4897 DEBONO Juliette

Déchiffrement de mots de passe : Étude de différentes méthodes.

La cybersécurité est un sujet qui me passionne, et l'aborder avec un sujet aussi courant que les mots de passe est une approche que je trouve intéressante. En étudiant ce sujet j'ai pu comprendre comment mieux protéger mes comptes internet.
Comprendre comment fonctionnent les techniques pour décrypter des mots de passe est utile pour mieux s'en protéger, et donc pour garder sécurisé nos données en ligne. Or la sécurité de nos données est aujourd'hui un enjeu majeur dans notre société.

Ce TIPE fait l'objet d'un travail de groupe.

Liste des membres du groupe :

- *GRAS Romain*

Positionnement thématique (ETAPE 1)

INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Cryptanalyse	*Cryptanalysis*
Hachage	*Hash*
Compromis temps mémoires	*Time-memory trade-off*
Mot de passe	*Password*
Table arc-en-ciel	*Rainbow table*

Bibliographie commentée

La cryptologie est l'étude des méthodes de protection de messages. Les mots de passe sont très utilisés sur Internet pour sauvegarder avec sécurité les données des utilisateurs. Avec l'augmentation de cette utilisation, de plus en plus de personnes se sont penchées sur ses limites, donc comment accéder aux comptes protégés par un mot de passe. Le gouvernement à travers l'ANSSI essaye de sensibiliser la population sur ce sujet. [1]

Bien que les sites internets soient généralement faits pour se bloquer après quelques essais infructueux, les attaquants contournent ce problème en récupérant les bases de données des mots de passe du site. Mais pour lutter contre ça, les sites stockent les mots de passe chiffrés. [2]

Il existe différentes méthodes pour coder ces mots de passe, la plus utilisée étant les fonctions de hachage. En effet, le site va récupérer le mot de passe de l'utilisateur, le coder par une fonction et vérifier si l'empreinte correspond à celle stockée. Il faut donc une fonction injective très rapide pour coder un mot mais dont il est impossible de retrouver l'antécédent d'une empreinte. Les fonctions

de hachage tentent de correspondre le plus possible à ces paramètres. De plus, une légère modification d'un caractère modifie complètement l'empreinte. [3]

Ainsi, l'attaquant qui obtient la base, même si il sait quelle fonction de hachage a été utilisé, ne peut pas trouver simplement les mots de passe. Les attaques par force brute (tester tous les mots de passe jusqu'à avoir le bon hash) et par mémoire (stocker les hash correspondants à tous les mots) sont des méthodes naïves suffisantes pour des petits mots de passe mais vite dépassées pour de plus grands mots de passe. [2]

Il existe des méthodes de compromis temps mémoire. Martin Hellman développe le concept de table de compromis en 1980, où il imagine qu'on réalise des calculs au préalable dont on ne stocke que certains résultats. Ainsi, grâce à ces tables, peu de mémoire est nécéssaire et moins de calculs que la force brute, mais la recherche d'un mot dans la table nécessite de refaire certains calculs. [4]

Ronald Rivest ajoute une amélioration en 1982 pour retrouver plus vite les mots de passe en introduisant la méthode des points distingués. [5]

En 2003, Philippe Oechslin conçoit les tables arc-en-ciel en reprenant le concept de Hellman mais plus efficacement. [6][7]

Ces méthodes sont très efficaces pour trouver des mots de passe dont on dispose des empreintes et de la fonction de hachage utilisée. Cependant, pour lutter contre celles-ci, les sites internet utilisent le salage qui réduisent l'utilisation de ces tables à un seul utilisateur. [8]

Problématique retenue

Quelles sont les meilleures méthodes pour déchiffrer un mot de passe ?

Objectifs du TIPE

1. Présenter le fonctionnement des chiffrages des mots de passe sur le web.

2. Chercher des méthodes simpes pour les déchiffrer, les implémenter et voir leurs limites.

3. Étudier des améliorations appélées tables de compromis temps mémoire.

4. Comparer ces méthodes pour voir lesquelles sont les plus appropriées.

Références bibliographiques (ETAPE 1)

[1] Agence nationale de la sécurité des systèmes d'information (ANSSI) : Recommandations de sécurité relatives aux mots de passe :
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf
[2] Jean-Paul Delahaye : L'art et la science des mots de passe : *Pour la science, 492, (octobre 2018) 80-85*

[3] Whitson Gordon : How Your Passwords Are Stored on the Internet : *https://lifehacker.com/how-your-passwords-are-stored-on-the-internet-and-when-5919918*

[4] Martin Hellman : A Cryptanalytic Time - Memory Trade-Off : *IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-26, NO. 4 (JULY 1980) 401*

[5] Dorothy Denning : Cryptography and Data Security : *Addison-Wesley Longman Publishing Co. (1982), ISBN:978-0-201-10150-8, p100*

[6] Philippe Oechslin : Making a Faster Cryptanalytic Time-Memory Trade-Off : *https://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf*

[7] Université de Savoie : compromis temps / mémoire, les tables arc-en-ciel : *https://www.lama.univ-savoie.fr/pagesmembres/hyvernat/Enseignement/2021/info910/tp2.html*

[8] Philippe Oechslin : Security and Privacy : *Slides récuperées auprès de M. Oechslin*

DOT

[1] *Mars - Mai 2020 : Découverte des fonctions de hachage, programmation de SHA256 et MD5*

[2] *Septembre 2020 : Travail sur les fonctions de hachage*

[3] *Octobre 2020 : Changement d'objectif, découverte des tables arc en ciel, début de la programmation*

[4] *Novembre 2020 : Fin de la programmation des tables classique et arc-en-ciel*

[5] *Début Décembre 2020 : Entretien avec Philippe Oechslin*

[6] *Décembre 2020 - Janvier 2021 : Programmation des autres méthodes : Force brute, attaque par mémoire et dictionnaire*

[7] *Janvier 2021 : tests pratiques avec les programmes, comparaison avec les probabilités*

[8] *Février 2021 : Programmations des fusions, du hachage visuel.*