Module Sécurité Informatique (F332)

Plan du Module

- **Partie I**:Notions de Base sur la Sécurité Informatiques
  - Introduction à la sécurité informatique
  - Panorama des menaces, risques et attaques de sécurité
  - Gestion de risque informatique
  - Contre mesure
- **Partie II**: Cryptographie et Sécurité Informatique
  - La cryptographie comme pierre angulaire à la sécurité informatique
  - Panorama des solutions/techniques de sécurité (algorithmes, protocoles, etc.) au niveau système, applicatif et réseau.

Bibliographie

- Livre: « Sécurité informatique Ethical Hacking -Apprendre l'attaque pour mieux se défendre », Editions ENI - Octobre 2009 ISBN: 978-2-7460-5105-8

- ETHICAL HACKING AND PENETRATION TESTING GUIDE, CRC Press Taylor & Francis Group ISBN-2015 : 13: 978-1-4822-3162-5

- Ethical Hacking & Countermeasures- Threats & Defense Mechanisms, EC-Council | Press 2010 ISBN- 13 978-1-4354-8361-3

- Cours « Menaces et attaques », http://odile.papini.perso.esil.univmed.fr/sources/SSI.html

Partie I

Chapitre 1
Introduction à la Sécurité Informatique

A propos de la sécurité au quotidien (classique)

- Sécurité des biens, personnes, territoire, Pourquoi?

- Nous ne vivons pas dans un monde **idéal** et **parfait**

- Voleurs, Arnaques, terroristes, criminels, délinquants, bandes organisés, espions, etc.
- Nous avons des **biens**/**actifs** (habitations, argent, banques, postes, infrastructures économiques, transports, documents, etc.) à **protéger** et à **préserver**
- Besoins des différents services: Armée, Police, Gendarmerie, Douanes, Justice, Renseignement, Citoyen, etc.

Information

- L’avènement de l'informatique et des télécommunications à créer d'immenses opportunités, pour les individus, les états, les industriels (économie, médias, etc.)

- L’**information/donnée** -numérique-, sous ses différentes formes est devenue le “nerf de la guerre”

- Les **systèmes d’informations** sont devenus indispensable pour la gestion de ces données (collecter, classifier, stocker, restituer, diffuser les informations)

Information Omniprésente (1)

De nos jours, pratiquement tout le monde est passé au tout numérique

- *E-administration*: démarches administratives électronique (demande actes états civils, CNI, Passeport, Casier judiciaires, inscriptions, etc.)

- *E-commerce*: Une grande partie des sociétés/Entreprises commercialisent leur services/produits via Internet. Certaines entreprises/sociétés existent exclusivement sur le net (pas d'agences, pas entrepôts)

Information Omniprésente (2)

- *E-Learning*: Apprentissage à distance où en ligne via Internet
- *E-Health*: Informatisation du fichier patient. Consultation et suivi à distance du patient en utilisant les TIC
- *Les moyens de transports (avions, trains, voitures) sont tous équipés d'ordinateurs de bord traitant les différents informations et agissant par conséquent*

- Métro, avion(drône), voiture entièrement automatisé : pas de présence humaine

Information Omniprésente (3)

- *L'industrie*: automatisation de la chaîne de production grâce à des automates programmable pilotés par ordinateurs (chaînes de montage voiture, TV, etc.)
- Centrale nucléaire, génération d'électricité: pilotés par des systèmes de contrôle SCADA
- Les individus:Réseaux sociaux, emails, surfer sur Internet, stockage HDD, USB/DVD, Cloud, etc.

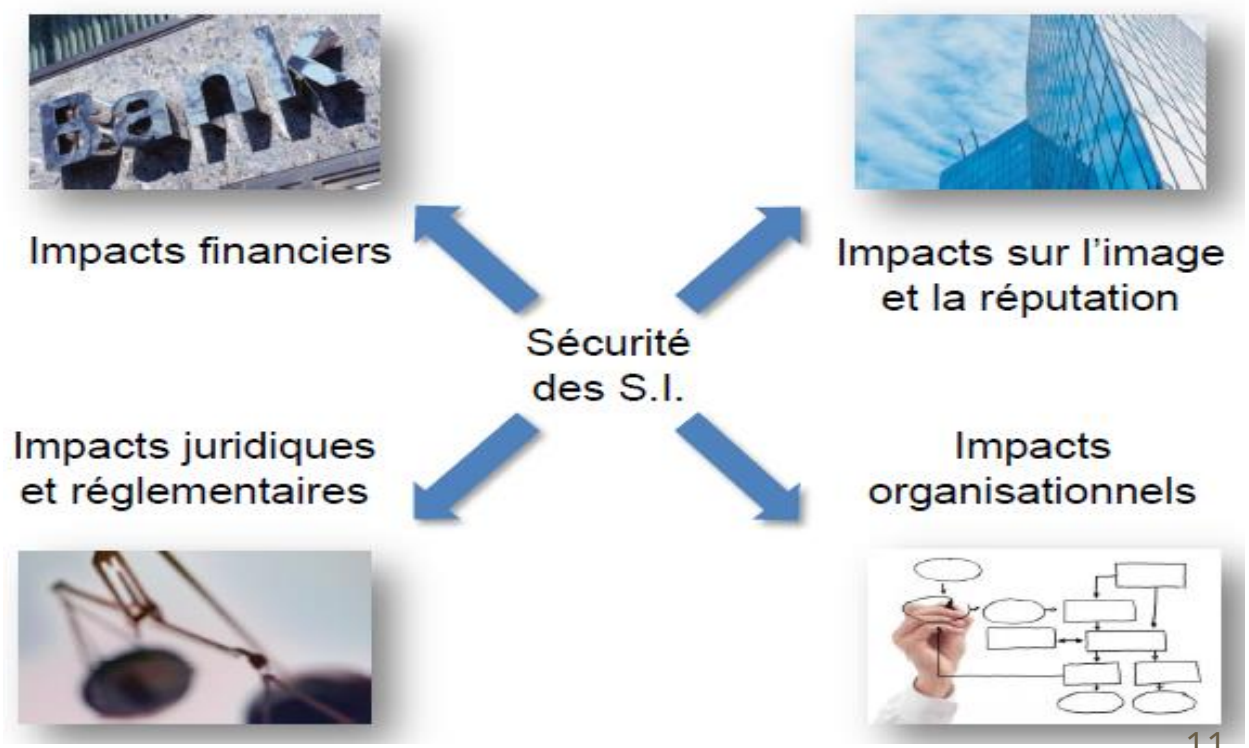
Sécurité Informatique, Pourquoi?

- Les systèmes d'informations (toute la chaîne) d’une organisation ou les données/PC d’un individu peuvent être la **cible** à des individus/organisations/pays voulant porter **préjudice** (vole, destruction, manipulation, etc.)

- La **sécurité** a pour objectif de **réduire** -voir **éliminer**- les **risques** pesant sur le système d’information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations...

Sécurité Informatique, les Enjeux

Enjeux: C'est ce qu'on risque de gagner ou de perdre en adoptant ou en omettant la sécurité



Impact Financiers

- Supposant qu’une entreprise innovant ne sécurise pas sans SI

  Risque de vol des inventions en cours de réalisation et qui ne sont pas encore breveté → Une perte financière pour l’entreprise, car elle ne pourras pas prouver son antériorité, surtout si l’attaquant brevette/rend publique l’invention

Impact sur l’image et la réputation

- Supposons que le système de passeport biométrique Algérien n’est pas sécurisé

  Risque de délivrer un passeport falsifié → L’image du pays et sa réputation au niveau internationale sera fortement affectée

- Supposons que le SI d’une banque est attaqué, et que les informations des clients divulgués

  Risque de ne plus attirer de nouveaux client et de voir ces clients actuel partir

Impact Juridique/réglementaire

- Supposons que mon PC n’est pas sécurisé (pas d’antivirus), et qu’un virus a infecté mon PC et par la suite une attaque a été lancé de mon PC à mon insu!

  Je suis juridiquement responsable de l’attaque malgré moi! → C’est comme si tu prends en STOP quelqu’un en voiture, et lors d’un contrôle de police on trouve sur lui de la drogue!

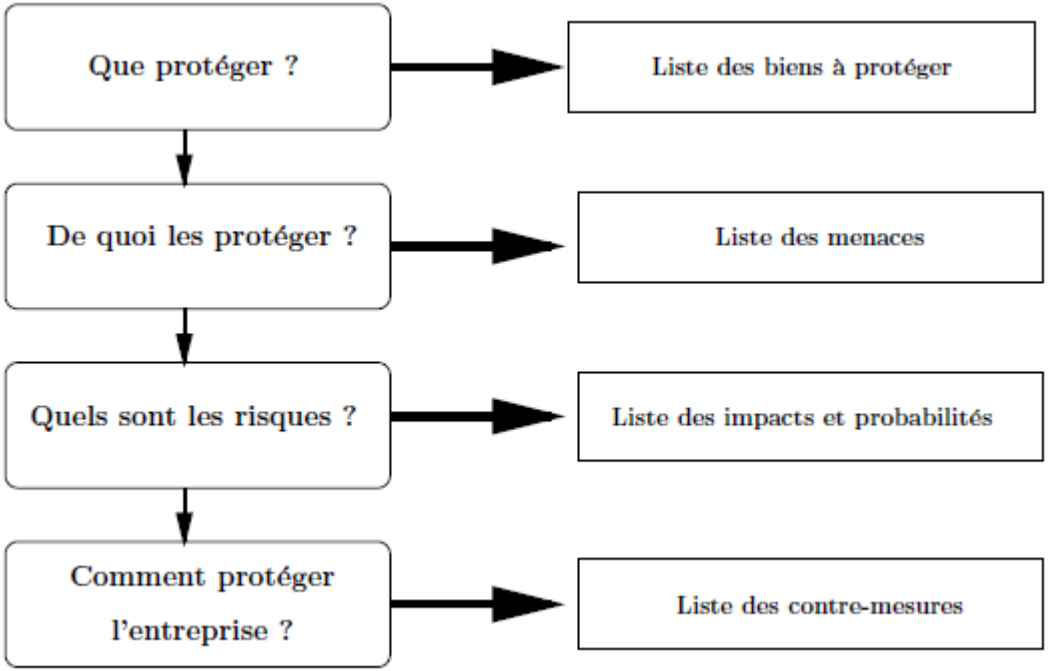
  C’est pas le même cas pour une voiture de location!

Impacts ORGANISATIONNEL

- Si jamais une attaque ce produit, les personnes ayant été la causes devront être sanctionnés (dégradés, radiés, etc.), ce qui pourra perturber l'organisation existante de l'entreprise

Enjeux de la sécurité Informatique

DEMARCHE NORME ISO 17799



Quelques concepts(1)

Menace: est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'entreprise

Vulnérabilité: représente les failles, les brèches dans le système, tout ce qui expose le système à la menace

Attaque: Action malveillante qui tente d'exploiter une vulnérabilité dans le système et de violer un ou plusieurs besoins de sécurité

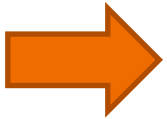
Quelques concepts(2)

Intrusion: Opération qui consiste à accéder, sans autorisation, aux données d'un système **informatique** ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

Contre-mesures: sont les actions mises en œuvre pour prévenir la menace, une fois qu'elle est mesurée

Pourquoi faut-il plus de sécurité informatique ?

Développement d'internet



de plus en plus d'organismes ouvrent leur systèmes d'informations à leurs partenaires (fournisseurs , clients, …)

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

Objectifs de la Sécurité Informatique

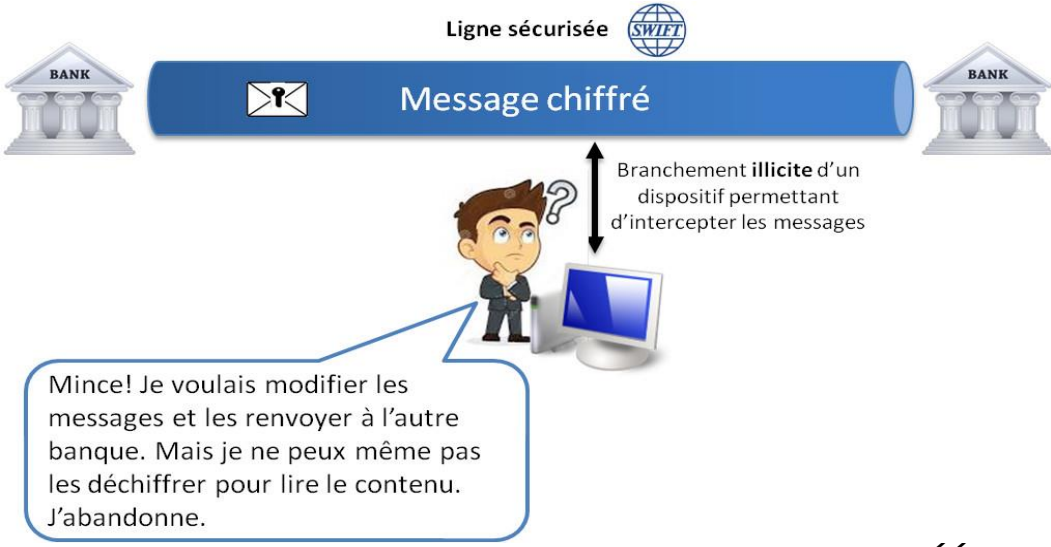
La sécurité d'un système repose sur cinq grands principes:

- ❑ Intégrité des données
- ❑ Confidentialité des données
- ❑ Disponibilité des ressources
- ❑ Authentification des utilisateurs
- ❑ Non répudiation des données

Objectifs de la Sécurité Informatique

L'intégrité des données: il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication.

La confidentialité : seules les personnes habilitées doivent avoir accès aux données.
Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées,
seuls les acteurs de la transaction possédant la clé de compréhension.



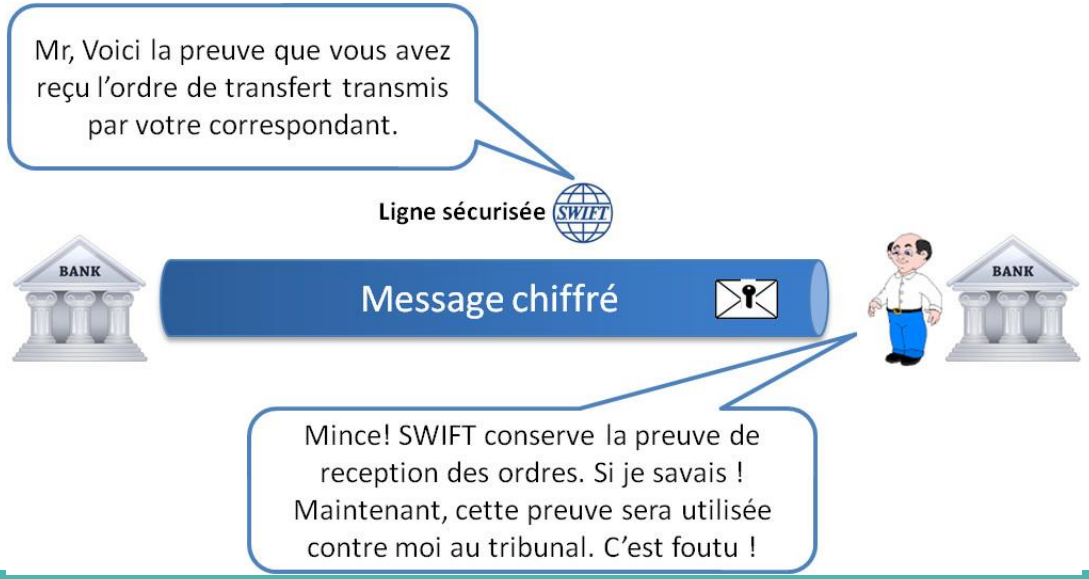
Objectifs de la Sécurité Informatique

- **La disponibilité:** il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment.

- **L'authentification :** elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

Objectifs de la Sécurité Informatique

La non-répudiation des données : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues.



Mise en place d’une politique de sécurité

La sécurité informatique, n’est pas qu’un mot de passe !

Il est inutile de blinder la porte alors que les fenêtres sont ouvertes !

Il est nécessaire d’entreprendre la sécurité informatique dans un cadre global : il faut une politique de sécurité

Mise en place d’une politique de sécurité

Dans un contexte global, la sécurité doit être assurée:

- **au niveau utilisateur**: les acteurs doivent comprendre l'importance de leur position.
- **au niveau des technologies utilisées**: elles doivent être sûres et ne pas présenter de failles.
- **au niveau des données en elles-mêmes**: avec une bonne gestion des droits d'accès (authentification et contrôle) l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires.

Mise en place d’une politique de sécurité

- **au niveau physique** (accès à l'infrastructure, au matériel): rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

Mise en place d’une politique de sécurité

Démarche de mise en place d’une politique de sécurité:

1. Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences
2. Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
3. Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
4. Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;