Comment choisir un bon mot de passe ?

Gildas Avoine, Diane Leblanc-Albarel

THE CONVERSATION

L’expertise universitaire, l’exigence journalistique

Mots de passe compliqués, gestionnaires de mots de passe, ça vaut le coup? Jason Dent, Unsplash, CC BY

Comment choisir un bon mot de passe ?

Publié: 8 janvier 2023, 17:43 CET

Diane Leblanc-Albarel
Doctorante en Cybersécurité, INSA Rennes

Gildas Avoine
Professeur en Cybersécurité, INSA Rennes

Alors que les cyberattaques se multiplient, chacun d'entre nous peut potentiellement y être confronté. Certes, nous avons tous nos astuces pour les mots de passe que nous utilisons dans nos ordinateurs et nos portables : cachés sous un clavier, écrits sur un bout de papier ou issus de la date d’anniversaire du petit dernier.

Mais comment faire pour s'assurer que son mot de passe est véritablement in-cra-qua-ble ?

De nombreuses études constatent qu’une part importante des mots de passe ne protègent pas suffisamment les utilisateurs : les mots de passe sont trop faibles et trop souvent réutilisés. Par exemple, 51 % des Français utiliseraient le même mot de passe pour des usages professionnels et personnels – une statistique que l’on retrouve aux États-Unis.

À partir d'un mot de passe, les cybercriminels pourront récupérer des informations privées en se connectant à nos comptes en ligne (messageries, réseaux sociaux, etc.), notamment nos comptes bancaires ou de e-commerce, mais aussi pénétrer sur notre ordinateur et en chiffrer le contenu en vue d'obtenir une rançon.

Le vol d'un mot de passe peut avoir des conséquences financières, mais aussi psychologiques à travers des pratiques comme le « doxxing » (publier des informations sur l'identité ou la vie privée d'une personne dans le but de lui nuire) ou le « revenge porn ». Dans le cadre professionnel, les fuites de mot de passe exposent l'entreprise à des attaques par chantage, à des « dénis de service » (des cyberattaques consistant à interrompre ou malmener le service fourni par un tiers), ou encore à de l'espionnage économique.

À lire aussi : Cryptographie : comment ma carte à puce résiste-t-elle aux attaques ?

Comment un fraudeur récupère-t-il des mots de passe ?

Les deux grandes approches utilisées par les cybercriminels pour récupérer des mots de passe sont l'ingénierie sociale et le vol de bases de données d'identifiants.

L'ingénierie sociale consiste pour le cybercriminel à convaincre sa victime de révéler son mot de passe en ayant, typiquement, recours à l'hameçonnage : la grande majorité des attaques ne ciblent pas une victime prédéfinie et ces attaques de masse ont pour but d'hameçonner des victimes quelconques. C'est seulement dans un second temps que le cybercriminel concentrera ses forces sur la personne hameçonnée.

Quant au vol de bases de données d'identifiants, l'attaque consiste généralement à pirater un site web pour voler les noms et mots de passe des utilisateurs afin de se connecter sur le compte des victimes, de les utiliser sur d'autres comptes (par exemple, le fraudeur testera les identifiants Google de sa victime sur Twitter) ou de les revendre sur le *dark web*. Le site web « Have I been pwned ? » permet à chacun de vérifier si son mot de passe a fuité sur Internet ; il recense actuellement presque 12 milliards de comptes dont les identifiants ont fuité.

Dans la majorité des cas, ces bases de données d'identifiants ne contiennent pas des mots de passe, mais des empreintes de mots de passe : l'empreinte est le résultat d'une fonction dite « à sens unique » qui est appliquée sur le mot de passe. Par analogie, l'empreinte est au mot de passe ce que l'empreinte digitale est à l'humain : deux mots de passe différents ont des empreintes différentes et étant donné une empreinte, on ne peut pas identifier l'humain. Mais étant donné une empreinte et un humain, on peut dire si l'empreinte provient de cet humain. Dans le cas des mots de passe, on ne peut donc pas retrouver le mot de passe à partir de son empreinte, mais on peut tester un mot de passe pour voir s'il correspond à l'empreinte : on dit alors que le mot de passe est « cassé ».

Les casseurs de mots de passe utilisent différentes approches pour tester les mots de passe les plus probables : d'abord les plus courts, puis les mots du dictionnaire et leurs variantes (par exemple « repas », puis « Repas », « RepaS », « saper », « repas1 »…) et les mots de passe fortement structurés (par exemple démarrant par une majuscule, puis des minuscules, des chiffres et enfin des caractères spéciaux).

Les casseurs modernes peuvent également utiliser des techniques évoluées reposant sur l'intelligence artificielle ou l'algorithmique.

Enfin, tous les mots de passe possibles sont testés si les autres tentatives ont échoué : c'est ce que l'on appelle une recherche exhaustive, qui a généralement peu d'espoir de rencontrer un succès en un temps raisonnable. Notamment, les attaques qui consistent à tester directement sur un site web différents mots de passe pour un utilisateur donné jusqu'à réussir à se connecter sont peu praticables : elles sont très lentes à cause du temps de réponse du serveur web et facilement détectables.

Qu'est-ce qu'un mot de passe robuste ?

Pour se protéger efficacement, il faut utiliser des mots de passe robustes, ne pas utiliser un même mot de passe pour plusieurs usages et changer de mots de passe régulièrement.

Pour qu'un mot de passe soit robuste, il faut qu'il soit choisi aléatoirement dans un ensemble de mots de passe ayant la même chance d'être choisis : par exemple, un mot présent dans le dictionnaire serait cassé en une poignée de secondes. Ajouter une majuscule ou des chiffres à la fin n'apporte qu'une sécurité illusoire.

À lire aussi : Cryptographie : à quoi servent les nombres aléatoires ?

Afin de mesurer la robustesse d'un mot de passe choisi aléatoirement (cas idéal, rarement atteint sans gestionnaire de mots de passe), on compte le nombre de tests que devra faire un pirate dans le pire des cas pour le casser. Cette valeur est généralement calculée par la formule n^c_ où c est la longueur du mot de passe et n la taille de l'ensemble des éléments parmi lesquels piocher pour composer le mot de passe. Par exemple, dans le cas d'un mot de passe de longueur 8 (c=8), composé de lettres minuscules uniquement (n=26), le pirate devra tester 26^8 mots de passe (soit 208 milliards) dans le pire des cas. Bien que le chiffre semble astronomique, un ordinateur standard mettra moins d'une seconde pour le casser en utilisant la puissance de calcul de sa carte graphique.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) définit la robustesse d'un mot de passe par la taille de l'espace dans lequel il est choisi aléatoirement, et distingue quatre catégories.

La robustesse d'un mot de passe d'après l'ANSSI

Un mot de passe aléatoire, construit à partir d'un alphabet constitué de lettres, de chiffres et de 8 caractères spéciaux, devra ainsi contenir au moins 17 caractères (par exemple, « b !sDzf5w,5+W2s3k ») pour être considéré comme fort selon l'ANSSI, et il sera considéré comme très faible s'il est de taille inférieure ou égale à 10 caractères (« b !sDzf5w,5 »). Même très faible, le mot de passe sera difficile à mémoriser… surtout qu'il faut en mémoriser des dizaines !

Pour faciliter la mémorisation des mots de passe, une technique de plus en plus recommandée consiste à utiliser des « phrases de passe », c'est-à-dire des suites de mots choisis aléatoirement. Une phrase de passe de sept mots choisis dans un dictionnaire de 60000 mots pourrait ainsi être « contrefort fatalement semelle signifié distance revergète fourguer », plus facile à mémoriser que « b !sDzf5w,5+W2s3k » pour une sécurité équivalente.

Mais il est difficile pour un humain de choisir aléatoirement des mots dans un ensemble suffisamment grand, car nous n'utilisons que quelques centaines de mots au quotidien. Il est alors conseillé de rajouter des minuscules, majuscules et caractères spéciaux dans la phrase de passe.

Faut-il utiliser un gestionnaire de mots de passe ?

Un gestionnaire de mots de passe est une application qui stocke de manière sécurisée tous les mots de passe de l'utilisateur pour qu'il n'ait pas besoin de les mémoriser. Il lui suffit de se souvenir d'un seul mot de passe, le mot de passe maître, qui doit être le plus fort possible tout en restant mémorisable. L'utilisation d'un gestionnaire de mots de passe, par exemple KeyPass, est recommandée par les grands acteurs de la cybersécurité tels que l'ANSSI, son homologue allemand, le BSI ou l'agence européenne ENISA, ainsi que par des organisations comme Reporters sans Frontières. Certains gestionnaires de mots de passe sont stockés dans le cloud, par exemple Bitwarden (gratuit et open source), 1Password (payant), DashLane (payant), ou encore LastPass (payant, mais il existe une version gratuite assez évoluée) qui est le gestionnaire le plus utilisé mais aussi le plus attaqué.

Notons que les gestionnaires intégrés dans les navigateurs (qui ne nécessitent pas d'installation) ne sont pas recommandés pour des raisons de sécurité, comme le souligne le BSI allemand.

Dans le cas où le gestionnaire stocke les mots de passe dans le cloud, il est fondamental que les mots de passe maîtres soient forts, au sens de l'ANSSI. Dans le cas contraire, un prestataire ayant accès au cloud pourrait les casser et ainsi accéder à tous les mots de passe qu'ils protègent. Il s'agit d'une menace sérieuse à prendre en compte par les entreprises, dans un monde où l'espionnage économique est légion. Recommander aux entreprises d'héberger elles-mêmes les gestionnaires de mots de passe de leurs employés n'est certainement pas un excès de prudence.

Enfin, l'usage de l'authentification par double facteur (par exemple la réception d'un code par mail) est fortement recommandé… même s'il ne faut pas pour autant baisser la garde.