CHAPITRE III : Les Cyberattaques et les Outils de sécurité.

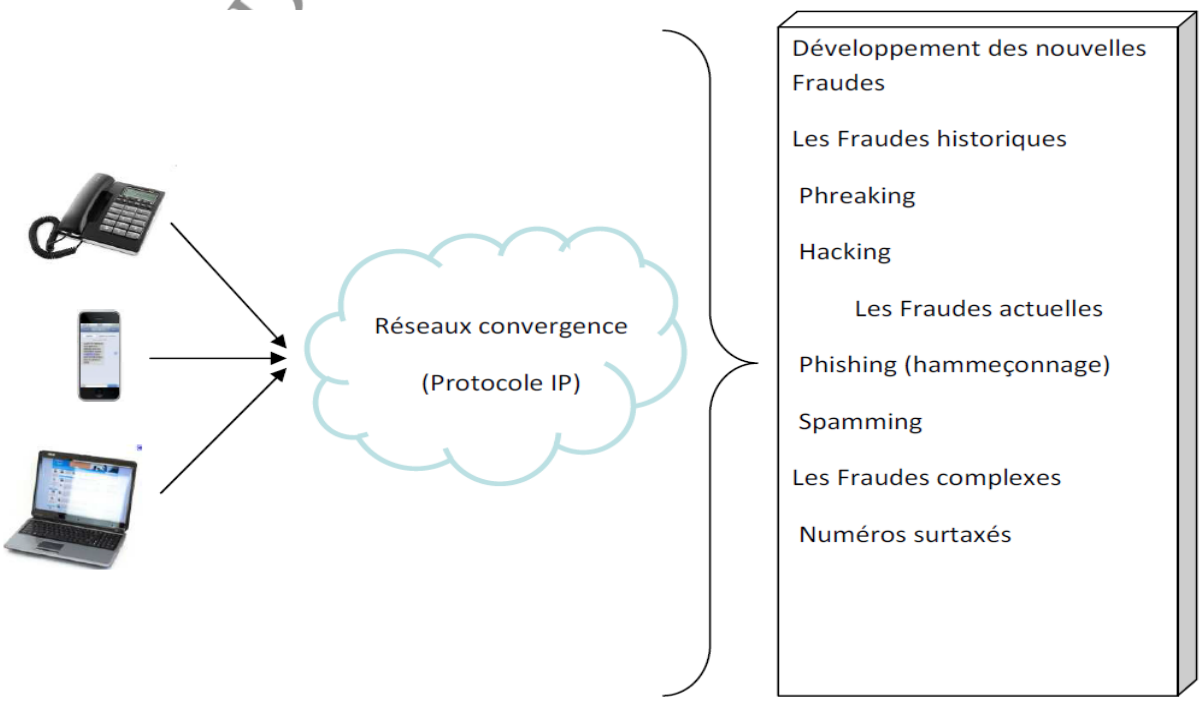
I. INTRODUCTION

D'après l'étude mondiale de **PwC** « Global Economic Crime Survey 2011» «le classement d'un crime ou d'un incident en tant que cybercriminalité varie d'un individu ou d'une entreprise à l'autre. Peu importe la catégorie dans laquelle on les affecte (i.e. crime économique, espionnage, activisme), les cyber-attaques représentent 23% des incidents pour les entreprises ayant déclaré avoir été victime de criminalité économique au cours de ces dernières années. Parmi les impacts de ces attaques, les entreprises considèrent que celui lié à leur réputation est le plus important (40%) ; viennent ensuite : la perte (ou le vol) de données personnelles (36%), la perte de propriété intellectuelle (incluant la perte de données industrielles) à 35%, l'interruption de service pour 34%, la perte financière effective pour 31% et le risque réglementaire pour 22% ».

Ainsi, l'avènement des nouvelles technologies durant ces dernières années au sein de la société internationale a induit le développement de nouvelles formes de délinquance dont les conséquences doivent être largement prises en compte par les entreprises et notamment par les opérateurs de communications électroniques. Si chacun s'accorde à percevoir le risque externe comme le plus fréquent, en revanche ils prennent de plus en plus conscience de la menace interne.

II. Les menaces cybercriminelles externes aux entreprises de communications électroniques.

La convergence des réseaux de télécommunications, de l'Internet (prenant appui sur la communication IP (Internet protocole) et l'ingénierie informatique) est exploitée par les cybercriminels afin de commettre leurs actes délictueux. Le développement de leurs activités se concentre notamment autour de trois familles de fraudes: les fraudes historiques ou indémodables, les fraudes actuelles et les fraudes complexes. Seules les fraudes les plus significatives seront envisagées dans cette étude.



A) Les fraudes historiques ou indémodables.

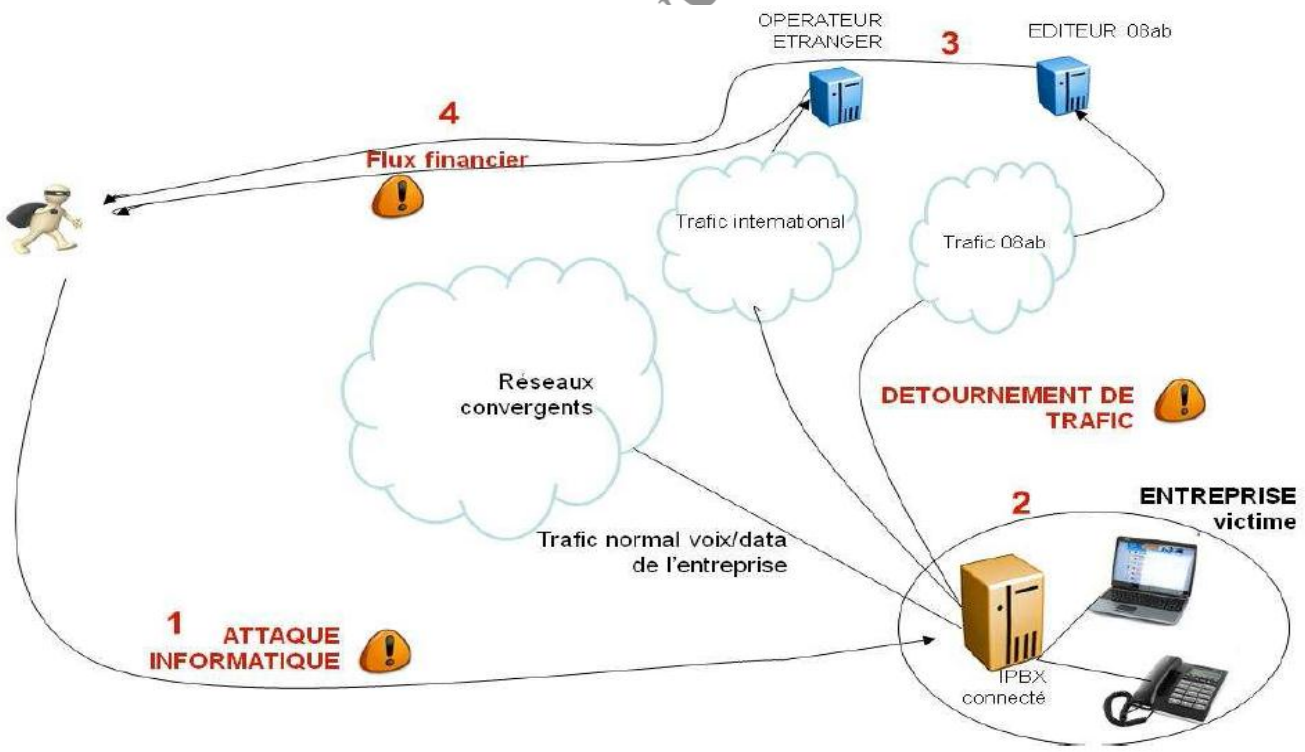
1) Le Phreaking

Le **phreaking** est le piratage de systèmes de téléphonie filaire ou sans-fil. Le terme provient d'une contraction entre les termes anglais « phone », pour téléphone, et « freak », signifiant marginal, ou personne appartenant à une contre-culture. Initialement, le phreaking consistait à mettre en place des moyens pour contourner la facturation des usages téléphoniques. Cette fraude est également utilisée pour établir des communications anonymes ou écouter des conversations téléphoniques. L'exemple typique de **phreaking** consiste à se brancher sur la ligne téléphonique d'un tiers afin de passer, au moyen de sa ligne téléphonique, des communications à l'insu de celui-ci et lui faire supporter le coût de ces communications.

2) Le Hacking

Le hacking regroupe un ensemble de techniques exploitant des failles et vulnérabilités d'un élément ou d'un groupe d'éléments d'un système d'information. Il correspond à l'utilisation de connaissances informatiques à des fins illégales.

Exemple de hacking permettant une fraude au Phreaking : le Piratage d'IPBX



1. Attaque informatique du fraudeur, via Internet pour prendre le contrôle distant de l'IPBX de l'entreprise (serveur téléphonique et Internet de l'entreprise).
2. Utilisation de l'IPBX, pour détourner les appels téléphoniques aux profits du fraudeur : pour appeler (au compte de l'entreprise) des opérateurs étrangers et des numéros surtaxés. L'entreprise est utilisée comme une «cabine téléphonique».
3. SFR reverse aux opérateurs étrangers et aux éditeurs de numéros surtaxés leurs parts du prix des communications passées et factures l'entreprise desdites communications.
4. Le fraudeur récupère de l'opérateur étranger ou/et l'éditeur 08ab une partie des bénéfices de la fraude.

Les victimes directes du hacking sont les abonnés et clients de l'opérateur, qui se voient pirater leurs box, installations informatiques et téléphoniques d'entreprises. L'opérateur est une victime indirecte, dans la mesure où le hacking de ses abonnés et clients permet aux fraudeurs de commettre, par ricochet, d'autres agissements préjudiciables (par exemple, le **phreaking**).

B) Les fraudes actuelles

1) Le spamming

Le **spamming** est l'envoi d'un même message électronique non-sollicité à un très grand nombre de destinataires au risque de les importuner. L'acte de spamming, a pour conséquence de saturer un serveur de mails.
En outre, le spamming, pour être réalisé, nécessite la collecte frauduleuse des données à caractère personnel des destinataires: adresses mails, numéro de téléphone fixe ou mobile.

a. *Le spam courriel*

Le spam courriel est principalement utilisé à des fins publicitaires, d'hameçonnage ou de propagation de virus. C'est une pratique consistant à envoyer en masse des e-mails publicitaires à des personnes ne souhaitant pas les recevoir. Ces e-mails font fréquemment la promotion illicite de produits pharmaceutiques, de sites pornographiques ou de sites de jeux.

b. Le Spam SMS

Le spammeur envoie un message SMS non-sollicité qui invite à appeler un numéro surtaxé (08ab) ou à renvoyer un SMS surtaxé (SMS+).
A titre d'exemple, des utilisateurs peuvent recevoir sur leur mobile le spam suivant:« Répondeur MMS: (1) nouveau message vidéo; a 15:37.\nCsqdq cliquez sur le lien pour déclencher sa lecture: http://video-sms.com/5/632323224 \nAcces Gratuit».

c. Le Spam vocal

Le **spam vocal** (ou « **ping call** ») consiste à appeler un numéro fixe ou mobile depuis un numéro surtaxé et à raccrocher au bout d'une ou deux sonneries, avant que l'appelé n'ait eu le temps de décrocher. Lorsque l'appelant rappelle le numéro indiqué, qui se trouve être un numéro surtaxé, il est alors facturé d'un coût forfaitaire par appel et d'un coût en fonction de la durée de l'appel, sans contrepartie d'un service.

2) Le phishing ou hameçonnage

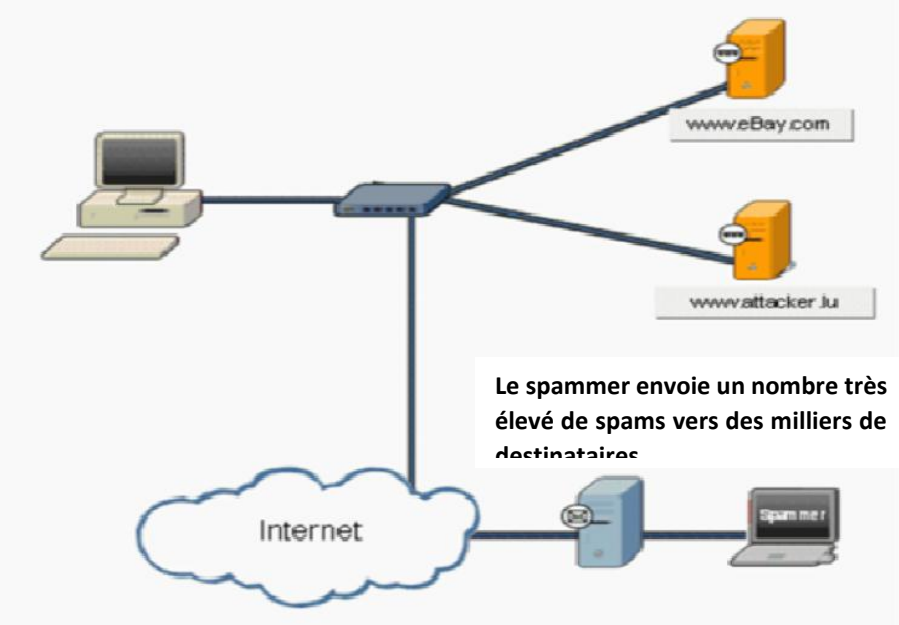
Le **phishing**, est une technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales37connues et réputées. Cette technique peut prendre plusieurs formes: site web, mails et SMS, appels vocaux, et avoirs des objectifs multiples.

a. *Le mode opératoire des phishers*

Ils envoient des courriels en très grand nombre, à l'aide d'automates informatiques. Les adresses des victimes sont généralement collectées illégalement ou forgées à partir de données d'annuaires publics ou de portails sociaux. Les emails reprennent les logos et les typographies officiels de l'entreprise phishée et demandent à l'internaute de cliquer sur un lien hypertexte inclus dans le message. L'adresse URL du lien dans l'email est «travaillée» afin de paraître la plus authentique possible. Les courriels amènent les

internautes sur un site frauduleux imitant parfaitement le site web phishé. Ce site frauduleux est très souvent hébergé de manière illégale sur un serveur préalablement piraté par l'attaquant. Le site frauduleux présente des pages web incitant la victime à saisir des données personnelles et confidentielles.

b. Phishing sur Internet

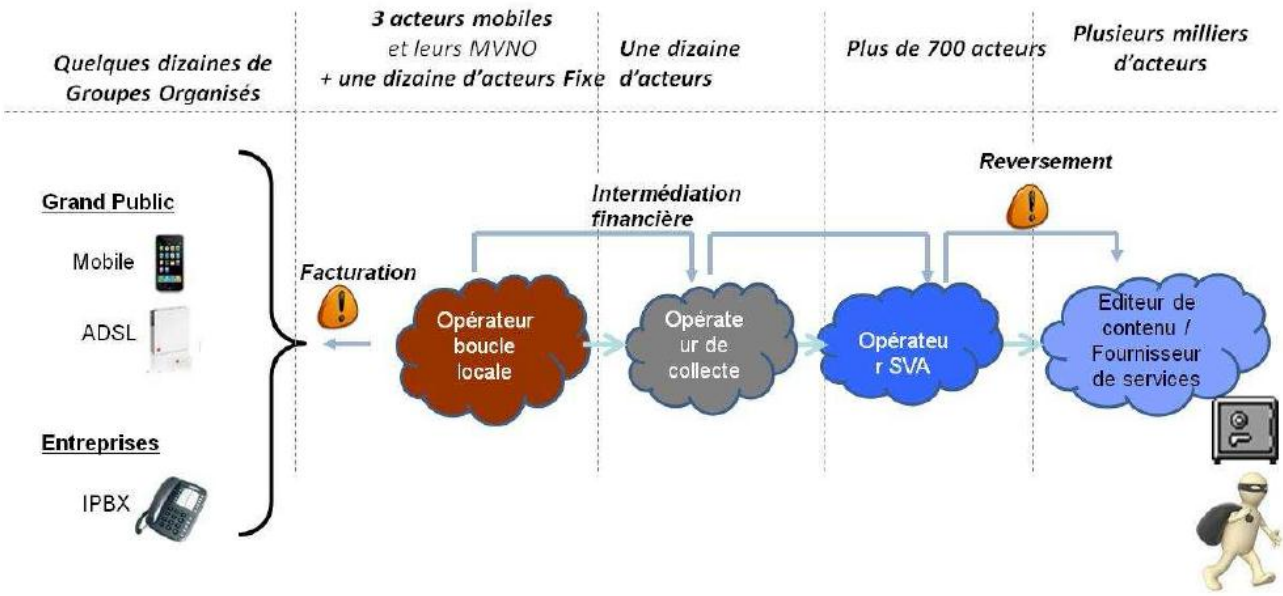


c. Le phishing SMS

«Le titulaire du 06XXXXXXXX Gagne le Cheque No 1111 Composez le 0899XXXXXX pour le retirer. Jeu sous Contrôle **d'Huissier\sdfsttp://stopsms.mobi».**
Les victimes directes du phishing sont les abonnés et clients de l'opérateur, dont les données personnelles seront utilisées par les fraudeurs. L'opérateur est une victime directe lorsque le fraudeur usurpe son identité, afin de commettre ses agissements.
Afin de collecter les adresses mails, des robots sont programmés pour récupérer les données apparaissant sur des forums. Ces emails reprennent les logos et typographies officiels de l'entreprise Phishée et demandent à l'internaute de cliquer sur un lien URL hypertexte inclus dans le message. L'adresse URL du lien dans l'email est « travaillée» afin de paraître la plus authentique possible.
Par exemple: **http://www.sfr.com**
www.azefdvdf.net constituant la balise html créant un lien hypertext et permettant d'accéder au site frauduleux.
http://www.sfr.com étant le lien vu par l'internaute et qui le trompe.

C) Les fraudes complexes: l'exemple de la fraude aux numéros surtaxés

En pratique, la fraude consiste à appeler en masse des numéros surtaxés en piratant une ligne de l'appelant, générant ainsi un préjudice financier pour la victime (client ou opérateur), et un revenu «in-shore» ou «off-shore» pour le fraudeur. Les appels sont passés à l'aide de détournement de cartes SIM, piratage de box, ping call, détournement d'IPBX…



III. Les FAILLES DE SECURITE DES APPLICATIONS WEB : PRINCIPES, PARADES ET BONNES PRATIQUES DE DEVELOPPEMENT

Le **WASC** établie dans son rapport « WASC Threat Classification » une liste exhaustive des menaces qui pèsent sur la sécurité des applications Web. Elles sont regroupées dans six catégories.

- La catégorie « **authentification** » regroupe les attaques de sites Web dont la cible est le système de validation de l'identité d'un utilisateur, d'un service ou d'une application.
- La catégorie « **autorisation** » couvre l'ensemble des attaques de sites Web dont la cible est le système de vérification des droits d'un utilisateur, d'un service ou d'une application pour effectuer une action dans l'application.
- La catégorie « **attaques côté client** » rassemble les attaques visant l'utilisateur pendant qu'il utilise l'application.
- La catégorie « **exécution de commandes** » englobe toutes les attaques qui permettent d'exécuter des commandes sur un des composants de l'architecture du site Web.
- La catégorie « **révélation d'informations** » définit l'ensemble des attaques permettant de découvrir des informations ou des fonctionnalités cachées.
- La catégorie « **attaques logiques** » caractérise les attaques qui utilisent les processus applicatifs (système de changement de mot de passe, système de création de compte, …) à des fins hostiles.

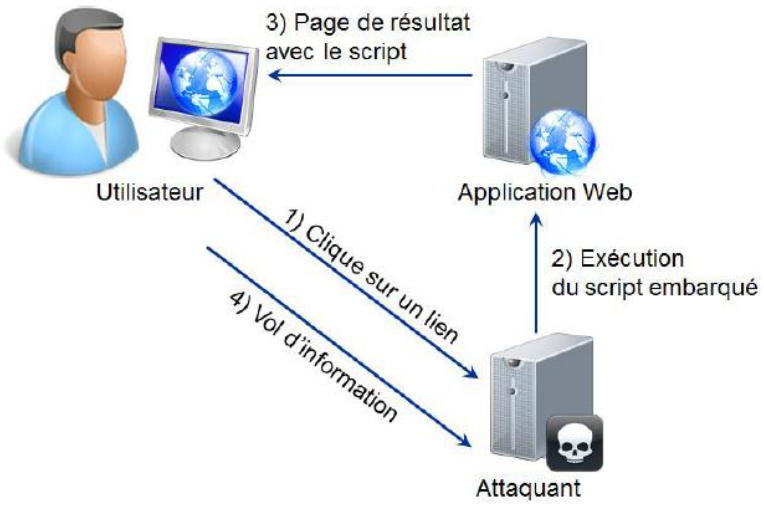
1) L'attaque par injection

Pour réaliser une attaque de ce type, il faut injecter dans les zones de saisie classiques présentées à l'utilisateur du code malicieux. Ces données seront interprétées comme des instructions par un des composants de l'application Web. Cela permet par exemple d'usurper une identité pour se connecter à une application Web, de rendre l'application inutilisable ou de supprimer toutes les données de la table visée, voire même de la base de données complète.

2) Le Cross-Site Scripting (XSS)

Cette attaque s'appuie principalement sur les formulaires des applications Web. Les victimes sont les utilisateurs des applications Web vulnérables.

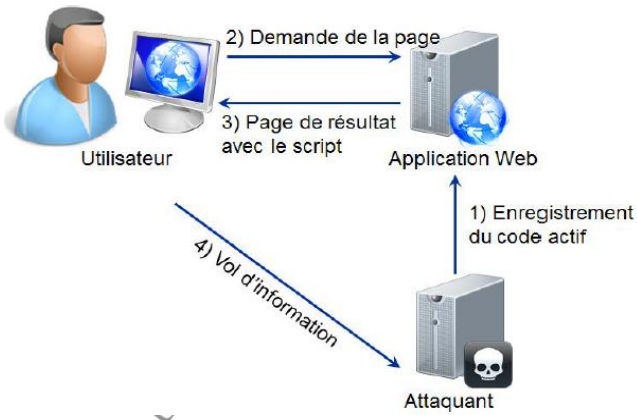
L'attaque XSS par réflexion (reflected XSS) s'appuie sur le fait que l'application Web affiche ce que l'utilisateur vient de saisir dans un formulaire dans une page de résultat. Le navigateur de la victime exécute alors le code frauduleux généré dans la page de résultat. Tous les champs de formulaire sont donc une faille de sécurité potentielle que l'attaquant peut exploiter par XSS. L'attaquant crée un lien déguisé vers l'application Web dont un des paramètres contient du code JavaScript frauduleux. En utilisant ce lien, la victime fait exécuter par son navigateur le code JavaScript.



Principe d'une attaque XSS par réflexion

3) L'Attaque XSS stockée (stored XSS)

L'attaque XSS stockée (stored XSS) s'appuie sur le fait que l'attaquant réussisse à stocker dans la base de données du code frauduleux qui sera exécuté par la victime lorsqu'elle tentera d'afficher la donnée malveillante. Cette attaque est plus dangereuse que la première car le code fait partie intégrante des données de l'application Web et peut atteindre plusieurs victimes.



Principe d'une attaque XSS stockée

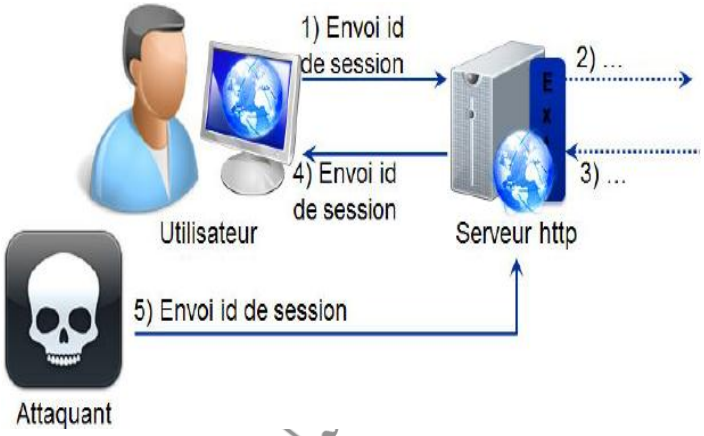
4) La Violation de gestion d'authentification et de session

Cette faille de sécurité regroupe toutes les vulnérabilités pouvant mener à une usurpation d'identité. Cela peut donc leur permettre de voler des informations ou d'endommager le bon fonctionnement de l'application. La protection des accès à l'application repose généralement sur un système d'authentification. Parmi les attaques contre les systèmes d'authentification, la plus répandue est l'utilisation de la force brute.

Pour comprendre comment les attaques peuvent être menées, il faut comprendre le mécanisme d'authentification le plus commun des applications Web.

a) L'utilisateur non authentifié demande l'accès à une page Web ;
b) Le serveur renvoie une page d'authentification ;
c) L'utilisateur rempli le formulaire en fournissant un identifiant et un mot de passe et revoie ces informations au serveur web ;
d) Le serveur web fait appel à un service pour vérifier la validité du couple identifiant/mot de passe
e) Si la validité est avérée, le serveur web fournit un identifiant de session à l'utilisateur. Comme expliqué précédemment http est un protocole déconnecté, donc entre deux requêtes http la connexion

entre le navigateur et le serveur http est coupée. Donc le serveur http ne peut pas reconnaître un utilisateur qui s'est déjà authentifié et ouvert une session de travail dans l'application Web. Pour remédier à cela, la plupart des systèmes d'authentification repose sur un identifiant de session. Celui-ci est envoyé à chaque page entre le client et le serveur par le biais d'un cookie, d'un paramètre d'adresse ou d'un champ de formulaire invisible pour l'utilisateur ;



f) L'utilisateur peut utiliser l'application Web tant que la session est ouverte.

Les attaques pour usurper une identité peuvent être regroupées en deux catégories :

- Les attaques contre le système d'authentification qui cherchent à obtenir un droit d'accès ;
- Les usurpations de session qui permettent de s'affranchir de l'étape d'authentification.

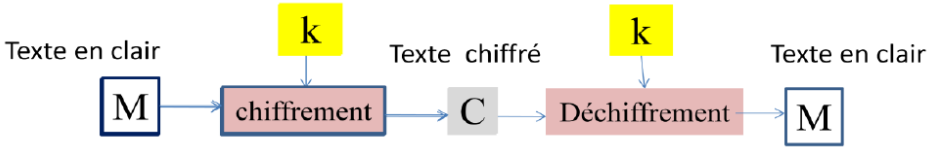
Principe de détournement de session

IV. Les Outils de la sécurité

Assurer la sécurité des informations, des services, des systèmes et des réseaux consiste à réaliser la disponibilité, l'intégrité, la confidentialité des ressources ainsi que la non-répudiation de certaines actions, ou l'authenticité d'évènements ou de ressources.
La sécurité des informations n'a de sens que si elle s'applique sur des données et des processus dont on est sûr de l'exactitude (notion de qualité des données et des processus) afin qu'ils soient pérennes dans le temps (notion de pérennité des données et de continuité des services).
Les principales solutions de sécurité se basent sur la mise en œuvre de techniques de chiffrement, d'isolation d'environnements, sur la redondance des ressources, sur des procédures de surveillance, de contrôle, de gestion des incidents, de maintenance, de contrôle d'accès ou de gestion de systèmes.

A) Chiffrement des données

La mise en œuvre de techniques de chiffrement permet de réaliser la confidentialité des données, de vérifier leur intégrité et d'authentifier des entités.
Il existe deux grands types de système de chiffrement de données: le chiffrement symétrique (à clé secrète) et le chiffrement asymétrique (à clé publique).



Texte en clair : c'est le message à protéger (à chiffrer).
Texte chiffré : (cryptogramme) , c'est le résultat du chiffrement du texte en clair.
Chiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
Déchiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
Clé : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

Cryptosystème : algorithmes + clés

Cryptographie : cette branche regroupe l'ensemble des méthodes (algorithmes) qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer.

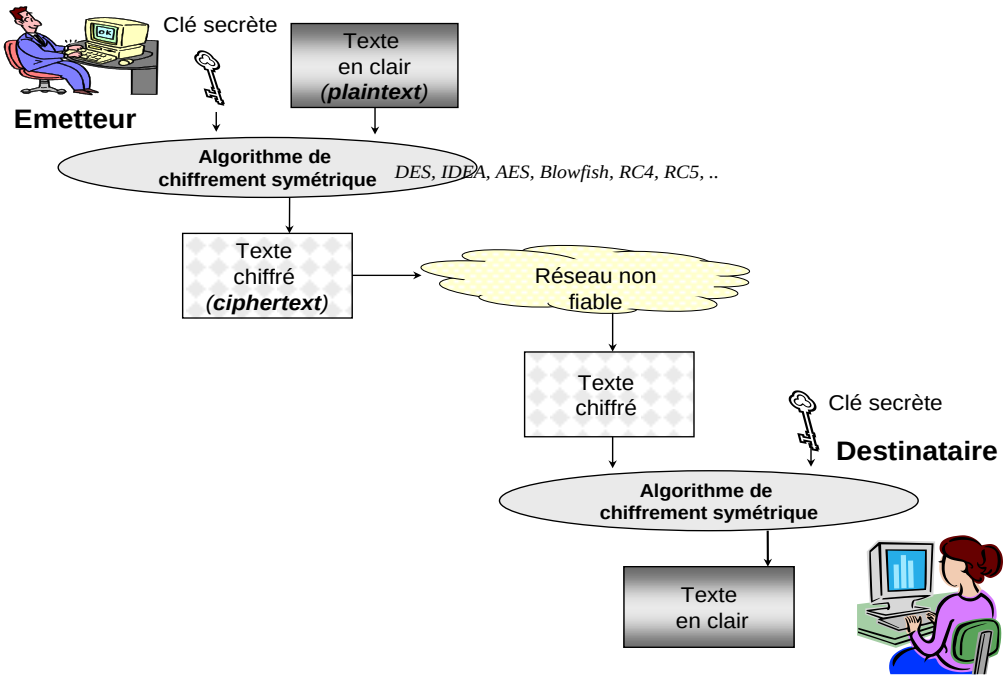
Cryptanalyse : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.

Cryptologie : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.

1) Chiffrement symétrique

Pour chiffrer ou déchiffrer un texte, il faut détenir une clé et à un algorithme de chiffrement. S'il s'agit de la même clé pour effectuer ces deux opérations, le système de chiffrement est qualifié de symétrique. L'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre, ceci qui pose le problème de la gestion et de la diffusion des clés secrètes.

Dans la **cryptographie symétrique**, la clé de chiffrement est la même que la clé de déchiffrement. De ce fait, la clé doit être un secret partagé uniquement entre l'émetteur et le destinataire. Il existe plusieurs algorithmes qui fonctionnent sur ce principe : **DES, RC4, RC5, Blowfish, IDEA, AES, ….**



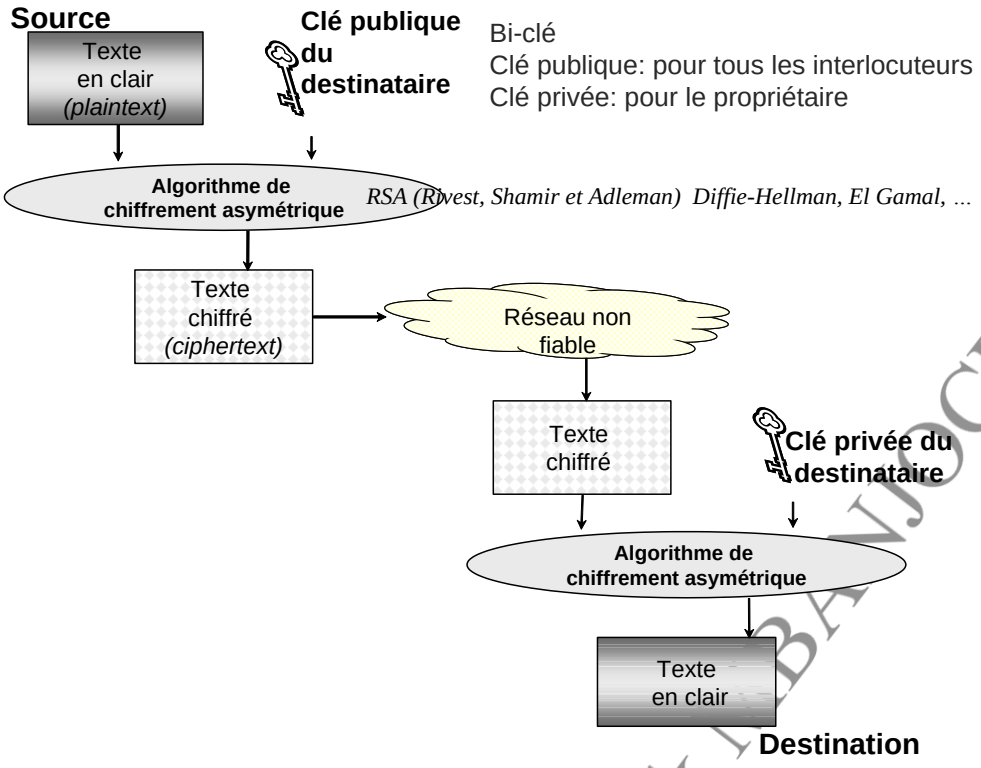
Le chiffrement symétrique

2) Chiffrement asymétrique ou à clé publique

Un **système de chiffrement asymétrique** est basé sur l'usage d'un couple unique de deux clés, calculées l'une par rapport à l'autre. Cette bi-clé est constituée d'une clé publique et d'une clé privée. Seule la clé dite publique peut être connue de tous, tandis que la clé privée doit être confidentielle et traitée comme un secret. L'émetteur chiffre un message avec la clé publique du destinataire du message et le destinataire le déchiffre avec sa clé privée.

Dans la cryptographie asymétrique, la clé de chiffrement n"est pas la même que la clé de déchiffrement.

Les algorithmes les plus connus sont : RSA, Diffie-Hellman, El Gamal.



3) Les Clés de chiffrement

Une clé de chiffrement est le secret du secret. Les clés secrètes des systèmes de chiffrement, doivent être gérées de manière confidentielle. La sécurité du processus de chiffrement, repose en grande partie sur la confidentialité et la longueur des clés utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.

4) L'Infrastructure de gestion de clés

Une infrastructure de gestion de clés – IGC, (PKI – *Public Key Infrastructure*) permet de mettre en œuvre des systèmes de chiffrement asymétrique. Les principales fonctions supportées sont:

- la génération d'un couple unique de clés (clé privée – clé publique), son attribution à une entité et la sauvegarde des informations nécessaires à sa gestion, archivage des clés, procédures de recouvrement en cas de perte par l'utilisateur ou de demande de mise à disposition par les autorités judiciaires;
- la gestion des certificats numériques, création, signature, émission, validation, révocation, renouvellement des certificats;
- la diffusion des clés publiques aux ressources qui la solliciteraient et qui seraient habilitées à l'obtenir;
- la certification des clés publiques (signature des certificats numériques).

Les limites inhérentes aux infrastructures de gestion de clés résident dans:

- la complexité, le coût du déploiement et de la gestion d'une infrastructure;
- le haut niveau de sécurité nécessaire à la réalisation des services des infrastructures de gestion de clés;

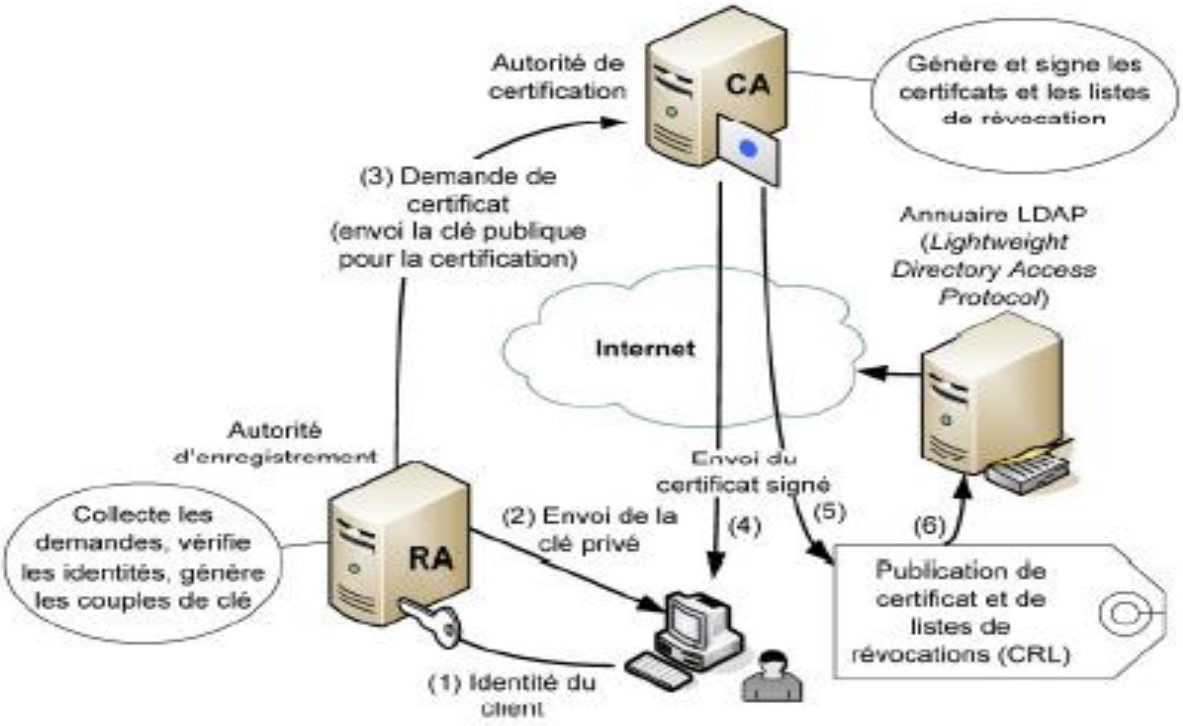
- la validité, la durée de vie, la résiliation des certificats.

- **Problème technologique**: les systèmes de chiffrement classiques peuvent être cassés, certains certificats numériques n'ont aucune valeur sécuritaire et ne garantissent rien.
- **Problème politique**: la majorité des infrastructures PKI – Autorités de certification, appartient à des entités américaines (USA).
- **Problème organisationnel**: interopérabilité des infrastructures, déploiement, gestion, maintenance, sécurité, complexité, etc.

Une **PKI** est constituée des éléments suivants :

- Une ***autorité d'enregistrement*** ou **RA** (*Register Authority*) qui a pour rôle d'authentifier chaque nouveau participant (ceux-ci doivent présenter des informations prouvant leur identité).
  - ***Le participant*** peut alors générer par son intermédiaire une paire de clés publique/privée (il peut aussi générer lui-même sa paire de clés et joindre directement sa clé publique à sa demande de certificat au CA).
- ***Une autorité de certification*** ou **CA** (*Certification Authority*) qui crée et signe les certificats avec l'identité du participant, sa clé publique, une date d'expiration et sa propre signature.
  - La CA fournit une copie de sa propre clé publique au participant.
  - Muni de son certificat et de la clé publique de la **CA**, le nouveau participant peut communiquer avec tous les autres participants certifiés par la même **CA** (la **RA** peut être intégrée à la CA).
- Des **annuaires** de certificats.

Les clés publiques des principales CA sont mémorisées dans les navigateurs et ne nécessitent pas d'installation de la part des usagers.



Architecture d'une PKI

5) Signature et authentification

Un émetteur chiffre avec sa clé privée un message. Toute entité connaissant la clé publique de cet émetteur déchiffrera le message, ce qui validera le fait qu'il a bien été créé à l'aide de la clé privée correspondante.
Un document peut être signé électroniquement (notion de signature numérique) via un algorithme de chiffrement à clé publique. Les actions suivantes sont alors réalisées:

- création d'un message de déclaration d'identité qui est la signature (ex. «Je m'appelle Alpha Tango Charlie») qui est chiffrée avec la clé privée de l'émetteur et associée au message à transmettre;
- le message et sa signature sont chiffrés avec la clé publique du destinataire et transmis;
- le destinataire déchiffre le message avec sa clé privée et détache la signature qu'il déchiffre avec la clé publique de l'émetteur.

6) Intégrité des données

Vérifier que les données n'ont pas été modifiées lors de leur transfert est possible en y associant un résumé (condensé) qui est émis en même tant que les données. Celui-ci est le résultat d'une fonction de calcul appliquée aux données. Le destinataire recalcule avec la même fonction la valeur du résumé à partir de données reçues. Si la valeur obtenue diffère, il en déduit que les données ont été modifiées. Le résumé peut être lui-même chiffré avant que les données ne soient émises ou stockées.

Pour un contrôle d'intégrité plus performant, on applique au message original une fonction le transformant en une petite suite aléatoire de bits qui constitue en quelque sorte son empreinte digitale (*digest – résumé – condensé*).
Une fonction dite fonction *digest* (ou *one-way hash function*), génère un message *digest*, c'est-à-dire son empreinte digitale, plus courte que le message original et incompréhensible. Celle-ci est ensuite chiffrée avec la clé privée de l'émetteur et associée au message à transmettre. Sur réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur puis, recalcule à partir du message reçu avec la même fonction *hash*, l'empreinte et la compare ensuite avec celle reçue. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

7) La Non-répudiation

Le service de non-répudiation consiste à prévenir le refus, le démenti qu'un message ait été émis ou reçu ou qu'une action, transaction ait eu lieu. Cela permet de prouver par exemple qu'une entité est liée à une action ou à un événement.
La non-répudiation est basée sur une signature unique ou sur une identification qui prouve qui a créé le message. Pour assurer ce service, on peut faire appel à un algorithme de chiffrement à clé publique. On peut également avoir recours à un tiers de confiance pour lui faire jouer un rôle de **cybernotaire**.

B) Les Protocoles de Sécurité

1. Le Protocole IPv6

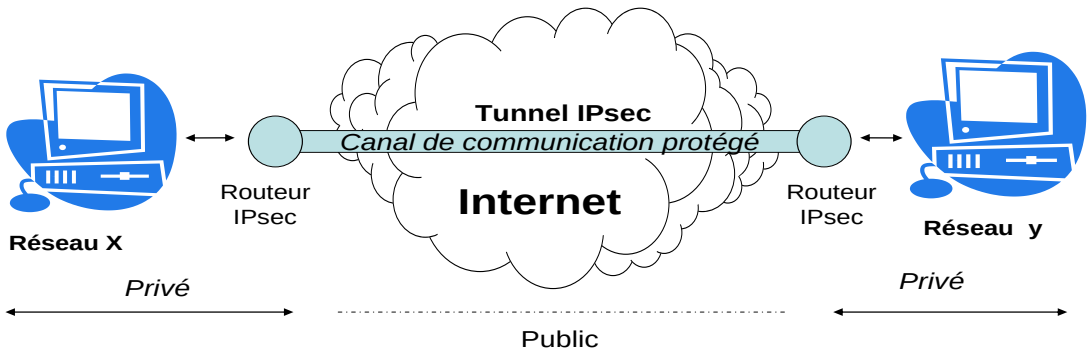
La version 6 du protocole IP (IPv6) inclut des facilités d'authentification et de confidentialité.
Les principales évolutions d'IPv6 par rapport à IPv4 portent sur les points suivants [RFC 2460]:

- le support d'un adressage étendu et hiérarchisé; les adresses sont codées sur 128 bits (16 octets) et non plus sur 32 bits (4 octets); la représentation des adresses s'effectue en nombres hexadécimaux séparés par des deux points tous les 2 octets et non plus en notation décimale pointée; (exemple: 0123:4567:89ab:cdef:0123:4567:89ab:cdef);
- la possibilité de pouvoir faire de l'allocation dynamique de bande passante pour le support d'applications multimédias;
- la capacité à créer des réseaux IP virtuels;
- le support de procédures d'authentification et de chiffrement, via des en-tête à options;
- la simplification des en-têtes des paquets afin de faciliter et accélérer le routage.

2. Le Protocole IPSec

IPSec permet de rendre confidentiel le contenu des paquets véhiculés par le protocole. IPSec propose des services de confidentialité et d'authentification des données au niveau de leur transfert par le protocole IP, via l'implantation de l'en-tête d'extension d'authentification (*Authentication Header* [AH]) ou de l'en-tête de confidentialité – authentification (*Encapsulating Security Payload Header* [ESP]).

L'en-tête d'authentification (AH) offre des services d'authentification et d'intégrité des paquets IP. Cela permet de garantir que les données n'ont pas pu être modifiées lors de leur transfert et que l'adresse source est bien celle qui figure sur le paquet.
L'en-tête d'*Encapsulating Security Payload* (ESP) permet la réalisation de mécanismes de chiffrement (chiffrement symétrique comme DES, Triple DES, RC5 ou IDEA) et propose des services d'authentification similaires à ceux proposés par l'*Authentication Header* (AH).



Constitution d'un réseau privé virtuel par un canal de communication IPsec

3. Les Protocoles de sécurité SSL (Secure Sockets Layer) et S-HTTP (Secure HTTP)

SSL (*Secure Sockets Layer*) est un logiciel assurant la sécurité des échanges applicatifs, qui est d'ailleurs supporté par la majorité des navigateurs web du marché.

Les deux entités communicantes d'une connexion SSL s'authentifient en faisant appel à une procédure de certification et à un tiers de confiance. Elles négocient ensuite le niveau de sécurité à appliquer au transfert. Les données transmises sont alors chiffrées pour cette communication via SSL (Figure III.9).
L'implantation de SSL a un fort impact du côté du serveur du fait de la nécessaire certification. Cela implique un dialogue avec une autorité de certification reconnue et demande également que les relais applicatifs des *firewalls* supportent le mode de fonctionnement de SSL. La certification est parfois considérée comme un frein au déploiement de cette solution.
L'extension au protocole **HTTP** (*Secure* HTTP, **S-HTTP**) est une solution alternative développée par l'association CommerceNet. S-HTTP offre les mêmes facilités de sécurité que SSL, avec les mêmes contraintes de certification, mais ne supporte que les flux de données du protocole HTTP.

SSL intervient au-dessus de la couche transport et peut être utilisé pour sécuriser pratiquement n'importe quel protocole utilisant **TCP/IP** (**SMTP, POP3, IMAP**...) en créant un tunnel dans lequel toutes les données échangées seront automatiquement chiffrées.

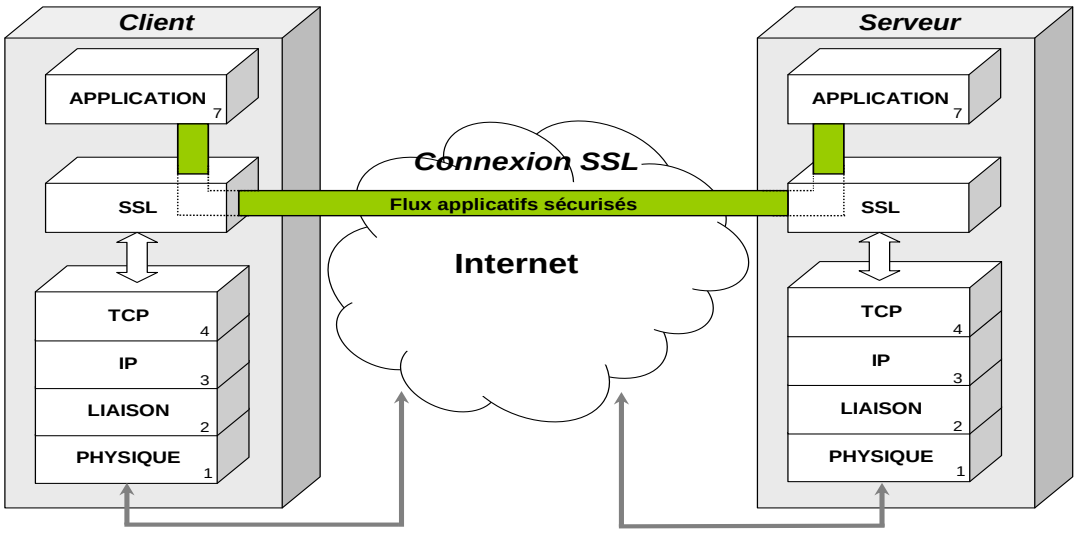
HTTPS (HTTP+SSL) est inclus dans tous les navigateurs et permet par exemple de consulter des comptes bancaires par le web de façon sécurisée.
Les données **HTTP** sont échangées à l'intérieur d'un **tunnel SSL**.
HTTPS utilise le port 443
HTTPS garantit l'intégrité et la confidentialité.
La **non-répudiation** n'est pas établie dans **HTTPS** ;
Seuls les échanges lors de l'établissement de la session **SSL/TLS sont signés**, le reste des données échangées ne l'est pas.

4. La Sécurité de la messagerie électronique et des serveurs de noms

Les risques de sécurité encourus, relatifs à l'usage d'un système de messagerie, sont liés à:

- la perte, l'interception, l'altération, la destruction de messages;
- l'infection des systèmes par le biais de messages contenant des virus, vers ou cheval de Troie;
- l'harcèlement: inondation de messages, junk mail, messages non sollicités (spam) à des personnes dont l'adresse e-mail est utilisée sans leur accord préalable et avec lesquelles l'expéditeur (le spammeur) n'a jamais eu de contact.

- l'usurpation d'identité des utilisateurs (un intrus se fait passer pour quelqu'un d'autre, un élément du système émet, écoute, intercepte des messages qui ne lui sont pas destinés, etc.);
- des messages peuvent être introduits, rejoués, mélangés, supprimés, retardés;
- un refus de service par défection d'un élément de la chaîne du système de messagerie;
- la divulgation d'informations confidentielles;
- la répudiation (un acteur du système nie avoir envoyé ou reçu un message).



5. La Détection d'intrusion

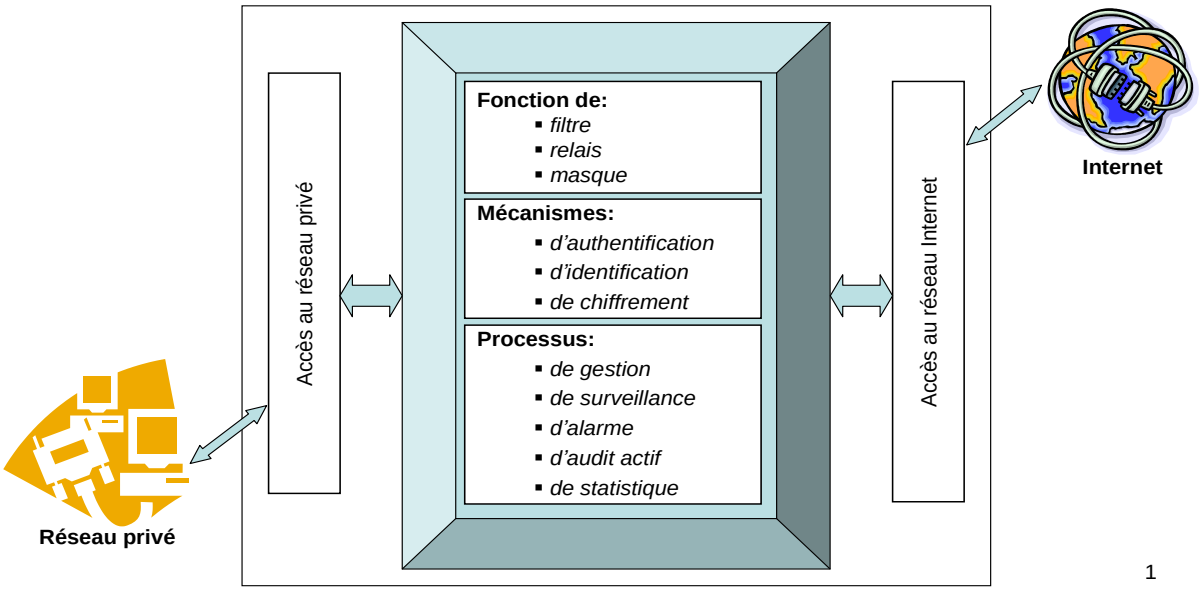
Un incident est un évènement qui survient inopinément. Il est le plus souvent sans gravitée en lui-même mais il peut engendrer des conséquences graves.
Une anomalie est une exception, elle peut induire un fonctionnement anormal du système d'information pouvant conduire à une violation de la politique de sécurité en vigueur. Elle peut être d'origine accidentelle (par exemple une erreur de configuration) ou volontaire (une attaque ciblée du système d'information). Une intrusion est caractéristique d'une attaque et peut être considérée comme un incident ou une anomalie.

La détection d'intrusion est l'ensemble de pratiques et de mécanismes utilisés afin de détecter des erreurs qui pourraient conduire à des violations de la politique de sécurité et de diagnostiquer les intrusions et les attaques (sont inclus la détection d'anomalies et l'usage abusif des ressources).

Un système de détection d'intrusions (**IDS** – *Intrusions Detection System*) se compose de trois blocs fonctionnels essentiels: la collecte des informations, l'analyse des informations récupérées, la détection des intrusions et les réponses à donner à la suite d'une intrusion décelée.

6. Le Cloisonnement des environnements

La séparation et le masquage d'un environnement privé vis-à-vis de l' Internet public repose sur l'installation d'un ou plusieurs systèmes pare-feu (*firewalls*).
Un *firewall* est un système qui permet de bloquer et de filtrer les flux qui lui parviennent, de les analyser et de les autoriser s'ils remplissent certaines conditions, de les rejeter dans le cas contraire. Le cloisonnement d'un réseau permet de constituer des environnements IP disjoints, en rendant physiquement indépendants les accès des réseaux que l'on désire séparer. Cela permet d'interconnecter deux réseaux de niveaux de sécurité différents.
Un *firewall* applicatif encore dénommé proxy (serveur proxy, *firewall proxy*) joue un rôle de relais applicatif. Il établit en lieu et place de l'utilisateur le service invoqué par celui-ci. L'objectif d'un système qualifié de proxy est de réaliser un masquage d'adresse par relais applicatif, et de rendre transparent l'environnement interne de l'organisation.



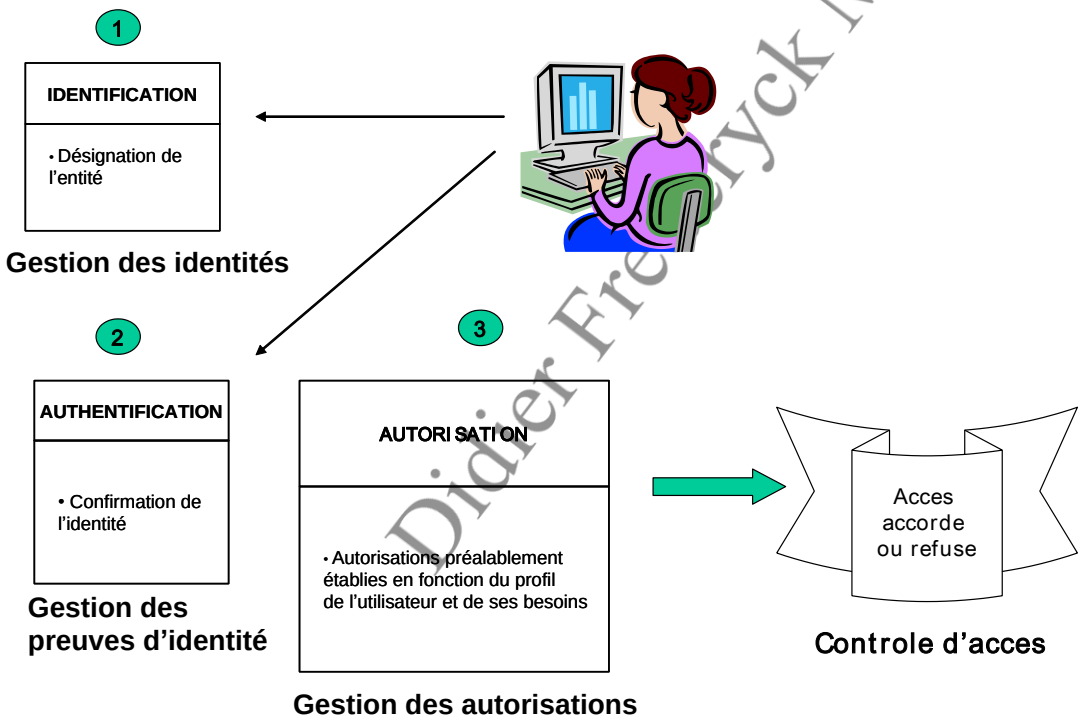
1

Structure fonctionnelle d'un firewall

7. Le Contrôle d'accès

a. Principes généraux

Un mécanisme de contrôle d'accès logique aux ressources informatiques est basé sur l'identification des personnes, leur authentification et sur les permissions ou droits d'accès qui leurs sont accordés.



Sur la base d'une identification authentifiée, le mécanisme de contrôle d'accès accorde, en fonction du profil de l'utilisateur, l'accès aux ressources sollicitées. Cela suppose que l'identification de l'usager (Gestion des identités – *Identity management*), que les preuves de son identité (gestion des preuves de l'identité – *Identity proof management*) et que ses droits d'accès, soient correctement gérés (gestion des autorisations – *Authorization management*).

L'authentification permet de lier la notion d'identité à une personne. Les autorisations d'accès permettent de filtrer sélectivement les demandes d'accès aux ressources et aux services offerts via le réseau afin d'en accorder l'accès qu'aux seules entités habilitées.

b. Apports et limites de la biométrie

L'application de la **biométrie au contrôle d'accès** aux ressources informatiques permettrait de se soustraire de l'usage de mot de passe en les substituant par une caractéristique physique dont on pourrait aisément extraire une donnée binaire.
Afin d'utiliser des caractéristiques physique des personnes pour les identifier et valider leur identification, il est nécessaire d'extraire et d'enregistrer au préalable les caractéristiques biométriques des individus (notion de gabarit). Ces enregistrements doivent être réalisés d'une manière fiable et sauvegardés de façon sécurisée

Les limites de l'usage de données biométriques pour le contrôle d'accès :

- les données biométriques contribuant à identifier un individu varient au cours du temps;
- les données biométriques doivent être saisies pour constituer un échantillon de référence qui sera sauvegardé dans une base de données. En devenant numériques ses données deviennent fragiles (et donc modifiables), elles devront être protégées de manière optimale. A chaque demande d'accès, les données biométriques de l'utilisateur devront être captées. Ceci pose un problème d'acceptation de la méthode de saisie, le sentiment d'intrusion est souvent mal toléré;
- la technique de contrôle d'accès basée sur l'usage du biométrique n'est pas sûre à 100%, du fait de la variabilité de l'échantillon humain dont le processus d'authentification doit tenir compte.