LA SÉCURITÉ DES SI

3ieme année ISIL
Université 8 Mai 45 Guelma

Dr. Djalila Boughareb

Système d'information (définition)

- Un système d'information comprend
- Les matériels informatiques et les équipements périphériques,
- Les logiciels et microprogrammes,
- Les algorithmes et spécifications internes aux programmes,
- La documentation,
- Les moyens de transmission,
- Les procédures, les données et les informations qui sont collectées, gardées, traitées, recherchées ou transmises par ces moyens ainsi que les ressources humaines qui les mettent en œuvre.

Sécurité :

- Protection contre les accidents
- Protection physique
- Qualité de l'environnement
- Fiabilité des systèmes: pannes, tolérance de pannes
- Systèmes de secours, sauvegardes, maintenance
- Qualité de base des logiciels
- Confidentialité, intégrité, disponibilité
- Protection contre les Intrusion réseau, virus, piratage, · · ·

Vulnérabilité de l'information

- Peut être détruite, amputée, falsifiée, modifiée.

- L'information numérique est volatile peut être ajustée, personnalisée, un document générique peut être particularisé pour un destinataire spécifique.

sécurité des SSI : concepts clés (1)

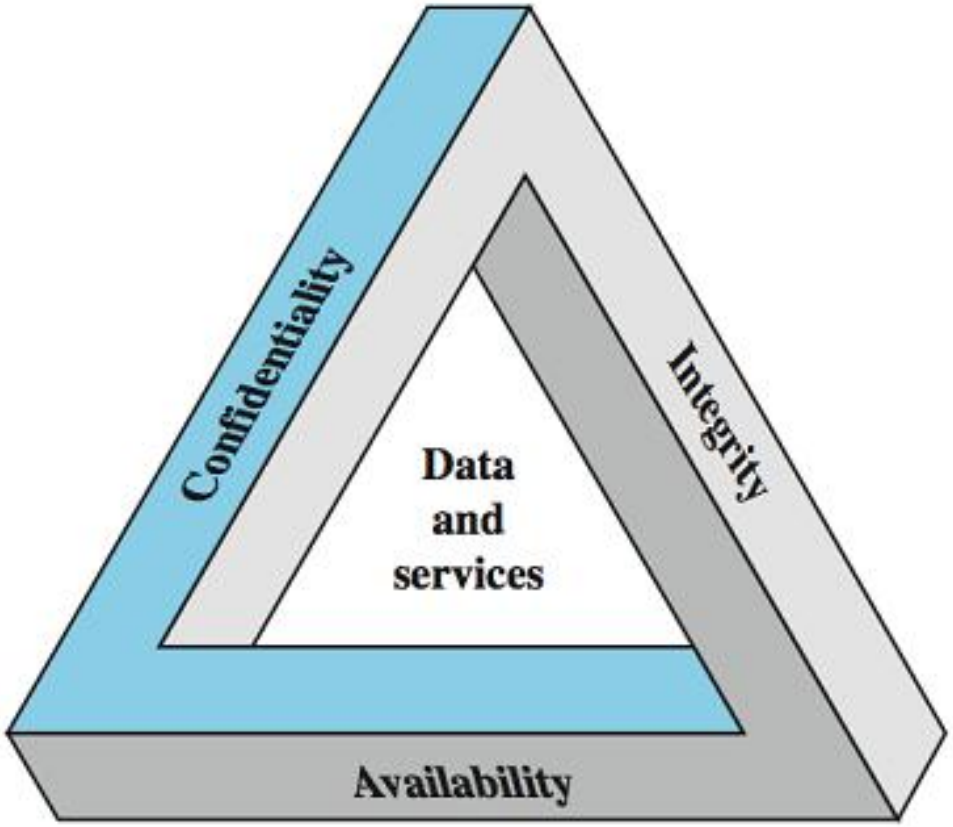


FIG.: source : W. Stallings & L. Brown

sécurité des SSI : concepts clés (2)

- La norme identifie des objectifs pour la sécurité informatique selon 3 critères :
- Confidentialité : protection des données contre une divulgation non autorisée.
- Intégrité : prévention de modifications ou de suppressions non autorisée d'informations
- Disponibilité : garantit l'accès aux informations du système

sécurité des SSI : concepts clés (3)

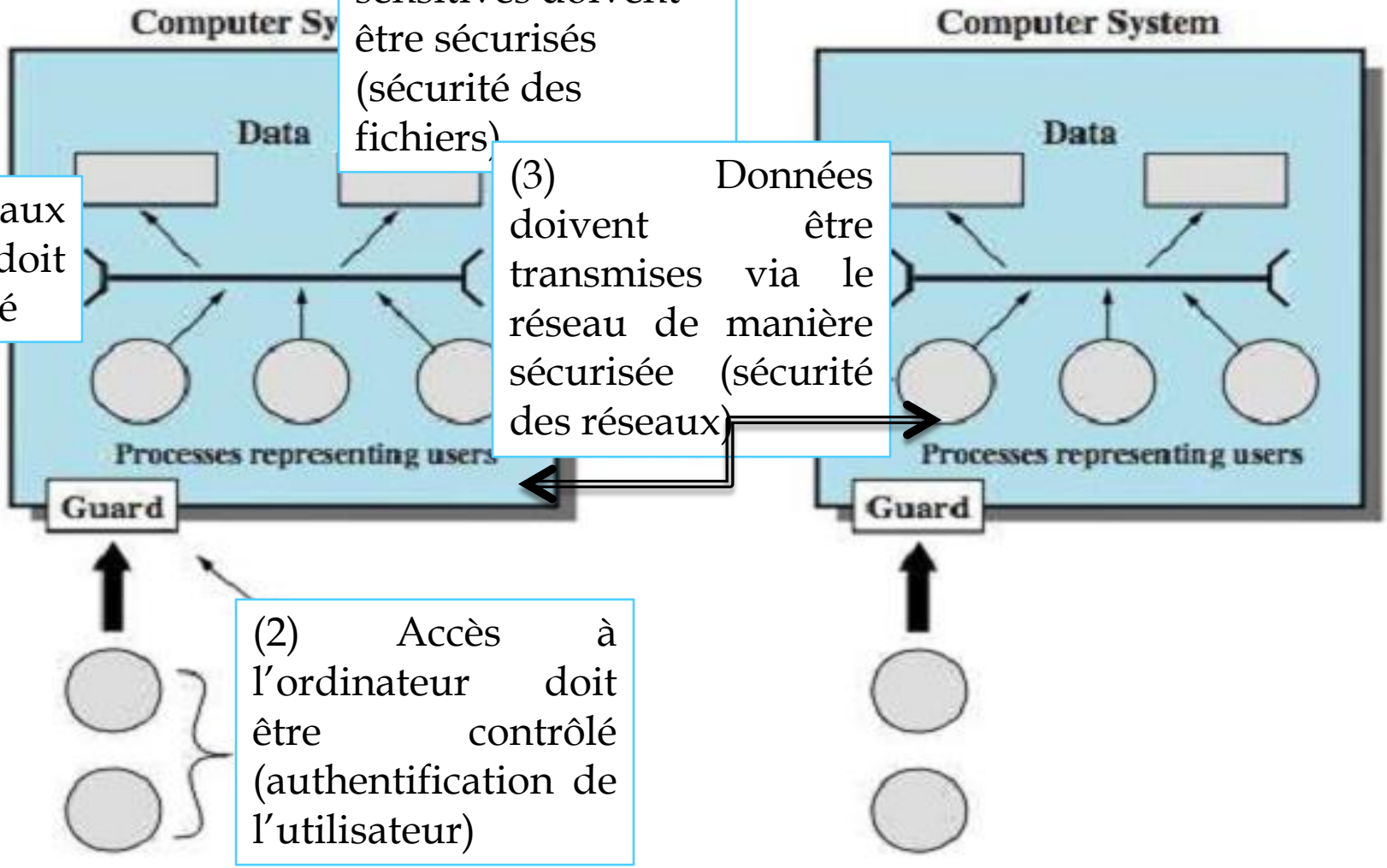
- À ces trois critères s'ajoutent :
- Authentification: permet de prouver l'identité des entités
- Non répudiation: est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu.

Périmètre de la sécurité des SI

(4) Fichiers sensitives doivent être sécurisés (sécurité des fichiers)

(1) Accès aux données doit être contrôlé

(3) Données doivent être transmises via le réseau de manière sécurisée (sécurité des réseaux)



(2) Accès à l'ordinateur doit être contrôlé (authentification de l'utilisateur)

FIG.: source : W. Stallings & L. Brown

Les enjeux de la sécurité des SI

- Maitriser le traitement, le stockage, le transport de l'information
- Valoriser les contenus multimédia, logiciel, propriétés intellectuelles, · · ·, Libre circulation des contenus
- Asseoir la confiance dans l'univers numérique: e-commerce, e-buisness, e-gouvernement, · · ·
- Sécuriser
  - Les personnes (libertés, protection de d'intimité)
  - Les entreprises et organisations (prévention des risques)

Origine des sinistres

- Attaques logiques
- Virus
- Malveillance
- Erreurs / négligence
- Catastrophes naturelles
- Terrorisme · · ·

Conséquences :

- Fermeture de l'entreprise
- Perte financière
- Perte de contrat
- Mesentente
- . . .

Type de Sécurité

- L'aspect sécurité doit êtres pris en considération pendant l'implémentation du système.

- Sécurité physique : est le control de l'accès aux ressources physique de l'ordinateur.
- Sécurité logique est le control de l'accès logiciel.
- Sécurité comportementale est la création de procédures pour empêcher les personnes de l'utilisation vulnérable des logiciels et du matériels de l'ordinateur.

Programmes malveillants

- Programmes qui exploitent les vulnérabilités du système appelés “malware”
- ✓ Fragments de programmes nécessitant un programme hôte (virus, bombe logique, porte dérobée)
- ✓ Programmes autonomes indépendants (vers, robot)
- Menaces sophistiquées sur les systèmes informatiques

Menaces

- 7 menaces.

1. Perte et destruction de données.
2. Modification de données.
3. Interception de données (vol et espionnage).
4. Indisponibilité des systèmes.
5. Dégradation de l'image de marque.
6. Détournement d'activité via les technologies de l'Information et de la communication
7. Sanctions juridiques pour défaut de protection de données des tiers ou utilisation prohibée (même involontaire) des technologies, par les membres d'une entreprise.

Panorama des attaques

Type d’attaques

- Attaques virales
- Attaques techniques
- Attaques classiques

Attaques virales : Porte dérobée (backdoor)

- Fragments de programmes nécessitant un programme hôte;
- Il ne participe en rien aux objectifs officiels d'un programme.
- À priori malveillante;
- D'aucune utilité autre que pour son concepteur;
- S'exécute à l'insu de l'utilisateur;
- L'ouverture d'une porte dérobée permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur;

Attaques virales : Cheval de Troie (Tojan)

- Programme, jeu, commande ayant une fonction annoncée et en réalisant une autre (illicite)
- Il tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations.
- S'exécute à l'insu de l'utilisateur
  - Exemple 2005 : cheval de Troie envoyé par email ou intégré à un CD contenant une fausse proposition commerciale.
  - Une fois installée et contre 3000 euros, le concepteur fournissait à son client une adresse IP, un nom d'utilisateur et un mot de passe pour accéder au pc de sa victime

Attaques virales : Cheval de Troie

Exemples

- Back Orifice : logiciel d'administration et de prise de contrôle à distance de machines utilisant Windows
- Subseven : l'un des chevaux de Troie les plus connus, en 2000 il a introduit :
  - Surveillance par caméra (webcam capture)
  - Surveillance en temps réel du bureau windows (desktop capture)
  - Le vol de mots de passe (recorded password) par lequel subseven détecte les écrans de demande de mot de passe(windows, internet · · ·)
  - Permet la capture-clavier (keylogger) pour récupérer les numéros de cartes de crédits
- Autres chevaux de troie : byteverify, xxxdial, · · ·

Attaques virales : Bombe logique

- Programme informatique illicite,

- Obj: attaquer un SI suite à un événement particulier (exp: anniversaire) afin d'éxécuter une action illicite (exemple :Effacer des données)

Attaques virales : Virus

- Fragments de Programme illicite qui s'insère dans des programmes légitimes appelés hôtes
- Se reproduit automatiquement soit à l'identique soit en se modifiant (virus polymorphe) à chaque fois que le système infecté se démarre.
- Il se transmet, il peut avoir des actions retardées
- Se répand au travers d'internet, de disquettes, de clés USB
- Analogie avec la biologie : contagion
- Exemple: Virus système, virus résident en mémoire, Virus programme, virus macro,Virus polymorphe ou mutant, virus de scripts

Structure d'un virus

- Composants :
  - Mécanisme d'infection : permet la reproduction
  - Déclenchement : évènement qui rend la charge active
  - Charge du virus : ce qu'il fait, action malveillante ou bénigne
- Le virus s'ajout au début à la fin au milieu d'un programme exécutable;
- Moyen de protection?
  - Blocage de l'infection initiale (difficile)
  - Blocage de la propagation (contrôle d'accès)

Virus Macro

- Très courant depuis le milieu des années 1990
  - Indépendant des plateformes
  - Infecte les documents, se répand facilement
- Exploite les capacités des applications de logiciels de bureautique (word, excel, $\cdots$)
  - Programme exécutable incorporé dans un document
  - Infecte les documents
- Versions récentes des logiciels de bureautique ont des protections
- Reconnus par de nombreux programmes anti-virus

Virus e-mail

- Développements plus récents
- En général :
  - Utilise les macros d'un document attaché (en word)
  - À l'ouverture du document attaché la macro est activée :
    - Le virus envoie des messages à toutes les adresses de la liste d'adresses de l'utilisateur
    - Localement, il occasionne des dégâts sur le système de l'utilisateur
- Version plus récentes : déclenchement du virus à lecture du message (propagation encore plus rapide)

Mesures contre les virus

- Prévention : solution idéale mais difficile
- Réaction : plus réaliste
  - Détection
  - Identification
  - Retrait
- En cas de détection mais impossibilité
  - D' identification
  - Ou de retrait

➔Remplacement du programme infecté

Évolution des anti-virus

- Les technologies des virus et anti-virus ont évolué ensemble
- Premiers virus : fragments de code faciles à retirer
- Virus de plus en plus complexes : les contre-mesures aussi
- 4 générations de logiciels anti-virus
  - Première génération : scanners simples (recherche de signature)
  - Deuxième génération : règles heuristiques pour la recherche de fragments de code
  - Troisième génération : identification des actions du virus
  - Quatrième génération : combinaison de plusieurs techniques

Attaques virales : Vers (worm)

- Processus parasite qui consomme, détruit et se propage sur le réseau
  - N'a pas besoin d'un programme hôte pour se reproduire (contrairement au virus)
  - Se reproduit par ses propres moyens sans contaminer de programme hôte
  - Souvent écrits sous forme de script intégrés dans un courriel ou une page html

Attaques virales : Vers (worm)

- Comporte des phases comme un virus
  - Dormant, propagation, déclenchement, exécution
  - Lors de la phase de propagation le vers recherche d'autres systèmes, il établit une connexion à ceux-ci, il s'autocopie sur ceux-ci puis il s'exécute
- Un vers peut se déguiser en processus système

Attaques techniques : Hameçonnage (Phishing)

- Appelé aussi filoutage : il s'agit de piéger l'utilisateur en lui faisant croire qu'il s'adresse à un tiers de confiance pour lui soutirer des informations confidentielles (mot de passe, n° de carte de crédit ...)
  - On lui demande son mot de passe
  - On lui demande de le changer
- Exemple : Hameçonnage des services bancaires en ligne, ou des sites de ventes aux enchères (ebay)
- **Exemple**
- Il va cliquer sur le lien
- Il croit qu'il se connecte sur le site LCL
- Il saisit des informations confidentielles
- MAIS il ne se connecte sur un faux site LCL et un pirate
- Récupère ces informations

Attaques techniques : Craquage (Cracking)

- Cassage des protections dites de sécurité (ex : protection anticopie) des logiciels, notamment des logiciels (qui nécessitent des clés d'enregistrement)
- Utilisation d'un générateur de clés

- Exemple : craquage de jeux ou de logiciels

Attaques techniques : Renifflage (Sniffing)

- Analyse du trafic pour récupérer les mots de passe et les informations confidentielles
- Utilise des sondes placées sur le réseau pour écouter et récupérer des informations à la volée

- solutions : protocoles de communication sécurisés (ex SSH, SSL)

Attaques techniques : Mascarade (Spoofing)

- Attaque Réseau TCP/IP
- Utilisation de l'adresse IP d'une machine afin d'en usurper l'identité (déguisement).
  - Récupération de l'accès à des informations en se faisant passer la machine dont elle a usurpé l'adresse IP
  - Création de paquets IP avec une adresse IP source Appartenant à quelqu'un d'autre

Attaques techniques : smurfing

- Attaque du réseau TCP/IP
  - Envoi d'un message à une adresse fausse
  - Provoque la saturation et le blocage du réseau

Attaques techniques : Piratage téléphonique (Phreaking)

- Utilisation du réseau téléphonique d'une manière non prévue par l'operateur, afin d'accéder à des fonctions spéciales, en général pour ne pas payer les communications et rester anonyme
- Exemple : captain crunch

Attaques techniques : rootkit

- Programme ou ensemble de programmes permettant de maintenir dans le temps un accès frauduleux à un SI
  - S'utilise après une intrusion et l'installation d'une porte dérobée
  - Fonction principale : camoufler la mise en place de plusieurs portes dérobées
  - Opère des modifications sur les commandes systèmes
  - L'installation d'un rootkit nécessite des droits d'administrateur
- Exemple : octobre 2005 rootkit SONY-BMG

Attaques techniques : Dénis de service (DoS)

- Le but est de rendre une application informatique incapable de répondre aux requêtes des utilisateurs
- Types d'attaques nombreux :
  - Débranchement de la prise d'un serveur
  - Saturation d'un élément chargé d'animer l'application
  - Exemple : bombe fork
- Dénis de service distribués (DDOS)
  - Repose sur la parallélisations d'attaques DOS menées simultanément par plusieurs systèmes

Attaques techniques : robots

- Programmes malveillants permettant une prise de contrôle à distance de machines vulnérables afin de former un réseau d'attaque caché (botnet)
- Pour s'implanter le robot utilise une méthode classique
  - Il peut être déposé sur la cible par spam, vers, virus, cheval de troie ...
  - Il peut posséder son propre module de propagation et exploite :
    - Une vulnérabilité
    - Des partages ouverts (open share)
    - Des mots de passe faibles ou manquants
- Exemple : hollande octobre 2005 (rapport CLUSIF)

Attaques classiques

- Vol
- Détournement
- Destruction
- Sabotage
- Chantage

Autres attaques

- Brouillage : attaque de haut niveau utilisant les rayonnements électromagnétiques qui rendent le SI inopérant.
- Exploitation d'un défaut (bug) : De nombreuses failles sont présentes dans les logiciels commerciaux. Ces failles sont exploitées à des fins malveillantes par les pirates.
- Pourriel (spam) : courrier électronique indésirable transmis à une multitude de destinataires envoyés sans que l'émetteur ne soit au courant. Le spam contribue à la pollution voir à la saturation des boîtes aux lettres électroniques.

Mise en œuvre d'une politique de sécurité :

- Système d'authentification (biométrie, serveur d'authentification , · · ·)
- Chiffrement (PKI, mécanismes intégrés à des protocoles de communication (ipsec), · · ·)
- Pare feux (firewall)
- Système anti-virus
- Outil de détection de failles de sécurité
- Système de détection d'intrusions
- Système d'exploitation sécurisé
- · · ·