Module Sécurité Informatique (F332)

Organisation du module

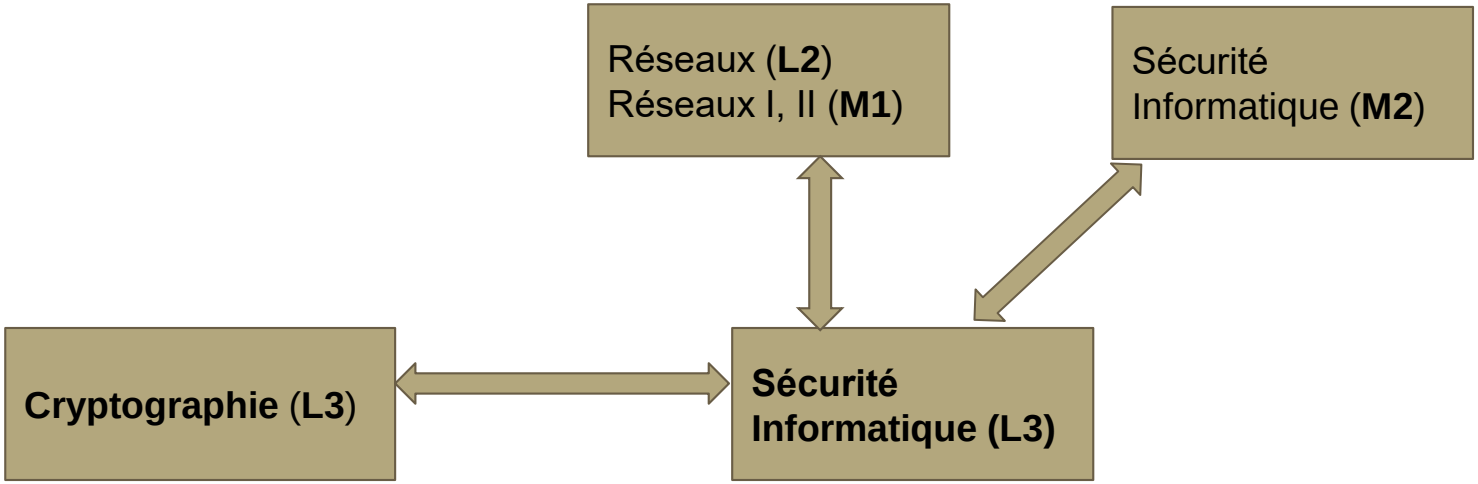
- 12/13 semaines d'enseignement :
  1.5 H cours magistrale (CM)
  1.5 H Travaux dirigés (TD)
  Pas de séances de TP

- Évaluation: Examen Final, Contrôle Continu

A propos du module Sécurité Informatique

- Un **nouveau** module de la formation **L3** depuis 2015-2016
- Au paravent, il était enseigner en **M1** ou **M2**

Interactions avec d'autres modules



- En pratique le module sécurité s'intègre, interagit avec tous les autres modules (BDD, OS, P2P, Web, etc.)

Plan du Module

- **Partie I**:Notions de Base sur la Sécurité Informatiques
  - Comprendre les motivations, les besoin de sécurité
  - Panorama des menaces, risques et attaques de sécurité
  - Les besoins en services de sécurité
  - 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:Notions de Base sur la Sécurité Informatique

Cours 1- Introduction: De la sécurité des biens et des personnes 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.

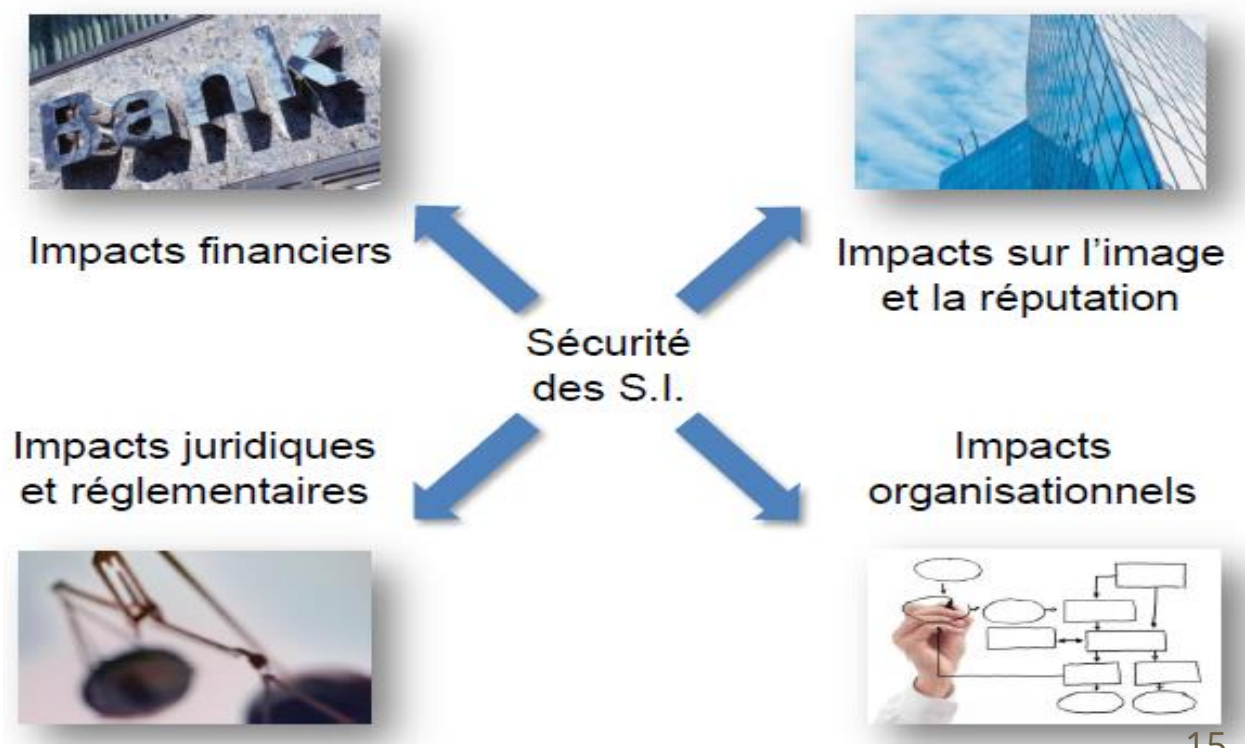
Sécurité Informatique, Pourquoi?

- 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