A Review of Graphical Passwords and Their Viability in Real-time Application

Wilson Xu*

wilson.xu.16@dartmouth.edu

May 31, 2016

Abstract

In this age of security, it becomes incredibly important to improve everyday authentication systems. Graphical passwords offer an enticing alternative to standard alphanumerical passwords by utilizing the dual theory of memory to allow improved recall. Combined with large password spaces and a variety of authentication systems to select from, graphical passwords seem to be the next logical step in security. This paper is a review of current literature, as well as including a new survey looking to analyze the effects of user preference on password choice. Graphical passwords demonstrate viability in specific environments, but may require more research before they can be implemented as the industry standard.

I. Background of Graphical Passwords

In this section, we will mainly be discussing the background of graphical passwords. This will include an introduction of what graphical passwords are, the forms they can take, and what this paper will be focusing on in future chapters.

i. History of Graphical Passwords

The first instance of graphical passwords was noted in 1994 when Greg E. Blonder filed a patent for a basic tap-based password. This type of password stored "a predetermined number of predetermined positions" in an image as a password. The user would tap the screen at those specified locations to login in or confirm their identity. The original idea was motivated by security for personal data assistants, which featured a primarily stylus input. Blonder wanted to tackle the issue of conventional alphanumeric passwords forcing users to either remember long arbitrary sequences, or put themselves in danger by selecting passwords vulnerable to dictionary attacks. Blonder noted that people tend to be able to recall images with personal meaning more than alphanumeric sequences, alleviating the need for longer passwords. These images also provided greater security since tap regions were only limited by the size of the image and the size of error assigned to each region. Blonder specifies that "in an arrangement that uses a 3 inch-by-5 inch (7.5 cm -by- 12.5 cm) display with one-quarter inch square (6 mm-by-6 mm) tap regions and that requires the user to touch three tap regions in the correct order, there are 13.6 million possible combinations. In comparison, a four-digit password like a personal identification number (PIN) is one of only 10,000 possible combinations, and a three-letter password is one of only 17,000 possible combinations." It should be noted that the 13.6

*

million possible combinations represented an upper bound in Blonder's scheme as the user was required to select one of a limited number of "tap regions"[8]. Graphical passwords have since expanded from Blonder's template. Development of password schemes in the security field have been divided into three main systems: recall, recognition, and cued-recall.

ii. Recall and Cued-Recall Systems

Recall and cued-recall are both based on the ability for the user to remember a password that they have come up with themselves. Recall, or pure recall, is entirely dependent on the user to remember their authentication. These usually take the form of user-created doodles. More notable examples of pure-recall systems include: "Draw-A-Secret" (DAS) and Passdoodle.

Passdoodle represents the more traditional form of pure recall, where the user provides his authentication by drawing a design onto a touch screen. In addition to the stroke patterns, Passdoodle also took into account velocity of the user when creating the design, giving another component to the authentication.

According to Christopher Varenhorst's paper investigating Passdoodle, this method could generate an upper bound of 10^{400} different 100-point doodles in a 100x100 grid, without accounting for velocity. Comparing this to the $2.08x10^{11}$ 8-letter passwords available, we can see that the upper bound of Passdoodle far exceeds that of a conventional alphanumeric password. Memorability of the complete doodle was comparable to memorability of conventional alphanumeric passwords; however, users, over long periods of time, became unable to recall the order of the strokes used to draw their doodle. This problem ended up being a large weakness of the doodle scheme [67].

DAS was created the same year that Passdoodle was, but added a grid to impose the design on top of. The password authentication was determined by the path the design took through each grid cell. The design was able to be multi-stroke, with each stroke being determined by when the user lifted up their "pen" and placed it down again in a different grid that the previous stroke ended in. For a max length of 12, DAS's password space had an upper bound of 2^{58} . At length 8, DAS's password space has an upper bound of 2^{38}, compared to the $2.08x10^{11}$ 8-letter passwords available. DAS shared both the strengths and weaknesses of Passdoodle, but struggled with the additional problem of weaker passwords being vulnerable to dictionary attacks. Unlike Passdoodle, which had the doodle itself be the graphical password, DAS only takes the grid sequence. Thus, it is possible to more efficiently build a dictionary given a maximum length .

Subsequent password systems wanted to improve on the weaknesses identified in the recall-based system examples. In order to improve password memorability, newer recall- based systems used cued-recall. Cued-recall usually includes a background image, which allowing users to create their password based on reference points. A study done by Hollingworth and Henderson revealed that "people retain accurate, detailed, and visual memories of objects to which they previously attended in visual scenes". Thus, a background image should improve recall percentages from users. Blonder's original design was the earliest example of cued-recall, while the current cued-recall standard is PassPoints [27].

PassPoints looked to improve upon Blonder's basic design. The main weaknesses were the limited options in choosing a password image and the limited regions able to be selected as elements of the password sequence. PassPoints allowed the user to use any image with the requirement that the image be intricate enough such that enough click points are available. The weaknesses of having too few click points will be addressed later, as an overarching problem of graphical passwords. PassPoints also allowed users to select their own points, rather than have them select from a predetermined number of them. This change improved security, as malicious users would have to iterate through far more choices. How-

ever, allowing more choices initially caused problems in storing the password itself. It is almost impossible for users to click exactly on their password pixel, so systems give the user space for error. As such, selecting different pixels, which still correspond to the same click point, result in different values when hashing. A solution was found that discretized the image into squares that covered a realistic bound for user error. To ensure that users didn't accidentally click on the edge between two squares, Jean-Camille Birget utilized robust discretization, ensuring that the click point was a safe distance from the edge in at least one of three discretization grids. The system would then use the safe grid to hash the click point [18].

PassPoint also demonstrated a much larger password space than alphanumeric passwords with greater length. At a length of 8 and an alphabet size of 96, alphanumeric passwords came out to an upper limit of $7.2x10^{15}$. Alternatively, with an image size of 1024x752, a selection square size of 20x20, and only 5 click points, PassPoints shows an upper bound of $2.6x10^{16}$, with smaller selection square sizes yielding much high bounds. Wiedenbeck's evaluation of PassPoints did reveal some severe weaknesses in the system. While the password was very easy to come up with, members of the Wiedenbeck's PassPoints study ran into problems during the learning period. 70% of the group that was assigned to create an alphanumeric password input the correct password 10 times without error. On the other side, only 40% percent of the PassPoints group were able to input the correct graphical password 10 times without errors. Even more telling, the least successful 20% made between 17 and 20 incorrect password inputs [71].

Recall and cued-recall systems both exhibited similar strengths and weaknesses. Recall systems definitely exhibited high values of password spaces for fewer elements in the password sequence. While most of the studies only really looked at short sequences, this establishes a stronger deterrence if we can to go higher than the typical 8 length click point sequences. However, both methods still had a steep learning curve. Cued-recall, which seemed to solve many of pure-recall's memorability issues, still faced user issue with remember the order and locations of the click points. Error could be attributed to users clicking outside of the grid square, but this reflected a large problem involving the ability for human users to replicate successes. On a side note, PassPoints users often needed a longer time to enter their graphical password than their alphanumeric counterparts. This weakness will be addressed in future sections.

iii. Recognition Systems

While recall-based systems relied on the user to replicate the image, design, or sequence that they created, recognition systems instead only require the user to remember their pre-selected images among decoy images. Recognition systems build off of the ability for humans to recognize images that they have seen before to a greater extent than recall systems. These systems, however, do run into a problem with having relatively small password spaces, since the system can only display so many decoys before it becomes more of a hindrance for the user to login than to deter phishing attacks. To put these strengths and weaknesses into scope, this section will focus on the PassFaces system, which is the canonical example of recognition systems.

PassFaces presents the user with four rounds of 3x3 boards containing portraits images. Within each of these boards is one pre-selected image that the user has chosen to represent an element in his or her password sequence. On a basic level, PassFaces typically has a password space of M^N , where M is the number of images per board and the N being the number of boards. Initially, PassFaces suffered from an issue with shoulder-surfing attacks. Shoulder-surfing attacks occur when an attacker can "record or observe the images selected by users during login". Since PassFaces already has a relatively small password space, attackers would be able to identify images that were extremely memorable in relation to their sur-

roundings. Dunphy investigated in a study if Passfaces were vulnerable to social engineering attacks where attackers were able to obtain descriptions of the images chosen for passwords. He found that in 8% of 158 attempts, users were able to log on based on the verbal description of the image alone [20]. To counteract this, PassFaces have started to introduce decoy images that are visually very similar to the correct image. This method depends on the user's innate ability to clearly remember small details of the image they have chosen, while not sacrificing speed on login.

In Valentine's study, 77 users were compared based on their abilities to remember Passface style passwords and their ability to remember conventional alphanumeric passwords. The study found that over extended periods of time showed a success rate between 72% and 100% by three attempts, even for time intervals over 5 months [20]. While this does show immense improvement over statistics for recall systems, recognition systems suffered from longer login times compared to their alphanumerical counter parts. This illustrates some of recognition-based securities biggest weaknesses. Recognition systems appear to be extremely weak against multiple avenues of attack. Because of the critically long login times, shoulder surfing becomes a very powerful way to phish passwords. Especially in an environment where the attacker is regularly in the vicinity of the user when logging in, the long login process presents numerous opportunities for the attacker to catch one or two boards at a time. This is furthered by the way many of these systems work. Because there is a limited number of decoys that can be presented before overwhelming the user, the selection pool remains incredibly small. Coupled with the necessity that there exists one of the correct images, systems that maintain identical image cues per login attempt are at risk of being brute forced.

iv. Strengths of Graphical Passwords

The strengths of graphical passwords can usually be condensed into two main avenues: picture superiority and password space. Password space has been addressed above, so this section will not focus on it. Picture superiority refers to the ability of the brain to "better memory for pictures than for corresponding words". This superiority is justified in Paivio's dual code theory. According to Paivio, the brain stores verbal input and pictorial input in two separate memory locations. For words, the brain only stores a singular verbal input, whereas images store both a pictorial and a verbal input. Having two memory locations allows people to have more options to retrieve the memory in question. This effect is corroborated by a study done by Standing, Conezio, and Haber in 1970. Participants were asked to study 2000 pictures for 10 seconds each and given a recognition test a few days later. Participants were able to recognize the pictures with over 90% accuracy. Interestingly, a study done by De Angeli showed that while conventional passwords inputs were slightly faster than graphical password inputs, conventional passwords were more susceptible to long-term decay than sequences of images[55]. There are many other factors that affect the ability for users to better memorize their password phrases, but that will be looked at in a later section.

v. Weaknesses of Graphical Passwords

Graphical passwords suffer from longer than average login time as compared to alphanumeric passwords. In the same study done by De Angeli, participants spent more time on logging in using graphical passwords; however, this difference was attributed to the users being unfamiliar with the graphical style of passwords. Graphical passwords tend to rely on mouse inputs, which is usually slower. This new style of authentication also leads to longer learning curves when learning the authentication, resulting in a lack of early results. Graphical passwords are also susceptible to several bi-

ases that reduce password spaces. With respect to cognitive bias and vision bias, humans are more attracted to some parts of images than others. This leads to high concentrations of user choices in specific regions of the password image. Furthermore, this bias also appears when selecting images in picture story passwords. Users will select images that align with their own preferences. These weaknesses will be addressed in more depth later.

vi. Moving Forward

This section introduced graphical passwords and established some points that will be addressed later in the paper. Graphical passwords are a strong candidate for secure authentication, but it is important to understand its competitors and their strengths and weaknesses. The following sections will focus on comparing other means of authentication, primarily alphanumeric and biometric, while exploring how external factors affect the viability of graphical passwords in private and public sectors.

II. Choosing Graphical Passwords Over Other Options

The previous section gave insight into the strengths and weaknesses of various graphical password systems. This section will look to compare those systems to the currently available alternatives: alphanumerical and biometric passwords.

i. Overview of Alphanumeric Passwords

The greatest incentives for switching over to a graphical password system are the weaknesses of alphanumeric passwords. In Blonder" patent background, he notes some of the more upfront weaknesses. He describes conventional alphanumeric passwords as "difficult for the users to remember, particularly if they are arbitrary alphanumeric sequences". Blonder also mentions that "alphanumeric sequences are also more susceptible to dictionary attacks"[8]. In Klein's 1990 case study, 25% of the observed 14,000 user passwords were found in a dictionary of only 3 x 10^6 [63]. While this seems like a relatively large dictionary to look through, it should be noted that most users tend to select short passwords or passwords that are easy to remember. Shorter passwords are put into a reasonable brute force range, where malicious users might see greater trade offs when it comes to guessing passwords.

This problem is magnified when looking at the sheer number of accounts that a user has to manage. With the rise of social media and other apps that require authentication of sorts, users are required to create passwords for upwards of twelve accounts at a time. A study done by Adams and Sasse revealed that half of those surveyed relied on writing their passwords down on physical places to keep them memorized. This puts authentication in danger, as social bias means of attacks become more possible and accessible [3]. Users can misplace their post-its, or their passwords can be easily stolen. What's even more alarming is the lack of variation in these numerous passwords. The same study showed that a large percentage of the users surveyed added limited variation between passwords on difference accounts. This creates two major weaknesses in the password pool. Primarily, if an attacker is able to discover one password, it is extremely likely that they will be able to hack into those other accounts. Another less talked about weakness is the lack of password knowledge present in most users. A user can lack in password knowledge from two perspectives. The first is not knowing proper password security procedure. While most people in computer security fields know that writing down their passwords is an extremely dangerous practice, the average corporate user does not have the training or knowledge to avoid these dangerous practices. Disregarding security procedure also limits the frequency that passwords are changed. Frequent changes limit the time span that a particular malicious user has access to important information. Much like how credit cards have

expiration dates that limit the extent of damage someone can do, passwords realistically should have expiration dates that prevent damage to an account over a long period of time. A consumer survey done by CSID showed that 44% of those surveyed changed their password only once a year or less, while 61% reused passwords across multiple websites. These percentages seem almost frighteningly high when 89% of the same group felt secure with their current password management and 21% had an online account be compromised [14].

These users also tend not to know how password guessing works. Unaware victims use the names of pets or loved ones as passwords, thinking that the only hackers would be strangers. However, due to the rise of social media accounts, this knowledge has become more widely available to users from a simple Google search. Using these easy to guess passwords creates a false sense of security since this is information that is personal, but not private.

ii. Advantages of Graphical Passwords over Alphanumeric Passwords

Current alphanumeric systems are not user-centric. They often require arbitrary sequences of characters, numbers, and symbols that is not conducive to memorability. As was seen with recognition based graphical password systems, users were better able or felt better able to remember their password sequences. This is a huge advantage that graphical passwords have over alphanumeric passwords. Since the human brain tends to make strong associations and connections to images that it has seen, the user does not have to memorize each character individually, but instead can create more meaningful and memorable associations with other image.

A common strategy for memorizing phrases is to use mnemonic. While most alphabet mnemonics run the risk of creating a mnemonic phrase that is harder for the user to utilize, image mnemonics take the form of stories about the pictures seen, which is a lot easier to memorize, especially since it is unlikely that the user needs a pixel-perfect image in memory. With images, it is a lot easier to get away with not memorizing the entire picture and, instead, focus on looking at more memorable parts of the images.

The second point has already been visited, but merits visiting again. Because of the format of some of the passwords, specifically recall-based systems, the password space of graphical passwords is functionally much larger than that of alphanumeric passwords. Of course, it should be prefaced that for practical purposes, the functional password space is more telling than the upper bounded password space. Even when having a relatively large bound for error, graphical passwords still show a much larger password space than alphanumeric. Let's take a graphical password of size 480x480. Assuming that a square of size 16x16 pixels is a large enough confidence boundary for users, a 480x480 image would produce 900 squares to choose from, far exceeding most common alphanumeric password spaces. Given the ability for humans to create strong associations with images they have seen in the past, it might be easier for users to differentiate between these 900 squares than it would be to remember a specific character in the sequence.

The last point is from a security point of view, which will be focused more on in the next section. Because of the novelty of most graphical password systems, hackers and phishers do not have set procedures for securing graphical passwords. Inserting keyloggers is the most common way to obtain alphanumeric passwords, but keyloggers do not work when the password is a mouse prompt. Given the numerous combinations of input available for graphical passwords, isolating a singular logger to use is incredibly difficult, so hackers will have a harder time brute forcing or phishing a password. This concept will be expanded on in the next section.

iii. Overview of Biometric Passwords

Biometric authentication is part of a new wave of security that has become a popular in re-

cent years as a secure alternative in authentication. Biometric systems currently take the form of finger print scans, retina or iris scans, voice recognition, and facial recognition. Biometric systems tend to flow the same basic flowchart. They first collect the sample data from users and transfer the received information to a central location. This data is usually collected using sensors that try to focus on the biometric characteristics that that particular form of authentication will reference against. This information is then transmitted to a location where it is processed. If needed, the data is compressed before it is sent. Upon receiving the the compressed data, systems look to decipher the signal they receive and extract the biometric pattern enclosed. This pattern is then compared to what the system has saved as a standard, and the decision is made to accept or decline the sample.

These patterns and samples are defined between two criteria: either being a sample that is known by the system, or a sample that is not known by the system. Identification of these samples usually fall under one of two types: positive and negative identification. Positive identification systems try to prevent multiple people using a single identity, while negative identification tries to prevent a single user having multiple identities.

An example of positive identification is a system used by the San Francisco International Airport. The system requires employees to first activate the system by swiping an ID card through a reader and then placing their hand on a reader. The reader confirms the hand geometry with a template currently stored in memory and allows the employee in [69]. Since only one user is supposed to have access that that particular ID card, this biometric system check-in ensures that only one person can use one single identity. Positive identification tends to be a little redundant as there are other ways to prove that the user is the user in particular. These methods include, but are not limited to, checking driver licenses, passports, or other documents that guarantee a singular identity.

Santa Clara County's social service benefits represents a negative identification system. Users are required to scan their left and right thumbprints verify their identity [69]. The system checks to see if the fingerprint has been enrolled in the system already. If it has, the user is not given the benefits, whereas if the fingerprint has not been, the benefits are given out. This system makes sure to not allow a single user to collect multiple benefits. In contrast to positive identification, negative identification requires biometric identification. To ensure that there is only one person that can possibly authenticate, there is a need for that method of authentication to be foolproof. Biometric authentication provides that absolute verification that negative identification requires.

Biometric passwords serve as one of the most absolute authentication systems. Iris scans and fingerprints are incredibly hard to replicate and are accepted as being the best ways to confirm an individual's identity. For this reason, biometric passwords are held as the most exact means. While there is no real password space, biometric systems are extremely hard to phish, as the effort that needs to go into counterfeiting a fingerprint is pretty complex. Furthermore, sensors are getting cheaper to produce, allowing for more ubiquitous implementation of these systems. Most smartphones come with a fingerprint scanner and Apple's new Retina screen iMac come equipped with facial recognition software. An underappreciated strength of biometric password is the login speed. Since the majority of biometric authentication does not require users to provide multiple selection or input, the login speed is usually quite fast.

iv. Weaknesses of Biometric Passwords

Since biometric systems are very new technology and not widely implemented, there are not that many statistics available addressing their security in comparison to graphical passwords. However, there is some data addressing some of the weaknesses of biometric authentication. The most common problem with biometric au-

thentication is the likelihood of false negative decisions. A false negative occurs when the system makes a mistake parsing the biometric pattern and returns a "no entry in system" and prevents access. A face recognition system developed by a corporation in Burlington, Ontario returned a 3.1% false negative rate. While this system provided a 0% false positive rate, meaning that the system never let a stranger into the system, having a significant failure rate does spawn some worry. Most of these biometric systems are set up in high security locations or in locations where quick biometric verification is necessary [**?**]. If a biometric authentication is setup in a hospital surgery room, the possibility of a doctor being temporarily locked out of the operation room is incredibly frightening to think about. In fact, biometric passwords are the only type of authentication that have the possibility to return a negative decision despite receiving a theoretically correct input.

One of the largest concerns involving biometric authentication is user privacy. While other types of passwords usually contain minimal levels of personal information, biometric patterns are entirely personal data. Users have the fear that security companies will have access to their biometric data. This fear is unrealistic in that names are rarely attached to each biometric pattern, so no one will know which biometric signature belongs to whom. However, the fear is justified when governmental bodies are able to connect fingerprints and the such to the actual person. Much like how credit card statements are able to determine activity, fingerprint logins will be able to determine to a guaranteed extent if that particular user was present at login. Unfortunately, this makes cases of fraud incredibly hard to pursue and recover from. While credit cards can be changed, fingerprints and iris scans are permanent. There is no way to ensure that an identity is no longer compromised. In this scope, it becomes even more important to protect personal information from being stolen and replicated.

v. Advantages of Graphical Passwords over Biometric

Biometric authentication theoretically is more secure than graphical passwords. The absolute nature of biometric patterns gives an advantage over password spaces, as outside of counterfeiting prints or scans, there is no other way to fool the system. The majority of advantages that graphical passwords hold over biometric authentication are user centric. Graphical passwords are relatively easy to change when an identity has been compromised and still offer a higher level of security than alphanumeric. Graphical passwords do not suffer from the false negative phenomenon that biometric authentication does and is more "accurate" in that respect. Finally, people will feel more comfortable inputting unbiased image sequences than personal information when they login.

vi. Approaching Graphical Passwords Differently

This section mainly looked to address the advantages that graphical passwords have over their competitors. While alphanumeric systems proved to be the weakest out of the three, biometrics actually emerged as the most secure system. However, there are more factors in choosing a password system than just security. From a consumer perspective, biometric systems are relatively new technology. Even though they represent more secure authentication, the population doesn't trust it yet. A system is only as strong as how much faith the people who use have in it. If a doctor doesn't trust the fingerprint reader and has his assistant open the door from the inside instead, the biometric system in place is not as secure as intended. For this reason, the most viable security systems are those that the users trust enough and are knowledgeable enough to operate the system properly. Thus, Graphical passwords are the perfect middle ground for security. They embody a stronger authentication style and also address many of the issues that conventional alphanumerical pass-

words face. Graphical password systems are also more mainstream and in their limited capacity have seen to be relatively successful. The following sections will be looking to analyze graphical passwords in a way to measure the viability of these systems in different environments, as well as accounting for vulnerabilities that emerge from real-time usage.

III. Addressing the Weaknesses of Graphical Passwords

Previous sections addressed the strengths of graphical passwords, but it is equally important to address some of the weaknesses.

i. Weakness 1: Shoulder Surfing

Shoulder surfing is the non-technical term for local attackers who are able to garner information about the victim through being within close proximity during the login process. Techniques can include looking at keyboard inputs, regions where the mouse is clicked, or even having access to physical locations where passwords or clues to passwords are kept. Due to the heavy vision component of graphical passwords, shoulder surfing is especially dangerous to graphical password authentication. Shoulder surfing is strongest in environments were another user has ready access to the input process of the password. This can take the form of a co-worker looking over your shoulder as you type, or maybe even having a person sharing a cubicle with you seeing your login procedure day after day. In either case, the more time that the person in particular has vision of the medium of input, the more likely it is that they will be able to guess the password. This section will examine important workarounds for graphical passwords, as well as explore important qualities that quality passwords need to make shoulder surfing a less viable method to steal passwords.

ii. Using Input Style to Reduce Shoulder Surfing

When considering the entry of graphical authentication, one must consider the effects on medium of entry have on the viability of the system. Currently, alphanumerical passwords rely solely on keyboard entry, and in some extremely rare cases, the occasional mouse assisted entry. Graphical passwords, focusing on image identification, are built to rely on mouse selection rather than keyboard entry. Mouse based selection inherently has some very wide weaknesses when it comes to security. Graphical passwords suffer from a unique type of malicious attack called shoulder surfing attack. These attack occurs when a user nearby the authentication user is able to see the image sequence or region that is chosen when authentication. While this attack still happens with alphanumerical passwords, current security systems replace entries with asterisks to cover up the sequence entered, reducing the likelihood of someone inadvertently seeing the password. Unfortunately for graphical passwords, the intended entry method leaves authenticators at risk for shoulder surfing attacks.

In terms of the level of risk from the different types of graphical passwords, pure recall-systems are the least vulnerable, as they require almost exact replication by the attacker, while but cued-recall and recognition based systems are at medium to high risk depending on the system. Cued-recall systems, like PassPoints, are at medium risk due to the ease shoulder surfers have at identifying objects in the image that can serve as strong reference points guessing particular regions. If the authentication user clicks near a car, the shoulder surfing user may not be able to guess the exact location, but will be able to use the vicinity to the car in the image as a good estimator for the region. Cued-recall systems that are variations on pure-recall systems are at a much smaller risk. Background Draw-A-Secret, which is a variation on the DAS that includes a background to ease drawing the user image, is relatively safer from shoulder surfing attacks, as this form of authen-

tication still requires the attacker to be able to exactly replicate the pattern. Finally, recognition based systems are realistically at the most risk to be attacked by shoulder surfers. Because they only require users to choose from a preset selection of images, shoulder surfers have an advantage by limiting the options have to guess from. In addition, if the images are not similar enough, getting a glimpse of a distinctive part of an image is usually enough to guess that part of the sequence.

With that knowledge, graphical password systems have started to implement different means to avoid the shoulder surfer problem. The simplest method would be to alter graphical password entry from mouse only to include keyboard input. While this is a simple solution, it does resolve many of the immediate weaknesses to shoulder surfing. Keyboard use is much more covert than using a mouse to select an image on a screen, as the user can hide input with his or her body. However, since graphical passwords are created with mouse use in mind, it is important to compare the entry speed of keyboards versus mouse input.

There are a few variations on keyboard input graphical passwords, but the focus will be on recognition and cued-recall systems. Pure recall methods that involve mouse drawings are almost impossible to replicate with a keyboard only. With respect to recognition based systems that require the user to select images that match the user's authentication, the system will assign letters or keyboard buttons to images available for selection. The user will utilize the keyboard to select their image. This should result in minimal changes in how the system works, as selection is pretty straight forward. For cued-recall, the keyboard can be used to assign keys to different regions that are pre-highlighted. While this is probably the most secure version of the cued-recall system, it no longer functions as the traditional PassPoints system. Because one of the pre-highlighted points must be a correct region, it limits the password space that is presented at one time. An alternative would be to highlight one region at a time for user selection. While this maintains the password space, since any region can be selected, it forces the system to present a correct region within a reasonable number of tries. If it was to truly represent the proper password space, there would be the likelihood that the region appears after an extremely large number of highlighted choices. This is unreasonable as it would take much more time than most users would be comfortable with. For the meantime, these methods will be used when comparing keyboard alternatives.

iii. Effects of Speed on Shoulder Surfing

The easiest way to deny shoulder surfing is to limit the amount of time the attacker has to look at the password. Aside from the method of entry, another way to make it more difficult for malicious users to take advantage of the graphical password system is to main a low login time.

To analyze entry speeds, this paper utilized the GOMS model, which analyzes "user complexity of interactive system". Created by Card and Moran in 1980, the GOMS model and the simplified version, Keystroke-Level Model, break down individual operations and use predetermined values to estimate the effective amount of time required to input a series of commands by keyboard or mouse. The time analysis was estimated by summing together appropriate operators to obtain a time estimate of how long the input process would take. For example, given an input that took three keyboard inputs and one mouse click on a field, the equation would look like this:

$$H + 3K + P + K = H + 4 * K + P \qquad (1)$$

where H is the time spent homing the hands on the keyboard, K is the time for a keystroke or button press, and P is time to point at a target with a mouse. Each variable is assigned a value determined by a study that observed "1,280 user-system-task interactions" from "28 users, 10 systems, and 14 tasks" [32]. These users were of variation proficiency at typing,

Table 1: *KLM Table*

operator	time(sec)
k	.08 (best), .12 (good), .20 (55 wpm), 1.20 (worst typist)
P	1.1
H	0.4
D(Drawing manually)	.9n+. 16 l

giving a decent range of values to use when estimating values. Some of these values are displayed in Table 1.

An initial look at the list of values reveals a set of interesting conclusions. First, the operation of pointing to a target on the screen has a constant value of 1.1 seconds. This value obviously differs based on the distance and size of the target, but to keep calculations close, the constant value will be used. Since most password sequence selections are made up of a mouse movement (P) and a click(K), the combined action costs a total of 1.2 seconds. This is in contrast to a single keystroke entry, which for a good typist costs .52 seconds. However, if the typist is very poor and unfamiliar with the keyboard, the time rises to 1.60. The gap in time spent between keyboard entry and mouse entry shows that keyboard entry is actually much more efficient than mouse selection, given a strong familiarity with the keyboard. Furthermore, the KLM actually shows the cost for homing onto the keyboard is a one time cost, whereas pointing to a specific target with the mouse is a constant cost. This means that if the keystroke sequence is longer, the more efficient keyboard entry ends up being.

The KLM actually address DAS style passwords as well. It attributes drawing n straight line segments having a total length of l cm with the equation:

$$.9 * n + .16 * l \tag{2}$$

The determining factor is the number of line segments being drawn. Looking at a study done by Paul Dunphy, the average strokes produced by DAS and BDAS schemes are 4.9 and 5.8 strokes respectively, with an average password length of 17.5 and 26.6 respectively [19]. Applying this data to the equation above, DAS comes out with an average login time of 7.21 seconds, and BDAS comes out with an average login time of 9.476 seconds. Comparing both of these to the average speeds generated by the KLM model, we can see that login times become comparable once the number of characters' reach around 79 characters at a rate of 90 words per minute. Using a keyboard input that designates each box in the DAS scheme with a character actually makes the entering of 27 characters take less time than drawing out the model. This shows that keyboard input in theory should be faster than mouse usage, creating less time for shoulder surfers to have vision of the password.

While having recognition and cued-recall based authentications use keyboard alternatives makes sense, the amount of typing required in pure recall authentication becomes too cumbersome to use in the scope of keyboard authentication. It may make sense to explore other options other than keyboard entry. One alternative that is has only recently become viable is touchscreen selection. Graphical password authentication seems to be more built for smartphones or tablet authentication. Fingers can easily be substituted for mouse inputs, which allows for more efficient manipulating of DAS authentication schemes. A study done by Chiang took 31 students and tasked them with creating passwords in graphical password systems and then testing them on both phones and tablets. The data given for this study was represented in graph form, without accurate numbers corresponding the averages and quartiles. Nonetheless, DAS systems on the phone had a median of about 12 seconds, which tablets showed a median time of 7.5 seconds. It should be noted that for phones, the data is skewed towards the lower range, meaning the average is probably smaller than 12 seconds [11]. This input data is relatively comparable to mouse inputs for graphical passwords, showing that at least on a larger touchscreen, the switch to graphical password

is viable.

iv. Effects of Low Error Rates on Shoulder Surfing

Another way to disrupt shoulder surfers is to have very short and effective learning curves for graphical passwords. The more comfortable a user is with the authentication system, the more likely they will be able to use it securely and optimally. If the user uses the system as intended, the system maintains the level of security that it is meant to have. Short learning curves can typically be measured by high levels of retention rates and maintenance of these high rates over long periods of time. Basically, a graphical password system is most secure when the users are able to remember their passwords and the entry method over a long period of time. Having short learning curves always for users to reduce login times and increase memorability over a short span of time, leaving a small window for shoulder surfers to attack new users. Analytically, this section will look at the memorability of the various input methods for graphical passwords.

With respect to the Deja vu system, which falls under recognition based authentication, Dhamija conducted a study involving 20 users who tested out this system. The Deja vu system works by having users pick a small portfolio of images from a larger sample that the server presents. The user then chooses his or her selected images from a larger sample upon login. These participants take part in two sessions: the first involved creating a 4-digit PIN and a six-character password; the second involved creating an image portfolio in the style of Deja vu using either an art or a photo image. The results were very supportive of graphical passwords. After creating the passwords, the users were able to replicate both graphical styles without errors, while having a 5% error with respect to the PIN and password formats. In the scope of the study, this comes out to one person out of the 20 not being able to remember either form of the password. However, in comparison, the graphical password system seemed to give users very little difficulty in that regard. The users were tested again in a week, and the results seemed a lot clearer. The failed login rate for the alphanumerical passwords rose from 5% to 35% for the PIN style and 30% for the password style. On the other hand, graphical passwords only saw an increase from 0 to 10% for art and 5% for photo. This is indicative of a shallow learning curve and possibly better memorability for graphical password systems [17].

Better memorability means a few things. Primarily, it means that users will not need assistance or rely on external cues to memorize their passwords. Having hard to remember password sequences leads to dangerous behaviors, such as writing the password down in open areas, or near the device being used. Graphical passwords remedy this problem two fold. First, because it is memorable, the user will probably not write down clues to the password, eliminating the paper trail. Next, since the portfolio is made up of random art samples, the elements in the portfolio become hard to describe and communicate to other people. It is also important to discuss learning curves in the scope of input style. There are many different ways to selection options in creating graphical password sequences; however, user preference is very important in evaluating how viable each option is. If the user is unable to adapt quickly to the different method of input, he or she will probably not trust the system and be at risk of using the system improperly. Thus, it becomes important to examine error rates over time and learning curves corresponding to the different methods of entry.

With respect to the different methods of input, the one that will be examined most is keyboard input. Most graphical password entry is currently done by mouse, so many of the figures displayed above already encompass the error rates for mouse based passwords. On the other hand, there hasn't been as much research done in the scope of graphical passwords on touch screen devices. In addition, many computers in corporate or governmental settings tend to not have touchscreens, which renders

comparative analysis irrelevant since they are not viable options. Thus, the one method that will be looked at is keyboard input.

Komanduri's study utilized a picture-password system that matched letters with random images. Users would use the keyboard to enter the randomly assigned letter or character corresponding with each image in place of clicking on the image itself. In terms of graphical passwords, the study considered two scenarios: a password with an ordered sequence of images and a password where all the images must be selected regardless of order. Komanduri tested these uses after one day of creating the passwords and then another time after a week. In comparison, users were also measured on their ability to remember a typical alphanumerical password, although it was set up in the same format as the graphical password. Picture passwords showed showed a retention rate of 100% for both ordered and unordered options after one day, while character passwords returned a 75% retention rate for the order sequence and 87.5% for the unordered. After a week, keyboard inputs only deteriorated down to 67% down for ordered options only. Surprisingly, the retention rated stayed at 100% for the unordered option. Character passwords dropped a lot more with ordered dropping to 50% and unordered dropping to 67% [34]. While this study was not done explicitly to test keyboard analysis, this study is different in that it is one of the only studies that incorporated keyboard inputs into their testing. Nonetheless, the results are pretty telling. Graphical formats outperformed character formats by a large margin even over a relatively long period of time. Despite both alphanumeric and graphical passwords being presented in a new way to the members of the study, it looks like the learning curve for keyboard entry of graphical passwords is shorter than alphanumerical styles.

v. Concluding Shoulder Surfing

By offering more alternatives to entering graphical passwords than just the mouse, shoulder surfing is heavily limited in how strong of an attack it can be. As demonstrated above, keyboard input return low error rates over a long period of time, while also being faster in cued-recall and recognition conditions. Touchscreens show promise in pure-recall password formats, like DAS, but have not been explored as thoroughly in other forms. Shoulder surfing is not a solution that can be immediately solved, but there are many remedies that can be used to alleviate the risk.

IV. Weakness 2: Visual Biases and Social Engineering

Graphical passwords are also weak to social engineering attacks. These attacks usually involve the abuse of known user biases. User biases involve some combination of human biases, which include tendencies based on implicit memory or innate preferences, and mechanical biases, which focus on biases that are inherent in graphical authentication systems that are used. This section looks to explain the mechanics behind these biases, how attackers can abuse them, and what alternatives are available to combat attackers.

i. Human bias

Human biases can be simplified into preferences that make people more likely to pick a specific area or an image over another. While these preferences do not guarantee that a specific region is choice, it does allow outside users to narrow down realistic options. This narrowing of choices is especially important when evaluating the actual security of graphical passwords. As explored prior, graphical passwords, given a comparable size to alphanumerical passwords, have larger theoretical password spaces. The word theoretical is used deliberately, as not every square or region has an equal chance of being selected. Factoring the effects of the biases mentioned it is possible that a malicious user would be able to guess the graphical sequence given limited information about the user.

The main biases that will be looked into are preferences based on the location of the selected region in the image, preferences for specific images being selected, and finally low level image features. Each preference is important to analyze for different graphical password systems. Locations of the image have the largest influence on PassPoints type passwords, where the user is left to select the password regions, since location ends up having the most important. Locations may also have a strong influence on PassFaces style passwords, where the user is tasked with selecting the image they will use initially. The position of the images when presented will have an impact on which ones are picked. Preferences for the image itself affect all password systems, although to different extents. Obviously, preference for what is in the image plays a larger role when making PassFaces or similar systems that require the user to select single images, but preference for content also plays a huge role when selecting within a larger image, as user preferences could determine if a certain area is selected, narrowing down choices. Lastly, low level image features refer to basic attributes of the image, like color, orientations, and frequency with color being the most prevalent in graphical passwords.

The goal is to evaluate the relative influence of these preferences on graphical passwords. This section will look to prove whether these preferences have a negative effect on the password space to ensure that graphical password systems are as secure as they have been shown to be theoretically.

ii. Location Preference

Before delving into the details of location preference, it is important to understand the concept of salience, as it will be visited often. Salience is the visual quality that makes some items stand out versus others. Effectively, salience causes users to pay more attention to specific areas and, in the context of graphical passwords, makes certain areas more likely to be chosen. Salience plays a large part in what is known as central bias. Central bias is the tendency that people have to look towards the center of images because the distribution of subjects of interest and salience is biased towards the center [66]. This is especially important tin the evaluation of graphical passwords, as this should theoretically group user choices towards the center of the picture. An important theme when choosing a region is to choose one that is easy to remember. This can be reflected in selecting a region that is easily noticed, or catches the eyes of the user.

A study done by Benjamin Tatler looked to examine the impact of central bias. The experiment recorded the eye movements of twenty-two participants to determine if there was indeed a link between image feature distribution and if the human eye was more likely to fixate on those locations with more features. Each participant was tasked to either "view the scenes freely or to search for a small luminance target embedded in the scene". The scenes themselves were categorized based on whether features were distributed towards the center or the periphery of the image, with an added category based on left/right and top/bottom divisions. To avoid camera bias, the images were taken to avoid having prominent objects and features grouped in the center. Before presenting each scene, participants were asked to fixate on a small marker randomly generated to avoid motor bias that may have caused users to be more accustomed to look at a specific part of the screen to start the picture [60]. The study showed pretty convincing results. Despite purposely avoiding centering obstacles of interest, in free viewing tests for both center biased scenes and periphery biased scenes, user fixation was still heavily centered. In search task testing, despite most objects of prominence being on the periphery, the majority of fixations were still centered around the middle of the image. These findings showed that central bias was not simply a symptom of centered features. Since the concentration of choices should be based around the center, those regions are the first that will be look at by users and, thus, be more likely to be remembered and used as

passwords.

In addition to looking at the effects of center bias on fixation, it is also important to look at the influence objects have on graphical password viability. In Tatler's work, he showed central bias exists regardless of where the objects are positioned. Aydin's study on the role of visual coherence in graphical passwords answers a few of the questions concerning how important having reference images are. Reference images are background images imposed on grids that allows for better recall on passwords. The participants of Aydin's study were first divided into two groups that worked with either a coherent background image or a jumbled background image. The jumbled image was used to test for the effects of visual coherence on memory. After creating a password, each group was then required to complete the password entering session twice, one with the background image and one without.

Immediately, having a coherent image returned a positive effect on memorability. The group with the coherent image recorded a success rate of 88%, whereas the jumbled image only recorded a success rate for 73%. While this was not the most intensive test, this did enough to show that having a coherent picture and being able to select passwords with relation to objects was beneficial to the password remembering process. The second session revealed more of the same. In tests without the background images, coherent images and jumbled images saw little change in memorability, with the success rate for jumbled images dropping slightly from 73% to 72% and the success rate for coherent images increasing from 88% to 90% [5]. While there wasn't much decline between the two success rates after removing the background image, the large difference in success rates between jumbled and coherent images did show that visual coherence played a huge part in user memorability in passwords.

Aydin's study used an algorithm provided by Walther and Koch to compute the saliency maps of both the jumbled and coherent images. The maps were then compared to the participants' password region choices to determine any possible relationships. Neither the jumbled map nor the coherent map indicated any sort of relationship between saliency distribution and user choice. This strengthens the realistic strength of graphical passwords, since grid systems are shown to be able to improve retention rates, while also not sacrificing available password spaces due to having areas of strong saliency values.

iii. User Preferences

Aside from innate vision biases that humans cannot avoid, another important bias is user preferences. Especially in this age where social information is so readily available to potential malicious users, social engineering has become a very effective method of retrieving potential passwords. In order to measure the effects of user preference, I created a survey to test the effects that race and color preference had on selecting password choices from PassFaces style authentication, as well as similar grid formatted authentication. A more detailed analysis of this survey is available in Appendix A

A PassFaces sample was presented to the participants as a 3x3 grid of faces with varying ethnicities and genders. Participants were asked to choose one of the images that they would remember best. Each image was not described by the ethnicities or gender of the person shown, as to avoid enforcing a bias on the users, but instead by its position on the grid itself. Each user was asked at the end of the survey to provide the ethnicity that they defined themselves. Of the 34 users, 20 defined themselves as "white" or "Caucasian"; 2 defined themselves as "black"; 5 defined themselves as "Asian"; 2 defined themselves as "Hispanic" or "Latinx"; 1 was defined as "Indian". There were 4 users that did not choose to define themselves as any ethnicity. Of the nine images available to be selected from, 4 of 9 could have been considered to be of Caucasian descent, 2 of 9 could be considered to be of African or Caribbean descent, and the remaining 3 looked to have Asian ancestry. This study looked to see if there was indeed a strong relationship

in preference for race overall and whether a user's race affected the choice of image. Ignoring location bias, each image should on the surface have an equal chance of being picks. Given the number of images of each race, the breakdown of the 34 choices should have been as follows: 15 choices for Caucasian, 7 choices for African or Caribbean, and 11 choices for Asian. The breakdown of actual user choices actually turned out to be extremely close to the this estimated spread. The Asian images were selected 12 times; the Caucasian images were selected 14 times; the African or Caribbean images were selected 8 times.

Taking the user's ethnicity into account revealed a little more. Of the 6 users that identified themselves as Asian or Indian, 5 users chose the images that could be identified to be of Asian ancestry. Since Asian images made up only a third of the total nine images, it would have been accurate to assume that, barring all location bias, of the 6 users only 2 would have chosen Asian faces. This elevated level of same race selection is reflected in those self-identifying as "black", which showed a 100% chance of selecting an image of "African" or "Caribbean" descent, despite only 2 of the 9 images being considered "African" or "Caribbean" images. The results for self-identifying Hispanics in the survey were hard to quantify, as there were no images in the grid for Hispanic users. The remaining users that identified as "Caucasian" matched the elevated rate of same race selection. While the "Caucasian" users tended to be more varied with their choices, 50% of the users chose "Caucasian" images, despite the expected rate to be around 44.4%.

This study was done on a small scale, but some interesting relations could be looked to be expanded upon in future studies. The most interesting portion is that on an overall level, the distribution for selected images was almost exactly the same as expected. Despite a skewed rate of selection for same race, there does not seem to be a bias towards a specific race overall. Thus, given an equal division of different faces with different ethnicities, PassFaces should be able to provide a relatively secure password to account for ethnicity bias. However, the extremely high rate of same ethnicity selecting does leave PassFaces weak to social engineering attacks on its users. By figuring out the ethnicity of the user, it may be easier to weed out the choices for a PassFaces like system. For this reason, more secure versions of PassFaces focus on creating safer dummy images that may be able to deter social engineering. Current setups look to match similar pictures with each, often matching hair color, facial features, and ethnicity to be able to better hide the image itself. While this may lower the individual memorability of the chosen image due to the user having to remember more components of the image, it would boost an added defense to social attacks. Unfortunately, the study did not include data on gender, due to its complex nature as a means for identifying the user, but gender definitely seems to be another area of study to look into in terms of bias.

The effects of user choice expand beyond specific instances, such as ethnic preference. Graphical memory has very strong ties to implicit memory. Whereas explicit memory deals with "conscious recollection of an event", implicit memory deals with "an improvement in some task performance as the result of having experienced the event". In the context of images, implicit memory means that users are better able to remember objects if they have seen them before. Implicit memory plays a huge role in deciding graphical password sequences since the user is more inclined to pick an image that he or she has seen before, or is more accustomed to, because it is easier to remember over long periods of time. A paper written by Angela Lee looked to examine how strong the effect of implicit memory was on memory-based versus stimulus-based choices. Participants were measured on their ability to recall brand names of consumer goods based on whether they had been presented to them before or not. As expected, users were able to, on average, remember 53% of the brands if they had seen them before versus an average of 20% if they had not been presented [37]. This demonstrates how power seeing an image

before is and how influential it can be when it comes to make password decisions. From a security standpoint, implicit memory acts as both a positive and a negative for graphical systems. As a positive, implicit memory improves memorability and improves recall for graphical images. This leads to faster login times and more efficient success rates. On the other hand, implicit memory also leads to more predictable password choices. Since users are more likely to remember things that they seen before, this also means that they are more likely to select objects that they have an affinity for. For example, in the situation where a dog was present in either a PassPoints-like scene system, or a grid-style system, a dog owner may be more inclined to choose that image as an element in his or her password sequence. Especially in a system that has relatively low password spaces, this becomes especially dangerous. This is not to reduce the risk of running into this problem in scene-based systems either. Since these scenes usually have large areas for error around each region, knowing what object will more likely be clicked shrinks the password space available.

iv. Low Level Image Bias

Low level image biases refer to biases involving basic attributes of images, such as color and orientation. Studies have shown that user attraction to specific regions can be mapped onto focus of attention maps. Ahmet Dirik proposed a formula that took into account object luminosity, color contrast, and foreground to determine which areas of the image were considered high values in the Focus of Attention map.

$$\begin{aligned} Focus of Attention(R) = W_1 * Luminosity(R) \\ + W_2 * ColorContrast(R) \\ + W_3 * Foreground(R) \end{aligned} \tag{3}$$

W_1, W_2, W_3 are calculated constants, R is the point being examined

Luminosity can be calculated by taking the grey level (or brightness) of a segment and comparing it to the segments neighboring it. Color contrast refers to the difference in hue levels, which are assigned a normalized RGB value. Lastly, foreground takes advantage of the fact that background images tend to have longer segments as opposed to objects in the foreground. This model was applied in Dirik's paper to a few practice images called Birds Image and People Image. Participants in the study were asked to create graphical passwords on one of these two images consisting of five clicks. To confirm that the chosen passwords were viable, the participants were required to enter it a second time. The predicted regions were compared against actual selected values, returning 80% accuracy on the Birds Image. The People image was much more clustered than the Bird image, but still returned a prediction accuracy of 71% [18]. These high accuracy of prediction values show that user preference is very attached to the values presented in the model. While the model could probably be improved by including additional variables involving corner points, the model based on color seems to be promising enough to focus on it. User preference for color is actually much larger than user preference for any other attribute. According to a study done by Muhammad Abdullah, 89% of the 63 people surveyed preferred color to black and white images for graphical passwords. This difference between the two was the largest out of all components including size and presentation. This shows that given systems that require strict image memory or region memory users prioritize color above increased size for security and presentation of the password on different screens [1].

To test color bias, the study referenced in Appendix A also included questions prompting for favorite color after selecting from a screen of possible color related graphical passwords. No option was made up of a solid color, which limited how accurate color preference could be. Out of the 32 entries that listed a color preference, 15 color preferences were in the palette of the chosen image. While this finding seems

to demonstrate that color choice is not a very good indicator for image selection, of the 15 participants that indicated blue to be their favorite color, 12 selected images that contained blue in them. Looking at each image, it can be seen that blue is a heavily featured color in of 8 of the 15 presented images. This distribution actually strongly influences both of the previously represented statistic. Since blue is the largest represented color, it skews the likelihood that blue is selected in any of the images. Thus, the 15 color preference matches could be overestimated since there is such a high probability that the large number of participants who chose blue were attracted to other aspects of the images that had just so happened to also contained blue. Color bias definitely leaves much more to be examined. Showing users color choices in the same format as other grid styles leaves the choice to be influenced by location bias, which was unable to be accounted for in the Dartmouth survey. With that being said, being able to create different image choices that better embodied the parameters and colors that were being tested may have improved the accuracy of the study.

It can be drawn from the two studies done that there are indeed a few ways that low level bias can affect graphical password security. First, the combination of factors that build into Focus of Attention maps is a strong indicator of preference. While this mainly affects selections in scenes, it does demonstrate the viability of malicious users minimizing possible choices given images with fewer focus of attention areas. Secondly, color bias alone seems to be a relatively weak determiner on its own. This is not to say that color preference has no role in strengthening memory, but instead may have skewed results based on the pool of images shown. Systems can look to weaken the effects that low level bias has by first adding more objects with level focus of attention levels, to open password spaces and reduce the likelihood that malicious users will be able to brute force passwords. Grid style images can also look to develop images that avoid possible color preference bias, while maintaining higher levels of memorability.

v. Concluding Visual Biases and Social Engineering

Visual biases and human preference are not easy weaknesses to overcome in a short interval of time. Graphical passwords unfortunately suffer from an extreme reliance on the strengths and weaknesses of images and memory. While images often improve memory, they become too imbedded into the user's mind, creating subconscious user bias. This may result in the user choosing images that he or she has close affiliation for, such a tennis player choosing a tennis racquet image for an element in a password sequence. These biases on a whole lower the effective security level of graphical password authentication because of reducing the real password spaces. To improve security, there must be an investment in creating images that reduce the impact of bias. PassFaces already accomplishes this by forcing users to choose their password image from a group of very visually similar photos, while PassPoints requires background to have multiple objects of focus. This weakness is definitely the hardest obstacle for graphical passwords to overcome because of how ingrained some of these weaknesses are. But given enough time, systems will adjust and compensate for their weaknesses and be able to put forward more secure authentication options

vi. Concluding Weaknesses and Looking Forward

This section has exposed two of the main weaknesses that graphical passwords face when it comes to real time usage. Shoulder surfing is an underestimated technique that exposes the weaknesses of graphical passwords, while human bias is an innate problem that comes with user interaction with the system itself. Both problems limit the effective password space that was previously shown to be much larger than those of alphanumerical passwords. This shows that graphical passwords are not as se-

cure as have been demonstrated in theoretical research. This is not to say that solutions to these weaknesses are not currently available, but that these solutions may not be the best choice to make. There is a fine balance between improving security and maintaining a good level of usability. Introducing keyboard entry is a strong counter to shoulder surfing, but may increase password entry time, turning off users from consistently choosing the method. Color and location bias adjustments may reduce the number of images that can be used as backgrounds, forcing default backgrounds to be offered, reducing the variability in password choice. Nonetheless, at the end of the day, it comes down to how much the strengths of the authentication methods offset or compensate for the weaknesses.

The next section will be focusing on bringing together the strengths and weaknesses of graphical passwords to explore the viability of graphical password in different environments and usage scenarios.

V. Addressing Viability

Having already looked at the strengths and weaknesses of graphical passwords, it is important to address these in the scope of real-time usability. Passwords and authentication are used in many different environments and with different expectations. Depending on the situation, user convenience may take priority over higher levels of security and vice versa. This section will look at the three major environments for authentication: personal, professional, and governmental/high security.

i. Personal Viability

Personal viability is characterized by usage in a home or in an environment where other people usually do not have access to your work station. This can range anywhere from the laptop in a dorm room to a computer in a personal office. These environments usually prioritize usability over any other factor, including security. Since these environments are usually isolated from any potential shoulder surfing or local threats, there is no visible need to create extremely complicated password sequences. Users will gladly sacrifice security for a shorter login entry time. This is usually because the user will most likely access their computer multiple times a day and are unwilling to enter long complicated passwords each time to login, especially if it is to perform common tasks, like sending emails.

For this reason, alphanumerical passwords are usually the authentication of choice for machines that are normally used in personal environments. Alphanumerical passwords are quicker to enter than graphical passwords and usually have very low tradeoff between increasing length and time required to log in. This means that if the need to increase security presents itself, users will be able to make small adjustments to their passwords without sacrificing convenience. While from a speed angle, biometric passwords seem to be much quicker and more secure, it is unrealistic to assume that everyone has the money to afford biometric scanners on their desktops or laptops, especially if they do not come preloaded onto the computer. However, retina scans and fingerprints are both widely available, but the wear and tear of hourly use on these home quality scanners will result in shorter lifespans for the hardware itself. Until biometric scanners become more prevalent in everyday, it is unrealistic to assume that biometric authentication is the most viable means for personal use.

Furthermore, alphanumerical passwords have been the standard for so long that every device basically uses a form of it. This means that regardless of whether someone owns a computer, they will know the basics on how to enter a password. Graphical passwords do not have that luxury and may require the user to spend time learning the system, which may be inconvenient.

With that being said, graphical passwords definitely do show signs of rapidly becoming accepted. In the survey referenced in the Appendix, users were prompted for how much longer they were willing to extend their login

time by if they were guaranteed better security. Only 20.5% of the participants indicated that they were unwilling to extend their log in time at all, with 58.8% willing to extend it for 1-5 seconds. This indicates a willingness to sacrifice time to improve security, as long as the tradeoff in time is not egregious. Thus, PassFaces and other simpler forms of graphical passwords will be acceptable means of personal security, especially if they can be demonstrated to the public, as being more secure.

ii. Professional Viability

Professional viability is harder to quantify since there are many different types of careers, but authentication is usually held to a higher security standard and companies are more willing to sacrifice time for greater security. For the sake of encompassing the majority of careers, professional viability will be looked at from two angles: intensive computer usage and non-intensive computer usage.

Careers that have intensive computer usage will tend to value authentication measures that have both high security and a relatively low password entry time. This actually makes them the most suitable candidate for graphical passwords. Previous sections have already shown the high password space that graphical passwords provide, as well as a comparable login speed. Susan Wiedenbeck's PassPoints study showed that immediately after creation graphical passwords only took on average 3.55 seconds longer to log in. Week one represented the largest difference with a gap of 14.83 seconds, but by four weeks, the time had shrunk to 10.14 seconds [71]. While we do see a noticeable difference in performance, the shrinking of the gap between week two and week three is optimistic for better performances in the future. Reducing the gap to around 5 seconds definitely seems completely possible, putting it in the range of what the Dartmouth study showed to be a reasonable extension of login time, making it a viable option for intensive computer careers. The main qualm with graphical passwords in computer intensive environments is the problem of shoulder surfing. Many of these computer intensive careers have users work in cubicles or in close proximity to other employees. This means that, even without the malicious intent to break into another account, the likelihood of accidentally seeing the graphical password is relatively high. This can be adjusted for by requiring, as most companies already do, that employees change their passwords every few weeks to prevent phished or stale passwords from being used.

Alternatively, careers that do not have intensive computer usage also may look into graphical passwords, although a slightly different reason. Since these occupations, like nurses and other service industry jobs, do not require the active use of a computer, it can be expected that they will only log on after long periods of time. These jobs will tend to value memorability and usability of passwords rather than high levels of security. Because of the lack of consistent traffic from a specific user, the probability that the user will have their information phished is incredibly small. However, the password must also be memorable enough for the user to enter the password after a long period of not using it. Graphical passwords satisfy this need incredibly well. Previously, graphical passwords have been shown to have a retention rate equal to or better than the standard alphanumeric. Since infrequent usage gives fewer opportunities for other users to shoulder surf, there is very little trade off for security. Another reason is that graphical passwords are less likely to face detrimental memory shortcuts than alphanumerical passwords are. As has been stressed in previous sections, graphical passwords are very strongly imaged based, which means that the user is often times remembering the image itself, rather than a sequence of words that describe the picture or region in the sequence. This means that users often have a difficult time describe to other people what their password is, especially if they are selecting from a grid of very similar images. By having a harder time describing their image with words, the user is less likely to attach notes or hints to their workstations to help remember their

password. This prevents malicious users from abusing these shortcuts to undermine security.

In the scope of professional authentication, the graphical password does well because of the lack of emphasis on having the quickest entry time. Biometric authentication may be a better answer for non-computer intensive fields, as it is the most secure and has probably the shortest entry time of all methods. However, there currently still is some ethical reservations about giving private companies access to their employees' biometric information. Until then, graphical passwords will see a raise in share of authentication in the near future.

iii. Governmental Viability

Governmental viability is characterized by high levels of security and the willingness to sacrifice speed for stronger authentication measures. While this environment seems to be the strongest avenue for graphical password use, due to its low prioritization of speed, biometric authentication fits this niche perfectly.

Biometric authentication remains currently the strongest form of authentication available. This is because no two people can have the same fingerprint or retina pattern. This means that if the scan or the pattern matches, the person authenticating must be the same person that has his or her information stored in the system. This level of confirmation is much stronger than graphical or alphanumeric passwords, where any user can realistically enter another user's password without the system being able to tell the difference. As much of these governmental institutions have the resources to install top of the line scanners and hardware, the normally expensive hurdle to implementing biometric authentication is overcome. At the same time, there is much less of an ethic issue if the government keeps ahold of biometric signatures because of the relatively ease that most citizens feel with their government keeping information.

There really is not as much to elaborate on since it is hard to argue for a switch to a weaker from of authentication when the means and infrastructure of a stronger one has already been implemented and brought to protocol.

iv. Concluding Viability

Graphical passwords perform comparably with alphanumerical passwords, but do not do well enough in most cases to justify replacing alphanumerical passwords. Much of the reluctance to switch comes from the infrastructure and protocol that has been instated already. However, this is not to say that graphical passwords will not see real time usage in the near future. The strengths of providing high security along with high retention rates will become infinitely more important once malicious users have faster computers to beat current password encryption. Graphical passwords offer very high password spaces in proportion to the size of the graphical image or grids being used. Combined with high retention rates, these systems look to be the next avenue of exploration for everyday authentication.

VI. Conclusion

Graphical passwords are arguably the most exciting form of authentication in recent years. From Blonder's vision in his patent to the Android Pattern Lock available today, graphical passwords have only started to recognize their full potential. This thesis looked to analyze viability of graphical passwords from both a theoretical and real world application level. Theoretically, graphical passwords are extremely sound; the large password spaces and utilization of the dual-code theory of memory allow for high retention rates, while also maintaining a high level of security. Effectively, graphical passwords on the surface should fill the niche of alphanumerical passwords quite well and offer a convenient solution to faster computer built to break current encryption.

However, as we have come to see, graphical passwords still have a lot of work before they can be introduced commercially, but have quite a high ceiling of potential. Graphical passwords have to deal with a lot of the weaknesses

in dealing with images. Vision and preference bias reduce the effective password spaces and careful Focus of Attention analysis could result in abuse of hotspots in graphical passwords. Shoulder surfing and long entry times introduce problems unique to graphical passwords, creating problems for entering passwords in the close proximity of a possible malicious user. Alternatives to click based passwords are still in the works, but the suggested mediums of entry prove to be cumbersome and may detract from the overall security level.

Nonetheless, graphical passwords do offer shallow learning curves coupled with better retention rates than alphanumerical passwords. Combined with the numerous different styles of authentication, graphical passwords have the potential to be ubiquitous and satisfy the needs of many different environments. Their ability to protect themselves from more common sources of phishing, like keyloggers and users writing down passwords, makes them more secure for the average user. The only thing standing in the way is overcoming old standards and creating more comfort for users today.

Given enough time to develop more protocols and infrastructure, graphical passwords will be the standard for authentication and are indeed viable for real-time use.

VII. Appendix A

To augment my thesis, I created a survey to look for the effect of color preference and ethnicity on graphical password selection. The questions and requested information are represented below. Full sized images will be available in th

i. Methodology

The survey was sent out through the Dartmouth Ultimate Frisbee listserv to search for participants. The choice of listserv was intentional, as the listserv contains a wide variety of people with varying ethnicities and preferences. This should give us a relatively good distribution of students to retrieve data from. The survey itself was designed on Qualtrics. Qualtrics was chosen because of my familiarity with the service, having used it in CS 55: Security and Privacy before. Qualtrics surveys

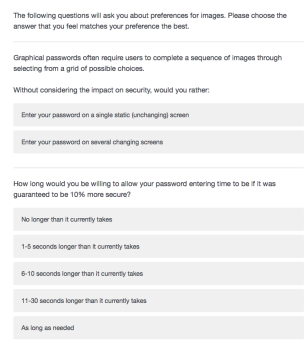

Figure 1: *Question 1 and 2*

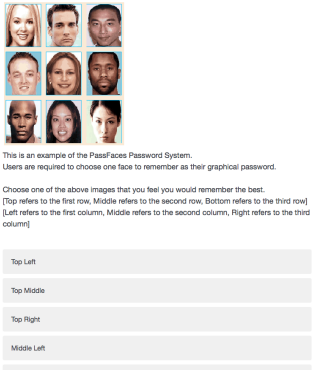

Figure 2: *Question 3*

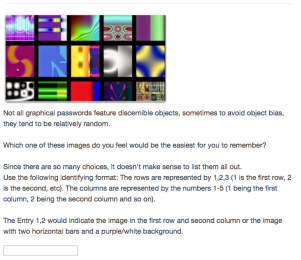

Figure 3: *Question 4*

Figure 4: *Question 5*

are also usually very readable on mobile devices, which would increase convenience and encourage more people to participate in the survey.

The participants were told in advance that the questions would ask about preferences for images, but were not prepped on the purpose of each question, nor briefed any background of graphical passwords. This was done specifically to prevent any bias that would result from knowing the style or input that the graphical password required.

At the end of the survey, participants were asked to indicate some basic information about themselves. This information included: Student Year, Type of Mobile Device, Ethnicity, Favorite Color, and Favorite Type of Animal. The most important pieces of information listed here were Ethnicity and Favorite Color, since the two were the factors that the study was specifically examining for. I did not ask for the gender nor name of the participant, as I felt that it would have provided too many variables to account for.

All of the raw data entered by users will be kept as an CSV file that will be included in the git-hub accompanying this thesis.

ii. Question Analysis

While there were 4 questions asked overall, not including the last information gathering portion, only questions 2, 3, and 4 were really applicable to the study. I will go over the reasoning behind each question and try to illustrate what information could gather from the results.

iii. Question 2

Question 2 focused on seeing how long of an extended period logging in most users would tolerate for a password 10% more secure. Graphical passwords on average take longer to authentication than alphanumerical passwords. This question was inserted to mainly check for user preference for speed and ease of use. The results are indicated below:

#	Answer		Response	%
1	No longer than it currently takes		9	25%
2	1-5 seconds longer than it currently takes		22	61%
3	6-10 seconds longer than it currently takes		3	8%
4	11-30 seconds longer than it currently takes		1	3%
5	As long as needed		1	3%
	Total		36	100%

Figure 5: *Statistics for Question 2*

For the most part, users demonstrated a reluctance to extend their login process by more than 5 seconds, with 86% of those survey selecting an option 5 seconds or under. This indicates that time is extremely precious to users, especially if the security gained is not super noticeable.

iv. Question 3

Question 3 was focused on exposing participants to a real-life sample of the PassFaces Password System.

The users were asked to pick a face that they would be able to remember best. In order to avoid influencing the users by applying ethnic descriptions to the faces, I used positions to allow participants to indicate preference.

The portraits in the top left, top middle, middle left, and middle middle were classified as Caucasian.

The portraits in the top right, bottom middle, and bottom left were classified as Asian.

The portraits in the middle right and bottom left were classified as African or Caribbean descent.

#	Answer		Response	%
1	Top Left		3	8%
2	Top Middle		3	8%
3	Top Right		7	19%
4	Middle Left		8	22%
5	Middle Middle		0	0%
6	Middle Right		4	11%
7	Bottom Left		6	17%
8	Bottom Middle		1	3%
9	Bottom Right		4	11%
	Total		36	100%

Figure 6: *Statistics for Question 3*

The statistics and more specific analysis was completed in Section 3. This section wanted to focus on how much ethnic preference affected user choice of the pictures. Question 5 included a place for the participant to self

identify their ethnicity, which gave us a factor to base preference off of.

v. Question 4

This section was focused on presenting participants with a grid style graphical authentication that mainly looked to test user preference for color. In order to prevent color preference bias, I used a coordinate system model to allow users to pick.

Obviously, each image is a mix of colors, but the focus was to determine if the color that the user indicated as a preference, in question 5, was present at all in the palette of the image chosen.

To quickly illustrate which colors were considered to be visible in each palette and the number of times chosen:
Entry 1,1: Purple and White (1)
Entry 1,2: Purple, White, Blue (1)
Entry 1,3: Red, Green, Blue, (3)
Entry 1,4: Blue and red (2)
Entry 1,5: Purple and Green (1)
Entry 2,1: Orange and Red(Magenta) (6)
Entry 2,2: Blue (3)
Entry 2,3: Yellow, Pink, Blue (2)
Entry 2,4: Black and White (1)
Entry 2,5: Yellow and Blue (3)
Entry 3,1: Black and white (7)
Entry 3,2: Green and Black (3)
Entry 3,3: Red and Blue (1)
Entry 3,4: Purple, Blue (0)
Entry 3,5: Red and Green (1)

vi. Question 5

Question 5 was mainly just a data gathering portion. The key points to notice are the ethnicity and favorite color columns. These statistics are analyzed more in depth in Section 3.

vii. Note

Please find the larger images in my github. I will also provide larger copies of the images and a raw copy of the CSV in my submissions as well.

References

[1] Abdullah, Muhammad Daniel Hafiz B., Abdul Hanan B. Abdullah, Norafida Ithnin, and Hazinah Kutty Mammi. 2008. "Graphical password: User's affinity of choice - an analysis of picture attributes selection." 2008 International Symposium on Information Technology 1-6.

[2] Accot, Johnny, and Shumin Zhai. 1999. "Performance evaluation of input devices in trajectory-based tasks: an application of the steering law." Proceedings of the SIGCHI conference on Human Factors in Computing Systems 466-472.

[3] Adams, Anne, and Martina Angela Sasse. 1999. "Users are not the enemy." Communications of the ACM 1999.

[4] Angeli, Antonella De, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. " Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems." International Journal of Human-Computer Studies 128-152.

[5] Aydïn, Ülkü Arslan, and Cengiz Acartürk. 2013. "The Role of Visual Coherence in Graphical Passwords." Proceedings of the 35th Annual Meeting of the Cognitive Science Society 1774-1779.

[6] Biddle, Robert, Sonia Chiasson, and P.C. Van Oorschot. 2012. "Graphical passwords: Learning from the first twelve years." ACM Computing Surveys 1-1.

[7] Bindemann, Markus. 2010. "Scene and screen center bias early eye movements in scene viewing." Vision Research 2577-2587.

[8] Blonder, Greg E. 1996. Graphical password . USA Patent US5559961 A. September 24.

[9] Card, Stuart K., Allen Newell, and Thomas P. Moran. 1983. The Psychology of

Human-Computer Interaction. Hillsdale, NJ: L. Erlbaum Associates Inc.

[10] Card, Stuart K., Thomas P. Moran, and Allen Newell. 1980. "The keystroke-level model for user performance time with interactive systems." Communications of the ACM 396-410.

[11] Chiang, Hsin-Yi, and Sonia Chiasson. 2013. " Improving user authentication on mobile devices: a touchscreen graphical password." Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services 251-260.

[12] Chiasson, Sonia, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. 2009. "Multiple password interference in text passwords and click-based graphical passwords." Proceedings of the 16th ACM conference on Computer and communications security 500-511.

[13] Chong, Ming Ki, and Gary Marsden. 2009. "Exploring the Use of Discrete Gestures for Authentication." Human-Computer Interaction âĂŞ INTERACT 2009 205-213.

[14] CSID. 2012. Consumer Survey: Password A study of password habits among American consumers. September. https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf.

[15] Davis, Darren, Fabian Monrose, and Michael K. Reiter. 2004. "On user choice in graphical password schemes." Proceedings of the 13th conference on USENIX Security Symposium 11-11.

[16] Derrick Parkhurst, Klinton Law, Ernst Niebur. 2002. "Modeling the role of salience in the allocation of overt visual attention." Vision Research 107-123.

[17] Dhamija, Rachna, and Adrian Perrig. 2000. " Dëjä Vu: a user study using images for authentication." Proceedings of the 9th conference on USENIX Security Symposium 4-4.

[18] Dirik, Ahmet Emir, Nasir Memon, and Jean-Camille Birget. 2007. " Modeling user choice in the PassPoints graphical password scheme." Proceedings of the 3rd symposium on Usable privacy and security 20-28.

[19] Dunphy, Paul, and Jeff Yan. 2007. "Do background images improve "draw a secret" graphical passwords?" Proceedings of the 14th ACM conference on Computer and communications security 36-47.

[20] Dunphy, Paul, James Nicholson, and Patrick Olivier. 2008. "Securing passfaces for description." Proceedings of the 4th symposium on Usable privacy and security 24-35.

[21] Everitt, Katherine M., Tanya Bragin, James Fogarty, and Tadayoshi Kohno. 2009. " A comprehensive study of frequency, interference, and training of multiple graphical passwords." Proceedings of the SIGCHI Conference on Human Factors in Computing Syste 889-898.

[22] Fecteaua, Jillian H., Ilia Korjoukova, and Pieter R. Roelfsemaa. 2009. "Location and color biases have different influences on selective attention." Vision Research 996-1005.

[23] Forlines, Clifton, Daniel Wigdor, Chia Shen, and Ravin Balakrishnan. 2007. "Direct-touch vs. mouse input for tabletop displays." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 647-656.

[24] G, Pramoth, and Mukesh Krishnan M. B. 2014. "Achieving Shoulder Surfing Resistant Authentication Using Graphical Password." International Journal of Engineering Research & Technology.

[25] Hartanto, Budi, Bagus Santoso, and Siauw Welly. 2007. "The usage of graphical pass-

word as a replacement to the alphanumerical password." Jurnal Informatika 7, no. 2 -91.

[26] Hochstein, Lorin. 2002. GOMS. October. http://www.cs.umd.edu/class/fall2002/cmsc838s/tichi/printer/goms.html.

[27] Hollingworth, A., and J. M. Henderson. 2002. "Accurate visual memory for previously attended objects in natural scenes." Journal of Experimental Psychology: Human Perception and Performance 113-136.

[28] Hollingworth, Andrew. 2009. "Two forms of scene memory guide visual search: Memory for scene context and memory for the binding of target object to scene location." Visual Cognition 273-291.

[29] Itti, Laurent, and Christof Koch. 2001. "Computational modelling of visual attention." Nature reviews neuroscience 2 194-203.

[30] Itti, Laurent, Christof Koch, and Ernst Niebur. 1968. "A Model of Saliency-Based Visual Attention for Rapid Scene Analysis." IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 1254-1258.

[31] Jermyn, Ian, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. 1999. "The Design and Analysis of Graphical Passwords ." Proceedings of the 8th USENIX Security Symposium 1-15.

[32] Kieras, David. 2001. Using the Keystroke-Level Model to Estimate Execution Times. http://www-personal.umich.edu/~itm/688/KierasKLMTutorial2001.pdf.

[33] Kimwele, Michael, Waweru Mwangi, and Stephen Kimani. 2009. "Strengths of a Colored Graphical Password Scheme." International Journal of Reviews in Computing 64-69.

[34] Komanduri, Saranga, and Dugald R. Hutchings. 2008. "Order and entropy in picture passwords." Proceedings of Graphics Interface 2008 115-122.

[35] Kumar, Manu, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. "Reducing Shoulder-surfing by Using Gaze-based Password Entry." Proceedings of the 3rd symposium on Usable privacy and security 13-19.

[36] Lashkari, Arash Habibi, Samaneh Farmand, Dr. Omar Bin Zakaria, and Dr. Rosli Saleh. 2009. "Shoulder Surfing attack in graphical password authentication." International Journal of Computer Science and Information Security 145-154.

[37] Lee, Angela Y. 2002. "Effects of Implicit Memory on Memory-Based versus Stimulus-Based Brand Choice." Journal of Marketing Research 440-454.

[38] Mackenzie, I. Scott, Abigail Sellen, and William A. S. Buxton. 1991. "A comparison of input devices in element pointing and dragging tasks." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 161-166 .

[39] Man, Shushuang, Dawei Hong, and Manton M. Matthews. 2003. "A Shoulder-Surfing Resistant Graphical Password Scheme-WIW." Security and Management 105-111.

[40] Marat, Sophie, Anis Rahman, Denis Pellerin, Nathalie Guyader, and Dominique Houzet. 2013. "Improving Visual Saliency by Adding 'Face Feature Map' and 'Center Bias'." Cognitive Computation 63-75.

[41] Martin, Maryanne, and Gregory V. Jones. 1995. "Integral bias in the cognitive processing of emotionally linked pictures." British Journal of Psychology 419-435.

[42] Massey, James L. 1994. "Guessing and entropy." 1994 IEEE International Symposium on Information Theory 204.

[43] Nelson, Douglas L., Valerie S. Reed, and Cathy L. McEvoy. 1977. "Learning to order

pictures and words: A model of sensory and semantic encoding." Journal of Experimental Psychology: Human Learning and Memory 485-497.

[44] Omanson, Richard C., Craig S. Miller, Elizabeth Yang, and David Schwantes. 2010. "Comparison of Mouse and Keyboard Efficiency." Proceedings of the Human Factors and Ergonomics Society 600-604.

[45] Parkhurst, Derrick J., and Ernst Niebur. 2003. "Scene content selected by active vision." Spatial Vision 125-154.

[46] Peng Foong Ho, Yvonne Hwei-Syn Kam, Mee Chin Wee, Yu Nam Chong, and Lip Yee Por. 2014. "Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information." The Scientific World Journal 1-12.

[47] Peters, Robert J., Asha Iyer, Laurent Itti, and Christof Koch. 2005. "Components of bottom-up gaze allocation in natural images." Vision Research 2397-2416.

[48] Prakash, M. Arun, and T. R. Gokul. 2011. " Network security-overcome password hacking through graphical password authentication." Innovations in Emerging Technology (NCOIET), 2011 National Conference on 43-48.

[49] Salehi-Abari, Amirali, Julie Thorpe, and P. C. van Oorschot. 2008. "On Purely Automated Attacks and Click-Based Graphical Passwords." Annual Computer Security Applications Conference 111-120.

[50] Schaub, Florian, Ruben Deyhle, and Michael Weber. 2012. "Password entry usability and shoulder surfing susceptibility on different smartphone platforms." Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia 13-13.

[51] Schneier, Bruce. 2010. Schneier on Security. November 11. https://www.schneier.com/blog/archives/2010/11/changing_passwo.html.

[52] Schumann, Frank, Wolfgang Einhäuser, Johannes Vockeroth, Klaus Bartl, Erich Schneider, and Peter König. 2008. "Salient features in gaze-aligned recordings of human visual input during free exploration of natural environments." Journal of Vision 1-1.

[53] Sears, Andrew, and Ben Shneiderman. 1991. "High precision touchscreens: design strategies and comparisons with a mouse." International Journal of Man-Machine Studies 593-613.

[54] Sears, Andrew, Catherine Plaisant, and Ben Shneiderman. 1992. A new era for high precision touchscreens. Norwood, NJ: Ablex Publishing Corp.

[55] Stenberg, Georg. 2006. " Conceptual and perceptual factors in the picture superiority effect." EUROPEAN JOURNAL OF COGNITIVE PSYCHOLOGY 1-35.

[56] Stobert, Elizabeth, Sonia Chiasson, and Robert Biddle. 2011. "User-choice patterns in passtiles graphical passwords." Annual Computer Security Applications Conference (ACSAC), vol. 2011 1-1.

[57] Suo, Xiaoyuan, Ying Zhu, and G. Scott. Owen. 2005. "Graphical Passwords: A Survey." Proceedings of the 21st Annual Computer Security Applications Conference 462-472.

[58] Tao, Ha. 2006. Pass-Go, a new graphical password scheme. PhD diss., University of Ottawa.

[59] Tari, Furkan, A. Ant Ozok, and Stephen H. Holden. 2006. " A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." Proceedings of the second symposium on Usable privacy and security 56-66.

[60] Tatler, Benjamin W. 2007. "The central fixation bias in scene viewing: Selecting an optimal viewing position independently

of motor biases and image feature distributions." Journal of Vision 1-1.

[61] Thorpe, Julie, and P. C. van Oorschot. 2007. "Human-seeded attacks and exploiting hot-spots in graphical passwords." Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium 8-8.

[62] Thorpe, Julie, and P.C. van Oorschot. 2004. "Towards Secure Design Choices for Implementing Graphical Passwords." Proceedings of the 20th Annual Computer Security Applications Conference 50-60.

[63] Thorpe, Julie, and Paul van Oorschot. 2004. "Graphical Dictionaries and the Memorable Space of Graphical Passwords." Proceedings of the 13th USENIX Security Symposium 135-150.

[64] Towhidi, Farnaz, and Maslin Masrom. 2009. " A Survey on Recognition-Based Graphical User Authentication Algorithms." International Journal of Computer Science and Information Security, 119-127.

[65] Treisman, Anne M., and Garry Gelade. 1980. "A Feature-Integration Theory of Attention." Cognitive Psychology 97-136.

[66] Tseng, Po-He, Ran Carmi, Ian G. M. Cameron, Douglas P. Munoz, and Laurent Itti. 2009. "Quantifying center bias of observers in free viewing of dynamic natural scenes." Journal of Vision 1-16.

[67] Varenhorst, Christopher, M. V. Kleek, and Larry Rudolph. 2004. "Passdoodles: A lightweight authentication method." Research Science Institute.

[68] Wayman, James, Anil Jain, Davide Maltoni, and Dario Maio. ”An introduction to biometric authentication systems”. Springer London, 2005.

[69] Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. "Authentication using graphical passwords: effects of tolerance and image choice." Proceedings of the 2005 symposium on Usable privacy and security 1-12.

[70] Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. "PassPoints: Design and longitudinal evaluation of a graphical password system." International Journal of Human-Computer Studies 102-127.

[71] Wiedenbeck, Susan, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. "Design and evaluation of a shoulder-surfing resistant graphical password scheme." Proceedings of the working conference on Advanced visual interfaces 177-184.

[72] Williams, Leonard J. 1988. " Tunnel Vision or General Interference? Cognitive Load and Attentional Bias Are Both Important." The American Journal of Psychology 171-191.

[73] Yan, Jianxin, Alan Blackwell, Ross Anderson, and Alasdair Grant. 2004. "Password Memorability and Security: Empirical Results." IEEE Security and Privacy 25-31.

[74] Yang, Yulong, Janne Lindqvist, and Antti Oulasvirta. 2014. "Text entry method affects password security." The LASER Workshop: Learning from Authoritative Security Experiment Results.

[75] Zhai, Shumin, Barton A. Smith, and Ted Selker. 1997. "Improving Browsing Performance: A study of four input devices for scrolling and pointing tasks." Proceedings of INTERACT97: The Sixth IFIP Conference on Human-Computer Interaction 286-292.

[76] Zimmerman, Michael. 2002. Biometrics and User Authentication. SANS Institute.