CHAPITRE 1 :
Concepts fondamentaux de la sécurité informatique

Mohammed SABER

Département Électronique, Informatique et Télécommunications
École Nationale des Sciences Appliquées "ENSA"
Université Mohammed Premier OUJDA

Année Universitaire : 2017-2018

Plan de chapitre

Plan de chapitre

Introduction

- Avec le développement de l'utilisation d'Internet, de plus en plus les entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs.
- Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.
- La connexion des personnels au système d'information à partir de n'importe quel endroit. Ils sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise.

Que faut-il protéger ?

- L'information stockée ;
- La pertinence et la valeur de l'information ;
- L'accès aux services externes (Site web, messagerie) ;
- L'accès aux services internes (Intranet, Extranet, bases de données,....) ;
- La sécurité des données :
  - Qui peut accéder aux données ?
  - Comment peut-on y accéder ?

Introduction

De qui faut-il se protéger ?

- Les pirates informatique ;
  - Utilisent des logiciels d'attaque trouvés sur Internet ;
  - Les vrais pirates qui connaissent les protocoles et les systèmes ;
- Les intrus criminels ;
  - Ils ont plus de moyens que les pirates ;
- Terroristes industriels ;
  - Ils ont d'énormes ressources ;
- Employés ou fournisseurs ;
  - Où comment la faille peut-elle venir de l'intérieur ?.

Plan de chapitre

Sécurité d'un Système d'Information

- Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.
- Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser un Système informatique.

Sécurité d'un Système d'Information

Définition 1

La Sécurité d'un système d'information, d'une manière générale, consiste à s'assurer que les ressources matérielles ou logicielles d'une organisation ne sont utilisées que dans le cadre où il est prévu.

Définition 2

La Sécurité des systèmes d'information est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver ou rétablir la disponibilité, l'intégrité et la confidentialité des informations ou du système.

Définition 3

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

Sécurité d'un Système d'Information

Pourquoi sécuriser ?

- Les SI sont de plus en plus considérés comme les centres névralgiques des organismes (au cœur de l'activité de l'organisme).
- Les SI sont de plus en plus connectés à Internet.
- Toutes les attaques exploitent des faiblesses de sécurité au niveau du SI et du réseau sous-jacent ;
- Les pertes dues à une attaque peuvent être très grandes (d'après une étude faite en l'an 2015 "The Global State of Information Security Survey et the Global Cost of Cybercrime", sont de 100 milliards d'euros par an l'échelle mondiale !).

Sécurité d'un Système d'Information

Motivations pour attaquer un SI ?

Il existe différentes motivations pour attaquer un SI, dont :

- Bénéfices financiers (vol d'argent, vol de numéro de carte de crédit, espionnage industriel, nuisance à l'image de marque profitant aux concurrents, ...) ;
- Satisfaction personnelle (plaisir/jeu, fierté maladive, concurrence entre Hackers, . . .) ;
- Vengeance (salarié licencié et/ou sous estimé, ...)
- Convictions politiques et/ou idéologiques (partisans d'un parti, terroristes, ...) ;
- Espionnage d'état.

Plan de chapitre

Les attaques

- Une attaque est une action malveillante visant à tenter de contourner les mesures de sécurité d'un système d'information
- Une attaque est un ensemble d'un ou plusieurs évènements qui peuvent avoir une ou plusieurs conséquences en termes de sécurité.
- Elle peut être **passive** (contre uniquement la confidentialité) ou **active** (contre l'intégrité, l'authentification, le contrôle d'accès).

Objectifs des Attaques

- Désinformer ;
- Empêcher l'accès à une ressource ;
- Prendre le contrôle d'une ressource ;
- Récupérer de l'information présente sur le système ;
- Utiliser le système compromis pour rebondir.

Les attaques
Cibles des Attaques

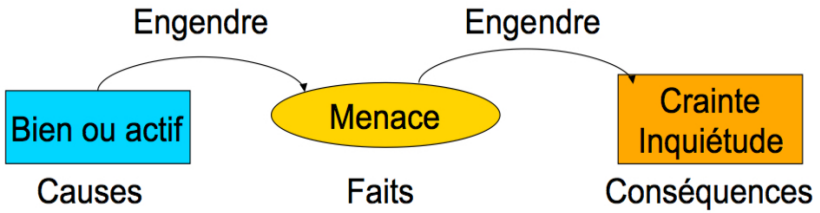
Cibles des Attaques

- Les états ;
- Serveurs militaires ;
- Banques ;
- Universités ;
- Tout le monde ;
- ....

Les attaques
Déroulement d'une Attaque

Phase 1

Une menace naît de la présence d'un bien ou d'un actif. Cette menace, de par son existence, engendre des craintes et des inquiétudes.



Actif ou bien

- Information ou composant d'un système, qui possède une valeur ou un intérêt.
- Il conviendra donc de le protéger.

Les attaques
Déroulement d'une Attaque

Menaces

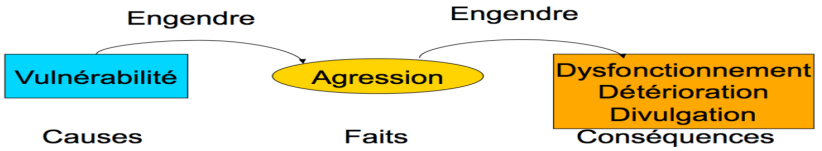
La menace est définie dans la norme ISO-7498-2-89, comme une violation potentielle de la sécurité (accident, erreur, malveillance). La norme ISO-7498-2-89, distingue quatre types de menace :

- **Menace accidentelle** : menace d'un dommage non intentionnel envers le SI :
  - Pannes/dysfonctionnements du matériel ; Pannes/dysfonctionnements du logiciel de base ;
  - Erreurs d'exploitation (oubli de sauvegarde ; écrasement de fichiers) ; Erreurs de manipulation des informations (erreur de saisie ; erreur de transmission ; erreur d'utilisation).
  - Erreurs de conception des applications ; Erreurs d'implantation.
- **Menace intentionnelle ou délibérée** : menace de modification non autorisée et délibérée de l'état du système.
  - **Menaces passives :** Détournement des données (l'écoute, les indiscrétions) Exemples : (espionnage industriel ; espionnage commercial ; violations déontologiques) ; Détournement des logiciels (Exemple : copies illicites).
  - **Menaces actives :** Modifications des informations ; Modification des logiciels (Exemples : Bombes logiques, virus, ver).
- **Menace physique :** menace qui pèse sur l'existence même et sur l'état physique du SI.

Les attaques
Déroulement d'une Attaque

Phase 2

- Cette menace pourra se concrétiser en agression. Cela n'est possible que s'il existe des vulnérabilités dans le SI.
- Cette dernière va engendrer des dysfonctionnements, des détériorations ou la divulgation de services ou de données.



Vulnérabilités

Elle peut être due à :

- Sont des faiblesses ou des failles du SI qui pourraient être exploitées pour obtenir un accès non autorisé ;
- Une faiblesse ou une faille dans les protocoles, la topologie, les méca-

Les attaques
Déroulement d'une Attaque

Risque

Elle peut être due à :

- Peut se définir comme étant la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée (Il est fonction de la menace et des vulnérabilités).
- Risque peut être représenté par «l'équation »suivante :

$$RISQUE = MENACE \times VULNERABILITES \times SENSIBILITE$$

- Que l'un des facteurs soit nul $\Rightarrow$ le risque n'existe pas !

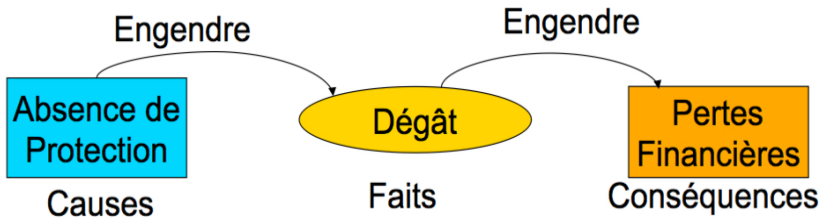
Agression

attaque portée au système, qu'elle soit réussie ou non.

Les attaques
Déroulement d'une Attaque

Phase 3

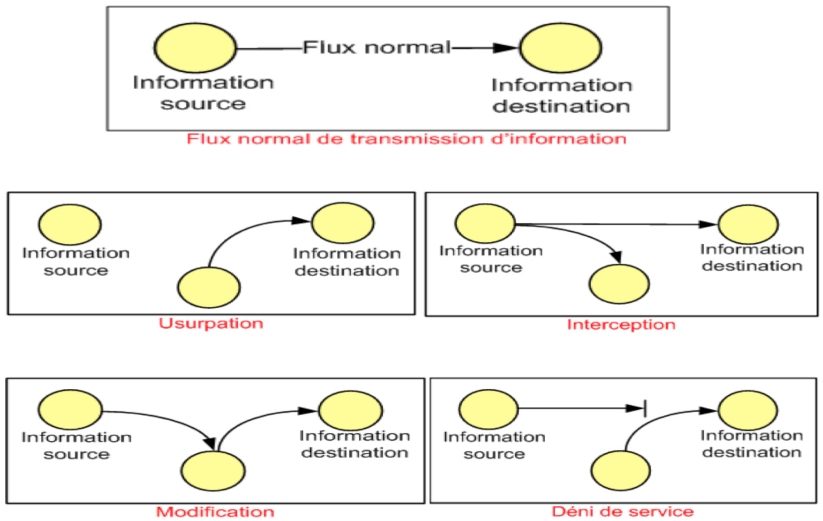
- Si le SI n'est pas protégé, des dégâts vont apparaître.
- Et ceux-ci vont occasionner des pertes financières.



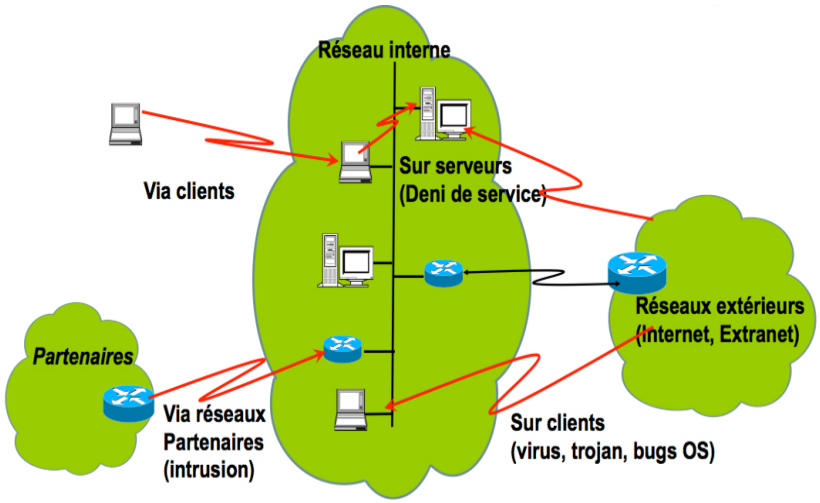
Dégât

Pertes irrécupérables de services ou de données.

Les attaques
Les modèles d'attaques



Les attaques
D'où viennent les intrusions et les attaques ?



Plan de chapitre

Objectifs de la sécurité informatique

Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

- Confidentialité ;
- Intégrité ;
- Authentification ;
- La non-répudiation ;
- Disponibilité.

Confidentialité des données

- C'est la propriété qui assure que seuls les utilisateurs habilités, dans des conditions prédéfinies, ont accès aux informations.
- Dans le domaine de l'entreprise cette garantie concerne :
  - Le droit de propriété :
    - Des secrets de fabrication ;
    - Des informations stratégiques entreprise ;
    - Niveau de production, de résultats ;
  - Fichier clientèle ;
    - Le droit des individus :
    - Défini par la loi informatique et liberté ;

Objectifs de la sécurité informatique

Intégrité des données

- C'est la propriété qui assure qu'une information n'est modifiée que dans des conditions pré définies (selon des contraintes précises)
- Contraintes d'intégrité : l'ensemble des assertions qui définissent la cohérence du système d'information (Toute règle de cohérence d'une base de données).

Authentification

- C'est la propriété qui assure que seules les entités autorisées ont accès au système.
- L'authentification protège de l'usurpation (modification) d'identité.
- Entités à authentifier : Une personne ; Un processus en exécution ; Une machine dans un réseau.
- Ne pas confondre authentification avec confidentialité ou intégrité.
- L'authentification c'est un moyen clé de la sécurité pour assurer :

Objectifs de la sécurité informatique

Non répudiation

- Signature (au sens habituel) = Non répudiation $\Rightarrow$ Traces ;
- C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué.
- La seconde idée contenue dans la notion habituelle de signature est que le signataire s'engage à honorer sa signature : engagement contractuel, juridique, il ne peut plus revenir en arrière.
- Deux aspects spécifiques de la non répudiation dans les transactions électroniques :
  - La preuve d'origine : Un message (une transaction) ne peut être dénié par son émetteur.
  - La preuve de réception : Un récepteur ne peut ultérieurement dénier avoir reçu un ordre s'il ne lui a pas plus de l'exécuter alors qu'il le devait juridiquement.
- La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message(certificat numérique).

Objectifs de la sécurité informatique

Disponibilité

- Terminologie du milieu de la sécurité pour caractériser le bon fonctionnement du système informatique.
- En termes de la sûreté de fonctionnement on parle de :
  - **Disponibilité/Indisponibilité :**
    - L'aptitude d'un système informatique à pouvoir être employé à un instant donné par les utilisateurs.
    - L'indisponibilité est une composante de la sécurité en ce sens qu'elle entraîne des pertes financières.
  - **Fiabilité :** L'aptitude d'un système informatique à fonctionner correctement de manière continue pendant une période donnée.

QUESTIONS ?