1. Introduction à la Sécurité Informatique

Noureddine AZZOUZA Riadh MEGHATRIA

[1]Université Djilali BOUNAAMA Khemis Miliana, Algérie

Cours de Sécurité Informatique, M2GLSD

Plan

Objectifs

1. Se sensibiliser aux risques liés aux attaques sur les systèmes d'information.
2. Se familiariser avec les concepts de la sécurité informatique.
3. Connaître les différents services de sécurité.
4. Savoir utiliser des mécanismes cryptographiques pour garantir différents services de sécurité.
5. Analyser un protocole cryptographique

Définitions

1. l'ensemble des techniques qui assurent que les ressources du système d'information d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.
2. recouvre l'ensemble des techniques informatiques permettant de réduire au maximum les chances de fuites d'information, de modification de données ou de détérioration des services.

La sécurité informatique :

Ensemble des moyens techniques, organisationnels, juridiques et humains mis en ?uvre pour minimiser la vulnérabilité des systèmes informatiques contre les : MENACES

Ressources à protéger

1. Les données
   - la forme prise par l'information
   - les moyens par lesquels elle est transmise ou stockée
   - toujours protégée de manière appropriée

   Protéger :
   - communications, fichiers de données et bases de données
2. Les systèmes
   - contre les virus, attaques ...

   Protéger :
   - Les logiciels, les Systèmes d'exploitation, les outils de développement, les utilitaires . . .
3. Les infrastructures réseaux
   - contre le vol, destruction ...

   Protéger :
   - Les serveurs informatiques, PC, portables, Matériels réseaux, Alimentation Électrique, Climatisation . . .

Besoins de protection

Insécurité et cibles attrayantes

- de conception et de mise en oeuvre,
- de gestion et contrôle de l'informatique et des incompétences
- de pannes et des catastrophes naturelles
- des erreurs,

Infractions

- Vol d'informations et du savoir faire
- sabotage d'informations
- violation du secret professionnel
- diffusion de fausses informations

Définitions

Vulnérabilité

Une faille du système : Faiblesse dans les procédures de sécurité qui pourrait être exploitée pour obtenir un accès non autorisé au système.

1. Vulnérabilité au niveau conceptuel
2. Vulnérabilité au niveau de l'implémentation.
3. Vulnérabilité dans la configuration, ou l'exploitation.

Définitions

Menace

une violation potentielle de la sécurité.

1. engendrent des risques et coûts humains et financiers
2. perte de confidentialité de données.
3. indisponibilité des infrastructures.
4. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilité

Catégories des menaces

- Menaces accidentelles
- Menaces intentionnelle

Menaces accidentelles

Menaces accidentelles

ne supposent aucune préméditation. Généralement, signifie une pannes ou erreurs

1. Panne / dysfonctionnement du matériel
2. Panne / dysfonctionnement du logiciel
3. Erreur de conception
4. Erreur de mis en place
5. Erreur d'exploitation
6. Erreur de manipulation

Menaces intentionnelles

Menaces intentionnelles

le fait d'un acte délibéré, Action exécutée pour violer la sécurité.(Actions malveillantes)

1. L'espionnage
2. Le vol
3. La perturbation
4. Le sabotage
5. La fraude physique
6. Accès illégitimes

On parle dans ce cas d'Attaques

Attaques

Attaque

une concrétisation d'une menace

- Une menace peut être concrétisée de différentes attaques
- les attaques peuvent être classés en 2 types

Catégories des Attaques

- Attaques passives
- Attaques actives

Attaques Passives

- menace contre la confidentialité de l'information
- Difficile à détecter

Interception

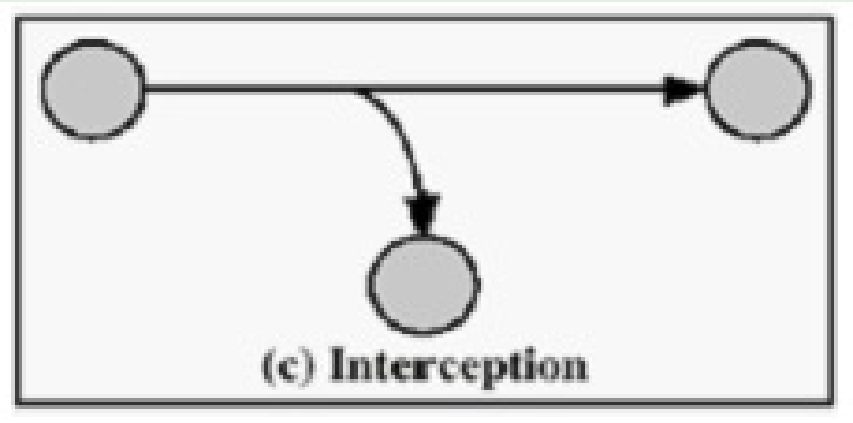
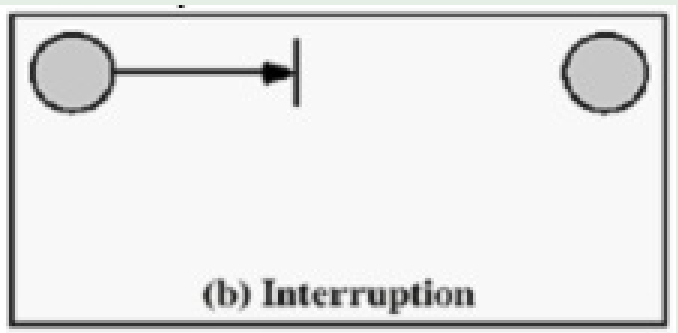


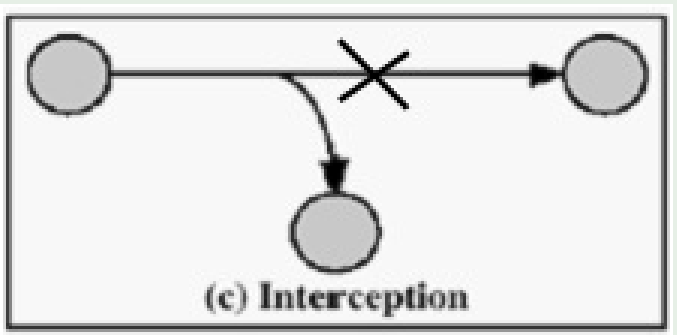
FIGURE – Interception

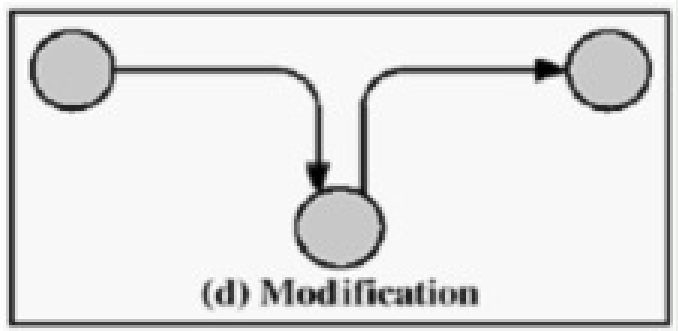
Attaques Actives

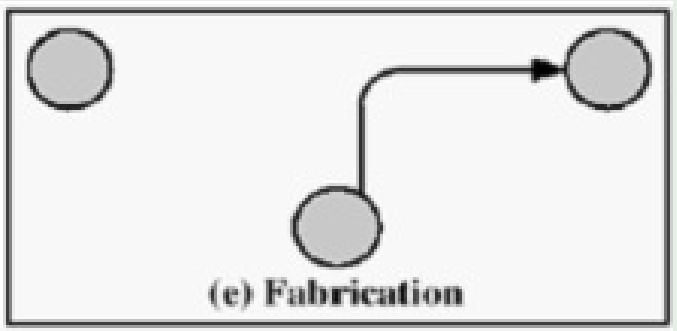
- menace contre l'intégrité de l'information
- Destruction, modification, fabrication (authenticité) ou interruption (disponibilité) des données

Attaques Actives









Attaques Actives : Exemples

1. Les Intrusions
   - Le Spoofing, Les sniffers, Les scanners et Les exploits
   - Denis de service (DOS et DDOS)
2. Le phising
   - Technique frauduleuse utilisée pour récupérer des informations
3. Le Hoax
   - Courrier électronique propageant une fausse information
4. Les Virus
   - Programme informatique situé dans le corps d'un autre
   - Les vers, Les trojans, Les bombes logiques, Les spywares

Sécurité des Systèmes d'information

l'ensemble des mesures techniques, organisationnelles ou juridiques à prendre et à mettre en place

- empêcher la détérioration.
- détecter toute atteinte, malveillante ou non.
- intervenir afin d ?en limiter les conséquences

Sécuriser un système

1. Définir les services
2. Connaitre les différentes menaces
3. Évaluer le coût

Objectifs de la Sécurité

La sécurité doit garantir les services suivants :

1. Confidentialité
2. Authentification
3. Intégrité
4. Non-Répudiation
5. Contrôle d'accès
6. Disponibilité

Mécanismes et Solutions

Mécanismes de Sécurités

1. Prévention
2. Détection
3. Recouvrement

Solutions

1. Cryptographie
2. Pare-feu (Firewall)
3. Contrôle d'accès
4. Log (Journalisation)
5. Audit
6. VPN (Réseaux Privées Virtuels)
7. SSL (Sécurité des Services)