Université Kasdi Merbah Ouargla

Département informatique

Introduction : généralités sur la sécurité informatique et motivations

Master RCS

Octobre 2014

Sommaire

1- Généralités : concepts de base et motivations

- Sécurité des systèmes informatiques
- Diverses sources de menaces
- Objectifs de la sécurité informatique
- Les critères de sécurité informatique

2- Sécurité informatique

- Définition
- Niveaux de sécurisation et domaines d'intervention de la sécurité
- Menaces informatiques
- Motivations des attaques

3- Criminalité informatique

- Crime informatique, cybercrime
- Internet : un facteur aggravant
- Typologie des attaques
- Logiciels malveillants
- Menaces nouvelles

Sommaire

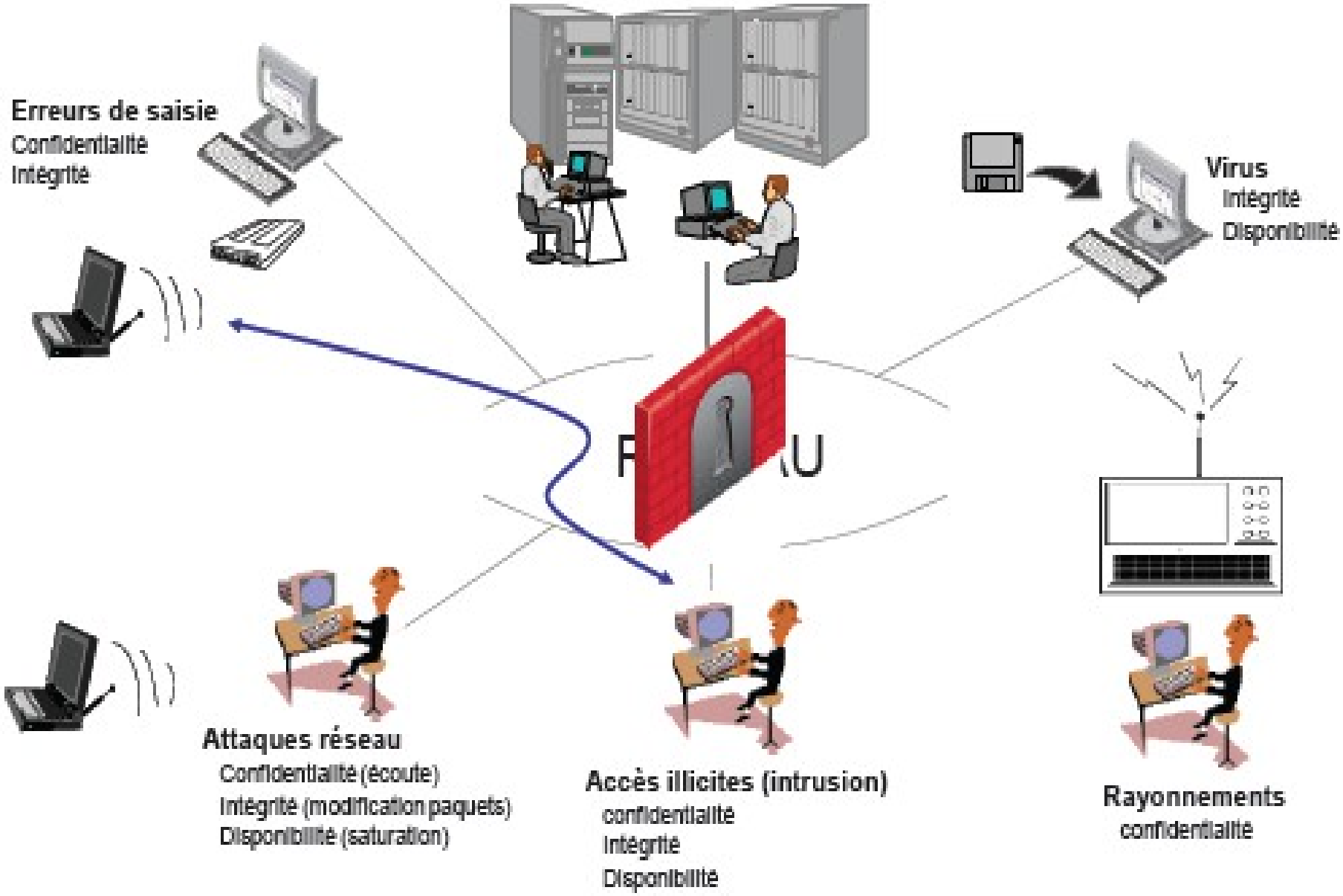
- ***Un système d'information :***
  - organisation des activités consistant à acquérir, stocker, transformer, diffuser, exploiter, gérer ... les informations et produire des services

- Pour faire fonctionner un système d'information, le moyen technique moderne est d'utiliser **un système informatique** (plate forme matériel, logiciel de base (S.E) et des logiciels applicatifs)

La sécurité des systèmes informatiques

- Les systèmes informatiques sont au cœur des systèmes d´information.
- Ils sont devenus la cible de ceux qui convoitent l'information.
- Assurer la sécurité de l'information c'est assurer la sécurité des systèmes informatiques.

Différentes sources des menaces



La sécurité informatique consiste à protéger des systèmes d'information et des services contre les menaces accidentelles ou délibérées touchant la confidentialité, l'intégrité de l'information et la disponibilité des systèmes informatiques et leurs services.

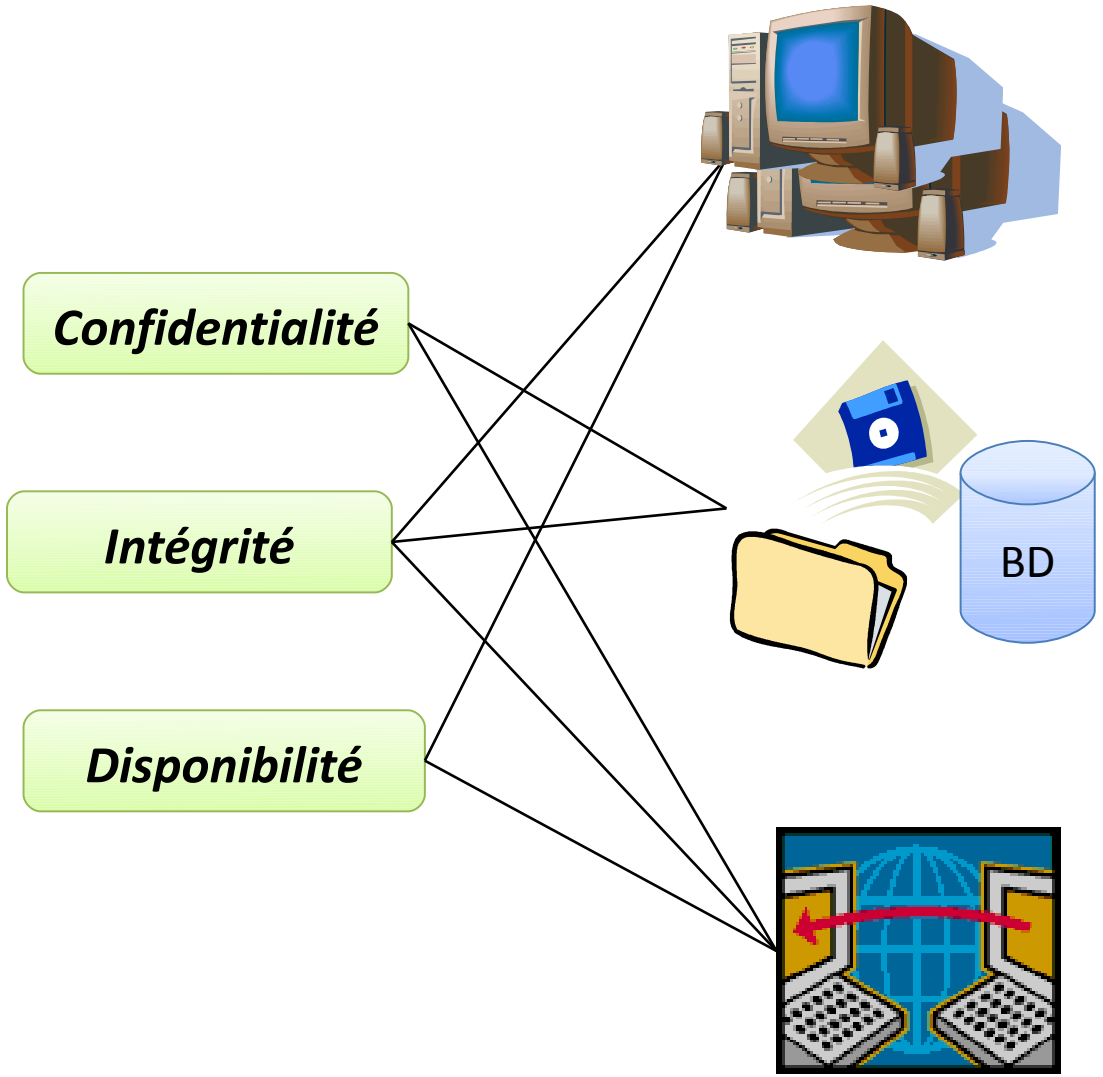
Objectifs de la sécurité informatique

- Les principaux objectifs à garantir:

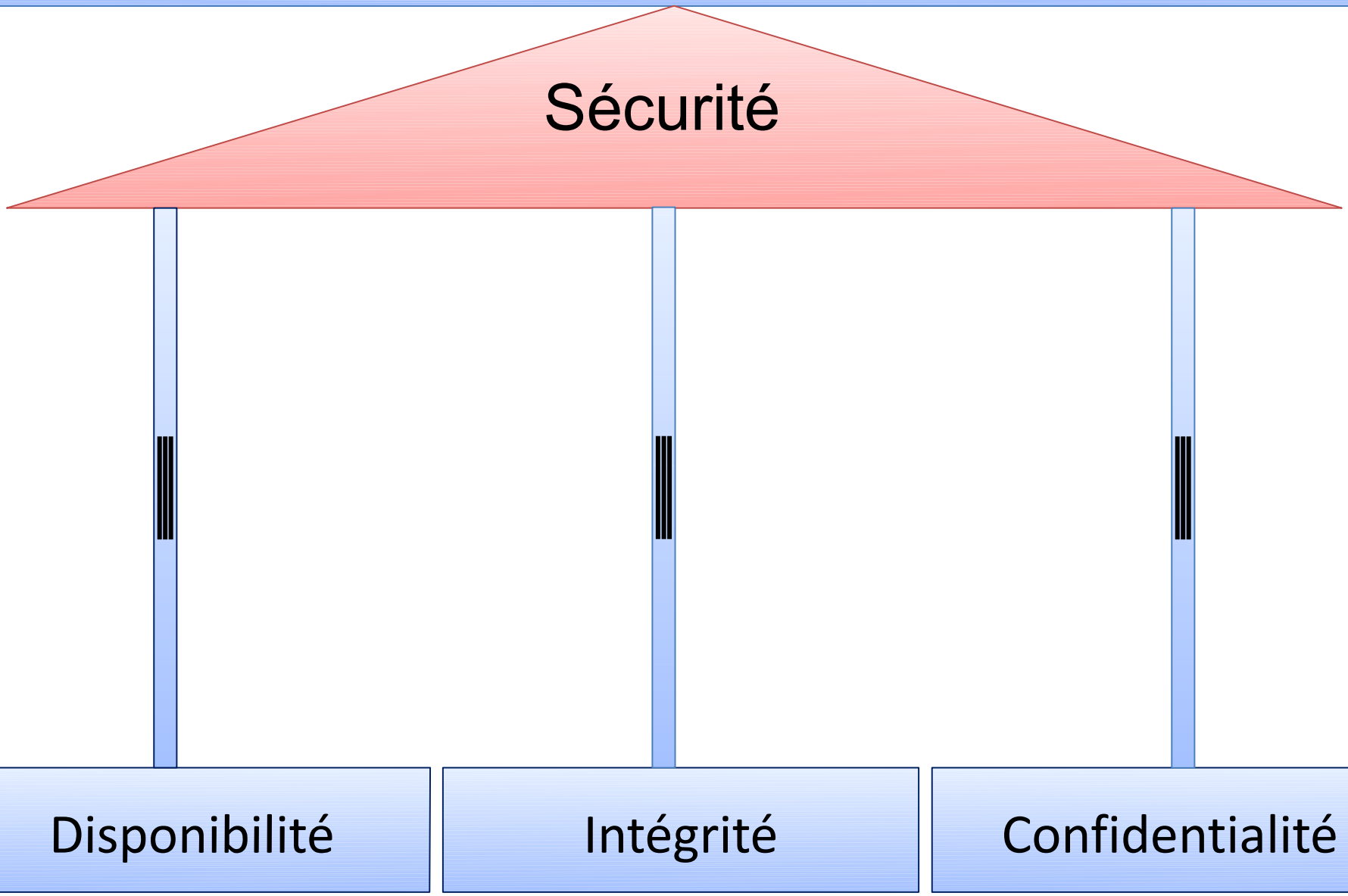
– intégrité

– confidentialité

– disponibilité



Les fondements de la sécurité informatique



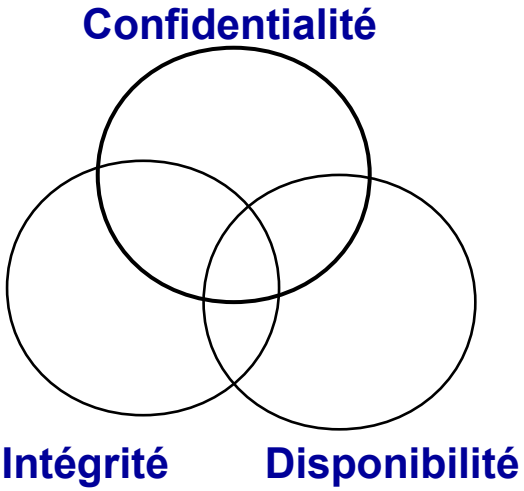
L'authentification

- Pour assurer la confidentialité et l'intégrité de l'information, le système informatique doit authentifier les entités voulant y accéder.
- Les entités autorisées seulement ont accès au système (contrôle d'accès).

Les critères de sécurité informatique

1. Confidentialité

- Seuls les utilisateurs habilités (autorisés) ont accès à l'information
- qui peut "voir" quoi?



2. Intégrité

- Une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).
- Les contraintes d'intégrité : l'ensemble des règles (des assertions) qui définissent la cohérence d'un système d'information. Ex: toute règle de cohérence d'une base de données.
- L'intégrité veut dire : exactitude, précision, modifications autorisées seulement, cohérence.

3. *Disponibilité et fiabilité (pérennité)*

- Terminologie du milieu de la sécurité pour caractériser le bon fonctionnement d'un système informatique.
- Un système informatique doit être disponible à ses utilisateurs autorisés selon les conditions prédéfinies.
- Présence sous forme utilisable (besoins et spécifications) satisfaisant des contraintes de temps, performance et qualité
- La fiabilité est l'aptitude d'un système informatique à fonctionner d'une manière continue pendant une période donnée (sa durée de vie). Un système informatique ne doit pas avoir de bugs liés à des problèmes techniques de conception ou de programmation.

4. Authentification

- Seules les entités autorisées ont accès au système.
- L'authentification protège de l'usurpation d'identité : la signature au sens classique est une authentification.
- Les entités à authentifier : une personne, un processus (un programme en exécution), une machine dans le réseau.
- Ne pas confondre authentification avec confidentialité ou intégrité.
- L'authentification est le moyen clé de sécurité pour assurer :
  - La confidentialité : c'est lui qui lit une donnée est bien celui qui est autorisé à le faire.
  - L'intégrité : celui qui a émis un message , un virement,… est bien celui dont le nom figure dans le message , le virement,…
  - La signature numérique assure l'authentification.

5. Non repudiation

- Une règle de sécurité exigée dans des domaines de traitement de données sensibles (par exemple : une transaction commerciale impliquant un transfert monétaire)
- Elle assure que l'auteur de l'acte ne peut ensuite nier l'avoir effectué (la signature au sens habituel = non-repudiation).
- La signature est un engagement contractuel, juridique, le signataire ne peut revenir en arrière.
- La non-repudiation fournit la preuve d'origine (un message ne peut être dénié par son émetteur) et la preuve de réception (un récepteur ne peut ultérieurement nier avoir reçu un ordre ou un message)

2 – Sécurité informatique : définition

- Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour garantir la sécurité des systèmes informatiques.
- Notamment, on veut préserver
  - l'intégrité de l'information ,
  - la confidentialité de l'information
  - et la disponibilité des systèmes.
- Systèmes informatiques soumis à des menaces
  - utilisateur du système
  - personne malveillante
  - programme malveillant
  - sinistre (vol, incendie, dégât des eaux)

Domaines d'intervention de la sécurité

- sécurité physique
  - environnement humain (politique de sécurité, éducation, charte)
  - environnement matériel (incendie, dégâts des eaux, protection des salles, sauvegardes, alimentations électriques)
- sécurité de l'exploitation
  - hôte (système d'exploitation à jour, authentification)
- sécurité logique
  - données (accès aux fichiers, autorisations, chiffrements, sauvegarde)

Domaines d'intervention de la sécurité

- sécurité applicative
  - applications : virus, vers, chevaux de Troie, espiogiciels (spywares), spam, restrictions et localisations des applications
- sécurité des réseaux et télécommunications
  - réseau interne (protocoles sécurisés, dimensionnement)
  - alentours (pare-feu , vpn, nomadisme,…)

Menaces informatiques

menace : action susceptible de nuire

vulnérabilité ou faille : niveau d'exposition face à une menace dans un certain contexte

contre-mesure : ensemble des actions mises en œuvres en prévention d'une menace

attaque : exploitation d'une faille (d'un syst info) à des fins non connus de l'exploitant du système et généralement pour nuire :

- En permanence sur Internet par machines infectées (les virus)
- rarement pirates

Deux types de menaces (ou attaques): actives (DOS: dénis de service) et passives (écoute)

Motivations des attaques

- Intrusion dans le système
- Vol d'informations industrielles (brevets), personnelles (bancaires), commerciales (contrats), organisationnelles
- Troubler le bon fonctionnement d'un service (déni de service) : Empêcher l'accès à une ressource ou prendre le contrôle d'une ressource
- Utiliser les ressources d'un système (ex : bonne bande passante)
- Désinformer, défis intellectuels, pbs politique/religion
- Utiliser le système comme rebond pour une autre attaque
- Constituer un réseau de « botnet » (ou réseau de machines zombies)

3 - Criminalité informatique : Crime informatique, cybercrime

- **Crime informatique** : délit où le système informatique est l'objet du délit et/ou le moyen de le réaliser.
- **Cybercrime** : forme du crime informatique qui utilise Internet
  - en 2007, la cybercriminalité pèse 7,1 milliards de dollars aux USA
  - Typologie : malveillance, erreur, accident
  - Cibles : états, organisations, individus
  - Vol d'identité, Chantage, Fraude financière, détournements de fonds, vol de biens virtuels, atteinte à la dignité, dénonciation calomnieuses, espionnage, désinformation, escroqueries, atteinte aux mineurs, atteinte à la vie privée, incitation à la haine raciale, . . .

Internet : un facteur aggravant

- dématérialisation des acteurs du délit, des objets du délit
- vulnérabilité : complexité des infrastructures informatique et réseaux
- automatisation, réalisation à grande échelle -- > ubiquité, anonymat
- immatérialité : information numérique peut être détruite, modifiée, usurpée
- disponibilité d'outils, paradis numériques
- dépendance des états/organisations à l'informatique → facteur de risque

Typologie des attaques

- Accès physique : coupure électricité, vol de disque dur, écoute trafic réseau, récupération de matériels
- Interception de communications (l'écoute) : vol de session, usurpation d'identité, détournement de messages
- Pollupostage ou spam (98 % des mails)
- Dénis de services : faiblesse de protocoles TCP/IP, vulnérabilité de logiciels serveurs
- Intrusions : maliciels (virus, vers, chevaux de Troie), balayage de ports, élévation de privilèges, débordements de tampon (Overflow)
- Trappe : porte dérobée dans un logiciel
- Ingénierie sociale : contact direct de l'utilisateur

Logiciels malveillants : Virus I

Virus un segment d'un programme, qui lorsqu'il s'exécute, il se reproduit en se joignant à un autre programme (du système ou d'une application), le virus peut se propager à d'autres ordinateurs (via le réseau) à l'aide du programme légitime sur lequel il s'est greffé. Un virus peut nuire en perturbant plus ou moins le fonctionnement de l'ordinateur infecté. Exemple : psybOt (2009) infecte les routeurs et les modems haut-débit.

Un virus peut infecter des programmes, documents ou secteurs de boot.

Cheval de Troie (Trojan en anglais) Un programme qui effectue une fonction illicite (divulguer ou altérer des informations) tout en donnant l'apparence d'effectuer une fonction légitime.

Trojan.ByteVerify un cheval de Troie sous forme d'une applet Java , exploite une vulnérabilité de la machine virtuelle Java de Microsoft et permet à un pirate d'exécuter du code sur la machine infectée. Il peut par exemple modifier la page d'accueil d'Internet Explorer.

Logiciels malveillants : Ver III

Ver (Worm) un programme autonome se reproduit et se propage à l'insu de l'utilisateur, il a un objectif malicieux comme :

- ✓ Espionner l'ordinateur infecté
- ✓ Offrir une porte dérobée à des pirates informatiques
- ✓ Détruire des données sur l'ordinateur infecté
- ✓ Envoyer des requêtes multiples vers un serveur internet pour le saturer

Le ver Blaster (Août 2003, faiblesse RPC Windows), lance une attaque de déni de service sur le serveur de mise à jour de Microsoft. Welchia (qqs jours après, élimine Blaster);

Logiciels malveillants : Porte dérobée IV

Porte dérobée (ou backdoor en anglais)

Fonctionnalité inconnue de l'utilisateur, qui donne un accès secret au logiciel/système, elle est due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier)

Une porte dérobée dans le SGBD *interbase* de Borland (début des années 2000) : se connecter à la base avec les droits d'administrateur "politically/Correct".

Logiciels malveillants : machine Zombie, Botnet, bombe logique V

Machine zombie : ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique (suite à une infection par ver/cheval de Troie). Sert de rebond.

Botnet : Réseau de machines zombies. Utile pour lancer des attaques de déni de service ou spams

Bombes logiques : Programme se déclenchant suite à un événement particulier (date, signal distant)

CIH/Chernobyl (déclenchement 26 avril 1999, 26 avril 1986) virus destructeur

Virus mutants : réécriture de virus existants

Virus polymorphes : modifie son apparence, pour ne pas être reconnu

Rétro-Virus : attaque les signatures des antivirus

Virus boot : Virus s'installant sur un secteur d'amorçage (disquette, disque)

Les antivirus

Antivirus : Logiciel de détection et d'éradication de virus, trojans et vers

- Méthodes : dictionnaires, heuristiques, comportements suspects, émulation
- scanner sur accès : examine les fichiers/programmes à chaque accès
- scanner à la demande : examine les disques/fichiers/programmes suite à une demande

Spywares : espiogiciels

Espiogiciel : Programme collectant des informations d'une machine et les envoie à l'insu de l'utilisateur sans son consentement

- souvent avec des freewares ou sharewares
- intégrés (PKZip, KaZaA, Real Player) ou externes
- souvent légaux (dans la licence)
- ne pas installer de logiciels (!), antisypwares, firewall

Keylogger : enregistreur de touches : enregistrement des touches à l'insu de l'utilisateur. dispositif d'espionnage. Souvent un logiciel.

Menaces nouvelles I

Social engineering usage de ressorts psychologiques pour obtenir d'un tiers, information ou données fraude, intrusion réseau, espionnage industriel, vol d'identité.

Phishing/hameçonnage Arnaques via internet, usurper une identité fiable (genre banque), redirection vers site pirate données bancaires, mots de passe

http://www.mabanque.com@members.unsite.com/

http://www.mabanque.com.unsite.net/

Menaces nouvelles II

BNP PARIBAS

Cher client de **BNP Paribas**,

Le département technique de BNP Paribas procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.secure.bnpparibas.net/banque/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

Menaces nouvelles III

Pharming (empoisonnement DNS) exploite une vulnérabilité pour rediriger le trafic Internet d'un site Web vers un autre.

Complémentaire de chevaux de Troie, spywares et phishing.

Exemple : americanexpress.com, fedex.com, msn.com, Trendmicro.com (vulnérabilités dans le serveur DNS de Windows NT4 et Windows 2000, depuis corrigées).

Slamming fausse facture de renouvellement de nom de domaine, faux annuaires professionnels.

Menaces nouvelles VI

Vishing (VoIP + phishing). Serveurs VoixIP appelant des numéros fixes, redirection vers boîte vocale informant d'anomalie, invitation à contacter un serveur vocal où il donnera ses coordonnées bancaires.

Ransomwares code malveillant (virus ou cheval de troie) cryptant certaines données, exige une rançon après pour le déchiffrement. Exemple : Gpcode, scanne .xls .doc .txt .rtf ...

Cross Site Scripting (XSS) vulnérabilités dans serveur/app WEB pour insérer du code dans une page html renvoyée dynamiquement.

Redirection vers un autre site, vol d'identifiant de session

Injection de code vulnérabilités dans serveurs/apps (SQL, WEB/XSS, LDAP)

4 - Politique de sécurité

- Compromis fonctionnalité - sécurité.
- Identifier les risques et leurs conséquences (analyse de risque).
- Élaborer des règles et des procédures à mettre en œuvre pour les risques identifiés (contre mesures).
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

Quelques méthodes pour l'analyse de risque

- EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité)

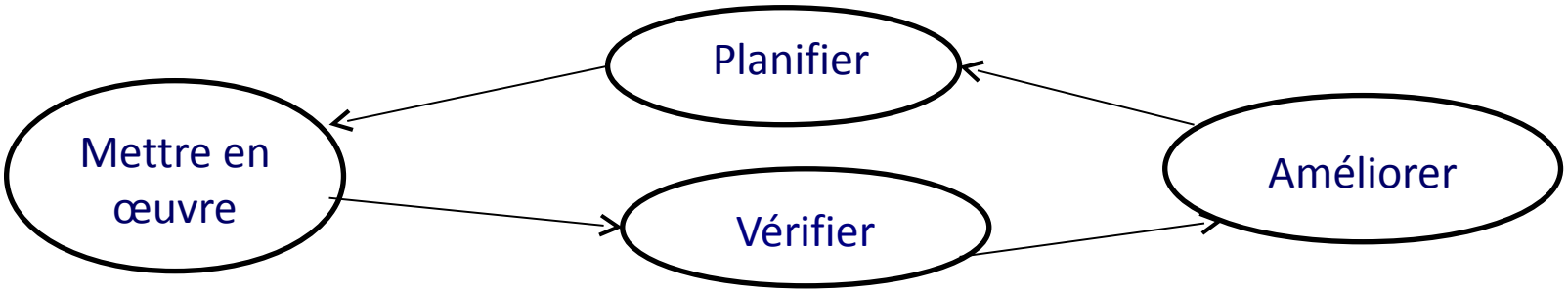
http://www.ssi.gouv.fr/fr/confiance/ebios.html

- MEHARI (MEthode Harmonisée d'Analyse de Risques)

http://www.clusif.asso.fr/fr/production/mehari

La norme ISO 27000

- ISO 2000 Vocabulaire et définitions
- ISO 27001 (octobre 2005) spécifie un Système de Gestion de la Sécurité des Systèmes d'Information (**Plan/Do/Check/Act)**



- ISO 27002 (remplaçant la norme 17799 depuis le 1er juillet 2007) est un code de bonnes pratiques
- Plus d'informations: http://www.iso27001security.com/

5 - Cryptographie et critères de sécurité

- Satisfaire les objectifs de sécurité via la cryptographie : confidentialité, intégrité, authentification, non-répudiation, disponibilité ?

- Outils : chiffrement, signature, fonctions de hachage et Mac (Message Authentication Code)

Cryptographie et cryptanalyse

[Source Wikipedia]

Définition (Cryptographie)

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

Définition (Cryptanalyse)

La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière.

Cryptographie : un outil pour la sécurité informatique

6 – Conclusions

- Aucune sécurité n'est parfaite. On définit juste un seuil.
- Des outils sont nécessaires, mais le travail quotidien est indispensable.
- Le niveau de sécurité d'un site est celui de son maillon le plus faible.
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre les décideurs de l'entreprise.