Revisiting Password Rules: Facilitating Human Management of Passwords

Leah Zhang-Kennedy
School of Computer Science
Carleton University
Email: leah.zhang@carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Email: chiasson@scs.carleton.ca

Paul van Oorschot
School of Computer Science
Carleton University
Email: paulv@scs.carleton.ca

***Abstract*—Password rules were established in the context of past security concerns. Recent work in computer security challenges the conventional wisdom of expert password advice, such as *change your passwords often*, *do not reuse your passwords*, or *do not write your passwords down*. The effectiveness of these rules for protecting user accounts against real world attacks is questioned. We review the latest research examining password rules for general-purpose user authentication on the web, and discuss the arguments behind the continued acceptance or the rejection of the rules based on empirical evidence and solid justifications. Following the review, we recommend an updated set of password rules.**

I. Introduction

Password rules have not kept up with the growing sophistication of computer security threats. The holy grail of password best practices, such as *change your passwords often*, *do not reuse your passwords*, or *do not write your passwords down*, may no longer be practical advice for end-users. A user manages on average 25 password-protected accounts [17] ranging from high-asset (e.g., banks) to low-asset (e.g., news) accounts. Remember strong passwords for all of the accounts exceed human memory capabilities [20], [21]. Users inevitably break password rules to cope with password management.

Several proposals were made to reduce the problems of text passwords (see Bonneau et al. [5] for a comprehensive summary and review). While some schemes offered significant security or usability gains, they were retained at a cost of other benefits. For example, one proposal is to use graphical passwords. They are easier remember, but vulnerable to shoulder surfing, require longer login times, and have poor accessibility (e.g., blind users). Like text passwords, the cognitive load also does not scale well as the number of accounts increase. Furthermore, password managers are proposed to reduce the cognitive burdens by requiring users to remember only a master password, but the schemes introduce their own security and usability problems [13]; passwords are nevertheless mainly user-chosen and prone to guessing attacks, and are vulnerable from a single point of failure. In the search for an ideal scheme to replace text passwords, researchers assessed that no one scheme proposed thus far retains the full set of benefits that text passwords already provide [5].

As metrics for measuring the guessing resistance of user-chosen passwords against online and offline guessing attacks improve, experts now recognize that traditional measures of strength, like the NIST (US National Institute of Standards and Technology) entropy [8], are very crude estimates of password strength. Leaked databases of user accounts (e.g., RockYou) provided many insights into the strength and composition of user-chosen passwords in the wild. This enabled a better understanding of the pros and cons of existing metrics, but many password policies have yet to reflect the findings from this body of research.

Password rules are often chosen by industry to meet with standard security policy and auditing guidelines, regardless of whether they make sense for the service provider and its users. The reasons behind many security requirements imposed on users are poorly understood — it is unclear what security benefits are met by the requirements, and at what cost. Furthermore, password mechanisms are often poorly implemented and managed. Many services store users' passwords in plaintext or reversibility encrypted [20], leaving users with no protection if the password file or the decryption key is compromised. Password attacks are becoming more sophisticated and complex, operating from various attack vectors. In some cases, the strength of a password is irrelevant to defend users, as with password capture (e.g., phishing, keylogging).

A growing body of work (e.g., [10], [20], [21], [44]) challenges the conventional wisdom of password rules. Given the increasing collection of empirical data of real world password practices and knowledge in password cracking methods, it is timely to review password rules using the latest research findings. The main contributions of this paper are a systematic review of the literature related to password rules for general-purpose user authentication on the web, highlighting empirical evidence that can be used to support guidelines, a primer on existing practices and rules, and a recommended set of updated rules that reflect today's environment of use and threats.

II. User Behaviour in Managing Passwords

The study of user behaviour in password management originated in the workplace over a decade ago. Adams and Sasse [1] found that password policies cause high levels of dissatisfaction because they do not meet users' work practices, and could lead to low motivation and insecure behaviour.

In 2004, Dourish and Grinter [16] studied users' difficulties in managing various aspects of security, including password

978-1-5090-2922-8/16/$31.00 ©2016 IEEE

management. Many users created passwords based on personally identifiable information. Similarly, Riley [34] found that users used meaningful words and numbers to create passwords, despite of knowing that they may be insecure. To cope with memorability challenges, users commonly select passwords composed of semantics and concatenated character strings or numbers (e.g., Password123), character substitutions (e.g., '@' for 'a'), and common passwords (e.g., qwerty). They also reuse a small set of passwords between various types of accounts and never change them unless required by the site. Gaw and Felten [22] found similar patterns of password reuse across multiple accounts; password reuse became more frequent when people accumulated more accounts because they did not create more passwords. It is unsurprising that password reuse makes remembering passwords easier. In 2007, Florêncio and Herley [17] found that the average web user manages 25 password-protected accounts with just 6.5 passwords shared between them. During the same year, Gross and Rossum [23] studied users' knowledge of security in an organizational context and analyzed users' perspectives on security management. They challenged the conventional view that users are the "weakest link" in computer security, and argued that users often have sophisticated coping strategies regarding sensitive information. In a 2007 study, Singh et al. [37] found that password sharing is common among couples, and Kaye [26] found in 2011 that approximately 20% of users reported sharing an email password with colleagues. Stobert and Biddle [38] confirms that most users cope with demanding password tasks by reusing passwords and writing them down. Coping behaviours do not stem out of users' ignorance of best password practices, but involve perceptive behaviours and careful self-management of user resources [38], [39].

A body of work supports that users' mental model of password security could impact usability and have negative consequences on security. A *mental model* is a simplified internal concept of how something works in the real world [14]. Camp [9] developed five conceptual models of security using analogies and metaphors: physical security, medical infections, criminal behaviour, warfare, and economic failure. In 2007, Asghapour et al. [3] performed a formal evaluation of Camp's conceptual models in a card sorting experiment. Findings suggest that gaps exist between the mental models of expert and novice users. In 2010, Wash [41] identified eight "folk models" of hackers and viruses. He found that users rely on these models to decide what security advice to follow and which security software to use. A qualitative study by Ur et al. [39] found that many weak passwords result from users' misconceptions about password strength. When making choices about password practices, inaccurate mental models can significantly influence user behaviour.

A study by Gaw and Felten [22] observed that users severely underestimate the guessability of their passwords due to the perception that attacks are carried out manually by humans instead of automated tools. Users often fail to recognize that personal information and dictionary words are easily guessable given enough computing power and a large number of guesses. Zhang-Kennedy et al. [45] found that users' mental models of password attacks revolved around targeted attacks, which influences how they choose passwords and their understanding of a strong password. In 2009, an insightful paper by Herley [24] proposed that users (rationally) reject security advice because it offers poor cost-benefit tradeoffs. Users could intentionally ignore good password advice if they believe the benefits are moot.

III. Password Rules

The intended security goal for password rules is to prevent users from choosing easy-to-guess passwords, and to guide users toward secure password management. An early example of comprehensive guidelines can be found in The Password Management Guide [7]. Today, several rules are automated as a password strength policy used to regulate password length and composition. Other password policies include blacklists (proactive password checking), password expiration/aging, rate-limiting, and lockout policies.

The most common password rules that users encounter fall into two categories: Password strength rules are enforced when a password is created, and password management rules guide users toward secure handling of passwords.

A. Strength rules

R1 *Length:* A password length policy prevents users from choosing passwords that are too short. Password policies typically require a length of at least 6 to 8 characters. There is considerable variability, where some websites may require a shorter length (e.g., a 4-digit PIN) while others enforce longer passwords (e.g., at least 8 characters or an exact length).

R2 *Composition:* A password composition policy prevents users from choosing passwords that are too simple. It enforces rules about what types of characters can be used. A password composition policy typically require passwords that contain characters from one or more of the following sets:

- Uppercase characters
- Lowercase characters
- Base 10 digits
- Non-alphanumeric ASCII characters

A very loose policy may only insist on a minimum composition (e.g., numbers only), while others enforce a more complex composition (e.g., uppercase and lowercase letters, numbers, and special characters). It is suggested that varying complex rules across multiple sites could make cross-site password sharing more difficult [18], but there is little evidence to support that this is the primary purpose of a composition policy.

R3 *Blacklist:* Some sites prohibit the use of dictionary words due to the susceptibility of human-chosen passwords to dictionary password guessing attacks (attackers use dictionary lists or high probability candidate passwords for guessing). Others enforce this rule by banning the use of the most common passwords. For example, users could be banned from choosing passwords from a blacklist of the top 1000 frequently used passwords. Typically, lists of the most commonly used passwords are obtained from leaked datasets (e.g., RockYou).

Although password strength policy can help to protect against guessing attacks, it cannot protect users against password capture by malware, social engineering, or physical observation.

B. Management rules

R4 *Change-it-often:* A password expiration or *password aging* policy requires users to change their passwords at a set interval (e.g., every 90 days). Regular password change is recommended by NIST [35]. The historical security intent is to protect users from the risk of undetected password compromise over a length of time [10], [20]. The longer a password is used for authentication purposes, the higher the probability of exposure to attackers. Presently, password expiration is rarely enforced among general-purpose websites [18], but are commonly used by government and academic institutions.

R5 *Do-not-reuse:* The number of passwords that a single user manages increases with every account sign-up. When passwords are reused across multiple accounts, an attacker who is able to compromise one site can leverage the same password reused on another site. Bonneau and Preibusch [6] observed that low-asset sites such as news websites tend to have poor security, which could compromise high-asset sites due to password reuse. It is suggested that composition polices make reuse more difficult [18], but they do not directly prevent reuse. Password policies across different sites are diverse; a single password policy is only relevant on the site that enforces it.

R6 *Do-not-write-it-down:* Users are advised to never write down their passwords. The original security intent of this rule is to prevent local attacks from friends, co-workers, family, or other on-site observers. Although plain text passwords should never be stored on unprotected computers with network access, writing down paper copies of passwords may not pose a serious security risk [10].

R7 *Do-not-share-it-with-anyone:* Users are advised to not share their passwords with anyone. The security reasons seem obvious, but user practice indicates that passwords are frequently shared with close family members and colleagues. Some security experts [10], [38] argue that password sharing may be appropriate under certain circumstances, such as during account recovery or in an emergency situation.

C. Enforcement of password rules across the web

The enforcement of some minimum password length appears to be the only consistent aspect of password requirements on the web [6]. A 2010 study [18] of password policies across 75 different websites found no standard or preferred policy. The strength of password policies is enormously diverse. Some sites will accept simple six-character passwords, while others require more advanced rules. There appears to be no correlation between policy strength and the security needs of the site. Password policy decisions are made independently at different sites. Therefore, they do not help with password management across multiple accounts.

Florêncio and Herley [18] suggest that the reason behind strong policies lies not within greater security concerns, but in greater insulation from the consequences of poor usability. Bonneau and Preibusch's empirical study of password implementations [6] reveals that business incentives for offering password-protected accounts where there is little security need are driven by the desire to collect user information and to establish a feeling of trust with users through account registration. Furthermore, Inglesant and Sasse [25] suggest that passwords are encountered in many ways in the workplace beyond authenticating for a service or a device, but existing password policies do not reflect this trend. They caution that strict password policies could actually decrease security as users adopt insecure coping strategies. At the other extreme, many online services have incentives to avoid complex password policies that impose a strain on usability because they wish to avoid a poor user experience.

IV. Security Benefits vs. Usability Burdens

In this section, we review the latest work examining password rules, and discuss the arguments behind the continued acceptance or the rejection of the rules based on empirical evidence and solid justifications.

A. Strength rules (length, composition, and blacklist)

The intent of a password length and composition policy is to force all users to comply with a minimally strong password [18]. Traditionally, $L_{min}Log_2C_{min}$ [18] is used to measure the strength of a policy in bits, where L_{min} meets the minimum required length, and C_{min} meets the minimum cardinality of characters. For example, a password policy that takes only lowercase letters (a – z) with a minimum length requirement of 6 characters has $L_{min} = 6$ and $C_{min} = 26$. In comparison, a password policy that takes uppercase and lowercase letters (a – z, A – Z), and digits (0 – 9), with a minimum length requirement of 8 characters has $L_{min} = 8$ and $C_{min} = 62$.

This approach is criticized for not factoring in weaknesses of user-chosen passwords. To give a representative example of the problem, consider a random 6-character password, $wduopv$, using lowercase letters that belongs to a 28-bit policy, and compare it to a human constructed 8-character password, $Pa\$\$w0rd$, that belongs to a 52-bit policy using uppercase and lowercase letters, digits, and non-alphanumeric ASCII characters. Presumably, the stronger policy would result in passwords that better resist a guessing attack, but this is obviously not the case. On the contrary, analysis of real world leaked datasets reveals that users are more likely to choose common, predictable (therefore more guessable) passwords. Relying solely on entropy oversimplifies how passwords withstand guessing attacks.

Historically, the NIST guideline [8] based on the Shannon Entropy was used for estimating password strength, and was the basis for creating password policies. The Shannon entropy measures the amount of information that is unknown to the attacker due to random variables, but studies [27], [42] show that it is only useful when all events are equally probable. Recent work [4], [42] on how passwords stand up to guessing attacks reveal that $L_{min}Log_2C_{min}$ is a very poor estimate of guessing resistance because many user-chosen passwords are selected from a highly skewed distribution. The NIST guideline overestimates the security of certain passwords that may be cracked quickly.

1) Online vs. offline attacks: Length and composition policies help users choose stronger passwords [28], but they also increase annoyance and fatigue [36]. The question comes down to what should be the minimal strength required to protect the majority of user accounts? Florêncio et al. [20] argue that there is an enormous gap between the guessing resistance needed to withstand online and offline attacks. For example, in a conceptual model of the number of guesses a password would withstand over a 4-month campaign, a password in an online attack may need to withstand only 10^6 guesses, while a password in an offline attack may need to withstand at least 10^{14} guesses. These thresholds for probable safety differ by 8 orders of magnitude. The authors argue that user effort spent on meeting strength requirements set by policies that fall between the two thresholds is entirely wasted to prevent offline attacks. Additionally, they argue that offline attacks occur in much more narrow circumstances compared to online attacks. Online attacks can be easily mounted by anyone at any time, although the number of guesses could be limited by lockout and rate-limiting policies. An offline attack scenario only occurs when a password file is leaked, goes undetected, and the passwords are hashed and salted. Otherwise, simpler attack methods can be used. For example, if the password file contains clear text, is hashed but not salted, or reversibility encrypted, then password cracking is either not necessary (attacker has the clear text password or the decryption key) or a simple rainbow table lookup of hashed passwords would suffice.

The exact effect of a strength policy on guessing resistance is difficult to measure because collections of passwords created with and without a policy could not yet be directly compared [20]. Although present measurements are not ideal, several studies provide insightful observations on the effect of password strength policies on password guessability. In a large-scale study of 70 million passwords [4], Bonneau found that user-chosen passwords provide roughly equivalent security to 10-bit random strings against online attacks, where an attacker who mounts 10 guesses per account will compromise around 1% of accounts. Furthermore, user-chosen passwords provide the equivalent to roughly 20-bit random strings against offline attacks, where an attacker performs unrestricted brute-force aiming to break half of all accounts. Kelley et al. [27] studied 12,000 passwords collected under seven composition policies of varying strength, and used a variety of cracking algorithms to evaluate their guessing resistance. They found that the best composition policy at resisting guessing attacks depends on how many guesses an attacker will make. After 10^{13} guesses, there is a huge variation in how passwords withstand guesses from standard algorithms. In the experiment, study condition *basic-length-16* passwords (i.e. at least length 16) faired better than *comprehensive-length-8* passwords (i.e. lowercase, uppercase, digits, and special characters of at least length 8) at one trillion guesses. At fewer than 10^6 guesses, however, passwords created under different policies are similarly vulnerable. 40.3% of passwords under several policies such as *basic-length-8*, *basic-length-16*, and *comprehensive-length-8* were successfully cracked. A study by Mazurek et al. [31] examined 25,000 university passwords created under a *comprehensive-length-8* policy that checks against a dictionary. They found that the success rates for guessing is minimal before 10^7 guesses, but drastically increases by 10^{14} guesses (48% of accounts were cracked). Participants found it most difficult to meet comprehensive-length-8 requirements, suggesting that a policy requiring longer length instead of more complexity is a more usable approach.

2) Delayed response and account locking: Delayed response and account locking policies are common countermeasures against online guessing attacks. The number of guesses that an attacker could attempt in a reasonable time can be controlled by a delayed response policy that incrementally slows the system response after a number of failed login attempts. Furthermore, the number of online guesses could be limited by a lockout policy that restricts access after a number of failed login attempts. Florêncio et al. [19] suggest that even a relative weak password from a 20-bit policy may suffice to prevent online attacks when a lockout policy is in place. In practice, however, Bonneau and Preibusch [6] found that few sites prevent ongoing guesses even after 100 failed logins.

The main concern with implementing an account locking policy is denial of service attacks. To prevent automated programs from submitting many false logins, Pinkas and Sander [32] introduced an authentication scheme where users are required to pass Automated Turing Tests (e.g., CAPTCHAs) before starting the authentication process, which significantly raises the cost of online guessing attacks.

The primary usability concern is that account locking and delayed response policies cause inconvenience to legitimate users. The usability of the scheme proposed by Pinkas and Sander [32] was improved by van Oorschot and Stubblebine [40] using a history-based login protocol to enable fewer Automated Turing Tests to legitimate users and allowing greater flexibility with protocol parameter customization for particular situations and users. Further, Alsaleh et al. [2]

raised inadequacies of past protocols to address large-scale online dictionary attacks and introduced a Password Guessing Resistance Protocol (PGRP) that limits the number of login attempts from unknown remote hosts while allowing several failed login attempts from known frequently-used machines belonging to legitimate users.

3) Blacklist: Restricting the use of dictionary words and frequently used passwords prevent users from choosing a password that is common and therefore easily guessed. Weir et al. [42] found that a significant improvement in the security of a system could be obtained with even a moderately sized blacklist. At 10^6, a blacklist seems to be of a practical size in terms of usability because the list only restricts the most common choices among users. A larger list of approximately 10^{14} would be required to protect users against offline attacks, but this would cause a much greater inconvenience [31].

B. Change-it-often rule

A password expiration policy forces users to change their password at a set interval. Presumably, it would prevent access to an account by an attacker who has obtained a user's old password. However, little empirical evidence exists to support its effectiveness. A study of password expiration conducted by Zhang et al. [44] in 2010 showed that forced password expiration was not as effective as previously believed. The study used a dataset of password histories of 7700 defunct ONYEN accounts, a single-sign-on system at the University of North Carolina. They analyzed which user-selected replacement passwords prevented the attacker's continued access. The study found that previous use of syntactic transforms in selecting passwords is a strong indicator of their future use. Leveraging patterns in subsequent user-chosen passwords, the researchers developed a transform-based algorithmic framework by which an attacker could search for a user's future password given an old one. The search tree of the algorithm considers a depth of up to 18 characters. A search begins at the root with an input such as `password`. Upon visiting a node, the last transform in the corresponding sequence is applied to the output of its parent node (so the input becomes `pa$sword`, and so on). The algorithm considers various sets of transforms like the number of character insertions, deletions, block moves, or string replacements.

The results for successfully guessing newly chosen passwords from old ones using the algorithmic framework are alarming. In online attacks, 17% of accounts were cracked with fewer than 5 guesses. In offline attacks, they guessed 41% of new passwords in just under 3 seconds per account. Although the study addresses implications for attacks occurring both online and offline, the work suggests that expiration policies are more beneficial to mitigate offline attacks because an online attacker gets much fewer guessing attempts (but attacks are easily mounted). However, Florêncio et al. argue that offline attacks occur in limited circumstances, as discussed in Section IV-A1. Expiration policies also do not help with password capture.

In a theoretical analysis quantifying the security advantages of password aging policies, Chiasson and van Oorschot [12] suggest that the optimal security benefit is relatively minor and outweighed by the negative usability impact that users experience. Additionally, the high predictability new passwords from knowledge of the old [44] suggest that imposing password aging policies on users is ineffective in meeting the intended security goals.

C. Do-not-reuse rule

The do-not-reuse rule prevents the following scenario: the user shares a password between account A and account B. If an attacker obtains the password from account A and knows the username of account B, both accounts could be compromised under the same password. Das et al. [15] examined several leaked password datasets to measure password reuse across Internet sites. The found that 43% of users directly reused passwords between sites, and that 19% of users used passwords that are substrings of one another from different accounts. Exact reuse is mitigated by different policies across sites. However, users used predictable strategies to work around the different policies. For example, they often make small edits to a common passphrase, such as adding a number "1" to the end of a password. Using a cross-site password guessing algorithm developed by Das et al. [15], they were able to guess approximately 10% of the non-identical password pairs in less than 10 attempts, and approximately 30% of such pairs in less than 100 attempts. The study confirms that password reuse is common, and identifies it as a serious security vulnerability.

Many studies [17], [36], [38] show that a significant number of users reuse their passwords across accounts. Given that reuse will likely be a part of users' password management coping strategy, a number of recent research papers inquire whether password reuse could be a sensible part of password portfolio management. Florêncio et al. [21] argue that the do-not-reuse rule ignores that fact that users have limited abilities to manage a large number of accounts. Ideally, a user with N accounts chooses N strong passwords. An active web-user may have a hundred or more password-protected accounts. Therefore, the effort required to manage a portfolio of N passwords, each with strength S of $logS$ bits, appears to be $NlogS$, but this estimate is an oversimplification. Beyond remembering N passwords, there is an additional memory burden of remembering which password matches which account. The number of bits to be remembered to manage a portfolio of N passwords, each of $logS$ bits, now become $NlogS+log(N!)$, where there are $N!$ possible mappings of N unique passwords to accounts that use $log(N!)$ bits. Using this model, assuming that a user who chooses a random password of 40 bits for each of the 100 accounts will have to remember 4525 bits of information. It is a burden that far exceeds human memory capabilities. Reusing passwords, therefore, helps to reduce this unreasonable memorability burden.

The authors also consider attack vectors where the compromise of one account could leak to others sharing the same password. Potential threats include phishing, password

Password Rules	Principle Threats Mitigated				Usability Cost
	T1 Password capture	T2 Online Password Guessing	T3 Offline Password Guessing	T4 Targeted Password Guessing	
Strength Rules **R1 Length** **R2 Composition** **R3 Blacklist**	None [25].	Mitigates online guessing attacks if a moderately strong strength policy with a lockout policy is enforced [20].	Reduces success rates of offline attacks if a very strong policy is enforced [20].	A blacklist protects users from choosing the most predictable passwords [20].	Moderate to withstand online attacks. High to withstand offline attacks [20]. Causes annoyance and fatigue [36].
R4 **Change-it-often**	Minimal to none [12], [25].	Minimal effect [10], [12]; users are likely to use a predictable variation of an old password [44].			High; annoying for users [10], [12], [25].
R5 **Do-not-reuse**	Minimal to none [21], [24].	Mitigates attacks on other accounts only if the password is shared [10], [21], [24].			Beyond cognitive capacity for password management [20], [21].
R6 Do-not-write-it-down	None [10], [24].			Only if the physical or digital copy is accessed [10], [24].	High cognitive cost; forget passwords [10], [24], [38].
R7 **Do-not-share**	None [10].			Some risks from the person sharing with [10], [33].	Moderate; Sharing is necessary under certain circumstances [10], [38].

TABLE I
THREATS MITIGATED BY EACH OF THE PASSWORD RULES AND THEIR ESTIMATED USABILITY COST

guessing, shoulder-surfing, system-side database compromise, and network channel compromise. Reuse is not relevant when all password-accounts are compromised (e.g., keylogger), or in situations where an attacker does not need to obtain the actual password (e.g., session hijacking). In an earlier paper, Herley [24] agrees that the risks associated with reuse appear to include only the cases where the user is phished, or if the user's credentials are stolen. If the attacker obtains the password by keylogging malware, both passwords could be captured regardless of whether the user reuses the same password. Therefore, he concludes that risk reduction is minor if the practice of password reuse is eliminated.

Password reuse may be a valuable coping strategy in balancing the allocation of user effort between accounts. To reduce the memorability burden, user effort should be unequally distributed across accounts, since not all accounts have the same security needs [21]. Stobert and Biddle [38] found that users are incorporating classifications of important (e.g., banking) vs. unimportant accounts (e.g., entertainment) as a part of their password management strategy. There is no empirical results quantifying the optimal classification of accounts, but many recommendations are made. Florêncio et al. [21] recommend strategic groupings of high value accounts with low probability of comprise, and low value accounts with high probability of compromise. Cheswick [11] suggests grouping accounts into three categories: no importance, inconvenient if stolen, or major problem if abused. Florêncio et al. [20] recommend grouping accounts based on potential personal and business consequences of account compromise.

D. Do-not-share rule

The obvious security reason for the do-not-share rule is to maintain a one-to-one mapping between individual users and accounts. In practice, however, several studies show that passwords are frequently shared. A 2011 study [26] found that one-third of users shared their personal email password. Another study [37] found that couples often share passwords to manage money and as a demonstration of trust. Some argue that there are certain situations when password sharing is appropriate and even necessary. Sharing passwords could help with account unlocking issues if the user forgets his password [10], or if the user is unavailable to provide the password in emergency situations [38].

Pew Internet research [30] found that 30% of teens surveyed share passwords with a friend, boyfriend or girlfriend as a demonstration of trust and intimacy. In the event of a fallout, however, consequences include a vengeful ex or a former friend sabotaging the account spreading humiliating messages or scouring private messages for clues of disloyalty or infidelity [33]. This suggests that even though users are selective about which password to share and with whom [26], there is always some risks from the person with whom the user is sharing. Therefore, passwords should always be shared with caution and only when absolutely necessary.

E. Do-not-write-it-down rule

Users are advised to never write down their passwords, but several security experts [10], [24] advocate that recording passwords on paper may not be a bad practice. Writing down passwords seems to have small security risks and a big usability gain. Cheswick [10] argues that in the presence of modern attack models, the practice is relatively safe since most attacks are mounted remotely and are much more common than a "check-the-post-it" attack. Herley [24] argues that stopping users from writing down their passwords further increases the memorability burden with little security gain.

Shay et al. [36] found that the practice is more rare than other coping strategies like reusing and sharing passwords. Users are more likely to write down their passwords as a fallback strategy [38] rather than using it as a day-to-day coping strategy because it is inconvenient to carry paper copies. Storing passwords in plain view is a bad idea, but a password kept in a notebook at home is only vulnerable to those who have access. To make written passwords less vulnerable to close observers, users could record a password hint or clue instead of the actual password. A study by Stobert and Biddle [38] showed that many users practice this strategy. Alternately, users could store protected digital copies of their passwords that are convenient to access and easy to update, but systems that require a master password could be attractive targets for attackers, as the compromise of the master password enables access to all stored passwords.

V. Implications of Password Rules

In order to evaluate the practically of passwords rules, it is sensible to assess whether they help to address the principle security threats that users face, and weigh the potential security benefits against the usability costs. Table I provides a summary of the threats that each rule helps to protect. The main threats against passwords faced by users are [19]:

T1 Password capture (e.g., phishing, keylogging, shoulder surfing)

T2 Online password guessing (e.g., a online brute-force or dictionary attack on the user's account)

T3 Offline password guessing (e.g., a offline bulk-guessing attack on all accounts at the server)

T4 Targeted (e.g., guessing based on user information).

A. Updated rules

Our literature review suggests that most users break some, if not all of the password rules to cope with using text passwords. We explore how these rules could be adapted to a more manageable set that considers usability factors while maintaining security. The results of our analysis are summarized in Table II. Ultimately, many password rules involve a trade-off between security and user effort. The updated rules should be viewed as a work in progress rather than an absolute set.

Moderate strength rules (R1 *strength*, R2 *composition*, and R3 *blacklist*) are recommended. It appears that password strength policies protect users more efficiently against online brute-force attacks. Users have no control over a server compromise of password files. Therefore, the burden of resisting offline attacks should not be put on users. There is a chasm between the guessing resistance needed to withstand online and offline guessing attacks [20] and user effort spent between the two thresholds are wasted. Practical strength rules should focus on spending users' effort on creating passwords that are strong enough to withstand online attacks; Florêncio et. al. [20] estimate that this is somewhere around 10^6 guesses. In an online attack, a minimal policy may be required with a supplementary lockout rule to restrict access after a few failed attempts. A lockout rule should account for repeated entries of the same password. They should be counted as one attempt since an attacker is unlikely to guess the same password twice, whereas it is common for a legitimate user to re-enter a password in case the first attempt contained a typographical error [10]. Therefore, counting repeat entries toward the lockout count only penalizes legitimate users while providing no added security benefit.

Mazurek et al. [31] found that demanding longer length provides greater security against current attacks compared to more complex policies that make creating and remembering a password more difficult. A short blacklist of the most common passwords is recommend to prevent users from choosing passwords that are easily guessed by dictionaries. Yan et al. [43] recommend mnemonic-based passwords, where a character (commonly the first letter) from each word of a memorable phrase is selected as the password. Mnemonic-based passwords are as memorable as naïvely selected passwords but as hard to guess as randomly chosen passwords [43]. Kuo et al. [29] caution that users should avoid selecting common phrases from popular sources because of the possibility that an attack dictionary could be compiled for mnemonic-based passwords. However, they conclude that building a comprehensive mnemonic dictionary is non-trivial due to the large search space of possible phrases. Consequently, it has lower success rates and less commonly deployed by attackers than regular dictionary attacks.

Users have misconceptions about how to interpret the strength of a password [45]. For example, some think $pa\$\$w0rd$ is strong due to crude entropy-based estimates and a limited understanding of how password guessing attacks work. Educational feedback and communication could be provided to help users learn why their choices are bad. In one approach [45], users who learned from an infographic and comic-based password education material were able to successfully identify weak passwords, create strong and memorable sample passwords, and showed an understanding of how the various types of attacks work.

> ***Updated R1-R3 – Create-strong-and-memorable-mnemonic-passwords:*** *Create strong and easy to remember passwords using original mnemonic-phrases. Passwords should be at least 8 characters long and do not contain common passwords (e.g., '123456', 'password'), predictable character substitutions (e.g.,'pa$$w0rd'.), or dictionary words.*

In general, R4 (*change-it-often*) is not recommended. Forced password expiration causes extreme annoyance and fatigue for users and has few security benefits. It provides minimal protection against access to an account by an attacker who has captured the account's expired password [44]. Users tend to make simple modifications to an existing password (e.g.,

Updated Password Rules	Principle Threats Mitigated				Usability Cost
	T1 Password capture	T2 Online Password Guessing	T3 Offline Password Guessing	T4 Targeted Password Guessing	
Updated R1-R3 Create-strong-and-memorable-mnemonic-passwords	None [20], [25].	Mitigates online dictionary and brute-force attacks supplemented by a moderately sized blacklist and a lockout policy. [19], [20], [43], [19], [42].	Provides improved protection against offline attacks [43].	Protects against targeted attacks [43].	Moderate cost to withstand online attacks [4], [20]. Longer length instead of more complexity is more secure and usable [27], [31].
Updated R4 Change-your-password-well:	Potentially effective if a password compromise is found [10].	Reduces the chance of ongoing compromise [10], [20].	Reduces the chance of initial or ongoing compromise [10], [20].	Reduces the chance of ongoing compromise [10], [20].	Moderate cost to change password when it is necessary [10].
Updated R5 Strategically-reuse-passwords	Minimal to none [21], [24].	Mitigate attacks on high-value accounts; Reduces risks between different account categories [10], [20], [21].			User cost is matched to account value (More effort is spent on high-value accounts) [10], [20], [21].
Updated R6 Keep-written-down-passwords-hidden	None [10], [24].			Only if the physical or digital copy is accessed [10], [24].	Reduces memorability cost; Use as a fallback strategy [10], [24], [38].
Updated R7 Share-passwords -with-caution	None [10].			Some risks from the person sharing with [10], [33].	Reduces memorability cost; Moderate burden to change password later [10], [38].

TABLE II
THREATS MITIGATED BY EACH OF THE UPDATED PASSWORD RULES AND THEIR ESTIMATED USABILITY COST

password1, password2, password3) when the password is changed, allowing attackers to guess the new password based on knowledge of the old password. Perhaps the only sensible time to force a password change is immediately after an account compromise is known, at which point users should be encouraged to select a distinct new password.

> ***Updated R4 – Change-your-password-well:*** *Change your password if you suspect that a service has been compromised. Create a new password that is not derived from a compromised password.*

R5 (*do-not-reuse*) is good advice, as the compromise of one account could affect other accounts protected with the same password. Although the security intention is good, Florêncio et al. [21] argue that this rule poses an impossible usability burden on users. As the size of a password portfolio increases without reuse, users cope by resorting to weaker passwords. Using weaker passwords only reduce the memorability burden slightly, as they also need to remember which password matches to which account. Therefore, password reuse may be a necessary coping strategy.

Security experts recommend dividing accounts into categories [11], [20], [21], but there is no consensus on the best way that this could be done. A general guideline appears to be that accounts should be categorized based on their importance, and that password reuse may be appropriate for low-assets accounts that would cause no effect or only minor inconvenience for the user if they were compromised. The observation by Bonneau and Preibusch [6] that low-asset websites usually have poor security suggests that these passwords should not be shared with high-asset websites due to the risk of cross-site compromise. Since reuse is unavoidable and there is no empirical data suggesting the optimal way to categorize accounts, the best advice to give to users is perhaps:

> ***Updated R5 – Strategically-reuse-passwords:*** *Categorize accounts based on their importance. Use unique passwords for high-value accounts (e.g., banking). Only reuse passwords for low-value accounts.*

R6 (*do-not-write-it-down*) should be updated to reflect current practices. Many security experts (e.g., [10], [18]) argue that writing down passwords is relatively safe considering the primary attack models that users face today (See T1-T4). Most attacks are mounted remotely from an anonymous attacker rather than a local knowledgeable adversary. Writing down passwords is typically not a primary coping strategy [36], but a fallback strategy [38].

Passwords kept securely at home are fairly safe, as it is only at risk to someone who has on-site access. Therefore, disallowing writing of passwords carries almost no benefit. To make a written password less obvious, Cheswick [10] recommends writing down a password hint. He suggests that storing passwords on the computer, such as in a password wallet, may be counter productive because they are prone to vulnerabilities on unsecured computers with network access.

> ***Updated R6 – Keep-written-down-passwords-hidden:*** *Store written-down passwords or password hints in a secure place hidden from view.*

There are some risks associated with sharing a password with someone, especially if the relationship turns sour. However, some security experts (e.g., [10]) argue that the convenience associated with sharing a password with a trusted spouse for account recovery may outweigh the potential risks. Sharing passwords may also be necessary for emergency situations or in special circumstances (e.g., access to important information when the spouse is away).

> ***Updated R7 – Share-passwords-with-caution*** *Share passwords with family, friends, or colleagues with caution. Change your password when the sharing obligation ends.*

B. Concluding Remarks

Giving definitive password advice to users is difficult because exact trade-offs between security benefits and usability costs are hard to quantify. Our literature review provided an overview of which password rules are supported with empirical evidence and which are outdated. Based on available evidence, we suggested an updated set of password rules that consider both the security and usability implications. Our effort was in building realistic, practical password rules given the current environment. These rules should continue to evolve as more empirical data becomes available, rather than remaining stagnant or gradually creeping towards increasingly unusable variations in response to new threats.

References

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] M. Alsaleh, M. Mannan, and P. C. Van Oorschot. Revisiting defenses against large-scale online password guessing attacks. *Dependable and Secure Computing, IEEE Transactions on*, 9(1):128–141, 2012.

[3] F. Asgharpour, D. Liu, and L. Camp. Mental models of security risks. *Financial Cryptography and Data Security*, pages 367–377, 2007.

[4] J. Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *IEEE Symposium on Security and Privacy (SP)*, pages 538–552. IEEE, 2012.

[5] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 553–567. IEEE, 2012.

[6] J. Bonneau and S. Preibusch. The password thicket: Technical and market failures in human authentication on the web. In *WEIS*, 2010.

[7] S. Brand. Department of Defense password management guideline. Technical Report CSC-STD-002-85, U.S. Department of Defense, Computer Security Center, 1985.

[8] W. E. Burr, D. F. Dodson, and W. T. Polk. NIST Special Publication 800-63: Electronic Authentication Guideline. Technical report, NIST: US National Institute of Standards and Technology, Gaithersburg, USA, 2006.

[9] L. Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37–46, 2009.

[10] W. Cheswick. Rethinking passwords. *Communications of the ACM*, 56(2):40–44, 2013.

[11] W. Cheswick. Rethinking passwords, Accessed March 2015. http://www.usenix.org/event/lisa10/tech/slides/cheswick.pdf.

[12] S. Chiasson and P. C. van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, pages 1–8, 2015.

[13] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *Usenix Security*, volume 6, 2006.

[14] K. Craik and W. James. *The nature of explanation*. Cambridge University Press, 1967.

[15] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[16] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[17] D. Florêncio and C. Herley. A large-scale study of web password habits. In *WWW '07: Proceedings of the 16th Internation Conference on World Wide Web*, New York, USA, 2007. ACM.

[18] D. Florêncio and C. Herley. Where do security policies come from. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[19] D. Florêncio, C. Herley, and B. Coskun. Do strong web passwords accomplish anything? *HotSec*, 7:6, 2007.

[20] D. Florêncio, C. Herley, and P. C. Van Oorschot. An administrators guide to internet password research. In *Proc. USENIX LISA*, 2014.

[21] D. Florêncio, C. Herley, and P. C. Van Oorschot. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proc. USENIX Security*, 2014.

[22] S. Gaw and E. Felten. Password management strategies for online accounts. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 44–55. ACM, 2006.

[23] J. B. Gross and M. B. Rosson. Looking for trouble: Understanding end-user security management. In *Proceedings of the Symposium on Computer Human Interaction For the Management of Information Technology*, page 10. ACM, 2007.

[24] C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *New Security Paradigms Workshop (NSPW)*, 2009.

[25] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392. ACM, 2010.

[26] J. Kaye. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2619–2622. ACM, 2011.

[27] 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 *IEEE Symposium on Security and Privacy (SP)*, pages 523–537. IEEE, 2012.

[28] 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*, pages 2595–2604. ACM, 2011.

[29] C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 67–78. ACM, 2006.

[30] A. Lenhart, M. Madden, A. Smith, K. Purcell, K. Zickuhr, and L. Rainie. Teens, kindness and cruelty on social network sites: How american teens navigate the new world of" digital citizenship". *Pew Internet & American Life Project*, 2011.

[31] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. Measuring password guessability for an entire university. In *Proceedings of the ACM Conference on Computer & Communications Security*, pages 173–186. ACM, 2013.

[32] B. Pinkas and T. Sander. Securing passwords against dictionary attacks. In *Proceedings of the ACM Conference on Computer & Communications Security*, pages 161–170. ACM, 2002.

[33] Richtel, M. Young, in Love and Sharing Everything, Including a Password, Accessed January 2016. http://www.nytimes.com/2012/01/18/us/teenagers-sharing-passwords-as-show-of-affection.html.

[34] S. Riley. Password security: What users know and what they actually do. *Usability News*, 8(1), 2006.

[35] K. Scarfone and M. Souppaya. Guide to enterprise password management: Recommendations of the national institute of standards and technology. *Gaithersburg, MD: US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology*, 2009.

[36] 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 *Symposium on Usable Privacy and Security (SOUPS)*, page 2. ACM, 2010.

[37] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: Implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 895–904. ACM, 2007.

[38] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[39] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. " i added'!'at the end to make it secure": Observing password creation in the lab. In *Symposium On Usable Privacy and Security (SOUPS)*, pages 123–140, 2015.

[40] P. C. Van Oorschot and S. Stubblebine. On countering online dictionary attacks with login histories and humans-in-the-loop. *ACM Transactions on Information and System Security (TISSEC)*, 9(3):235–258, 2006.

[41] R. Wash. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010.

[42] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the ACM Conference on Computer & Communications Security*, pages 162–175. ACM, 2010.

[43] J. Yan et al. Password memorability and security: Empirical results. *IEEE Security & Privacy*, (5):25–31, 2004.

[44] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the ACM Conference on Computer & Communications Security*, pages 176–186. ACM, 2010.

[45] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *APWG eCrime Summit*. IEEE, 2013.