Paradigmes de la cybersécurité

- Cyber défense : définition et limites
- Définition
  - Mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face aux cyber attaques
  - Exemples : IDS, SIEM, SOC
- Limites
  - Impossible d'assurer une détection à 100%
  - Attaques « zero day »
  - Techniques d'évasion
  - Attaques furtives

Paradigmes de la cybersécurité

- Cyber résilience
- Définition
  - Capacité d'un système à résister à des cyberattaques qui réussissent

La question n'est pas :

Mon système va-t-il être attaqué ?

Mais,

Quand mon système va-t-il être attaqué ?

Paradigmes de la cybersécurité

- Cyber résilience : d'autres propriétés
- Absorbabilité
  - Capacité du système à absorber les conséquence d'une attaque sous souffrir d'une défaillance complète
- Adaptabilité
  - Capacité du système d'ajuster son comportement en fonction des changements de l'environnement ou de sous-ensembles du système lui-même
- Recouvrabilité
  - Capacité du système de revenir dans un état normal

Paradigmes de la cybersécurité

- Cyber résilience : quelques exemples de solutions
  - Diversification fonctionnelle
  - Défense en profondeur
  - Défense dynamique et adaptative

Questions ?

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420a: Sécurité Informatique
Séance2 : Analyse et gestion des risques

Nora Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Contenu du cours

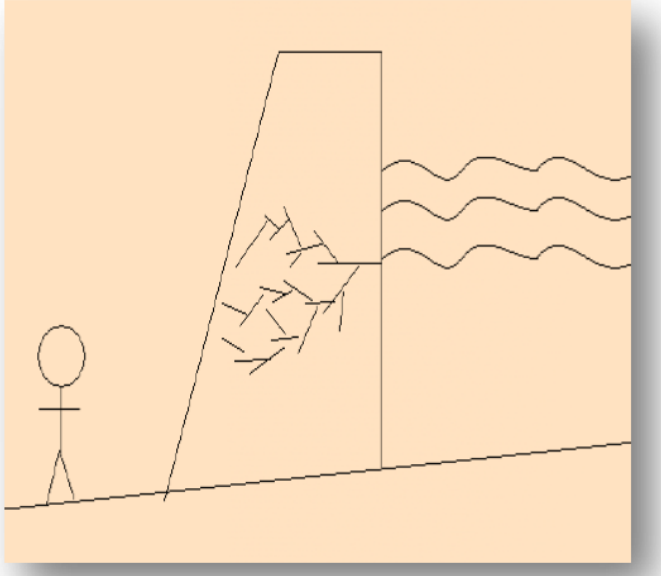
- Concept de menace
- Concept de vulnérabilité
- Concept de risque
- Evaluation des risques
- Réduction des risques
- Analyse de risques
- Méthodes d'analyse des risques

Objectifs de la SSI

- Empêcher l'exploitation de failles (vulnérabilités) contre le système d'information par des acteurs malveillants (menace)

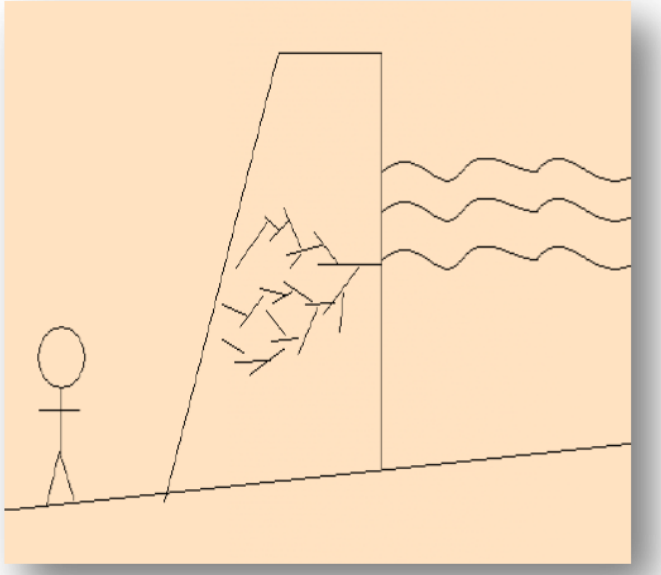
Menace

- Bien
  - Objet/personne ayant de la valeur
- Acteur/agent de menace
  - Objet/personne/entité qui met un bien à risque
- Scenario
  - Séquence d'évènement menant à la perte partielle ou totale de la valeur d'un bien



Attaque

- Concrétisation de la menace
  - Acteur + Scenario
  - « Une méthode (COMMENT)
    par laquelle un acteur particulier (QUI)
    entreprend une action (QUOI)
    pour faire subir un dommage à un bien
    (POURQUOI) »



La menace en sécurité informatique

- Quel type de menaces ?
  - Accidentelles (acteur inconscient ou absence d'acteur)
    - Catastrophes naturelles (« acts of God »)
      - feu, inondation, …
    - Actes humains involontaires
      - mauvaise entrée de données, erreur de frappe, de configuration, …
    - Performance imprévue des systèmes
      - Erreur de conception dans le logiciel ou le matériel
      - Erreur de fonctionnement dans le matériel

  ☚ Sûreté

  - Malveillantes ou Délibérées (acteur conscient)
    - Attaque de déni de service (atteinte à la disponibilité)
    - Vol d'informations (atteinte à la confidentialité)
    - Modification non-autorisée des systèmes (atteinte à l'intégrité)
    - …

  ☚ Sécurité

La menace en sécurité informatique

- Qui sont les « acteurs » ?
  - Catastrophes naturelles
  - Pirate/Hackers
    - "Script kiddies"
    - « Black hat » (et White Hat)
    - Professionels
  - Concurrents
  - États étrangers
  - Crime organisé
  - Groupe terroriste
  - Compagnie de marketing

☚ Externe

  - Ceux à qui vous faites confiance…

☚ Interne

Vulnérabilité

- Vulnérabilité
  - Faille qui offre l'opportunité de porter dommage à un bien
- Scénario
  - Exploitation d'une vulnérabilité par un acteur pour causer un impact
- Probabilité
  - Que la menace soit réalisée (dans une période de temps donné)
- Impact
  - Perte ou dommage à un bien

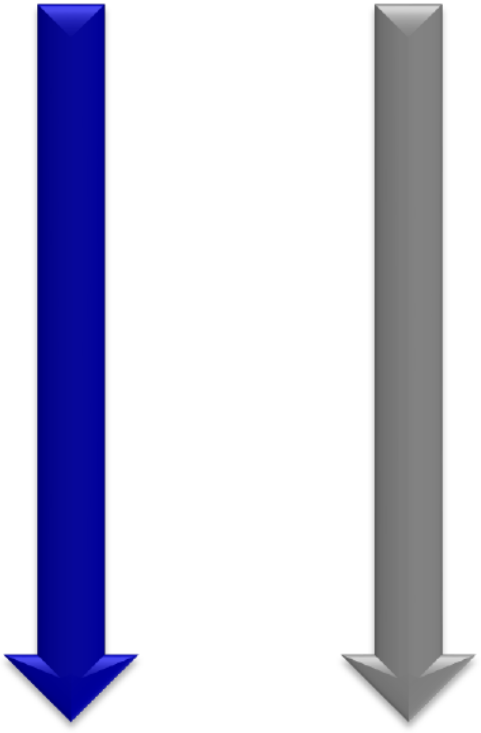
Vulnérabilité - exemple

- Biens
  - Barrage et Vies humaines
- Vulnérabilités
  - Faiblesse du barrage et
  - Usure de la vanne ou
  - Vulnérabilité logicielle de la vanne
- Menace
  - Panne accidentelle de la vanne ou
  - Attaque terroriste
- Risque
  - Rupture du barrage et
  - Perte de vies humaines

Vulnérabilité informatique

- Vulnérabilité = Faille
  - Causée par une erreur = bug

- Conception
- Implémentation
- Installation / Configuration
- Exploitation
- Mise à jour / Maintenance
- Suppression / Destruction



Vulnérabilité informatique Security vs. Safety

- Partie vulnérabilité
  - Pas de différence significative entre sécurité informatique et sureté de fonctionnement
- C'est la partie menace qui diffère
  - Menace accidentelle pour la sureté de fonctionnement
  - Menace délibérée pour la sécurité informatique
- Conséquence très importante pour évaluer les risques

Risque

- Définition qualitative
  - La prise en compte d'une exposition à un danger, un préjudice ou autre événement dommageable, inhérent à une situation ou une activité
  - Un risque correspond à la combinaison d'une vulnérabilité et d'une menace

Risque

- Définition quantitative

Risque = probabilité * impact
= espérance de perte

Il faut être conscient du niveau de risque avant de prendre une décision

- Le risque est inhérent à l'activité
  - Il est impossible de l'éliminer
  - On peut le « gérer » par
    - Réduction
    - Transfert
    - Acceptation
    - Arrêt de l'activité

Risque – « Reality Check »

- Il y a un risque s'il y a un enjeu réel relié au bien
  - Même si une vulnérabilité (scénario) et un acteur existent
    - Pas d'impact ➔ pas de risque
- Il y a un risque si un scénario a une chance de se réaliser
  - Même si une vulnérabilité existe
    - Pas d'acteur ➔ Pas de risque
  - Même s'il y a un acteur,
    - Pas de vulnérabilité ➔ pas de scénario ➔ pas de risque
- Mais comment gérer/estimer les risques potentiels ?
  - Vulnérabilité non encore identifiée
  - Menace non encore identifiée

Risque

- Le risque informatique s'apparente à
  - une loterie où on ne peut pas ~~perdre~~ gagner !

$$E = P \times I$$

Espérance de perte

Probabilité d'incident

Impact d'un incident