



# INF4420a: Sécurité Informatique

## Exercices séance 1

### Introduction : Concepts de base et motivation

Frédéric et Nora Cuppens

- Exemple 1 : Inondation (flooding)
  - Définition : Attaque qui consiste à envoyer une grande quantité de messages inutiles dans un réseau



# Exercice 1 : vocabulaire des attaques

- Question 1 : Le flooding permet une attaque contre,
  - a) La disponibilité
  - b) L'intégrité
  - c) La confidentialité
- Exemple 1 : Inondation (flooding)
  
- Réponse question 1
  - a) La disponibilité



# Exercice 1 : vocabulaire des attaques

- Exemple 2 : Écoute passive (sniffing)
  - Définition : Attaque qui consiste à capturer le trafic réseau en utilisant un « sniffer »
  
- Question 2 : Un sniffing permet une attaque contre,
  - a) La disponibilité
  - b) L'intégrité
  - c) La confidentialité



# Exercice 1 : vocabulaire des attaques

- Exemple 2 : Écoute passive (sniffing)
- Réponse question 2 :
  - c) La confidentialité



# Exercice 1 : vocabulaire des attaques

- Exemple 3 : Détournement de session (hijacking)
  - Définition : Attaque qui permet de prendre le contrôle d'une communication légitime
- Question 3 : Un hijacking permet une attaque contre,
  - a) La disponibilité
  - b) L'intégrité
  - c) La confidentialité



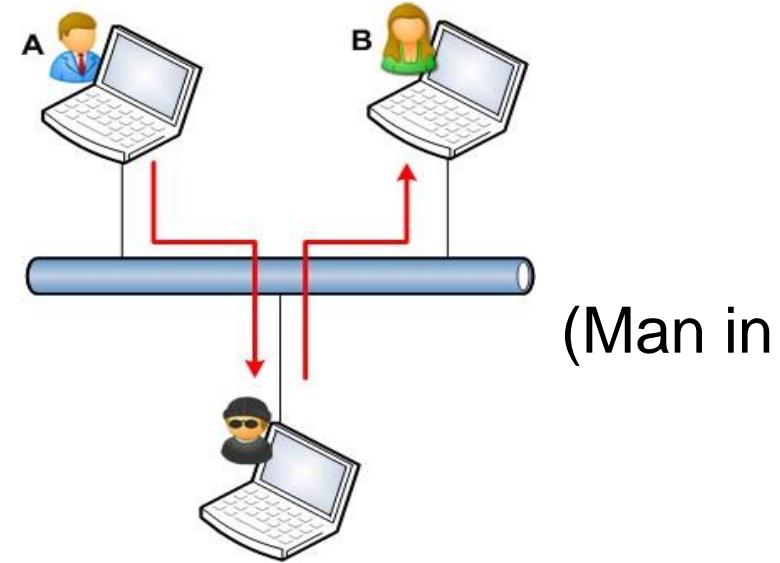
# Exercice 1 : vocabulaire des attaques

- Exemple 3 : Détournement de session (hijacking)
- Réponse question 3 :
  - a) La disponibilité
  - b) L'intégrité
  - c) La confidentialité
- Exemple 4 : Homme du milieu (Man in the Middle)
  - Définition : Attaque qui permet de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent



# Exercice 1 : vocabulaire des attaques

- Question 4 : Un Man in the Middle permet une attaque contre :
  - a) La disponibilité
  - b) L'intégrité
  - c) La confidentialité
- Exemple 4 : Homme du milieu (the Middle)





# Exercice 1 : vocabulaire des attaques

- Réponse question 4 :
  - b) L'intégrité
  - c) La confidentialité
- Exemple 4 : Homme du milieu (Man in the Middle)
- Question 5 : Une attaque Man in the Middle est plus facile à réaliser si le protocole est TCP que si c'est UDP
  - a) Vrai



# Exercice 1 : vocabulaire des attaques

- b) Faux
- Exemple 4 : Homme du milieu (Man in the Middle)
- Réponse question 5 :
  - b) Faux
    - Comme TCP est un protocole connecté, c'est en général plus difficile de s'insérer dans une connexion établie
    - En général, c'est plus facile avec UDP qui n'est pas connecté



# Exercice 2 : les propriétés de sécurité

- 3 propriétés de base
  - Confidentialité
  - Intégrité
  - Disponibilité
- On ajoute souvent une quatrième propriété
  - Auditabilité
- Et aussi de très nombreuses autres propriétés
  - Authenticité, Non-répudiation, Fraicheur, Horodatage, ...
- Pourquoi ?
- Données et métadonnées



# Exercice 2 : les propriétés de sécurité

- Exemple : envoi d'un message

Données =  
contenu du message

Métadonnées =  
associées au message



# Exercice 2 : les propriétés de sécurité

Hello,  
Aujourd'hui début du cours  
INF4420A

Event Viewer						
	Action	View	Help			
Tree View	Application	Security	System			
<b>Observateur d'événements (local)</b>						
Type	Date	Heure	Source	Catégorie	Événement	Utilisateur
✓ Audit des succès	24/09/2010	15:31:57	Security	Utilisatio...	576	ramerie
✓ Audit des succès	24/09/2010	15:31:55	Security	Utilisatio...	576	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:31:55	Security	Ouvrur...	528	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:31:52	Security	Utilisatio...	578	ramerie
✓ Audit des succès	24/09/2010	15:31:32	Security	Utilisatio...	578	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:29:55	Security	Ouvrur...	528	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:27:55	Security	Utilisatio...	576	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:27:54	Security	Ouvrur...	528	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:26:55	Security	Utilisatio...	577	SYSTÈME
✓ Audit des succès	24/09/2010	15:26:55	Security	Utilisatio...	576	SERVICE RÉSEAU
✓ Audit des succès	24/09/2010	15:26:55	Security	Ouvrur...	528	SERVICE RÉSEAU
✓ Audit des succès	24/09/2010	15:26:42	Security	Utilisatio...	578	ramerie
✓ Audit des succès	24/09/2010	15:26:42	Security	Utilisatio...	578	ramerie
✓ Audit des succès	24/09/2010	15:26:42	Security	Utilisatio...	578	ramerie
✓ Audit des succès	24/09/2010	15:26:05	Security	Utilisatio...	578	ramerie
✓ Audit des succès	24/09/2010	15:25:54	Security	Utilisatio...	576	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:25:54	Security	Ouvrur...	528	SERVICE LOCAL
✓ Audit des succès	24/09/2010	15:25:38	Security	Utilisatio...	578	ramerie

Journal d'audit = auditabilité  
du message

- On peut attaquer le contenu du message
  - Sa confidentialité
  - Son intégrité
  - Sa disponibilité

Emetteur / Destinataire  
Adresse de l'émetteur  
Adresse du destinataire  
Date d'émission  
Date de réception  
Route de transmission  
Flags : Urgent, prioritaire, ...  
Flags de sécurité : secret, confidentiel, ...  
Protocole de transmission  
...



## Exercice 2 : les propriétés de sécurité

- On peut attaquer les métadonnées associées au message
  - En général, leur intégrité
  - Mais aussi parfois leur confidentialité lorsque les métadonnées doivent elles-mêmes rester secrètes
- Exemple 1 : Authenticité
  - Définition : Garantie qu'il n'y a pas de falsification de l'émetteur et / ou de son adresse • Authenticité = Intégrité des métadonnées émetteur et adresse de l'émetteur



## Exercice 2 : les propriétés de sécurité

- Exemple 1 : Authenticité
- Question 1 : Donner un exemple d'attaque contre l'authenticité ?
  - a) Inondation (flooding)
  - b) Mascarade (spoofing)
  - c) Rejeu (Replay attack)
  - d) Effacer le fichier de log



## Exercice 2 : les propriétés de sécurité

- e) Écoute passive (sniffing)
- f) Détournement de session (hijacking)
- Exemple 1 : Authenticité
- Réponse question 1 :
  - b) Mascarade (spoofing)
  - f) Détournement de session (hijacking)
- Quelle est la différence entre les deux types d'attaque ?
- Exemple 2 : Non répudiation



## Exercice 2 : les propriétés de sécurité

- Définition : Garantie que l'émetteur ne peut nier avoir effectué une action
- Question 2 : Quelles actions permettent d'attaquer la propriété de non répudiation ?
  1. Inondation (flooding)
  2. Mascarade (spoofing)
  3. Rejeu (Replay attack)
  4. Effacer le fichier de log
  5. Attaquer l'intégrité de l'horloge du système
  6. Détournement de session (hijacking)
- Exemple 2 : Non répudiation



# Exercice 2 : les propriétés de sécurité

- Réponse question 2 :
  4. Effacer le fichier de log



# Exercice 2 : les propriétés de sécurité

- Exemple 2 : Non répudiation
- Question 3 : Quelles actions permettent d'assurer la propriété de non répudiation ?
  1. Vérifier l'émetteur du message
  2. Chiffrer les messages
  3. Signer les messages
  4. Enregistrer les échanges de message dans un fichier de log
  5. Assurer l'intégrité du fichier de log
  6. Envoyer les messages plusieurs fois
- Exemple 2 : Non répudiation



# Exercice 2 : les propriétés de sécurité

- Réponse question 3
  - 3. Signer les messages
  - 4. Enregistrer les échanges de message dans un fichier de log
  - 5. Assurer l'intégrité du fichier de log
- Exemple 3 : Fraîcheur (Freshness)
  - Définition : Garantie qu'un document est nouveau et n'a pas été utilisé auparavant
- Question 4 : Quelles actions permettent d'attaquer la propriété de fraîcheur ?
  - 1. Inondation (flooding)



## Exercice 2 : les propriétés de sécurité

- 2. Mascarade (spoofing)
- 3. Rejeu (Replay attack)
- 4. Effacer le fichier de log
- 5. Attaquer l'intégrité de l'horloge du système
- 6. Détournement de session (hijacking)
- Exemple 3 : Fraîcheur (Freshness)
- Réponse question 4 :
  - 3. Rejeu (Replay attack)

## Exercice 2 : les propriétés de sécurité

- Exemple 3 : Fraîcheur (Freshness)
- Question 5 : Quelles actions permettent d'assurer la propriété de fraîcheur ?
  1. Chiffrer les messages
  2. Signer les messages
  3. Assurer l'intégrité des métadonnées associées au message
  4. Aucune des réponses proposées
- Exemple 3 : Fraîcheur (Freshness)
- Réponse question 5 :



## Exercice 2 : les propriétés de sécurité

### 4. Aucune des réponses proposées

- Il faut générer des messages appelés « nonce » – Un nonce est un message qui a la propriété d'apparaître pour la première fois
- Exemple 4 : Horodatage
  - Définition : Garantie que la date et l'heure d'une opération ne peuvent être falsifiées
- Question 6 : Quelles actions permettent d'attaquer la propriété d'horodatage ?
  1. Inondation (flooding)



## Exercice 2 : les propriétés de sécurité

- 2. Mascarade (spoofing)
- 3. Rejeu (Replay attack)
- 4. Effacer le fichier de log
- 5. Attaquer l'intégrité de l'horloge du système
- 6. Détournement de session (hijacking)
- Exemple 4 : Horodatage
- Réponse question 6 :
  - 5. Attaquer l'intégrité de l'horloge du système
  - 6. Détournement de session (hijacking)
- Exemple 4 : Horodatage

## Exercice 2 : les propriétés de sécurité

- Question 7 : Quelles actions permettent d'assurer la propriété d'horodatage?
  1. Chiffrer les messages
  2. Signer les messages
  3. Assurer l'intégrité des métadonnées associées au message
  4. Aucune des réponses proposées
- Exemple 4 : Horodatage
- Réponse question 7 : Réponse 3
  3. Assurer l'intégrité des méta-données associées au message





POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉnierie

à la séance prochaine



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉnierie

# INF4420a : Sécurité Informatique

## Cours 2 : Exercices

Nora Cuppens



# 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 1 : Vulnérabilité, Menace et Risque



# Exercice d'analyse des risques

- Exemple 1 : Il risque de pleuvoir aujourd'hui
- Réponse question 1 :
  2. Menace
- 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



# Exercice d'analyse des risques

- 3. Je vais être mouillé
- 4. J'ai pris un parapluie ce matin
- Exercice 1 : Vulnérabilité, Menace et Risque
- Exemple 1 : Il risque de pleuvoir aujourd'hui
- Réponse question 2 :
  1. J'ai des gougounes, je n'ai pas de manteau
- Exercice 1 : Vulnérabilité, Menace et Risque
- Exemple 1 : Il risque de pleuvoir aujourd'hui



# Exercice d'analyse des risques

- Récapitulatif de la solution
  - Menace : il menace de pleuvoir aujourd'hui
  - Vulnérabilité : J'ai des gougounes, je n'ai pas de manteau
  - Risque : Je vais être mouillé
  - Contremesure : J'ai pris un parapluie ce matin
- 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 :



# Exercice d'analyse des risques

1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?
- 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
  - Réponse question 3 : 1. Vulnérabilité



# 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 1 : Vulnérabilité, Menace et Risque



# Exercice d'analyse des risques

- Exemple 2 (suite) : Le vice-président des Etats-Unis décide de désactiver la fonction sans-fil de son pacemaker
- Réponse question 4,
  4. Contremesure
- 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



# Exercice d'analyse des risques

- Récapitulatif de la solution
  - Vulnérabilité : Faille identifiée sur un pacemaker et le vice-président des Etats-Unis est équipé de cette marque de pacemaker
  - Menace : Quelqu'un veut supprimer le vice-président
  - Risque : Crise cardiaque
  - Contre-mesure : Débrancher la fonction sans-fil du pacemaker
- 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,



# Exercice d'analyse des risques

1. D'une vulnérabilité ?
  2. D'une menace ?
  3. D'un risque ?
  4. D'une contremesure ?
- Exercice 1 : Vulnérabilité, Menace et Risque
  - Exemple 3 : Un médecin chiffre ses données médicales sans séquestration de la clé de chiffrement
  - Réponse question 5,
    1. Une vulnérabilité
  - Exercice 1 : Vulnérabilité, Menace et Risque



# Exercice d'analyse des risques

- 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 1 : Vulnérabilité, Menace et Risque
- Exemple 3 : Les données médicales sont indisponibles



# Exercice d'analyse des risques

- Réponse question 6 :
  - 3. Risque
- Exercice 1 : Vulnérabilité, Menace et Risque
- Exemple 3 : Un médecin chiffre ses données médicales sans séquestration de la clé de chiffrement
- Récapitulatif de la solution
  - Vulnérabilité : Chiffrement des données sans séquestration de la clé
  - Menace : Absence ou décès du médecin
  - Risque : Indisponibilité des données médicales
  - Contre-mesure : (Avant) Séquestration de la clé de chiffrement



# Exercice d'analyse des risques

(Après) Force brute, peut s'avérer compliqué

- 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 ?



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉNIERIE

# Exercice d'analyse des risques

- Exercice 2 : Analyse de risque



# Exercice d'analyse des risques

## Agents de menace

## Scénarios Menaces

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



# Exercice d'analyse des risques

- Hackers
- Marchand malveillant
- Scénarios
  - Exploitation d'une vulnérabilité du serveur central – Exploitation d'une vulnérabilité chez le marchand
  - Falsification des données du marchand
- Menaces
  1. Hacker exploite une vulnérabilité du serveur central
  2. Hacker exploite une vulnérabilité chez un marchand
  3. Marchand exploite une vulnérabilité du serveur central
  4. Marchand abuse des ses privilèges pour fausser les données
- Menace 1 = (hacker, serveur)
  - Un hacker exploite une vulnérabilité du serveur central



# Exercice d'analyse des risques

- Question 1
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?
- Menace 1 = (hacker, serveur)
  - Impact : pourrait compromettre tous les résultats financiers !
  - Capacité : les hackers possèdent beaucoup de connaissances et de ressources
  - Motivation : de l'argent en jeu
  - Opportunité : le serveur est accessible à distance, donc accessible au Hacker



# Exercice d'analyse des risques

Menace 1					
Impact	C	M	O	P	R
4	3	4	3	3.33	13.33

- Menace 2 = (hacker, données marchand)
  - Un hacker exploite une vulnérabilité chez le marchand
- Question 2 (par rapport à menace 1)
  - Impact ?
  - Capacité ?
  - Motivation ?
  - Opportunité ?
- Menace 2 = (hacker, données marchand)



# Exercice d'analyse des risques

- Un hacker exploite une vulnérabilité chez le marchand
- Réponse question 2 (par rapport à Menace 1)

Menace 1					
Impact	C	M	O	P	R
4	3	4	3	3.33	13.33

Hacker,  
serveur

- Impact ? ⑦ Inférieur
- Capacité ? ⑦ Egal
- Motivation ? ⑦ Inférieur
- Opportunité ? ⑦ Egal
- Menace 2 = (hameau, données marchand)
- Impact : compromet uniquement les résultats d'un marchand



# Exercice d'analyse des risques

- Capacité : les hackers possèdent beaucoup de connaissances et de ressources
- Motivation : de l'argent en jeu, mais moins qu'en 1
- Opportunité : le serveur du marchand est accessible à distance, donc accessible au Hacker

Menace 2					
Impact	C	M	O	P	R
2	3	3	3	3	6

- Menace 3 = (marchand, serveur)
  - Un marchand malveillant exploite une vulnérabilité du serveur central
- Question 3 (par rapport aux Menaces 1 et 2)



# Exercice d'analyse des risques

- Impact ?
- Capacité ?
- Motivation ?
- Opportunité ?
- Menace 3 = (marchand, serveur)
  - Un marchand malveillant exploite une vulnérabilité du serveur central
- Réponse question 3 (par rapport à Menace 1)
  - Impact ? ⑦ Egal
  - Capacité ? ⑦ Inférieur
  - Motivation ? ⑦ Egal
  - Opportunité ? ⑦ Egal



# Exercice d'analyse des risques

Menace 1	Hacker, serveur				
Impact	C	M	O	P	R
4	3	4	3	3.33	13.33

- Menace 3 = (marchand, serveur)
  - Un marchand malveillant exploite une vulnérabilité du serveur central
- Réponse question 3 (par rapport à Menace 2)
  - Impact ? ⑦ Supérieur
  - Capacité ? ⑦ Inférieur
  - Motivation ? ⑦ Supérieur
  - Opportunité ? ⑦ Egal



# Exercice d'analyse des risques

Menace 2	Hacker, données marchand				
Impact	C	M	O	P	R
2	3	3	3	3	6

- Menace 3 = (marchand, serveur)
  - Impact : pourrait compromettre tous les résultats financiers !
  - Capacité : le marchand moyen possède peu de connaissances informatique
  - Motivation : de l'argent en jeu
  - Opportunité : le serveur est accessible à distance, donc accessible au marchand

Menace 3	C	M	O	P	R
Impact	4	1	4	3	2.66
4	1	4	3	2.66	9.33



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



# Exercice d'analyse des risques

## Menace 1

Hacker, serveur

Impact	C	M	O	P	R
4	3	4	3	3.33	13.33

## Menace 2

Hacker, données marchand

Impact	C	M	O	P	R
2	3	3	3	3	6

## Menace 3

Marchand, Serveur

Impact	C	M	O	P	R
4	1	4	3	2.66	9.33

- Réponse question 4 :
  - % Menace 1 : Inf / Sup / Inf / Sup
  - % Menace 2 : Egal / Sup / Egal / Sup – % Menace 3 : Inf / Sup / Inf / Sup
- Menace 4 = (marchand, données marchand)



# Exercice d'analyse des risques

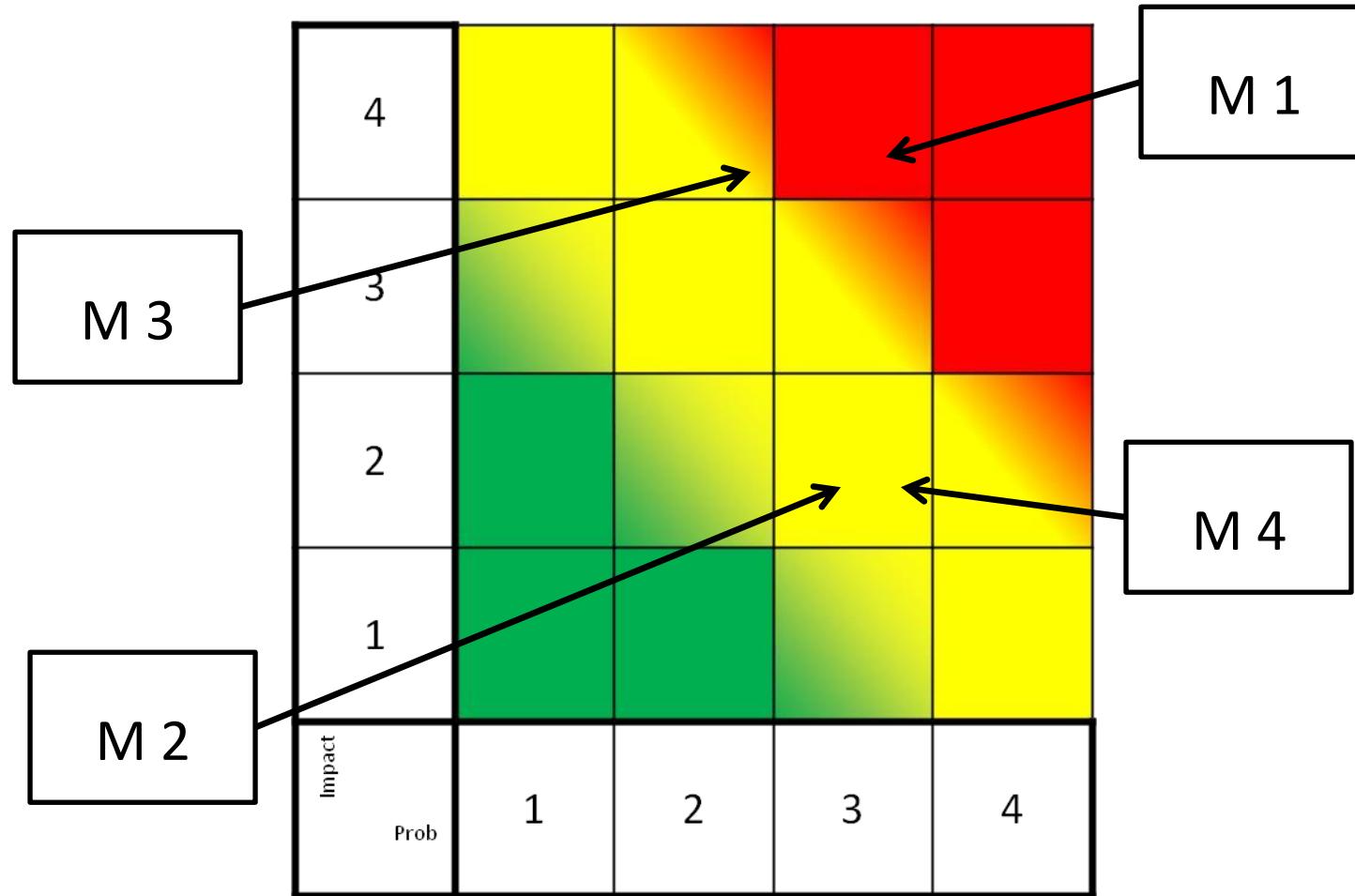
- Impact : compromet uniquement les résultats d'un marchand
- Capacité : le marchand est autorisé et possède les accès requis
- Motivation : de l'argent en jeu, mais moins qu'en 3
- Opportunité : le serveur du marchand est accessible au marchand et il a tous les accès

Menace 4					
Impact	C	M	O	P	R
2	4	3	4	3.66	7.33



# 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
- 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



# Études de cas - Analyse de risque

2. Évaluer le risque résiduel des différentes contremesures
  - Question 1 : Quelles sont les vulnérabilités (potentielles) du clavier sans-fil ?
    - Confidentialité ?
    - Intégrité ?
    - Disponibilité ?



# Études de cas - Analyse de risque

- Vulnérabilités (potentielles) du clavier sans-fil
  - Confidentialité : écoute passive (sniffing) entre le clavier et l'ordinateur
  - Intégrité : interception entre le clavier et l'ordinateur (man in middle)
  - Disponibilité : brouillage (jamming) entre le clavier et l'ordinateur



# 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

## A la semaine prochaine

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...).

Nora Cuppens



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉnierie

# INF4420a: Sécurité Informatique

## Exercice séance 2 : Cryptographie 1



# Exercices de crypto

- Exercice 1 : Calcul d'entropie
- Objectif
  - Savoir évaluer l'entropie d'une source



# Exercices de crypto

- Exercice 1 : Calcul d'entropie

- Vous avez une source sans mémoire qui sort un résultat pile ou face
- La source sort pile avec une proportion de 90 % et face avec une proportion de 10 %
- Vous placez 10 entrées dans un tampon (buffer) et vous voulez calculer l'entropie dans ce tampon



# Exercices de crypto

- Exercice 1 : Calcul d'entropie
- Question 1 : quelle est l'entropie de ce tampon ?
  1. 1.11 bits
  2. 3.32 bits
  3. 4.69 bits
  4. 10 bits



- Exercice 1 : Calcul d'entropie
- Réponse question 3 :
  3. 4,69 bits
- Définition de l'entropie de Shannon d'une source :
  - $H(S) = \sum_i p_i \log_2 (1/p_i)$  avec  $1 \leq i \leq N$
- Entropie de notre source :
  - $H(S) = 0,1 * \log_2 (1/0,1) + 0,9 * \log_2 (1/0,9)$
  - $H(S) = 0,1 * 3,32 + 0,9 * 0,152 = 0,332 + 0,137 = 0,469$  bit
- Entropie de notre tampon
  - $S^b$  : source obtenue en mettant b symboles de S dans un tampon
  - Si S est markovien, alors  $H(S^b) = b * H(S) = 10 * 0,469 = 4,69$  bits



- Exercice 2 : Entropie d'un mot de passe
  
- Objectif
  - Savoir calculer l'entropie d'un mot de passe
  - Savoir calculer la probabilité de casser un mot de passe
- Exercice 2 : Entropie d'un mot de passe



# Exercices de crypto

- Vous avez conçu un site proposant une application pour téléphone qui exige un nombre de 6 caractères alphanumériques pour un mot de passe (minuscules, majuscules et chiffres)
- On suppose que les usagers choisissent leur mot de passe de manière aléatoire, avec tous les caractères étant équiprobables
- Cependant, comme les utilisateurs doivent entrer leur mot de passe au téléphone, le quart des usagers utilisent un mot de passe composé uniquement de chiffres
- Exercice 2 : Entropie d'un mot de passe



# Exercices de crypto

- Question 1 : Calculez l'entropie moyenne du mot de passe choisi par les usagers
  1. Environ 20 bits
  2. Environ 26 bits
  3. Environ 32 bits
  4. Environ 36 bits



- Réponse question 1 :
- Pour les usagers ayant choisi uniquement des chiffres
  - Entropie de la source correspondant à chaque chiffre :
    - $H(S) = \sum_i p_i \log_2 (1/p_i)$  avec  $0 \leq i \leq 9$
    - $H(S) = 10 * 0,1 \log_2 (1/0,1) = \log_2 (10)$  (chaque chiffre est équiprobable)
    - $H(S) = 3,322$  bits
  - Entropie de la source correspondant au mot de passe
    - $H(S) = 6 * 3,322 = 19,93$  bits (source markovienne)
  - Remarque : on peut calculer ça différemment
    - Il y a 1000000 mots de passe possibles soit  $10^6$  combinaisons possibles
    - $10^6 \approx 2^{20}$
    - Un mot de passe correspond à une clé sur approximativement 20 bits
    - Donc l'entropie correspond à approximativement 20 bits



- Réponse question 1 :
- Pour les usagers ayant choisi un mot de passe alphanumérique
  - Entropie de la source correspondant à chaque caractère :
    - $H(S) = \sum_i p_i \log_2 (1/p_i)$  avec  $1 \leq i \leq 62$  ( $26 + 26 + 10$ )
    - $H(S) = \log_2 (62) = 5,954$
  - Entropie de la source correspondant au mot de passe
    - $H(S) = 6 * 5,954 = 35,72$  bits (source markovienne)
  - On vérifie le calcul différemment
    - Il y a maintenant  $62^6$  combinaisons possibles
    - $62^6 = 56\ 800\ 235\ 584 \approx 56,8 * 10^9 \approx 56,8 * 2^{30} \approx 2^6 * 2^{30} = 2^{36}$
    - Un mot de passe correspond à une clé sur approximativement 36 bits
    - Donc l'entropie correspond à approximativement 36 bits



- Réponse question 1 :
- Entropie de la source qui génère les mots de passe
  - Correspond à une source markovienne qui génère aléatoirement  $\frac{1}{4}$  de mot de passe numérique et  $\frac{3}{4}$  de mots de passe alphanumérique
  - $H(S) = \frac{1}{4} * 19,93 + \frac{3}{4} * 35,72 = 31,77$  bits
  - Attention : c'est différent d'une source qui générerait un chiffre dans  $\frac{1}{4}$  des cas et un caractère alphanumérique dans  $\frac{3}{4}$  des cas



# Exercices de crypto

- Vous êtes informés que plusieurs dizaines d'usagers se sont fait pirater leur application
- Un ordinateur est pris en flagrant délit d'usage d'un compte piraté
- L'investigation forensic de l'ordinateur permet de découvrir un maliciel qui transformait l'ordinateur en membre d'un réseau de zombis (botnet)
- L'investigation découvre aussi un script pour réaliser une attaque de force brute sur l'authentification de votre site



# Exercices de crypto

- Le réseau de botnet peut contenir 25 000 ordinateurs infectés
- Chacun ordinateur peut tenter 10 mots de passe par minute
- On suppose que l'attaquant dispose de la liste des noms d'usager
- Mais il ne sait pas quel usager a choisi un mot de passe numérique ou alphanumérique



# Exercices de crypto

- Question 2 : calculez le nombre de mots de passe composés d'une suite de 6 chiffres qui seront en moyenne cassés par jour (au minimum)
  1. Environ 50
  2. Environ 90
  3. Environ 120
  4. Environ 180



- Réponse question 2 :
  - Nombre de mots de passe testés par un ordinateur par jour
    - $10 * 60 * 24 = 14400$  mots de passe par jour
  - Nombre de mots de passe testés par le botnet par jour
    - $14400 * 25000 = 360\ 000\ 000 = 36 * 10^7$  mots de passe par jour
  - Supposons que ces  $36 * 10^7$  mots de passe sont envoyés aléatoirement à l'ensemble des usagers du site
  - Il y aura  $\frac{1}{4}$  de ces mots de passe qui seront envoyés à des usagers ayant choisi un mot de passe numérique, soit  $9 * 10^7$  mots de passe
  - Pour casser un mot de passe numérique, il faut  $10^6$  tentatives (cas pire)
  - L'attaquant va donc pouvoir casser le mot de passe de 90 usagers



- Réponse question 2 :
  - Remarque : s'il y a beaucoup d'usagers, il vaut mieux tester aléatoirement quelques mots de passe sur chaque usager
  - Statistiquement, la loi des grands nombres s'appliquent et l'attaquant parviendra à casser des mots de passe même s'il n'envoie que quelques tentatives sur chaque compte
  - Par contre, l'attaque sera beaucoup plus furtive
- Exercice 3 : Analyse fréquentielle de cryptogramme



# Exercices de crypto

- Objectifs :
    - Comprendre les limites du chiffrement mono-alphabétique
    - Savoir réaliser une analyse fréquentielle
  - Exercice 3 : Analyse fréquentielle de cryptogramme
- 
- Cassez un cryptogramme qui utilise une substitution mono-alphabétique
  - Le texte en clair est en français et ne contient que des lettres
  - C'est un extrait d'une fable de La Fontaine
  - Question 1 : Cassez le cryptogramme suivant,



# Exercices de crypto

gcxobwryv ib ogx tb syiib  
ysyxg ib ogx tbv qmgzev  
t cpb wgqrp wrox qysyib  
g tbv obiybwv t roxrigpv  
vco cp xgeyv tb xcojcyb  
ib qrctsbox vb xorcsq zyv  
ab igyvvb g ebpvbo ig syb  
jcb wyobpx qbv tbcd gzyv  
ib obfgi wcx wrox mrppbx  
oybp pb zgppjcgx gc wbvxyp

- Indication question 1



- Vous pouvez trouver des sites qui calculeront la fréquence d'apparition des caractères dans un texte
- Voir par exemple :
  - <https://www.dcode.fr/analyse-frequencies>
- Pour plus d'information sur l'analyse fréquentielle du français, voir par exemple :
  - [https://fr.wikipedia.org/wiki/Analyse\\_fran%C3%A9quentielle](https://fr.wikipedia.org/wiki/Analyse_fran%C3%A9quentielle)
- Réponse question 1 :



# Exercices de crypto

AUTREFOIS LE RAT DE VILLE  
INVITA LE RAT DES CHAMPS  
D UNE FACON FORT CIVILE  
A DES RELIEFS D ORTOLANS  
SUR UN TAPIS DE TURQUIE  
LE COUVERT SE TROUVA MIS  
JE LAISSE A PENSER LA VIE  
QUE FIRENT CES DEUX AMIS  
LE REGAL FUT FORT HONNETE  
RIEN NE MANQQUAIT AU FESTIN



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉNIERIE

# Exercices de crypto

E | A | I | S | T | N | R | U | L | O | D | M | P | C | V | Q | G | B | F | J | H | Z | X | Y | K | W



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉNIERIE

# Exercices de crypto

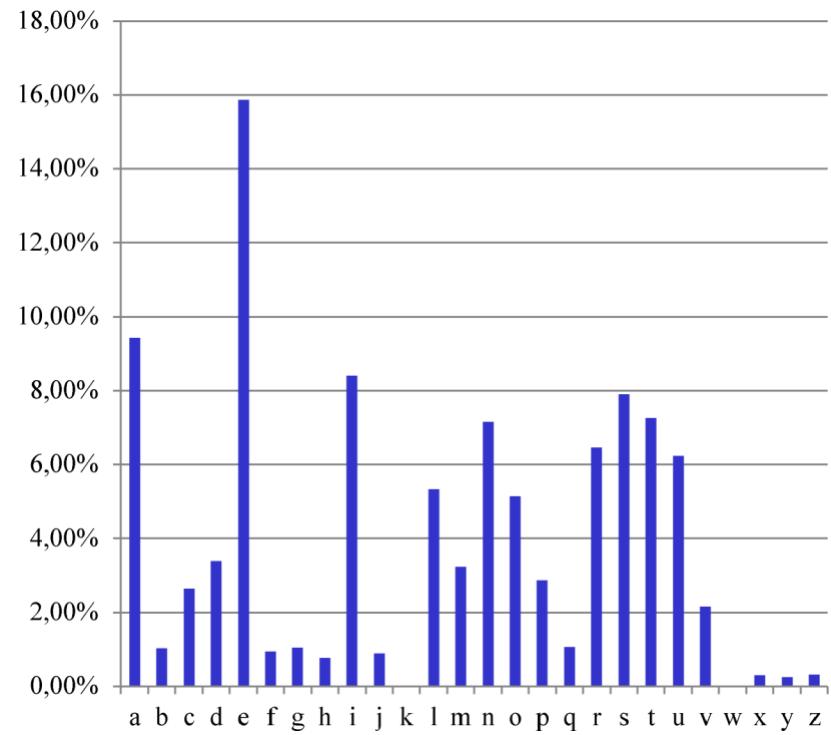
E	A	I	T	S	R	N	U	L	O	F	D	V	C	M	Q	P	H	J	X	G	Z	X	Y	K	W
B	G	Y	X	V	O	P	C	I	R	W	T	S	Q	Z	J	E	M	A	D	F	-	-	-	-	-



# Exercices de crypto

- Réponse question 1 :  
Histogramme des  
fréquence des lettres du  
français

Ci-dessous rangée  
Par fréquence



Histogramme ordonné du texte chiffré  
(en jaune quand il y a égalité)



- Réponse question 1 (complément) :
  - Possibilité de combiner l'analyse fréquentielle sur les caractères avec l'analyse des digrammes (couples de caractères), les trigrammes, ...

Digrammes les plus fréquents en français

Digrammes	Pourcentages
ES	3,15 %
LE	2,46 %
EN	2,42 %
DE	2,15 %
RE	2,09 %
NT	1,97 %

Digrammes les plus fréquents dans le texte

Digrammes	Pourcentages
LE	2,98 %
DE	2,48 %
IS	2,48 %
RT	1,98 %
RE	1,98 %
ES	1,98 %



POLYTECHNIQUE  
MONTRÉAL

UNIVERSITÉ  
D'INGÉnierie

# INF4420a: Sécurité Informatique

## Cours 4 : Exercices Crypto



# Exercice de crypto

- Exercice 1 : Sécurité de DES et 3DES
- Objectif :
  - Comprendre pourquoi en chiffrant plusieurs fois, avec des clés différentes, on ne rallonge pas forcément la longueur de la clé
  - Comprendre pourquoi 3DES reste aujourd'hui difficile à casser
- Exercice 1 : Sécurité de DES et 3DES



# Exercice de crypto

- Rappel de cours
  - DES = chiffrement symétrique (ou à clé secrète)
  - Clé de chiffrement = clé de déchiffrement
  - DES repose sur une clé de chiffrement de 64 bits
  - Mais en fait la clé correspond à 56 bits « utiles »
  - Les 8 derniers bits servent pour le contrôle de parité
  - DES est désormais considéré obsolète



# Exercice de crypto

- Question 1 : Si on applique DES 2 fois avec la même clé de chiffrement, le résultat obtenu va être équivalent à un chiffrement avec une clé de :
  - 56 bits ?
  - 57 bits ?
  - 112 bits ?



# Exercice de crypto

$$m \xrightarrow[k_1]{\quad} E(k_1, m) \xrightarrow[k_1]{\quad} E(k_1, E(k_1, m))$$

- Réponse question 1 : 56 bits
- Explication : Cassage de DES par force brute

$$E(k_1, m) \xrightarrow[k ?]{\quad} D(k, E(k_1, m)) = m \text{ si } k = k_1$$

- Clés de N bits =  $2^N$  clés possibles
- Plus facile de reconnaître m si l'attaquant connaît des correspondances ( $m, E(k_1, m)$ )
  - **Attaque à texte clair connu**



- Réponse question 1 (suite) : Cassage de  $E(k_1, E(k_1, m))$  par force brute

$$M = E(k_1, E(k_1, m)) \xrightarrow{k ?} D(k, M) \xrightarrow{k ?} D(k, D(k, M))$$

- On a  $D(k, D(k, M)) = m$  si  $k = k_1$
- On doit toujours tester  $2^N$  cas possibles pour une clé de  $N$  bits
  - C'est juste un peu plus long pour déchiffrer



# Exercice de crypto

- Question 2 : Si on applique DES 2 fois avec des clés de chiffrement différentes, le résultat obtenu va être équivalent à un chiffrement avec une clé de :
  - 56 bits ?
  - 57 bits ?
  - 112 bits ?



$$m \xrightarrow{k_1} E(k_1, m) \xrightarrow{k_2} E(k_2, E(k_1, m))$$

- Réponse question 2 : 57 bits (c'était dans le cours)
- Explication : Analyse de 2DES
  - On applique DES 2 fois avec des clés différentes

$$m \xrightarrow{k_1} E(k_1, m) \xrightarrow{k_2} E(k_2, E(k_1, m))$$

- On espère avoir ainsi « doublé » la taille de la clé
- Soit  $56 * 2 = 112$  bits
- Pourquoi ?



# Exercice de crypto

- Explication question 2 : Cassage de  $e(k_2, e(k_1, m))$  par force brute « naïve »

$$M = E(k_2, E(k_1, m)) \xrightarrow{k ?} D(k, M) \xrightarrow{k' ?} D(k', D(k, M))$$



# Exercice de crypto

- Dans ce cas, on a  $D(k', D(k, M)) = m$  si  $k = k_1$  ET  $k' = k_2$
- Mais on doit tester  $2^N * 2^N$  cas possibles soit  $2^{N+N} = 2^{2*N}$
- Il semble donc qu'on ait doublé la clé
- Question : Que peut faire l'attaquant pour faire (beaucoup) mieux ?
  - Indice 1 : Penser à une attaque à texte clair connu
  - Indice 2 : L'attaque s'appelle « rencontre du milieu »
    - Meet In the Middle Attack en Anglais (MITM)



- Réponse question 2 : L'attaquant réalise une attaque MITM
  - Supposons que l'attaquant connaît  $m$  et  $M = E(k_2, E(k_1, m))$  pour une paire  $(m, M)$
  - Alors l'attaquant peut calculer :

$$m \xrightarrow[k ?]{} C = E(k, m)$$



# Exercice de crypto

$$M \xrightarrow{k', ?} C' = D(k', M)$$

- Si  $C = C'$ , alors  $(k, k')$  est une paire de clés candidates
- Réponse question 2 (suite) : Attaque MITM
  - Les paires de clés candidates sont en général en petit nombre
  - L'attaquant peut ensuite tester les paires de clés candidates sur d'autres messages pour retrouver  $k_1$  et  $k_2$



- Réponse question 2 (suite) : Attaque MITM
  - Bilan de l'attaque

$$m \xrightarrow[k ?]{} C = E(k, m) \xrightarrow{\text{red arrow}} \mathbf{2^{56} \text{ cas possibles}}$$

$$M \xrightarrow[k' ?]{} C' = D(k', M) \xrightarrow{\text{red arrow}} \mathbf{2^{56} \text{ cas possibles}}$$



# Exercice de crypto

- L'attaquant doit donc faire de l'ordre de  $2^{56} + 2^{56} = 2^{57}$  calculs
- Le double DES est donc « équivalent » à un chiffrement avec une clé de 57 bits
- Une MITM est une attaque de type « compromis temps mémoire »
  
- Pour réaliser une attaque MITM, l'attaquant doit disposer :
  - D'un espace de stockage très grand (hypothèse 1)
  - D'un algorithme de comparaison de chaînes de caractères très rapide (hypothèse 2)



- Question 3 : Quel espace de stockage est nécessaire pour réaliser une attaque MITM dans le cas du 2DES ?
  1. Environ  $500 * 10^{12}$  octets (500 Téraoctets)
  2. Environ  $500 * 10^{15}$  octets (500 Pétaoctets)
  3. Environ  $500 * 10^{18}$  octets (500 Exaoctets)



# Exercice de crypto

- Réponse question 3 : Environ  $500 * 10^{15}$  octets (500 Pétaoctets)
  - Dans le cas de DES, clés de 56 bits et blocs de 64 bits
  - Espace de stockage nécessaire :
    - $2^{56} * 2^6 = 2^{62} = 4 * 2^{60} \approx 4 * 10^{18}$  bits
    - $4 * 10^{18}$  bits =  $500 * 10^{15}$  octets
  - Il faut donc disposer d'un espace de 500 pétaoctets
    - Soit 500 000 téraoctets
    - Irréalistes à la création de DES
    - Mais tout à fait possible aujourd'hui, voir :  
<http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/>



# Exercice de crypto

- Question : L'hypothèse 2 (besoin d'un algorithme de comparaison de chaînes de caractères très rapide) est-elle réaliste ?
  - Difficile de répondre
  - Des idées ?



# Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations:  $E(k_1, D(k_2, E(k_1, m)))$



# Exercice de crypto

- Question 4 : 3DES est équivalent à un chiffrement avec une longueur de clé égale à :
  - 57 bits ( $= 56 + 1$ )
  - 112 bits ( $= 56 * 2$ )
  - 113 bits ( $= 56 * 2 + 1$ )
  - 168 bits ( $= 56 * 3$ )
- Réponse question 4 : 112 bits est la bonne réponse !
  - C'était dans le cours...
- Pourquoi ?

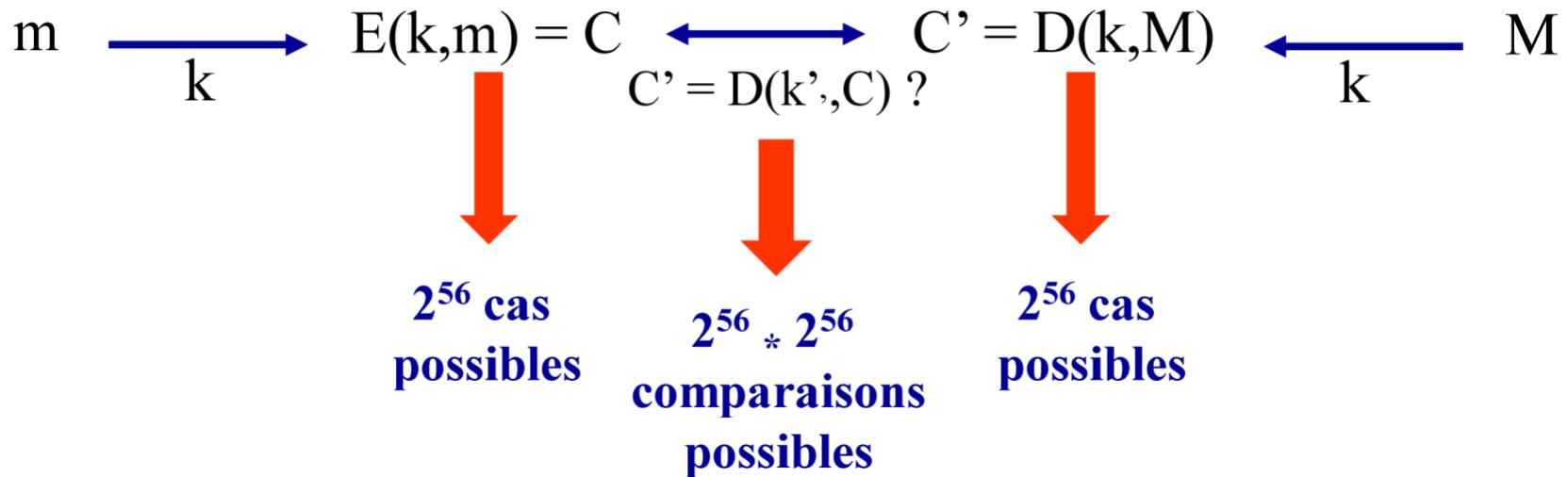


- Réponse question 4 :
  - Attaque en texte clair connu
  - L'attaquant connaît  $m$  et  $M = E(k_1, D(k_2, E(k_1, m)))$
  - Que peut faire l'attaquant ?
    - Une attaque MITM !
  - L'attaquant calcule  $E(k, m)$  pour toutes les clés possibles
    - Il obtient  $C = E(k_1, m)$  pour  $k = k_1$  mais il ne sait pas où est  $C$
  - L'attaquant calcule  $D(k, M)$  pour toutes les clés possibles
    - Il obtient  $C' = D(k_2, E(k_1, m))$  pour  $k = k_1$  mais il ne sait pas où est  $C'$
  - On a donc  $C' = D(k_2, C)$ 
    - Mais l'attaquant ne sait pas où est  $C$  ni où est  $C'$



# Exercice de crypto

- Réponse question 4 :



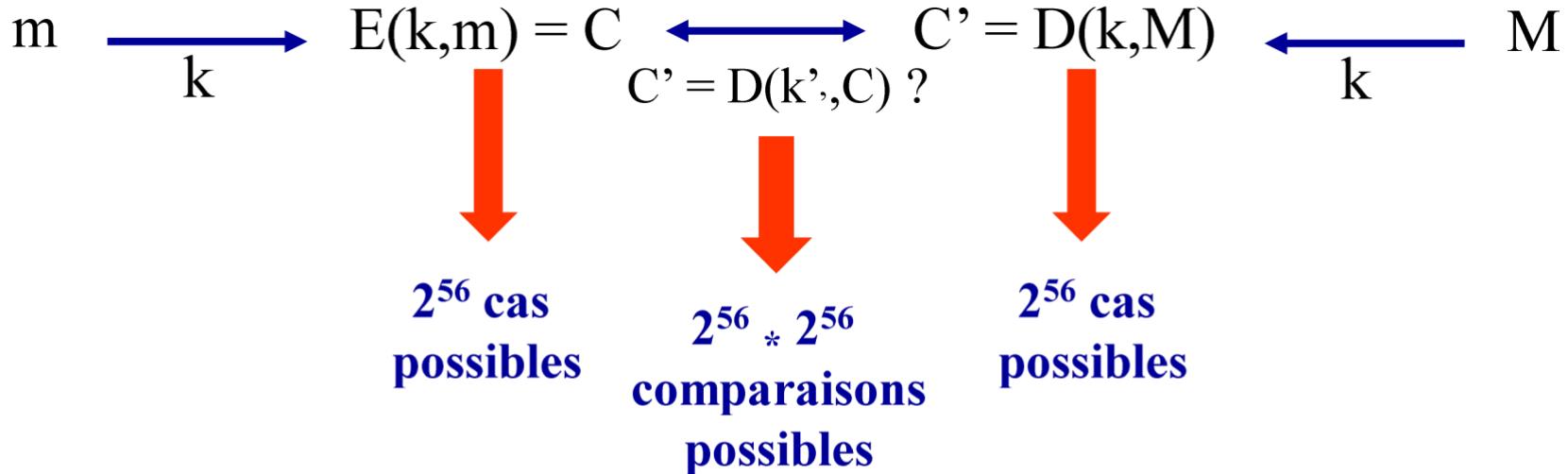


# Exercice de crypto

- Calculs de l'attaquant (cas pire)
  - $2^{56} + 2^{56} + 2^{56} * 2^{56} \approx 2^{112}$
  - Équivalent à une clé de 112 bits
- Réponse question 4 :



# Exercice de crypto



- Calculs de l'attaquant (cas pire)
  - Toujours besoin d'un espace de stockage de 500 pétaoctets !



- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations:  $E(k_1, E(k_2, E(k_1, m)))$ 
    - On a remplacé un déchiffrement par un chiffrement
- Question 5 : Est-ce que ça change quelque chose ?
  - Oui
  - Non



# Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations:  $E(k_1, E(k_2, E(k_1, m)))$ 
    - On a remplacé un déchiffrement par un chiffrement
- Question 5 : Est-ce que ça change quelque chose ?
  - Oui
  - Non



# Exercice de crypto

- Réponse question 5 : Non, ça ne change pas grand chose
  - Analyse de 3DES
    - On utilise toujours deux clefs
    - On réalise trois opérations:  $E(k_1, E(k_1, E(k_2, m)))$
    - On a changé l'ordre de chiffrement



# Exercice de crypto

- Question 6 : Est-ce que ça change quelque chose ?
  - Oui
  - Non
- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations:  $E(k_1, E(k_1, E(k_2, m)))$
  - On a changé l'ordre de chiffrement



- Réponse question 6 : Oui, ça change tout !
  - L'attaquant calcule  $E(k, m)$  et  $D(k', D(k', M))$
  - Il compare comme pour 2DES
  - On obtient une clé équivalente à 57 bits !
- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :

$$E(k_1, E(k_2, E(k_3, E(k_1, m))))$$



# Exercice de crypto

- Question 7 : 4DES serait équivalent à un chiffrement avec une longueur de clé égale à :
  - 112 bits ( $= 56 * 2$ )
  - 113 bits ( $= 56 * 2 + 1$ )
  - 168 bits ( $= 56 * 3$ )
- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :

$$E(k_1, E(k_2, E(k_3, E(k_1, m)))) = M$$



- Réponse question 7 : 113 bits
  - L'attaquant calcule  $D(k, D(k', m))$  pour tous les couples de clés  $(k, k') \rightarrow 2^{112}$  cas possibles
  - L'attaquant calcule  $D(k, D(k', M))$  pour tous les couples de clés  $(k, k') \rightarrow 2^{112}$  cas possibles
  - Il compare
- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :
$$E(k_1, E(k_2, E(k_3, E(k_1, m)))) = M$$



- Réponse question 7 : 113 bits
  - Au final, l'attaquant a fait de l'ordre de  $2^{112} + 2^{112} = 2^{113}$  calculs
  - Il faudrait passer au 5DES pour avoir une clé théorique de 168 bits
  - Par contre, l'attaque MITM n'est plus réaliste car il faudrait un espace mémoire de l'ordre de  $2^{112}$  blocs mémoire, soit  $2^{118}$  bits pour des blocs de 64 bits !
- Exercice 2 : Sécurité de 3DES



# Exercice de crypto

- Objectif :
  - Analyser la sécurité de 3DES
  - Autrement dit, est-ce qu'un algorithme de chiffrement symétrique avec une clé de 112 bits, est-il aujourd'hui sécuritaire ?
  - Et a fortiori, un chiffrement symétrique avec une clé de 128 bits comme conseillé pour AES



# Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Rappel de cours
  - 3DES est équivalent à un algorithme avec une clé de 112 bits
  - Un seul COPACABANA permet de tester environ  $2^{38}$  clés par seconde
- Question 1 : Avec un seul COPACABANA, combien de temps faudrait-il pour craquer 3DES par force brute ?
  1. Environ 500 ans
  2. Environ 500 000 ans
  3. Environ 500 milliards d'années
  4. Environ 500 000 milliards d'années



# Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Réponse question 1 : 4. 500 000 milliards d'années !



- Nombre de secondes nécessaires pour casser 3DES avec COPACABANA :
  - $2^{112} / 2^{38} = 2^{74}$  secondes
- Nombre de secondes dans une année :
  - $60 * 60 * 24 * 365 = 31\ 536\ 000 \approx 32 * 10^6 \approx 2^5 * 2^{20} = 2^{25}$
- Nombre d'années nécessaires pour casser 3DES
  - $2^{74} / 2^{25} = 2^{49} = 2^9 * 2^{40} \approx 500 * 10^{12} \approx 500\ 000$  milliards d'années
- Exercice 2 : Sécurité de 3DES



# Exercice de crypto

- On suppose un scenario apocalyptique comme dans le film “La Matrice” avec un COPACABANA et un panneau solaire sur chaque mètre carré de la Terre (océan et continent)
  - Exercice 2 : Sécurité de 3DES
- 
- Question 2 : Combien de temps faudrait-il « aux machines » pour craquer 3DES par force brute ?
    1. Environ 1 an
    2. Environ 10 ans
    3. Environ 100 ans
    4. Environ 1000 ans



# Exercice de crypto

- Indication :
  - La surface de la terre est d'environ 500 millions de km<sup>2</sup>
- Exercice 2 : Sécurité de 3DES
- Réponse question 2 : Environ 1 an
- Nombre de COPACABANA sur terre :
  - $500 \text{ millions de km}^2 = 500 * 10^6 * 10^6 = 500 * 10^{12}$
- Nombre d'années nécessaires aux machines pour casser 3DES
  - $500 * 10^{12} / 500 * 10^{12} = 1 \text{ an}$



- Exercice 2 : Sécurité de 3DES
- D'après la loi de Moore, la capacité de calcul d'un ordinateur double tous les 18 mois
- Question 3 : En supposant que COPACABANA va suivre la loi de Moore, dans combien de temps un COPACABANA mettra moins d'un an pour casser 3DES ?
  - Moins de 10 ans
  - Moins de 100 ans
  - Moins de 1000 ans
  - Moins de 10000 ans



# Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Réponse question 3 : 2. Moins de 100 ans
- Aujourd'hui, il faut  $2^{49}$  années pour casser 3DES
- On divise ce temps par 2 tous les 18 mois (soit 1,5 an)
- Nombre d'années nécessaires pour casser 3DES en moins d'un an :
  - $49 * 1,5 = 73,5$  années



# Exercice de crypto

- Exercice 3 : Sécurité de DES (question 18 de l'examen intra A2014)
- Vous êtes en possession d'une boîte noire qui fait 200 déchiffrements à la seconde. Quel est le temps moyen pour monter une attaque par force brute à l'aide d'un texte connu (vous possédez un exemplaire chiffré et déchiffré du même texte) pour un algorithme ayant une taille effective de clé de 56 bits ?
  - a. Approximativement 10 740 000 ans.
  - b. Approximativement 14 000 ans.
  - c. Approximativement 300 ans.
  - d. Approximativement 2 200 ans.
  - e. Approximativement 5 370 000 ans.



# Exercice de crypto

- Bonne réponse : e. 5 370 000 ans
- Nombre de seconde dans une année :
  - $60 * 60 * 24 * 365 = 31\ 536\ 000 \approx 32 * 10^6 \approx 2^{25}$
- Nombre d'opérations de déchiffrement réalisées par an :
  - $200 * 2^{25}$
- Nombre d'années nécessaires pour casser une clé de 56 bits par force brut (cas pire nécessaire pour tester toutes les clés possibles) :
  - $2^{56} / (200 * 2^{25}) \approx 10\ 737\ 418$  ans
- Le temps moyen sera statistiquement égal à la moitié du cas pire :
  - $10\ 337\ 418 / 2 = 5\ 368\ 709$  ans

# **INF4420a : Sécurité Informatique**

## **Cours 6 : Authentification – Exercices – Corrigés**

Nora Cuppens

- Question Quiz no. 1
- Choix d'une politique de mots de passe
- Deux politiques vous sont proposées : 1) choisir des mots de passe composés de 6 caractères (lettres minuscules a-z, majuscules A-Z et chiffres 0-9) choisis au hasard et 2) choisir une « phrase » de



# Exercices de crypto

passe composé de quatre mots du français courant, choisis au hasard. D'un point de vue de sécurité, la première option est plus désirable.

- Réponse : b. Faux
- Pourquoi ?
- Question Quiz no. 1
- Choix d'une phrase de passe (de longueur 4)
  - fraiseiPhonepouletrhododendron



# Exercices de crypto

- Choix d'un mot de passe de 6 caractères – rZakh1
- Question Quiz no. 1
- Force d'une phrase de passe (de longueur 4) – Nombre de combinaisons possibles :
  - Choisir un dictionnaire de 1000 mots
  - $1000^4$
  - $= 2^{40}$
- Force d'un mot de passe de 6 caractères – Nombre de combinaisons possibles :



# Exercices de crypto

- $62^6$
- $= 57^9$
- $= 2^{36}$  
- Question Quiz no. 1
- Est-ce que le choix de la langue de la phrase de passe est important ?
  1. Oui
  2. Non



# Exercices de crypto

- 3. Ca dépend
- Question Quiz no. 1
- Est-ce que le choix des mots de la phrase de passe est important ?
  - 1. Oui
  - 2. Non
  - 3. Ca dépend
- Question Quiz no. 1



# Exercices de crypto

- Est-ce qu'on prend un risque important si on révèle le dictionnaire utilisé pour générer la phrase de passe ?
  1. Oui
  2. Non
  3. Ca dépend
- Question Quiz no. 1
- Est-ce qu'on prend un risque important si on révèle le dictionnaire utilisé pour générer la phrase de passe ?



# Exercices de crypto

- Prenons un dictionnaire de 20000 mots
- Ça va engendrer  $20000^4$  combinaisons possibles
- $= 160 * 10^{15}$
- $= 2^7 * 2^{50}$
- $= 2^{57}$
- Même force qu'une clé DES



- Question Quiz no. 7



# Exercices de crypto

- Votre ancienne politique de mots de passe forçait vos usagers à utiliser un mot de passe d'exactement 6 caractères alphabétique en minuscules (a-z). Pour renforcer la sécurité, vous demandez maintenant des mots de passe de 8 caractères, pouvant contenir des minuscules, majuscules et chiffres (a-z + A-Z + 0-9). De combien de bits effectifs avez-vous renforcé le mot de passe si on considère que vos usagers choisissent des mots de passe complètement aléatoires ?
- Réponse : b. Augmentation de 19.4 bits effectifs
- Réponse Quiz question 7 :
- Entropie initiale du mot de passe sur 6 caractères



# Exercices de crypto

- Entropie de la source correspondant à chaque caractère :
  - $H(S) = \sum_i p_i \log_2 (1/p_i)$  avec  $0 \leq i \leq 25$
  - $H(S) = 26 * 1/26 \log_2 (26) = \log_2 (26)$  (chaque lettre est équiprobable)
  - $H(S) = 4,70$  bits
    - Entropie de la source correspondant au mot de passe
  - $H(S) = 6 * 4,70 = 28,20$  bits (source markovienne)
    - Méthode 2
  - Nombre de mots de passe possible  $26^6 \approx 309 * 10^6$
  - $2^{28} \leq 309 * 10^6 \leq 2^{29}$
  - Un mot de passe correspond à une clé entre 28 et 29 bits
  - Réponse Quiz question 7 :



# Exercices de crypto

- Entropie du mot de passe sur 8 caractères
  - Entropie de la source correspondant à chaque caractère :
- $H(S) = \log_2(62)$  (chaque caractère est équiprobable)
- $H(S) = 5,95$  bits
  - Entropie de la source correspondant au mot de passe
- $H(S) = 8 * 5,95 = 47,6$  bits (source markovienne)
  - Différence avant / après
- $47,6 - 28,2 = 19,4$  bits





# Exercices d'authentification

- Exercice 1 : Force d'un mot de passe
- Objectif :
  - Savoir choisir un mot de passe



# Exercices d'authentification

- Exercice 1 : Force d'un mot de passe
- Plusieurs sites possibles pour évaluer la force d'un mot de passe
- Voir par exemple :
  - <https://lowe.github.io/tryzxcvbn/>
- Question 1 : D'après vous, comment ça marche ?
- Réponse question 1 : A vous ...



# Exercices d'authentification

- Réponse question 1 : D'après vous, comment ça marche ?
- Principe de base
  - Repose sur la recherche dans un dictionnaire
  - Plusieurs dictionnaires
  - Dictionnaire multilingue
- Anglais / Français / Chinois
  - Recherche dans le dictionnaire les « patterns » présents dans le mot de passe
  - Lorsqu'un « pattern » apparaît dans plusieurs dictionnaire, le rang le plus bas est retenu
- Réponse question 1 : D'après vous, comment ça marche ?



# Exercices d'authentification

- Transformation sur les mots
  - Retrouve les substitutions « classiques »
- a ⑦ @
- o ⑦ 0
- s ⑦ \$
- Etc.
  - Prend en compte les inversions
- password ⑦ dorwssap
- Réponse question 1 : D'après vous, comment ça marche ?
- Estimation du temps pour casser le mot de passe
  - Dictionnaire ⑦ Rapide



# Exercices d'authentification

- Force brute ⑦ Plus lent
  - Phrase de passe ⑦ Beaucoup plus lent
  - Phrase de passe « complexe » ⑦ Très coûteux
- 
- Pour plus d'information
    - <https://www.usenix.org/conference/usenixsecurity16/technicalsessions/presentation/wheeler>
  - Exercice 1 : Force d'un mot de passe
  - Question 2 : Est-ce que les résultats vous paraissent fiables ?
    1. Oui
    2. Non



# Exercices d'authentification

- Exercice 1 : Force d'un mot de passe
- Réponse question 2 : Oui et non, mais plutôt oui
  - Réaliste pour les attaques par dictionnaire
  - Plus optimiste pour le reste
- Peu de surcout de temps de calcul pour les substitutions
- Peu clair comment est calculé le temps de calcul pour la force brute
- Peu clair comment est calculé le temps de calcul pour les « phrases de passe »





# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Objectifs
  - Savoir identifier les avantages et inconvénients des fonctions d'authentification
- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 1 : Authentification simple UserId + Mot de Passe tapé au clavier
- Voir par exemple :
  - <https://www.rbcroyalbank.com/fr/personal-c.html>



# Exercices d'authentification

- Question 1 : Avantages et risques de cette solution ?
- Réponse question 1 : A vous ...



# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Réponse question 1 :
  - Risque d'attaque par force brute si mot de passe de faible entropie
  - Risque d'interception du mot de passe par un keylogger
  - Risque de récupération du mot de passe
- Phishing, site pirate cloné, social engineering, « post-it »
  - Risque d'attaque contre le fichier des mots de passe
- Notamment attaques « internes »



# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 1 : Authentification simple UserId + Mot de Passe
- Question 2 : Comment limiter les risques de cette solution ?
- Réponse question 2 : A vous ...
- Risque d'attaque par force brute si mot de passe de faible entropie
- Risque d'interception du mot de passe par un keylogger
- Risque de récupération du mot de passe
- Risque d'attaque contre le fichier des mots de passe



# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Réponse question 2 :
  - Risque d'attaque par force brute si mot de passe de faible entropie
- Imposer le choix du mot de passe à l'utilisateur
- Ne pas laisser l'utilisateur choisir son mot de passe n'importe comment
- Obliger l'utilisateur à changer son mot de passe régulièrement
- Limiter le nombre de tentatives infructueuses
  - Risque d'interception du mot de passe par un keylogger
- Utilisation d'un anti-virus, mais pas solution à 100%
  - Risque de récupération du mot de passe
- Sensibilisation des utilisateurs



# Exercices d'authentification

- Risque d'attaque contre le fichier des mots de passe
- Limiter l'accès au fichier des mots de passe (voir cours « Autorisation » et « Sécurité OS »)
- Détection d'anomalies internes (voir cours de « sécurité réseau ») 
- Exercice 2 : Analyse de fonctions d'authentification
  
- Exemple 2 : Authentification simple UserId + Mot de Passe cliqué dans une fenêtre
  
- Voir par exemple :
  - <https://www.credit-agricole.fr/>
  - Identifiant = 11 chiffres (numéro de compte)
  - Code personnel = 6 chiffres



# Exercices d'authentification

- On va revenir là-dessus après l'exemple 3
- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 3 : Une variante intéressante
- Voir :
  - [mobile.free.fr/](http://mobile.free.fr/)
  - Identifiant = 8 chiffres
  - Code personnel = 10 caractères choisis par l'opérateur
- Question 3 : Qu'est-ce que vous trouvez bizarre ?



# Exercices d'authentification

Veuillez saisir votre identifiant grâce aux touches ci-dessous :

9	5	3	1	4
6	8	0	2	7

Identifiant : **Utilisez le pavé numérique ci-dessus.**

Mot de passe :

**Vous avez oublié votre mot de passe ou perdu vos identifiants ?**

- Réponse question 3 : A vous ...



# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 3 : Une variante intéressante
- Question 4 : Est-ce que vous trouvez ça pertinent ?
  1. Oui
  2. Non
- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 2 : Authentification simple UserId + Mot de Passe cliqué dans une fenêtre



# Exercices d'authentification

- Voir par exemple :
  - <https://www.credit-agricole.fr/ca-illeetvilaine/banqueprivee/acceder-a-mes-comptes.html>
  - Identifiant = 11 chiffres (numéro de comptes)
  - Code personnel = 6 chiffres
- Question 5 : Quels sont les risques de cette solution ?
- Réponse question 5 : A vous ...
  - Comparaison avec Exemple 1 (Authentification simple UserId + Mot de Passe)

Risque moins élevé      Risque plus élevé



# Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Réponse question 5 : Quels sont les risques de cette solution ?



# Exercices d'authentification

- Tous les risques identifiés dans l'exemple 1 restent présents dans l'exemple 2 sauf :
- Différence 1 : Risque d'interception du mot de passe assez faible
- Protection contre les keyloggers
- Transmission du mot de passe par https
- Risque de screen logger
  - Différence 2 : Risque élevé d'attaque par force brute contre le mot de passe
- Mot de passe sur 6 chiffres =  $10^6$  possibilités
- Équivalent à une clé sur 20 bits (ce n'est pas beaucoup)
- Exercice 2 : Analyse de fonctions d'authentification



# Exercices d'authentification

- Réponse question 5 (suite) : Quels sont les risques de cette solution ?
    - Risque élevé d'attaque par force brute contre le mot de passe
  - Collecter un grand nombre de numéros de compte ( $> 10^6$ )
  - Tester un ou deux mots de passe contre chaque compte
  - Permet de contourner le blocage des comptes au bout de 3 essais
    - Remarque : le compteur d'échec du mot de passe est remis à zéro lorsque l'utilisateur légitime se connecte
  - Ca devient une vulnérabilité qui permet de jouer le scénario d'attaques ci-dessus plusieurs fois
- 
- Exercice 3 : Politique d'authentification contextuelle





# Exercices d'authentification

- Objectifs
  - Comprendre le concept d'authentification contextuelle – Savoir utiliser ce concept
- Exercice 3 : Politique d'authentification contextuelle
- Retour sur l'exemple 2 de l'exercice 2
  - Supposons que le mot de passe d'un client de la banque soit cassé
- Question 1 : Est-ce que c'est « game over » pour ce client ?
  1. Oui
  2. Non



# Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle
- Retour sur l'exemple 2 de l'exercice 2 – Supposons que le mot de passe d'un client de la banque soit cassé
- Réponse question 1 : La réponse est non !
  - Plus précisément, c'est « game over » pour la confidentialité de ses comptes
  - Mais pas pour leur intégrité
- Question 2 : Pourquoi ?
- Réponse question 2 : A vous ...



# Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle
- Réponse question 2 : Parce que la banque a défini une politique d'authentification contextuelle
- Certaines opérations présentent un risque considéré comme faible
  - Consultation des comptes par le client
  - Les transferts vers les comptes du client
- Certaines opérations ont un risque élevé – Par exemple, transfert vers un compte qui n'appartient pas au client
- Exercice 3 : Politique d'authentification contextuelle



# Exercices d'authentification

- Réponse question 2 : Définition de la politique d'authentification contextuelle
  - Avec une authentification simple (Id du compte + Mot de passe), les opérations à risque faible sont permises
  - Pour réaliser une opération à risque élevée, une authentification forte est obligatoire (par Remote One Time Password via le téléphone cellulaire)
- Exercice 3 : Politique d'authentification contextuelle
- Conclusion Exercice 3



# Exercices d'authentification

- Conclusion 1 : Si le mot de passe d'un utilisateur est cassé
  - La confidentialité des comptes du client est perdue
  - L'intégrité des comptes du client peut être attaquée
  - Mais l'attaquant ne peut pas vider les comptes du client •
- Conclusion 2 : La politique d'authentification peut être beaucoup plus élaborée et dépendre par exemple :
  - De l'environnement (de l'heure, de la localisation du client, etc.) – D'une mise à jour du profil du client (changement d'adresse ou de numéro de téléphone cellulaire)
  - Etc.



*Frédéric Cuppens, José M. Fernandez, Nora Cuppens*

# INF4420a: Sécurité Informatique

## Exercices Crypto III

- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)
- Objectif :
  - Savoir évaluer le temps nécessaire pour casser une clé par force brute



# Exercice de crypto

- Savoir évaluer la taille de la clé en fonction des capacités de calcul de l'adversaire
- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)
- Les robots ont pris le contrôle de la planète
- Quelques humains résistent et communiquent avec un ordinateur Mainframe utilisant un chiffrement AES avec clés de 128 bits
- Les robots doivent prendre le contrôle de cet ordinateur avant que le prochain Néo n'arrive sur Terre dans 10000 ans pour organiser la révolte



# Exercice de crypto

- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)
- Il y a environ 500 milliard de machines sur toute la planète
- Chaque machine est capable de tester environ 1000 billions (billion =  $10^{12}$ ) de chiffrement AES par seconde (un chiffrement à chaque nanoseconde)
- Question 1 : Est-ce que les robots réussiront à prendre le contrôle du Mainframe avant le retour de Néo ?
  - Oui
  - Non



# Exercice de crypto

- Réponse question 1 :
  - Nombre total de clés AES à tester
- $2^{128}$  clés
  - 500 milliards de machines
- $500 * 10^9 \approx 500 * 2^{30} \approx 2^{39}$  machines – 1000 billion clés / s
- $10^{15}$  clés / s  $\approx 2^{50}$  clés par sec
  - Nombre total de clés essayées par seconde
- $2^{50} * 2^{39}$  clés / sec =  $2^{89}$  clés – Nombre de secondes par année
- $60*60*24*365 = 31\ 536\ 000 \approx 32 * 10^6$  sec  $\approx 2^{25}$  sec / année – Nombre total de clés essayées par année
- $2^{89} * 2^{25} = 2^{114}$  clés / année
  - Temps total pour essayer toutes les clés
- $2^{128} / 2^{114}$  clés =  $2^{14}$  année = 16384 années



# Exercice de crypto

- Réponse question 1 :
  - Non, les robots ne sont pas sûr de réussir à prendre le contrôle du Mainframe avant le retour de Néo !
  - Mais, ils ont quand même des chances d'y arriver



# Exercice de crypto

- Pour éviter l'attaque, les humains changent l'algorithme AES pour l'algorithme à clé publique RSA
- Pour transmettre leur message, les humains utilisent des capcha que les robots ne savent pas reconnaître
- Les robots entraînent des humains pour faire la reconnaissance à leur place
- Les humains entraînés sont connectés à la Matrice et peuvent tester jusqu'à 100 clés par seconde
- Les robots sont capables d'alimenter 100 milliards d'humains
- Question 2 : Quelle est la longueur minimum de clé RSA que les humains devraient choisir pour être protégés jusqu'à l'arrivée du prochain Néo ?



# Exercice de crypto

- Au minimum 45 bits – Au minimum 83 bits
- Au minimum 128 bits
- Au minimum 145 bits
- Réponse question 2 :
  - Nombre d'humains
- $100 * 10^9 \approx 100 * 2^{30} \approx 2^{37}$  humains
  - Nombre de clés / s par humain
- $100 \text{ clés / s} \approx 2^7 \text{ clés / s}$ 
  - Nombre total de clés testé / s
- $2^7 * 2^{37} = 2^{44}$  clés
  - Nombre de secondes avant l'arrivée du prochain Néo
- $10\,000 * 2^{25} < 2^{14} * 2^{25} = 2^{39}$ 
  - Nombre de clés essayées avant prochain Néo
- $2^{39} * 2^{44} = 2^{83}$



# Exercice de crypto

- Réponse question 2 :
  - Les robots pourront tester  $2^{83}$  clés en 10000 ans
  - Afin d'éviter une « bad luck » (les machines tombent sur la bonne clé rapidement), la clé devrait donc avoir idéalement au minimum 90 bits



# Exercice de crypto

- Les robots ont découvert qu'il existait une méthode beaucoup plus rapide de casser RSA que la force brute
- Pour cela, ils ont récupéré une implémentation de l'algorithme de factorisation de Pollard (la méthode de « rho ») qui a un temps d'exécution de  $O(2^{n/3})$  opérations, où  $n$  est la taille en bits de l'entier à factoriser
- En optimisant cet algorithme, les robots ont réussi à l'exécuter en exactement  $1/1000 \approx 2^{n/3}$  opérations pouvant être réparties sur l'ensemble des machines de la Terre
- Les robots ont aussi réussi à optimiser leurs machines pour que chacune calcule jusqu'à  $10^{18}$  opérations par seconde



# Exercice de crypto

- Question 3 : Évaluez l'impact que cette découverte pourrait avoir pour les humains. Quelle devra être la taille minimale de la clé dans ce cas ?
  1. 128 bits
  2. 190 bits
  3. 444 bits
  4. 500 bits
- Réponse question 3 :
  - Nombre de machines
- $2^{39}$  machines
  - Nombre d'opérations par seconde
- $10^{18} \approx 2^{60} / s$ 
  - Nombre d'opérations par année
- $2^{60} * 2^{25} = 2^{85} / \text{an}$



# Exercice de crypto

- Nombre d'opérations avant Néo
- $2^{85} * 2^{39} * 10000 < 2^{85} * 2^{39} * 2^{14} = 2^{138}$  opérations
  - Nombre d'opérations nécessaires en utilisant Pollard
- $2^{(n/3)} / 1000 \approx 2^{(n/3-10)}$  – Taille de clés minimum :
- $n/3 - 10 > 138$
- Donc  $n > 444$  bits
- Réponse question 3 :
  - Les humains devront utiliser une clé d'au moins 444 bits au lieu de 90 bits
  - Ils devront donc pratiquement quintupler la taille de la clé



# Exercice de crypto

- Question 4 : Sachant que le temps pour chiffrer/déchiffrer avec RSA est en  $O(n^3)$  où  $n$  est la taille de la clé, de combien de fois les opérations de chiffrement sont ralenties par ce rallongement de la clé ?
  - 24 fois – 48 fois – 96 fois
  - 120 fois
- Réponse question 4 :
  - On passe d'une clé de 90 bits à une clé de 444 bits
  - $444 / 90 \approx 4,93$
  - $4,93^3 \approx 120$
  - Les opérations de chiffrement/déchiffrement seront donc pratiquement 120 fois plus lentes
- Ca se complique pour les humains !



# Exercice de crypto

- Les robots ont réussi à construire un ordinateur quantique qui permet de casser RSA par factorisation en  $O(n^3)$  où  $n$  est la longueur de la clé
- L'algorithme n'est pas encore très optimisé : il peut être exécuté en  $10 \cdot n^3$  opérations et l'ordinateur quantique peut exécuter jusqu'à 1000 opérations par seconde • Pour le moment, les robots ne disposent que d'un seul ordinateur quantique
- Question 5 : De combien de temps les humains disposent-ils pour réagir ?
  1. 10 minutes
  2. 10 heures
  3. 10 jours
  4. 10 ans



# Exercice de crypto

- Réponse question 5 :
  - Nombre de machine : 1
  - Nombre d'opérations par seconde
- 1000
  - Nombre d'opérations par heure
- $1000 * 60 * 60 = 3\,600\,000$ 
  - Nombre d'opérations nécessaires en utilisant l'ordinateur quantique pour une clé de 444 bits  $\bullet 10 n^3 = 10 * (444^3) = 875\,283\,840$
  - Nombre d'heures pour réagir :
- $875\,283\,840 / 3\,600\,000 = 243,13$  heures  $\approx 10$  jours
- Question 6 : Que peuvent faire les humains pour éviter que les robots ne les exterminent ?



# Exercice de crypto

- Réponse question 6 :
  - Revenir à AES en allongeant la clé à 256 bits
- Résiste à l'ordinateur quantique mais chiffrement symétrique
  - Utiliser un chiffrement de Vernam (masque jetable)
  - Déployer un algorithme de chiffrement post-quantique
- Exemple : chiffrement de McEliece
- Mais longueur de la clé beaucoup plus longue
- Pas d'assurance qu'il n'y pas d'autres vulnérabilités – Utiliser un algorithme de cryptographie quantique
- Exercice 2 : El gamal
  - Pourquoi :  $D(y_1, y_2) = x$  ?
- Réponse



# Exercice de crypto

- $D(y_1, y_2) = y_2 / y_1^d \bmod p$
  - $y_1 = g^k \bmod p$
  - $y_2 = x e^k \bmod p$
  - $e = g^d \bmod p$
- 
- Donc :
    - $D(y_1, y_2) = x (g^d)^k \bmod p / (g^k)^d \bmod p = x \text{ (si } x \in \mathbb{Z}_p^*)$



# INF4420: Éléments de Sécurité Informatique

Corrigé des exercices : Autorisation, Contrôle d'accès



# Exercices Autorisation, Contrôle d'accès

- Exercice 1 : Expression de la politique d'autorisation d'une agence bancaire
- Objectif :
  - Savoir identifier les rôles et les ressources dans une politique d'autorisation
  - Savoir appliquer les modèles DAC, RBAC et ABAC
  - Comprendre les différences entre DAC, RBAC et ABAC
- Exercice 1 : Expression de la politique d'autorisation d'une agence bancaire



# Exercices Autorisation, Contrôle d'accès

- Vous venez d'être embauché comme administrateur de la sécurité dans un grand groupe bancaire
- Votre première mission consiste à redéfinir la politique d'autorisation des agences bancaires du groupe
- Pour réaliser cette mission, vous décidez de commencer par recenser les types d'usager (rôles) ainsi que les types de ressource présents dans les agences bancaires
- Question 1 : Quels sont les différents types d'usagers que vous avez identifiés ?



# Exercices Autorisation, Contrôle d'accès

- Réponse (possible) question 1 :
  - Responsable\_agence
  - Conseiller\_financier
  - Conseiller\_immobilier
  - Service\_clientele
  - Client



# Exercices Autorisation, Contrôle d'accès

- Question 2 : Quels sont les différents types de ressource que vous avez identifiés ?



# Exercices Autorisation, Contrôle d'accès

- Réponse (possible) question 2 :
  - Ressources logiques (données)
    - Profil\_client
    - Compte\_client
    - Carte\_client
    - Prêt (hypothèque)
    - Historique\_operation
    - Historique\_credit
  - Ressources physiques
    - Ordinateur
    - Imprimante
    - Coffre
    - Armoire
    - Porte
    - DAB
    - Etc.



# Exercices Autorisation, Contrôle d'accès

- Votre mission concerne la définition de la politique de contrôle d'accès aux données logiques



# Exercices Autorisation, Contrôle d'accès

- Vous décidez de faire une visite à une agence de la banque
  - Vous collectez les informations suivantes :
    - L'agence a 10 employés : 1 directeur, 3 conseillers, 1 conseiller immobilier et 5 service\_clientèle
    - L'agence a 50 clients ayant chacun un profil
    - En moyenne, chaque client a 3 comptes, un prêt hypothécaire et 1 carte
    - Un historique d'opération est associé à chaque compte
    - Un historique de crédit est associé à chaque carte



# Exercices Autorisation, Contrôle d'accès

- Question 3 : quelle serait, en moyenne, la taille de la matrice de contrôle d'accès si vous utilisez le modèle DAC ?
  1.  $5 * 6$
  2.  $60 * 60$
  3.  $12 * 500$
  4.  $60 * 500$



# Exercices Autorisation, Contrôle d'accès

- Réponse question 3 :  $60 * 500$ 
  - 60 lignes : 10 employés + 50 clients
  - 500 colonnes : 10 objets \* 50 clients
- Votre conclusion est que la matrice de contrôle d'accès est trop grande pour être gérable avec le modèle DAC



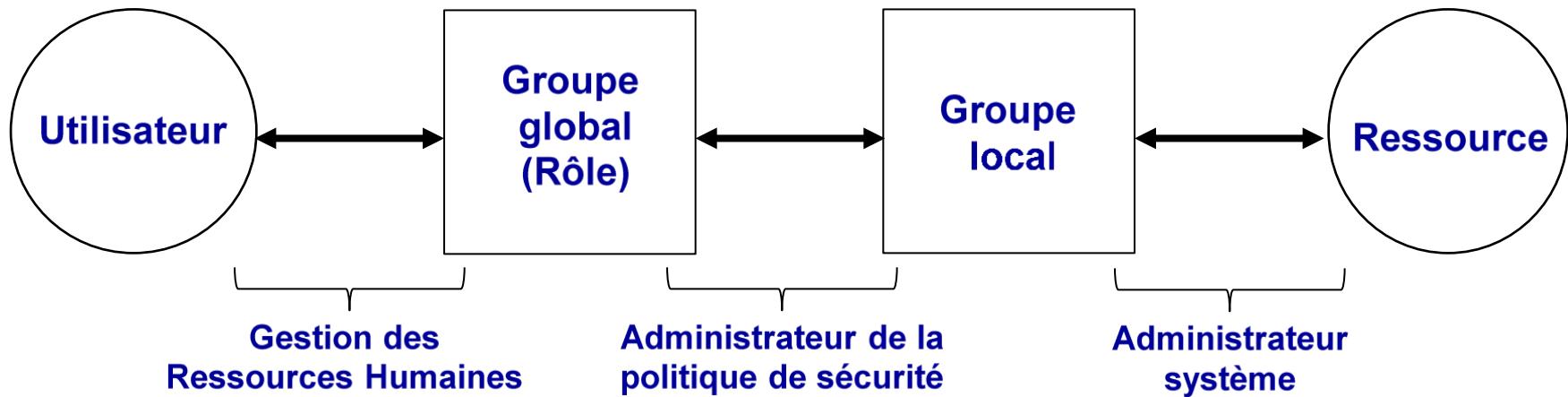
# Exercices Autorisation, Contrôle d'accès

- Vous décidez d'étudier si le modèle RBAC (Role Based Access Control) convient
- Comme la banque est sous Windows, vous optez pour l'implémentation AGLP (Access – Global – Local – Permissions) de RBAC



# Exercices Autorisation, Contrôle d'accès

- AGLP (Rappel)



- Après discussion avec la RH, vous décidez d'associer chaque type d'usager que vous avez identifié à un groupe global (rôle)
- Après discussion avec le sys admin, vous décidez d'associer chaque type de ressource que vous avez identifié à un groupe local



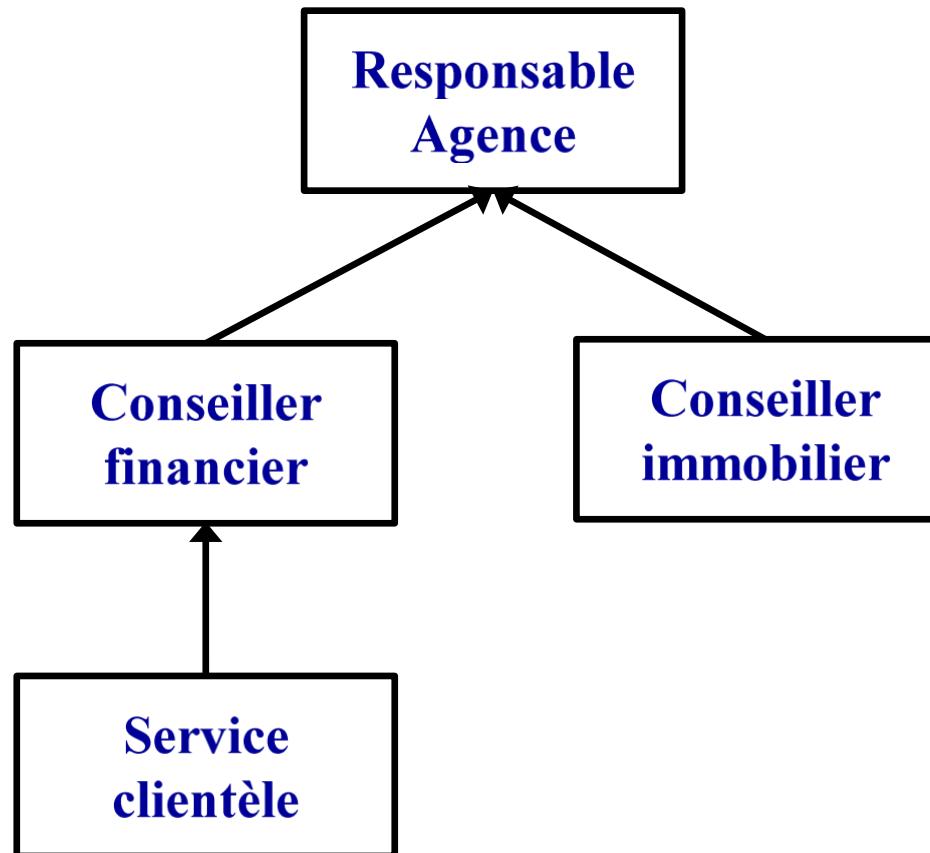
# Exercices Autorisation, Contrôle d'accès

- Vous apprenez que le conseiller\_financier peut jouer occasionnellement le rôle de service\_clientèle
- Vous apprenez également que le responsable\_agence peut jouer occasionnellement les rôles de conseiller\_financier et de conseiller\_immobilier
- Question 4 : Proposez une organisation hiérarchique des rôles correspondant à cette organisation
- Réponse question 4 :



# Exercices Autorisation, Contrôle d'accès

- Réponse question 4 :





# Exercices Autorisation, Contrôle d'accès

- Vous apprenez qu'aucun usager ne devrait pouvoir cumuler les permissions de conseiller immobilier et de conseiller financier (contrainte 1)
- Question 5 : Quelle anomalie cela crée-t-il dans votre modélisation ?



# Exercices Autorisation, Contrôle d'accès

- Réponse question 5 : Comme le responsable d'agence hérite des rôles de conseiller financier et de conseiller immobilier, il cumule les permissions de ces rôles. Ce qui viole la contrainte 1



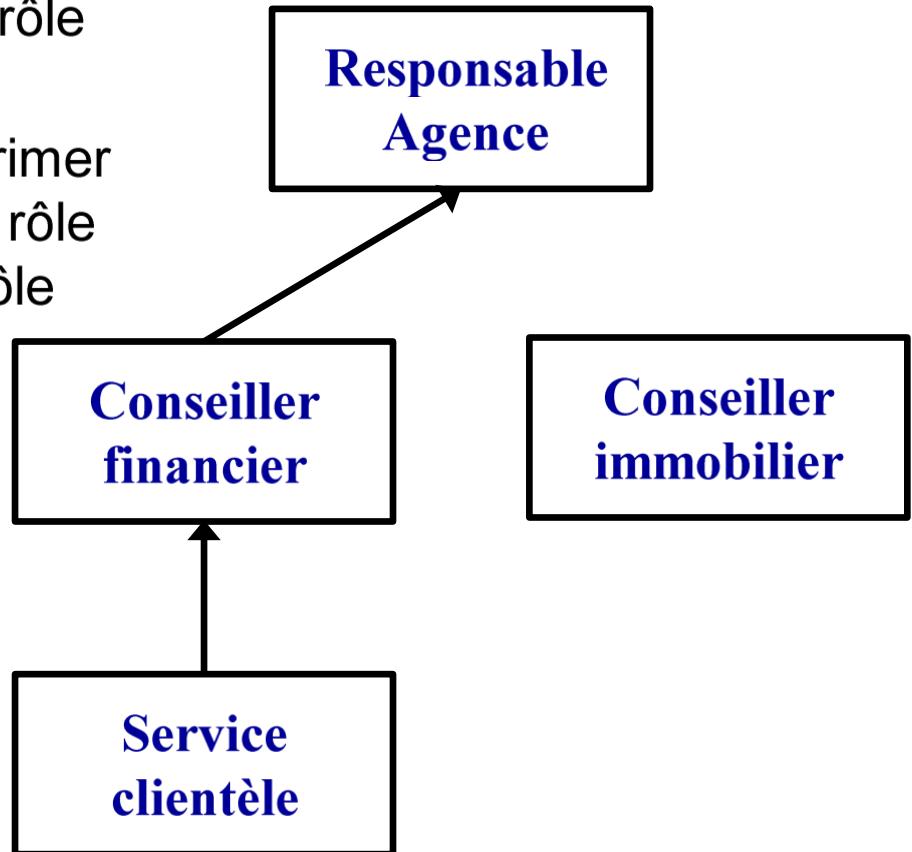
# Exercices Autorisation, Contrôle d'accès

- Question 6 : Comment proposez-vous de résoudre le problème ?



# Exercices Autorisation, Contrôle d'accès

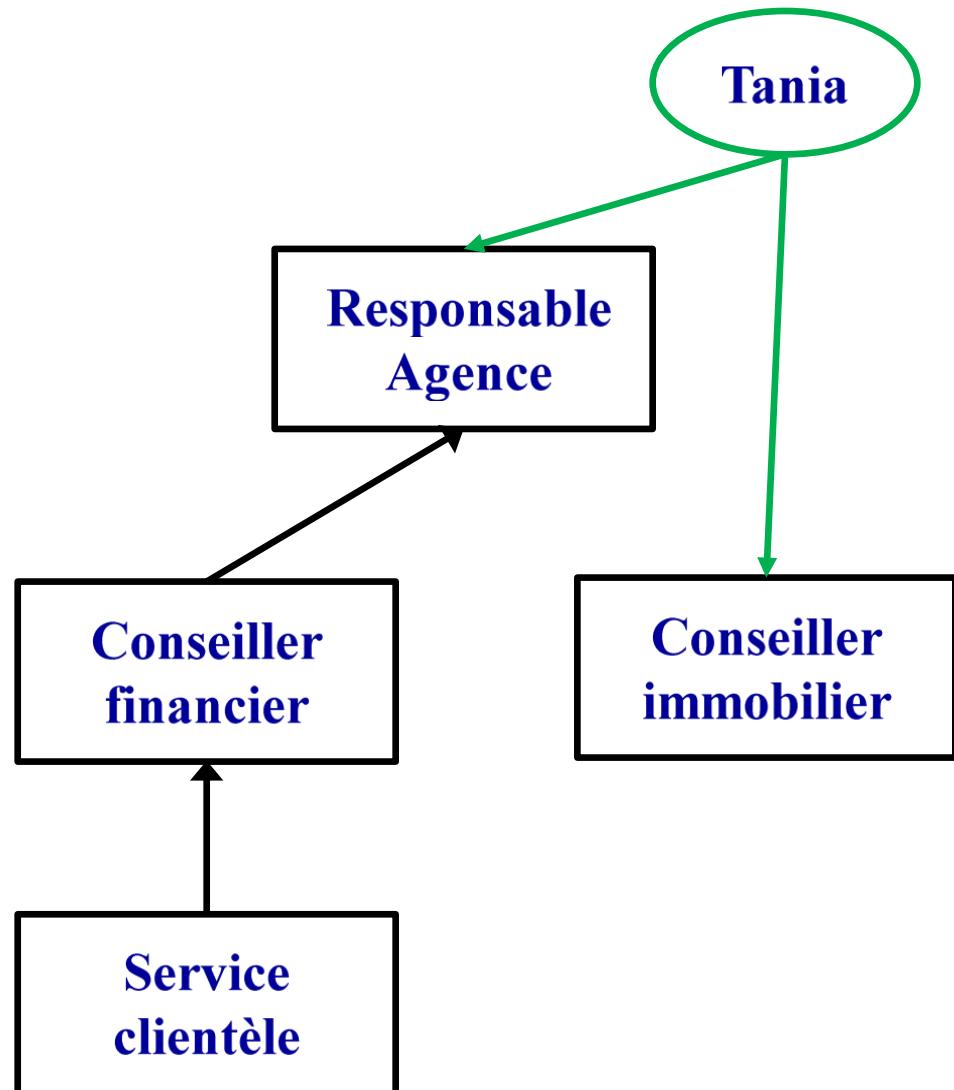
- Réponse question 6 :
  - Il faut modifier la hiérarchie de rôle pour éliminer le conflit
    - Par exemple, on peut supprimer le lien hiérarchique entre le rôle conseiller immobilier et le rôle responsable d'agence





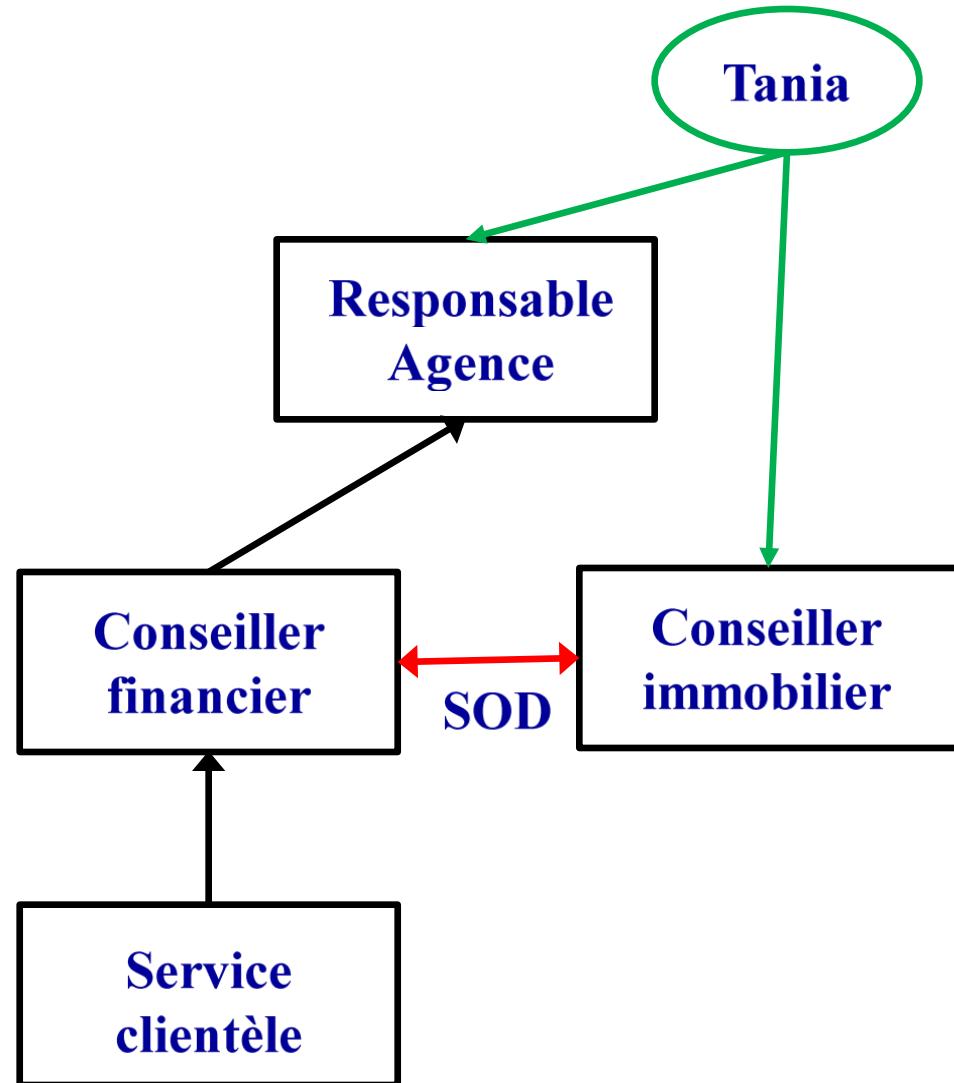
# Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Supposons que Tania soit la responsable d'agence et que Tania soit *explicitement* affectée aux deux rôles :
    - Responsable d'agence
    - Conseiller immobilier



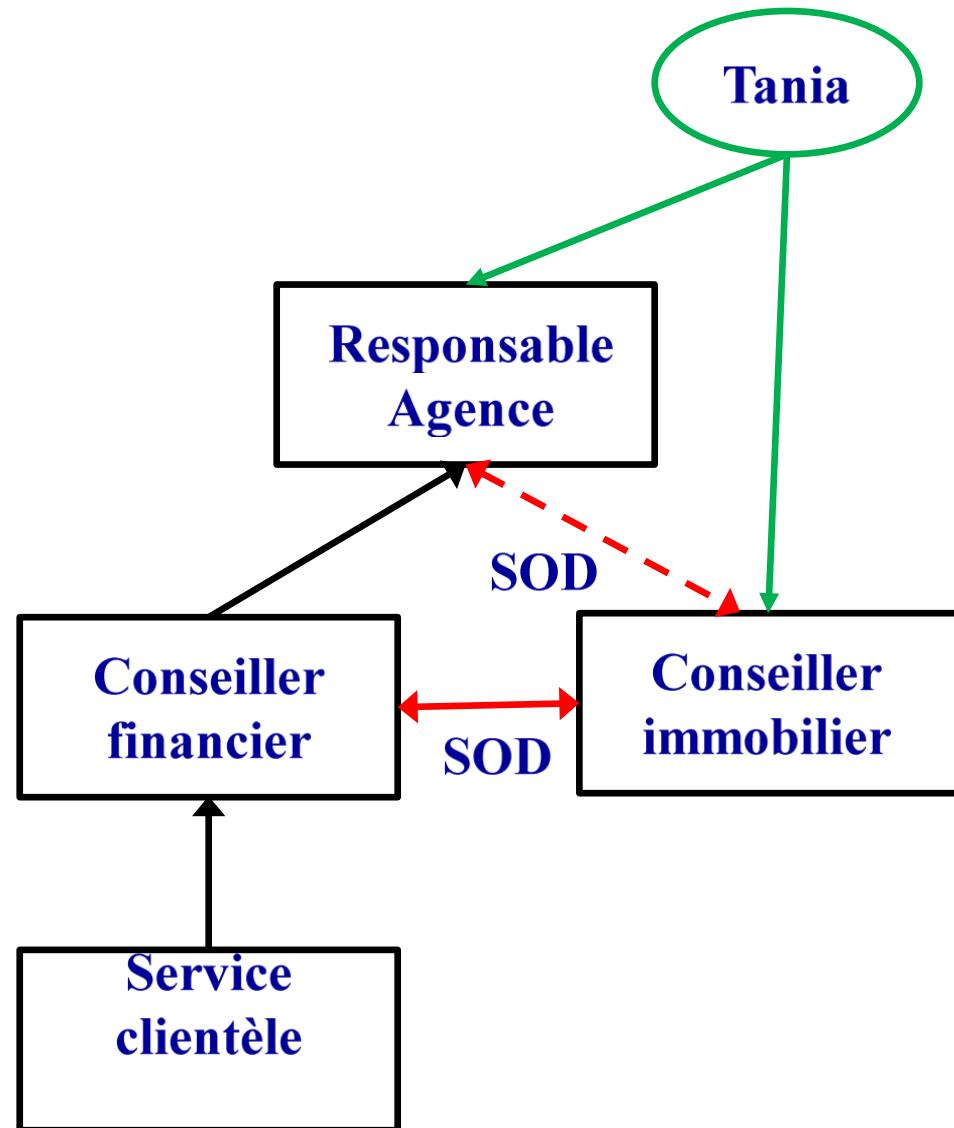


- Réponse question 6 :
  - Pour satisfaire la contrainte 1, il faut créer une règle de type « Séparation of Duty » entre les rôles :
    - Conseiller financier
    - Conseiller immobilier





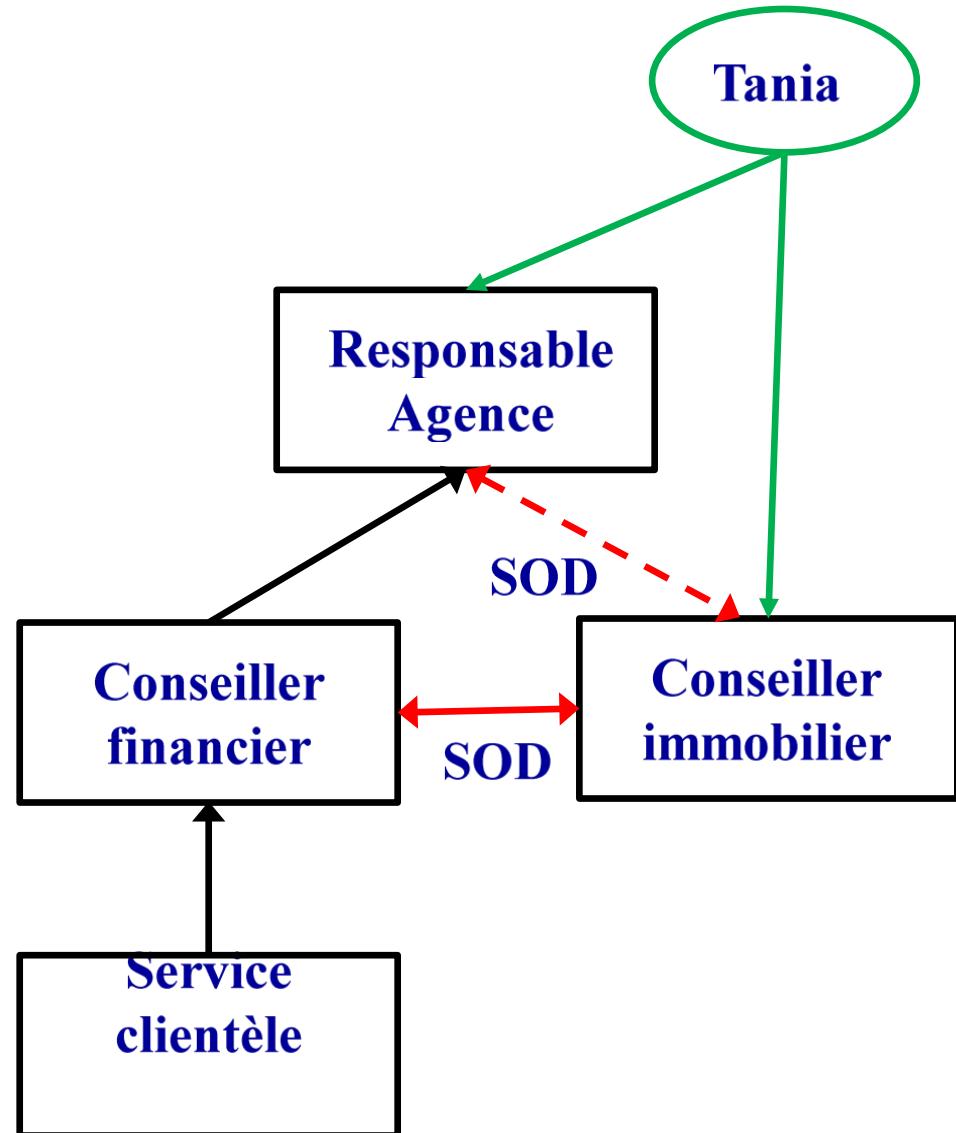
- Réponse question 6 :
  - Le responsable d'agence hérite implicitement de cette SOD





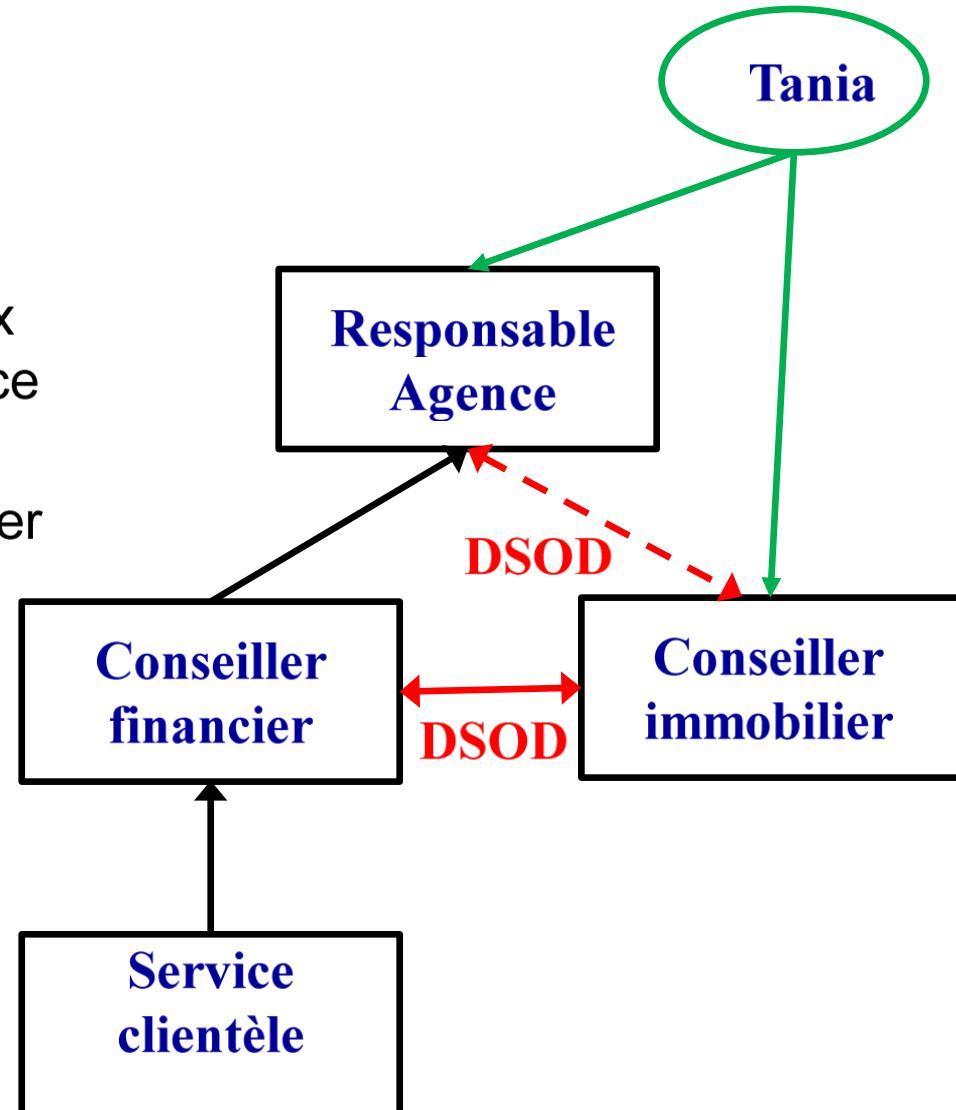
# Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Si la SOD est statique (SSOD), alors Tania ne peut pas être affectée aux rôles Responsable Agence et Conseiller immobilier
  - Problème !





- Réponse question 6 :
  - Solution : La SOD doit être dynamique (DSOD)
  - Tania est affectée aux deux rôles Responsable d'agence et Conseiller Immobilier
  - Mais elle ne peut pas activer ces deux rôles en même temps





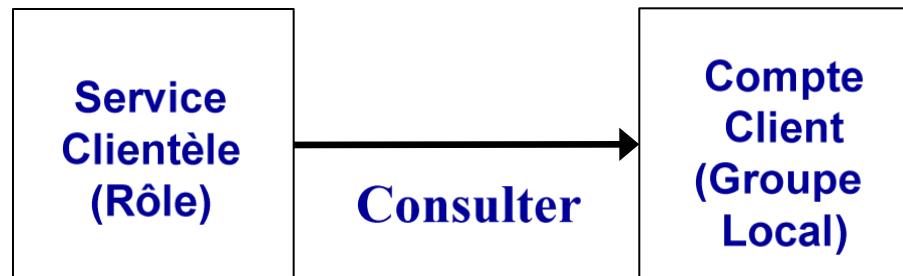
# Exercices Autorisation, Contrôle d'accès

- Vous devez maintenant utiliser le modèle RBAC / AGLP pour exprimer les règles d'autorisation de la politique d'autorisation s'appliquant à l'agence
- Exemple de règle :
  - Le rôle service\_client a la permission de consulter (lire) le compte des clients



# Exercices Autorisation, Contrôle d'accès

- Il n'y a pas de difficulté pour exprimer ce type de règle avec AGLP



- Vous rencontrez des difficultés pour exprimer les règles d'autorisation s'appliquant au rôle client
- Exemples
  - Un client peut consulter ses comptes
  - Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration



# Exercices Autorisation, Contrôle d'accès

- Question 7 : Est-il possible d'exprimer ce type de règle en utilisant AGLP ?
- Question 8 : Si oui, quelle est votre solution ?
- Réponse question 7 : La réponse est oui, mais c'est compliqué !

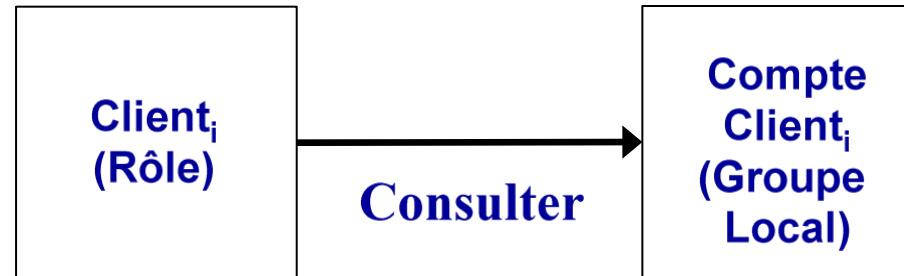


# Exercices Autorisation, Contrôle d'accès

- Réponse question 8 :
  - Il faut créer autant de rôles qu'il y a de clients :
    - Ensemble de rôles : Client<sub>i</sub> où i est un client
  - Il faut aussi créer des groupes locaux pour chaque client :
    - Ensemble de groupes locaux : Compte\_client<sub>i</sub> où i est un client
- Expression de la règle :
  - Un client peut consulter ses comptes



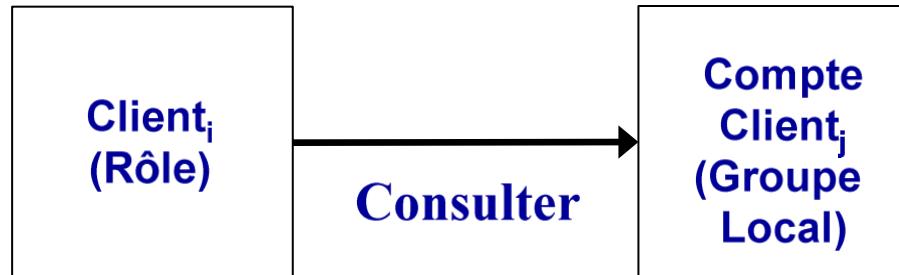
# Exercices Autorisation, Contrôle d'accès



- Réponse question 8 :
- Et si le client j a donné procuration au client i pour qu'il puisse consulter ses comptes



# Exercices Autorisation, Contrôle d'accès



- On perd complètement l'intérêt de RBAC !
  - Autant utiliser DAC !



# Exercices Autorisation, Contrôle d'accès

- Un collègue vous recommande de continuer à utiliser RBAC :
  - En conservant le rôle Client et le groupe local Compte\_client
  - En codant dans l'application « Consulter » le test que le compte consulté est bien un compte du client ou bien un compte pour lequel le client a procuration
- Question 9 : Que répondez-vous à ce collègue ?
- Réponse question 9 :



# Exercices Autorisation, Contrôle d'accès

- Réponse question 9 :
  - Il faut séparer l'expression de la politique d'autorisation de l'implantation de l'application « Consulter » (comme des autres applications d'ailleurs)
  - Sinon, c'est compliqué de savoir si la politique d'autorisation est correctement appliquée
  - Sinon, c'est compliqué de faire les mises à jour (politique & applications)
  - Et ce n'est pas le rôle du développeur d'application d'implanter la politique de sécurité
    - Separation of Duty appliquée au développeur d'application !



# Exercices Autorisation, Contrôle d'accès

- Vous décidez d'utiliser le modèle ABAC (Attribute Based Access Control) pour exprimer la politique de sécurité associée au rôle Client



# Exercices Autorisation, Contrôle d'accès

- Vous considérez les attributs suivants pour les sujets :
  - Attributs du sujet : Nom, Rôle
- Vous considérez les attributs suivants pour les ressources :
  - Attributs de la ressource : Type, Ident, Nom\_client, Liste\_procuration
- Question 10 : En utilisant le modèle ABAC, exprimer les règles suivantes :
  - Un client peut consulter ses comptes
  - Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration



# Exercices Autorisation, Contrôle d'accès

- Réponse question 10 :



# Exercices Autorisation, Contrôle d'accès

- Réponse question 10 :
  - Un client peut consulter ses comptes
  - Permettre si Role(Sujet)=Client et Type(Ressource)=Compte\_client et Non(sujet)=Nom\_client(Ressource) et Ident(Action)=Consulter



# Exercices Autorisation, Contrôle d'accès

- Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration
- Permettre si Role(Sujet)=Client et Type(Ressource)=Compte\_client et Nom(sujet) ∈ Liste\_procuration (Ressource) et Ident(Action)=Consulter