Atelier sécurité - première partie

Mots de passe, chiffrement et signature

Victor Stinner

Club des utilisateurs de logiciels libres de l'UTBM

Lolut Automne 2005

Sommaire

Stockage du mot de passe

- Stockage en clair. Exemple : Gaim.
- Codage standard comme base64. Exemples : evolution, ncftp, yafc.
- Codage maison. Exemple : gftp.
- Stockage sous forme de hash. Exemple : mot de passe Unix.
- Vrai chiffrement. Exemple : Firefox (si le mot de passe principal est défini) et KWallet (sous KDE).

Mots de passe circulant sur le réseau

- De nombreux protocoles de communications envoyent les mots de passe en clair : telnet, POP3, FTP, HTTP Basic, etc.
- On peut encapsuler ces protocoles dans un tunnel sécurisé tel que SSH.
- Ou bien utiliser des protocoles plus sûrs tel que POP3 par SSL, HTTPS, SFTP, SSH, etc.

Sommaire

Algorithmes de chiffrement

- Ancêtres : XOR, Cesar, etc.
- Symétriques : RC5, DES, AES, etc.
- Asymétriques : RSA, ElGamal, etc.

Algorithmes de signature

- Un hash est un condensat d'une longueur fixe d'une chaîne de caractère ou d'un fichier. On s'en sert pour signer un document électronique (vérifier qu'il n'a pas été modifié). En cryptographie, le but rechercher est qu'il soit difficile de revenir au mot de passe en partant du hash.
- Ancêtres : CRC32.
- Déconseillés : MD5 et SHA-1.
- Modernes : Whirlpool et Tiger (orientés sécurité).

Sommaire

Introduction

- La cryptanalyse est la science qui étudie les algorithmes de chiffrement et de signature.
- Le chiffrement et les signatures utilisent largement les mathématiques.
- Les algorithmes sont torturés pour qu'ils montrent leurs faiblesses. Lorsqu'un algorithme est "cassé", un nouveau va le remplacer.

Techniques de cryptanalyse

- Anlalyse fréquentielle permettant de casser des chiffrements XOR et Cesar.
- Cryptanalyse linéaire, différentielle, quadritique, etc.

Sommaire

Attaque par dictionnaire

- Pour attaquer un système d'authentification, on peut tester les mots de passe les plus courant. On utilise pour cela des dictionnaires.
- Le programme d'attaque utilise les astuces courantes comme ajouter un nombre à la fin d'un mot (jojo42) ou remplacer une lettre par un chiffre (h4k3r).
- La solution pour éviter ces attaques est de limiter le nombre d'essai d'authentification et/ou ajouter un délai après un échec.

Attaque par force brute

- Parfois, un attaque par force brute est envisageable. Elle consiste à tester tous les mots de passe possibles.
- On teste par exemple les mots de passe entre 1 et 8 caractères composés de lettres ou de chiffre.
- Mais c'est le cas de dernier recours, le social engineering est bien plus efficace !

Attaque de hash

- Une fonction de hashage est très difficilement réversible, mais c'est possible. Le principe consiste à essayer un mot de passe, calculer son hash et le comparer au hash qu'on veut "casser".
- Le logiciel RainbowCrack précalcule des hashs et possède un algorithme d'accès très rapide. Il produit des fichiers d'une taille allant jusqu'à 64 Go.

Social engineering

Because human stupidity has no limit

- Le social engineeing est une méthode permettant de soustraire une information ou un bien en usant de l'ignorance et la naïveté de sa victime.
- Cette technique peut se pratiquer par téléphone (moyen le plus simple et rapide), par email, par lettre, ou par contact direct.
- La méthode la plus connue est l'hameçonage (phishing en anglais) qui consiste à envoyer un email à sa victime lui demandant d'aller sur un faux site pour revalider son mot de passe.
- La meilleure solution reste la paranoïa