Benefits - supplementary material

Hazel Murray

December 2021

This document contains the rationale for how the security benefits were assigned to each advice statement.

1 User advice

1.1 Back up password options

Email up-to-date and secure. Email is used for password reset links and often as the method that a generated password is passed to users. Therefore having a secure email account can help against eavesdropping of passwords by attackers. It can also prevent unauthorized binding of a new password to a users' account through the form of an emailed password reset. Having an up-to-date and secure email system with a working spam/malware filter can help to protect against phishing and pharming attacks and compromise of an endpoint due to malware.

Do not store hints If hints were stolen then these hints could be used to facilitate online or offline guessing or to aid a social engineering attack.

1.2 Composition

Enforce restrictions on characters Researchers have shown that having complex password composition rules can make the resulting passwords more difficult to guess [1]. Though simply allowing only long (greater than 16 characters) passwords has a similar effect on guessability and may not cause as much hardship for users [1]. Having very stringent composition rules does have the effect of limiting the search space an attacker needs to look through. For example, a brute force exhaustive attacker has to search more possibilities for a password which can be made up of any type of 8 characters, than for an 8 characters password which has to have two numbers, two uppercase letters, two lower case letters and two symbols. But this only takes effect if the unconstrained user actually chooses from all 95 possible character options.

1.3 Keep your account safe

Check web pages for TLS This task helps users verify that communications to this webpage will be transmitted securely with encryption. However, it only has limited effectiveness as a strategy against phishing. In 2018, 49.4% of phishing sites were using SSL/TLS [2].

Manually type URLs Manually typing URLs can save a user from a Phishing attack as the user should recognize that the URL is not linking to the correct website. However, manually typing URLs makes a user vulnerable to typo-squatting/URL hijacking [3] e.g., `www.goggle.com`. A user is sent to the site with the similar URL which masquerades as the website of the user's intended destination. The site can then ask the user to enter their login details and store them to use on the real site. Thus the user's password is duplicated.

Keep software updated By keeping software updated a user gains protection against vulnerabilities as soon as the patch is released. This can save a user from eavesdropping, side channel and endpoint compromise.

Log out of public computers If a user does not log out of a public computer then the only protection a user has is the moral compass of the next person person who uses that computer. In this way a user's account can already be thought of as in a state of compromise. It is not obvious which of the 11 categories this opportunist attack comes under. We will somewhat arbitrarily place it under Eavesdropping.

Password protect your phone If a phone is password protected then the probability of endpoint compromise is lower.

1.4 Length

Minimum password length Inhibits brute force guessing as there are no passwords to guess with a very small number of characters, which are sometimes favoured by both users and guessers.

Enforce maximum length (<40) Requiring that passwords are less than a certain number of characters makes them easier for an eavesdropper to record them as they are less likely to cross packet boundaries. It also makes online and offline guessing easier as the attacker now need only guess passwords within the given range.

1.5 Password managers

Use a password manager The security benefits of a password manager will depend heavily on both how it is utilized by the user and also on the capabilities

on of the specific software that users are using. For this reason all benefits are dependent on the implementation.

A password manager greatly reduce the users' memory load and by extension then a user can use as long, random and complex of a password as they wish. Thus this act will increase security. A password manager does mean that the user is relying on an external agent to store their passwords and therefore if this agent is compromised or if the users password for this single account is compromised then the passwords of all the users' accounts are compromised. Therefore we consider this to be a new way in which the users' passwords can be duplicated.

Password managers which automatically fill in the users' credentials with no user interaction do have some corner case vulnerabilities [4]. Though this same paper shows that a password manager can provide more security that the normal manual typing of the password. For example, password managers can be effective against phishing and pharming attacks.

Create long random passwords This piece of advice was given in the context of a password manager. "Configure your password manager to create 30–50 random characters with a mixture of upper- and lower-case letters, numbers, and symbols." It has the same benefits as creating a complex long password but without the user memory costs.

1.6 Personal password storage

Don't store in a computer file. An attacker accessing this password file can duplicate the password.

Write down safely Even if the password is stored safely, the very act of writing it down makes it's duplication and physical theft possible. There is discussion as to whether the security risks of writing passwords are in fact very low [5]. And in fact, if users write down passwords, then they may be more confident making stronger password choices [6][7][8].

Don't choose "remember me". If the "remember me" option is not used then if an attacker steals a laptop or computer they should not automatically have access to the accounts on it. It is equivalent to not logging out of an account.

1.7 Reuse

Never reuse a password Reusing passwords has the security disadvantage that if an attacker compromises a password on one site then the password can be used to gain access to other sites. This means if passwords are reused then online and offline guessing becomes much easier for an attacker. In fact, if the

password is leaked elsewhere the chance of it being compromised for this given organization is just equal to be chance that an attacker tries.

However, even with different passwords at different sites, the attacker has a good chance of being able to leverage the information from a separate compromised site to mount effective phishing, social engineering and guessing attacks [9]. These will be at a higher cost to the attacker though.

Alter and reuse passwords Altering and reusing passwords means not directly reusing passwords between sites. It will make a guessing attack necessary for an attacker even if they have access to a password belonging to the same user from a different site. However, Das et al. [9] were able to guess approximately 10% of non-identical password pairs in less than 10 attempts and approximately 30% in less than 100 attempts. Therefore we mark it as a limited security improvement.

Don't reuse certain passwords. Asking users to not reuse certain passwords is equivalent to saying that a user can reuse some passwords.

In fact, if we look at the specific advice in this category we can see that most organizations are asking users to not reuse the password for *their* site. This does provide some security advantage as the attacker will not be able to directly access the protected account using the revealed password. But, as with "don't reuse you passwords" we know that an attacker can still leverage information from other compromised sites to attempt phishing, social engineering and guessing attacks.

1.8 Sharing

Never share your password In the process of sharing a password it could be eavesdropped. Not allowing users to share their passwords also helps to protect against social engineering. Though this is through the form of user education.

1.9 Two-factor authentication

Use Multi-factor authentication As mentioned before multi-factor authentication traditionally involves: *something you are*, *something you know*, and *something you have*. The *something you have* is susceptible to theft. However, if it is stolen the user if still protected by their other authentication factor. Using multi-factor authentication decreases the success of phishing (as second factors are often not subject to replay) and online guessing attacks (as both factors must be guessed). We underline some of the benefits as it depends on which factors the user or organization choose to use.

Use 2-step verification on phone The phone can be stolen or the code can be revealed by eavesdropping or a side channel attack. But again, if the phone is compromised, it is possible that the first step of the authentication process

will keep the users' account secure. 2-step verification decreases the success of an online guessing attack and a phishing attack.

Use for remote accounts Without knowledge of a specific second factor it is hard to say what the security effects are. Therefore, depending on what the second factor is, there is the potential for physical theft or endpoint compromise to jeopardize the authentication. The probability of the exchange being eavesdropped is much higher if used for remote accounts.

1.10 Username

Enforce composition restrictions on usernames Florêncio, Herley and Coskun argue that it is better to increase the strength of the userID rather than the passwords [10]. They propose that this will protect against online guessing attacks but will not majorly increase the cost to users since the username can be recorded visibly.

Don't reuse username If the same username is used for multiple accounts then once the password for one account is compromised, this password can be tried against the same person's other accounts. Das et al find that 3%, of users directly re-use passwords between sites and many others introduce small modifications to their passwords across sites [9]. Not reusing a username could be one way to protect against an attacker leveraging this vulnerability and could be less burdensome on the user than a restriction on altering and reusing passwords.

2 Organization advice

2.1 Administrator accounts

Not for everyday use It can be argued that the more times the authentication process is completed by the user, the more times it is susceptible to compromise during entry or transmission. We therefore say that not logging into the administrator account for everyday tasks decreases the chance of eavesdropping and side channel attacks.

Must have its own password If there is one administrator then ensuring that this administrator account has a distinct password means it is less vulnerable to eavesdropping and side channel attacks. However in most situations, many users will require privileged administrator access. In this case the problem depends on how you choose to implement this advice. If users access the administrator privileges by typing the administrator password via su then all privileged users must know the same password. This makes social engineering, phishing and endpoint compromise more likely. In addition if multiple users are

recording or sharing with others the same credentials then they are more likely to be duplicated and fall into the hands of an attacker.

Alternatively, there might be administrative access via the user's own password (e.g. via sudo) or a second administrative account/password corresponding to each user with administrative privileges.

All of these have associated security risks. In our table we have represented the case where there is one administrator who must create a second password which allows them access to administrator privileges.

Should have extra protection Depending on the extra protection the account is given this will have different benefits.

2.2 Backup work

Make digital & physical back-ups Having a back up of work means that attacks can be less harmful to the organization. Having backups does not directly decrease the chance of an attack but would be factored in relation to the costs of a breach. Having physical backups of work does mean that the potential for physical theft now exists.

2.3 Expiry

Store History to eliminate reuse This advice is given alongside "Change your password regularly". The password must now also not match any previous passwords. This means that knowledge of old passwords will not directly lead to an attacker knowing a current password.

However, even though users can no longer reuse prior passwords, alterations are still possible [11]. In fact, Zhang, Monrose and Reiter [12] identify that we can easily predict new passwords from old when password aging policies force updates.

In addition, if an attacker gains access to a users' account and changes their password, the user will be unable to change it again until the required number of days have elapsed, or with an administrator's help.

Finally, storing the history means there is an additional password file which needs to be protected. Because of the close relationship between old and new passwords [12], if this file is revealed then the information in it can be used to effectively guess the current password [9].

Change your password regularly In a certain situation changing your password regularly does decrease the probability of success of online guessing. Imagine an attacker cycling through a list of guesses. If a password is changed to something new during this guessing, then an attacker wishing to guess it must start their guessing process again from scratch.

However, most attackers will guess the most probable guesses first and since passwords follow a long tailed distribution [13, 14] a rational attacker will typi-

cally stop and move onto a new account if the password is not captured within the first few million guesses.

If the attacker correctly guesses the password within the time frame. Then the password will be changed at the beginning of the new period. This does bring some additional security but in reality once an attacker has access to the account they can set up a backdoor and will not need the password in future. Even if the attacker creates no backdoor the probability that they can guess the next period's password is high as users base their next password heavily on their previous password [12, 9]. Therefore, knowledge of the password from one period will strongly aid the attacker in guessing subsequent passwords.

Change if suspect compromise If the password has been leaked elsewhere then the advice is to change your password. This protects you from online or offline guessing attacks as otherwise an attacker with access to compromised password has immediate access to the account. Some of the caveats discussed above still apply. But the hope is that if a compromise is suspected, a user may be less likely to create a new password very similar to their old one. In addition the time scale to the creation of backdoor may be longer.

2.4 Generated passwords

Must be issued immediately This decreases the chance that generated passwords are stolen before they are told to the user. If passwords were created in advance they would likely be recorded as administrators could not remember multiple generated passwords. Therefore these passwords could be duplicated while in storage.

Distribute in a sealed envelope This increases the chance that the password is physically stolen as the envelope could be taken. The password could also be duplicated since it has been recorded. If an adversary opens the envelope and duplicates the password then it will go undiscovered if the adversary places the password page in a new envelope and reseals it. The benefit of the sealed envelope is that an observational, audible or network eavesdropping attack is less likely.

Only valid for first login Because these generated passwords are often issued and created by administrators the user has no confidence in the security of their password up until the point they receive it. Maintaining a rule that passwords must be changed at first login means that the user can now have complete control over the security of this new password. This advice then protects against previous duplication of the password.

2.5 Individual accounts

One account per user The alternative is multiple users using the one account. With multiple users using the same account one user could modify the

authentication information without informing other users (unauthorized binding). In addition, if multiple users are recording or sharing with others the same credentials, then they are more likely to be duplicated and fall into the hands of an attacker. Social engineering and phishing attacks and endpoint compromise are also more likely if there are multiple points of access.

Each account password protected If there is no password we can likely consider the account to already be in a state of compromise. Password protecting an account increases the security of the account by necessitating one of the attacks to take place before an attacker can gain access. It obviously protects against both online and offline guessing. In addition having a password makes a side channel attack more complex. An attacker should be able to differentiate the difference between an account login where no password is used and when a password is used.

2.6 Input

Don't performed truncation Truncating passwords makes online and offline guessing easier. It can also affect social engineering attacks. If the user does not know that the password will be truncated they may reveal the first few characters of the password without realizing the true security extent of this action.

Accept all characters This increases the necessary search space of an attacker attempting online or offline guessing. Allowing all characters could give more scope for a SQL injection attack, but the hope is that there would be adequate string escaping in place to mitigate this fear.

2.7 Keep accounts safe

Implement Defense in Depth Defense in depth can be divided into three categories: physical controls, technical controls and administrative controls. The security defense in depth can provide depends on exactly what strategies are deployed. They have the potential to mitigate any of the eleven attack types but without knowing what is implemented we cannot say exactly what the security advantages or disadvantages are.

Implement Technical Defenses The same argument as above can be used for this advice; it is not specific enough for us to know it's benefits. Though it is unlikely to aid against physical theft and social engineering.

Apply access control systems Access controls make sure that only certain users have access to their required aspects of the system. With respect to authentication, this means that only the privileged administrators have the power to view and control the authentication procedures and modify the stored

authentication data. This protects against a malicious employee "turning off" authentication or other security mechanics, duplicating the stored password dataset or downloading malware to attempt side channel or keylogging attacks. However, exactly what this advice protects against depends on which specific access controls are put in place.

Monitor and analyze intrusions Awareness of what an attacker is doing within the system and learning where the vulnerability is is important for security. However this advice has no direct security affect unless the analysis is acted on. For example, if an administrator witnesses an attacker duplicating the plaintext password file, then a forced password change might need to be implemented. Else if an administrator witness an attacker binding an additional form of authentication to a user or changing the credentials for a user, then these actions would need to be reversed. Monitoring and analyzing intrusions could also guide user education.

2.8 Policies

Establish clear policies This advice does not directly increasing or decrease the probability of success of an attack type.

2.9 Storage

Encrypt password files Encrypting password files will protect against the theft of the hard drive. However, the password used for encryption could still be read from the RAM. If the system can access the password without manual intervention then the password is likely to be stolen if the encrypted file is stolen. An attacker will have more difficulty downloading the password file for offline guessing.

Restrict access to password files Restricting access to password files will protect against certain types of unauthorized binding. If an attacker does not have access to the stored authentication details then the attacker will find it difficult to change the password stored for the user or link additional passwords or authenticators to the account. Preventing read access to a password file could prevent offline guessing attacks.

2.10 Throttling

Throttling (or rate limiting) password guesses drastically reduces the number of guesses an attacker can make. The attacker can no longer continuously make guesses until the correct password is accepted. However, because of the right-skewed nature of password distribution, the attacker does still have a high probability of success with a small number of guesses [14][13].

2.11 Additional advice

Don't allow users to paste passwords There appears to be no security benefits to this advice [15] and indeed in our model we cannot find any attack type that it mitigates.

References

[1] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 523–537, IEEE, 2012.

[2] V. Drury and U. Meyer, "Certified phishing: taking a look at public key certificates of phishing websites," in *15th Symposium on Usable Privacy and Security (SOUPS'19). USENIX Association, Berkeley, CA, USA*, pp. 211–223, 2019.

[3] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The long "taile" of typosquatting domain names," in *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 191–206, 2014.

[4] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 449–464, 2014.

[5] J. Leyden, "Write down your password today." `http://www.theregister.co.uk/2005/07/19/password_schneier/`, 2005. Accessed: 2017-01-20.

[6] W. Cheswick, "Rethinking passwords," *Communications of the ACM*, vol. 56, no. 2, pp. 40–44, 2013.

[7] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2595–2604, ACM, 2011.

[8] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133–144, ACM, 2009.

[9] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse.," in *NDSS*, vol. 14, pp. 23–26, 2014.

[10] D. Florêncio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?," *HotSec*, vol. 7, no. 6, 2007.

[11] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 2, ACM, 2010.

[12] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: An algorithmic framework and empirical analysis," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 176–186, ACM, 2010.

[13] H. Murray and D. Malone, "Exploring the impact of password dataset distribution on guessing," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pp. 1–8, IEEE, 2018.

[14] D. Malone and K. Maher, "Investigating the distribution of password choices," in *Proceedings of the 21st international conference on World Wide Web*, pp. 301–310, ACM, 2012.

[15] S. B, "Let them paste passwords." `https://www.ncsc.gov.uk/blog-post/let-them-paste-passwords`, 2017. Accessed: 2017-01-20.