INF8085: Cybersécurité
Cours 2 : Exercices

Frédéric Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Objectif
  - Savoir distinguer entre vulnérabilité, menace et risque
  - Savoir identifier un risque et une contre-mesure

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 1 : Il risque de pleuvoir aujourd'hui

- Question 1 : Est-ce qu'il s'agit,
  1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 1 : Il risque de pleuvoir aujourd'hui

- Question 2 : Identifier une vulnérabilité pour cette menace
  2. J'ai des gougounes, je n'ai pas de manteau
  3. Je vais être mouillé
  4. J'ai pris un parapluie ce matin

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 2 : Un hacker montre qu'il est possible de détourner à une dizaine de mètres un défibrillateur (pacemaker) pour envoyer des chocs électriques à distance

- Question 3 : Est-ce qu'il s'agit :
  1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 2 (suite) : Le vice-président des Etats-Unis décide de désactiver la fonction sans-fil de son pacemaker

- Question 4 : Est-ce qu'il s'agit,
  1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 3 : Un médecin chiffre ses données médicales sans séquestre de la clé de chiffrement

- Question 5 : Est-ce qu'il s'agit,
  1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?

Exercice d'analyse des risques

- Exercice 1 : Vulnérabilité, Menace et Risque

- Exemple 3 : Les données médicales sont indisponibles

- Question 6 : Est-ce qu'il s'agit,
  1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?

Exercice d'analyse des risques

- Exercice 2 : Analyse de risque

- Objectif
  - Savoir identifier les risques dans un cas simple

- Étude de cas
  - SuperMarché est une compagnie qui vend des franchises de commerce au détail. Elle a bâti une application pour permettre à ses franchisés de mettre à jour leurs ventes pour que SuperMarché redistribue les profits
  - L'intégrité des résultats financiers est la principale préoccupation de la compagnie

Exercice d'analyse des risques

- Exercice 2 : Analyse de risque

- Étape 1 : Définir les agents de menace et les scénarios
  - Agents de menace ?
  - Scénarios ?
  - Menaces ?

Exercice d'analyse des risques

- Exercice 2 : Analyse de risque

Agents de menace	Scénarios	Menaces

Exercice d'analyse des risques

- Menace 1 = (hacker, serveur central)
  - Un hacker exploite une vulnérabilité du serveur central

- Question 1
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?

Exercice d'analyse des risques

- Menace 2 = (hacker, données marchand)
  - Un hacker exploite une vulnérabilité chez le marchand

- Question 2 (par rapport à menace 1)
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?

Exercice d'analyse des risques

- Menace 3 = (marchand, serveur central)
  - Un marchand malveillant exploite une vulnérabilité du serveur central

- Question 3 (par rapport aux Menaces 1 et 2)
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?

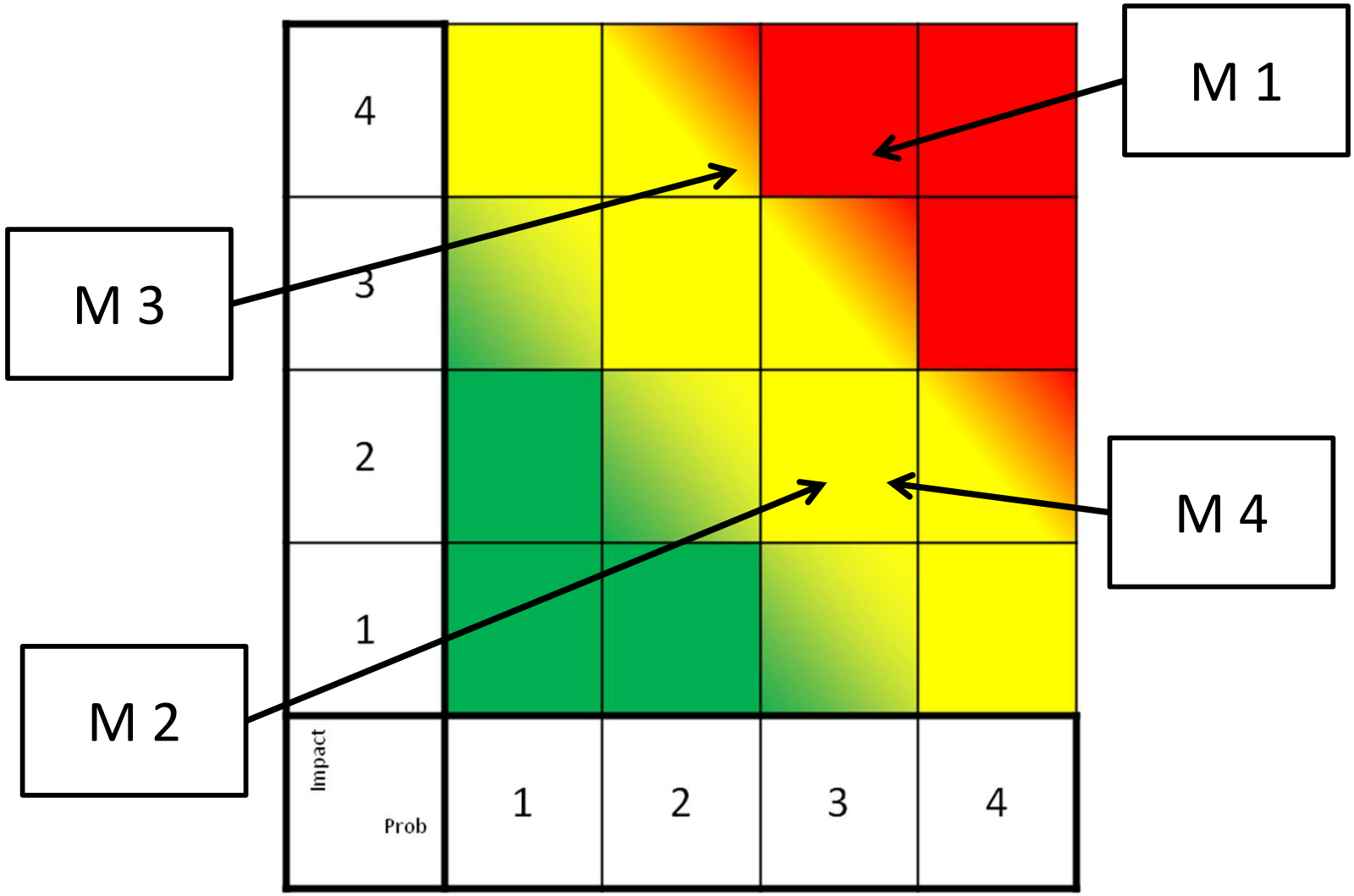
Exercice d'analyse des risques

- Menace 4 = (marchand, données marchand)
  - Un marchand malveillant falsifie ses données

- Question 4 (par rapport à menace 1, 2 et 3)
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?

Exercice d'analyse des risques

- Récapitulatif



Exercice d'analyse des risques

- Conclusion de l'analyse de risque

- On doit se préoccuper en priorité de Menace 1 et de Menace 3
- Selon notre tolérance au risque, il faut s'occuper de Menace 2 et Menace 4
  - Si très tolérant, on accepte dans la zone jaune
  - Si peu tolérant, on doit contrôler dans la zone jaune
- Comment contrôler ?
  - Application de contremesures

Exercice d'analyse des risques

- Question 5 : Proposition de contremesures ?
  - Réponse question 5 : voir la suite du cours INF4420A !

Études de cas - Analyse de risque

- Exercice 3 : Analyse de risque

- Étude de cas
  - L'introduction de technologie sans-fil pour les périphériques de PC (infrarouge, Bluetooth, etc.) a permis l'introduction à bas prix de clavier sans-fil
  - L'utilisation de ce type de dispositif à plusieurs avantages
    - Commodité d'utilisation
    - Prix peu élevé
- Objectifs
  1. Évaluer les risques inhérents liés à l'utilisation de ce type de dispositif
  2. Évaluer le risque résiduel des différentes contremesures

Études de cas - Analyse de risque

- Question 1 : Quelles sont les vulnérabilités (potentielles) du clavier sans-fil ?
  - Confidentialité ?
  - Intégrité ?
  - Disponibilité ?

Étude de cas – Scénarios

- Cas 1
  - Un fermier qui fait pousser du pot dans sa ferme isolée et qui utilise son ordinateur pour faire sa comptabilité (qui lui doit combien ou vice-versa, toutes ses commandes, etc.) et pour communiquer avec ses acheteurs (par courriel)
- Cas 2
  - Une étudiante en résidence qui a un chum très jaloux et qui utilise son ordinateur pour faire ses travaux, communiquer avec ses autres amis et payer ses factures
- Cas 3
  - Une secrétaire dans un bureau d'avocats dans une tour à bureau à Place Ville-Marie qui écrit et/ou édite toute la correspondance et les documents de sa patronne, une avocate en droit pénal (possiblement l'avocate du fermier…).

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

A la semaine prochaine

Frédéric Cuppens