

SAE 11

LUC Romain

DUCREY Maxence

BUT1 Réseaux et Télécommunications

LA SÉCURITÉ DES MOTS DE PASSE

Introduction : Bonjour, à travers ces pages, vous allez pouvoir en apprendre plus sur les mots de passe et ce qu'est la sécurité des mots de passe. Tout d'abord, la **sécurité des mots de passe** est en *constante évolution*. En effet, les technologies, les logiciels, et les techniques se font de plus en plus précises, complexes, et puissantes. De ce fait, il en va de soi que les outils de protection des données doivent aussi être au niveau des outils de piratage.

Pour nous protéger des attaques malveillantes, nous utilisons au quotidien les **mots de passe**.

Mais qu'est-ce qu'un mot de passe ? Un mot de passe est une série de caractères utilisé comme moyen d'**authentification** pour prouver son identité lorsque l'on désire accéder à un lieu protégé (par exemple : les digicodes à l'entrée de certaines résidences), à un compte informatique, un ordinateur, ou encore un logiciel.

Le mot de passe doit être tenu secret pour éviter qu'un tiers non autorisé puisse accéder à la ressource ou au service. C'est une méthode parmi d'autres pour vérifier qu'une personne correspond bien à l'identité déclarée. Il s'agit d'une preuve que l'on possède et que l'on communique au service chargé d'autoriser l'accès.

Il existe plusieurs types de mots de passe comme le code PIN, le schéma téléphonique, le mot de passe avec des lettres de l'alphabet, des caractères spéciaux, ou encore des nombres. Les codes PIN et les schémas sont souvent utilisés sur les téléphones portables comme moyen de déverrouiller rapidement le téléphone (par exemple : voir Figure 1 et Figure 2). À titre d'exemple de mots de passe avec des caractères, on a : C0r1eOn3 ou azertyuiop ou \$t@b1lO.



Figure 1.



Figure 2.

Ainsi, nous allons répondre à la problématique suivante :

Quels sont les enjeux de la sécurité des mots de passe ?

Dans un premier temps nous exprimerons les risques auxquels peuvent être soumis les mots de passe où nous verrons que peut donc faire une personne malveillante avec votre mot de passe puis quels sont les différents moyens pour pirater un ou des mots de passe. Subséquemment, nous découvrirons comment sécuriser les mots de passe grâce aux méthodes générales mais aussi

comment renforcer la sécurité de ceux-ci par l'intermédiaire de l'Authentification à Double Facteurs (A2F).

Ainsi, comme dit précédemment, tout le monde a besoin d'un mot de passe. En effet, tous les êtres humains ont des **informations confidentielles et personnelles**. C'est pourquoi, nous avons tous besoin d'un ou plusieurs mots de passe. Or, que se passe-t-il si un de nos mots de passe n'est pas assez sécurisé et que quelqu'un a, par diverses méthodes, réussi à récupérer ce mot de passe ?

Nous allons donc voir ce que peut faire une personne malveillante avec notre mot de passe.

Tout d'abord celui-là peut avoir **accès à nos données** à travers l'usurpation de notre authentification. Dans ces données on peut notamment citer l'accès aux e-mails où il est possible de voler des informations personnelles comme le nom de certains contacts comme des responsables hiérarchiques ou de la famille. Parfois, ces mails contiennent des informations sensibles (factures, photos de familles, etc..).

Ensuite, avec notre adresse e-mail, le **cybercriminel** peut potentiellement se connecter à un de nos comptes sur les réseaux sociaux. En effet, si le mot de passe de l'adresse mail est le même que celui sur le réseau social, alors il pourra aisément se connecter à notre compte. De ce fait, il pourrait avoir accès à nos conversations privées, et donc, à des informations sensibles. En conclusion, si vous avez le même mot de passe sur toutes les plateformes et que la personne malveillante a accès à votre mot de passe, alors il peut avoir accès à littéralement toute votre vie.

De plus, quand le cybercriminel aura votre mot de passe et qu'il aura essayé de se connecter un peu partout, il s'apercevra que vous avez énormément de données, dont des données qui peuvent valoir cher. De ce fait, le criminel pourrait vendre votre compte sur un site pas forcément légal qui peut être sur le Darknet ou encore sur l'Internet sur lequel nous naviguons tous ! Cette pratique de vente de données se voit beaucoup sur les jeux-vidéos. En effet, le cybercriminel arrive par plusieurs techniques à récupérer votre mot de passe et il se peut que sur votre compte, vous ayez des données très chères. Par exemple, sur Counter-Strike : Global Offensive, des récompenses dans le jeu peuvent se vendre à plusieurs dizaines de milliers d'euros, alors imaginez l'argent que peut se faire un cybercriminel s'il arrive à accéder à votre compte car votre mot de passe n'était pas assez sécurisé...

Maintenant, imaginons que vous soyez un utilisateur régulier du système de "Cloud". Vous avez toutes vos données sur cet espace de stockage et par diverses méthodes que nous verrons dans la prochaine partie, le pirate arrive à avoir votre mot de passe de votre Cloud. Vous pouvez être assuré que vos données sont perdues ou qu'elles seront en vente sur certains sites, ou que le pirate vous demande une rançon pouvant aller jusqu'à plusieurs milliers d'euros. En effet, il n'a qu'à changer le mot de passe de votre Cloud, ainsi vous n'y avez plus accès et il peut vous demander une rançon en échange de vos données.

Enfin pour finir cette partie il y a un risque de "sur-piratage" si quelqu'un a un de vos mots de passe. En effet, imaginons donc qu'il ait le mot de passe et qu'il puisse se connecter à votre adresse mail. Il peut créer une technique de "phishing" ou d'hameçonnage en français (nous détaillerons ce principe dans la seconde sous partie) et donc envoyer un mail malveillant depuis l'adresse de la victime à toute sa liste de contacts. Tous les contacts de la victime vont penser que c'est leur ami, leur collègue qui a envoyé le mail alors que pas du tout. De ce fait, si le pirate a bien préparé son coup,

tous les contacts vont rentrer leurs informations et le pirate aura accès aux données de sa victime initiale ainsi qu'aux données de tous ses contacts !

En conclusion de cette première sous-partie, une personne qui a notre mot de passe peut faire ce qu'il souhaite *sans aucune difficulté*. De ce fait, nous verrons dans la seconde partie comment sécuriser nos mots de passe pour éviter au maximum de nous faire pirater. D'abord, nous allons voir comment font les pirates pour récupérer nos mots de passe.

Pour finir cette première partie, nous allons traiter de *4 méthodes* que les pirates peuvent utiliser pour arriver à voler nos mots de passe.

La première méthode est le **"phishing"** ou l'hameçonnage en français. C'est sans aucun doute la technique la plus connue pour voler un mot de passe étant donné qu'il y a eu plusieurs campagnes pour sensibiliser les gens à ce phénomène et pour le combattre. Malgré toutes les campagnes de prévention et de sensibilisation, encore trop de gens se font avoir par le phishing. Cette pratique vise à voler votre mot de passe et ce, vraiment très facilement. Nous avons tous déjà reçu des mails dans nos spams qui nous disent que nous avons gagné le tout dernier téléphone ou encore plus répandu, un mail d'*arnaque à la carte bancaire*. Cette dernière est la plus connue de toutes les techniques de phishing. Pour faire simple, le pirate crée une page web presque identique à celle de votre banque. Ensuite, il vous envoie un mail qui peut ne pas être considéré comme un spam en usurpant l'identité de votre banque et peut dire : "Bonjour, nous avons remarquer une tentative de dépense inhabituel sur votre compte bancaire. Veuillez vous connecter à votre espace personnel pour régler ce problème : <http://phishing.com> ". Maintenant, vous cliquez sur le lien, rentrez votre mot de passe, et vos coordonnées bancaires, et le pirate a accès à votre compte. Bien sûr, nous pouvons le contrer. D'abord, dans le mail, le pirate n'est souvent pas français, de ce fait, il y a beaucoup de fautes d'orthographe. De plus, si vous recevez un mail comme ça, appelez votre banque pour avoir la confirmation qu'il y a un bien un problème et que c'est bien eux qui vous ont envoyé ce mail. C'est pourquoi, il est nécessaire de nous méfier de tout ce que nous recevons dans notre boîte mail.

En guise de deuxième méthode, nous allons parler d'une pratique bien moins connue mais très utilisée dans le domaine de la cybersécurité : **l'ingénierie sociale**.

Cette pratique consiste simplement à **manipuler** des personnes pour arriver à un but bien précis. Bien sûr, il y a ceux qui vont pratiquer cette discipline avec de mauvaises intentions sur le plan mental (on parle littéralement de manipulation pour faire mal). D'autres vont s'en servir pour récupérer les informations qu'ils souhaitent. En cybersécurité, les "pentesters" peuvent être amenés à s'en servir s'ils souhaitent s'introduire dans le réseau d'une entreprise par exemple. À titre d'exemple (voir *Source n°8*), en 2020, pendant la pandémie du COVID, un jeune américain de 17 ans, a pris le contrôle de Twitter. Il a simplement utilisé ses capacités de manipulation (ingénierie sociale) et de programmation pour manipuler un simple employé de Twitter. Il a envoyé un mail à cet employé en se faisant passer pour le service technique du réseau social et en disant qu'il y avait un problème sur le réseau et que l'employé devait se connecter à son compte Twitter sur une certaine page de connexion. L'employé s'est fait avoir et le pirate avait accès à son compte, et il a en plus

continué en arrivant à avoir un compte Twitter d'un des administrateurs. De ce fait, il avait le contrôle de tous les comptes existants. Et c'est ce qu'il a exploité. Il a envoyé des Tweet sur des comptes de personnes connus comme (Joe Biden, Elon Musk, etc..) en disant que si les gens donnaient du Bitcoin à une certaine adresse, la personne recevrait 2 Bitcoin le lendemain. Des gens se sont fait avoir et ont perdu de l'argent. Juste avec cet exemple, nous avons pu voir le *pouvoir* qu'avait une personne qui maîtrisait l'ingénierie sociale et le phishing. Ces deux pratiques combinées peuvent être dévastatrices pour toutes les personnes non préparées et pas assez méfiantes sur Internet.

Pour la troisième méthode, on va s'attarder sur les **logiciels malveillants**, ou les "virus" dans le langage courant. En simplifiant, un virus est un logiciel qui permet au développeur de récupérer énormément de données. Il en existe de plusieurs types (les chevaux de Troie, les ransomwares, les *keyloggers*, ...). Le *cheval de Troie* est un virus de type *backdoor*, autrement dit, la personne qui vous a fait télécharger le virus peut contrôler votre PC à distance et donc accéder à vos données facilement. Ensuite, nous pouvons télécharger par mégarde un *ransomware*. Ce logiciel malveillant chiffre simplement nos données et les envoient à la personne qui nous a envoyé ou qui a développé le logiciel en les rendant inutilisables pour nous. Une interface graphique s'affiche nous disant de payer une certaine *rançon* à un compte en cryptomonnaie. Nous avons souvent un compteur qui s'affiche (voir Figure 3.) pour nous dire combien de temps il nous reste pour payer la rançon et espérer récupérer nos données. Bien sûr, il ne faut pas payer et aller directement porter plainte !



Figure 3. Wannacry, un des ransomwares les plus connus

La dernière méthode est elle aussi très connue, nous parlons désormais de l'**attaque par force brute**. Elle consiste à tester des millions de mots de passe en espérant tomber sur le votre. En effet, si le mot de passe n'est pas sécurisé (ex : 0000 ou 1234 ou encore azertyuiop), le pirate peut très rapidement récupérer votre mot de passe (voir Figure 4.). Pour se faire, les pirates utilisent un simple fichier de texte avec des millions de mots de passe possibles (souvent les plus utilisés). Ensuite, ils utilisent le logiciel sur Linux "John The Ripper" qui va tester tous les mots de passe jusqu'à tomber sur le bon. Mais, cette attaque est de moins en moins utilisée. En effet, les applications et les sites sont habitués à cette attaque. De ce fait, de plus en plus d'applications et de sites instaurent un quota maximum de tentatives de connexion à un compte (par ex : s'il y a eu trois

tentatives de mots de passe et qu'elles ont toutes échouées, alors le site verrouillera l'accès à votre compte pendant quelques minutes, vous empêchant de réessayer de mettre un mot de passe).

Figure 4. Tableau de bruteforce des mots de passe

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	8k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

On voit bien que pour minimiser les risques, il faut un mot de passe le plus long possible avec des nombres, des lettres majuscules et minuscules, ainsi que des caractères spéciaux.

En conclusion de cette première partie, nous avons pu voir qu'une personne qui a accès à nos mots de passe a le contrôle de ce qu'il souhaite. De plus, nous avons étudié certaines de leurs méthodes. De fait, nous pouvons constater que ce n'est pas si compliqué de trouver un mot de passe. C'est pourquoi il faut être vigilant et apprendre à sécuriser nos mots de passe avec les conseils qui vont suivre.

Pour la seconde et dernière partie, nous allons apprendre à sécuriser nos mots de passe dans un premier temps pour ensuite dériver vers une nouvelle méthode de sécurisation : l'Authentification à Double Facteur (A2F).

Étudions déjà les méthodes générales. Tout d'abord, pour sécuriser nos mots de passe le plus simplement et efficacement possible, il faut utiliser un **mot de passe fort** (Figure 5.). En effet, plus il aura de caractères différents de tous types, alors il sera quasiment impossible à bruteforce ! Juste avec un mot de passe fort, nous pouvons contourner l'attaque par bruteforce. De ce fait, il est judicieux d'utiliser un mot de passe fort **différent pour chacun de nos comptes**, notamment pour les comptes bancaires.

De plus, il faut éviter d'utiliser les mêmes mots de passe sur des comptes différents. En effet, si un pirate arrive à avoir un mot de passe, alors il pourra se connecter à tous nos comptes...

Ensuite, nous pouvons utiliser un **gestionnaire de mots de passe** qui stocke les mots de passe de tous nos sites. C'est pourquoi, nous ne devons retenir qu'un seul mot de passe, celui pour se connecter au gestionnaire. Le seul problème que nous pouvons rencontrer est si le pirate arrive à trouver le mot de passe de notre gestionnaire, c'est pourquoi il faut un mot de passe fort que nous pouvons retenir et que nous devons donner à personne.

Puis, il faut impérativement **ne jamais ouvrir les pièces jointes de mails non sollicités**. En effet, il y a des chances que ce mail soit une tentative de phishing donc il ne faut pas se faire avoir.

Il faut aussi **éviter d'installer des applications sur des sites non officiels** pour éviter tous logiciels malveillants comme vus précédemment.

De plus, munissez-vous d'un **antivirus** dans le but qu'il puisse vous éviter un piratage de vos données à cause d'un potentiel virus.

Ne jamais se connecter sur un réseau Wi-Fi public. Si c'est vraiment urgent, **utilisez un VPN**.

Enfin, le conseil à respecter à tout prix : Toujours **se méfier des personnes** que nous rencontrons sur Internet. Nous ne connaissons pas leurs véritables intentions. Il faut quoi qu'il arrive se protéger contre une tentative de manipulation, d'ingénierie sociale.

Pour clôturer ce développement sur la sécurité des mots, nous allons voir comment aller encore plus loin. Pour cela, nous traitons de l'**Authentification à Double Facteur** (A2F).

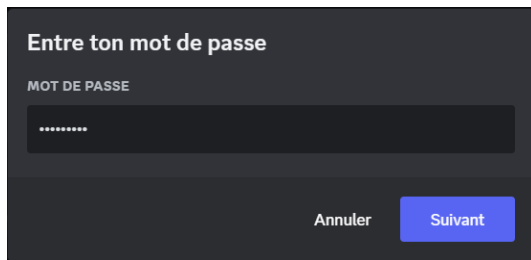
La double authentification est une méthode d'authentification forte par laquelle un utilisateur peut accéder à une ressource informatique seulement après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification. En effet pour se faire, nous renseignons notre mot de passe, et ensuite, si nous l'avons configurée, nous sommes redirigés sur une page nous demandant ce que nous préférons : **un mail de confirmation ou un SMS de confirmation**. Seulement quand nous aurons rentré le code reçu soit par mail soit par SMS, nous serons connectés au site qui nous intéresse. L'A2F est une **seconde barrière** vraiment très puissante pour sécuriser nos données et renforcer encore la sécurité de nos mots de passe. Le code reçu est à usage unique et s'il n'est pas correct, l'authentification échoue même si le mot de passe renseigné correspond à celui relié au compte. Bien sûr, il y a plusieurs types d'A2F. Par exemple : il existe des sites qui nous demandent de renseigner une **phrase secrète** ou une réponse à une question quand nous nous inscrivons dessus comme "Quel est le nom de votre animal de compagnie ?". De ce fait, à l'avenir, le site ou l'application pourrait se servir de cette phrase en tant que seconde barrière avant la connexion pour déterminer si c'est bien vous qui essayez de vous connecter à votre compte. Il existe aussi des sites ou des applications qui utilisent des codes à usage unique en guise d'A2F (voir *Figure 5.*).

AUTHENTIFICATION À DEUX FACTEURS ACTIVÉE

L'authentification à deux facteurs (A2F pour faire court) est une manière efficace d'ajouter une barrière de sécurité supplémentaire à ton compte Discord et de t'assurer que personne d'autre ne peut s'y connecter.

[Voir les codes de sauvegarde](#)

[Supprimer l'A2F](#)



Entre ton mot de passe

MOT DE PASSE

Annuler Suivant

En conclusion de ce développement sur la sécurité des mots de passe, nos données, nos mots de passe sont très vulnérables, c'est pourquoi nous nous devons de les sécuriser. Nous avons pu traiter beaucoup de risques auxquels ils étaient soumis. En exemple, si quelqu'un a un de nos mots de passe, il peut peut-être se connecter à notre espace bancaire, à notre adresse mail, à nos comptes sur les réseaux sociaux. Il peut se connecter un peu partout là où il le souhaite.

Ensuite, nous avons étudié quatre formes d'attaques pour voler un mot de passe : le phishing, l'ingénierie sociale, les virus, et les attaques par force brute. Les attaques par force brute sont un peu moins présentes qu'avant mais les logiciels de rançon sont toujours là et il faut donc faire très attention à ce que nous installons sur Internet. Le phishing et l'ingénierie sociale sont aussi omniprésents, c'est pourquoi il faut à tout prix faire attention à nos fréquentations sur Internet.

Enfin, nous avons appris à sécuriser nos mots de passe avec des méthodes très basiques mais qui fonctionnent très bien : utiliser un mot de passe fort, avoir plusieurs mots de passe, utiliser un gestionnaire de mots de passe, ne pas ouvrir les mauvaises pièces jointes de certains mails, utiliser un antivirus, se méfier des gens sur Internet, et utiliser un VPN si vous êtes connectés sur un réseau public. Et pour finir, activer l'Authentification à Double Facteur (A2F) sur tous les sites et toutes les applications qui la propose pour avoir une sécurité supplémentaire.

N'oubliez pas, les technologies sont en constante évolution. De ce fait, la sécurité des mots de passe et les méthodes pour les dérober vont très probablement changer dans les années à venir.

Sources :

Source 1 : CNIL

Source 2 : Wikipédia

Source 3 : <https://www.passwordmonster.com/>

Source 4 : <https://www.welivesecurity.com/fr/2022/01/07/pirates-mots-de-passe/#:~:text=De%20l%27ing%C3%A9n%C3%A9rie%20sociale%20%C3%A0%20l%27attaque%20par%20force%20brute%2C,malveillants%20utilisent%20pour%20voler%20vos%20mots%20de%20passe.>

Source 5 : https://fr.wikipedia.org/wiki/Double_authentication

Source 6 : <https://www.onelogin.com/fr-fr/learn/what-is-mfa>

Source 7 : <https://www.microsoft.com/fr-ca/security/business/security-101/what-is-two-factor-authentication-2fa>

Source 8 : https://www.lemonde.fr/pixels/article/2020/08/04/piratage-de-twitter-le-principal-suspect-age-de-17-ans-a-deja-un-passe-charge_6048129_4408996.html

Source 9 : <https://www.cnil.fr/fr/definition/force-brute-attaque-informatique>



DUCREY Maxence

LUC Romain BUT1 Réseaux et Télécommunications

Clermont-Ferrand