plus sure jusqu'au serveur d'authentification.
- Sur le Web, le protocole ***HTTPS*** se base sur le procédé de cryptographie ***SSL*** (*Secure Sockets Layers*) qui s'assure que les paquets échangés entre le serveur et le client ne sont pas lisibles de l'extérieur.
- Dans les réseaux étendus d'entreprise, cette fonction est assumée par le protocole ***IPSec***, géré par la majorité des réseaux privés virtuels (***RPV/VPN***).
- Dans les réseaux internes, il existe différentes couches de sécurité. Sur les réseaux mobiles, le protocole ***802.11i*** remplit ce rôle de cryptage tandis que les réseaux fixes utilisent depuis longtemps le ***802.10***.
- En ce qui concerne le chiffrement il s'opère avec ***AES*** avec des clefs à 128 ou 256 bits.
- Le chiffrement des échanges s'opère avec ***PGP***.

Authentifications fortes.

Exemples d'offres du marché

Editeur	Solutions	Type de solutions	Technologies	Prix *
RSA	SecurID 700 SecurID Software SmartCard 5200 USB Authenticator 6100	Calculette Token Carte à puces Clef USB Appliance	DES/3DES and RSA (512-768-1024-bit) RSA signature: 512-768-1024 bit, DES, 3DES(CBC,EBC), SHA-1 ANSI X9.31 PRNGe Fonctionne sous Windows 2000/2003, Unix (Solaris, HP-UX, AIX)	**SecurID 700 : 65 $** **SmartCard 5200 : 23.66 $** **USB 6100 : 58.50 $** **Software Token :** **33.15 $ par utilisateur**
VeriSign	Multipurpose First Generation Token	Clef USB Calculette	RSA 1024-bit, DES, 3DES (Triple DES), SHA1, (MD5 - optionel) Fonctionne sous Windows 2000/XP/2003	NC
Safenet	iKey 2032 Model 330 SmartCard	Clef USB Carte à puces	RSA (1024 et 2048 bits), DES, 3DES, RC2, SHA-1, MDS	NC
Safeboot	Content Encryption 2.1	Algorithme de chiffrement	AES 256 bit AES 256bit (FIPS certified) DES 56bit RC5 32-12-1024 RC5 32,18,1024 Fonctionne sous Windows NT/2000/2003, Novell, Terminal	NC
Aladdin	eToken NG-OTP eToken Pro USB eToken Pro SmartCard	Carte à puces Clef USB Calculette	RSA (1024 et 2048 bits), DES, Triple DES, SHA1 Fonctionne sous Windows 9x/ME/NT4/2000/XP, Novell	**SmartCard : 17.50 € HT** **USB :** **62.40 € HT** **NG-OTP : 89.00 € HT**
ActivCard	ActivKey ActivClient ActivCard SoftToken ActivCard One ActivCard Keychain	Clef USB Carte à puces Calculette	RSA (de 512 à 2048 bits), DES, Triple DES, SHA-1 Fonctionne sous Windows 98/NT4/2000/XP/2003, Linux, Unix (Solaris, AIX, HP-UX, IBM MVS)	NC
Ilex	Certatoo Applatoo	Gestion des certificats e-signature	DES, Triple DES, RC2, RC4, RC6, IDEA, AES, RSA (de 512 à 2048 bits), DSA, SHA-1, MD5 Fonctionne sous Windows 98, 2000, XP, 2003 - Macintosh 8, 9, X - Linux	**Applatoo :** **20 000 € (pour 5000 utilisateurs)** **Certatoo :** **37 500 € (pour un processeur)**
CryptMe	Esa, Pathword	Calculette	Spécifique Fonctionne sous Windows XP/2000/2003	**Carte : 3.50 euros** **Esa : 25 euros par poste (carte comprise et 100 utilisateurs Esa)**
Axalto	eGate Cryptoflex	Clef USB Carte à puces	RSA (de 512 à 2048 bits), DES, Triple DES, SHA-1 Fonctionne sous Windows 2000/XP	NC
Vasco	Digipass	Calculette	DES, Triple DES Fonctionne sous Windows 2000/XP	**Digipass : 515 HT (10 calculettes + garantie 10 ans)**

Source : Journal du Net

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des accès et des contrôle d'identités**
    - *Identification et authentification des utilisateurs. Mots de passe. Sécurité du poste de travail.*
    - *Authentifications fortes. Systèmes biométriques.*
    - **Authentification LDAP et SSO**
    - *Nouvel enjeu pour la fédération d'identités : intégrer le SaaS. SAML comme norme d'échange*

Authentification LDAP

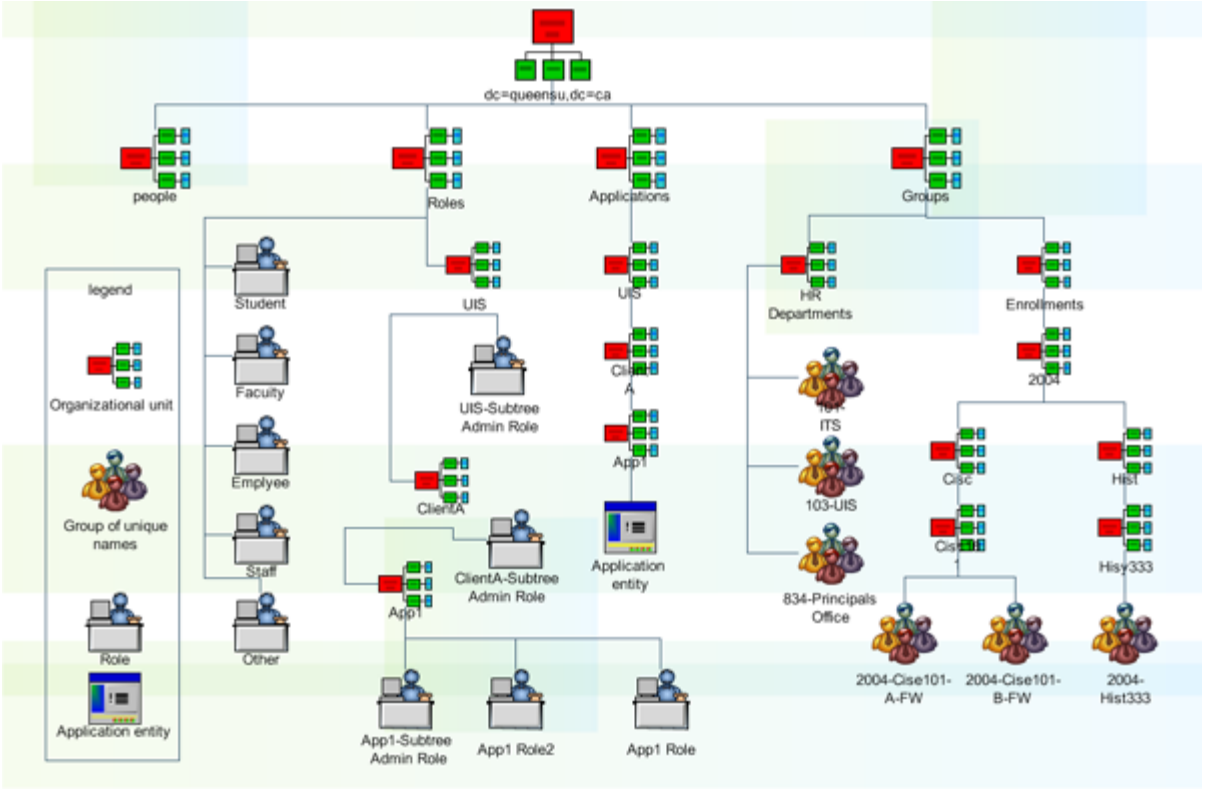
- ***LDAP*** (*Lightweight Directory Access Protocol*) est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire des protocoles TCP/IP.
- *LDAP* fournit à l'utilisateur des méthodes lui permettant de :
  - se connecter
  - se déconnecter
  - rechercher des informations
  - comparer des informations
  - insérer des entrées
  - modifier des entrées
  - supprimer des entrées
- D'autre part le protocole LDAP (dans sa version 3) propose des mécanismes de chiffrement (SSL, ...) et d'authentification (SASL) permettant de sécuriser l'accès aux informations stockées dans la base.

Authentification LDAP

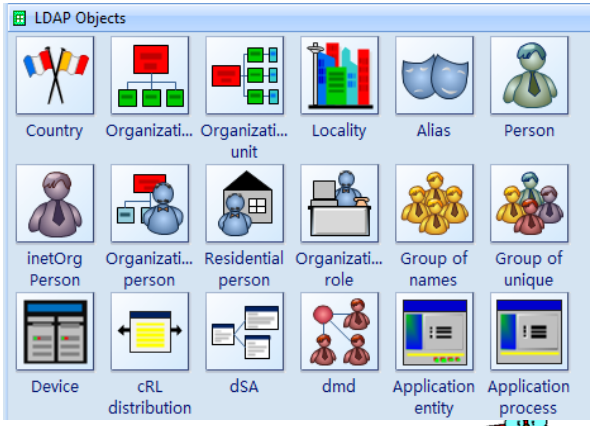
- *LDAP* présente les informations sous forme d'une arborescence d'informations hiérarchique appelée DIT (*Directory Information Tree*), dans laquelle les informations, appelées entrées (ou encore DSE, *Directory Service Entry*), sont représentées sous forme de branches.
- Une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais *root entry*).
- Chaque entrée de l'annuaire *LDAP* correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...).

Authentification LDAP et SSO.

Authentification LDAP



Représentation graphique d'un réseau LDAP avec Edraw



SSO

- L'objet du *Single Sign-On*, noté **SSO**, est de centraliser l'authentification afin de permettre à l'utilisateur d'accéder à toutes les ressources (machines, systèmes, réseaux) auxquels il est autorisé d'accéder, en s'étant identifié une seule fois sur le réseau.
- Le *SSO* propage ainsi l'information d'authentification aux différents services du réseau, voire aux autres réseaux et d'éviter ainsi à l'utilisateur de multiples identifications par mot de passe.
- Toute la difficulté de l'exercice réside dans le niveau de confiance entre les entités d'une part et la mise en place d'une procédure de propagation commune à toutes les entités à fédérer.

Authentification LDAP et SSO.

SSO

- Les objectifs du SSO sont multiples :
- P46

Exemples d'offres du marché

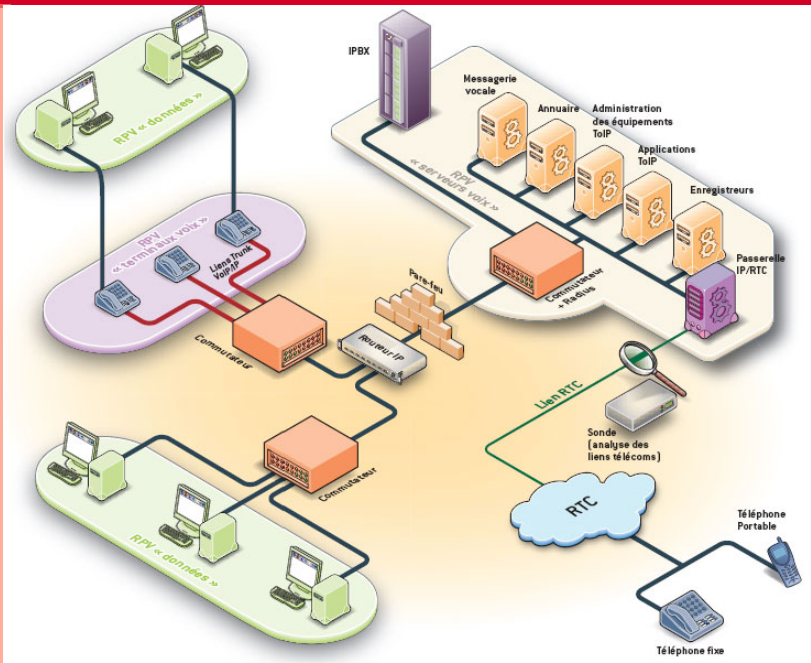
Éditeur	Produit	Commentaire	Siteweb
Computer Associates	eTrust SSO	Couvre à la fois les applications client-serveur et les applications web. Gère plusieurs méthodes d'authentification. S'intègre à de nombreuses plates-formes, y compris les mainframes.	www3.ca.com/Solutions/Product.asp?ID=166
Evidian	SSO Xpress Standard Edition (client-serveur) ou Web Edition	Exige un annuaire LDAP v.3, mais s'intègre aussi à Microsoft Active Directory et à Lotus Domino. Disponible pour Windows, Unix et Linux.	www.evidian.com/security/ssoweb/index.htm
Ilex	Sign&go	SSO client-serveur et web français. S'intègre à un grand nombre d'annuaires (Critical Path, Sun ONE, Novell eDirectory, Microsoft Active Directory, LDAP). Disponible pour Windows, Solaris, Linux, AIX.	www.ilex.fr
Netegrity	SiteMinder	WebSSO avec des fonctions de contrôle d'accès et de gestion des droits évoluées (Role Based Access Control, par exemple). Gère de nombreuses plates-formes, annuaires, applications métier (Oracle, PeopleSoft, Siebel, etc.) et méthodes d'authentification.	www.netegrity.com/products/products.cfm?page=Smoverview
Novell	Nsure SecureLogin	SSO client-serveur (Windows) et web. Reconnaît les annuaires Novell mais aussi Active Directory, LDAP v.3 et les domaines NT.	www.novell.com/fr-fr/products/securelogin/
Passlogix	v-GO SSO	Livré préconfiguré pour de nombreuses applications client-serveur et web (Citrix, Novell GroupWise, Oracle, Siebel Sales, Microsoft Outlook, etc.), et systèmes d'exploitation, dont AS/400.	www.passlogix.com/products/v-go_sso/overview.asp
Prologue Software	CryptoGram SSO	Solution bureautique sans serveur centralisé. Les mots de passe sont stockés sur un support externe (carte à puce ou clé USB) fourni à chaque utilisateur, et qui fait office d'authentification forte.	www.cryptogram-fr.com/french/sso.php

En dehors des produits de grands éditeurs, des SSII disposant de compétences dans les technologies open source peuvent également développer un webSSO sur mesure.

Déploiement SSO

«Le déploiement de notre SSO sur nos applications métier exige de remettre à plat toutes les procédures d'authentification de ces dernières pour arriver à une base d'utilisateurs unique. Rien que cela nous a demandé environ quatre à six mois de travail. Nous devons également modifier notre référentiel unique actuel avec Active Directory afin de lui adjoindre un annuaire LDAP pour stocker les certificats.

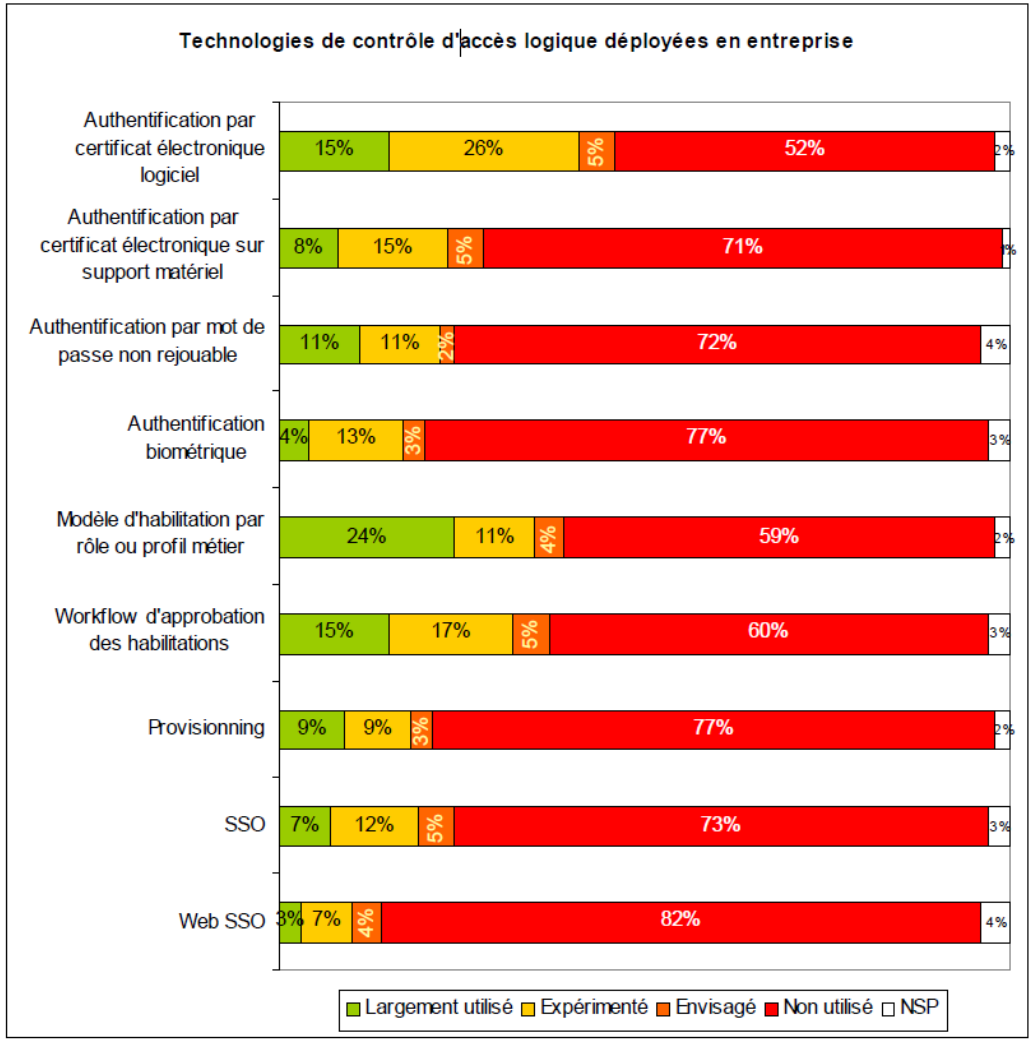
En cascade, cette modification entraîne également le changement du serveur d'applications (WebLogic), qui doit évoluer de la version 6 à la version 8, car seule cette dernière peut gérer les extensions de certificats et la récupération de mots de passe. Sans compter que le projet oblige à revoir toute la politique de mots de passe de l'entreprise, les accès externes, la messagerie. C'est un gros chantier ! On se rend compte que, finalement, monter un SSO oblige à avoir une vision très claire de toutes les briques techniques mises en œuvre dans l'entreprise et de bien vérifier, à chaque étape, que chaque brique que l'on s'apprête à déployer est compatible avec l'existant. »



Frank Moussé
Dexia Sofaxis

Renforcer la sécurité des réseaux et des systèmes

Contrôle d'accès : Qui utilise quoi ?



Source : Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Plan

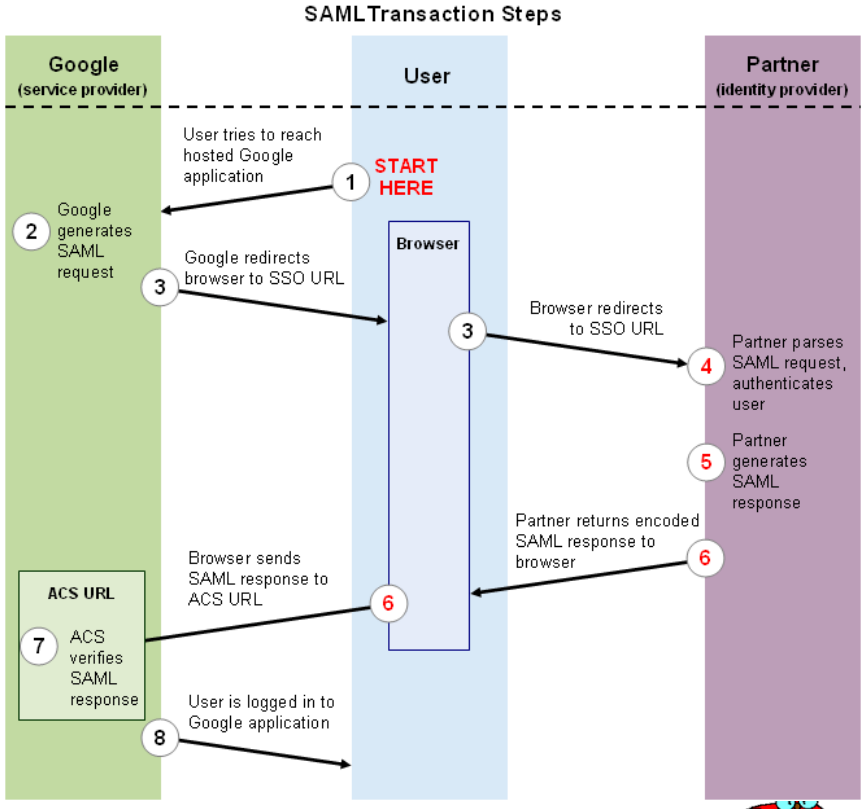
- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des accès et des contrôle d'identités***
    - *Identification et authentification des utilisateurs. Mots de passe. Sécurité du poste de travail.*
    - *Authentifications fortes. Systèmes biométriques.*
    - *Authentification LDAP et SSO*
    - ***Nouvel enjeu pour la fédération d'identités : intégrer le SaaS. SAML comme norme d'échange***

Fédération d'identités

- Alors que les systèmes de *SSO* au sein des organisations sont largement répandus, on cherche aujourd'hui à les étendre vers l'extérieur, vers les organismes et services partenaires, et vers les prestataires *SaaS*.
- Il s'agit avant tout d'une démarche de simplification pour l'utilisateur, lui évitant une multitude de saisies et de créations de comptes.
- Elle permet d'autre part aux sites partenaires, susceptibles d'utiliser des systèmes potentiellement faillibles, de déléguer l'authentification d'un utilisateur au système d'authentification forte, centralisé et maitrisé par le SI de l'organisme.
- Cette délégation est particulièrement critique pour les entreprises.
- A cela s'ajoute la gestion de l'identité numérique et de la diffusion des informations nominatives des utilisateurs.
- Ces problématiques s'articulent autour de la **fédération d'identités**.

SAML

- Dans le contexte professionnel, la fédération d'identités repose sur le standard ***SAML*** (***Security Assertion Markup Language***) pour échanger des données d'authentification et d'attributs entre les fournisseurs de services Web et les fournisseurs d'identités.
- Normalisé par l'*OASIS*, *SAML* permet l'échange sécurisé d'informations d'identités.
- Il définit un format du message *XML*, appelé assertion, ainsi qu'un ensemble de profils.
- Ces profils sont des cas d'utilisation détaillés qui présentent la cinématique d'échange des messages, les paramètres attendus et renvoyés.



SAML

- *SAML* définit deux briques essentielles pour sécuriser les échanges :
  - Le *SP (Service Provider*), fournisseur de service, protège l'accès aux applications. Il refuse tout accès sans authentification préalable et redirige l'utilisateur non authentifié vers son fournisseur d'identité.
  - L'*IdP (Identity Provider),* fournisseur d'identité, s'occupe d'authentifier l'utilisateur ainsi que de récupérer des informations additionnelles associées à son identité.
- Ce mode de fonctionnement est suffisant pour une utilisation cantonnée à l'entreprise avec un annuaire des identités centralisé.
- Dans le cadre d'une fédération entre plusieurs domaines d'identification, *SAML* définit une troisième brique appelée le *DS* (*Discovery Service*) qui permet à l'utilisateur de sélectionner manuellement son domaine parmi une liste.

Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - ***C08 Renforcer la sécurité des applications et des services***
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- ***B. Les méthodes et les outils***
  - ***Renforcer la sécurité des applications et des services***
    - ***Analyse de la vulnérabilité des applications et des services.***
    - *Sécurité du web. Protocoles (HTPP + SSL/TLS => HTTPS).*
    - *Sécurité des applications web. L'Open Web Application Security Project.*
    - *Sécurisation des web services.*
    - *Principes du développement sécurisé.*

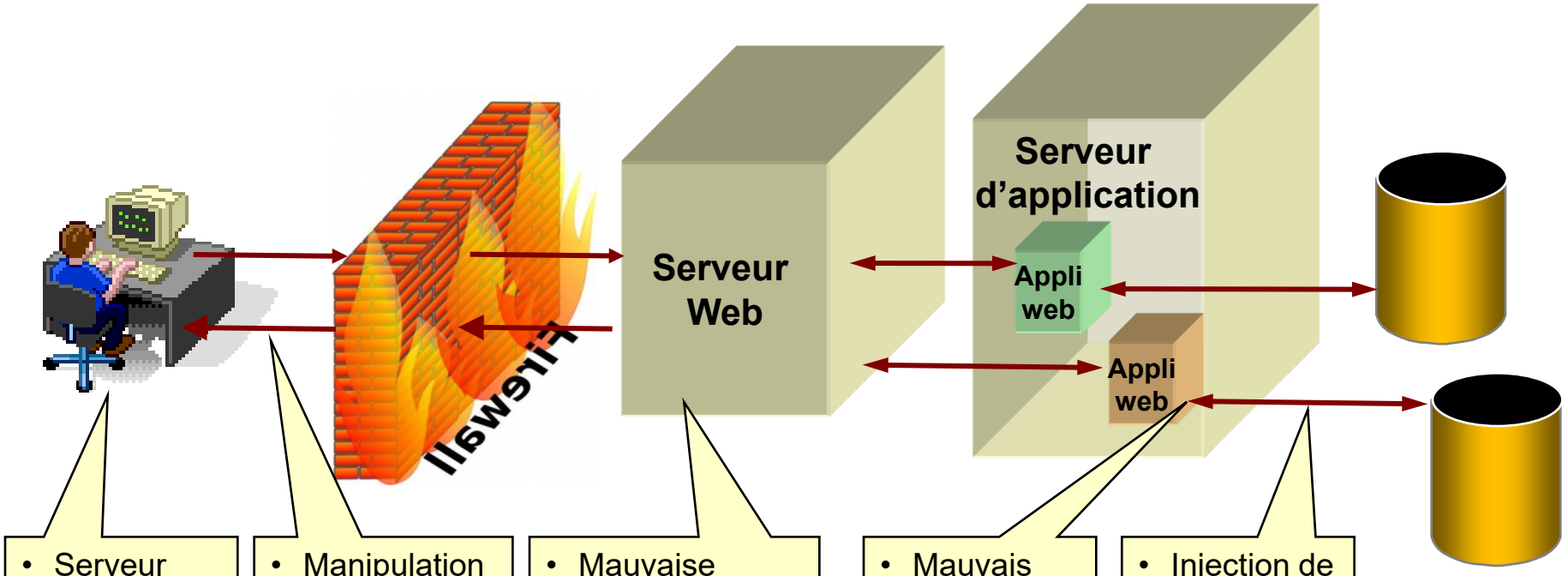
Renforcer la sécurité des applications et des services.

Vulnérabilité des composants d'une application web

- Pour permettre l'utilisation d'une application Web, il suffit que le pare-feu protégeant celle-ci ne laisse entrer que le protocole HTTP, en général sur le port TCP 80 (et éventuellement HTTPS sur le port TCP 443).
- Dans ces conditions, il semble difficile d'attaquer une application Web.
- Pourtant, à travers ce seuls ports, considérés comme « amicaux » passent de plus en plus de flux et de protocoles (*DCOM, RPC, SOAP, XML, streaming sur HTTP*, …), il est possible de lancer des attaques extrêmement dangereuses.
- Les différentes sortes d'attaques sur les applications Web passant le filte des pare-feux sont les suivantes :
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting (XSS)
  - Autres attaques (Mécanismes d'authentification basés sur Java, JavaScript ou ActiveX, Contrôle d'accès basé sur le header HTTP_REFERER, Manque de ré-authentification à l'occasion du changement d'un mot de passe, Mauvaise gestion du contexte utilisateur, attaque côté client, attaque « *man in the middle* »)

Renforcer la sécurité des applications et des services

Vulnérabilité des composants d'une application web



- Serveur hostile
- Cross site scripting

- Manipulation des identifiants de session

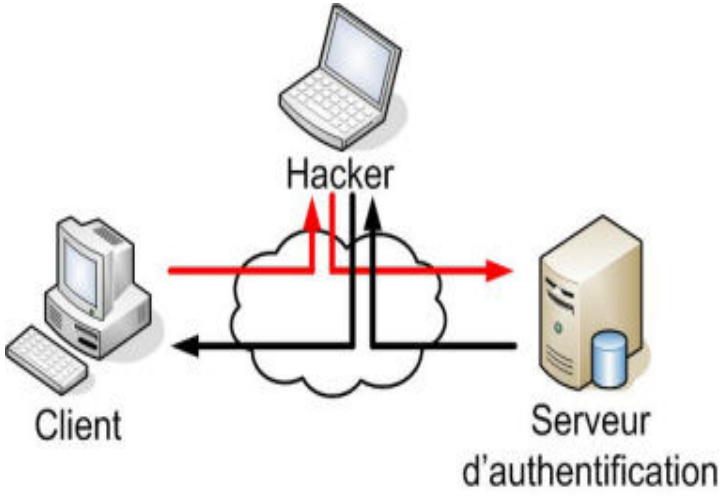
- Mauvaise interprétation des URLs
- Mauvaise configuration

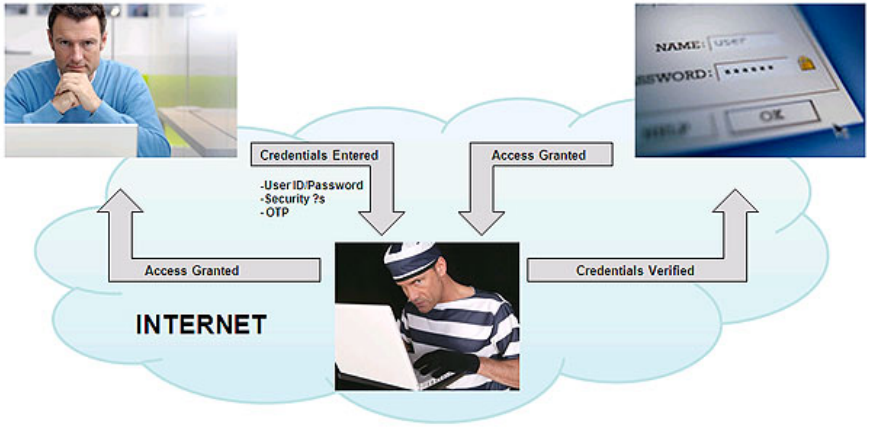
- Mauvais contrôle des entrées utilisateurs

- Injection de code SQL
- Dénis de service

Exemple du « man in the middle »

- Une attaque dite "**man in the middle**" consiste à intercepter les requêtes du client et à les relayer vers le serveur distant légitime et inversement à intercepter les réponses du serveur et à les relayer vers le client.
- Il est possible au passage, si nécessaire, de modifier à la volée les données fournies par le client et/ou les réponses du serveur.
- Cette attaque est possible même si le serveur de destination utilise un chiffrement par SSL : il suffit que le serveur intercepteur possède lui aussi un certificat serveur et que le client clique sur « Accepter » lorsque son navigateur lui propose d'utiliser ce certificat pour dialoguer avec le serveur distant légitime.
- C'est ce que fera tout utilisateur peu attentif ou qui ne sera pas au fait des problèmes de sécurité.
- Il ne reste plus alors au serveur intercepteur qu'à déchiffrer d'un côté et rechiffrer de l'autre, à la volée.
- Le seul moyen de se prémunir contre ce type d'attaque est d'imposer une authentification côté client par l'utilisation de certificats clients X.509.
- Le serveur intercepteur ne pourra alors plus se faire passer pour le client auprès du serveur distant légitime car il ne dispose pas de la clé privée du client.





La réponse : le filtrage applicatif

- Le **filtrage applicatif** consiste à effectuer un filtrage des requêtes et des réponses non pas au niveau réseau (couche OSI 2 pour Ethernet au niveau d'un switch par exemple, couche 3 pour IP, couche 4 pour TCP et UDP au niveau d'un firewall) mais au niveau application (couche OSI 7).
- Le filtrage applicatif suppose donc la connaissance de l'application et de ses protocoles afin de connaître la structure des données échangées.
- Dans le cas particulier des applications Web, il s'agit d'interpréter intégralement le protocole HTTP pour en extraire les URLs, les headers, les cookies, les authentifiants, etc…
- L'avantage du filtrage applicatif apparaît donc clairement : les règles utilisées à ce niveau peuvent se fonder sur tous ces paramètres de niveau élevé et permettre un filtrage beaucoup plus élaboré qu'un simple filtrage TCP/IP.
- Il s'agit en fait d'un filtrage de contenu.
- Celui-ci peut aller jusqu'au filtrage du code mobile hostile véhiculé dans les pages HTML, sous forme de scripts Javascript ou d'ActiveX.
- Le filtre applicatif HTTP couramment utilisé pour la protection d'une application Web est le « **reverse proxy** », appelé aussi relais inverse.
- Il s'agit d'un relais applicatif agissant en coupure, qui va s'intercaler entre le serveur Web et les clients extérieurs.
- C'est le reverse proxy qui répond aux requêtes des clients, et c'est lui qui effectue les requêtes vers le serveur Web final.

La réponse : agir au niveau du code

- Il n'existe pas de solution miracle pour détecter les vulnérabilités des applications Web.
- Pour ce faire, la stratégie est la même que l'approche multicouches utilisée pour garantir la sécurité sur un réseau.
- La détection et la remédiation de certaines vulnérabilités impose l'analyse du code source, en particulier pour les applications Web d'entreprise complexes.
- La détection des autres vulnérabilités peut également nécessiter des tests de pénétration sur site.
- La plupart des vulnérabilités courantes des applications Web peuvent également être détectées à l'aide d'un scanner automatisé.
- Pour réussir dans ce type de démarche, les problématiques sécuritaires doivent être prises en compte le plus en amont possible dans le projet (phase de conception de l'architecture applicative) et être suivie tout au long de la vie de l'application (nouvelles versions, patches de sécurité, etc.).
- Enfin, un audit effectué par une société externe est quasiment obligatoire afin de contrôler les mesures mises en place, tout au moins pour les sites les plus sensibles.

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des applications et des services**
    - Analyse de la vulnérabilité des applications et des services.
    - **Sécurité du web. Protocoles (HTPP + SSL/TLS => HTTPS).**
    - Sécurité des applications web. L'Open Web Application Security Project.
    - Sécurisation des web services.
    - Principes du développement sécurisé.

HTTP/S

- Le besoin de sécuriser les sites web a rapidement conduit au développement du protocole ***HTTP/S*.**
- *HTTP/S* correspond au protocole *HTTP* associé aux protocoles de sécurité *SSL* ou *TLS* (*Transport Layer Security*, Sécurité de la Couche Transport).
- Lorsqu'un utilisateur se connecte à un site Web via *HTTP/S*, le site Web crypte la session à l'aide d'un certificat électronique, et établit une connexion sécurisée qui empêche l'interception des données par un tiers.
- Sur le Web, le protocole *HTTP/S* se base sur le procédé de cryptographie SSL (Secure Sockets Layers) qui s'assure que les paquets échangés entre le serveur et le client ne sont pas lisibles de l'extérieur.
- Nous avons évoqué le protocole *HTTP/S* dans la première partie (diapositive 245) à propos de la sécurisation des paiements.

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des applications et des services**
    - Analyse de la vulnérabilité des applications et des services.
    - Sécurité du web. Protocoles (HTPP + SSL/TLS => HTTPS).
    - **Sécurité des applications web. L'Open Web Application Security Project.**
    - Sécurisation des web services.
    - Principes du développement sécurisé.

L'Open Web Application Security Project

- ***OWASP*** (*Open Web Application Security Project*) est une communauté travaillant sur la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous.
- *OWASP* est aujourd'hui reconnu dans le monde de la sécurité des systèmes d'information pour ses travaux sur les applications Web.
- Parmi eux, les projets les plus connus sont les suivants :
  - ***Top Ten OWASP*** : liste des dix risques de sécurité les plus critiques dans les applicatifs Web. Ce classement fait aujourd'hui référence .
  - ***WebGoat*** : Plateforme de formation permettant à un utilisateur d'apprendre à exploiter les vulnérabilités les plus courantes sur une application Web.
  - ***WebScarab*** : Proxy disposant de nombreuses fonctionnalités utiles lors de la réalisation d'audits de sécurité.
  - ***OWASP Testing Guide*** : document de plusieurs centaines de pages destiné à aider une personne à évaluer le niveau de sécurité d'une application Web.
  - ***OWASP Code Review Guide*** : document de plusieurs centaines de pages présentant une méthode de revue de code sécurisé.

Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des applications et des services**
    - *Analyse de la vulnérabilité des applications et des services.*
    - *Sécurité du web. Protocoles (HTPP + SSL/TLS => HTTPS).*
    - *Sécurité des applications web. L'Open Web Application Security Project.*
    - ***Sécurisation des web services.***
    - *Principes du développement sécurisé.*

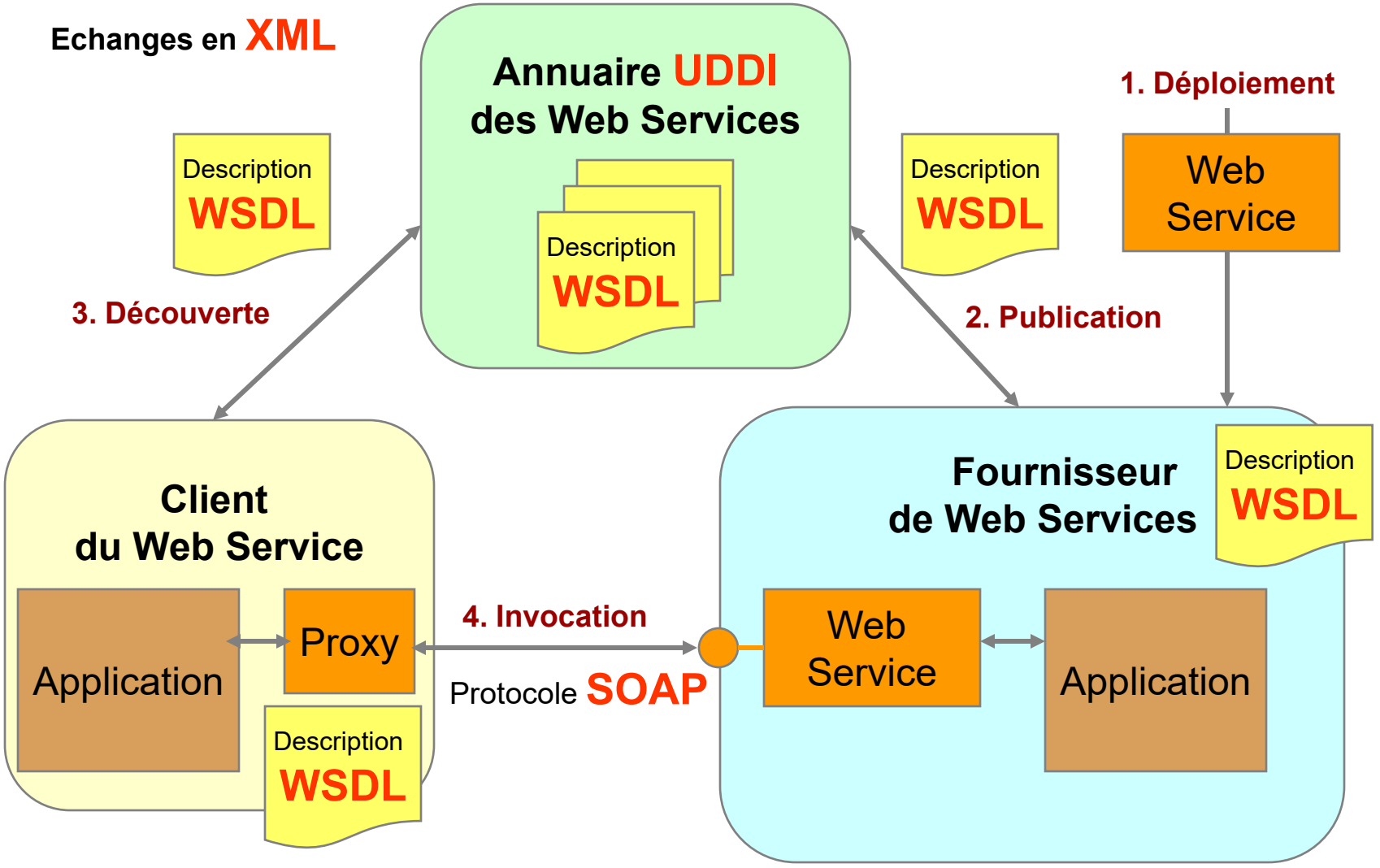
Renforcer la sécurité des applications et des services.

Web services

- Un ***Web Service*** est donc une application modulaire :
  - Mise à disposition sur l'Internet ou sur un réseau privé (Intranet),
  - Auto-descriptive (*WSDL*), publiable (*UDDI*) et accessible (*SOAP*) en utilisant le langage *XML* et les protocoles standards du Web,
  - Indépendante du système d'exploitation et du langage de programmation,
  - Visant à exposer une ou plusieurs fonctionnalités métier ou de gestion.
- Un ensemble de *Web Services* élémentaires peut être combiné (*WS-BPEL*) pour aboutir à un *Web Service* à valeur ajoutée.

Renforcer la sécurité des applications et des services.

Web services



Renforcer la sécurité des applications et des services.

Sécurité et XML

- Signature XML
  - Objectif: signature numérique d'un document XML
  - Garantir l'authenticité et l'intégrité du document
  - Recommandation W3C: XML Signature Syntax and Processing
  - http://www.w3.org/TR/xmldsig-core/
  - Types de signature
    - Enveloppante ('enveloping')
    - Enveloppée ('enveloped')
    - Détachée ('detached')

Renforcer la sécurité des applications et des services.

WS-Security

- Standard OASIS
- V1.0 – 2004, V1.1 – 2006
- Objectifs
  - Authentification
  - Confidentialité des messages
  - Intégrité des messages
- Intégration de différentes technologies
  - Certificats, SAML, Sécurité XML…
  - pour protéger les messages WS de bout en bout

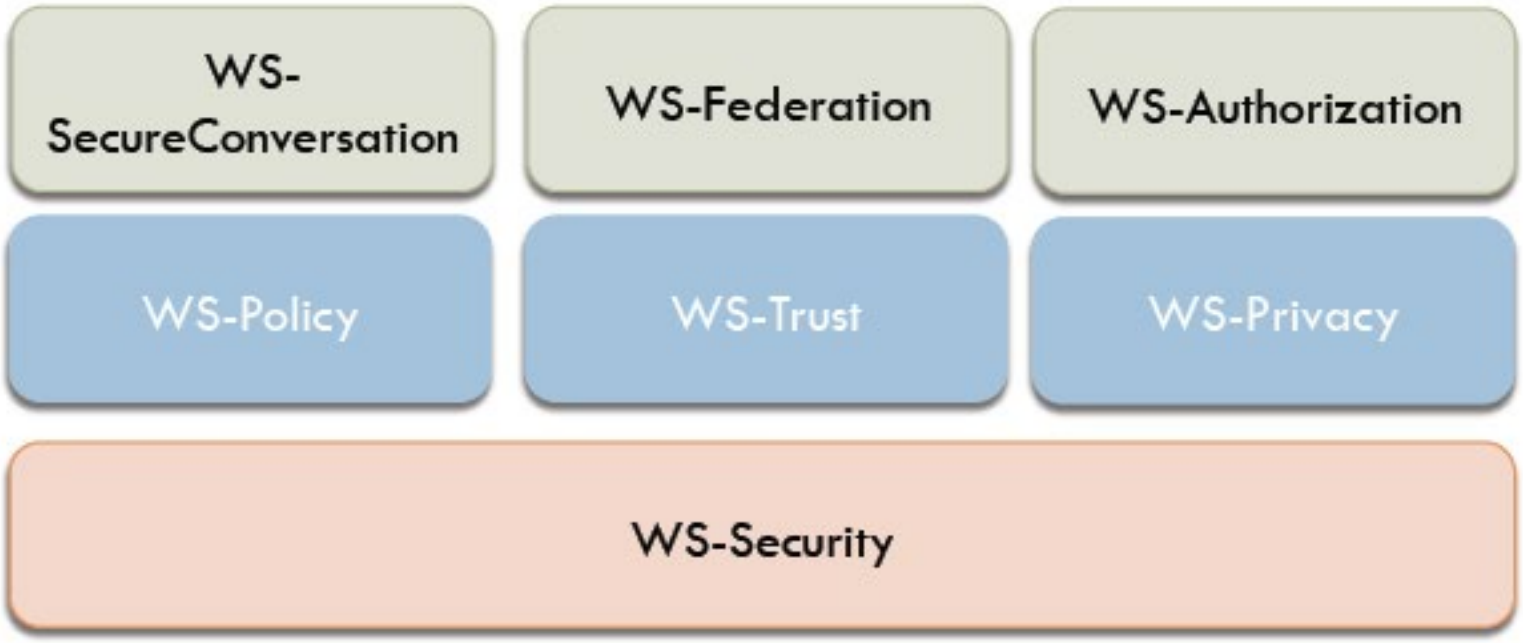
Renforcer la sécurité des applications et des services.

WS-Security

- *WS-Policy* : formalisme pour la définition de politiques s'appliquant à un WS
  - Assertion = caractéristique ou exigence d'un sujet
    - Sujet : endpoint, message, operation…
    - Contient des 'policy expression'
  - *Policy alternative* : collection d'assertions
  - *Policy*: ensemble de policy alternatives
  - Opérateurs : ExactlyOne ou All
- *WS-PolicyAttachment* : lie les politiques et les ressources auxquelles elles s'appliquent
  - 2 stratégies
    - Policy incluse dans le WSDL
    - Document indépendant liant le WS et la policy applicable
  - *WS-PolicyAssertions* : ensemble de politiques pré-définies

Renforcer la sécurité des applications et des services.

WS-Security



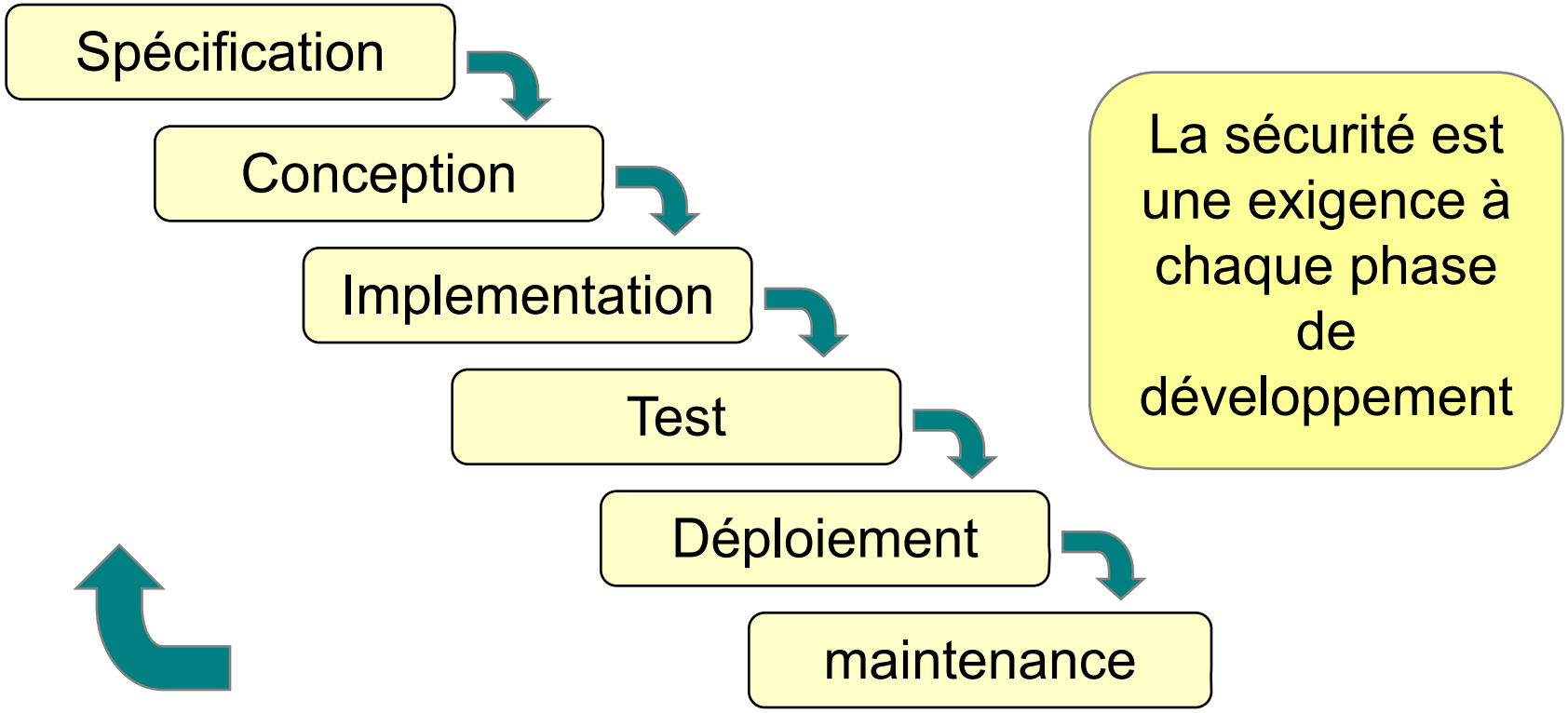
Plan

- **B. Les méthodes et les outils**
  - **Renforcer la sécurité des applications et des services**
    - *Analyse de la vulnérabilité des applications et des services.*
    - *Sécurité du web. Protocoles (HTPP + SSL/TLS => HTTPS).*
    - *Sécurité des applications web. L'Open Web Application Security Project.*
    - *Sécurisation des web services.*
    - ***Principes du développement sécurisé.***

Principes du développement sécurisé

- La sécurité informatique ne peut être considérée comme une "couche" supplémentaire aux développements.
- C'est dès le coeur de la logique interne d'une application que le problème de la sécurité doit être prise en compte.
- *Initiative Secure Development Lifecycle* de *Microsoft* :
  - Nommer un coach sécurité
  - Modéliser les menaces
  - Phase d'implémentation
  - Test de sécurité ciblés
  - Revue finale de sécurité
  - Mise à jour correctives

Principes du développement sécurisé



La sécurité est une exigence à chaque phase de développement

Principes du développement sécurisé

- Voir les chapitres Sécurité et Identification/Authentification du cours PHP
- En faire une étude de cas

A voir

- Privilégier une approche *bottom-up* plutôt que *top down* (cf rapport de Rchard Feynman sur les causes de la catastrophe de la navette Challenger)
- **Modularité**: Diviser le programme en petits modules semi-indépendants, aux interfaces bien définies pour chaque module / fonction.
- **Isolation**: Chaque partie doit fonctionner correctement même si d'autres échouent (retour de résultats incorrects, envoi de requêtes avec des arguments non valides).
- **Mettre en place une défense en profondeur**: construire plusieurs couches de défense.
- **Simplicité** (complexe => non sécurisé).
- Définir et respecter la chaîne de confiance.
- Penser globalement sur l'ensemble du système.
- Redondance plutôt qu'un point de défaillance unique.

Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - ***C09 Renforcer la sécurité des dispositifs mobiles***
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Wifi

- Wi-Fi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11).
- Algorithmes de chiffrement symétrique pour le wifi :
  - RC4
  - DES (Digital Encryption System) : chiffrage de blocs de 64 bits avec une clef de 64 bits
  - 3DES : DES avec trois clefs
  - AES : chiffrage de blocs de 128/192/256 bits avec une clef de 128/192/256 bits
- Protocoles de sécurisation pour le wifi :
  - Radius
  - EAP
  - 802.1X

Radius

- ***RADIUS*** (*Remote Authentication Dial In User Service*) a été conçu à l'origine pour permettre aux fournisseurs d'accès à Internet d'authentifier les utilisateurs distants utilisant les connexions par modem RTC à partir de multiples serveurs mais d'une seule base utilisateurs.
- Principes
  - Le serveur est responsable de :
    - la réception des demandes de connections de l'authentification de l'utilisateur;
    - du renvoi de la configuration nécessaire au client pour offrir l'accès au réseau à l 'utilisateur.
  - Le client collecte les informations d 'authentification et les transmet au serveur.
- Propriétés
  - Les transactions entre le client et le serveur sont authentifiées par une clef partagée.
  - Les mots de passe sont cryptés dans une empreinte MD5.
  - Le serveur supporte l'authentification PAP, CHAP, Unix login, mais le protocole est facilement extensible.

Extension de Radius

- ***EAP*** (*Extensible Authentication Protocol*) est un protocole conçu pour étendre les fonctions du protocole Radius à des types d'identification plus complexes;
- **802.1X** est un protocole assurant l'identification par port pour l'accès à un réseau ;
- Il n'est pas lié explicitement à RADIUS dans son principe mais toutes les mises en œuvre de 802.1X connues s'appuient donc sur RADIUS et EAP.

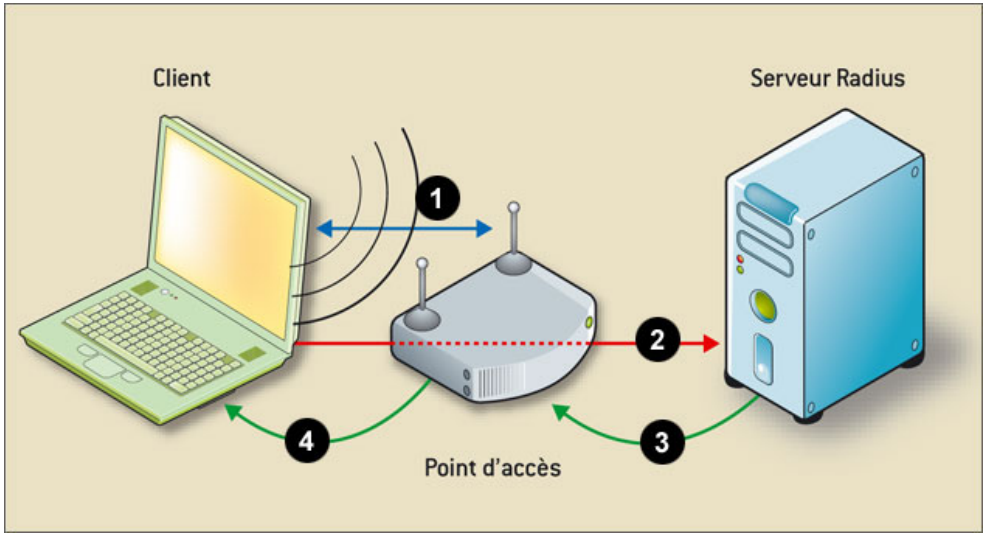
Sécurisation wifi

- Depuis 2004, les entreprises utilisent le standard 802.11i, connu sous l'appellation commerciale de WPA2, pour sécuriser l'accès à leur réseau sans fil.
- Il est désormais acquis que le protocole WEP (*Wired Equivalent Privacy*) n'est pas efficace, loin s'en faut, pour sécuriser l'accès radio.
- L'algorithme qui sert au chiffrement (RC4) est très léger.
- WEP s'appuie, en outre, sur un système de clés fixes, et quelques heures suffisent pour passer en revue l'ensemble des combinaisons possibles.
- Face à ce constat d'échec, une nouvelle technique de sécurisation a fait son apparition en 2002.
- Baptisée WPA (*Wi-Fi Protected Access*), celle-ci utilise pour le chiffrement le protocole TKIP (*Temporal Key Internet Protocol*), qui n'est rien d'autre qu'une évolution de RC4.
- Mais, à la différence de WEP, WPA repose sur un système de clé dynamique, et requiert surtout l'authentification de l'utilisateur, et non plus de la machine qui souhaite se connecter au réseau sans fil.

Sécurisation wifi

- C'est en 2004 que les choses ont vraiment avancé.
- L'IEEE a, en effet, ratifié le standard 802.11i, également connu sous l'appellation commerciale de WPA2.
- La technique de chiffrement RC4 est alors abandonnée pour AES (*Advanced Encryption Standard*), déjà éprouvé dans les réseaux fixes.
- Il s'agit d'une méthode de chiffrement par blocs, alors que RC4, avec une clé à 64 ou 128 bits, effectue le chiffrement au fil de l'eau, dans l'ordre des bits transmis ou reçus.
- La longueur de clé d'AES reste la même qu'avec TKIP (128 bits), mais l'algorithme de chiffrement est plus puissant.
- En entreprise, le standard 802.11i met en œuvre le protocole d'authentification 802.1x avec utilisation d'un serveur d'authentification de type Radius.

Sécurisation wifi



SOLUTION	PROTOCOLE	AUTHENTIFICATION	CHIFFREMENT
WEP	WEP	Optionnelle	RC4
WPA pour la maison	TKIP	Clé partagée	RC4
WPA entreprise	TKIP	802.1x	RC4
WPA2 maison	CCMP	Clé partagée	AES
WPA2 entreprise	CCMP	802.1x	AES

- 1. **Demande d'identité** : Un client envoie un message de démarrage à un point d'accès qui demande en retour l'identité du client.
- 2. **Réponse** : Le client répond avec un paquet de réponses contenant une identité. Le point d'accès envoie le paquet à un serveur d'authentification.
- 3. **Authentification** : Le serveur de type Radius envoie un paquet d'acceptation au point d'accès après consultation de la base de données utilisateur.
- 4. **Autorisation** : Le point d'accès place alors le port client en état autorisé et le trafic est désormais autorisé sur le réseau local.

Téléphonie mobile

- Un téléphone mobile a beaucoup moins tendance à être protégé qu'un ordinateur portable ou de bureau.
- Les utilisateurs de smartphones ne pensent généralement pas que lorsqu'ils surfent sur Internet avec leurs mobiles, ils s'exposent éventuellement à rencontrer par malchance des programmes malveillants tout comme s'ils naviguaient depuis leur ordinateur standard.
- Or, la problématique est la même.
- Toutes les activités sur mobile sont des manipulations qui peuvent s'avérer vulnérables : lire et gérer le courrier électronique, naviguer, télécharger etc.
- Les menaces pèsent ,de la même manière sur le système d'exploitation du téléphone, les applications, les informations personnelles, les contacts etc.
- Les effets sont les mêmes : perte de données, fichiers corrompus, transmission illicite d'information privées, dégradation matérielle (batterie).

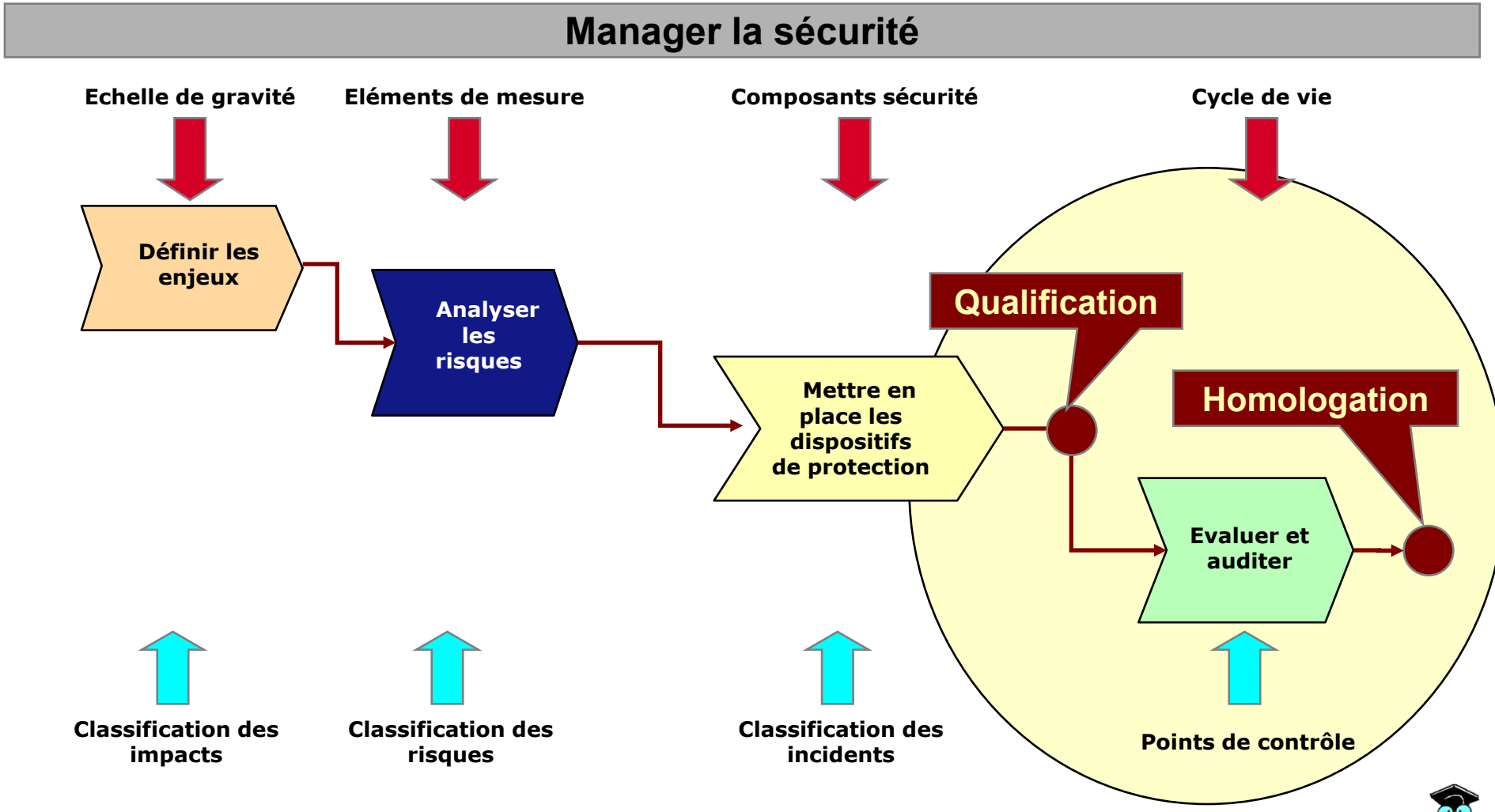
Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - ***C10 Evaluer la sécurité***
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- ***B. Les méthodes et les outils***
  - ***C10 Evaluer la sécurité***
    - ***Qualifier et auditer la sécurité***
    - *Comportement personnel. Principes essentiels et bonnes pratiques.*

Evaluer la sécurité



Un jalon, une étape

- **Jalon de qualification :** Dans ce jalon il s'agit de conduire la qualification (validation de l'organisation et de l'architecture) du système qui résulte de deux approches :
  - la première est qualitative;
  - la seconde est démonstrative au travers de l'étude des scénarios applicables.
- **Etape d'évaluation/audit :** l'évaluation doit être à la fois périodique (mise en place initiale et révision périodique proprement dite) et permanente (exploitation du retour d'expérience et de la veille technologique).

Approche qualitative de qualification

- Cette approche formelle vise à vérifier le respect des principes de la défense en profondeur définis en amont.
- Elle vérifie aussi le respect de la méthode telle qu'elle peut être formalisée au niveau de l'organisme.
- Cette partie s'apparente donc à une démarche qualité.
- Elle est très proche de l'objectif de la norme ISO 15408 (critères communs) qui vise à démontrer la complétude des objectifs de sécurité au regard des menaces retenues.

Approche démonstrative de qualification

- La méthode de qualification doit être cohérente avec la méthode globale de défense en profondeur telle qu'elle a été construite et en particulier s'appuyer sur les résultats produits au cours des différentes étapes.
- Elle utilise donc deux méthodes démonstratives d'analyse qui sont :
  - **l'analyse par scénario "enveloppe"** : cette analyse consiste à établir un scénario couvrant le risque maximum (la destruction du site principal) et de montrer que les autres scénarios (impossibilité de rentrer dans le site principal par exemple) sont inclus dans le cas "enveloppe" et donc que la solution retenue les couvre. Cette approche permet de vérifier la cohérence du nombre de barrières avec la gravité de l'événement redouté ;
  - **l'analyse par "composant défaillant".** Il s'agit de postuler un incident de sécurité et une défaillance aléatoire d'un autre composant situé entre l'incident et l'événement redouté pour analyser la protection restante et vérifier qu'elle est suffisante.

Etape d'évaluation

- Cette étape a pour objet d'évaluer la défense de manière systématique :
  - étude statique des composants ;
  - dynamique sur incident (retour d'expérience) ;
  - tableau de bord ;
  - audit périodique ;
  - rétroaction.
- Cette étape est étroitement liée à la suivante car elle participe au même but, actualiser la défense et la renforcer en prenant deux critères essentiels pour les cas non quantifiables en terme de coût/gain :
  - ne pas régresser ;
  - améliorer si le coût en vaut la peine.

Etape d'évaluation

- Les résultats de cette étape doivent permettre de présenter aux décideurs les mesures prises pour satisfaire aux besoins de sécurité définis à l'étape #1 et démontrer ainsi que les objectifs sont bien atteints.
- Un effort de communication est à effectuer lors cette étape pour regrouper les scénarios par famille et mettre en évidence les principales lignes de défense ainsi que les mesures planifiées de réactions prévues.
- Cette étape s'inscrit dans le cycle de vie du système, et à ce titre elle doit en prendre en compte les opérations de maintien en condition opérationnelle lié à des évolutions des organisations, des technologies et des procédures.
- Cette étape peut déboucher sur une décision d'homologation de sécurité permettant de déclarer le système d'information, apte à traiter d'information d'un niveau de sensibilité donné.
- Cette homologation est intimement liée au cycle de vie du système et n'est jamais une décision permanente.

Audit de sécurité

- L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système.
- L'analyse des informations des dispositifs IDS/IPS permet de détecter d'éventuelles intrusions.
- Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi.
- Les différents évènements du système d'information sont enregistrés dans des journaux d'audit qui devront être analysés fréquemment, voire en permanence.
- Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

Audit de sécurité

- Les informations à collecter :
  - Informations sur les accès au système d'information (qui y a accédé, quand et comment ?) ;
  - Informations sur l'usage fait des serveurs (utilisation du processeur, de la mémoire ou des entrées/sorties) ;
  - Informations sur l'usage fait des fichiers ;
  - Informations relatives à chaque application (lancement ou arrêt des différents modules, variables d'entrée et de sortie et différentes commandes exécutées) ;
  - Informations sur les violations éventuelles de la sécurité (tentatives de commandes non autorisées) ;
  - Informations statistiques sur les systèmes d'exploitation.
- Notons que ces nombreuses informations occupent beaucoup de place et sont très longues à analyser.

Plan

- ***B. Les méthodes et les outils***
  - ***C10 Evaluer la sécurité***
    - *Qualifier et auditer la sécurité*
    - ***Comportement personnel. Principes essentiels et bonnes pratiques***

Principes essentiels pour les utilisateurs

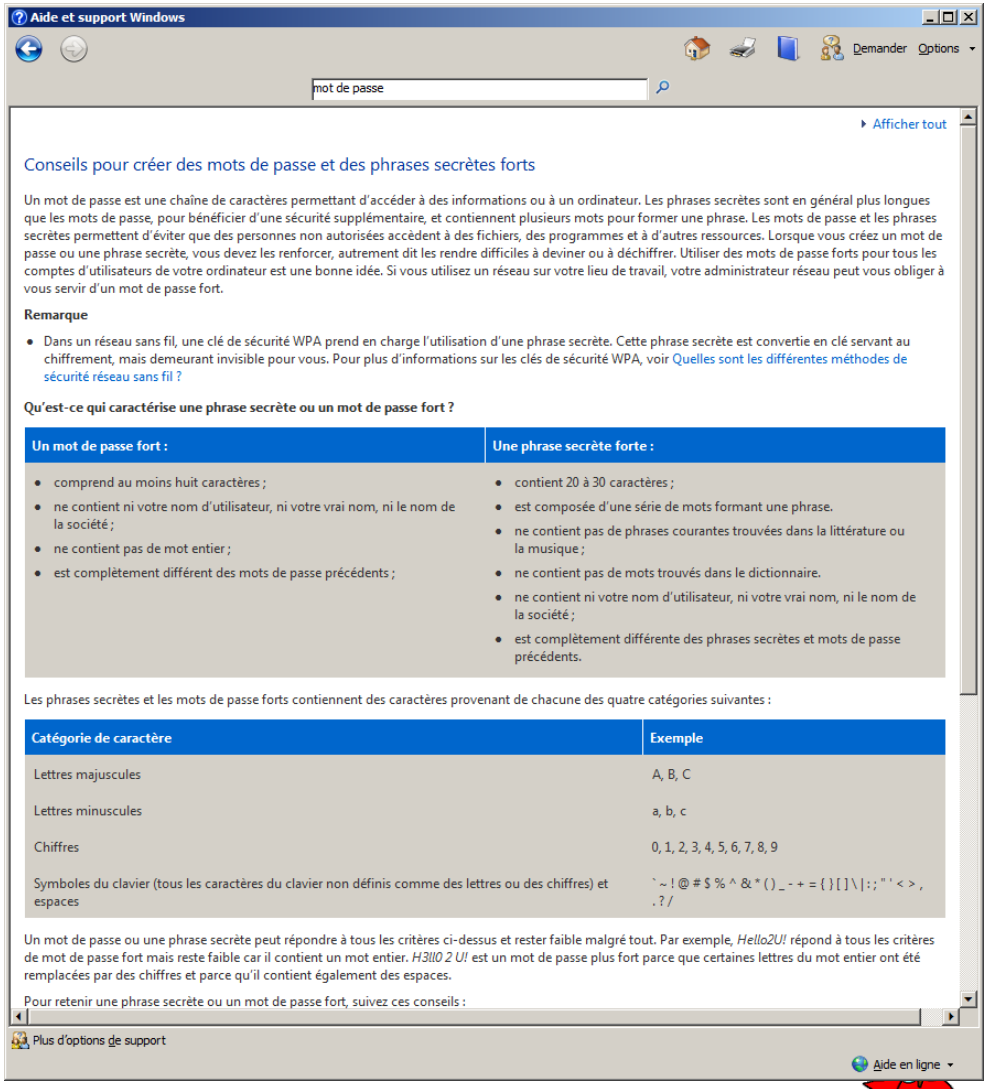
- Choisir un bon mot de passe
- Faire les mises à jour de sécurité et avoir un antivirus à jour
- Effectuer les sauvegardes régulières
- Bien configurer son navigateur
- Naviguer prudemment sur l'Internet
- Télécharger prudemment
- Se méfier de l'hameçonnage (phishing)
- Ne jamais relayer les canulars par messagerie

Choisir un bon mot de passe

- La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant.
- Un mot de passe composé de caractères minuscules, majuscules, chiffres et caractères spéciaux sera de meilleure qualité qu'un mot de passe composé uniquement de minuscules.
- Un mot de passe long et ne comportant pas de mots du dictionnaire peut être difficile à retenir, et sera souvent inscrit sur un bout de papier à côté du poste, ce qui pourrait compromettre la sécurité de celui-ci dans un environnement partagé.
- Ne jamais mettre en place de protocole de création de mot de passe, car si ce protocole est découvert, tous les mots de passe générés deviennent vulnérables, et donc les informations qu'ils protégent aussi.

Choisir un bon mot de passe

- Les conseils dans Windows :
- (Tapez « mot de passe » dans Aide et support windows)



Choisir un bon mot de passe

- Il faut donc trouver des moyens mnémotechniques pour fabriquer et retenir facilement de tels mots de passe.
- Exemples
  - Phonétique : "J'ai acheté 3 CD pour cent euros cet après-midi" : ght3CD%E7am ; L SEP
  - Méthode des premières lettres : "Un tiens vaut mieux que deux tu l'auras" : 1tvmQ2tl'A.
- L'utilisation de caractères spéciaux, de chiffres et de majuscules peut être réalisée avec ces deux méthodes.

Faire les mises à jour de sécurité

- La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels, dites vulnérabilités).
- En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire.
- C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.

Effectuer les sauvegardes régulières

- Sauvegarder, c'est mettre en lieu sûr des informations pour les récupérer en cas de besoin.
- Le meilleur moyen de ne pas perdre ses données est d'avoir toujours au moins une copie en lieu sûr, appelée sauvegarde.
- Il est primordial d'effectuer régulièrement des sauvegardes.
- La fréquence des sauvegardes dépend de la quantité de données que vous acceptez de perdre en cas de destruction de vos données.
- Sauvegarder c'est bien, mais l'important c'est de pouvoir récupérer les données (les restaurer).

Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - ***C11 Manager les risques dans les projets SI***
- ***C. Bilan et perspectives***

Plan

- **B. Les méthodes et les outils**
  - **Manager les risques dans les projets SI**
    - **Nature des risques dans un projet SI**
    - *Typologie des risques projet*
    - *Analyse quantitative du risque*
    - *Analyse qualitative du risque*
    - *Maîtriser le risque projet*
    - *Le coût de la sécurité*

Nature des risques dans un projet SI

- Le risque est « *la possibilité qu'un projet ne s'exécute pas conformément aux prévisions de date d'achèvement, de coût et de spécifications* », ces écarts par rapport aux prévisions étant considérés comme difficilement acceptables voire inacceptables.
- Cette prise en compte du risque peut s'effectuer lors de la définition du projet ou en cours d'exécution du projet.
- La fiabilité du système d'information est devenue un élément clef.
- Ce système est composé d'éléments physiques matériels et humains, donc de composants vulnérables aux dangers que nous évoquions dans la première partie.
- La gestion des risques dans le contexte d'un projet implique d'anticiper le déroulement des activités pour recenser tout événement, aléatoire ou non, susceptible d'en affecter leur réalisation, de dégrader la qualité des performances, des coûts et des délais et/ou de remettre en cause les objectifs du dit projet.

Nature des risques dans un projet SI

Facteur humain

Management déficient

Planification utopique

Risques externes force majeure

Méthodologie inadéquate

Problèmes de trésorerie

Contrôles insuffisants

Difficultés juridiques (propriété, contrat, ..)

Remises en cause trop fréquentes et non maîtrisées

Problèmes sur matériels, logiciels

Plan

- ***B. Les méthodes et les outils***
  - ***Manager les risques dans les projets SI***
    - *Nature des risques dans un projet SI*
    - ***Typologie des risques projet***
    - *Analyse quantitative du risque*
    - *Analyse qualitative du risque*
    - *Maîtriser le risque projet*
    - *Le coût de la sécurité*

Typologie des risques dans un projet SI

- **Les risques génériques :**
  - Risques d'expression des besoins et leur spécification,
  - Risques de stratégie de développement,
  - Risques d'organisation de projet,
  - Risques d'interfaces contractuelles,
  - Risques de conduite de projet,
  - Risques de gestion financière du projet,
  - Risques de gestion calendaire du projet,
  - Risques de performances techniques et opérationnelles,
  - Risques liés aux utilisateurs et aux sites d'exploitation ;
- **Les risques de retard :**
  - Risques liés à l'historique des consultations et des réponses,
  - Risques liés à l'évolutivité des spécifications des lots de travaux ;
- **Les risques de surcoût**
  - Risques liés à la nature et la propriété des lots de travaux,
  - Risques liés à l'enchaînement et la durée des lots du chemin critique

Exemple des risques de conduite de projet

N°	Facteur de risque	Risque consécutif direct
1	Absence de gestion de projet	*Mauvaise connaissance des états financiers et calendaires et des dérives associées*
2	Absence de plan de management de projet, AQ, SdF, ...	*Absence de certitude que les objectifs associés à l'activité ont bien été compris et que les méthodes et moyens humains et matériels mis en place sont en cohérence avec ces objectifs*
3	Retard ou absence de décision	*Arrêt ou dérive d'activité*
4	Absence de réunions de coordination ou d'avancement (= absence d'informations transverses formalisées)	*Incohérence des activités projet* *Mauvaise communication sur l'état des composantes du projet*
5	Absence ou mauvaise identification des activités critiques	*Non mise en place de mesures particulières d'évaluation et de maîtrise des risques*
6	Absence de jalons ou de revues	*Non possibilité de minimiser les problèmes potentiels avant passage à une nouvelle phase*
7	Absence de gestion du suivi des actions	*Non garantie de leur prise en compte*
8	Absence ou mauvaise répercution et suivi d'actions	*Non prise en compte nominale par les destinataires*
9	Absence ou mauvais contrôle de la disponibilité des données d'entrées de la phase	*Non respect du plan de développement*
10	Développement dépendant de fournitures externes (= avancement non maîtrisé)	*Remise en cause de la définition technique et du plan de développement*
12	Indisponibilité des fournitures externes (équipes et/ou moyens d'essais...)	*Non respect du plan de développement*

***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

Typologie des risques dans un projet SI

- On définit ensuite une échelle de **gravité** :
  - Mineur,
  - Significatif,
  - Grave,
  - Critique,
  - Catastrophique
- une échelle de **vraisemblance** :
  - Impossible,
  - Très peu probable,
  - Peu probable,
  - Probable,
  - Très probable
  - Certain
- et des classes d'**acceptabilité** :
  - Accepté en l'état,
  - Tolérable sous contrôle
  - Inacceptable
- dans un repère (vraisemblance, gravité).
- Cette approche permet de définir une véritable cartographie des risques d'un projet.

Plan

- ***B. Les méthodes et les outils***
  - ***Manager les risques dans les projets SI***
    - *Nature des risques dans un projet SI*
    - *Typologie des risques projet*
    - ***Analyse quantitative du risque***
    - *Analyse qualitative du risque*
    - *Maîtriser le risque projet*
    - *Le coût de la sécurité*

Analyse quantitative du risque

- Une première approche s'appuie sur le calcul des probabilités et repose sur une vision stochastique du problème.
- Elle vise à quantifier la dispersion de la réalisation prévisionnelle d'un objectif quantifié de durée (risque-délai) ou de coût (risque-coût).
- Prenons l'exemple du risque-délai.
- On affecte à la variable « durée » de chaque tâche du chemin une loi de distribution théorique ou empirique (par exemple la loi normale).
- L'espérance mathématique de la loi qui régit la durée totale du projet se calcule comme la somme des espérances mathématiques des durées de chaque tâche du chemin critique.
- La connaissance de la loi de la durée du projet permet de calculer des intervalles de confiance ou la probabilité qu'une durée donnée soit dépassée.

Analyse quantitative du risque

- On peut aussi utiliser des méthodes de simulation sur la base d'un scénario privilégié pour chacune des tâches (Méthode de Monte-Carlo).
- Ceci permet d'explorer plusieurs ordonnancements combinant des scénarios différents.
- On aboutit ainsi à une analyse probabiliste de la durée du projet ou à la mesure de la probabilité qu'une tâche a d'être critique.
- En raison de la complexité de l'approche, ces méthodes intéressent essentiellement les grands projets au sein de grandes organisations.

Plan

- **B. Les méthodes et les outils**
  - **Manager les risques dans les projets SI**
    - Nature des risques dans un projet SI
    - Typologie des risques projet
    - Gérer le risque projet
    - Analyse quantitative du risque
    - **Analyse qualitative du risque**
    - Maîtriser le risque projet
    - Le coût de la sécurité

Analyse qualitative du risque

- L'analyse qualitative vise à mieux comprendre les causes possibles de dérapage des délais et donc de mieux prévenir ou de réagir.
- Elle tente de structurer le raisonnement à l'aide de listes de contrôle (check-list) qui permettent un diagnostic plus rapide et plus sûr.
- Aussi, la conduite d'un projet passe par une phase de préparation (Étapes 1 à 3) au cours de laquelle le travail à exécuter est techniquement défini, sur la base d'un certain nombre d'hypothèses de travail, et un ordonnancement arrêté, puis par la phase de réalisation (Étapes 4 et 5) au cours de laquelle développement et déploiement sont mis en œuvre.
- Les problèmes rencontrés en cours d'exécution peuvent conduire à une révision de l'analyse du projet et de ce fait à une itération sur la phase de préparation.

Risques encourus en phase de préparation

- Certains risques sont encourus lors de la phase prévisionnelle, lorsque le responsable du projet et son équipe définissent le travail à exécuter et les ressources à mettre en œuvre.
- Selon la typologie connue, certains de ces risques sont **endogènes** :
  - Mauvaise identification des enjeux du projet ;
  - Mauvaise définition des objectifs du projet ;
  - Incohérence du cahier des charges ;
  - Définition imprécise des tâches ;
  - Mauvaise estimation des charges de travail ;
  - Affectation de ressources incompétentes ou indisponibles ;
  - Inexistence d'une structure d'arbitrage ;
  - Absence de maîtrise du processus de pilotage.
- D'autres sont **exogènes** :
  - Demande sujette à une certaine obsolescence (réglementaire, technique, commerciale) ;
  - Choix d'une technologie qui va être prochainement dépassée ;
  - Modification des attentes des usagers/clients :
  - Modification de facteurs habituellement stables (législation, règles comptables.....).

Risques encourus en phase d'exécution

- En cours d'exécution du projet, des événements défavorables (prévus ou non) peuvent compromettre les objectifs du projet. Les risques encourus tiennent à :
  - une **détection tardive du problème** : pour opérer un bon diagnostic, il faut, disposer rapidement des bonnes informations et les traiter correctement et en temps utile ;
  - un **diagnostic erroné** : l'analyse d'informations récentes et partielles peut amener à surestimer ou à sous-estimer un problème. Un diagnostic peut être erroné parce ce que le phénomène redouté n'a pas l'ampleur perçue. Mais très souvent l'erreur de diagnostic porte sur l'interprétation des faits.
  - une **réaction inappropriée** : la réponse retenue peut être inappropriée si elle repose sur une logique locale, parce qu'elle reporte le problème sur des tiers ou qu'elle ne fait que temporiser en repoussant à plus tard des solutions qui s'imposent mais implique des conflits ouverts.

Plan

- **B. Les méthodes et les outils**
  - **Manager les risques dans les projets SI**
    - *Nature des risques dans un projet SI*
    - *Typologie des risques projet*
    - *Analyse quantitative du risque*
    - *Analyse qualitative du risque*
    - **Maîtriser le risque projet**
    - *Le coût de la sécurité*

Maîtriser le risque projet

- Les actions envisageables différent selon les étapes du projet.
  - En phase d'élaboration (Identification et faisabilité, analyse des scénarios, étude détaillée) des stratégies de diminution peuvent être mises en œuvre.
  - En phase d'exécution (Réalisation et déploiement) la gestion du risque passe par une organisation de la réactivité.

La diminution du risque en phase de préparation

- Les actions envisageables :
  - **Amélioration du niveau de l'information** : Le nombre, la qualité et la pertinence des informations relatives aux tâches restant à exécuter s'améliorent au fur et à mesure que le projet avance ;
  - **Externalisation des risques** : Elle consiste à définir précisément quels sont les risques que l'organisation accepte d'assumer elle-même et ceux qu'elle désire transférer sur d'autres agents économiques.

L'organisation de la réactivité en phase d'exécution

- **Réactivité** : capacité à modifier rapidement le périmètre et les autres éléments caractéristiques du projet pour tenir compte d'informations nouvelles remettant en cause de manière significative des hypothèses de travail (ressources disponibles, contenu des tâches, liens entre les tâches et délai admissible d'exécution du projet) sur lesquelles la planification courante est fondée.
- Les actions envisageables :
  - Modification de certaines caractéristiques du projet ;
  - Adaptation aux dérives constatées : Le chef de projet peut réagir aux imprévus :
    - En réajustant les objectifs qu'on s'était fixés initialement, afin qu'ils restent réalistes (dates des jalons, nature des livrables, niveau de qualité, coût du projet),
    - En mobilisant momentanément des ressources additionnelles (internes et/ou externes) ;
  - Réactivité organisationnelle : le chef de projet (ou le comité de pilotage en cas de carence du chef de projet) peut adapter les structures existantes pour qu'elles deviennent plus efficaces :
    - en mettant en place une véritable structure de pilotage du projet, avec des procédures de circulation de l'information fiables et rapides,
    - en développant les compétences en matière de maîtrise du risque,
    - en créant une véritable dynamique de groupe.

Plan

- **B. Les méthodes et les outils**
  - **Manager les risques dans les projets SI**
    - *Nature des risques dans un projet SI*
    - *Typologie des risques projet*
    - *Analyse quantitative du risque*
    - *Analyse qualitative du risque*
    - *Maîtriser le risque projet*
    - **Le coût de la sécurité**

Le coût de la sécurité

- La mise en place d'un projet PKI peut coûter de 500 k€ (quelques centaines d'utilisateurs) à 10 000 K€ (plusieurs dizaines de milliers d'utilisateurs, services étendus, haute disponibilité, vente de certificats à des clients et partenaires externes).
- Les postes de coût d'un tel projet sont intéressants à analyser car ils permettent de lister des composants qui se retrouvent à plus ou moins grande échelle dans tout projet de déploiement d'une solution de sécurité.

Le coût de la sécurité

Nature des coûts	Composant
Investissements	Etude préalable (Opportunité, Faisabilité, Scénarios, étude détaillée)
	Définition des processus
	Matériel (serveurs, supports pour le stockage des clefs privées et des certificats : Hardware Security Module, cartes à puces, jetons –token- sur port USB, …)
	Logiciel spécialisé (Module d'enregistrement, Module de certification, Online Certificate Status Protocol OCSP, annuaire, horodatage)
	Intégration
	Sécurisation des locaux (sécurité physique)
	Audit sécurité et certification
	Pilote
	Déploiement
Coûts exploitation	Maintenance (matériel + logiciel)
	Exploitation informatique
	licences logiciels
	Renouvellement cartes et jetons
	Back office (enregistrements, révocations, renouvellement)
	Support utilisateurs

So cyberspace is real. And so are the risks that come with it.

In short, America's economic prosperity in the 21st century will depend on cybersecurity.

Barack Obama
Président des Etats-Unis

Avons-nous atteint nos objectifs ?

- *Comme tous les progrès technologiques, depuis l'aube de l'humanité, les réseaux informatiques ouverts en général et l'Internet en particulier représentent à la fois des opportunités et des menaces.*
- *Ce sont des opportunités pour s'ouvrir sur le monde, pour trouver l'information pertinente ou le partenaire attendu, pour présenter les produits et les services proposés par l'entreprise, pour acheter au meilleur prix.*
- *Ce sont aussi des menaces directement liées à l'ouverture. La progression des attaques est en croissance exponentielle et celles-ci sont de plus en plus virulentes.*
- *La protection des réseaux est plus que jamais à l'ordre du jour, particulièrement dans le secteur des établissements financiers.*

Avons-nous atteint nos objectifs ?

- *Quels sont les principaux risques qui pèsent sur les systèmes d 'information ?*
  - Risques exogènes et endogènes
  - Accidents : Accidents physiques, Pannes et dysfonctionnements, Force majeure, Pertes de services essentiels
  - Erreurs à la conception, au développement, au déploiement et en exploitation
  - Malveillance : Vols et vandalisme, Fraude, Sabotage, Attaques logiques, Divulgations
  - Autres : les attaquants ont beaucoup d'imagination et savent méler divers modes d'attaque au sein de véritables opérations de cyberguerre.

Avons-nous atteint nos objectifs ?

- *Quels sont les différents aspects de la sécurité des systèmes d 'information ?*
  - Assurance de la disponibilité des données et des application
  - Assurance de l'intégrité des processus et des données
  - Respect de la confidentialité
  - Assurance du contrôle de la preuve et de la non répudiation des transactions et des échanges
- *Quelle actions en matière de sécurité doit conduire la DSI ?*
  - Actions au niveau physique (protection des locaux et des accès, protection des réseaux (pare-feux, RPV), mise en place de solutions de sauvegarde et de reprise, etc.)
  - Actions au niveau logique (mots de passe, chiffrement, PKI, etc.)
  - Actions de motivation du personnel
  - Plan de Reprise Informatique et Plan de Continuité des Activités
  - Organiser une défense multi-niveaux en profondeur