ATTAQUES DE MOT DE PASSE

Par SAHA Pierre

Généralités

- La plupart des systèmes sont sécurisés par Mots de passe
  - ⇒ Il faut donc convenablement le choisir
- Certains systèmes limites le nombre de tentatives d'accès par mot de passe
  - ⇒ Malheureusement cette technique peut être utilisée pour provoquer une dénis de service
- D'autres systèmes stockent les mots de passe de manière haché dans une BD ou un fichier
  - ⇒ Il faut utiliser la bonne fonction de hachage (exemple SHA1, 2, 3…)
  - ⇒ Si un attaquant a accès à la Base de Données ou au fichier, il peut y réaliser plusieurs attaques
- Plusieurs attaques possibles:
  - Attaque du dictionnaire
  - Attaque par force brute
  - Keyloggers
  - L'ingénierie sociale
  - L'espionnage

Quelques attaques

- Attaque du dictionnaire
  - Exploite le fait que les utilisateurs choisissent très souvent comme mot de passe des mots qui sont significatifs pour eux (les mots du dictionnaire)
  - L'attaquant tente de se connecter au compte utilisateur en essayant tous les mots du dictionnaire
- Attaque par force brute /attaque exhaustive
  - L'attaquant tente de se connecter au compte utilisateur en testant toutes les combinaisons possibles de caractères, de chiffres et de symboles possibles
- Surveillance électronique
  - Écoute du trafic réseau pour capturer des informations, en particulier lorsqu'un utilisateur envoie son mot de passe à un serveur d'authentification.
- Accéder au fichier de mot de passe
  - Le fichier de mots de passe contient de nombreux mots de passe d'utilisateurs et, s'il est compromis, peut être à l'origine de nombreux dommages. Il doit être protégé par des mécanismes de contrôle d'accès et un cryptage.

Attaques de mots de passe

- Ingénierie sociale
  - L’ attaquante convainc faussement l’utilisateur de lui donner son mot de passe.
- Rainbow table attack
  - L’attaquant utilise une table qui contient tous les mots de passe possibles déjà dans un format de hachage.

Contremesures aux attaques de mots de passe

- Utilisation des vérificateurs de mot de passe (password checker) ou des craqueur de mot de passe (Password cracker)
  - Ces outils permettent aux professionnels de la sécurité de tester la robustesse du mot de passe
- Hachage ou cryptage des mots de passe
  - Permet de lutter contre le sniffing
  - Les mots de passe sont hachés ou cryptés avant leur enregistrement dans la base de données ou dans le fichier de mots de passe
  - Utiliser des algorithmes de hachage non sujet aux collisions
  - Renforcer cette technique en utilisant les mécanismes de sel (salt en anglais). Les sels sont des valeurs aléatoires ajoutées au processus de cryptage pour ajouter plus de complexité et de caractère aléatoire. Ainsi, l'on peut utiliser le même mot de passe plusieurs fois en stockant dans le système de sauvegarde des mots de passe des valeurs complètements différentes.
- Vieillissement de mot de passe (password aging)
  - Forcer l'utilisateur à renouveler régulièrement son mot de passe après un certain délais
  - On peut aussi conserver une liste des mots de passe antérieurement utilisé afin d'empêcher leur réutilisation par le même utilisateur

Contremesures aux attaques de mots de passe

- Limitation du nombre de tentatives d'accès
  - Fixer un seuil de tentative infructueuses d'authentification
  - Après avoir atteint ce seuil, soit l'utilisateur attend un certain délais, soit c'est l'administrateur qui soit réactualiser son compte
  - Ceci permet de lutter contre les attaques de dictionnaire.
- Usage des mots de passe cognitif (cognitive password)
  - L'utilisateur est authentifié à travers des réponses aux questions qui lui sont posées
  - Très indiqué pour les systèmes dont les accès se font après de longues périodes
  - Permet de lutter contre l'oubli de mot de passe
- Utilisation des mots de passe à usage unique (One Time Password :OTP)
  - Le mot de passe n'est utilisé qu'une seule fois
  - Très indiqué dans les environnement requérant un haut niveau de sécurité
  - Pour cela, l'on fait recours aux Token (Token device). C'est cet équipement qui se charge de générer le mot de passe.
  - Le token peut être **synchrone** (par temp ou compteur) ou **asynchrone** (par challenge)

Contremesures aux attaques de mots de passe

- Utilisation des clés cryptographique
  - Du fait de la faiblesse de l'authentification par mot de passe, l'on peut exploite de plus en plus la cryptographie asymétrique (notamment la signature numérique et les certificats)
- Utilisation des passphrases
  - Séquence de caractères bien plus longue que les mots de passe habituels
  - L'utilisateur saisie une phrase et le système se charge de le transformer en mot de passe
  - Un peu plus sûr que le mot de passe car plus long et facile à mémoriser
- Faire un choix approprié du mot de passe
  - Éviter les nom, date de naissances, lieu de travail, mots du disctionnaire, mot suivi de chiffre, identifiant etc…
  - Obéir à une politique qui définit le nombre minimum de caractère

    Savoir que quatre lettre sera toujours préférable à 4 chiffres ($10^4<26^4$)
  - Introduire les caractères particuliers
  - Changer la casse (majuscule et minuscules)