Spring 2021

Authentication Schemes' Impact on Working Memory

Janine D. Mator
Old Dominion University, jdmator@gmail.com

AUTHENTICATION SCHEMES' IMPACT ON WORKING MEMORY

by

Janine D. Mator
B.A. August 2016, Michigan State University

A Thesis Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

PSYCHOLOGY

OLD DOMINION UNIVERSITY
May 2021

Approved by:

Jeremiah D. Still (Director)

Jing Chen (Member)

Krystall Dunaway (Member)

ABSTRACT

AUTHENTICATION SCHEMES' IMPACT ON WORKING MEMORY

Janine D. Mator
Old Dominion University, 2021
Director: Dr. Jeremiah D. Still

Authentication is the process by which a computing system validates a user's identity. Although this process is necessary for system security, users view authentication as a frequent disruption to their primary tasks. During this disruption, primary task information must be actively maintained in working memory. As a result, primary task information stored in working memory is at risk of being lost or corrupted while users authenticate. For over two decades, researchers have focused on developing more memorable passwords by replacing alphanumeric text with visual graphics (Biddle et al., 2012). However, very little attention has been given to the impact authentication has on working memory. A recent exploratory study suggests that working memory can be disrupted during graphical authentication (Still & Cain, 2019). In this study, we take the next step by controlling for task difficulty and contrasting performance with conventional password-based authentication. Baddeley's model was employed to examine the impact of authentication on verbal, visuospatial, and central executive working memory (Baddeley & Hitch, 1974). Our findings may help designers select authentication systems that minimize adverse effects on users' critical primary task performance. For instance, we revealed that conventional passwords do not have a greater negative impact on verbal primary task information compared to graphical passcodes. We also replicated findings reported by Still and Cain (2019), where visuospatial was least impaired by authentication. These findings are not

intuitive, highlighting the need for further investigation of how authentication impacts primary task information in working memory.

ACKNOWLEDGMENTS

There are more than a few people who deserve my gratitude for their support. My research adviser, Dr. Jeremiah Still, has been a well of encouragement and constructive feedback from start to finish. Thank you to my other committee members, Dr. Jing Chen and Dr. Krystall Dunaway, for their time and insight that has improved my research. I am also thankful to my family, whose support is still felt as far as 700 miles away; my close friend Renee Shedlock, for her contagious laughter when I need it most; my wonderful partner, Guilford Stancill, for keeping me silly but grounded; my fellow lab mates, especially John Hicks, Alex Proaps, Paige DuPlantis, and Lauren Tiller; and all of my other Norfolk companions who have made this a worthwhile odyssey.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Figure Page

CHAPTER I

INTRODUCTION

Alphanumeric passwords have been a ubiquitous method of authentication since the 1960s (Sobrado & Birget, 2002). Although their continued deployment can be attributed to benefits such as convenience and low cost (Herley & Oorschot, 2011), their security has long been of concern (Morris & Thompson, 1979). Billions of passwords have been stolen through brute-force attacks (Perlroth & Gelles, 2014), in which an automated program inputs different combinations of password characters until the correct combination is found (Curtin, 2005; Kirushnaamoni, 2013). Some brute-force attacks are especially effective at cracking weak passwords (Herley & Florêncio, 2008), which contain dictionary words, predictable patterns such as "1234," or personal information, such as birthdays (Vu et al., 2007; Weir et al., 2010). According to a report from Verizon Data Breach Investigations (2017), weak or stolen passwords are responsible for more than 80% of breaches. To the user, of course, weak passwords are appealing because they are easier to remember than strong ones (Wright et al., 2012). In addition to omitting dictionary words and personal information, strong passwords typically require a minimum length of eight characters, a mix of upper and lowercase letters, and at least one number and special character (Raderman, 2017).

The security risk of weak passwords is escalated when users engage in poor cyber hygiene (Pfleeger & Caputo, 2012); for example, intentionally sharing passwords with others, writing down passwords where others might see them, and failing to periodically update them or create new ones for different accounts (Huth et al., 2012). When a password is reused across accounts, a successful brute-force attack against one account can become a security risk for all

others associated with that password (Wang et al., 2014). However, a survey of more than 20,000 users found an average of 130 accounts associated with a single email address (Le Bras, 2015).

Some accounts, such as email or social media accounts, may be accessed on a daily basis. Others, such as DMV or social security accounts, may be accessed more sporadically. Frequency of use is an important consideration for which authentication scheme is most appropriate to protect a particular account. Applying an authentication scheme without considering frequency of use assumes that the user is willing and able to manage that login credential (e.g., another unique password) in addition to those they are already responsible for. Expectations from a cybersecurity standpoint are therefore becoming impractical and inefficient from a usability standpoint. In the trade-off between security and usability, the commonly held view is that "increasing one necessarily decreases the other" (Biddle et al., 2012, p. 5). The resulting need for authentication that meets dual standards of usability and security has long generated interest in alternatives to the alphanumeric password (Biddle et al., 2012; Dhamija & Perrig, 2000).

Graphical authentication is one alternative that has been a subject of research for more than twenty years (Biddle et al., 2012). Rather than typing a string of characters, graphical schemes implement picture-based passcodes to authenticate (Sobrado & Birget, 2002). For example, a user may be asked to select their passcode images from a grid of distractor images (Brostoff & Sasse, 2000; Dhamija & Perrig, 2000; Hayashi et al., 2008). From a usability perspective, graphical passcodes benefit from increased memorability relative to passwords (Brostoff & Sasse, 2000; Moncur & Leplâtre, 2007), since pictures are more memorable than text (Nelson et al., 1976; Paivio et al., 1968). From a cybersecurity perspective, graphical passcodes are thought to be more resistant to brute-force attacks because it is more difficult for a

computer to recognize the many bytes contained in an image compared to the few contained in a text character (Linju & Krishnan, 2014; Sobrado & Birget, 2002).

However, graphical passcodes face other cybersecurity risks. Of primary concern are shoulder-surfing attacks, or over-the-shoulder attacks (OSAs), during which attackers observe a user's password or passcode input with the intention of replicating it later to gain unauthorized access (Li et al., 2005). For example, an attacker within the workplace may employ an OSA by closely watching a user as they select passcode images on a desktop login screen. The greater memorability of graphical passcodes benefits malicious observers and the intended user (Sobrado & Birget, 2002). Because it is easier to recognize passcode images from a set than to recall and repeat a string of password characters (Still et al., 2017), OSAs on graphical passcodes are made easier as well.

Some graphical authentication schemes have been designed to prevent OSAs (Lashkari et al., 2009). The Use Your Illusion (UYI) scheme developed by Hayashi et al. (2008), for example, prevents OSAs by distorting the quality of images and randomizing their locations on a grid. When users are first assigned a graphical passcode, images are shown in their original quality. When logging in, however, visual quality is distorted. This renders the passcode images less recognizable to those unfamiliar with the original versions (Cain & Still, 2017; Hayashi et al., 2008). To authenticate, the user searches a series of three 3x3 grids and selects each passcode image located among eight distractor images. Multiple grids are implemented to prevent unauthorized logins due to lucky guesswork (Hayashi et al., 2008). System-assigning the passcode images also eliminates any personal bias from the user that may be evident to a potential hacker, such as a favorite color (Biddle et al., 2012).

Of course, users do not authenticate simply for the sake of authenticating. The login process is less important for users than the task motivating them to log in (Sasse et al., 2001; Whitten & Tygar, 1999). Ideally, remembering and inputting one's password or passcode should come at minimal cost to primary task information already held in working memory. Through working memory, users can preserve one piece of information while processing a new piece of information (Salthouse & Babcock, 1991). In other words, working memory is a form of limited and temporary storage that uses information from short-term memory to complete a task (Baddeley, 2010; Halarewich, 2016). If authentication significantly interferes with working memory, primary task performance may suffer. For example, suppose an employee is tasked with sending a set of instructions to a specific email address. In that case, this working memory load may be negatively impacted if the login process is overly taxing (i.e., typing a complex password or selecting graphical passcode images that require complex visual searches). Of course, there are more troubling consequences to forgotten working memory load than an incorrect email address. Primary tasks while authenticating may be as critical as patient care or heavy machinery's operation (Ghorsad, 2014). According to Trewin et al. (2012), "[…] authentication is an interruption in the user's primary task flow, and a disruption to working memory. The greater the demands on working memory from the authentication process, the greater the risk of forgetting aspects of the task at hand" (p. 160). To date, however, little research has addressed how authentication schemes impact primary task information. This is surprising, given how often users must authenticate. One study by Mare et al. (2016) found that users authenticated an average of 45 times a day.

A recent exploratory study by Still and Cain (2019) measured the impact of graphical authentication on the three components of working memory included in Baddeley's model: verbal, visuospatial, and central executive (Baddeley & Hitch, 1974). In Still and Cain's study, working memory performance was measured for tasks that relied upon each component. Verbal tasks required participants to remember four consonant letters, and visuospatial tasks required them to remember the placement of four dots on a 3x3 grid. Tasks for central executive working memory, which incorporates information from both verbal and visuospatial (Baddeley & Hitch, 1974), required users to remember the placement of four letters on a 3x3 grid. Once users loaded their working memory, they were asked to authenticate through UYI and then report the working memory load.

The results of this study indicated an overall negative impact of authentication on working memory performance. With working memory tasks interrupted by UYI, users reported correct information approximately 55% of the time. Although two other graphical schemes were included in the study, they did not significantly differ from UYI in working memory performance. There was also no significant interaction between authentication scheme and type of working memory task. Across schemes, results suggested that visuospatial working memory performance was best retained. There was no significant difference in performance between verbal and central executive working memory. However, because load conditions were not introduced in this study, performance may have been influenced by a confound of task difficulty.

Although some exploratory research has addressed the impact of graphical passcodes on each working memory component, no previous study has addressed the same impact for alphanumeric passwords. Comparisons between graphical and alphanumeric authentication are therefore unclear in this domain. This is unfortunate, considering that comparisons are likely to

be useful in informing the suitability of an authentication scheme for different settings. For example, if one scheme has a significant negative impact on verbal working memory, that scheme may be inadvisable in situations where users are frequently under verbal load. Because alphanumeric passwords are comprised of verbal information, it is possible that they impair users' ability to remember other verbal information during login. Similarly, since graphical passcodes are embedded with visual information, one might assume that they impair visuospatial working memory. However, Still and Cain (2019) found that visuospatial working memory was *best* retained after using graphical authentication. It is also unclear how the various authentication schemes may influence central executive working memory, which necessitates the storage of both verbal and visuospatial information.

An earlier study by Cain and Still (2018) assessed graphical authentication schemes by usability as well. Participants indicated the pleasantness of their experience with each scheme, also known as subjective satisfaction (Brooke, 1996). Overall, participants reported low subjective satisfaction with graphical schemes (Cain & Still, 2018). Perhaps due to their novelty, users have shown reluctance to use graphical passcodes in place of alphanumeric passwords (Malek et al., 2006). Nevertheless, with passwords already so widely adopted, it is important to gauge users' reactions toward schemes like UYI as a potential alternative.

One way of measuring subjective satisfaction, as in Cain and Still's (2018) study, is the System Usability Scale, or SUS (Brooke, 1996). The SUS is a well-validated usability questionnaire (Bangor et al., 2008) comprised of 10 questions on a Likert scale of 0 ("strongly disagree") to 5 ("strongly agree") (Brooke, 1996). SUS scores ranges range from 0 to 100, with a score of 68 indicating "average" usability (Sauro, 2011, p. 37). In Cain and Still's (2018) study, participants reported an SUS score of 64.53/100 for the UYI scheme when authenticating was

their primary task. This study used the SUS to capture users' satisfaction with UYI when authenticating was their secondary task, and remembering unrelated working memory load was their primary task.

Altogether, this study seeks to compare the effects of a newly assigned alphanumeric password and UYI graphical passcode on working memory performance for all three components. By incorporating both low and high load conditions, concerns about task difficulty are removed. Using the SUS, we can also assess subjective satisfaction with graphical authentication while under working memory load.

CHAPTER II

AUTHENTICATION

Authentication may be classified as knowledge-based (something you know), token-based (something you have), or biometric (something you are) (Hayashi et al., 2008). Biometric authentication, such as fingerprint-scanning and voice or facial recognition, is relatively quick and easy (Bhattacharyya et al., 2009). However, a major vulnerability to biometric authentication is the permanence of users' data. In 2015, fingerprint data for 5.6 million federal U.S. employees were breached in a cyberattack (Peterson, 2015). In this case, a major concern to security experts was that users could not mitigate further risk by changing their fingerprints, as they can with passwords and passcodes (Peterson, 2015). Token-based authentication (for example, proximity cards) is another method that requires relatively low effort from the user (Hayashi et al., 2008). However, they are vulnerable to theft and inconvenient to replace, resulting in delayed accessibility for authorized users (Hayashi et al., 2008; Sathish et al., 2013).

Alphanumeric and graphical authentication are knowledge-based, requiring the user to know a password or passcode (Biddle et al., 2012). In the literature of graphical alternatives to alphanumeric authentication, UYI is a promising scheme that was developed to maintain sufficient usability while providing defense against OSAs (Hayashi et al., 2008). However, graphical schemes have both advantages and disadvantages to security and usability.

Cybersecurity: Resistance to Brute-Force Attacks and Over-the-Shoulder Attacks

Advantages. The wide variety of images employed in graphical authentication suggests that graphical passcodes may be more secure against brute-force attacks. According to Suru and Murano (2019), brute-force attacks use an algorithm that tests "all possible combinations of user passwords" to hack an account (p. 26). The total number of possible passwords is referred to as

theoretical password space (Biddle et al., 2012). For alphanumeric passwords, the theoretical password space is restricted to combinations of numbers, letters, and special characters (Hu et al., 2010). However, the theoretical password space for graphical schemes can be expanded by increasing the library of images (Hu et al., 2010). By expanding the list of combinations to be attempted, brute-force attacks become more difficult (Hu et al., 2010). The greater volume of bytes may also hamper brute-force attacks that a computer must recognize in passcode images (Linju & Krishnan, 2014; Sobrado & Birget, 2002).

Disadvantages. Unlike alphanumeric passwords, graphical passcodes can be directly selected by tapping or clicking (Biddle et al., 2012). However, direct selection of images with a mouse or touch screen means that some schemes are more visible to observers (Darbanian, 2015). This renders them more susceptible to OSAs (Li et al., 2005). Although OSAs are a threat to alphanumeric passwords, input is usually concealed somehow (i.e., by replacing each typed character with a dot or an asterisk). For many graphical schemes, image selection is less easily concealed, and preventing OSAs while maintaining usability becomes a challenge (Darbanian, 2015; Lashkari et al., 2009). Developing authentication schemes that resist OSAs while maintaining usability for the authorized user is a common goal in the literature (Hayashi et al., 2008).

More usable graphical schemes, however, are often limited by smaller theoretical password spaces (Biddle et al., 2012). For example, a grid with fewer images for the user to consider will be more usable, but the theoretical password space will be reduced by the smaller selection of images (Biddle et al., 2012; Schaub et al., 2013). This places more usable graphical schemes at increased risk of brute-force attacks (Biddle et al., 2012). Schemes such as UYI

mitigate this risk by increasing the number of grids to be searched, rather than the number of images within each grid (Hayashi et al., 2008).

Usability: Memorability, Efficiency, and Subjective Satisfaction

Advantages. Interest in graphical passcodes as an alternative to alphanumeric passwords has arisen, in part, from their potential for increased memorability (Biddle et al., 2012). According to Gartner Group (2010), forgotten passwords are responsible for 20-30% of help desk calls. Compared to the strings of characters contained in alphanumeric passwords, the images contained in graphical passcodes are easier for users to remember (Brostoff & Sasse, 2000; Dhajima & Perrig, 2000; De Angelini et al., 2005). The memorability advantage for graphical passcodes has been associated with the picture superiority effect, the long-held finding that people tend to better recall and recognize images compared to text (Nelson et al., 1976; Paivio et al., 1968; Stobert & Biddle, 2013). Whereas text is semantically encoded, images are both visually and semantically encoded. The presence of both visual and semantic encoding enhances recall (Paivio, 1979). Because passcode images are encoded in both forms, they are easier for users to recall than passwords (Brostoff & Sasse, 2000; Dhajima & Perrig, 2000; De Angelini et al., 2005). Even with distorted edges and colors, UYI passcode images remain memorable. One week after receiving system-assigned passcode images, users demonstrated 94% login accuracy in Hayashi et al.'s (2008) study.

Disadvantages. Due to their novelty, graphical passcodes such as UYI require training in a secure environment before they can be employed by users (Hayashi et al., 2008). Alphanumeric passwords, being so widely recognized, do not typically require instruction before use. However, the training phase for graphical passcodes need not be time-consuming. In

Hayashi et al.'s (2008) study, the training phase for UYI lasted no more than five minutes. This phase is also thought to improve long-term memorability (Hayashi et al., 2008).

Subjective satisfaction is another usability dimension needing improvement. Despite the advantages of graphical authentication, users are resistant to change (Malek et al., 2006). When asked whether they would be willing to switch from using alphanumeric authentication to a more secure graphical authentication scheme, only 64.7% of users indicated their willingness to do so (Malek et al., 2006).

User Selection vs. System Assignment

Several authentication studies have allowed users to select their own passwords or passcode images (Dhamija & Perrig, 2000; Forget et al., 2008; Goldberg et al., 2002; Vu et al., 2007). However, such studies focus on the strength or memorability of user-selected passwords rather than the effect of authentication on other performance measures. Passwords that are user-selected vary in length and complexity, and thus their potential interference on working memory would also vary from user to user. In comparison, studies in which passwords are system-assigned ensure the same level of difficulty across study conditions (Wright et al., 2012). Similarly, for graphical authentication schemes, Cain and Still (2018) recommend system-assigned graphical passcodes to avoid user biases in image selection. For example, users might select passcode images that are similar in color to reduce the effort required for detection.

System Usability Scale for Authentication

Although users are reluctant to authenticate using alternatives to the alphanumeric password, many are also unwilling to strengthen their passwords (Warkentin et al., 2004). With users resistant to both strong passwords and password alternatives, user satisfaction is important in considering the deployment of graphical schemes.

The SUS has been used as a "quick and dirty" tool to measure user satisfaction with authentication schemes in several studies (Bindu, 2015; Cain & Still, 2018; Chowdhury et al., 2013; Fraune et al., 2013; Zimmerman & Gerber, 2020). However, none required participants to be under working memory load while authenticating. According to Still and Cain (2019), "the amount/type of working memory an authentication system drains might also predict its perceived 'ease of use'" (p. 80). As a rule, user experience designers should avoid overtaxing users' working memory to prevent information overload from making an interaction unpleasant and unusable (Budiu, 2018). Greater working memory load strains users' limited cognitive resources, which may frustrate the user and diminish satisfaction with the interaction (Jen-Hwa Hu et al., 2017). However, little research has explicitly measured the influence of load on users' subjective satisfaction (Jen-Hwa Hu et al., 2017). When participants in Still and Cain's (2018) experiment were simply asked to authenticate using UYI, they reported a mean SUS score of 64.53. This score falls below the threshold of 68 for "average" system usability (Sauro, 2011). In this study, we draw a comparison by measuring subjective satisfaction with UYI when participants are under working memory load.

Authentication as a Secondary Task

To the user, authentication is merely an interruption to some other task (Subils, 2019). Primary task information, such as a file name or confirmation code, takes precedence over authentication (Chiasson & Biddle, 2007). Thus, when a primary task requires users to log in, they are met with the dual task of holding primary task information in working memory while inputting their password or passcode.

The ability to complete these dual tasks quickly and successfully is limited by the amount of working memory resources that are available. More difficult tasks require greater working

memory resources and therefore place a greater load on working memory (Kahneman, 1973). In turn, greater load negatively impacts working memory performance (Eggemeier, 1988).

The type of dual task load may further influence performance. That is, how well the user retains primary task information depends on the extent to which it demands the same mental resource as a secondary task (Wickens, 1984). Wickens accounts for this intrusiveness through multiple resource theory (1984). For example, if an air traffic controller's primary task is to gauge an aircraft's position, spatial resources will be consumed. If she is also tasked with vocally acknowledging updates from the pilot, verbal resources will be consumed. Because the two tasks do not draw from the same type of resource, primary task performance would not be expected to change. However, if the air traffic controller's secondary task also consumed spatial resources, a negative impact would be expected (Wickens, 2002). In other words, the type of primary task load affects the intrusiveness of the secondary task (Eggemeier, 1988).

With authentication as a secondary task, an authentication scheme's intrusiveness may depend on the type and amount of working memory resources required by the user's primary task. The level of intrusiveness on certain resources may then inform an authentication scheme's suitability for various work environments. When working memory performance suffers, the user risks forgetting the information that may have motivated them to authenticate in the first place. Therefore, it is important to understand how well different types of information loaded before login will be retained after using a graphical passcode compared to an alphanumeric password.

CHAPTER III

WORKING MEMORY

In this study, we seek to understand the influence of alphanumeric and graphical authentication on working memory performance for tasks that vary in type and difficulty. Specifically, we measure their impact on the accuracy of low-load and high-load tasks requiring varying levels of verbal, visuospatial, and central executive working memory. To better understand this relationship, we begin with an overview of the roles that information processing and attention play in working memory; the three components of working memory conceptualized in Baddeley's model (1974); and finally, the difference between interactions with an authentication system and mental representations of a password or passcode.

Information Processing: Attention and Working Memory

Before information enters working memory, it must be processed through several stages. According to Atkinson and Shiffrin (1968), information first enters sensory memory, an initial stage which lasts a few seconds at most. From sensory memory, information enters short-term memory, which lasts approximately 15-20 seconds (Brown, 1958; Peterson & Peterson, 1959) and has a maximum capacity of approximately five to nine pieces of information (Miller, 1956). As a result of these limitations, attention plays a vital role in working memory by enabling focus on specific pieces of information (Awh et al., 2006). In other words, attention functions as a selective mechanism (Johnston & Dark, 1986) for information that is "most relevant to the current processing goals" (Awh et al., 2006, p. 202). Rehearsal of this information enables its maintenance in short-term memory and, potentially, its transfer to long-term memory (Atkinson & Shiffrin, 1968). Working memory has commonly been conceptualized as a mental workbench for both short- and long-term memory (Baddeley, 1986; Klatzky, 1980). In this analogy, short-

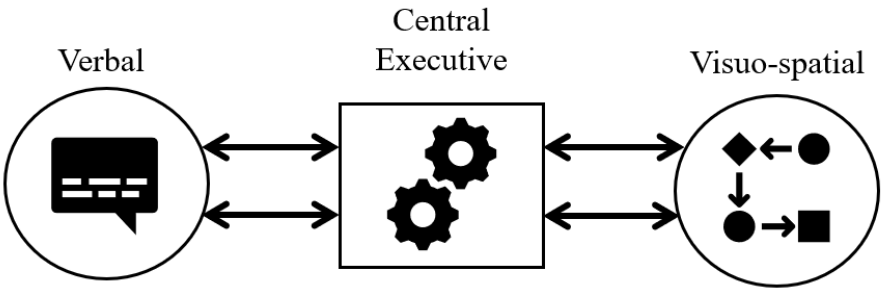
term memory is represented by materials on the surface of the workbench, whereas long-term memory may be likened to materials within reach on a nearby shelf (Klatzky, 1980).

Baddeley's Model of Working Memory

Baddeley's model of working memory (1974) introduced three components: verbal, visuospatial, and central executive. Verbal and visuospatial working memory operate as subordinate systems under central executive working memory, which integrates information from both (Baddeley, 1974). One might consider the central executive a kind of business executive, receiving input from its verbal and visuospatial sub-systems and then incorporating both into useful business decisions (Baddeley, 1986). Figure 1 provides a representation of the relationships between the three components.

Figure 1

Baddeley's Components of Working Memory (Baddeley & Hitch, 1974)



Verbal. Under the central executive, verbal working memory is the subordinate system responsible for briefly retaining verbal and written information (Baddeley, 1974). This process is often referred to as the phonological loop, in which limited verbal information may be briefly

held in the phonological store and sustained through rehearsal. Without sufficient rehearsal, information held in the phonological store will be forgotten (Baddeley, 2002).

Previous studies have measured verbal working memory recall by asking participants to memorize and report a set of random letters. In Helton and Russell's (2013) dual-task study, verbal tasks required participants to remember four letters while completing a secondary vigilance task. In other studies by Desmond et al. (2003) and Chen and Desmond (2005), load conditions were designated by one letter for low load and six letters for high load. For Still and Dark (2010), low load consisted of two letters, and high load consisted of four. Overall, testing recall of varying sets of letters is a prevalent method for verbal working memory tasks.

In Still and Cain's (2019) exploratory study, verbal working memory tasks required participants to remember a set of four letters, which they typed after using a graphical authentication scheme. Overall, verbal working memory performance was found to be significantly worse than visuospatial, but not central executive, performance (Still & Cain, 2019). However, the authentication schemes in this study did not include an alphanumeric password. According to Wickens' multiple resource theory (1984), the resources required by a secondary verbal task should impair performance on a primary verbal task. Typing a recently assigned alphanumeric password would require verbal resources from the user, whereas selecting graphical passcodes would not. Therefore, verbal working memory performance should be significantly worse after using an alphanumeric password compared to a graphical passcode. However, this was not the case for an authentication study by Trewin et al. (2012), which tested participants' verbal working memory of a three-digit number and two-digit unit of measurement (i.e., "152mg"). Participants entered the verbal load after authenticating with a biometric scheme or system-assigned alphanumeric password. Verbal working memory performance after using

the password was not found to be significantly worse compared to the biometric authentication schemes. The lack of interference in this study may be due to the memorability of the relatively weak password ("securit3"), which contained no upper-case letters or special characters and closely resembled a dictionary word. No load conditions, graphical authentication schemes, or other components of working memory were explored in this study.

Visuospatial. Visuospatial working memory, also known as the visuospatial sketchpad, is the second subordinate system which acts as a "rehearsal system for visual input" (Benton et al., 2005, p. 486). Examples of tasks that load visuospatial working memory include web navigation, mental image transformations, and maintaining points of view (Ang & Lee, 2008; Garden et al., 2002; Laberge & Scialfa, 2005; Schmidt et al., 2007). Whereas verbal working memory would help remember a search phrase, visuospatial would help remember a file path, for example.

Visuospatial working memory is also used to memorize images (Kak, 2011) and has been suggested to play a role in visual search tasks, which occur when looking for one target among others (Goldstein, 2014; Kak, 2011; Woodman et al., 2001). When authenticating through UYI, visuospatial working memory is used to remember passcode images and search for them on a grid of distractor images. Because of the demands that UYI places on visuospatial resources, performance on another visuospatial task might be expected to suffer. However, Still and Cain (2019) found that, compared to verbal and central executive, visuospatial working memory was *best* preserved after using UYI.

One possibility for this finding is a distinction in visuospatial abilities. Previous research indicates a discrepancy between the ability to remember spatial targets versus visual targets (Woodman et al., 2001; Woodman & Luck, 2004). Because image positions change within each

grid, UYI does not rely on the user's memory for spatial information. Rather, it relies on the user's memory for visual targets, the passcode images themselves. Still and Cain's (2019) visuospatial tasks required users to remember spatial information: the positions of identical dots on a grid. Therefore, even though UYI relies on visuospatial working memory to some degree, the primary and secondary tasks, in this case, might not interfere with one another. A second possibility is that participants encoded their passcode images through verbal working memory (e.g., remembering the word "bicycle" rather than the visual bicycle in their passcode). In this case, different resources would be consumed. As a result, we do not anticipate a significant difference in visuospatial performance between graphical and alphanumeric authentication.

Central executive. Central executive working memory plays the critical role of incorporating information from both verbal and visuospatial working memory. It has even been considered "the core of the working memory model" altogether (Collette & Van der Linden, 2002, p.106). The more intricate demands of reasoning, decision-making, attentional control, dual-task coordination, verbal fluency, and selective attention all fall under the domain of central executive working memory (Blackler et al., 2010; Collette & Van der Linden, 2002).

Although many studies have implemented task-specific measures to assess verbal and visuospatial working memory, central executive is less easy to fractionate as it incorporates information from both systems (Baddeley et al., 2001). Whereas verbal working memory would be used to remember a search phrase and visuospatial working memory would be used to remember a file path, central executive memory would serve the more difficult task of remembering some combination of the two.

In Still and Cain's (2019) experiment, recall that for verbal tasks, users were asked to remember four consecutive letters, while visuospatial tasks required users to remember the

location of four dots on a 3x3 grid. Similarly, central executive tasks required users to remember both the location and identity of four letters on a 3x3 grid. Although central executive performance was found to be significantly worse than visuospatial, it was not found to be significantly worse than verbal performance. This is surprising, given that central executive working memory must integrate verbal and visuospatial tasks concurrently (Baddeley, 1974).

Password/Passcode Retrieval and Input

When users authenticate, two separate tasks contribute to overall mental workload. Retrieval of the password or passcode itself presents one task, as users are loaded with its representation in their memory. When the password or passcode is novel, as in our study, we can expect this load to be rehearsed in working memory (Woods & Siponen, 2019). With enough repetition and familiarity, however, passwords and passcodes start to become automatically processed (Shiffrin & Schneider, 1977).

Interaction with the authentication scheme itself is another task. With UYI, for example, the user must visually search for passcode images whose locations are randomized within each grid. Because of this randomization, interaction with the UYI scheme requires controlled processing – the ability to give conscious and deliberate attention to a task (Sweller, 1994). In contrast, alphanumeric passwords are entered using keys with fixed, static positions on the keyboard. Users may anticipate the consistent location of each character. The alphanumeric scheme therefore engages automatic processing, which requires minimal working memory resources without conscious or deliberate thought (Shiffrin & Schneider, 1977; Sweller, 1994).

Altogether, several factors contribute to knowledge-based authentication, including the user's familiarity with a password or passcode image, representation of the passcode/password in the user's memory, and whether interaction with the authentication scheme requires automatic or

controlled processing. Because the alphanumeric password assigned in this experiment is completely novel to participants, lack of experience prevents its input from becoming an entirely automatic process. With sufficient trials for rehearsal, password entry should become more automatized. Although the visual search required by graphical schemes like UYI will always require some level of controlled processing, their rehearsal also benefits users. Identifying the same targets (e.g., passcode images) enables the user's attention to become more automatically directed toward the correct target (Schneider & Shiffrin, 1977).

Hypotheses

1. For verbal and central executive working memory, low load performance will be significantly better than high for both UYI and alphanumeric authentication.
2. For visuospatial, low load performance will not be significantly better than high load for both UYI and alphanumeric authentication.
3. Verbal performance will be significantly worse for alphanumeric authentication compared to graphical.
4. The mean SUS score for UYI authentication will be significantly lower than 64.53.

CHAPTER IV

METHODOLOGY

Participants

To determine minimum sample size, we conducted a power analysis using MorePower 6.0, a software program designed to work with more complex ANOVA designs (Campbell & Thompson, 2012). Based on the effect sizes from Still and Cain's (2019) 2x3 ANOVA (partial η^2 = .66-.81), we implemented the convention for a large effect size for partial η^2 (.25) (Cohen, 1988). Solving for a sample size to achieve 90% power (α = .05) resulted in n = 26 (see Appendix). However, technical error and COVID-19 restrictions on in-person data collection reduced our final sample to n = 16.

Undergraduate (freshman and sophomore) participants were recruited through the SONA Research Participation system and compensated with course research credit. It should be noted that this sample reflects a long-held research bias toward American college students and therefore limits generalization to a broader population (Sears, 1986). All participants were 18 years or older and reported having normal or normal-to-corrected vision.

Equipment

Two Windows desktop computers with 24" monitors were used to display working memory tasks on the left and authentication tasks on the right. Standard desktop keyboards were used for working memory task responses and alphanumeric authentication. UYI passcode images were selected using a mouse.

Stimuli

Working memory tasks. All stimuli for working memory tasks were created and presented through E-Prime software (v2.0.10; Psychology Software Tools, Pittsburgh, PA). Verbal task stimuli consisted of two (low load) and five (high load) randomly generated, non-

repeating consonants. Vowels were excluded to prevent words from forming accidentally. Visuospatial task stimuli consisted of two (low load) and four (high load) dots randomly positioned on a 3x3 grid. Central executive task stimuli consisted of two (low load) and four (high load) non-repeating consonant letters also randomly positioned on a 3x3 grid.

The number of items (i.e., letters) was increased for verbal high load tasks. Whereas previous research demonstrates a capacity of 4 ± 2 items for visuospatial working memory, the capacity for verbal working memory is comparatively higher when rehearsal of verbal load is not suppressed (Chen & Cowan, 2009; Vogel et al., 2001). Classic working memory studies have taken measures to suppress rehearsal of verbal working memory, often by asking participants to repeat an irrelevant sound (Baddeley et al., 1975; Baddeley et al., 1984). In this experiment, however, rehearsal was not suppressed. Therefore, to balance the difficulty of high load tasks across working memory components, an additional letter was added to the verbal high load condition.

Working memory task stimuli were designed to be fundamental representations of all three working memory components. More "meaningful" stimuli (e.g., file names for verbal tasks) might have provided greater ecological validity; however, such procedures might have introduced potential confounds, such as memory aids (e.g., chunking). Rather than simulating arbitrary real-world scenarios, this experiment utilized simplified tasks, well documented in previous literature (Helton and Russell, 2013; Desmond et al., 2003; Bethell-Fox & Shepard, 1988; Miyake et al., 2001), to inform more practical applications.

Authentication tasks. The UYI authentication prototype was created and presented in Paradigm Experiment Builder (v2.5.08; Perception Research Systems, 2007). The prototype was based on the original scheme developed by Hayashi et al. (2008). Twenty-seven stock images

were obtained through Pexels, a free-to-use website for open-source images, and distorted through an oil painting filter on Gimp 2.8 open-source graphics editor (www.gimp.org). Following original design recommendations by Hayashi et al. (2008), images were distorted in such a way that colors and general shapes were preserved. A brushstroke size of 10 was applied, following additional design recommendations by Tiller et al. (2018), to strike a balance between low image distortion for easy recognition from users and high image distortion for defense against OSAs.

For each UYI login attempt, one passcode image and eight distractor images were randomly positioned on a series of three 3x3 grids. A random number generator was used to determine the passcode image and distractor images in each grid, as well as their locations. Each grid was 774x471 pixels, and passcode and distractor images were 213x175 pixels (see Figure 2).

Figure 2

UYI Passcode Images)

Note. Participants were shown passcode images in their original quality when first assigned (left). During login trials, participants were shown distorted versions (right).

Stimuli for the alphanumeric authentication task were created and presented in E-Prime. Participants were assigned the same case-sensitive eight-digit password, Boga@411, for both practice and experimental trials. The password Boga@411 meets the National Institute of Standards and Technology's requirements for password strength (Grassi et al., 2017). Additionally, a security rating of 80% was calculated by the Password Strength Checker at passwordmeter.com ("Password Strength Checker," passwordmeter.com). This percentage reflects a cumulation of password strengths (number of characters, inclusion of upper- and

lower-case letters, and middle placement of numbers and one symbol), with deductions for repeat characters (e.g., 11).

Procedures

All participants were presented with an informed consent form and given the opportunity to ask questions before proceeding with the study. Participants were run individually. Once seated in front of the monitors, they followed on-screen instructions to complete six practice trials. Each practice trial reflected one condition of working memory component and load. Instructions were stated as three goals: 1) Memorize information on the left-hand monitor, 2) Successfully log in on the right-hand monitor, and 3) Input the previously shown information on the left-hand monitor. Participants had one attempt to authenticate in each trial.

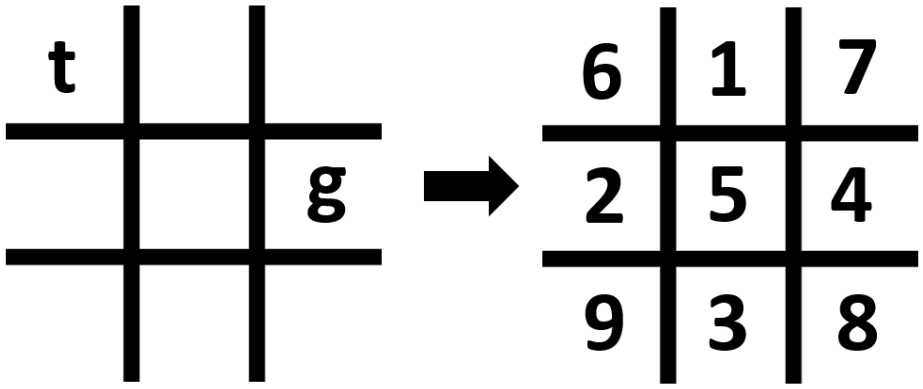
For the UYI scheme, the same three passcode images were used across all participants for both practice and experimental trials. A login was considered successful when the participant correctly selected all three UYI target passcode images. The researcher provided verbal feedback ("correct" or "incorrect") for each attempt. For alphanumeric password input, on-screen text feedback was provided. A login was considered successful when the participant correctly typed all eight characters. Participants were given an on-screen reminder of their password or passcode images after every 20 trials.

For the verbal working memory task, participants were shown either two or five consonant letters for 3000ms depending on the load condition. After authenticating, they typed the letters in the same order in which they appeared. Letters were not case-sensitive. For the visuospatial task, participants were shown two or four dots on an otherwise empty 3x3 grid. Dots appeared for 3000ms, after which grid spaces were randomly numbered (1-9). Participants were asked to look away from the screen as soon as the dots disappeared. After authenticating,

participants indicated the positions of the dots by typing their corresponding numbers in any order. The central executive task was executed similarly. On a 3x3 grid, either two or four letters were shown for 3000ms. Grid spaces were then randomly numbered. A correct response required participants to first type the corresponding number, followed by the letter previously shown, for each letter. Responses could be entered in any order so long as each number was followed by the correct letter (see Figure 3). Letters were not case-sensitive, and backspacing was not permitted for any working memory task response.

Figure 3

Example of low-load central executive task



Note. A correct response for this task would be “6t4g” or “4g6t.”

After practice trials, participants completed a total of 60 working memory trials interrupted by 60 authentication trials for each scheme (see Figure 4). This within-subjects

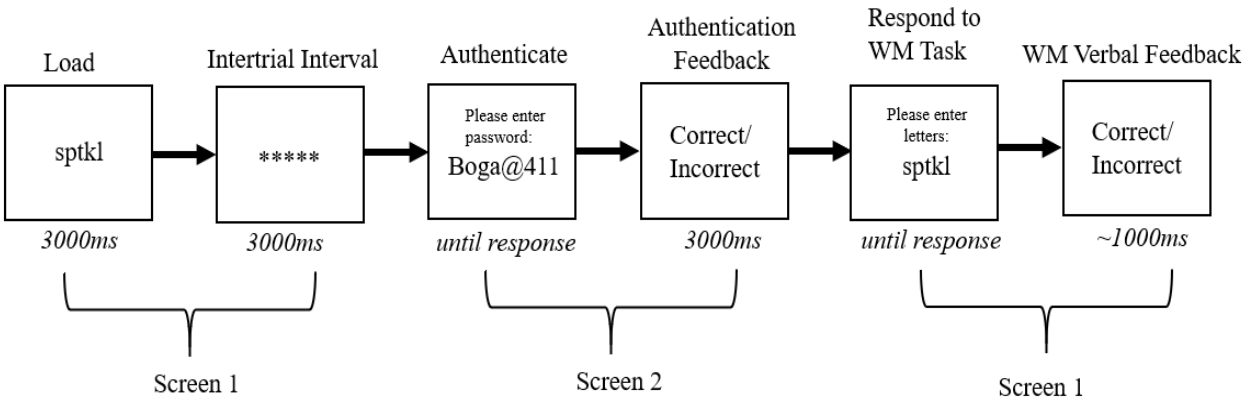
experimental design included the following factors: 2 authentication schemes (alphanumeric password or UYI graphical passcode) x 3 working memory components (verbal, visuospatial or central executive) x 2 load conditions (low or high).

Ten trials were completed for each condition.[1] To prevent fatigue and practice carryover effects on working memory trials, presentation order of authentication schemes was counterbalanced such that half of participants began with UYI authentication and half began with alphanumeric. Presentation order of working memory task type was established using a Latin square generator, resulting in the following three order conditions: 1) Verbal, Visuospatial, Central Executive; 2) Visuospatial, Central executive, Verbal; and 3) Central Executive, Verbal, Visuospatial. Within each condition of working memory task type, load was randomized within E-Prime such that participants either began with 10 low-load trials, followed by 10 high-load trials, or vice versa.

[1] Pilot data collection required participants to complete 20 trials per working memory condition. However, this resulted in a time shortage during the experiment. We therefore reduced the number of trials to ensure that participants completed all tasks within the one-hour session and did not experience significant levels of fatigue.

Figure 4

Workflow diagram of a single working memory task (verbal, high load) with embedded authentication task



CHAPTER V

RESULTS

The primary focus of this study was the impact of alphanumeric and graphical authentication on working memory performance. Only trials associated with correct logins were included in working memory analyses, ensuring that participants were under appropriate load during login. Due to technical error and the need to maintain resulting counterbalances, the minimum sample size of 26 participants was not met (n = 16). Because the experiment was conducted during the onset of the COVID-19 pandemic, public health restrictions on in-person data collection prevented any additional recruitment. Technical error prevented five participants' alphanumeric password performance from being captured; working memory performance from these participants was therefore excluded. To maintain an even counterbalance of authentication and working memory task order, data from three participants were also excluded. Counterbalance orders for the remaining two participants cancelled out. In the reduced sample, incorrect login attempts totaled 50 for the alphanumeric password and five for the graphical passcode. As a result, approximately .03% of trials were excluded. Finally, outlier scores with z-scores > 3 or < -3 were excluded, ensuring that analyses only considered trials in which participants made an acceptable attempt to complete the working memory tasks. Two outlier scores totaling less than .01% of the dataset were found from a single participant. An alpha level of .05 determined statistical significance for all analyses.

Authentication Performance

A paired-samples t-test was conducted to compare authentication performance. Because participants used both the alphanumeric password and the UYI passcode, this analysis was appropriate to compare the paired observations.

A significant difference, $t(1, 16) = -3.511$, $p = .003$, between alphanumeric ($M = 94.96$, $SD = 5.80$) and UYI authentication performance ($M = 99.69$, $SD = .91$) was found. Therefore, authenticating by selecting UYI passcode images resulted in significantly fewer errors than by typing the password. This is likely because UYI only required users to make three selections with a mouse instead of the eight characters that must be typed for Boga@411, not including the shift key.

Working Memory Performance

A 2x2x3 repeated-measures ANOVA examined the impact of authentication (alphanumeric or UYI), load (low or high), and working memory component (verbal, visuospatial, or central executive) on working memory performance. Along with determining any main effects of these categorical predictor variables, the three-way ANOVA enabled us to test for a three-way relationship among them.

Results indicated no such three-way interaction between working memory component, load, and authentication ($p = .802$). There were no significant interactions between authentication and load ($p = .413$) or authentication and working memory component ($p = .122$). Moreover, there were no significant differences in working memory between the password and graphical passcode under any condition. Because participants' verbal working memory was not significantly worse after using the password compared to the UYI passcode, Hypothesis 3 was not supported. Interestingly, the interaction between working memory component and load was found to be significant, $F(2, 30) = 18.16$, $p < .001$, partial $\eta 2 = .548$.

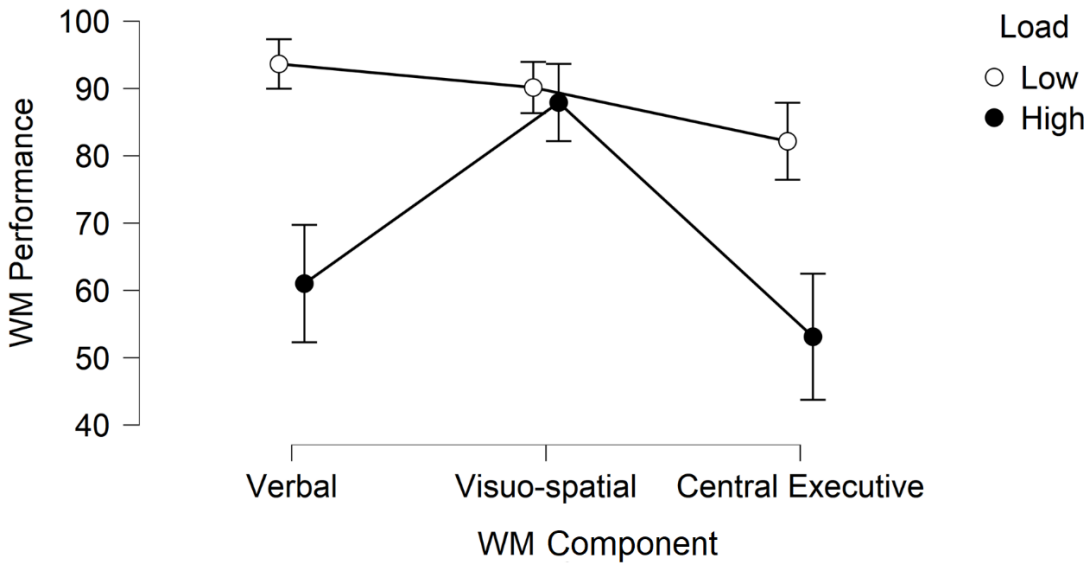
All three main effects were also significant. The main effect of authentication, $F(1, 15) = 4.69$, $p = .047$, partial $\eta 2 = .238$, revealed better overall working memory performance after using UYI (M = 80.15, $SE = 2.65$) compared to the alphanumeric password (M = 75.84, $SE =$

3.25). The main effect of load, $F(1, 15) = 60.72$, $p < .001$, partial $\eta 2 = .802$, revealed better performance when under low load (M = 88.65, *SE* = 1.92) than high (M = 67.34, *SE* = 3.96), $p < .001$. Finally, the main effect of working memory component, $F(2, 30) = 22.73$, $p < .001$, partial $\eta 2 = .602$, was significant, such that verbal performance (M = 77.33, *SE* = 3.28) was better than central executive (M = 67.63, *SE* = 3.99), $p = .031$, and visuospatial (M = 89.02, *SE* = 2.61) was better than both verbal, $p = .006$, and central executive, $p < .001$.

To further explore the significant interaction between load and working memory, a 2x3 repeated-measures ANOVA was conducted on working memory performance (see Figure 5). Simple main effects were explored through pairwise comparisons with Bonferroni corrections. It was found that when under low load, working memory performance was significantly better for verbal than for central executive, $p = .015$. When under high load, visuospatial was significantly better than both verbal, $p < .001$, and central executive, $p < .001$. Performance for low load was significantly better than high load for verbal, $p < .001$, and central executive, $p < .001$, but not for visuospatial, $p = .331$, which supports Hypotheses 1 and 2.

Figure 5

Working memory (WM) performance by component and load



Note. Error bars represent 95% confidence intervals.

Subjective Satisfaction

To test Hypothesis 4, a one-sample *t*-test was conducted to find differences between the mean SUS score reported in this sample and the mean found by Cain and Still (2018). The one-sample *t*-test is ideal when comparing a sample mean to the mean of a known population.

The SUS contains 10 items on a 5-point Likert scale, with scores ranging from 0-100. Cain and Still reported a mean SUS score of 64.53 for UYI after initial use, where a score of 68 reflects average usability (Sauro, 2011). Although this slightly below-average score may have been influenced by higher than recommended levels of image distortion (Tiller et al., 2018), users were not under working memory load during the experiment and only completed three

logins, compared to the consecutive 60 logins in this experiment. Using the SUS score reported by Still and Cain, a comparison may be drawn for subjective satisfaction toward UYI after participants were under load.

Surprisingly, results of the one-sample *t*-test revealed that SUS scores for UYI (M = 68.44, SD = 16.23) were not significantly lower than the mean score of 64.53 found by Cain and Still (n = 20), $t(23) = 1.179$, $p = .250$, thus failing to support Hypothesis 4. In fact, the mean score of 68.44 meets Sauro's (2011) threshold for "above average."

An additional item in the questionnaire asked participants to rate, from 1-10, whether they would recommend the UYI authentication system to a friend (M = 7.14, SD = 1.96). Two participants did not complete this question (n = 22). Overall, our mean of 7.14/10 indicates that most participants found UYI usable enough to recommend to others.

CHAPTER VI

DISCUSSION

Hypotheses and Findings

This study primarily investigated the impact of alphanumeric and graphical authentication on working memory. To date, only Still and Cain (2019) have examined the influence of authentication on verbal, visuospatial, and central executive working memory. However, this exploratory study only considered graphical authentication schemes. In our study, we included the traditional alphanumeric password for comparison and a high/low load condition to account for task difficulty.

Contrary to Still and Cain (2019), we found central executive performance to be significantly worse than verbal. This finding is more intuitive, given that central executive working memory must incorporate information from the verbal and visuospatial components (Baddeley & Hitch, 1974). Participants also performed significantly better in the low load condition compared to high load. This finding is consistent with previous studies in which greater load leads to poorer working memory performance (Braver et al., 2007; Krimsky et al., 2017). As expected, a significant interaction between working memory component and load indicated that this effect was only observed for verbal and central executive working memory. Whereas participants performed significantly better on verbal and central executive tasks when load was low compared to high, this was not true of visuospatial tasks. For visuospatial, performance between low load and high load tasks did not significantly differ. Thus, Hypotheses 1 and 2 were supported. In addition, high load performance for visuospatial working memory was significantly better than high load for verbal and central executive. This further supports Still and Cain's (2019) suggestion that authentication poses limited visuospatial working

memory interference. In other words, visuospatial task information appears to be most resistant to loss or corruption during login.

When averaged across load conditions and working memory components, performance was significantly better after using UYI than the alphanumeric password. However, no significant interactions included authentication, thus failing to support Hypothesis 3. Based on Wickens' multiple resource theory, we predicted that verbal performance would be significantly worse after using the alphanumeric password compared to UYI. However, we were surprised to find that alphanumeric authentication did not significantly interfere with verbal working memory. It is unclear why participants' ability to recall verbal information was not hindered by alphanumeric authentication. Both tasks presumably rely on verbal working memory, implying some level of interference on primary task performance.

One possibility is that participants utilized "chunking" to better remember their password. Chunking is a memory aid that enables a set of information to be consolidated into a single unit, or chunk (Miller, 1956). For example, the phone number 757-555-8913 may be chunked into the three units "757," "555," and "8913." Previous research demonstrates that chunking strategies facilitate better recall for alphanumeric passwords (Carstens & Malone, 2006; Nelson & Vu, 2010). Chunking can also reduce working memory load, thereby increasing storage capacity for new information (Cowan, 2001; Ericsson, 1980; Miller, 1956). Through chunking, participants may have consolidated the password Boga@411 into two (Boga and @411) or three (Boga, @, and 411) chunks, reducing interference on the verbal working memory task.

Theoretically, multiple resource theory would also predict worse visuospatial performance after using the graphical UYI passcode compared to the password. However, in Still and Cain's (2019) study using only graphical authentication schemes, visuospatial performance

was better than both verbal and central executive. As a result, we did not predict that visuospatial performance would be significantly worse for UYI, and our results demonstrate that this was not the case. We attribute this finding to a few possible causes. First, recall that visuospatial tasks can be further differentiated according to visual or spatial targets (Vergauwe et al., 2009; Woodman et al., 2001; Woodman & Luck, 2004). Authenticating with UYI required participants to remember visual targets (their passcode images), whereas the visuospatial task required participants to remember spatial targets (the locations of dots on a 3x3 grid). As a result of this discrepancy, the two tasks may have posed limited interference on visuospatial task performance. Second, participants may have inadvertently benefited from their passcode images containing distinct objects. Rather than remembering their passcode images' visual representation, participants may have simply encoded the images as verbal information (e.g., “bicycle”). This would also result in participants utilizing two different resources, verbal and visuospatial, thus accounting for the lack of negative impact on visuospatial task performance. However, to the best of our knowledge, our visuospatial task originally implemented by Still and Cain (2019) is the only one to be implemented in a study of authentication on working memory.

Our final prediction was that participants in our study would report significantly less subjective satisfaction for the UYI scheme compared to participants in Still and Cain’s (2018) study, which did not require them to be under working memory load. Specifically, we predicted that our mean SUS score for UYI would be significantly lower than their mean of 64.53. Interestingly, the additional burden of working memory load did not appear to detract from users’ enjoyment of this novel graphical authentication scheme. In fact, our mean SUS score of 68.44 met the threshold of 68 for average usability (Sauro, 2011). Although this unexpected

finding failed to support Hypothesis 4, it demonstrates promise for UYI as an enjoyable authentication scheme, even under potentially stressful circumstances.

Because usability data for alphanumeric passwords is biased due to their pervasiveness and familiarity to users (Biddle et al., 2012), we did not collect measures of subjective satisfaction for comparison. Trewin et al. (2012) reported a mean SUS score of 78 for the alphanumeric password used in their experiment ("securit3"). As in our experiment, authentication was interrupted by a working memory task. However, this password is less complex than our "Boga@411". It is likely that omitting uppercase and special characters from their password and forming a near-dictionary word contributed to a higher SUS score than would be expected for our alphanumeric password.

Finally, it should be noted that authentication with UYI requires the user to engage in controlled processing. That is, finding and selecting one's randomly placed passcode images requires conscious and deliberate attention. As a result, UYI may be better suited for accounts with intermediate use than accounts that must be accessed very frequently. In contrast, alphanumeric passwords can be entered with consistently placed keys, and therefore engage automatic processing if rehearsed enough. For situations that require frequent and highly efficient authentication, passwords may be a better solution than graphical schemes like UYI that rely on controlled processing. However, graphical schemes that rely on automatic processing may be a suitable alternative for everyday use. For example, the Cued Click Points (CCP) scheme developed by Chiasson et al. (2007) requires users to select the correct regions, or "click-points," within a series of five static images. Over time, selection within these unchanging images should become an automatic process. Future work might consider how familiar

passwords/passcodes and graphical schemes like CCP affect working memory performance through the user's engagement in automatic processing.

Practical Implications

In our study, participants' overall working memory was better retained after authenticating with the graphical UYI scheme compared to the password, although UYI was an utterly novel authentication scheme for them. However, we did not detect any significant interaction between authentication and working memory component. This suggests that, while recommendations for an authentication scheme in particular work settings are not yet clear, graphical schemes such as UYI may have less negative impact on users' primary task information in general.

Because workflow interruptions lead to decreased primary task performance (Gillie & Broadbent, 1989; Gupta et al., 2013; McFarlane, 2002), this finding holds significant implications. In healthcare settings, for example, entering alphanumeric passwords has been shown to interrupt practitioners' workflow (Bardram, 2005; Frankel & Saleem, 2013). However, navigating patient records requires frequent authentication to confirm the practitioner's identity (Bardram, 2005). This places working memory load (i.e., dosage of a patient's medication) at risk of being forgotten. Similarly, Electronic Health Record (EHR) systems often require healthcare practitioners to load their working memory by piecing together medical information between screens (Koopman et al., 2015; Mator et al., 2020). When interrupted by authentication, the practitioner may unknowingly forget this information, leading to incorrect treatment actions or improper care. In other high-stakes situations, such as emergency dispatching, the user may also be tasked with remembering critical information (e.g., an address or set of directions) when they are interrupted by an authentication system. In cases

such as these, lives can be saved by implementing the lighter system on working memory. Based on our findings, graphical authentication is a promising alternative to alphanumeric passwords with less adverse effects on users' working memory.

It is important to note that some of our findings were unintuitive. Alphanumeric authentication did not significantly interfere with verbal working memory, and graphical authentication did not significantly interfere with visuospatial. These results contradict predictions based on multiple resource theory, highlighting the need for empirically based decisions in applied settings. Without empirical data, designers might make inappropriate recommendations.

Currently, working memory is not considered as a design factor of authentication schemes. Benchmarks, specifications, and usability guidelines are a much-needed tool for designers, who ought to consider how different interfaces will benefit from users' natural abilities (Adams & Sasse, 1999; Still, Cain, & Schuster, 2017). The few existing benchmarks for authentication schemes concern other user metrics, such as login time and accuracy (Braz & Roberts, 2006). Although lengthy login times or additional login attempts may pose a brief delay to the user, the repercussions of poor primary task performance may be far more damaging. Users may fail to notice their errors until it is too late; e.g., until incorrect input on an EHR system results in a patient receiving the wrong medication. Benchmarks for authentication schemes would enable comparison between schemes and establish standards for post-login primary task performance.

CHAPTER VII

CONCLUSION

The present study explored differences in the impact that alphanumeric and graphical authentication has on verbal, visuospatial, and central executive working memory. As expected, low load performance was significantly better than high load performance, but only for verbal and central executive working memory. For visuospatial alone, this difference was not significant. We also replicated findings by Still and Cain (2019), where visuospatial working memory was best preserved compared to verbal and central executive. This suggests that visuospatial working memory for primary tasks may be more resilient to the impact of authentication, a secondary task.

Overall, participants demonstrated better working memory performance after authenticating with UYI, a graphical scheme, compared to an alphanumeric password. However, alphanumeric and graphical authentication schemes did not vary in their impact on various working memory components. This was surprising, as we anticipated that alphanumeric authentication would significantly impair verbal working memory compared to graphical authentication. Our hypothesis was informed by multiple resource theory, given that alphanumeric authentication and verbal working memory ostensibly consume the same resource. Similarly, graphical authentication did not impair visuospatial working memory any more than alphanumeric authentication.

These unintuitive findings may have resulted from the characteristics of our graphical passcode images. Each passcode image featured a distinct object, which may have enabled participants to remember their labels as verbal information, rather than their visual features as visuospatial information. With graphical authentication demanding verbal resources instead,

there may have been minimal interference on visuospatial performance. Additionally, the UYI scheme required participants to remember visual targets. They were asked to find and select each passcode image (the "target") among a grid of distractor images. Our visuospatial task, on the other hand, required participants to remember spatial targets. In this case, they needed to remember where identical dots were randomly positioned on a series of 3x3 grids. There may be a distinction in the resources required to remember visual versus spatial targets, which would also reduce the potential interference of graphical authentication on a visuospatial working memory task.

Finally, we were surprised to find that participants reported greater satisfaction with the UYI scheme in our study compared to Cain and Still's (2018), even though participants in their experiment were not required to be under working memory load while authenticating. This demonstrates promise for UYI as an authentication scheme that exemplifies usability in addition to security.

These findings will hopefully benefit designers in establishing authentication schemes that best support users' primary tasks. Forgetting primary task information is not only inconvenient to the user, but may have greater consequences depending on the gravity of the information. Emergency dispatchers and healthcare professionals, for example, must quickly and efficiently act on life-or-death information stored in their working memory. Authentication, although necessary to confirm users' identities, warrants wider recognition as a contributing factor to working memory performance.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Ang, S. Y., & Lee, K. (2008). Central executive involvement in children's spatial memory. *Memory*, *16*(8), 918-933.

Atkinson, R. C., & Shiffrin, R. M. (1968). Human memory: A proposed system and its control processes. *Psychology of Learning and Motivation*, *2*(4), 89-195.

Awh, E., Vogel, E. K., & Oh, S. H. (2006). Interactions between attention and working memory. *Neuroscience*, *139*(1), 201-208.

Baddeley, A. (1986). *Working memory.* Oxford: Oxford University Press.

Baddeley, A. D. (2002). Is working memory still working?. *European Psychologist*, *7*(2).

Baddeley, A. (2010). Working memory. *Current Biology*, *20*(4), R136-R140.

Baddeley, A., Chincotta, D., & Adlam, A. (2001). Working memory and the control of action: Evidence from task switching. *Journal of Experimental Psychology: General, 130*(4), 641.

Baddeley, A. D., & Hitch, G. (1974). Working memory. In *Psychology of Learning and Motivation*, *8*, pp. 47-89. Academic Press.

Baddeley, A., Lewis, V., & Vallar, G. (1984). Exploring the articulatory loop. *The Quarterly Journal of Experimental Psychology Section A*, *36*(2), 233-252.

Baddeley, A. D., Thomson, N., & Buchanan, M. (1975). Word length and the structure of short-term memory. *Journal of Verbal Learning and Verbal Behavior*, *14*(6), 575-589.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *The International Journal of Human-Computer Interaction*, *24*(6), 574-594.

Bardram, J. E. (2005). The trouble with login: On usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing, 9*(6), 357-367.

Benton, D., Kallus, K. W., & Schmitt, J. A. (2005). How should we measure nutrition-induced improvements in memory?. *European Journal of Nutrition*, *44*(8).

Bethell-Fox, C. E., & Shepard, R. N. (1988). Mental rotation: Effects of stimulus complexity and familiarity. *Journal of Experimental Psychology: Human Perception and Performance, 14*, 12-23.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, *2*(3), 13-28.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 1-41.

Bindu, C. S. (2015). Secure usable authentication using strong pass text passwords. *IJ Computer Network and Information Security*, *7*(4), 57-64.

Blackler, A., Mahar, D., & Popovic, V. (2010). Older adults, interface experience and cognitive decline. In *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction* (pp. 172-175). ACM.

Braver, T. S., Gray, J. R., & Burgess, G. C. (2007). Explaining the many varieties of working memory variation: Dual mechanisms of cognitive control. In *A. R. A. Conway, C.*

Jarrold, M. J. Kane (Eds.) & A. Miyake & J. N. Towse (Ed.), Variation in working memory (p. 76–106). Oxford University Press.

Braz, C., & Robert, J. M. (2006). Security and usability: The case of the user authentication methods. In *Proceedings of the 18th Conference on l'Interaction Homme-Machine* (pp. 199-203).

Brooke, J. (1996). SUS: A quick and dirty usability scale. *Usability Evaluation in Industry, 189*(194), 4-10.

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV — Usability or Else!* (pp. 405-424). Springer, London.

Brown, J. (1958). Some tests of the decay theory of immediate memory. *Quarterly Journal of Experimental Psychology*, *10*, 12–21

Budiu, R. (2018, April 29). *Working memory and external memory.* Nielsen Norman Group. https://www.nngroup.com/articles/working-memory-external-memory/

Cain, A. A., & Still, J. D. (2017). RSVP a temporal method for graphical authentication. *Journal of Information Privacy and Security, 13*, 226-237.

Cain, A. A., & Still, J. D. (2018). Usability Comparison of Over-the-Shoulder Attack Resistant Authentication Schemes. *Journal of Usability Studies, 13*(4).

Campbell, J. I., & Thompson, V. A. (2012). MorePower 6.0 for ANOVA with relational confidence intervals and Bayesian analysis. *Behavior Research Methods*, *44*(4), 1255-1265.

Carstens, D. S., & Malone, L. C. (2006). Applying chunking theory in organizational password guidelines. *Journal of Information, Information Technology, and Organizations*, *1*, 97-113.

Chen, Z., & Cowan, N. (2009). Core verbal working-memory capacity: The limit in words retained without covert articulation. *Quarterly Journal of Experimental Psychology*, *62*(7), 1420-1429.

Chen, S. A., & Desmond, J. E. (2005). Cerebrocerebellar networks during articulatory rehearsal and verbal working memory tasks. *Neuroimage*, *24*(2), 332-338.

Chiasson, S., & Biddle, R. (2007). Issues in user authentication. In *CHI Workshop Security User Studies Methodologies and Best Practices*.

Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security* (pp. 359-374).

Chowdhury, S., Poet, R., & Mackenzie, L. (2013). A comprehensive study of the usability of multiple graphical passwords. In *IFIP Conference on Human-Computer Interaction* (pp. 424-441). Springer, Berlin, Heidelberg.

Cohen, J. (1988). Statistical power analysis for the behavioural sciences, 2nd edn. (Hillsdale, NJ: L. Erlbaum Associates).

Collette, F., & Van der Linden, M. (2002). Brain imaging of the central executive component of working memory. *Neuroscience & Biobehavioral Reviews*, *26*(2), 105-125.

Cowan, N. (2001). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences*, *24*(1), 87-114.

Curtin, M. (2005). *Brute force: Cracking the data encryption standard.* New York: Copernicus Books.

Darbanian, E. (2015). A graphical password against spyware and shoulder-surfing attacks. In *2015 International Symposium on Computer Science and Software Engineering (CSSE)* (pp. 1-6). IEEE.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1-2), 128-152.

Desmond, J. E., Chen, S. A., DeRosa, E., Pryor, M. R., Pfefferbaum, A., & Sullivan, E. V. (2003). Increased frontocerebellar activation in alcoholics during verbal working memory: An fMRI study. *Neuroimage, 19*(4), 1510-1520.

Dhamija, R., & Perrig, A. (2000). Déjà vu - A user study: Using images for authentication. In *9th USENIX Security Symposium,* pp. 45-58.

Eggemeier, F. T. (1988). Properties of workload assessment techniques. In *Advances in Psychology, 52,* 41-62. North-Holland.

Ericsson, K. A., Chase, W. G., & Faloon, S. (1980). Acquisition of a memory skill. *Science, 208*(4448), 1181-1182.

Forget, A., Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2008). Improving text passwords through persuasion. In *Proceedings of the 4th Symposium on Usable Privacy and Security* (pp. 1-12).

Frankel, R. M., & Saleem, J. J. (2013). "Attention on the flight deck": What ambulatory care providers can learn from pilots about complex coordinated actions. *Patient Education and Counseling, 93*(3), 367-372.

Fraune, M. R., Juang, K. A., Greenstein, J. S., Madathil, K. C., & Koikkara, R. (2013). Employing user-created pictures to enhance the recall of system-generated mnemonic phrases and the security of passwords. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), pp. 419-423. Sage CA: Los Angeles, CA: SAGE Publications.

Garden, S., Cornoldi, C., & Logie, R. H. (2002). Visuo spatial working memory in navigation. - *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *16*(1), 35-50.

Gartner highlights four myths surrounding IT self-service. (2010, August 25). Gartner Group. http://www.gartner.com/newsroom/id/1426813

Ghorsad, T. (2014). Adventures and Ethics in MF Authentication. *International Journal of Research*, *1*, 329-338.

Gillie, T., & Broadbent, D. (1989). What makes interruptions disruptive? A study of length, similarity, and complexity. *Psychological Research, 50*(4), 243-250.

Goldstein, E. B. (2014). *Cognitive psychology: Connecting mind, research and everyday experience*. Nelson Education.

Grassi, P. A., Perlner, R. A., Newton, E. M., Regenscheid, A. R., Burr, W. E., Richer, J. P., ... & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management [including updates as of 12-01-2017*] (No. Special Publication (NIST SP)-800-63B).

Gupta, A., Li, H., & Sharda, R. (2013). Should I send this message? Understanding the impact of interruptions, social hierarchy and perceived task complexity on user performance and perceived workload. *Decision Support Systems, 55*(1), 135-145.

Halarewich, D. (2016, September 9). *Reducing cognitive overload for a better user experience.* Smashing Magazine. https://www.smashingmagazine.com/2016/09/reducing-cognitive-overload-for-a-better-user-experience/

Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: Secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security* (pp. 35–45). New York, NY: ACM.

Helton, W. S., & Russell, P. N. (2013). Visuospatial and verbal working memory load: Effects on visuospatial vigilance. *Experimental Brain Research, 224*(3), 429-436.

Herley, C., & Florêncio, D. (2008). Protecting financial institutions from brute-force attacks. In *IFIP International Information Security Conference* (pp. 681-685). Springer, Boston, MA.

Herley, C., & Van Oorschot, P. (2011). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, *10*(1), 28-36.

Hu, W., Wu, X., & Wei, G. (2010). The security analysis of graphical passwords. In *2010 International Conference on Communications and Intelligence Information Security* (pp. 200-203). IEEE.

Huth, A., Orlando, M., & Pesante, L. (2012). Password security, protection, and management. *United States Computer Emergency Readiness Team.*

Jen-Hwa Hu, P., Han-fen, H., & Xiao, F. (2017). Examining the mediating roles of cognitive load and performance outcomes in user satisfaction with a website: A field quasi-experiment. *MIS Quarterly*, *41*(3).

Johnston, W. A., & Dark, V. J. (1986). Selective attention. *Annual Review of Psychology*, *37*(1), 43-75.

Kahneman, D. (1973). *Attention and effort* (Vol. 1063). Englewood Cliffs, NJ: Prentice-Hall.

Kak, S. (2011). Information and learning in neural systems. *NeuroQuantology, 9*(3), 393-401.

Kirushnaamoni, R. (2013). Defenses to curb online password guessing attacks. In *2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 317-322). IEEE.

Klatzky, R. L. (1980). Human memory: Structures and processes . San Francisco: William H.

Koopman, R. J., Steege, L. M. B., Moore, J. L., Clarke, M. A., Canfield, S. M., Kim, M. S., & Belden, J. L. (2015). Physician information needs and electronic health records (EHRs): Time to reengineer the clinic note. *The Journal of the American Board of Family Medicine*, *28*(3), 316-323.

Krimsky, M., Forster, D. E., Llabre, M. M., & Jha, A. P. (2017). The influence of time on task on mind wandering and visual working memory. *Cognition, 169*, 84-90.

Laberge, J. C., & Scialfa, C. T. (2005). Predictors of web navigation performance in a life span sample of adults. *Human Factors*, *47*(2), 289-302.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security (IJCSIS)*, *6*(2), 145–154.

Le Bras, T. (2015, July 21). *Online Overload—It's Worse Than You Thought*. Dash Lane. https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/.

Li, Z., Sun, Q., Lian, Y., & Giusto, D. D. (2005). An association-based graphical password design resistant to shoulder-surfing attack. In *2005 IEEE International Conference on Multimedia and Expo* (pp. 245-248). IEEE.

Linju, P. S., & Krishnan, P. (2014). A mustang security user authentication scheme based on graphical password. *International Journal of Research in Computer and Communication Technology,* 41-47.

Malek, B., Orozco, M., & El Saddik, A. (2006). Novel shoulder-surfing resistant haptic-based graphical password. In *Proceedings of the Euro Haptics Conference, 6* (pp. 1-6).

Mare, S., Baker, M., & Gummeson, J. (2016). A study of authentication in daily life. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2016)* (pp. 189-206). USENIX Association.

Mator, J. D., Lehman, W. E., McManus, W., Powers, S., Tiller, L., Unverricht, J. R., & Still, J. D. (2020). Usability: Adoption, Measurement, Value. *Human Factors,* 0018720819895098.

McFarlane, D. C. (2002). Comparison of four primary methods for coordinating the interruption of people in human-computer interaction. *Human-Computer Interaction, 17*(1), 63-139.

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *The Psychological Review, 63*(2), 81-97.

Miyake, A., Friedman, N. P., Rettinger, D. A., Shah, P., Hegarty, M. (2001). How are visuospatial working memory, executive functioning, and spatial abilities related? A latent-variable analysis. *Journal of Experimental Psychology: General, 130,* 621-640.

Moncur, W., & Leplâtre, G. (2007). Pictures at the ATM: Exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 887-894).

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, *22*(11), 594-597.

Nelson, D. L., Reed, V. S., & Walling, J. R. (1976). Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, *2*(5), 523-528.

Nelson, D., & Vu, K. P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, *26*(4), 705-715.

Paivio, A. (1979). Imagery and Verbal Processes. London, Ontario: Psychology Press.

Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words?. *Psychonomic Science*, *11*(4), 137-138.

The Password Meter. (2016). http://www.passwordmeter.com

Perception Research Systems (2007). *Paradigm Stimulus Presentation.*

Perlroth, N., & Gelles, D. (2014, August 5*). Russian hackers amass over a billion internet passwords.* New York Times. https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html.

Peterson, A. (2015). *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*. The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/

Peterson, L. R., & Peterson, M. J. (1959). Short-term retention of individual items. *Journal of Experimental Psychology, 61*, 12–21.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611.

Raderman, L. (2017). *Guidelines for Password Management.* Carnegie Mellon University Information Security Office. https://www.cmu.edu/iso/governance/guidelines/password-management.html

Salthouse, T. A., & Babcock, R. L. (1991). Decomposing adult age differences in working memory. *Developmental Psychology*, *27*(5), 763-776.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Sathish, S., Joshi, A. B., & Shidaganti, G. I. (2013). User Authentication Methods and Techniques by Graphical Password: A Survey. *International Journal of Computer Applications & Information Technology*, *2*(3), 1-4.

Sauro, J. (2011). A practical guide to the system usability scale: Background, benchmarks, & best practices. Denver, CO: Measuring Usability LLC.

Schaub, F., Walch, M., Könings, B., & Weber, M. (2013). Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (pp. 1-14).

Schmidt, D., Krause, B. J., Weiss, P. H., Fink, G. R., Shah, N. J., Amorim, M. A., ... & Berthoz, A. (2007). Visuospatial working memory and changes of the point of view in 3D space. N*euroimage*, *36*(3), 955-968.

Schneider, W., Eschmann, A., & Zuccolotto, A. (2002). E-Prime (Version 2.0.8.90). Pittsburgh, PA: Psychology Software Tools, Inc.

Schneider, W., & Shiffrin, R. M. (1977). Controlled and automatic human information processing: I. Detection, search, and attention. *Psychological Review, 84*(1), 1-66.

Sears, D. O. (1986). College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology, 51*(3), 515-530.

Shiffrin, R. M., & Schneider, W. (1977). Controlled and automatic human information processing: II. Perceptual learning, automatic attending and a general theory. *Psychological Review, 84*(2), 127-190.

Sobrado, L., & Birget, J. C. (2002). Graphical passwords. *The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research, 4*, 12-18.

Still, J. D., & Cain, A. A. (2019). Over-the-shoulder attack resistant graphical authentication schemes impact on working memory. In *International Conference on Applied Human Factors and Ergonomics* (pp. 79-86). Springer, Cham.

Still, J. D., Cain, A., & Schuster, D. (2017). Human-centered authentication guidelines. *Information & Computer Security*, 25(4), 437-453.

Still, J. D., & Dark, V. J. (2010). Examining working memory load and congruency effects on affordances and conventions. *International Journal of Human-Computer Studies, 68*(9), 561-571.

Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (pp. 1-14). ACM.

Subils, J. B. (2019). *Authentication Usability Methodology.* (Doctoral dissertation, University of South Florida).

Suru, H. U., & Murano, P. (2019). Security and user interface usability of graphical authentication systems – A review. *International Journal of Computer Trends and Technology*, *67*(2), 17-36.

Sweller, J. (1994). Cognitive load theory, learning difficulty, and instructional design. *Learning and Instruction*, *4*(4), 295-312.

Tiller, L., Cain, A., Potter, L., Still, J.D. (2018). Graphical authentication schemes: Balancing amount of image distortion. In *International Conference on Applied Human Factors and Ergonomics* (pp. 88–98). Springer, Cham.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-David, S. (2012). Biometric authentication on a mobile device: A study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference* (pp. 159-168).

Vergauwe, E., Barrouillet, P., & Camos, V. (2009). Visual and spatial working memory are not that dissociated after all: A time-based resource-sharing account. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 35*(4), 10121028.

Verizon RISK Team (2017). 2017 data breach investigations report.

Vogel, E. K., Woodman, G. F., & Luck, S. J. (2001). Storage of features, conjunctions, and objects in visual working memory. *Journal of Experimental Psychology: Human Perception and Performance*, *27*(1), 92-114.

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and

organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744-757.

Wang, X., Kohno, T., & Blakley, B. (2014). Polymorphism as a defense for automated attack of websites. In *International Conference on Applied Cryptography and Network Security* (pp. 513-530). Springer, Cham.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the check-off password system (COPS): An advancement in user authentication methods and information security. *Journal of Organizational and End User Computing (JOEUC)*, *16*(3), 41-58.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 162-175).

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In 8th *USENIX Security Symposium* (pp. 169-184). New York: ACM.

Wickens, C.D. (1984). Processing resources in attention. In *R. Parasuraman & D.R. Davies (Eds.), Varieties of Attention* (pp. 63-101). Orlando, FL: Academic Press

Wickens, C. D. (2002). Multiple resources and performance prediction. *Theoretical Issues in Ergonomics Science*, *3*(2), 159-177.

Woodman, G. F., & Luck, S. J. (2004). Visual search is slowed when visuospatial working memory is occupied. *Psychonomic Bulletin & Review*, *11*(2), 269-274.

Woodman, G. F., Vogel, E. K., & Luck, S. J. (2001). Visual search remains efficient when visual working memory is full. *Psychological Science*, *12*(3), 219-224.

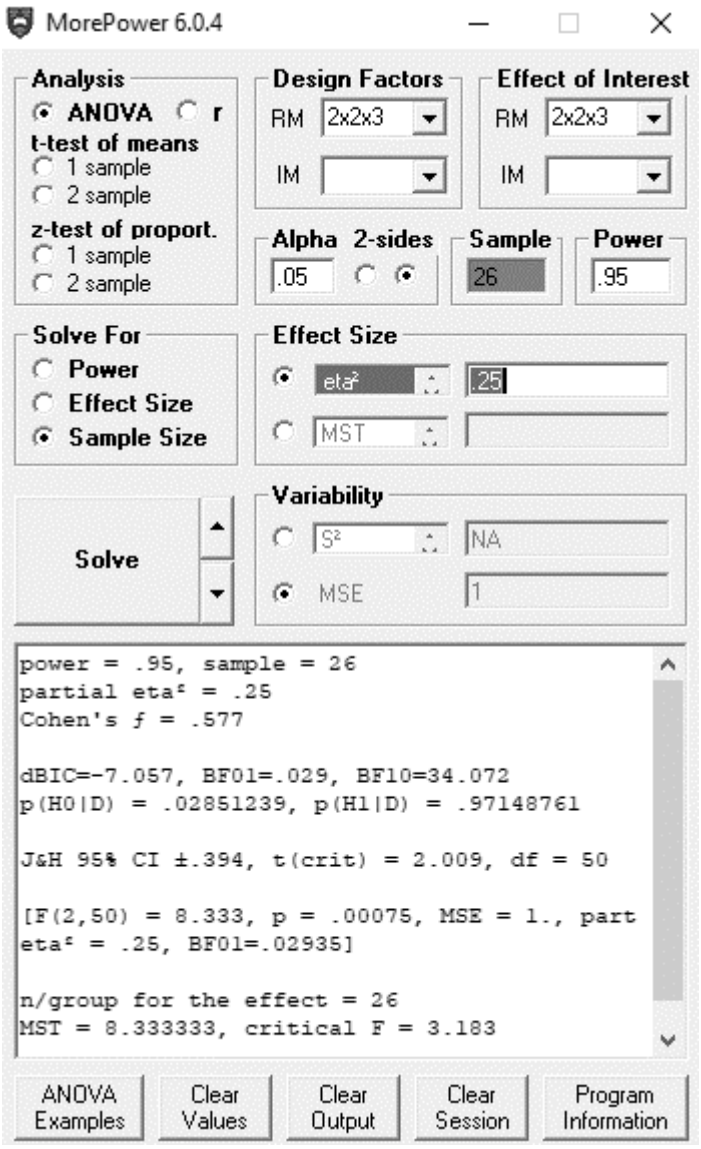
Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*, 61-71.

Wright, N., Patrick, A. S., & Biddle, R. (2012). Do you see your password?: Applying recognition to textual passwords. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (pp. 1-14). ACM.

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies, 133*, 26-44.

APPENDIX

POWER ANALYSIS FOR MINIMUM SAMPLE SIZE



VITA

Janine D. Mator

250 Mills Godwin Life Sciences Bld

Norfolk, VA 23529

Janine is a graduate student in the Human Factors Psychology program at Old Dominion University, where her current research concerns cybersecurity with an emphasis on usability. She graduated cum laude with a bachelor's degree in psychology from Michigan State University in 2016.