Cognition and Predictors of Password Selection and Usability

Lila A. Loos(✉) and Martha E. Crosby(✉)

University of Hawai'i at Mānoa, Honolulu, HI 96822, USA
{lila7194,crosby}@hawaii.edu

Abstract. Computer passwords represent a secure authentication process used to access electronic information. Inconsequential of data storage location many of us utilize multiple unique computer passwords to access information on a daily basis. Since the design of password requirements are contingent upon the system provider, recalling various passwords is cognitively demanding and results in insecure practices such as writing down passwords visible to passerby. This study examines the task of password selection to improve human computer interaction. Categorizing personality through the locus of control internal and external scale and cognitive factors through memory associations advances understanding of password decision making. These classifications establish associations for predictive password selection informed by the behavioral decision process. This study addresses a design gap in the utility of passwords and describes quantified convergent dispositional factors gathered through valid instruments. Psychological fields of personality, memory cognition and behavioral decision making inform usability in the human computer interaction area of computer science.

Keywords: Authentication · Usability · Cognition · Memory · Password
Locus of control

1 Introduction

The goal of this study is to improve awareness of computer password selection and augment the security mechanism by evaluating locus of control and cognitive memory dynamics for human centered design enhancement. Most users choose short passwords to facilitate memorability and facilitate memorability with short passwords [27]. Studies excluding memorability from password security are able to determine the effect of visual password strength meters as a method to address security concerns with weak passwords. User behavior was positively affected by circumstantial messages from the strength meter resulting in users creating stronger passwords. Their meter was constructed with contextual information appealing to the users as well as a link providing training on password security [35]. Similarly, Jang-Jaccard and Nepal [34] argue for visual or biometric passwords as an option as they don't require memory.

Evaluating individual password decision making supports user centric factors. "While there is no silver bullet solution to the user authentication problem, it is still important to work toward improvements in password usage, security systems, and

D. D. Schmorrow and C. M. Fidopiastis (Eds.): AC 2018, LNAI 10916, pp. 117–132, 2018.
https://doi.org/10.1007/978-3-319-91467-1_10

understanding threats" [33, p. 78]. A study exposing the differences in awareness and practice of strong password use among college students found most authenticate utilizing seven passwords. As a result, a security awareness strategy established unique passwords for each login, changing passwords on a regular basis and keeping passwords private. In an effort to create passwords that are difficult to guess by hackers, it was suggested to make simple changes such as adding a symbol or upper-case letter to existing passwords [6].

Considering the number of unique passwords used for educational, personal and occupational purposes, "a solution to the problem of password security versus memorability has yet to be found" [25, p. 3761]. Additionally, this study of weak passwords employed persuasive technology to strengthen user security and memorability by inserting random characters into the password string. The experiment results improved password security for users with weak and strong original passwords, however, memorability was not improved for users with strong passwords. Likewise, Gehringer [26] recognizes that multiple password logins necessitate recording them for future retrieval and advises to involve the human component of security and memorability to future inquiry. As this study combines cognitive behavioral activities with technology, Choong [15] suggests a holistic approach to alleviate the memorability burden on users and brings attention to the need of usability research.

2 Human Computer Interaction: Usability

According to Norman [47] usability design combines psychology, computer science, engineering and analytical disciplines. Security is a technical issue imposed on humanity and disrupted by excessively complex technology measures that daunt employee behaviors leading to insecure conduct such as posting passwords in their work spaces in open view. A gap between usability and security is acknowledged and password usability is deserving of examination.

Jang-Jaccard's and Nepal [34] study addresses the relationship between usability and security resulting in higher recall between passphrases and self-selected passwords compared with random passwords. Unlike self-selected passwords, the passphrases withstood simulated dictionary and brute force attacks. Another memorability study indicated difficulty with learnability and recall when using more secure passwords [31]. Likewise, Greene et al. [28] agree that passwords are not memorable and security is threatened by compromised password data banks. Employing security and usability experts, the study measured the loss of security in passwords specific to the multiple keyboards presented on mobile devices. Results define effectiveness measured through password or character login success and failures; efficiency is measured by the length of time it takes to enter a password and satisfaction is measured through subjective user experiences. Similarly, Grassi et al. [27] define usability as the "extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" (p. 61). Choong [15] argues that usability is the main concern for users managing multiple passwords.

> Research focusing on human factors and usability of passwords has been challenging the view that users are the primary cause for cyber security issues and pointing out that security policies are often imposing unreasonable requirements and pushing users' cognitive limits. (p. 128)

Although people prefer to use memorable passwords, favoring usability over security presents authentication risks to defending systems as the goals between usability and security are dissimilar [2]. Likewise, Choong [15] suggests collaboration among interdisciplinary influences to discover the intersection between security and usability and acknowledges the need for research to ensure security while reducing the burden on users. Considering the weakest link in security systems are individuals, human computer interaction principals rooted in psychology and cognition impact behavior and warrant further study to improve the authentication processes.

Norman [48] argues "without usable systems, the security and privacy simply disappear as people defeat the processes in order to get their work done" and furthermore, "the more secure you make something, the less secure it becomes" (p. 60). Security professionals attest to challenges between security and usability that trigger insecure behaviors in response to usability difficulties. "The reasonableness of the effort required" (p. 61) to comply with security requirements is a design issue yet to be solved. Renaud's et al. [52] framework considers usability and offers authentication options for decision makers based on their system requirements and preferences. The value given to a resource is aligned with the authentication method. Alternative authentication allows the decision maker to personalize memorability and risk mitigation properties such as strength of password. This framework considers the quality of password authentication for the business and the user as an alternative approach to computer security.

3 Risk Assessment and Authentication

Risk assessments examine computer authentication, human computer interaction and fiscal responsibilities to secure information systems. Grassi et al. [27] defines authentication as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources" (p. 47). Additionally, an authentication secret is a "value that an attacker could use to impersonate the subscriber in an authentication protocol" (p. 47). Passwords are defined as "a type of authenticator comprised of a character string to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process" (p. 54). This study considers passwords an authentication secret and investigates the process of password construction and memorability to impede risk.

Security insurance levels examined by protection requirements create digital authentication realities affecting anyone who accesses an information system through a login dialogue. The interface is primarily evaluated by the user who adheres to the login requirements or who may create a supplemental coping mechanism to successfully authenticate. Grassi et al. [27] integrates organizational risk to operational security practice.

> The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, resulting from the operation of a system. It is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (p. 59)

Organizational risk focuses on insider threats to computer security systems. Unlike external exploiters, privileged users hold company knowledge threatening the integrity of information systems. Nurse et al. [49] explores the impact of fraud, theft of intellectual property, and sabotage of infrastructure and provides insight to detecting and preventing malicious behavior utilizing automated analytical tools along with policy awareness to protect organizations. An environment in which access to information is controlled by users compels memorable password authentication, devoid of non-secure actions such as writing down passwords that are difficult to recall. According to Choong et al. [16] "an alarming finding is that employees seem to have a false perception of security around their work-related accounts" (p. 13) and consider prevention of system attacks and security breaches the responsibility of their organization. Furthermore, these Federal employees prescribe to the notion that government work is transparent to the public and without consequences resulting from a system compromise.

Organizational property risk is pivotal to security and requires assessing types of authentication attacks, secrets uncovered, stolen, or tampered, copied intellectual property and replication of user identity [27]. Watkins [64] value assessment of information security is estimated by the impact of the following values: "Risk = Likelihood $\times$ Impact Relationship" (p. 22). The possible vulnerabilities and impact range from very low to very high and apply to all risk involving information assets and security. Calder [11] recommends assessing risk with goals to remove, reduce, tolerate or transfer risk through a contract such as an insurance policy to protect organizations from business harm. Furthermore, a risk management plan identifies action, responsibilities, and priorities of information security while management details changes, corrective and preventative action, and recommends improvement.

An alternative study suggested by Cavusoglu et al. [12] involve game theory as a security investment decision maker.

> The firm's payoff from security investment depends on the extent of hacking it is subjected to. The hacker's payoff from hacking depends on the likelihood he or she will be caught. Thus, the likelihood of the firm getting hacked depends on the likelihood the hacker will be caught, which, in turn, depends on the level of investment the firm makes in IT security. (p. 90)

Selecting the preventative scheme results in maximum savings. Therefore, each recommended security option is weighed against its cost and estimated intrusion parameters. Cost savings are determined by comparing the cost of implementing or not implementing security technology.

Risk assessments indicate password attack methods involve guessing by brute force or dictionary listing of words, guessing, eavesdropping, social engineering, and physical presence. Since text passwords continue to be the dominating login for authentication, Ives et al. [33] exploit reuse of passwords for multiple accounts to obtain higher level system access. Furthermore, authenticating to e-commerce sites

using the same password presents security risks for the user as hackers could obtain access to multiple sites, "there is an obvious and probably sizeable overlap between AOL and Citibank or BankOne and Amazon.com customers" (p. 75). Jang-Jaccard and Nepal [34] discuss the significance of acquiring passwords through deceptive practices: cyber-attacks by malware phishing or injecting computer code to obtain a database of passwords using unsecure technologies such as Wi-Fi or Bluetooth connections. Defense mechanisms include locking an account after failed attempts, establishing secure connectivity during communication, and enforcing password requirements [28]. Although password managers address memorability by collecting user identification and passwords used on various web sites, such tools become susceptible to attack [57]. Aurigemma et al. [4] suggest password managers provide a security mechanism for home-end users however their investigation discovered that insufficient time was the main inhibitor to adoption followed by threat apathy or lack of password security threats.

Growing threats to technology and malicious attack patterns compel security policies to embrace usability and safeguard information systems. Adams and Sasse [1] recognize the shift to user centric design of security systems by determining how their systems are utilized. Although text-based passwords pose a security risk to dictionary attacks [14, 65], Wu's [65] study allows the use of simple passwords defended by encryption against such attacks. Notwithstanding user involvement risk in security technology, passwords and usability are coupled in human computer interaction and form the basis of this study.

4 Authentication and the Human Factor of Text Passwords

According to Norman [47] password security continues to be problematically a human element. In response to security procedures paired with bad password policies, the human factor creatively adapts to solve forgotten password problems. As the majority of individuals compose passwords using the name of a person, place or thing, date, and number, Brown et al. [9] suggest passwords to be easily recalled by the user and not others. Nevertheless, the conditions of creating a password are often rushed without much time for thoughtful composition. In response to security concerns, mechanisms exist to warn users of insecure password fields on web browsers [36].

Creating a password is one part of the authentication process. Users participate in a password lifecycle system to generate, maintain, and authenticate using a process comprised of goals, constraints, memory storage, and authentication experiences that influence the recurrence of password selection [15]. This repetitive method includes individual factors such as attitudes, motivations, and emotions to comply with password requirements and individual needs. Workarounds to password memorability utilize a special character and digit to user generated passwords or created a password from the first letter of a phrase [62]. Having the user login multiple times produced secure and memorable passwords. Varying password requirements include regularly changing passwords circumvent memorability [61]. Additionally, their study suggests short-term recall testing, unlike immediately using the password, improves password retention since retrieval is from long term retention rather than from working memory.

Furthermore, using a mnemonic method to generate a password containing the first letter of a phrase along with a maximum of three attempts to authenticate is recommended to overcome the security and memorability tradeoff.

Once a password is generated, it is combined with random data or salt which is then cryptographically hashed before it is stored in a database. During authentication, the password is decrypted and compared with the stored salted hash [28]. Bonneau et al. [8] recognize the unbalance between security and authentication and focus on uniting their differing roles. Although passwords were initially designed to access mainframe systems, today's graphical environment is dominated by web authentication.

> Failure to recognize the broad range of usability, deployability, and security challenges in Web authentication has produced both a long list of mutually incompatible password requirements for users and countless attempts by researchers to find a magic-bullet solution despite drastically different requirements in different applications. No single technology is likely to 'solve' authentication perfectly for all cases: a synergistic combination is required. (p. 79)

Usability calls for examinations in password selection united with security. Komanduri et al. [37] study of password policies on password strength and user behavior found that crafting a password policy using 16-characters without additional requirements provides greater resistance to brute force attacks with an increase in usability compared with eight-characters containing a number and symbol requirement.

5 Cognition and User Behavior of Text Passwords

According to Michaelian and Sutton [44] "cognitive science is the interdisciplinary study of mind and intelligence, embracing philosophy, psychology, artificial intelligence, neuroscience, linguistics, and anthropology" (p. 1). Norman [46] combines cognition with emotion as part of the psychology of design. "Cognition provides understanding: emotion provides value judgements. A human without a working emotional system has difficulty making choices. A human without a cognitive system is dysfunctional" (p. 47). The study emphasizes emotion produced from well-designed devices can lead to pleasure or despair and poses the question, "do we count our technology as an extension of our memory systems" (p. 46). "It is one thing to have to memorize one or two secrets: a combination, or a password, or the secret to opening a door. But when the number of secret codes gets too large, memory fails" (p. 86). Memory overload is addressed by using few passwords for multiple logins. "Even security professionals admit to this, thereby hypocritically violating their own rules" (p. 87). Furthermore, complex passwords stymie memory leading to security violations by employees who use external memory options such as paper to aid in password retrieval.

Users employ risky behaviors when engaging in simple passwords, writing down or sharing passwords and not changing passwords on a regular basis [64]. Simple passwords manifest as "proper names and birthdays are the primary information used in constructing passwords, accounting for about half of all passwords. Almost all respondents reuse passwords" [9, p. 641]. Study results found that participants had a mean of about eight passwords and half are unique.

Individuals with numerous passwords inherit usability problems; a decrease in memorability was associated with an increase in cognitive overhead [1]. Likewise, insecure password behaviors are a result of insufficient awareness of password procedures and security threats like password cracking [1]. Similarly, Florencio's and Herley [23] study of more than 500,000 users each having 25 accounts who use an average of eight passwords a day, resulted in participants remembering groups of passwords through combinations of memory, writing them down, and password resets. Users select weak passwords consisting mostly of lowercase letters, unless required to use uppercase and special characters, and reuse passwords for multiple authentication across websites. Moreover, a case study of Federal employees resulted in an average of nine accounts requiring logins. Twenty five percent of employees managed 11 through 20 passwords. Password requirements are considered complex with frequent changes. Frustrations of mistyping and forgetting often resulted in getting locked out of their account make the password management lifecycle of generating and tracking troublesome. Eighty one percent of respondents prefer passwords that are easy to remember and prefer a single sign on system [16]. Pilar et al. [51] acknowledge the need to improve password-based authentication procedures. Their study showed respondents utilized approximately eight passwords of which at least one password is reused. Memory difficulties in the form of forgetting or mixing up passwords increased with groups using multiple unique passwords. Password lengths increased with the younger and more educated group.

To overcome excessive demands on memory, España [22] examined a technique that combines pieces of information that result in positive memorability for standard passwords and not for multiword or mnemonic passwords. An approach by Tam et al. [59] suggest that users select common passwords based on convenience. "Focusing on the user is important because, although stronger authentication techniques are available, corporations tend to continue to use a password-based system to control system access" (p. 233). Therefore, understanding why users mismanage passwords is essential to enhancing password behavior. Their study showed that users value convenience even though compromising password practices could lead to security breaches of their personal data. Such findings are a result of users placing emphasis on near versus distant future events. Thus, importance of convenience or feasibility of a near future event is favored over the security of a distant future event. However, the study suggests that stronger passwords are chosen for bank accounts than for email accounts resulting in a tradeoff between convenience and security.

Norman [46] explains the encoding of mnemonic phrases help memory retention as it is affected by time and quantity. "Most of us can't (remember all these secret things) even with the use of mnemonics to make some sense of nonsensical material" (p. 88). Users cognitively problem-solve and reason when selecting characters to create a password [15]. Factors affecting the authentication process include the frequency of use, maintenance and interferences from other passwords.

In addition to the great number of complex passwords and memory overload, Greene et al. [29] detail increased task constrictions on mobile devices; it is an overall challenging authentication method requiring smaller keys, multiple character keyboards and task interruptions associated with switching screens. Their study of 158 participants averaging 33.2 years in age suggests constraints of password recall between mobile and desktop platforms.

6 Locus of Control Personality Variables

Applying psychological variables of locus of control to technology is expected to increase understanding of personality influences on the selection and construction of computer passwords and contribute to the design of memorable passwords. This study operationalizes internal and external locus of control as an influencer to decision making in computer security. Individuals respond to perception based on attitudes and behavior. External control "is typically perceived as the result of luck, chance, fate, as under the control of powerful others, or as unpredictable because of the great complexity of the forces surrounding him" while internal control is "contingent upon his own behavior or his own relatively permanent characteristics" [53, p. 1]. Based on social learning theory, the relationship between behavior and consequences is evident in Rotter's [53] hypotheses "when the reinforcement is seen not contingent upon the subject's own behavior that its occurrence will not increase an expectancy as much as when it is seen as contingent" (p. 2). Furthermore, "once a person has established a concept of randomness or chance the effects of reinforcement will vary depending upon what relationship he assigns to the behavior reinforcement sequence" (p. 4). Therefore, a person's internal (skill) control or external (chance) control variable affects reinforcement and subsequently, behavior. The study determined that same situations are considered differently depending if the individual's personality is characteristic of internal or external control factors and predictions of behavior can then be determined. Likewise, reinforcement is perceived as:

> Learning processes such that people with a belief in internal control are more likely to change their behavior following a positive or negative reinforcement than are people with a belief in external control. For behavior change to occur, however, the reinforcement must be of value to the person. [42, p. 251]

Various technology studies apply locus of control to better understand user behavior. Coovert and Goldstein [18] demonstrate the use of locus of control to understand how employees perceive computer related changes in the work environment; internal control personnel resulted with a higher positive attitude compared with external control personnel. Chak and Leung [13] suggest external locus of control or trust on chance contributes to Internet addiction disorder. Li et al. [39] indicate internal locus of control individuals are more likely to regulate mobile phone use to not interfere with their well-being. Fong's et al. [24] research on the re-adoption of mobile phone applications determined that locus of control is an influencer through self-efficacy. Individuals with internal locus of control are driven by success and are likely to overcome operational difficulties with the mobile applications and adopt reuse.

Specialized studies [10, 32, 41, 45, 55, 58, 63] modify locus of control's general internal and external variables instrument to determine control beliefs and behavior in various sectors including consumer strategic shopping, e-learning systems, organizational impression management, meta-analysis of well-being including motivation and behavioral orientation, preventive tobacco, work settings, and health care.

Alternate scale formats deviate from Rotter's [53] forced choice instrument. Studies opting for Likert's multidimensional scale [3, 40] measure social and cultural situations and aspects pertaining to personal well-being. Supported by Rotter [53], the locus of

control internal-external scale "correlates satisfactorily with other methods of assessing the same variable such as questionnaire, Likert scale, interview assessments, and ratings from a story-completion technique" (p. 25).

Although Rotter's [53] locus of control is a unified measurement of personality constructs by design, Lange and Tiggemann [38] suggest multidimensionality in the widely used personality scale consisting of 29 questions on topics such as "social-political events, social recognition, academic recognition and general life philosophy" (p. 398). However, Rotter [54] argues for instrument validity to generalize situational reinforcement of internal or external control variables for potential behavior expectancy where "expectancies in each situation are determined not only by specific experiences in that situation but also, to some varying extent, by experiences in other situations that the individual perceives as similar" (p. 57). Moreover, Ng et al. [45] operationalize locus of control as a continuous variable using Rotter's [53] scale to predict workplace attitudes and behavioral intent to control.

7 Memory Cognition Factor

This study identifies memory aptitude factor using Ekstrom's et al. [21] cognitive tests. Although "there are probably no such things as truly 'pure' factors, a study of individual differences in abilities can profit greatly if it is closely tied to the experimental analysis of particular cognitive tasks" (p. 3). Memory cognition is explored to better understand password recall abilities.

Baddeley [5] defines working memory as "temporary storage and manipulation of the information necessary for such complex tasks as language comprehension, learning, and reasoning" which "evolved from the concept of a unitary short-term memory system" (p. 556). Additional findings associate memory cognition with attention and behavior control. Similarly, the ability to encode active information to long-term memory corresponds with maintaining information in working memory aided by attention control [60]. Moreover, working memory's storage and attention control operations have the ability to sidestep disturbances; increased awareness in a discipline contributes to working memory capacity [17]. Norman [46] suggests information stored in working memory disappears with distraction. Therefore, it is suggested to portray information in various forms to enhance memory recall.

Although immediate memory retrieval is described as effortless recollection, recollection difficulty increases as time passes [46]. Without repetition, working memory's capacity is seven items compared with 10 or 12. Since recalling arbitrary items like passwords is considerably challenging, individuals learn to develop associations by creating organization. Generating meaningful understanding to mixtures of characters, numbers, and symbols is an effective memorability technique. Recalling a password whose length is greater than working memory capacity or numerous passwords with diverse conditions is yet to be solved. Continued development is vital to enhance interfaces and interaction toward usable security [48].

8 Behavioral Decision Theory

Decision making is an action mechanism encountered by individuals during the construction of computer passwords as is organized by gathering information and evaluating alternatives to reach a specified goal.

> The importance of behavioral decision theory lies in the fact that even if one were willing to accept instrumental rationality as the sole criterion for evaluating decisions, knowledge of how tasks are represented is crucial since people's goals form part of their models of the world. [20, p. 60]

Decision behavior is subject to information processing of the task resulting from a cost benefit approach. Evaluating decision promptness against effort are deliberated resulting in lessening alternatives or processing complexity. Cost benefit is characterized as effort error [50].

> Furthermore, the cost of thinking is simply the number of comparisons that are made. The number of comparisons is seen as a function of (a) the desired probability of making a correct choice and (b) the difficulty of making a choice. (p. 396)

Additional studies [20, 50] imply decision strategies depend on past learning experiences of task variables and expected cost. Consequently, while comparisons between high benefit and low-cost decision outcomes create a good decision, Higgins [30] suggests regulatory fit increases the choice value of judging criteria. The favored result produces experiences of motivation and positivity of the decision-making process. Accordingly, decision making is dependent upon a cost benefit framework where the cost of the resource is attributed to the most advantageous result selected [7]. Although personality factors contributing to decision making are ignored because of lack of priori research, the study acknowledges individual characteristics, opinions, perception and knowledge factors leading to a decision. Simplifying alternatives in the decision-making process produces an alternative measurement of the cost of thinking [54].

Norman [47] argues emotion is cognition's necessary partner of judgments that enhance our decision-making process. Influencing behavior are cognitive and emotional factors that interplay in determining how we respond to technical problems with security. The elements specific to this study examine psychology factors and the assessment of memory encoding and decoding capacity that are associated with the decision-making process of creating passwords.

9 Methodology

The purpose of this study is to improve attentiveness of computer password selection and heighten the security mechanism by presenting design conclusions based on results. Outcomes from descriptive quantitative research will suggest associations between the operationalized variables and the represented population. Rooted in psychological variables and memory cognition constructs, assessments in control beliefs are applied to technology to predict security-based behavior. Results will increase

understanding of personality influences and password recall abilities on the selection and construction of passwords to enhance human centered design.

The significance of personality and cognitive factors has serious and practical applications addressing information security and usability. Contributions from user interpretations drive reinforcement of personal traits and its association with behavior. The combination of theoretical perspectives provides objective methods of assessment for predictive technological decision making. "Cognitive style research is based on Carl Jung's 1921 premise that the mental functions related to information gathering and decision making are central to one's personality" [43, p. 811]. Their predictive Internet acceptance study operationalized personality and cognitive dispositional factors that had been ignored in prior research. Although personality resulted as a predictor of Internet adoption, other measures of cognitive style may be influencers.

The research instruments consist of Rotter's Locus of Control Internal External self-evaluation questionnaire, Memory Associative Factor-Referenced Cognitive Tests), Password Selection Survey (Appendix) and Password Recall Survey. These mechanisms operate to produce a descriptive quantitative research study in two phases. The first phase pilots a study of adult university computer science students with objectives to test the validity of the instruments. The second phase applies the research methods to a larger study consisting of an employee population who authenticate to business applications with multiple passwords.

The data collected will not contain personal information. To ensure confidentiality, the research data will not be shared with anyone. To ensure anonymity, no identifying characteristics are recorded on the data and therefore, the researcher will not know who contributes a given piece of data. Pseudonyms may be used to report findings in a way that protects privacy and confidentiality. Participating in either study is optional.

The statistical analysis on the data collected will be logged and represented as patterns of decision making to determine relationships in answering the research questions. ANOVA will determine the main effects and interactions among the locus of control and memory associative factors and password selection. Correlation and linear regression will determine the relationships among the personality and cognitive factors and password selection. ANOVA is designed to contribute to decision making about the differences among the personality groups and selected passwords that contribute to usability. Depending on the sample size, either the z-test or t-test that compare the means of populations will be analyzed along with the f-ratio that finds variance or measure of sample dispersion from the mean.

10 Future Studies

Enhancing authentication security involves incorporating augmented cognition in the usability equation. Considerations of physiological measures enhance psychological factors and further understanding in behavioral decision making of password construction. Future sensory input measurements from eye movements and body heat including perspiration support opportunities to discover cognitive variable associations in the design of system interfaces that aid memorability.

Appendix

Password Selection Survey

Introduction. From the Desk of Thomas F. Duffy, Chair, MS-ISAC
Cybersecurity experts continually identify the use of strong, unique passwords as one of their top recommendations. However, this is also one of the least commonly followed recommendations because unless you know the tricks, it's difficult to remember strong, unique passwords for every login and website.

Why Strong, Unique Passwords Matter
Cybersecurity experts make the recommendation for strong, unique passwords for several reasons – the first being that every day malicious cyber threat actors compromise websites and online accounts, and post lists of usernames, email addresses, and passwords online. This exposes people's passwords, and worse yet, they are exposed with information that uniquely identifies the user, such as an email address. That means that a malicious actor can look for other accounts associated with that same person, such as work related, personal social media, or banking accounts. When the malicious actor finds those accounts, they can try logging in with the exposed password and if the password is reused, they can gain access. This is why unique passwords matter.
Secondly, when malicious cyber threat actors can't easily find or a guess the password, they can use a technique called brute forcing. This is a technique where they try every possible password until the correct password is identified. Computers can try thousands of passwords per second, but for this technique to be worthwhile, the malicious cyber threat actor needs the password to be easy to identify, which is why a strong password matters. The stronger the password the less likely brute forcing will be successful.

When malicious actors use brute forcing techniques they often try every word in the dictionary because it's easier to remember words than random letter combinations. This technique is not limited to English-language dictionaries, so switching languages will not help. And since many passwords require a combination of uppercase and lowercase letters, numbers, and symbols, the malicious actors rely on human instinct to narrow down the possibilities. For instance, most users when faced with choosing a password that fits these requirements, will pick a word, put the uppercase letter first, and end the password with the number and symbol. Alternatively, many people will replace common letters with a number or symbol that represents that letter. This changes a common password, such as "password," into the only slightly more complex password of "p@ssw0rd," which is still an easy to guess pattern.

Another technique to assist in building strong, unique passwords, is to choose a repeatable pattern for your password, such as choosing a sentence that incorporates something unique about the website or account, and then using the first letter of each word as your password. For example, the sentence: "This is my January password for the Center for Internet Security website." would become "TimJp4tCfISw." This password capitalizes 5 letters within the sentence, swaps the word "for" to the number "4," and adds the period to include a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern.

Variations on this technique include using the first letters from a line in a favorite song or a poem.

1. Select the most memorable password from the following list of random passwords:
   (a) ksitjgJ8@9
   (b) i5euyrpAT(
   (c) TimMp4ticsPSRp
   (d) 2jU40t#fBa
   (e) tcJotr2atM
2. Modify one of the passwords in question #1 shown above to make it memorable for you. You may also select one of the given random passwords.
3. Enter a strong password of your choice that is memorable for you. A strong password is a unique password that is only used with one account and follows the following format. The password should be at least ten (10) characters in length and include uppercase and lowercase letters, at least one number, and at least one symbol.
4. Describe how you created the strong password and made it memorable for you

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999)
2. Andriotis, P., Tryfonas, T., Oikonomou, G.: Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 115–126. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_11
3. Ashkanasy, N.M.: Rotter's internal-external scale: confirmatory factor analysis and correlation with social desirability for alternative scale formats. J. Pers. Soc. Psychol. **48** (5), 1328 (1985)
4. Aurigemma, S., Mattson, T., Leonard, L.: So much promise, so little use: what is stopping home end-users from using password manager applications? In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
5. Baddeley, A.: Working memory. Science **255**(5044), 556–559 (1992)
6. Bain, L.Z., Hayden, M., Sneesby, S.: An empirical study of user authentication: the perceptions versus practice of strong passwords. Issues Inf. Syst. **XI**(1), 256–265 (2010)
7. Beach, L.R., Mitchell, T.R.: A contingency model for the selection of decision strategies. Acad. Manag. Rev. **3**(3), 439–449 (1978)
8. Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F.: Passwords and the evolution of imperfect authentication. Commun. ACM **58**(7), 78–87 (2015)
9. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Appl. Cogn. Psychol. **18**(6), 641–651 (2004)
10. Busseri, M.A., Lefcourt, H.M., Kerton, R.R.: Locus of control for consumer outcomes: Predicting consumer behavior. J. Appl. Soc. Psychol. **28**(12), 1067–1087 (1998)
11. Calder, A.: ISO27001/ISO27002 A Pocket Guide. IT Governance Pub (2008)
12. Cavusoglu, H., Mishra, B., Raghunathan, S.: A model for evaluating IT security investments. Commun. ACM **47**(7), 87–92 (2004)
13. Chak, K., Leung, L.: Shyness and locus of control as predictors of internet addiction and internet use. CyberPsychol. Behav. **7**(5), 559–570 (2004)

14. Chang, T.Y., Tsai, C.J., Lin, J.H.: A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. J. Syst. Softw. **85**(5), 1157–1165 (2012)
15. Choong, Y.-Y.: A cognitive-behavioral framework of user password management lifecycle. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 127–137. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_12
16. Choong, Y.Y., Theofanos, M., Liu, H.K.: United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study. US Department of Commerce, National Institute of Standards and Technology (2014)
17. Conway, A.R., Cowan, N., Bunting, M.F., Therriault, D.J., Minkoff, S.R.: A latent variable analysis of working memory capacity, short-term memory capacity, processing speed, and general fluid intelligence. Intelligence **30**(2), 163–183 (2002)
18. Coovert, M.D., Goldstein, M.: Locus of control as a predictor of users' attitude toward computers. Psychol. Rep. **47**(3_suppl), 1167–1173 (1980)
19. Duffy, T.F.: Why Strong, Unique Passwords Matter - Office of Enterprise (n.d.). http://ets.hawaii.gov/why-strong-unique-passwords-matter. Accessed 8 Feb 2018
20. Einhorn, H.J., Hogarth, R.M.: Behavioral decision theory: processes of judgement and choice. Annu. Rev. Psychol. **32**(1), 53–88 (1981)
21. Ekstrom, R.B., Dermen, D., Harman, H.H.: Manual for Kit of Factor-Referenced Cognitive Tests, vol. 102. Educational Testing Service, Princeton (1976)
22. España, L.Y.: Effects of password type and memory techniques on user password memory. Psi Chi J. Psychol. Res. **21**(4) (2016)
23. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657–666. ACM (2007)
24. Fong, L.H.N., Lam, L.W., Law, R.: How locus of control shapes intention to reuse mobile apps for making hotel reservations: evidence from Chinese consumers. Tour. Manag. **61**, 331–342 (2017)
25. Forget, A., Biddle, R.: Memorability of persuasive passwords. In: CHI 2008 Extended Abstracts on Human Factors in Computing Systems, pp. 3759–3764 (2008). https://doi.org/10.1145/1358628.1358926
26. Gehringer, E.: Choosing passwords: security and human factors. In: Proceedings of the IEEE 2002 International Symposium on Technology and Society (ISTAS 2002). Social Implications of Information and Communication Technology, (Cat. No.02CH37293) (2002). https://doi.org/10.1109/istas.2002.1013839
27. Grassi, P.A., Garcia, M.E., Fenton, J.L.: Digital identity guidelines (2017). https://doi.org/10.6028/NIST.SP.800-63-3
28. Greene, K.K., Franklin, J.M., Greene, K.K., Kelsey, J.: Measuring the Usability and Security of Permuted Passwords on Mobile Platforms. US Department of Commerce, National Institute of Standards and Technology (2016)
29. Greene, K.K., Gallagher, M.A., Stanton, B.C., Lee, P.Y.: I can't type that! P@$$w0rd entry on mobile devices. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 160–171. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_15
30. Higgins, E.T.: Making a good decision: value from fit. Am. Psychol. **55**(11), 1217 (2000)
31. Hub, M., Capek, J., Myskova, R.: Relationship between security and usability-authentication case study. Int. J. Comput. Commun. **5**, 1–9 (2011)
32. Hsia, J.W., Chang, C.C., Tseng, A.H.: Effects of individuals' locus of control and computer self-efficacy on their e-learning acceptance in high-tech companies. Behav. Inf. Technol. **33**(1), 51–64 (2014)
33. Ives, B., Walsh, K.R., Schneider, H.: The domino effect of password reuse. Commun. ACM **47**(4), 75–78 (2004)

34. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. **80**(5), 973–993 (2014)
35. Khern-am-nuai, W., Yang, W., Li, N.: Using context-based password strength meter to nudge users' password generating behavior: a randomized experiment (2016)
36. Kolb, N., Bartsch, S., Volkamer, M., Vogt, J.: Capturing Attention for Warnings about Insecure Password Fields - Systematic Development of a Passive Security Intervention (2014). https://doi.org/10.1007/978-3-319-07620-1_16
37. Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F., Egelman, S.: 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)
38. Lange, R.V., Tiggemann, M.: Dimensionality and reliability of the Rotter IE locus of control scale. J. Pers. Assess. **45**(4), 398–406 (1981)
39. Li, J., Lepp, A., Barkley, J.E.: Locus of control and cell phone use: implications for sleep quality, academic performance, and subjective well-being. Comput. Hum. Behav. **52**, 450–457 (2015)
40. Lumpkin, J.R.: Validity of a brief locus of control scale for survey research. Psychol. Rep. **57**(2), 655–659 (1985)
41. Madan, P., Srivastava, S.: Investigating the personality variable (LOC) & impression management relationship: exploring the role of demographic variables & sectoral difference of managers. OPUS **7**(1), 52–71 (2016)
42. Marks, L.I.: Deconstructing locus of control: Implications for practitioners. J. Couns. Dev. **76**(3), 251–260 (1998)
43. McElroy, J.C., Hendrickson, A.R., Townsend, A.M., DeMarie, S.M.: Dispositional factors in internet use: personality versus cognitive style. MIS Q. **31**, 809–820 (2007)
44. Michaelian, K., Sutton, J.: Memory. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (2017). https://plato.stanford.edu/archives/sum2017/entries/memory
45. Ng, T.W., Sorensen, K.L., Eby, L.T.: Locus of control at work: a meta-analysis. J. Organ. Behav. **27**(8), 1057–1087 (2006)
46. Norman, D.: The Design of Everyday Things: Revised and Expanded Edition. Basic Books AZ, New York (2013)
47. Norman, D.A.: Emotional Design: Why We Love (or Hate) Everyday Things. Basic Civitas Books, New York (2004)
48. Norman, D.A.: THE WAY I SEE IT when security gets in the way. Interactions **16**(6), 60–63 (2009). https://doi.org/10.1145/1620693.1620708
49. Nurse, J.R.C., Legg, P.A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., Creese, S.: A critical reflection on the threat from human insiders – its nature, industry perceptions, and detection approaches. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 270–281. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_24
50. Payne, J.W.: Contingent decision behavior. Psychol. Bull. **92**(2), 382 (1982)
51. Pilar, D.R., Jaeger, A., Gomes, C.F., Stein, L.M.: Passwords usage and human memory limitations: a survey across age and educational background. PLoS One **7**(12), e51067 (2012)
52. Renaud, K., Volkamer, M., Maguire, J.: ACCESS: describing and contrasting. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 183–194. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_17
53. Rotter, J.B.: Generalized expectancies for internal versus external control of reinforcement. Psychol. Monogr.: Gen. Appl. **80**(1), 1 (1966)

54. Rotter, J.B.: Some problems and misconceptions related to the construct of internal versus external control of reinforcement. J. Consult. Clin. Psychol. **43**(1), 56 (1975)
55. Sheffer, C., MacKillop, J., McGeary, J., Landes, R., Carter, L., Yi, R., Jones, B., Christensen, D., Stitzer, M., Jackson, L., Bickel, W.: Delay discounting, locus of control, and cognitive impulsiveness independently predict tobacco dependence treatment outcomes in a highly dependent, lower socioeconomic group of smokers. Am. J. Addict. **21**(3), 221–232 (2012)
56. Shugan, S.M.: The cost of thinking. J. Consum. Res. **7**(2), 99–111 (1980)
57. Silver, D., Jana, S., Boneh, D., Chen, E.Y., Jackson, C.: Password managers: attacks and defenses. In: USENIX Security Symposium, pp. 449–464 (2014)
58. Spector, P.E.: Development of the work locus of control scale. J. Occup. Organ. Psychol. **61** (4), 335–340 (1988)
59. Tam, L., Glassman, M., Vandenwauver, M.: The psychology of password management: a tradeoff between security and convenience. Behav. Inf. Technol. **29**(3), 233–244 (2010)
60. Unsworth, N., Fukuda, K., Awh, E., Vogel, E.K.: Working memory and fluid intelligence: capacity, attention control, and secondary memory retrieval. Cogn. Psychol. **71**, 1–26 (2014)
61. Vu, K.L., Cook, J., Bhargav-Spantzel, A., Proctor, R.W.: Short- and long-term retention of passwords generated by first-letter and entire- word mnemonic methods. In: Proceedings of the 5th Annual Security Conference, Las Vegas, NV, pp. 1–13 (2006). https://doi.org/10.15417/1881
62. Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., Schultz, E.E.: Improving password security and memorability to protect personal and organizational information. Int. J. Hum Comput Stud. **65**(8), 744–757 (2007). https://doi.org/10.1016/j.ijhcs.2007.03.007
63. Wallston, B.S., Wallston, K.A., Kaplan, G.D., Maides, S.A.: Development and validation of the health locus of control (HLC) scale. J. Consult. Clin. Psychol. **44**(4), 580 (1976)
64. Watkins, S.G.: An introduction to information security and ISO27001. IT Governance Pub (2008)
65. Wu, T.D.: A real-world analysis of Kerberos password security. In: NDSS (1999)