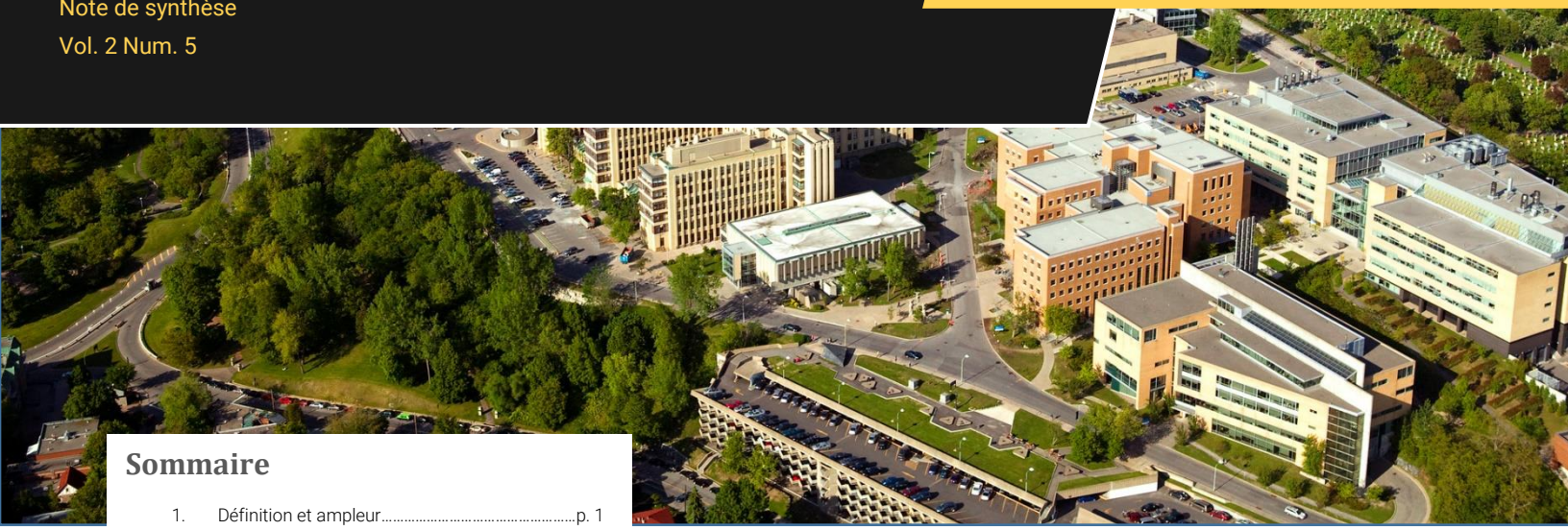
Les tentatives de découverte de mot de passe

Traian Toma, candidat à la maîtrise

Note de synthèse
Vol. 2 Num. 5

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

1. Définition et ampleur....p. 1
2. Les facteurs liés à la création de mot de passe faibles....p. 2
3. La détection des tentatives de découverte de mots de passe....p. 3
4. La réponse aux tentatives de découverte de mots de passe....p. 3
5. Comment prévenir les tentatives de découverte de mots de passe....p. 3
    1. Les politiques de mots de passe et le « nudging »....p. 3
    2. Les gestionnaires de mots de passe....p. 5
    3. D'autres solutions envisageables....p. 6
6. Conclusion....p. 6
7. Références....p. 6
8. Annexe....p. 9

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Définition et ampleur

Malgré l'augmentation du recours aux données biométriques ou aux jetons de sécurité comme moyen d'authentification, le mot de passe reste le moyen le plus utilisé par la majorité des organisations (74%) pour valider l'identité des usagers[1, 2]. Sa popularité en fait une cible privilégiée des cybercriminels motivés et sophistiqués[3]. Les tentatives de découverte du mot de passe impliquent un processus dans lequel un criminel tente de deviner le mot de passe d'une victime pour accéder au compte de cette dernière[1]. L'attaque par force brute, qui implique d'essayer de manière systématique toutes les combinaisons d'un mot de passe jusqu'à l'obtention d'une correspondance, est une méthode souvent utilisée par les cybercriminels. L'attaque par force brute peut être laborieuse au fur et à mesure que s'accroissent la longueur et la complexité des mots de passe, par l'inclusion de majuscules, caractères spéciaux et de chiffres par exemple. Ainsi, le Tableau 1 (en annexe) montre comment l'ajout de quelques caractères augmente de considérablement le nombre des combinaisons possibles d'un mot de passe, particulièrement si le mot de passe contient des caractères minuscules et majuscules, des chiffres ainsi que des symboles.

Par conséquent, des outils automatisés ont été conçus pour lancer des attaques par force brute avec une vitesse sans précédent[5]. En fonction de la puissance des outils à sa disposition, un cybercriminel peut tester de quelques milliers à des millions de combinaisons seconde[5].

Les mots de passe faibles sont notamment vulnérables aux attaques par dictionnaire, un sous-ensemble d'attaques par force brute. Ce type d'attaque implique que le cyberdélinquant teste des mots de passe connus ainsi que toutes autres combinaisons de termes couramment utilisés au quotidien, dans l'espoir d'obtenir une correspondance[6]. Par exemple, dans leur étude, des chercheurs ont réussi à deviner le tiers d'un échantillon de 520 mots de passe en moins d'une minute grâce à cette méthode, et la moitié après 4 heures[7].

Ainsi, la robustesse du mot de passe de la victime joue un rôle important dans le temps requis pour qu'une attaque par force brute réussisse à compromettre des identités[4]. Le Tableau 2 (en annexe) montre le temps nécessaire à un système informatique pour découvrir un mot de passe (selon la complexité et la longueur de celui-ci) si 1 000 000 mots de passe sont traités par seconde.

La création d'un mot de passe robuste repose souvent sur l'utilisateur, et les études montrent de façon récurrente que les internautes optent couramment pour des mots de passe faibles[8, 9, 10, 11, 12]. Certaines études montrent notamment que la majorité des mots de passe utilisent des séries de caractères prévisibles pour former des noms communs, des marques populaires ou encore des dates de naissance[13]. D'ailleurs, le National Cyber Security Centre rapporte que la série de chiffres 123456 constitue toujours le mot de passe le plus populaire[14].

Ainsi, les organisations doivent inciter leurs employés et collaborateurs à choisir des mots de passe suffisamment robustes pour éviter leur découverte par des acteurs malintentionnés et la compromission subséquente des comptes. Cette fiche synthèse explique pourquoi les internautes choisissent des mots de passe faibles et offre par la suite des pistes d'intervention pertinentes. Des solutions envisageables en lien avec la détection et la réponse aux tentatives de découverte du mot de passe sont aussi présentées.

Les facteurs liés à la création de mots de passe faibles

Plusieurs études ont montré que les usagers savent concevoir des mots de passe robustes[15], mais qu'ils choisissent malgré tout des combinaisons vulnérables[16]. Ce phénomène s'explique par une perception inexacte des tentatives de découverte du mot de passe[15]. Par exemple, dans leur étude, un tiers des participants ont jugé qu'un mot de passe est sécuritaire s'il est capable de résister à une douzaine d'essais. De plus, les utilisateurs ne sont pas conscients de la popularité des mots de passe qu'ils utilisent. En effets, les utilisateurs peuvent faire l'expérience de la fatigue du mot de passe, c'est-à-dire la difficulté pour les utilisateurs à se remémorer les mots de passe au fur et à mesure qu'ils se créent des comptes sur l'Internet (une personne détient aujourd'hui 38 comptes en moyenne)[17, 18, 19]. Les utilisateurs diminuent cette surcharge cognitive en optant pour des mots de passe peu robustes[20]. D'autres études montrent que les internautes conservent leurs ressources mentales pour les plateformes traitant des données confidentielles (comme les sites bancaires)[16]. Une étude a cependant montré que cette stratégie expose l'ensemble des comptes détenus par un utilisateur à des attaques par dictionnaire parce que ses mots de passe partagent par inadvertance des similarités avec les mots de passe moins faibles[21].

En s'appuyant sur la théorie de la motivation à la protection (TMP), des chercheurs ont montré que les coûts cognitifs liés à la création d'un mot de passe robuste représentent un obstacle important[22]. Selon la TMP, les comportements sains sont le résultat de deux processus d'évaluation : les perceptions par rapport à la menace (la vulnérabilité, c'est-à-dire la probabilité d'être touché ; et la sévérité des préjudices attendus) et les solutions envisageables (l'efficacité de la réponse ; l'auto-efficacité, c'est-à-dire les compétences de la personne pour implanter adéquatement la solution ; et les coûts associés à la mise en œuvre des solutions)[23]. Des chercheurs argumentent qu'en plus des coûts cognitifs, une personne ne créera pas un mot de passe robuste si elle estime que cela ne la

protégera pas adéquatement contre la compromission de ses identifiants[22]. En revanche, les perceptions liées à la probabilité et la sévérité de la menace ne jouent pas un rôle important dans la création de mots de passe robustes, bien que les individus ne craignant pas la compromission de leur identité aient peu tendance à adopter des mots de passe sûrs.

La détection des tentatives de découverte du mot de passe

Étant donné que les attaques par force brute impliquent un nombre volumineux de combinaisons de mots de passe, une organisation doit évidemment rester à l'affût des tentatives infructueuses de connexion qui surviennent dans un court laps de temps[24]. Des échecs de connexion provenant de la même adresse IP représentent par ailleurs un fort indicateur d'une attaque par force brute[25]. De même, des tentatives répétées d'authentification provenant de multiples adresses IP pour un seul compte constituent un autre indice d'attaque par force brute plus sophistiquée. Enfin, une organisation peut toujours évaluer l'empreinte numérique habituelle (l'appareil utilisé, la position géographique, etc.) de la personne qui tente de s'authentifier et ainsi détecter toute anomalie[26]. D'autres auteurs suggèrent également de combiner les mots de passe avec la biométrie comportementale, notamment les dynamiques de frappe habituelles sur le clavier, en vue de détecter d'éventuelles anomalies[27].

La réponse aux tentatives de découverte du mot de passe

En guise de réponse à la découverte d'un mot de passe, certaines études montrent que l'authentification à facteurs multiples constitue une piste essentielle de résilience[28]. En effet, même si le mot de passe est compromis, le cybercriminel se retrouvera devant une seconde couche d'authentification avant de pouvoir obtenir l'accès non autorisé à un compte[29, 30, 31]. Toutefois, comme les procédures d'authentification supplémentaires empiètent sur la commodité d'usage[32], les organisations doivent adopter un modèle fondé sur les risques. Autrement dit, si une personne soumet un mot de passe et que son empreinte numérique ne correspond pas à celle établie à sa première utilisation de la plateforme de l'organisation, elle devra effectuer des procédures d'authentification supplémentaires[26]. Certaines études proposent également d'intégrer la biométrie comportementale (comme les mouvements de souris) pour détecter les tendances anormales et déclencher l'authentification multifacteur[33]. Les tests Captcha (« Completely Automated Public Turing Test to Tell Computers and People Apart ») sont également efficaces pour arrêter les attaques par force brute dans leur lancée[31, 34]. Ces tests demandent à un utilisateur d'accomplir une tâche supplémentaire (comme traduire une série déformée de caractères) avant de les authentifier avec succès en présumant que les robots ne sauraient les compléter[35]. Certaines études soulignent cependant que les tests Captcha sont peu conviviaux pour les personnes avec des handicaps et que des services dévoués à la résolution des Captchas rendent cette solution moins efficace qu'espéré[36]. Ils devraient ainsi suivre les principes de l'authentification basée sur les risques, comme le propose la solution reCaptcha Enterprise[37]. Celle-ci calcule un résultat de risque à partir du comportement de l'utilisateur qui fait une requête en vue de déterminer s'il doit y avoir un test et sa difficulté le cas échéant.

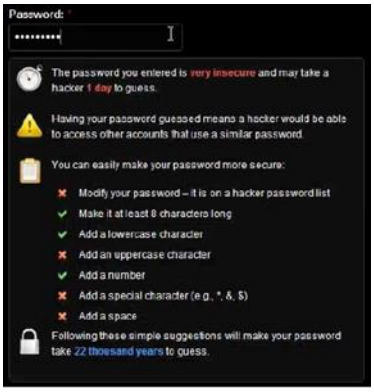
Comment prévenir les tentatives de découverte du mot de passe

Les politiques de mots de passe et le « nudging »

Comme il est difficile, voire impossible d'empêcher un fraudeur de se doter d'outils technologiques facilitant la découverte de mot de passe, les organisations doivent inciter les usagers à créer des mots de passe robustes qui empêcheront la compromission de leur compte. Une première piste envisageable concerne les politiques de mots de passe, c'est-à-dire les règlements liés à la création d'un mot de passe (par exemple, le fait de contenir au moins huit caractères, dont au moins un caractère spécial et au moins un chiffre, etc.)[38] Pourtant, les études montrent que les politiques à elles seules n'empêchent pas la création de mots de passe peu robustes[38, 39, 40]. Des chercheurs ont constaté que les individus renégocient les consignes pour créer un mot de passe qui se conforme certes aux normes, mais qui reste facile

à deviner[41]. Par exemple, des critères tels que l'emploi d'un minimum de 8 caractères, d'un chiffre et d'un caractère spécial permettent toujours l'utilisation de « Password!1 ». Ce phénomène concerne notamment les utilisateurs sur les plateformes mobiles en raison de l'inconvénient lié au clavier virtuel et à l'accès aux majuscules, chiffres et caractères spéciaux[42]. Afin de surmonter ce défi, le National Institute of Standards and Technology (NIST) recommande l'utilisation des listes noires, sur lesquelles se retrouvent des mots de passe communs et prévisibles[43]. Cependant, d'autres chercheurs argumentent que les listes noires sont insuffisantes parce que les usagers peuvent toujours tenter d'apporter des modifications mineures à leurs mots de passe déjà peu robustes et ainsi contourner les listes noires[44]. Pour y remédier, les auteurs recommandent de mettre en place un mécanisme de rétroaction textuelle qui conseille aux usagers les éléments à inclure afin d'augmenter la robustesse de leur mot de passe.

Ce type de procédure fait référence à la notion de l'incitation douce ou du coup de pouce (*nudging* en anglais), autrement dit l'ensemble de techniques incitant délicatement une personne à l'adoption d'un comportement sécuritaire[45]. Certains chercheurs ayant examiné l'effet du *nudging* des barres indicatrices du degré de complexité d'un mot de passe montrent qu'elles encouragent effectivement la création de mots de passe robustes[46], mais seulement pour les comptes dits « importants », renvoyant au constat que les usagers réservent leurs ressources cognitives pour protéger les données qu'ils considèrent comme importantes[16]. D'autres études montrent en revanche que cette solution n'est efficace que si elle s'accompagne de messages d'avertissement dynamiques (voir la figure 1 en annexe pour une représentation visuelle)[47, 48, 49]. En effet, cette manière de procéder permet aux utilisateurs d'en apprendre plus sur la création d'un mot de passe robuste[47], et l'addition de conseils invite davantage les individus à se créer de meilleurs mots de passe[38].



Certaines études se sont également penchées sur les politiques d'expiration du mot de passe, c'est-à-dire les règlements qui obligent les internautes à changer leur mot de passe après chaque intervalle de temps prédéfini (30 jours, 90 jours, etc.), dans le but de réinitialiser le cycle d'une attaque à force brute potentiellement en cours[50, 51]. Autrement dit, le progrès réalisé par les tentatives de découverte du mot de passe est perdu à chaque fois que les mots de passe sont expirés et doivent être changés. Ces politiques amènent toutefois une charge cognitive additionnelle sur les individus et poussent ces derniers à adopter des mots de passe faibles[52]. Ces études laissent présager que les coûts des politiques d'expiration du mot de passe dépassent leurs bienfaits, bien que d'autres suggèrent qu'il soit possible de les améliorer grâce à l'incitation douce. Par exemple, le rappel de la date d'expiration du mot de passe sur la page de connexion, l'inclusion d'un lien permettant le changement, ainsi que l'offre de conseils sur l'adoption d'un mot de passe long et complexe encouragent la création de mots de passe robustes[45].

Toutefois, les requêtes de changement de mot de passe doivent être communiquées selon certaines conditions. En effet, la théorie des niveaux de représentation (*Construal Level Theory*) postule que les perceptions de faisabilité déterminent les actions d'un individu dans le présent[11]. Autrement dit, si l'utilisateur est obligé de changer son mot de passe à l'instant, il adoptera un mot de passe faible parce qu'il doute ses compétences de mémorisation (la convenance l'emporte sur la sécurité). En contrepartie, lorsque la personne sait qu'elle doit changer son mot de passe dans le futur,

elle focalise davantage son attention sur ce qui lui serait désirable – dans ce cas, avoir un mot de passe sécuritaire – que sur la faisabilité de la chose (la sécurité l'emporte sur la convenance). Il suffirait d'avertir à l'utilisateur que son mot de passe sera expiré à un délai prescrit et d'en choisir un autre d'ici là. Des chercheurs soulignent toutefois que l'échéance doit rester de courte durée. Avertir qu'un mot de passe expire le lendemain suscite de meilleurs mots de passe, mais les internautes semblent ignorer les échéances lointaines (comme trois semaines ou plus)[11].

Cela dit, malgré l'intention des politiques d'expiration du mot de passe de rendre plus coûteuses les tentatives de découverte du mot de passe, il serait plus avantageux de simplement encourager des mots de passe robustes pour prolonger suffisamment le temps de succès des tentatives de découverte du mot de passe[50, 51, 52]. Par exemple, le Tableau 2 indiquait qu'un mot de passe aléatoire avec 16 caractères incluant des caractères minuscules, majuscules, spéciaux et des chiffres prendrait 1,4 quintillion d'années à deviner pourvu qu'une attaque par force brute teste 1 million de mots de passe par seconde.

Les gestionnaires de mots de passe

Les gestionnaires de mots de passe ont été conçus pour surmonter les problèmes de mémorabilité tels que déjà soulignés dans ce texte. Plus spécifiquement, ces outils chiffrent, stockent et gèrent les mots de passe, le tout étant verrouillés à l'aide d'un mot de passe maître — le seul identifiant que l'usager doit mémoriser[53]. Les gestionnaires de mot de passe peuvent également générer des mots de passe robustes et les insérer automatiquement sur les pages de connexion, facilitant ainsi le processus d'authentification. Une étude montre effectivement que les gestionnaires de mot de passe créent des mots de passe sécuritaires[54]. Qu'ils représentent la solution ultime ou non à la gestion des mots de passe, certaines études soulignent que l'adoption des gestionnaires de mots de passe dépend des perceptions « sécurité-convenance » des utilisateurs à leur égard. Par exemple, les non-utilisateurs se méfient des gestionnaires de mots de passe et disent avoir peur qu'un pirate informatique ait accès à tous les mots de passe stockés s'il réussit à compromettre le gestionnaire[55]. Les utilisateurs estiment aussi avoir peu d'incitatifs à installer l'outil ou encore que son implantation exige trop d'efforts[55, 56]. Les utilisateurs de gestionnaires de mots de passe, quant à eux, privilégient plutôt sur les bienfaits ergonomiques tels que décrits au début de ce paragraphe. Tout de même, les utilisateurs font peu confiance aux gestionnaires de mots de passe pour protéger l'accès aux comptes qualifiés de plus confidentiels (bancaires et autres)[55]. De plus, les utilisateurs expriment leur inconfort envers les gestionnaires en ligne (mots de passe stockés sur un serveur tiers) et préfèrent ceux qui sont locaux (hébergés sur leur machine), et ce, même s'ils sont obligés de retranscrire manuellement les mots de passe sur les pages de connexion[57]. Bien que les études mettent en avant l'importance de la convenance pour les utilisateurs, il semblerait que les internautes sont méfiants vis-à-vis des gestionnaires de mots de passe, qu'ils soient utilisateurs ou non[58], et ce, malgré le fait que leur utilisation soit considérée comme une des meilleures pratiques de sécurité[59]. Fin de convaincre les sceptiques des qualités des gestionnaires de mots de passe, les organisations doivent vulgariser les processus technologiques mis en place par ces outils pour protéger les mots de passe stockés[55] et de les recommander un gestionnaire ergonomique[58]. Les usagers devront aussi être sensibilisés à créer un mot de passe maître robuste, mais facile à retenir.

Quant à la sensibilisation sur les mots, de passe, une étude montre une baisse de 30 % des mots de passe faibles après l'implantation d'un programme d'intervention et de formation à la création des mots de passe[60]. Des affiches, graphiques, ainsi que des animations ont été utilisées pour mieux vulgariser le contenu. D'autres chercheurs ont pour leur part conçu un programme de sensibilisation qui conscientise davantage le public-cible sur les cybermenaces auxquelles sont confrontés leurs mots de passe, de même que des conseils pour rendre ces derniers robustes, avec un accent sur les techniques mnémoniques, c'est-à-dire les mots de passe construits à partir de la première lettre de chaque mot d'une phrase personnelle[61]. Les chercheurs ont conclu que les participants créent par la suite de meilleurs mots de passe, mais que l'effet disparaît après six semaines et que l'intervention devrait donc s'effectuer

mensuellement. D'autres sources recommandent les phrases de passe parce qu'elles sont robustes, mais restent conviviales[62, 63].

D'autres solutions envisageables

Certaines sources, dont le National Institute of Standards and Technology (NIST), proposent de limiter les essais de mots de passe pour rendre plus coûteuses les attaques par force brute[5, 25, 43]. Il n'est toutefois pas conseillé de verrouiller un compte indéfiniment si la limite de tentatives de connexion est atteinte, car les pirates informatiques peuvent dans ce cas compromettre la dimension « disponibilité » de la cybersécurité en verrouillant un grand nombre d'usagers de leurs comptes respectifs [31][34]. Il se pourrait d'ailleurs qu'un usager légitime tente plusieurs combinaisons de mots de passe dans l'espoir de se remémorer son identifiant. Après un certain nombre de tentatives, l'organisation devrait plutôt imposer de brefs intervalles de temps entre les tentatives pour dissuader suffisamment les attaques automatisées sans toutefois compromettre l'ergonomie du système[31].

D'autres solutions techniques cherchent à réduire le phénomène de la « fatigue du mot de passe ». Par exemple, l'identification unique, ou Single Sign-On (SSO) permet à l'utilisateur de se connecter, par l'entremise d'un mot de passe à la solution SSO pour avoir accès à toutes les applications associées à celle-ci[64]. Il n'a donc besoin que de retenir un mot de passe complexe. Une autre solution émergente concerne l'authentification sans mot de passe : un utilisateur est amené à saisir un mot de passe à usage unique reçu par SMS ou courriel[65]. De même, il pourrait plutôt être invité à entrer une clé de sécurité pour s'authentifier avec succès : les participants dans d'une étude estiment que cette méthode d'authentification est plus ergonomique que les mots de passe, bien qu'ils aient peur de perdre la clé[66]. Enfin, la biométrie permet de s'authentifier grâce à une information inhérente à l'individu (sa voix, son empreinte digitale, son visage, etc.). Certaines études mettent cependant en lumière certains défis en lien avec son ergonomie. Par exemple, des personnes estiment que le délai de validation pour un FaceID est plus long que la saisie d'un mot de passe[67]. Les utilisateurs sont également inquiets quant à la protection des données biométriques, et les entreprises canadiennes doivent s'assurer d'obtenir le consentement de l'individu et prendre les mesures de sécurité nécessaires en vertu des lois sur la protection des données personnelles, comme la Loi sur la protection des renseignements personnels et les documents électroniques[68, 69].

Conclusion

En conclusion, les tentatives de découverte du mot de passe sont efficaces dans la mesure où la longueur et la complexité des mots de passe des utilisateurs laissent à désirer[8, 9, 10, 11, 12]. La création de mots de passe faibles s'explique bien par les méconnaissances liées à ses dangers ainsi que les coûts cognitifs par rapport à la conception d'un mot de passe robuste[15, 22]. Les entreprises doivent certes mettre en place des solutions technologiques pour prévenir, détecter et répondre aux tentatives de découverte du mot de passe, mais elles doivent notamment sensibiliser leurs parties prenantes à utiliser un gestionnaire de mots de passe et à se créer des mots de passe complexes, mais conviviaux, comme les mots de passe mnémoniques ou les phrases de passe[60, 61, 62, 63].

Références

1. Conrad, E., Misenar, S. et Feldman, J. (2016). Chapter 6 - Domain 5: Identity and Access Management (Controlling Access and Managing Identity). Dans E. Conrad, S. Misenar et J. Feldman (dir.), *CISSP Study Guide* (Third Edition).

2. Das, A., Bonneau, J., Caesar, M., Borisov, N. et Wang, X. (2014). The Tangled Web of Password Reuse. Communication présentée au Proceedings 2014 Network and Distributed System Security Symposium.

3. Medina, M., Serna, J., Sfakianakis, A., Aguilá, J., Fernández, L. Á. et European Network and Information Security Agency. (2013). *EID authentication methods in e-Finance and e-Payment services: current practices and recommendations*, December 2013.

4. Martin, S. et Tokutomi, M. (2012). Password cracking.

5. Kaspersky. (2020). What's a Brute Force Attack?

6. Raza, M., Iqbal, M., Sharif, M. et Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, *19*(4), 439-444.

7. Cazier, J. A. et Medlin, B. D. (2006). Password security: an empirical investigation into e-commerce passwords and their crack times. *Information Systems Security*, *15*(6), 45-55.

8. Bonneau, J. (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. Communication présentée au *2012 IEEE Symposium on Security and Privacy*.

[9] Florencio, D. et Herley, C. (2007). A large-scale study of web password habits. Communication présentée au Proceedings of the 16th International Conference on World Wide Web.

[10] Gaw, S. et Felten, E. W. (2006). Password management strategies for online accounts. Communication présentée au *Proceedings of the Second Symposium on Usable Privacy and Security*.

[11] Tam, L., Glassman, M. et Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244.

[12] Weber, J., Guster, D. et Safonov, P. (2008). A developmental perspective on weak passwords and password security. *Journal of Information Technology Management*, *19*(3), 1-8.

[13] Zviran, M. et Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161-185.

[14] NCSC. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security.

[15] Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N. et Cranor, L. F. (2016). Do Users' Perceptions of Password Security Match Reality? *Communication présentée au Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.

[16] von Zezschwitz, E., De Luca, A. et Hussmann, H. (2013). Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson et M. Winckler (dir.), Communication présentée au Human-Computer Interaction.

[17] Florencio, D., Herley, C. et van Oorschot, P. C. (2014). Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. Communication présentée au 23rd USENIX Security Symposium.

[18] LastPass. (2020). Psychology of passwords: The online behavior that's putting you at risk.

[19] Sanchez, H. et Murray, J. (2016). Putting Your Passwords on Self-destruct Mode: Beating Password Fatigue. *Communication présentée au Twelfth Symposium on Usable Privacy and Security*.

[20] Adams, A. et Sasse, A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 41-46.

[21] Haque, S. M., Wright, M. et Scielzo, S. (2013). A study of user password strategy for multiple accounts. Communication présentée au *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY 2013)*.

[22] Zhang, L. et McDowell, W. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, *8*, 180-197.

[23] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Dans J. Cacioppo et R. Petty (dir.), Social psychophysiology.

[24] Shezaf, O. (2017). Brute Force: Anatomy of an Attack. Inside Out Security.

[25] Gross, G. (2016). Brute Force Attack Mitigation: Methods & Best Practices.

[26] Alaca, F. et van Oorschot, P. C. (2016). Device fingerprinting for augmenting web authentication: classification and analysis of methods. Communication présentée au Proceedings of the 32nd Annual Conference on Computer Security Applications.

[27] Pahuja, G. et Nagabhushan, T. N. (2015). Biometric authentication identification through behavioral biometrics: a survey. Communication présentée au 2015 International Conference on Cognitive Computing and Information Processing.

[28] Aldwairi, M. et Aldhanhani, S. (2017). Multi-Factor Authentication System. Communication présentée au 2017 International Conference on Research and Innovation in Computer Engineering and Computer Sciences.

[29] Cisco. (2018). Multi-factor Authentication and Password Security.

[30] OneLogin. (s. d.). Understand How SSO and MFA Improve Security.

[31] Tucakov, D. (2018). How To Prevent Brute Force Attacks With 8 Easy Tactics.

[32] Holmes, M. et Ophoff, J. (2019). Online security behaviour: factors influencing intention to adopt two-factor authentication. *Communication présentée au ICCWS 2019 14th International Conference on Cyber Warfare and Security*.

[33] Traore, I., Woungang, I., Obaidat, M. S., Nakkabi, Y. et Lai, I. (2014). Online risk-based authentication using behavioral biometrics. *Multimedia Tools and Applications*, *71*(2), 575-605.

[34] Waller, D. (2020). Blocking Brute Force Attacks Control | OWASP Foundation.

[35] Abdalla, K. H. et Kaya, M. (2016). An evaluation of different types of Captcha: Effectiveness, user-friendliness, and limitations. International Journal of Scientific Research in Information Systems and Engineering, 2(3), 12-19.

[36] Priyanka, Kaur, H. et Kushwaha, D. K. (2013). Reviewing effectiveness of CAPTCHA. *International Journal of Computer Trends and Technology*, *4*(5), 1306-1311.

[37] Google. (2020). reCAPTCHA Enterprise | reCAPTCHA Enterprise.

[38] Yıldırım, M. et Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741-759.

[39] Campbell, J., Ma, W. et Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379-388.

[40] Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., … Ur, B. (2013). Measuring password guessability for an entire university. Communication présentée au *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*.

[41] Weir, M., Aggarwal, S., Collins, M. et Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. Communication présentée au *Proceedings of the 17th ACM Conference on Computer and Communications Security*.

[42] Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., … Mazurek, M. L. (2016). Usability and Security of Text Passwords on Mobile Devices. Communication présentée au *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.

[43] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E. et Richer, J. P. (2017). Digital identity guidelines: authentication and lifestyle management (no NIST SP 800-63B) (p. NIST SP 800-63-3). National Institute of Standards and Technology.

[44] Habib, H., Colnago, J., Melicher, W., Ur, B., Segreti, S., Bauer, L., … Cranor, L. (2017). Password Creation in the Presence of Blacklists. Communication présentée au *Proceedings 2017 Workshop on Usable Security, San Diego, CA*.

[45] Renaud, K. et Zimmermann, V. (2019). Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, *3*(2), 228-258.

[46] Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. et Cranor, L. F. (2012). How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. *Communication présentée au 21st Security Symposium*.

[47] Khern-am-nuai, W., Yang, W. et Li, N. (2017). Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment. *Communication présentée au Hawaii International Conference on System Sciences 2017*.

[48] Shay, R., Bauer, L., Christin, N., Cranor, L. F., Forget, A., Komanduri, S., … Ur, B. (2015). A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior. Communication présentée au *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*.

[49]. Vance, A., Eargle, D., Ouimet, K. et Straub, D. (2013). Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. Communication présentée au 2013 46th Hawaii International Conference on System Sciences.

[50]. Chiasson, S. et van Oorschot, P. C. (2015). Quantifying the security advantage of password expiration policies. Designs, Codes and Cryptography, 77(2-3), 401-408.

[51]. Spitzner, L. (2017). Time for Password Expiration to Die.

[52]. Inglesant, P. G. et Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. Communication présentée au Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10.

[53]. Educause. (2019). Password managers.

[54]. Lyastani, S. G., Schilling, M., Fahl, S., Backes, M. et Bugiel, S. (2018). Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. Communication présentée au 27th USENIX Security Symposium.

[55]. Fagan, M., Albayram, Y., Khan, M. M. H. et Buck, R. (2017). An investigation into users' considerations towards using password managers. Human-Centric Computing and Information Sciences, 7(1), 1-20.

[56]. Aurigemma, S., Mattson, T. et Leonard, L. (2019). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? Communication présentée au Proceedings of the 50th Hawaii International Conference on System Sciences.

[57]. Karole, A., Saxena, N. et Christin, N. (2011). A Comparative Usability Evaluation of Traditional Password Managers. K.-H. Rhee et D. Nyang (dir.), Communication présentée au Information Security and Cryptology - ICISC 2010.

[58]. Chiasson, S., van Oorschot, P. C. et Biddle, R. (2006). A Usability Study and Critique of Two Password Managers. Communication présentée au Security '06: 15th USENIX Security Symposium.

[59]. NIST (2020). NIST Special Publication 800-63: Digital Identity Guidelines—Frequently Asked Questions.

[60]. Eminağaoğlu, M., Uçar, E. et Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. Information Security Technical Report, 14(4), 223-229.

[61]. Mwagwabi, F., McGill, T. et Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. Communications of the Association for Information Systems, 42(1), 147-182.

[62]. Centre canadien pour la cybersécurité (2019). Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032).

[63]. Keith, M., Shao, B. et Steinbart, P. J. (2009). A behavioral analysis of passphrase design and effectiveness. Journal of the Association for Information Systems, 10(2), 63-89.

[64]. Auth0. (2020b). Single Sign-On.

[65]. Auth0. (2020a). Passwordless Connections.

[66]. Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M. et Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *Communication présentée au 2020 IEEE Symposium on Security and Privacy*.

[67]. De Luca, A., Hang, A., von Zezschwitz, E. et Hussmann, H. (2015). I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. *Communication présentée au The 33rd Annual ACM Conference*.

[68]. Wolf, F., Kuber, R. et Aviv, A. J. (2019). « Pretty Close to a Must-Have »: Balancing Usability Desire and Security Concern in Biometric Adoption. *Communication présentée au The 2019 CHI Conference*.

[69]. LPRPDE. (2016). Lignes directrices en matière d'identification et d'authentification.

Annexe

Nombre de caractères	Minuscules	Minuscules/ majuscules	Minuscules/ majuscules/ chiffres	Minuscules/ majuscules/ chiffres/ symboles
1	26	52	62	95
2	676	2704	3844	9025
4	456 976	7 311 616	14 766 336	81 450 625
8	$2.09x10^{11}$	$5.35x10^{13}$	$2.18x10^{14}$	$6.63x10^{15}$
16	$4.36x10^{22}$	$2.86x10^{27}$	$4.77x10^{28}$	$4.40x10^{31}$

Tableau 1 : Nombre de combinaisons possibles d'un mot de passe selon le nombre de caractères

Nombre de caractères	Minuscules	Minuscules/ Majuscules	Minuscules/ Majuscules/ Chiffres	Minuscules/ Majuscules/ Chiffres/ Symboles
1	26 microsecondes	52 microsecondes	62 microsecondes	95 microsecondes
2	676 microsecondes	2.704 millisecondes	3.844 millisecondes	9.025 millisecondes
4	≈ .5 secondes	≈ 7 secondes	≈ 14 secondes	≈ 81 secondes
8	≈ 2.42 jours	≈ 1.7 années	≈ 6.9 années	≈ 210 années
16	≈ 1.38 milliards d'années	≈ 91 trillions d'années	≈ 1.5 quadrillion d'années	≈ 1.4 quintillion d'années

Tableau 2 : Temps nécessaire pour découvrir un mot de passe par force brute selon le nombre de caractères