Notes de cours de Sécurité internet et réseaux

Yann Miguel

19 novembre 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

3 Cours 1

<table>
<tr><td colspan="2"></td><td>cryptographie symétrique</td><td>cryptographie asymétrique</td></tr>
<tr><td colspan="2">confidentialité</td><td>chiffrement</td><td>chiffrement à clef publique</td></tr>
<tr><td colspan="2">intégrité</td><td rowspan="3">code
d'authentification
de message MAC</td><td rowspan="3">signature
numérique</td></tr>
<tr><td rowspan="2">authentification</td><td>données</td></tr>
<tr><td>entités</td></tr>
<tr><td colspan="2">non répudation</td><td>aucune primitive</td></tr>
</table>

Il n'y a aucune primitive de non répudation pour la cryptographie asymétrique car il n'est pas possible de différencier les interlocuteurs. Il existe trois types d'architectures:

1. fermée: Il y a peu d'acteurs, ou la structure est autonome
2. hiérarchisée: Il y a de nombreux acteurs et peu d'autorités de confiance
3. décentraliée: Il y a de nombreux acteurs et la certification des connaissances se base se fait de proche en proche

Chaque type d'architecture a ça propre façon d'être sécurisée:

1. fermée: Kerberos, IPSec
2. hiérarchisée: PKI à base d'authentification X509: IPSec, SSL
3. décentralisée: PGP/GnuPG, réseau P2P/F2F crypté, ...

La clef doit être signée par une figure d'autorité, qui peux être soi-même. Un clef signée par soi-même est dite auto-signée. PKI= Public Key Infrastructure Il est possible de révoquer un certificat si les informations ont chagées, ou bien si la clef privée est compromise, ou encore si il y a des changements dans l'institution.

Certaines fonctions de hachage sont déconseillées, dû aux failles et aux collisions, comme MD5.

4 Cours 2

Le plus grand problème des protocoles cryptographiques n'est pas le chiffrement, mais le partage sécurisé des clés.

On peux faire un système similaire au VPN sans protocoles cryptographiques, en utilisant un système filiaire.

L'envoi de mails via le protocole SMTP peux utiliser le protocole STARTSSL.

Il y a deux moyens de sécuriser des pacquets web:

- AH: on peux lire l'information, mais on ne peux pas la modifier de l'extérieur.
- ESP: one ne peux ni lire ni modifier l'information de l'extérieur.

Les en-têtes des deux protocoles sont similaires.

Les RFC sont des protocoles internet standardisés.

Afin de contrer les attaques sur l'intégrité de la session, on peux hacher et signer les précédents messages et les renvoyer vers le serveur, afin qu'il puisse vérifier que le contenu n'ai pas été altéré.

La compression est supposée diminuer les répétitions, afin d'éviter les attaques l'utilisant. En plus, cela diminue la taille du pacquet. Mais, la taille du message compressé peux donner certaines informations sur les octets et bits du message initial.

DHE: Deffie-Helmann Ephemeral Ephemeral: les clés sont jetées dès qu'elles ne sont plus utiles.

UDP a une version de TLS qui est adaptée afin de gérer le problème de pacquet qui se perd, et qui s'appelle DTLS.

5 Cours 3

On peux tromper les pare-feu via des tunnels, en envoyant des données par un canal différent.

On préfère les règles sans-états, car moins coûteuses, mais certains protocoles obligent celles avec états. Le pare-feu aide donc à déterminer ce qui est accessible depuis l'extérieur.

Une règle a deux aprties:

1. garde: condition déterminant l'action à réaliser
2. action: l'action à réaliser

Sur iptables, si la règle est un LOG, le logiciel continue de chercher des règkes après.