Notes de cours de Sécurité internet et réseaux

Yann Miguel

24 septembre 2021

Table des matières

1 Vocabulaire

- confidentialité: L'accès des données échangées n'est disponible que à l'expéditeur et au destinataire
- intégrité: rendre possible la détection de toute modification des données
- authentification: les interlocuteurs sont connus et vérifiés. Cela peux être fait via méta données
- confidentialité futur parfaite: la découverte d'un secret ne compromet pas toutes les conversations futur et passées
- anonymat: les identités des participants du dialogue sont inconnues depuis l'extérieur du dit dialogue
- non-répudation: l'e=échange est un comme un contrat entre les interlocuteurs, et peux servir dans un cadre juridique
- protocoles cryptographiques: technologies mises en œuvre afin d'assurer la sécurité des données
- chiffrement:
  - symétrique: la même clé est utilisée pour chiffrer et déchiffrer les données
  - asymétrique: la clé de chiffrement et celle de déchiffrement sont différentes

2 Introduction

La sécurité n'est pas seulement un problème technique. En effet, si une clé privée devient publique, alors peu importe l'algorithme de chiffrage, il ne sera plus aussi résistant car on pourra utiliser la clé pour déchiffrer les messages chiffrés, ou pour usurper l'identité de l'auteur.

La sécurisation des terminaux est toute aussi importante que la sécurisation des terminaux, afin d'éviter:

- les sniffeurd de claviers et chevaux de troie
- la collecte de données sans accord
- les techniques TEMPEST, qui peuvent entraîner la collecte d'infos et de daat sans programmes externes
- le vol et/ou la perte de différents moyens de stockage:
  - disque dur
  - clé USB
  - téléphone
  - ets...
- les techniques d'ingégnerie sociale
- etc...

Il existe deux types de menaces:

- les menaces involontaires, qui sont liées à des accidents ou des erreurs, et qui sont liées à la fiabilité et la qualité
- les menaces volontaires, qui sont liés à des attaques, et qui sont liées à la sécurité

Lors du design de système d'informations, on peux considérer un accident trs improbable comme inexistant.

Il y a deux types d'attaques de réseaux:

- l'attaque passive, ou d'écoute, qui consiste en un accès de contenu dont on est pas destinataire ou propriétaire, dont les sources peuvent être:
  - TCP/IP non sécurisé, ce qui mène à une vue intégrale des pacquets, ce qui permet une attaque du protocole afin de devenir intermédiaire
  - un document publié par erreur, qui peux être trouvé sur internet
  - une violation des systèmes de contrôle d'accès, qui peux être dû à des mot de apsse faibles ou des injections SQL
  - des écoutes légales
- l'attaque active, qui consiste en une interception de contenu dont on est ni le propriétaire, ni le destinataire, et peux

permettre la modification des données en plus de l'accès, et dont la source peut être:
- TCP/IP non sécurisé, comme dans le point précédent
- une attaque sur des protocoles permettant le vol de la session

On peux se protéger des attaques sur le réseaux en appliquant de bonnes pratiques:
- En intégrant la sécurité dans la conception:
  - en vérifiants les besoins de chaque utilisateurs
  - en ne donnant pas aux utilisateurs plus de droits que requis pour leur travail
- En ayant une bonne admininstration:
  - les mises à jour permettent la correction d'erreurs et de bugs dans le code
  - le contrôle des accès permet une meilleure gestion des droits serveurs et machines
  - la surveillance permet la vérification du système et des utilisateurs
  - les audits permettent de tester le niveau de sécurité

Il y a différentes méthodes de cryptage de données, qui ont leur propres vulnérabilités:
- méthode par substitution, qui est vulnérable à une attaque par fréquence, qui consiste à analyser la fréquences des lettres pour déchiffrer le message
- les méthodes complexes, et paramétrées par clés, qui sont solides