

Image-Based Password Usability Study

By

Stephen Dolan

A Master's Paper Submitted to the Faculty of the

DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

ELLER COLLEGE OF MANAGEMENT

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2016

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona.

Brief quotations from this thesis are allowable without special permission, provided that an accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Stephen Dolan

APPROVAL BY MASTERS PAPER ADVISOR

This thesis has been approved on the date shown below:

_____ 05/17/2016

Dr. Jesse Bockstedt

Date

Associate Professor of Management Information Systems

_____ 05/17/2016

Dr. Matthew Hashin

Date

Assistant Professor of Management Information Systems

TABLE OF CONTENTS

LIST OF FIGURES	6
LIST OF TABLES	7
ABSTRACT	8
1 INTRODUCTION	8
2 BACKGROUND AND RESEARCH QUESTIONS.....	10
2.1 Background and Literature Review.....	10
2.1.1 Insecure Passwords	10
2.1.2 Password Creation Policies.....	13
2.1.3 Large Scale Data Breaches	19
2.1.4 Research Gaps and Questions.....	21
3 EXPERIMENT METHODOLOGY	23
3.1 Introduction / Approach	23
3.2 Experiment Methodolgy.....	25
3.2.1 Questions to be Answered	25
3.2.2 A 2x2 Approach.....	25
3.2.3 Conducting the Study.....	26
3.3 Results	27
3.3.1 Initial Password Recollection	27
3.3.2 Long-Term Password Recollection.....	28

3.3.3	The Effect of Time.....	29
4	REFERENCES	31

LIST OF FIGURES

Figure 1: Most Commonly Occurring Passwords for RockYou.com, Faithwriters.com, and Myspace.com	11
Figure 2: Effect of Limiting Dictionary Words	13
Figure 3: Effect of Adding Special Characters	14
Figure 4: Effect of Adding Uppercase	15
Figure 5: Effect of Increasing Password Length.....	16
Figure 6: Authentication Flow	24
Figure 7: 2x2 Methodology	26
Figure 8: 2nd Password Attempt.....	28
Figure 9: 3rd Password Attempt	29
Figure 10: Recollection After One Week	30

LIST OF TABLES

Table 1: Most Commonly Occurring Passwords Among Various Sites.....	12
Table 2: Password Traits.....	12
Table 3: Most Frequent Numerical Values.....	18
Table 4: Placement of Numerals.....	18
Table 5: Successful Memory Recalls.....	23

ABSTRACT

Online authentication methods have long been considered insecure and vulnerable to theft and attack. Previous research has identified password creation habits, semantics in passwords, and the effects of password creation policies on user behavior. Additionally, studies have measured password strength using cracking algorithms and developed adaptive password-strength models. However, little work has been done to identify a method of online user authentication that differs from traditionally accepted passwords. In this research, we develop a new way to create a password, using images instead of ASCII characters. We also gather data from multiple password creation interfaces to analyze the usability of image-based passwords.

1 INTRODUCTION

It is no surprise that data security has been brought to the attention of the public in recent years. Many large organization have reported data breaches and thefts that have left millions of users vulnerable. In 2014 alone, more than one billion personal records were illegally accessed, including health, financial, email and home address data, and other personal information like Social Security numbers. That's up more than 54 percent on the year prior (Whittaker, 2016). Data theft has become an increasingly serious problem as attackers evolve quickly to stay ahead of security technology. Their motivation is simple: financial gain. "These days, criminal hacking is a business," Patrick Thomas, a security consultant at [Neohapsis](#), tells *Fast Company*. "Everything that is done has a chain linked to real dollars. And hackers are looking for the shortest chain."

Sometimes, that entails stealing credit card numbers directly. Other times, it's selling user emails and passwords en masse on the deep web. Whether it involves an SQL injection or the exploitation of faulty script (Gayomali, 2014). Organizations have responded to this growing threat, as evidenced by their ever-expanding information security spending. Worldwide spending on information security will reach \$75.4 billion in 2015, an increase of 4.7 percent over 2014, according to the latest forecast from Gartner, Inc. The increase in spending is being driven by government initiatives, increased legislation and high-profile data breaches (Moore, 2015). However, even with the exponential increase in spending on information security, data breaches and thefts still happen far too often. But why? Doesn't the increased spending provide enough security to prevent these attacks from occurring on such a frequent basis? The answer is people. Human beings are still the weakest link in the aforementioned chain to real dollars. "Humans can't be upgraded," says security blogger Graham Cluley. "You can't fix the bug in people's brain that makes them click a link, or choose a really dumb password" (Gayomali, 2014). All this means that regardless of an organization's spending on enhanced information security methods, users' data still remains vulnerable to theft because of their own lack of security concern. But how we can influence users to be more mindful of the risks associated with weak passwords? Many organizations incorporate password creation policies in their online authentication methods. These policies require users to use specified characters when creating their passwords. By adding uppercase and lowercase letters, numbers, and special characters to a password greatly increases its strength, as measured in its inability to be compromised during an attack. However, as research has shown, password creation policies are often negated by creating an even less secure password for the sake of memorability. So, if we can't get users to create stronger passwords, how do we increase data security online? We have designed and developed a new method of online authentication. Rather than the traditional ASCII-based passwords, we propose using images to authenticate a users' identity online. Research has shown that pictures are easier to recall than printed words. This is known as the picture superiority effect. In 2002, Paul Foos and Paula Goolkasian conducted experiments on human memory in regards to recognition rates of pictures and words. Participants attempted to remember concrete nouns, presented as printed words, spoken words, or pictures, while verifying the accuracy of math sentences. The results showed that items presented as spoken words or as pictures produced

better recall and recognition than printed words did. Reaction time and accuracy on the processing component of the dual task were maintained at a relatively stable rate despite variation in modality/format for the to-be-remembered items. These results suggest that the previously found advantages of pictures over printed words and of spoken words (auditory presentation) over printed words may be due to the same mechanism(s) (Foos & Goolkasian, 2005). This research suggests that a password based on images would be easier to remember than a one based on letters or words. In theory, if a password was easier to remember, users would be more likely to consider security when creating theirs. This would result in stronger passwords across all organizations that implemented this image-based system. Hopefully, reducing the number of data breaches that occur as a direct result of weak password creation.

2 BACKGROUND AND RESEARCH QUESTIONS

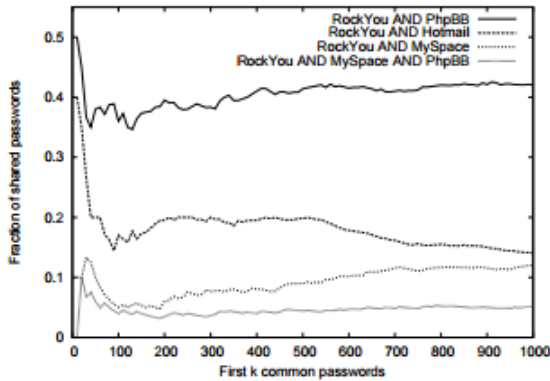
2.1 *Background and Literature Review*

Much research has been conducted regarding the vulnerabilities of online authentication methods. Trying to determine the cause of data breaches often points to weak passwords. Logically following those conclusions, studies have been conducted examining the password creation habits of users and why they are generally weak and easily attacked. In response to those studies many organizations began to implement password creation policies. These are regulations that require the inclusion of specific characters when creating a password for online authentication.

2.1.1 Insecure Passwords

Countless studies have been conducted regarding online authentications methods and their effectiveness in regards to protecting data. And time and time again, they have been proven vulnerable to attacks. This is due, in part, to lazy human habits. We create passwords that satisfy minimum requirements so that we can log into social media quickly, without thinking. This has resulted in a large number of online passwords being easily identifiable by potential attackers. For

example, the following charts depict the most common passwords used among many well-known websites:



(a) Fraction of passwords that are used in common by different sites

RockYou	Faithwriters	MySpace
<u>123456</u>	<u>123456</u>	password1
12345	writer	<u>abc123</u>
123456789	jesus1	fuckyou
<u>password</u>	christ	monkey1
iloveyou	blessed	iloveyou1
princess	john316	myspace1
1234567	jesuschrist	fuckyou1
rockyou	<u>password</u>	number1
12345678	heaven	football1
<u>abc123</u>	faithwriters	nicole1

(b) Ten most frequent passwords for different sites. Passwords underlined are shared by at least two services. The wide difference likely depend on background (e.g., Faithwriters) or password rules (e.g., MySpace).

Figure 1: Most Commonly Occurring Passwords for RockYou.com, Faithwriters.com, and Myspace.com

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

The most commonly used passwords in these revealed data sets are easily identifiable. “123456”, “password”, and “abc123” are among the most frequently used authentication credentials. Having such a large number of password be so weak and easily identifiable creates a security vulnerability that hackers are all too quick to exploit. These known passwords are among the most frequently attempted by hacking algorithms and brute force attacks. And unfortunately, because of their frequency of use, these attacks are often successful. Additionally, the eighth most common password for RockYou.com was simply “rockyou”. Using the name of the organization as the password for logging in to it is also incredibly insecure. These revealed passwords indicate a severe lack of consideration from users and create unnecessary security vulnerabilities.

These weak password traits are not limited to RockYou and MySpace. When examining frequently used passwords for other sites, the same commonalities can be observed:

Rank	hotmail	#users	flirtlife	#users	computerbits	#users	rockyou	#users
1	123456	48	123456	1432	password	20	123456	290729
2	123456789	15	ficken	407	computerbits	10	12345	79076
3	111111	10	12345	365	123456	7	123456789	76789
4	12345678	9	hallo	348	dublin	6	password	59462
5	tequiero	8	123456789	258	letmein	5	iloveyou	49952
6	000000	7	schatz	230	qwerty	4	princess	33291
7	alejandro	7	12345678	223	ireland	4	1234567	21725
8	sebastian	6	daniel	185	1234567	3	rockyou	20901
9	estrella	6	1234	175	liverpool	3	12345678	20553
10	1234567	6	askim	171	munster	3	abc123	16648

Table 1: Most Commonly Occurring Passwords Among Various Sites

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

As you can see from figure 3, the vast majority of passwords across a variety of online organizations contain only lowercase letters and digits. In fact, over 90 percent of all passwords used for authentication on these sites contain only lowercase letters and digits. This drastically reduces the number of guesses required by an attacker before they will be successful.

	RockYou.com*	FaithWriters.com	Singles.org	Neopets.com	Phpbb.com**
Number of Passwords	32,603,388 total	6,193	24,870	11,732	259,424
Average Password Length	7.88 characters	7.69 characters	6.62 characters	6.68 characters	7.27 characters
% that Contain Uppercase	5.95	9.43	8.51	2.53	7.21
% that Contain Digits	54.08	43.54	32.88	57.19	45.77
% that Contain Special Chars	3.45	0.14	0.20	1.78	1.33
% that Only Contain Lowercase Letters and Digits	90.76	90.50	91.31	95.61	91.55
% that are 7+ Chars Long, and Contain Uppercase, Lowercase, Digits + Special	0.14	0.03	0	0	0.11

*The RockYou password statistics are taken from the RockYou32 training list which contained 1 million randomly selected passwords

**The Phpbb statistics only include the 97% of passwords we managed to crack

Table 2: Password Traits

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

Despite talk of sophisticated cyber criminals compromising point of sale systems with deceptive malware, it is weak passwords and weak remote-access security that are to blame for almost all of the POS system breaches examined by security firm Trustwave. Overall, weak passwords and

weak remote-access security accounted for 56 percent of the 574 breaches examined by Trustwave’s SpiderLabs researchers in the 2015 Trustwave Global Security Report. And POS breaches made up 40 percent of the breaches examined in the report (Donovan, 2015).

2.1.2 Password Creation Policies

Initial analysis indicates that password creation policies are the solution. Directing users to create passwords based on specified criteria will ensure that their authentications meet minimum strength criteria. This, overall, will lead to more secure credentials. Many common password creation policies focus on a few, traditional criteria; limiting dictionary words, adding numerical values, including uppercase and lowercase letters, and adding special characters. As Weir, Aggarwal, Collins, and Stern have discovered, each of these password creation policies lend to security in their own right. The following charts depict the number of passwords cracked over the number of guesses attempted. Each chart represents a single password creation policy.

Limiting dictionary words:

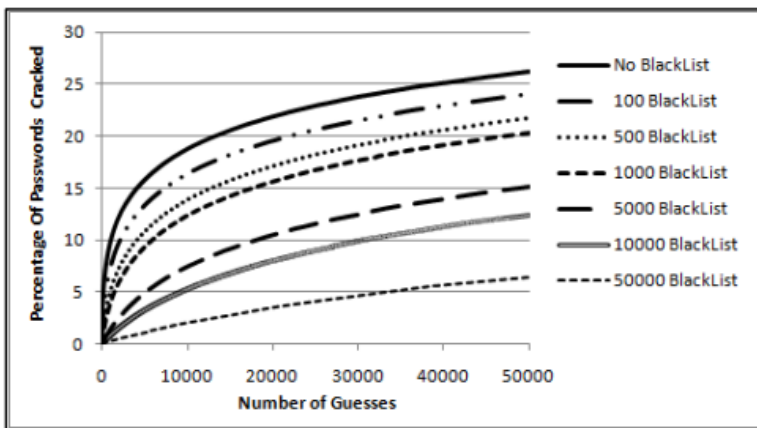


Figure 2: Effect of Limiting Dictionary Words

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

A blacklist is a list of dictionary words that is not permitted for use when creating a password. As you can see, without a blacklist, 15 percent of the passwords were cracked with less than 10,000 guesses. When you increase the number of guesses to 50,000, the ratio of passwords cracked is greater than one in four. However, as you begin to limit dictionary words from being used, the number of passwords cracked diminishes. The larger the blacklist, the fewer passwords cracked. With a blacklist of 50,000 words, after 10,000 guesses, less than three percent of the passwords had been cracked. After the maximum 50,000 guesses of the study, approximately six percent of passwords had been cracked. This is a drastic improvement of the passwords that were not influence by a blacklist of prohibited words.

Adding Special Characters:

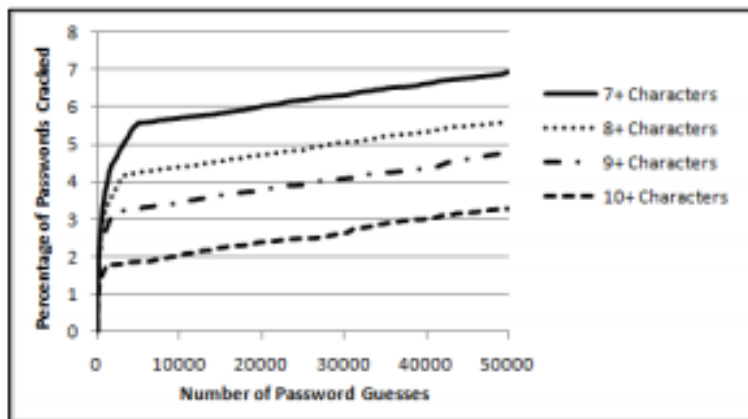


Figure 3: Effect of Adding Special Characters

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

Adding special characters to a password reduced the number of passwords cracked after 50,000 attempts to less than seven percent. This was the most effective reduction of attack success among all password creation policies. Additionally, that was the result when measuring passwords with a length of only seven characters, relatively short considering today's password creation policies.

When analyzing longer passwords, the results continued to improve. A password of 10 characters that contained a special character performed significantly better. Less than two percent of those passwords were cracked after 10,000 guesses. And, just over three percent after 50,000 attempts.

It should be noted that when special characters were required, even in the initial first thousand guesses the attack was much less successful then with the previous password creation rules, such as requiring a digit or capitalized character (Weir, Aggarwal, Collins, & Stern, 2010).

Requiring Uppercase Letters:

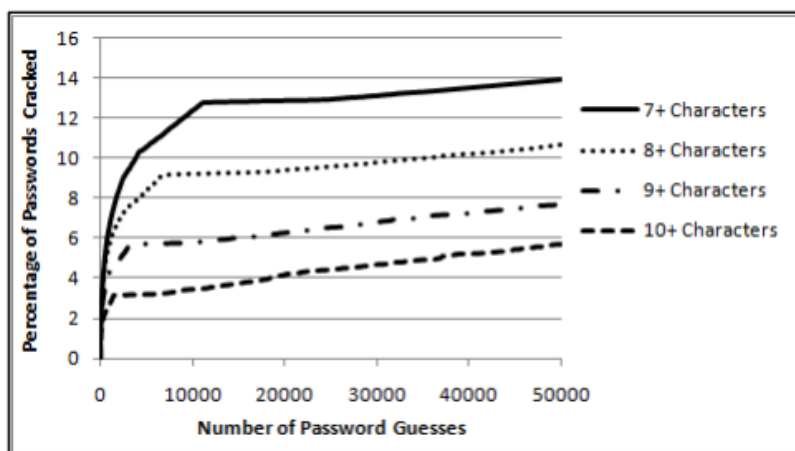


Figure 4: Effect of Adding Uppercase

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

What immediately sticks out is that the password cracking sessions start out much like the other attacks, but quickly hit a plateau where they become significantly less effective. Unfortunately this means that there still are a sizable number of users who pick weak passwords and would be compromised in an online cracking attack (Weir, Aggarwal, Collins, & Stern, 2010).

The passwords that contain an uppercase letter show similar results to other password creation policies. The initial 10,000 guesses cracked a significant number of the passwords. 12,000

passwords with a length of seven characters were cracked with only 10,000 attempts. Nearly four percent of those passwords with a length of 10 characters were cracked with the same number of guesses. However, unlike with other password creation policies, the number of passwords cracked as the number of guesses increased seemed to plateau. This proved to be true across passwords of all lengths, as well. The passwords with a length of seven characters that were cracked only increased from 12 percent at 10,000 attempts, to 14 percent at 50,000 attempts. Furthermore, the passwords with a length of 10 characters only increased by approximately two percent after the additional 40,000 guesses, as well.

Requiring a Minimum Length:

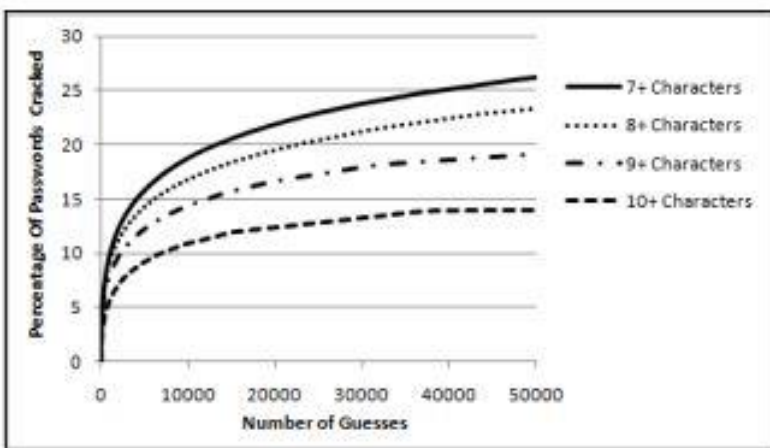


Figure 5: Effect of Increasing Password Length

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

The least effective password creation policy for increasing password strength is a minimum length requirement. The passwords tested here were created with the only requirement being a minimum character length. While many of them included other characters, those restrictions were not required. In the initial 10,000 guesses, nearly 20 percent of passwords required to have a minimum length of 7 characters were cracked. After the same number of attempts, only a little over 10

percent of the 10 character passwords had been cracked. As the number of guesses continues to grow, the shorter passwords get cracked at a higher rate than the longer passwords. An additional eight percent of the seven character passwords get cracked in the subsequent 40,000 attempts. Whereas, less than 15 percent of the 10 character passwords get cracked after 50,000 guesses.

However, even though password creation policies have been proven to increase security, they are often not implemented correctly, or at all. Most internet users get annoyed while signing up with a website that tells them their password must be eight characters long, must include both uppercase and lowercase, must contain at least one special character, and must have at least one numeric character. However, not every site provides a strong password setting mechanism, and this is why users are taking advantage of by relying on absolutely awful passwords. Even Google and Facebook allow users to set a weak password for their accounts, with just a minimum eight character condition, in order to target mass audience with better usability. Microsoft MVP of developer security Troy Hunt agrees to this by saying: “The problem is that website operators are faced with this paradox of security versus usability. If they enforced a minimum of 30 characters they’d be enormously secure...and have no customers. They’re forced to dumb down requirements in order to make the system appealing to the vast majority of people who don’t use password managers” (Khandelwal, 2016).

Furthermore, research has suggested that users’ behavior often attempts to satisfy password creation policies in the simplest way possible. When users are confronted with these additional regulations, their passwords do not become more secure. Instead, users will often just add the required characters to the end of their already insecure password. This can be seen in the MySpace column of *Figure 1*. Here, users simply added a single numerical digit to the end of their

passwords. Rather than incorporating digits throughout, as the password creation policy intended, the addition of a “1” satisfied the requirement without any additional user generated security.

Rank	Digit	Percentage	Rank	Digit	Percentage
#1	1	10.98%	#6	123456	1.74%
#2	2	2.79%	#7	12	1.49%
#3	123	2.29%	#8	7	1.20%
#4	4	2.10%	#9	13	1.07%
#5	3	2.02%	#10	5	1.04%

Table 3: Most Frequent Numerical Values

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

This chart indicates a severe bias to the numeral “1” in password inclusion. Users are far more likely to use 1 than any other number when a numeral is required in the password creation policy. While adding a digit makes a password harder to crack, when the bias to use the number 1 over any other digit is so heavy, attackers simply have to include that character in their guesses and algorithms.

Location	Example	Percentage
All Digits	1234567	20.51%
After	password123	64.28%
Before	123password	5.95%
Other	passw0rd, pass123word, pl1a2ssword, ...	9.24%

Table 4: Placement of Numerals

Note: Retrieved from (Weir, Aggarwal, Collins, & Stern, 2010)

Not only is the use of the number 1 more prevalent than any other number, the placement of numerical characters solely at the end of a password is far more common than incorporating those digits at the beginning, or throughout.

Obviously, password creation policies increase the strength of users' online authentication and reduce the ability of an attacker to compromise their data. Unfortunately, the research has shown that these same requirements for password creation are often not used, or simply circumvented by the user. This renders the additional security that can be achieved by these policies all but irrelevant.

2.1.3 Large Scale Data Breaches

While many of the password creation policies logically help to influence password strength in a positive manor, the reality is often not the case. The difficulty of a password to be cracked, or identified, is often not the only threat it may face. Once a user creates a password, that credential, or a version of it, is stored in a database by a third party for authentication. If an attacker is able to maliciously access a database of stored credentials, the hashing or encryption, of a password becomes irrelevant. "A common threat model is an attacker who steals a list of hashed passwords, enabling him to attempt to crack them offline at his leisure" (Kelley, et al., 2012). Many examples of attacks like these have been documented in recent years across a variety of industries and affecting many types of users.

Healthcare customers: Security experts warned in February that 2015 would be the year of the healthcare hack, and those forecasts have proven right. At the end of January, as many as 11 million Premera Blue Cross customers were affected by a hack. Anthem announced the following month that almost 80 million current and former customers' personal information had been breached. In May, CareFirst BlueCross BlueShield, serving Maryland, Washington and Virginia,

announced 1.1 million of its customers' personal information had been compromised. UCLA Health System announced a data breach in July affecting 4.5 million people. In September, Excellus BlueCross BlueShield, based in upstate New York, said as many as 10 million people's personal records had been exposed.

Ashley Madison users: Hackers stole and, in August, posted online the information for around 32 million users of the dating site, which is designed for married people looking for affairs.

Government employees: The hack, announced in June, impacted 21.5 million people who had a government background check, including government employees and some of their family members. More than 5 million fingerprints were also exposed—a security risk for spies abroad. The hack was so extensive that the United States reportedly pulled spies from China on Tuesday, since their identities may have been discovered.

Sony employees: Huge troves of company data were stolen and posted online, including sensitive executive emails, employees' personal information, and copies of upcoming films. The hack led to the resignation of Amy Pascal, Sony's co-chairman.

Home Depot shoppers: Last September, Home Depot announced it had been hacked, and 56 million payment cards were compromised, as well as 53 million email addresses.

JP Morgan customers: The information for 83 million customers and small businesses was compromised in a hack revealed in August 2014.

EBay users: In a hack reported in May of 2014, personal information for more than 145 million active users—including login credentials and physical addresses—was compromised.

Target shoppers: In December 2013, 110 million customers' personal and financial information was exposed. (Grodén, 2015)

2.1.4 Research Gaps and Questions

While significant research has been conducted about the security of current online authentication methods, very little has been done regarding alternative methods. The accepted form of password for online authentication is a combination of ASCII characters. That is to say, characters that are found on a standard, QWERTY keyboard. The combinations of passwords using ASCII characters is endless, and has the ability to provide incredible security. However, as previous research has shown, the real-world effectiveness of this authentication methods leaves much to be desired regarding security. Is there another way organizations could authenticate their online users? This paper attempts to address the possibility of using an image-based password system of authentication. However, in order to address whether or not such a system would be feasible, multiple questions must be answered. First and foremost, are images more easily remembered than words. If they are not, using images for passwords would clearly not be a solution. However, when addressing this particular question, multiple others arise. How do you compare a universally accepted keyboard with an array of images? Does muscle memory play a part in the selection of characters during password creation? Does the use of images influence users to create longer or shorter passwords? These are the questions we seek to answer with this experiment.

Before moving forward with experiment design, we needed to understand the picture superiority effect. Multiple studies have shown that the human brain can more easily recall an image than a word. The picture superiority effect is a well-documented phenomenon that is defined as the superior memory of pictorial stimuli compared to word stimuli. Psychologists have expansively studied the differences between the encoding and processing of words and pictures. The

predominant explanation for this effect is that pictures are encoded more effectively than words, and are therefore able to be better remembered. Research has demonstrated the benefit that pictures provide for remembering words (Hazamy, 2009).

To preface the following results, we must acknowledge the two bases of recognition memory that are widely accepted – perceptual and conceptual, or remember and know. The basic paradigm for exploring the role of conscious recollection in memory involves requiring people to make judgments regarding the nature of their memories for recalled or recognized items (e.g., Gardiner, 1988; Tulving, 1985), instead of assuming the involvement of conscious recollection on the basis of successful memory performance. One type of experience, which subjects judge as "remember," refers to those items for which they have a vivid memory, a subjective feeling of having seen the item during the study episode, and a conscious recollection of it occurring on the study list. The other type of experience, which subjects judge as "know," refers to items for which they can tell (usually with certainty) were on the study list, but cannot recollect the actual occurrence. It is assumed that this judgment is made on some other basis because the subject does not remember actually seeing the item on the study list, and does not have a conscious recollection of it (Rajaram, 1993).

Study Manipulation	Targets		Lures (False Alarms)
	Pictures	Words	
Overall Recognition	0.90	0.69	0.09
"Remember"	0.81	0.51	0.01
"Know"	0.09	0.18	0.08

Table 5: Successful Memory Recalls

Note: Retrieved from (Rajaram, 1993).

The overall recognition of a target memory is 21 percent higher for a picture than a word. This is a nearly 31 percent increase in recognition of an image over a word. Furthermore, when judging by the “remember” portion of a memory, the difference is even more drastic, 30 percent.

These results clearly indicate that humans tend to remember pictures more easily than words. And not just by a small margin. We overwhelmingly recognize images presented to us before their written counterparts.

3 EXPERIMENT METHODOLOGY

3.1 Introduction / Approach

Now, it is clear that traditional online authentication methods are severely flawed. In addition to that, attempts to correct the insecure nature of human password creation has provided lackluster results. In an attempt to increase online data security, we have proposed a new method of online user authentication. While our proposed system of authentication will incorporate two tiers, that particular subject is not discussed in this paper. Instead, the focus is on the replacement of traditional passwords, created with ASCII characters from a standard keyboard, with on created

with images. The most identifiable reason for creating a weak password is usability. Can a user remember a password that satisfies the creation policies requiring a minimum of 15 characters, the use of both uppercase and lowercase letters, at least one numerical character, and at least one special character? Not without using an easily identifiable password with the numerical and special characters left as an afterthought on the end of the password. Research has shown that images are more easily stored into memory and recalled than written words. Therefore, a password created with pictures instead of letters would be easier to remember. Furthermore, when the uncertainty of being able to recall a password decreases, average password length increases. And as we have seen in general, the longer the password, the more secure. And so it follows, an image-based password will be more secure than its ASCII-based counterpart.

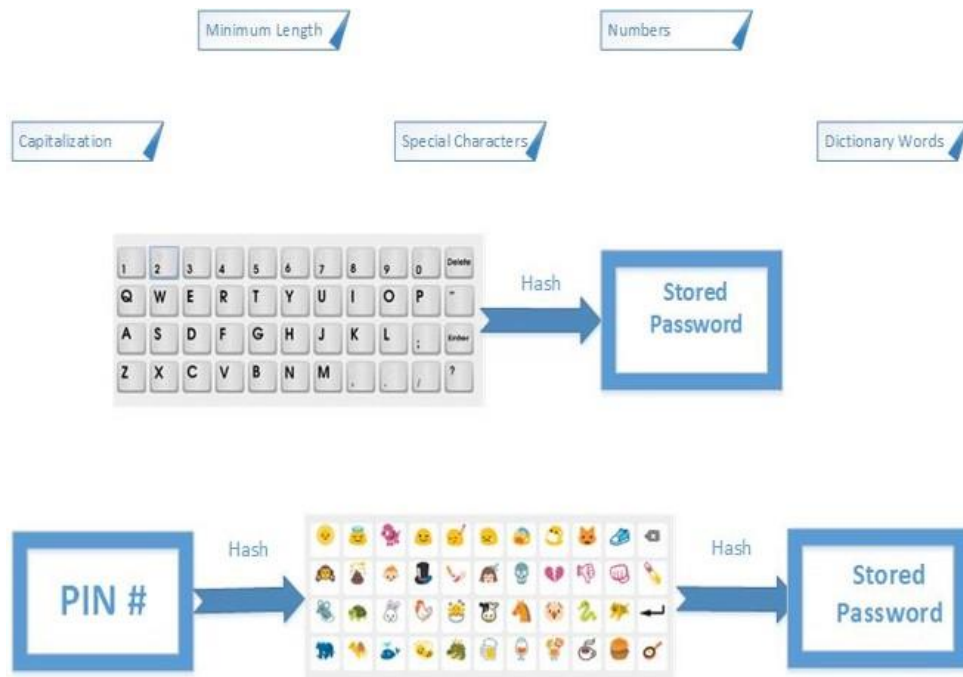


Figure 6: Authentication Flow

That being said, we have designed an experiment to test each of the conditions that we have identified.

3.2 Experiment Methodolgy

3.2.1 Questions to be Answered

1. Are image-based passwords easier to remember than ASCII-based passwords?
2. Does muscle memory play a part in password creation?
3. Does the randomization of characters effect memorability?
4. How do the image-based and ASCII-based results compare over time?
5. How do the QWERTY versus random results compare over time?

3.2.2 A 2x2 Approach

One of the key questions that has arisen is regarding the muscle memory of users to their keyboards. Typing classes are very familiar to elementary school classrooms. As such, we are trained to manipulate our keyboards in a specific way. Additionally, many people use identical, or at least similar, passwords for a variety of websites. These factors have conditioned our brains to consider, and over-utilize, pre-defined passwords. We have taken this bias into account and developed an additional experimental condition in response. This required a 2x2 experiment methodology. In other words, there would be four total conditions tested.

Condition 1: A traditional ASCII keyboard.

Condition 2: A randomized ASCII keyboard.

Condition 3: An image-based keyboard.

Condition 4: A randomized image-based keyboard.


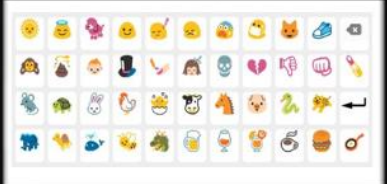

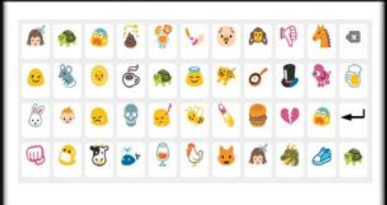
		Keyboard Type	
		ASCII	Emoji
Randomization	Standard		
	Random		

Figure 7: 2x2 Methodology

3.2.3 Conducting the Study

In order to gather data, we needed to have users create passwords without knowing that their password was the focus of our research. We created a Qualtrics based survey that included our four password interfaces. The link for the survey was distributed to undergraduate students at the University of Arizona’s Eller College of Management. Students were offered a marginal bit of extra credit for their participation. Once a student chose to participate, they were randomly directed to one of the four password interfaces. They were then instructed to input their University of Arizona email address as a username and to create a password in order to begin the study. They were encouraged to create a password that was unique and not anything similar to any password they have used for authentication anywhere else. After participants had submitted their username and created a password, they were redirected to a survey containing a series of questions. The questions included their opinion of the password interface they had just used, a brief walkthrough of an experimental anti-virus software, and questions about their concerns with internet privacy. Once participants had completed the survey questions, they were asked to enter their username,

their University of Arizona email address, one final time. This email addressed was used to retrieve the interface that they were presented with in the first step, and presented that interface again. We then asked them to re-enter the password they created at the beginning of the study. Their responses were recorded and this portion of the experiment was complete. One week following their completion of the online password creation study, a follow-up email was sent to each user. The email contained instructions to “sign in” to their study account one final time in order to receive compensation. Their interface was generated in the same manner as it was during the second password entry phase. This third password entry was also recorded.

3.3 Results

3.3.1 Initial Password Recollection

The results we gathered seem to contradict what we expected. With the research on password creation and the picture superiority effect, the natural conclusion to draw would be that an image-based password would be much easier to remember. And therefore, easier to use and more secure. However, the results paint a different picture.

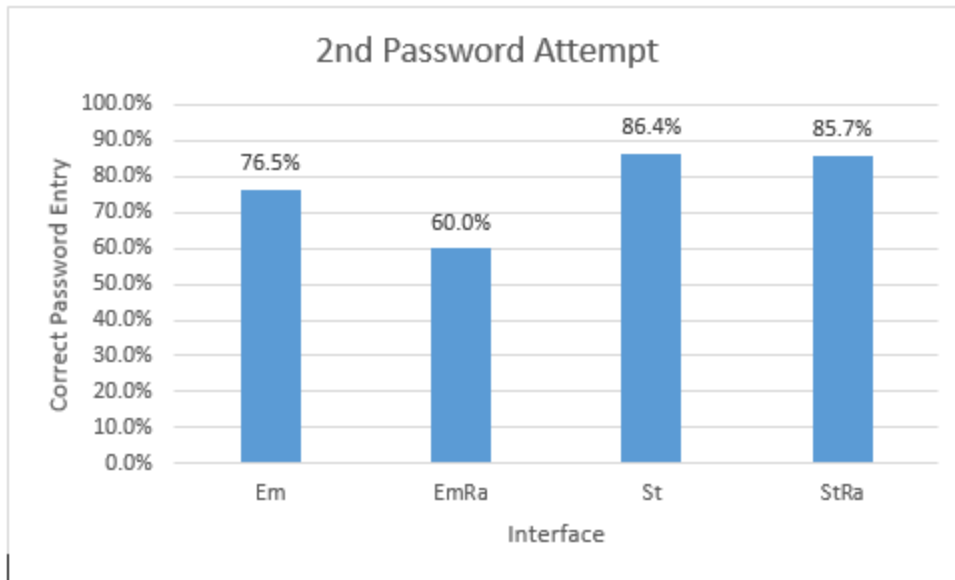


Figure 8: 2nd Password Attempt

The chart clearly shows that users of both the standard and the standardRandom keyboard recalled their original passwords with greater success than the users of the emoji and the emojiRandom keyboards. This “2nd Password Attempt” was recorded when a user re-entered their password at the end of the original survey

3.3.2 Long-Term Password Recollection

After the initial survey, participants believed that the experiment had ended. This was done by design. Exactly one week following their initial response, participants were contacted again, via email. They were informed that compensation was available if they were willing to input their username and password one final time. They were also informed that the amount of compensation they were entitled to was dependent on their response. In other words, they would be paid more if they could correctly recall the password they originally created for the study. These results, while encouraging, are still inconclusive.

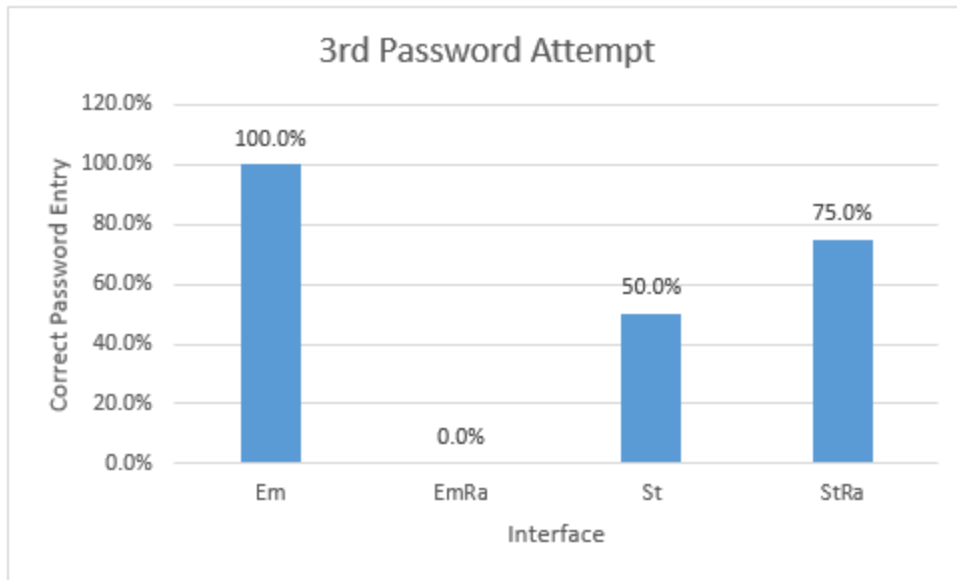


Figure 9: 3rd Password Attempt

At first glance, the users with the Em (emoji) keyboard had a significantly higher recollection rate than that of the QWERTY counterparts. However, this data is incomplete. At the time of this paper's completion, only nine participants had completed the follow-up portion of the study. With such a small sample size, no viable conclusions can be drawn.

3.3.3 The Effect of Time

Given that the 3rd Password Attempt data is incomplete; comparison of password entries over time is equally lacking. However, even though there is not significant enough contribution to draw conclusions, we can attempt to visualize how the passage of time effected the users' ability to remember their authentication credentials.

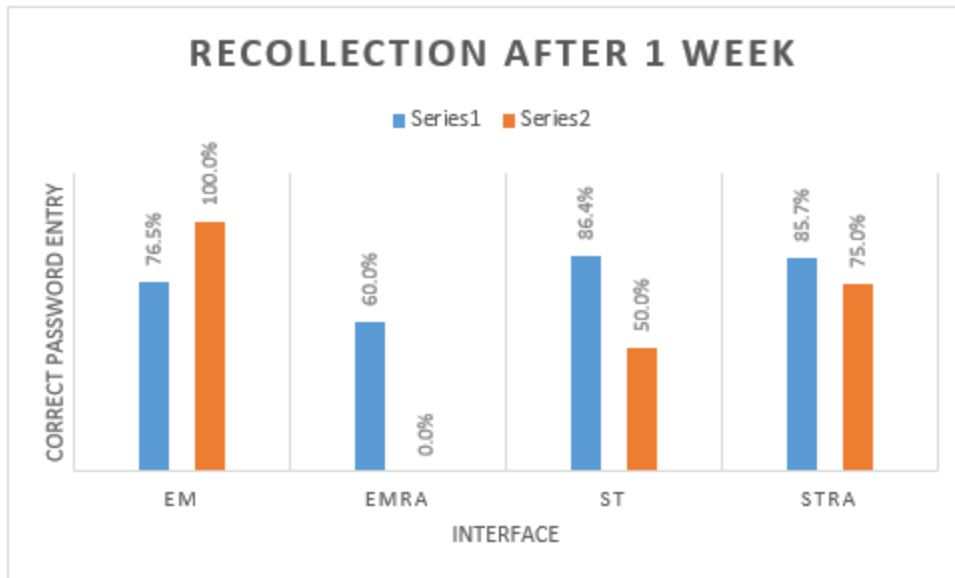


Figure 10: *Recollection After One Week*

Disregarding the EmRa (Emoji Random) results, as there were 0 participants with this interface that responded to the follow-up, it seems as though the image-based password was easier to recall than its ASCII-based counterpart. Again, these results can not be considered definitive due to the small sample size. However, with additional research and an expanded pool of participants, I am confident that the initial observations here will be confirmed.

4 REFERENCES

- Babb, J., Keith, M., & Steinbart, P. (2016). Can Relaxing Security Policy Restrictiveness Improve User Behavior? A Field Study of Authentication Credential Usage. Hawaii International Conference on System Sciences.
- Castellucia, C., Durmuth, M., & Perito, D. (2012). Adaptive Password-Strength Meters from Markov Models. *InternetSociety.org*.
- Donovan, F. (2015, June 11). Most POS System Breaches Due to Weak Passwords or Weak Remote-Access Security, says Trustwave. *ierceitsecurity.com*.
- Florencio, D., & Herley, C. (2007). *A Large-Scale Study of Web Password Habits*. Microsoft Research.
- Foos, P. W., & Goolkasian, P. (2005). *Presentation Format Effect in Working Memory: The Role of Attention*. Psychonomic Society.
- Gayomali, C. (2014, February 24). *Why do Companies Keep Getting Hacked*. Retrieved from fastcompany.com.
- Grajales, C. A. (2016). How Hacker are Making Use of Statistics to Steal Your Password. *Statistics View*.
- Groden, C. (2015, October 2). *Here's Who's Been Hacked in the Past Two Years*. Retrieved from fortune.com.
- Hazamy, A. A. (2009). *Influence of Pictures on Word Recognition*. Georgia Southern University.

- Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., . . . Lopez, J. (2012). Guess Again (and again and again): Measuring Password Strength by Simulating Password-Cracking Algorithms. IEEE.
- Khandelwal, S. (2016, January 26). *Password Security - Who's to Blame for Weak Passwords? Users, Really?* Retrieved from thehackernews.com.
- Malone, D., & Maher, K. (2012). Investigating the Distribution of Password Choices. *International World Wide Web Conference Committee*.
- Mersad. (2013). Adobe's Hackers Release Top 100 Most Common Passwords. *Online Computers and Communications*.
- Moore, S. (2015, September 23). Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach \$75.4 Billion in 2015. *Gartner.com*.
- Munger, D. (2006, October 25). *Actually, a Picture is Worth 1.5 Words*. Retrieved from scienceblogs.com.
- Ophoff, J., & Janowski, M. (2015). Examining Gamification as a Driver of Individual Information Security Behavior. *International Federation for Information Processing*.
- Rajaram, S. (1993). *Remembering and Knowing: Two Mean of Access to the Personal Past*. Temple University School of Medicine.
- Trustwave. (2015). *Trustwave Global Security Report*. Trustwave.
- Veras, R., Collins, C., & Thorpe, J. (2014). *On the Semantic Patterns of Passwords and their Security Impact*.

Veras, R., Thorpe, J., & Collins, C. (2012). Visualizing Semantics in Passwords: The Role of Dates.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). *Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords*.

Whittaker, Z. (2016, January 13). These Companies Lost Your Data in 2015's Biggest Hacks. *zdnet.com*.