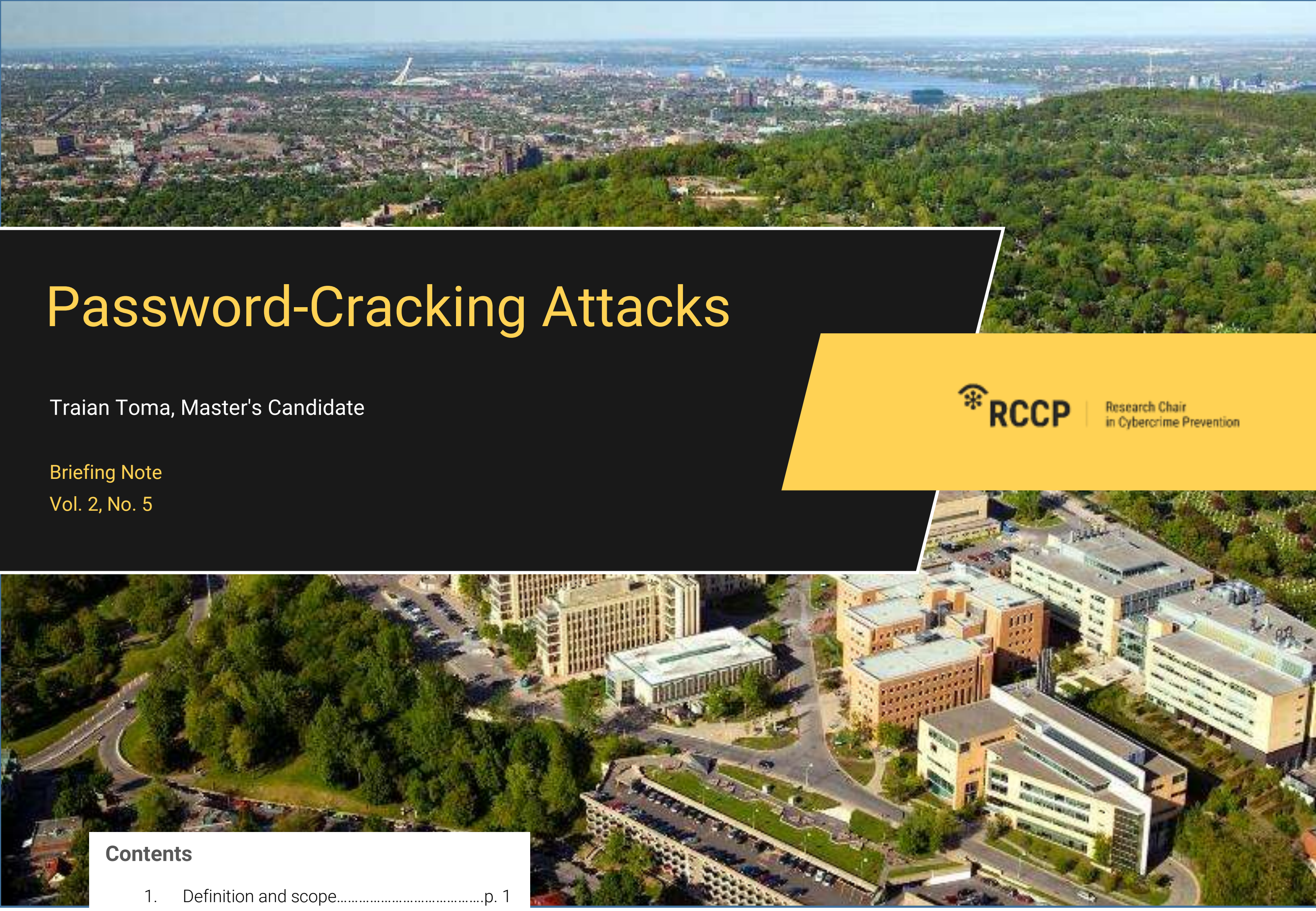


Password-Cracking Attacks

Traian Toma, Master's Candidate

Briefing Note
Vol. 2, No. 5

RCCP | Research Chair in Cybercrime Prevention

Contents

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Definition and scope

Despite the increased use of biometrics or security tokens as an authentication method, passwords are still the method most commonly used by most organizations (74%) to validate user identity.[1, 2] Their popularity makes them a prime target for motivated and sophisticated cybercriminals.[3] Password-cracking attacks involve a process in which a criminal attempts to guess a person's password to gain access to their account.[1] The brute-force attack, which involves systematically trying all combinations of a password until a match is obtained, is a method often used by cybercriminals. Brute-force attacks can be time-consuming when passwords are made longer and more complex, for example, by including uppercase letters, special characters and numbers. Table 1 (in the Appendix) shows how adding a few characters significantly increases the number of possible combinations of a password, particularly if the password contains lowercase and uppercase letters, numbers and symbols.

As a result, automated tools have been designed to launch brute-force attacks with unprecedented speed.[5] Depending on the power of the tools at their disposal, cybercriminals can test a few thousand to millions of combinations per second.[5]

Weak passwords are particularly vulnerable to dictionary attacks, a subset of brute-force attacks. In this type of attack, the cybercriminal tests known passwords and any other combination of terms commonly used on a daily basis in the hope of obtaining a match.[6] For example, in their study, researchers were able to guess a third of a sample of 520 passwords in less than a minute using this method and half within four hours.[7]

Thus, the strength of a person's password plays an important role in the time required for a brute-force attack to compromise login credentials successfully.[4] Table 2 (in the Appendix) shows the time it takes for a computer system to crack a password (depending on its complexity and length) if one million passwords are processed per second.

Creating a strong password often depends on the user. Studies repeatedly show that internet users often create weak passwords.[8, 9, 10, 11, 12] Some studies show that most passwords use predictable character sets to form common names, popular brands or birth dates.[13] In fact, the National Cyber Security Centre reports that 123456 is still the most popular password.[14]

Consequently, organizations must encourage their employees and collaborators to choose strong passwords to prevent ill-intentioned individuals from guessing them and then hacking their accounts. This briefing note explains why internet users choose weak passwords and then provides appropriate solutions for the problem. Possible solutions for detecting and dealing with password-cracking attacks are also presented.

Weak password creation factors

Several studies have shown that users know how to make strong passwords[15] but still choose vulnerable combinations.[16] This is due to an inaccurate perception of password-cracking attacks.[15] For example, in 1 study, a third of participants felt that a password is safe if it can withstand a dozen attempts. In addition, users aren't aware of the popularity of the passwords they use. Users can experience password fatigue or difficulty remembering passwords as they create accounts on the internet (the average number of accounts per person is now 38).[17, 18, 19] Users reduce this cognitive overload by choosing weak passwords.[20] Other studies show that internet users save their brainpower for platforms dealing with confidential data (such as banking sites). However, one study has shown that this strategy exposes all of a user's accounts to dictionary attacks because their passwords inadvertently share similarities with stronger passwords.[21]

Using Protection Motivation Theory (PMT), researchers have shown that the cognitive cost of creating a strong password is a significant barrier.[22] According to PMT, healthy behaviours are the result of two assessment processes: perception of a threat (including the perceived severity of the threat and perceived vulnerability to it) and possible solutions (referred to as response efficacy and self-efficacy; in other words, the person's ability to effectively implement the solution and the costs associated with that).[23] Researchers argue that, in addition to the cognitive cost, people won't create a strong password if they believe it won't effectively protect them against their login credentials being compromised.[22] Conversely, perceptions of the likelihood and severity of the threat do not play a significant role in creating strong passwords, although individuals who aren't afraid of their login credentials being compromised are unlikely to create secure passwords.

Detecting password-cracking attacks

Since brute-force attacks involve a large number of password combinations, organizations must obviously keep an eye out for unsuccessful login attempts occurring in a short period of time.[24] Login failures from the same IP address are also a strong indicator of a brute-force attack.[25] Similarly, repeated authentication attempts from multiple IP addresses for a single account are another sign of a more sophisticated brute-force attack. Lastly, an organization can always assess the customary digital footprint (device used, geographic location, etc.) of the person attempting to authenticate, and thus detect any anomalies.[26] Other authors suggest combining passwords with behavioural biometrics, including customary keystroke dynamics to detect possible anomalies.[27]

Dealing with password-cracking attacks

Some studies show that multi-factor authentication is the best way to make passwords attack-resistant.[28] Even if the password is compromised, the cybercriminal will have to get through a second authentication layer before gaining unauthorized access to an account.[29, 30, 31] However, since additional authentication procedures can be an inconvenience for users,[32] organizations must adopt a risk-based model. In other words, if a person submits a password and their digital footprint does not match the one established when they first used the organization's platform, they must complete additional authentication steps.[26]

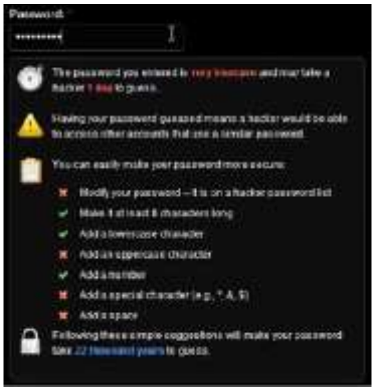
Some studies also suggest integrating behavioural biometrics (such as mouse movements) to detect abnormal trends and trigger multi-factor authentication.[33] CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) tests effectively combat brute-force attacks.[31, 34] These tests require users to complete an additional task (such as decrypting a distorted series of characters) before they can be successfully authenticated, based on the assumption that robots can't decrypt them.[35] However, some studies show that CAPTCHA tests are not user-friendly for people with disabilities and that dedicated CAPTCHA resolution services make this solution less effective than hoped.[36] reCAPTCHA Enterprise suggests following the principles of risk-based authentication.[37] This involves calculating a risk score based on the behaviour of the user making a query to determine whether a test is necessary and, if so, how difficult it should be.

Preventing password-cracking attacks

Password policies and "nudging"

Because it's difficult, if not impossible, to prevent a fraudster from acquiring password-cracking technology, organizations must encourage users to create strong passwords to prevent their accounts from being compromised. A possible initial solution is password policies, that is, rules for creating passwords (for example, must contain at least eight characters, at least one special character and at least one number, etc.).[38] Yet, studies show that policies alone do not prevent the creation of weak passwords.[38, 39, 40] Researchers have found that individuals renegotiate instructions to create a password that meets standards but is still easy to guess.[41] For example, criteria such as the use of a minimum of eight characters, a number and a special character still allow the use of "Password!1." This is particularly true of users on mobile platforms who are inconvenienced by the virtual keyboard and have trouble finding capital letters, numbers and special characters.[42] To overcome this challenge, the National Institute of Standards and Technology (NIST) recommends using blocklists, which contain commonly used or compromised passwords.[43] However, other researchers argue that blocklists are insufficient because users can still attempt to make minor changes to their already weak passwords and bypass blocklists.[44] In response, the authors recommend implementing a text feedback mechanism that tells users how to make their passwords stronger.

This type of procedure refers to the concept of gentle inducement or "nudging," or techniques that delicately induce a person to adopt safe behaviour.[45] Some researchers who have studied the nudging effect of visual bars indicating the degree of complexity of a password show that they do encourage the creation of strong passwords,[46] but only for so-called "important" accounts. This result corroborates the finding that users save their brainpower to protect data they consider important.[16] However, other studies show that this solution is only effective if accompanied by dynamic warning messages (see Figure 1 in the Appendix for a visual representation).[47, 48, 49] This allows users to learn more about creating a strong password,[47] and including tips encourages people to create better passwords.[3]



Password:

••••••••••

The password you entered is very insecure and may take a hacker 1 day to guess.

Having your password guessed means a hacker would be able to access other accounts that use a similar password.

You can easily make your password more secure:

- ✗ Modify your password—it is on a hacker password list
- ✓ Make it at least 8 characters long
- ✓ Add a lowercase character
- ✗ Add an uppercase character
- ✓ Add a number
- ✗ Add a special character (e.g., *, &, $)
- ✗ Add a space

Following these simple suggestions will make your password take 22 thousand years to guess.

Some studies have also looked at password expiration policies, in other words, rules requiring users to change their password after a given time interval (every 30 days, 90 days, etc.), in order to reset the cycle of a potentially active brute-force attack.[50, 51] In other words, the progress made in password-cracking attacks is lost every time the password expires and is changed. However, these policies place an additional cognitive burden on individuals and push them to adopt weak passwords.[52] These studies suggest that the costs of password expiration policies outweigh their benefits, although others suggest that such policies can be improved through soft incentives. For example, putting a reminder of the password expiry date on the login page, including a link to change the password, and providing guidance on how to create a long and complex password encourages the creation of strong passwords.[45]

However, password change requests must be sent under certain conditions. The Construal Level Theory postulates that perceptions of feasibility determine an individual's actions in the present.[11] In other words, if users are forced to change their password right away, they will create a weak one because they doubt their memory skills (convenience trumps security). Conversely, when they know they have to change their password in the future, they focus more on what is desirable—in this case, having a secure password—than on what is feasible (security trumps convenience). The user simply needs to be notified that their password will expire within a certain period of time and instructed to create a new one before that time is up. However, researchers stress that the time frame must still be short. Warning that a password will expire the following day results in better passwords, but internet users seem to ignore far-off deadlines (such as three weeks from today).[11]

That said, despite the intent of password expiration policies to make password-cracking attacks more costly, it would be better to simply encourage strong passwords to extend the time it takes for a password-cracking attack to succeed.[50, 51, 52.] For example, Table 2 indicates that a 16-character random password with lowercase and uppercase letters, special characters and numbers would take 1.4 quintillion years to guess if a brute-force attack tests one million passwords per second.

Password managers

Password managers have been designed to solve the problem mentioned above of users not remembering their passwords. More specifically, these tools encrypt, store and manage passwords, all of which are locked using a master password—the only thing the user needs to memorize.[53] Password managers can also generate strong passwords and automatically insert them in login pages, facilitating the authentication process. Research shows that password managers create secure passwords.[54] According to some studies, whether or not password managers are the ultimate password management solution, their adoption depends on users' perceptions of the "security-convenience tradeoff." For example, non-users are wary of password managers and say they're afraid that a hacker will have access to all stored passwords if they succeed in compromising the password manager.[55] Users also felt that there was little incentive to install the tool or that using it required too much effort.[55, 56] Users of password managers prefer the above-mentioned user-friendly benefits. However, they have little confidence in password managers to protect access to more confidential accounts (banking and others).[55] They also say they're not comfortable with online managers (passwords stored on a third-party server) and prefer those that are local (hosted on their machine), even though they're required to enter passwords on login pages manually.[57] Although studies highlight the importance of user convenience, it appears that internet users are distrustful of password managers, whether they use them or not,[58] even though using them is considered one of the best security practices.[59] To persuade skeptics of the benefits of password managers, organizations need to simplify the technological processes these tools use to protect stored passwords and recommend a more user-friendly password manager.[58] Users must also be told how to create a strong yet easy-to-remember master password.

As for password awareness, a study shows that weak passwords decreased by 30% after a password creation and training program was implemented.[60] Educational posters, animations and e-messages were used to explain the content. Other researchers have developed an awareness program to increase target audience awareness of the cyber threats to their passwords, including advice on how to make their passwords stronger through the mnemonic technique of using the first letter of each word in a sentence or familiar phrase to create a password.[61] The researchers concluded that the participants subsequently created better passwords but that the effect wore off after six weeks, and the program should therefore be rolled out monthly. Other sources recommend the use of passphrases because they are strong but still user-friendly.[62, 63]

Other possible solutions

Some sources, including the National Institute of Standards and Technology (NIST), propose that password testing be limited to make brute-force attacks more costly.[5, 25, 43] However, it's not advisable to lock an account indefinitely if the maximum number of login attempts has been reached, because then hackers can compromise cybersecurity access by locking a large number of users out of their accounts.[31, 34] Legitimate users may try multiple password combinations in an attempt to recall their login credentials. After several attempts, the organization should instead impose short intervals between attempts to sufficiently deter automated attacks without compromising system usability.[31]

Other technical solutions seek to reduce "password fatigue." For example, single sign-on (SSO) allows users to enter a password to log into the SSO session and user authentication service to access all SSO applications.[64] All they need to remember is one complex password. Another emerging solution is password-free authentication, whereby a user enters a 1-time password received by SMS or email.[65] Users can also be asked to enter a security key to authenticate themselves. Participants in a study believe that this authentication method is more user-friendly than passwords, although they're afraid of losing the key.[66] Lastly, biometrics can be used to authenticate individuals using information that is specific to them (voice, fingerprint, face, etc.). However, some studies highlight issues with the user-friendliness of this method. For example, some people believe that Face ID takes longer than entering a password.[67] Users are also concerned about the protection of biometric data, and Canadian companies must obtain users' consent and take the security measures required under personal data protection legislation, such as the *Personal Information Protection and Electronic Documents Act*.[68, 69]

Conclusion

In conclusion, password-cracking attacks are effective insofar as the length and complexity of user passwords are up to the task.[8, 9, 10, 11, 12] The creation of weak passwords can be explained by a lack of knowledge of the hazards and the cognitive cost of creating a strong password.[15, 22] Companies must certainly implement technology-based solutions to prevent, detect and deal with password-cracking attacks, but they also need to make their stakeholders aware of password managers and how to create complex but user-friendly passwords, such as mnemonic passwords or passphrases.[60, 61, 62, 63]

References

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

[2] Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. (2014). The Tangled Web of Password Reuse. Paper presented atPaper presented at the 2014 Network and Distributed System Security Symposium.

[3] Medina, M., Serna, J., Sfakianakis, A., Aguilá, J., Fernández, L. Á. and 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. and Tokutomi, M. (2012). Password cracking.

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

[6] Raza, M., Iqbal, M., Sharif, M. and 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. and 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. Paper presented atPaper presented at the 2012 IEEE Symposium on Security and Privacy.

[9] Florencio, D. and Herley, C. (2007). A large-scale study of web password habits. Paper presented atPaper presented at the 16th International World Wide Web Conference.

[10] Gaw, S. and Felten, E. W. (2006). Password management strategies for online accounts. Paper presented atPaper presented at the Second Symposium on Usable Privacy and Security.

[11] Tam, L., Glassman, M. and 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. and Safonov, P. (2008). A developmental perspective on weak passwords and password security. *Journal of Information Technology Management*, *19*(3), 1–8.

[13] Zviran, M. and 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. and Cranor, L. F. (2016). Do Users' Perceptions of Password Security Match Reality? *Paper presented at*Paper presented at the 2016 CHI Conference on Human Factors in Computing Systems.

[16] von Zezschwitz, E., De Luca, A. and Hussmann, H. (2013). Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson and M. Winckler (eds.), Paper presented atPaper presented at Human-Computer Interaction.

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

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

[19] Sanchez, H. and Murray, J. (2016). Putting Your Passwords on Self-destruct Mode: Beating Password Fatigue. *Paper presented at*Paper presented at the Twelfth Symposium on Usable Privacy and Security.

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

[21] Haque, S. M., Wright, M. and Scielzo, S. (2013). A study of user password strategy for multiple accounts. Paper presented at the Third ACM Conference on Data and Application Security and Privacy (CODASPY 2013).

[22] Zhang, L. and 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. In J. Cacioppo et R. Petty (eds.), 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. Paper presented at Proceedings of the 32nd Annual Conference on Computer Security Applications.

[27] Pahuja, G. and Nagabhushan, T. N. (2015). Biometric authentication identification through behavioral biometrics: a survey. Paper presented at the 2015 International Conference on Cognitive Computing and Information Processing.

[28] Aldwairi, M. and Aldhanhani, S. (2017). Multi-Factor Authentication System. Paper presented at the 2017 International Conference on Research and Innovation in Computer Engineering and Computer Sciences.

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

[30] OneLogin. (n.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. and Ophoff, J. (2019). Online security behaviour: factors influencing intention to adopt two-factor authentication. Paper presented at the ICCWS 2019 14th International Conference on Cyber Warfare and Security.

[33] Traore, I., Woungang, I., Obaidat, M. S., Nakkabi, Y. and 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. and 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. and 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. and 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. and 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.

Paper presented at the 2013 ACM SIGSAC Conference on Computer & Communications Security.

[41] Weir, M., Aggarwal, S., Collins, M. and Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. Paper presented at 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. Paper presented at 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. and 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. Paper presented at the 2017 Workshop on Usable Security, San Diego, CA.

[45] Renaud, K. and 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. and Cranor, L. F. (2012). How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. Paper presented at the 21st Security Symposium.

[47] Khern-am-nuai, W., Yang, W. and Li, N. (2017). Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment. Paper presented at the 2017 Hawaii International Conference on System Sciences.

[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. Paper presented at the 33rd Annual ACM Conference on Human Factors in Computing Systems.

[49]. Vance, A., Eargle, D., Ouimet, K. and Straub, D. (2013). Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. Paper presented at the 2013 Hawaii International Conference on System Sciences.

[50]. Chiasson, S. and 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. and Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. Paper presented at 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. and Bugiel, S. (2018). Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. Paper presented at the 27th USENIX Security Symposium.

[55]. Fagan, M., Albayram, Y., Khan, M. M. H. and 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. and Leonard, L. (2019). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? Paper presented at the 50th Hawaii International Conference on System Sciences.

[57]. Karole, A., Saxena, N. and Christin, N. (2011). A Comparative Usability Evaluation of Traditional Password Managers. K.-H. Rhee and D. Nyang (eds.), Paper presented at Information Security and Cryptology - ICISC 2010.

[58]. Chiasson, S., van Oorschot, P. C. and Biddle, R. (2006). A Usability Study and Critique of Two Password Managers. Paper presented at 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. and 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. and 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] Canadian Centre for Cyber Security (2019). Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032).

[63] Keith, M., Shao, B. and 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. and Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. Paper presented at the 2020 IEEE Symposium on Security and Privacy.

[67] De Luca, A., Hang, A., von Zezschwitz, E. and Hussmann, H. (2015). I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. Paper presented at the 33rd Annual ACM Conference.

[68] Wolf, F., Kuber, R. and Aviv, A. J. (2019). "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. Paper presented at the 2019 CHI Conference.

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

Appendix

Number of Characters	Lowercase	Lowercase/ Uppercase	Lowercase/ Uppercase/ Numbers	Lowercase/ Uppercase/ Numbers/ Symbols
1	26	52	62	95
2	676	2,704	3,844	9,025
4	456,976	7,311,616	14,766,336	81,450,625
8	2.09 x 10^{11}	5.35 x 10^{13}	2.18 x 10^{14}	6.63 x 10^{15}
16	4.36 x 10^{22}	2.86 x 10^{27}	4.77 x 10^{28}	4.40 x 10^{31}

Table 1: Number of possible combinations of a password, depending on the number of characters

Number of Characters	Lowercase	Lowercase/ Uppercase	Lowercase/ Uppercase/ Figures	Lowercase/ Uppercase/ Numbers/ Symbols
1	26 microseconds	52 microseconds	62 microseconds	95 microseconds
2	676 microseconds	2,704 milliseconds	3,844 milliseconds	9,025 milliseconds
4	≈ .5 seconds	≈ 7 seconds	≈ 14 seconds	≈ 81 seconds
8	≈ 2.42 days	≈ 1.7 years	≈ 6.9 years	≈ 210 years
16	≈ 1.38 billion years	≈ 91 trillion years	≈ 1.5 quadrillion years	≈ 1.4 quintillion years

Table 2: Time required for a brute-force attack to discover one password, broken down by number of characters