POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

INF4420a: Sécurité Informatique
Exercices séance1
Introduction : Concepts de base et motivation

Frédéric et Nora Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 1 : vocabulaire des attaques

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

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

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 1 : vocabulaire des attaques

- Exemple 1 : Inondation (flooding)

- Réponse question 1

  a) La disponibilité

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

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

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

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

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 1 : vocabulaire des attaques

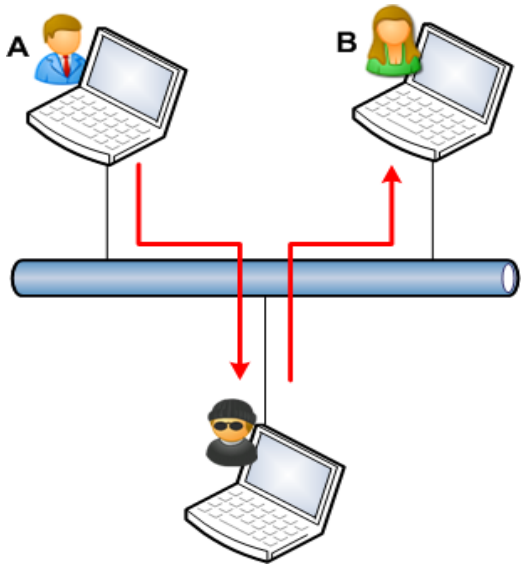
- Exemple 3 : Détournement de session (hijacking)

- Réponse question 3 :
  a) La disponibilité
  b) L'intégrité
  c) La confidentialité

Exercice 1 : vocabulaire des attaques

- 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

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



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 1 : vocabulaire des attaques

- Exemple 4 : Homme du milieu (Man in the Middle)

- Réponse question 4 :
  b) L'intégrité
  c) La confidentialité

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 1 : vocabulaire des attaques

- 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
  b) Faux

Exercice 1 : vocabulaire des attaques

- 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

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

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 ?

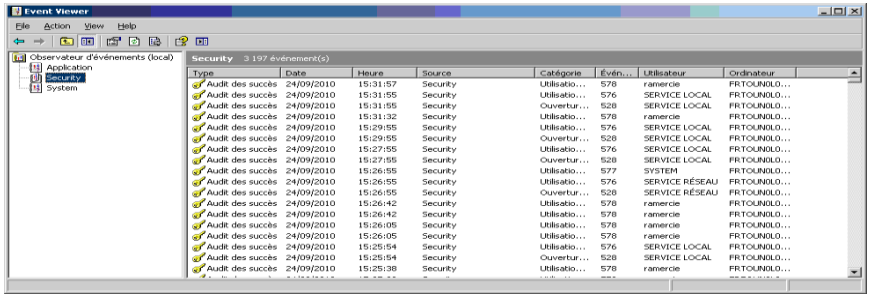
Exercice 2 : les propriétés de sécurité

- Données et métadonnées
- Exemple : envoi d'un message

Données =
contenu du message

Hello,
Aujourd'hui début du cours
INF4420A

Journal d'audit =
auditabilité du message



Métadonnées =
associées au message

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 le contenu du message
  - Sa confidentialité
  - Son intégrité
  - Sa disponibilité

- 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

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 2 : les propriétés de sécurité

- 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
  e) Écoute passive (sniffing)
  f) Détournement de session (hijacking)

Exercice 2 : les propriétés de sécurité

- Exemple 1 : Authenticité

- Réponse question 1 :
  b) Mascarade (spoofing)
  f) Détournement de session (hijacking)

  Quelle est la différence entre les deux types d'attaque ?

Exercice 2 : les propriétés de sécurité

- Exemple 2 : Non répudiation
  - 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)

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 2 : les propriétés de sécurité

- Exemple 2 : Non répudiation

- 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

Exercice 2 : les propriétés de sécurité

- Exemple 2 : Non répudiation

- 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

Exercice 2 : les propriétés de sécurité

- 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 fraicheur ?
  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)

Exercice 2 : les propriétés de sécurité

- Exemple 3 : Fraîcheur (Freshness)

- Réponse question 4 :
  3. Rejeu (Replay attack)

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice 2 : les propriétés de sécurité

- Exemple 3 : Fraîcheur (Freshness)

- Question 5 : Quelles actions permettent d'assurer la propriété de fraicheur ?
  1. Chiffrer les messages
  2. Signer les messages
  3. Assurer l'intégrité des métadonnées associées au message
  4. Aucune des réponses proposées

Exercice 2 : les propriétés de sécurité

- Exemple 3 : Fraîcheur (Freshness)

- Réponse question 5 :
  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

Exercice 2 : les propriétés de sécurité

- 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)
  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)

Exercice 2 : les propriétés de sécurité

- Exemple 4 : Horodatage

- Réponse question 6 :
  5. Attaquer l'intégrité de l'horloge du système
  6. Détournement de session (hijacking)

Exercice 2 : les propriétés de sécurité

- Exemple 4 : Horodatage

- 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

Exercice 2 : les propriétés de sécurité

- 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