La sécurité des mots de passe

Pr Chérif DIALLO, CISSP
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" La meilleure façon de contrôler sa femme aujourd'hui est d'avoir son mot de passe Facebook." El Commandante Alou Ouattara.

Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un problème courant de cybersécurité. Il s'agit des attaques sur les mots de passe qui constituent un vecteur d'attaque souvent utilisé pour contourner ou exploiter l'authentification des comptes d'utilisateurs. En tant que l'une des menaces de sécurité des applications les plus courantes, les attaques de mot de passe représentaient plus de 81% des violations de données en 2020. Cet article explique ce qu'est une attaque par mot de passe, les différents types d'attaques de mot de passe et les meilleures pratiques pour les empêcher.

Mots clés : Cybersécurité, Mot de passe, Attaque, Keyloggers, Authentification multi facteur, Biométrie.

---

1. Définition

Les mots de passe sont conçus pour authentifier l'accès aux services et aux systèmes de manière sécurisée. L'idée est de garder un mot de passe secret pour empêcher les autres d'accéder à des données personnelles et sensibles. Cependant, comme de nombreuses personnes utilisent des mots de passe faibles ou ne savent pas les conserver, les comptes sont plus vulnérables aux pirates.

Une attaque par mot de passe est un type de cyberattaque où les pirates tentent d'accéder à un fichier, un dossier, un compte ou un ordinateur sécurisé par un mot de passe. Cela se fait généralement à l'aide d'un logiciel qui accélère le déchiffrage ou la devinette des mots de passe. C'est pourquoi il est essentiel de suivre une pratique sécurisée lors de la création de mots de passe, comme par exemple, éviter d'utiliser le nom, les surnoms, l'adresse de l'appartement, le nom de votre animal, etc. Ces derniers sont faciles à deviner, notamment pour celui qui vous connait personnellement.

Les attaques par mot de passe en cybersécurité nécessitent des techniques et des logiciels spéciaux. Si quelqu'un est proche de vous, il peut essayer de deviner votre mot de passe en utilisant une combinaison de noms, de passe-temps, d'années essentielles ou de chiffres. Si cela ne fonctionne pas, il peut utiliser des applications spécialisées qui parcourent une liste de mots que de nombreuses personnes utilisent comme mots de passe. Étonnamment, plus de 75 % de la population Internet définit des mots de passe composés uniquement des 500 premiers mots.

2. Quelques récentes attaques de mot passe

En janvier 2021, le site Web de quiz DailyQuiz (anciennement ThisCrush) a subi une attaque par mot de passe où les attaquants ont exploité une base de données de plus de 13 millions de comptes. Les pirates ont volé des mots de passe, des adresses e-mail et des adresses IP en clair et les ont mis en vente dans le domaine public. Un mot de passe en clair est un moyen d'envoyer ou de stocker des mots de passe dans un format clairement lisible. Il est donc extrêmement risqué de stocker des informations sensibles sur les utilisateurs au format texte brut.

Le 15 septembre 2022, Uber Technologies Inc. a été victime d'un piratage par un jeune de 18 ans. Afin d'accéder au compte d'un employé, le pirate a obtenu des informations d'identification volées sur le dark Web.

En décembre 2022, LastPass, un gestionnaire de mots de passe, a informé certains clients que leurs informations avaient été compromises lors d'un récent incident de sécurité. En août 2022, l'environnement de développement de LastPass avait aussi été piraté.

3. Quelques statistiques sur les mots de passe

Ces statistiques sur les mots de passe aident à mieux comprendre à quel point il est crucial de choisir un mot de passe fort. Pour les entreprises et les organisations, elles soulignent l'importance de disposer d'un logiciel de sécurité informatique et l'impact que peuvent avoir les violations de mots de passe :

- Le premier mot de passe numérique au monde a été créé au MIT en 1961.
- 71% des comptes sont protégés par des mots de passe utilisés sur plusieurs sites web
- Un mot de passe est utilisé en moyenne pour accéder à cinq comptes.
- Il ne faut que 10 minutes en moyenne pour craquer un mot de passe minuscule contenant six caractères.
- Un mot de passe à 12 caractères est 62 trillions (i.e. un milliard de milliards) de fois plus difficile à craquer qu'un mot de passe à 6 caractères.
- 50% des internautes utilisent le même mot de passe pour tous leurs comptes.
- 66 % des personnes créent des mots de passe similaires à ceux qu'elles ont déjà utilisés.
- 336 millions d'utilisateurs ont été affectés par un bug de Twitter qui sauvegardait les mots de passe en texte clair.
- Un tiers des violations sont causées par des logiciels malveillants de type "password dumper".
- 81 % des violations de données d'entreprises sont dues à des mots de passe inadéquats.
- 80% des incidents de piratage en 2020 sont causés par des informations de connexion volées et réutilisées.
- Les attaques de piratage utilisant des scripts qui tentent de deviner les noms d'utilisateur et les mots de passe se produisent en moyenne toutes les 39 secondes, dans le monde entier (WebsiteBuilder.org, 2021).
- L'authentification multifactorielle bloque 99,9 % des attaques.

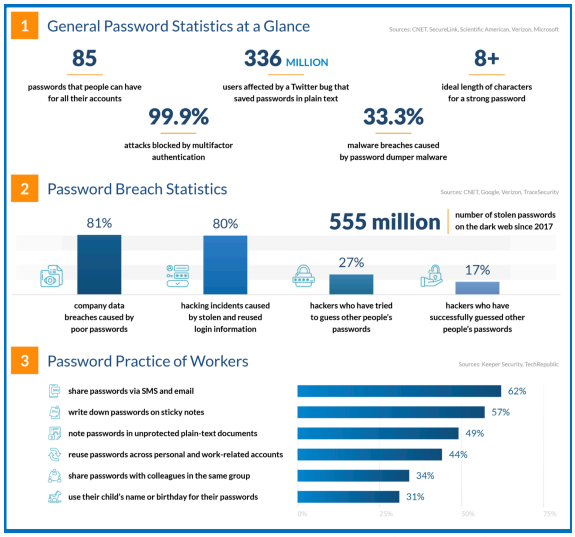

Figure 1: Statistiques à connaitre sur les mots de passe

4. Solutions

Il y a plusieurs types d'attaques sur les mots de passe. Les solutions dépendent, en général, du type d'attaque considéré :

- ***Attaque par force brute.*** Un pirate utilise la logique et les données d'un utilisateur pour deviner le mot de passe le plus probable. Cette technique est utilisée pour les mots de passe simples, tels que ceux contenant une combinaison du nom de l'animal, de l'année et des données de naissance. Un hacker utilisant un script peut essayer 2 180 milliards de combinaisons de mot de passe et nom d'utilisateur en 22 secondes. ***Pour éviter les attaques par force brute*** :
  - ***Utilisez un mot de passe complexe.*** La différence entre un mot de passe à six caractères entièrement alphabétiques et en minuscules et un mot de passe à dix caractères, mélangeant chiffres et lettres, tant minuscules que majuscules, est tout simplement énorme. Les chances de réussite d'une attaque par force brute diminuent proportionnellement selon la complexité de votre mot de passe.
  - ***Activez et configurez un accès à distance.*** Si votre entreprise a recours à la gestion des accès à distance. Un outil de gestion des accès permet de réduire le risque d'attaque par force brute.
  - ***Exigez l'authentification multi facteur.*** Si l'authentification multi facteur (AMF) est activée sur votre compte, un hacker potentiel n'aura probablement pas accès à votre second facteur (i.e. appareil mobile, empreinte digitale, visage, etc.).
- ***Attaque par dictionnaire***. L'attaque par dictionnaire est une attaque par force brute. Elle repose sur notre habitude de choisir des mots simples à titre de mot de passe, ce qui a permis aux hackers de réunir les plus courants d'entre eux dans des « dictionnaires de craquage ». Des attaques par dictionnaire plus

sophistiquées peuvent intégrer des mots qui sont importants pour vous à titre personnel, comme un lieu de naissance, un nom d'enfant ou un nom d'animal de compagnie. ***Pour éviter une attaque par dictionnaire :***

  - ***N'utilisez jamais un mot du dictionnaire comme mot de passe.*** Aucun mot apparaissant dans un livre ne devrait faire partie de votre mot de passe. Si vous devez utiliser un mot de passe au lieu d'un outil de gestion des accès, envisagez d'avoir recours à un système de gestion des mots de passe.
  - ***Verrouillez les comptes après un grand nombre d'échecs de tentative de connexion par mot de passe.*** Il peut être très frustrant de perdre accès à un compte si vous oubliez momentanément votre mot de passe, mais cela reste préférable à l'insécurité du compte. Accordez-vous un maximum de cinq tentatives avant que l'application ne vous arrête.
  - ***Envisagez d'investir dans un gestionnaire de mots de passe.*** Ceux-ci génèrent automatiquement des mots de passe complexes qui aident à prévenir les attaques par dictionnaire.

- ***Bourrage d'identifiants.*** Si vous avez été victime de piratage par le passé, vous savez que vos anciens mots de passe ont sans doute été divulgués à un site Web peu recommandable. Le bourrage d'identifiants profite des comptes dont le mot de passe n'a jamais été modifié après intrusion dans le compte associé. Les hackers essaient plusieurs combinaisons d'anciens noms d'utilisateur et mots de passe, en espérant que la victime ne les a jamais changés. ***Pour éviter le bourrage d'identifiants :***
  - ***Surveillez vos comptes.*** Il existe des services payants qui surveillent les identités en ligne, mais vous pouvez également avoir recours à des services gratuits pour voir si votre adresse e-mail est liée à de récentes fuites d'informations.
  - ***Changez régulièrement vos mots de passe.*** Plus longtemps un mot de passe reste inchangé, plus il est probable qu'un hacker trouve la façon de le craquer.
  - ***Utilisez un gestionnaire de mots de passe.*** Comme avec une attaque par dictionnaire, beaucoup d'attaques par bourrage d'identifiants peuvent être évitées grâce à un mot de passe fort et sécurisé. Un gestionnaire de mots de passe est utile pour cela.
- ***Keyloggers ou Enregistreurs de frappe.*** Il s'agit d'un dispositif d'espionnage informatique qui enregistre les suites de touches tapées sur un clavier. L'enregistreur de frappe est donc un type de logiciel malveillant conçu pour effectuer le suivi de chaque frappe sur le clavier en la communiquant à un hacker. En général, un utilisateur télécharge le logiciel en pensant qu'il s'agit d'un produit légitime, mais ce dernier installe un enregistreur de frappe sans qu'il le remarque. ***Pour vous protéger des keyloggers :***
  - ***Contrôlez votre matériel physique.*** Si quelqu'un a accès à votre station de travail, il peut installer un enregistreur de frappe matériel pour collecter des informations sur vos frappes sur le clavier. Inspectez régulièrement votre ordinateur et la zone environnante pour vérifier l'absence de matériel inconnu de vous.
  - ***Lancez une analyse antivirus.*** Utilisez un logiciel antivirus reconnu pour analyser votre ordinateur de manière régulière. Les fournisseurs d'antivirus disposent de listes des enregistreurs de frappe malveillants les plus courants et les marquent comme dangereux.

5. Pour finir

Voici quelques bonnes pratiques pour empêcher les attaques par mot de passe :

- ***Appliquer des politiques de mots de passe forts.*** Les administrateurs de sécurité doivent appliquer des politiques qui garantissent que les utilisateurs suivent des critères définis pour empêcher les acteurs malveillants de déchiffrer leurs mots de passe. Par exemple, le mot de passe doit comporter au moins 8 caractères et inclure des caractères spéciaux pour éviter les tentatives de force brute. De plus, les mots de passe ne doivent pas contenir d'informations d'identification personnelle, car cela pourrait favoriser les attaques par dictionnaire. Les utilisateurs doivent également utiliser des mots de passe uniques pour chaque service et alterner fréquemment les mots de passe pour empêcher les attaquants d'utiliser les bases de données d'informations d'identification exposées pour les attaques par mot de passe.
- ***Formation à la sécurité des mots de passe à l'échelle de l'organisation.*** Il est essentiel de s'assurer que chaque utilisateur comprend l'importance d'une politique de mot de passe solide et suit la sensibilisation de l'ensemble de l'organisation à la sécurité des mots de passe. De plus, chaque utilisateur d'application doit être conscient des attaques d'ingénierie sociale qui les incitent à soumettre leurs informations d'identification à des tiers malveillants.
- ***Authentification Multi Facteur (AMF).*** Les mots de passe en eux-mêmes n'offrent généralement pas une solution complète d'authentification des utilisateurs. L'authentification multi facteur implique l'utilisation de mots de passe en combinaison avec des contrôles de sécurité supplémentaires. Certaines implémentations AMF incluent le mot de passe à usage unique (OTP), l'authentification biométrique, les jetons logiciels et l'analyse comportementale.
- ***Gestionnaire de mots de passe.*** La fonction principale d'un gestionnaire de mots de passe est d'aider les administrateurs Web à stocker et à gérer les informations d'identification des utilisateurs. Les solutions de gestion des mots de passe génèrent également des mots de passe pour les utilisateurs conformément à des

politiques strictes et aux meilleures pratiques. De plus, ces outils stockent les informations d'identification des utilisateurs dans des bases de données fortement cryptées, ce qui les protège de manière robuste contre toute exposition à une violation de données.

- ***Biométrie.*** Une personne malveillante aura beaucoup de mal à répliquer vos empreintes digitales ou la forme de votre visage. L'activation de l'authentification biométrique renforce ainsi la sécurité de vos mots de passe.

Ainsi, alors que les attaques par mot de passe ont certainement évolué, les mesures pour atténuer ces menaces varient, mais les principes de base de sécurité restent toujours les mêmes : Mettez à jour vos systèmes et vos bases de données antivirus, formez vos employés, configurez votre pare-feu afin qu'il n'autorise que les communications vers les ports et les hôtes nécessaires, choisissez des mots de passe forts, appliquez le principe du moindre privilège dans votre environnement informatique, faites des sauvegardes régulières et vérifiez continuellement vos systèmes afin de détecter toute activité suspecte.