Computer and Information Security

Fitzroy Nembhard and Samir Mammadov

December 1, 2015

Password Authentication: Weaknesses, Strengths and Alternatives

1 ABSTRACT

Discussion about password security has been going on for a long time. It was noted in early Unix systems that users had bad habits of choosing weak and easily guessed passwords. Recent studies of web password selections show that users still choose very weak passwords when restrictions on password selections are not too stringent. Some users still ignore frequent warnings about account fraud and select weak passwords.

We reviewed several papers about the security of text-based passwords, password weaknesses and alternatives to passwords as a means of authentication. In this paper, we discuss and analyze our findings. We also compare some alternative techniques to text-based password authentication and provide a critique of the solutions we believe are more viable. The overarching message from our discussion is that within the next few years of this writing, no one solution will put an end to text-based password authentication. It may take a catastrophe or government regulation to cause companies to make a complete move away from password authentication. Alternatives such as two-factor authentication will continue to to be adopted gradually.

2 INTRODUCTION

Some researchers argue that if we are so smart, why are we still using passwords? Others suggest that we should not do away with passwords altogether but employ specialized hashing and encryption techniques when using passwords to authenticate users. A more modern approach is to introduce alternatives such as smart-cards, biometrics and two-factor or three-factor authentication. Some attacks on password authentication schemes include: replay attack, off-line guessing, stolen-verifier, denial of service, man-in-the-middle attacks, phishing, and social engineering. Due to the widespread use of text-based passwords (used hereinafter as simply ”passwords”), their security should be discussed and analyzed rigorously. This work attempts to provoke thought on the subject by focusing on both password strengths and weaknesses and also discussing some alternatives.

The paper is organized as follows: first, we review fifteen (15) research papers below that focus on challenges with passwords, password strength, improvement of password security, the use of

passwords in insecure communication, comparison of password techniques, and alternatives to text-based password authentication. In Section 4, we compare the techniques proposed in the selection of papers. Section 5 presents a discussion of the techniques and ideas proposed by the authors, and we conclude the paper in Section 6.

3 REVIEW

3.1 Choosing Passwords: Security and Human Factors

In his paper, *Choosing Passwords: Security and Human Factors*, Gehringer described some concerns about passwords from a human perspective. He postulated that human weaknesses make it nearly impossible to follow simultaneously the rules that govern password selection[5]. Some practices that were believed to be effective in the 1990s, such as the use of a catch-phrase acronym, (e.g. initials of a line from a song) do not work on all systems. Moreover, popular lyrics may be added to a cracker's dictionary and even though it is recommended that users include special characters in their passwords, they sometimes choose very obvious ones such as replacing an 's' with a '$', which are also included in password dictionaries. The author also criticized the challenges of using lifetime limits, lockouts and Wallets[1] as not very effective or usable. He suggested an alternative technique (to lifetime limits and lockouts) to foil password-guessing, which is introducing a delay of a few seconds between password attempts and suggested that this could be combined with lockouts, but with high threshold (e.g. giving the user 12 attempts instead of 3).

We agree with the author that Password Managers such as Q*Wallet, PasswordWallet, and Microsoft Passport do not provide optimal security because in most of these applications, a single password is used to protect a database of multiple passwords, and cracking one password makes it easier to get access to all passwords. Additionally, eavesdropping between client and merchant could reveal clues about the server, which risks impersonation attacks.

Further, as shown in Table 3.1, rules that work in one era have to be modified to support technological capabilities in another era. It can be seen in the table that users were cautioned against the use of words in a dictionary as passwords in 2001, but not cautioned in the 1990s due to the infrequency of dictionary attacks in the 1990s and the change in crackers' capabilities in the 2000s. With these rule changes especially across different platforms, it puts a burden on users and sometimes causes them to ignore the rules where possible, which makes systems more prone to attacks.

We do not agree with the author that a combination of high-threshold lockout and delay between password attempts will make systems that use password authentication more secure. While this may deter users from writing down passwords due to to the privilege of being allowed a high number of attempts, this could provide attackers with more time to carry out brute-force attacks.

[1] Now known as a Password Manager, which is a software application that helps a user store and organize passwords.

Suggestions 1991	**Suggestions 2001**
Has both upper and lower case letters	Not contain words found in a dictionary. (multilingual online dictionaries more than 100,000 words)
Has digits and/or punctuations & letters	Not be a name of a friend, relative, film star or person in a book.
Easy to remember, not written down	Not be a number
7/8 characters	$\geq$ 8 characters
Can be typed quickly (decrease shoulder-surfing)	Not contain a space.

Table 3.1: Comparison of password rules in 1991 with 2001 [5].

3.2 Password Entropy and Password Quality

The goal of Ma et al.'s paper, entitled *Password Entropy and Password Quality*, is to review studies that propose entropy as a measurement of password strength, point out the inapplicability of this proposal, and to advocate a different way of measuring password quality, known as a password quality indicator (PQI). Though password entropy, by definition, is a measure of the unpredictability of a password based on a certain character set, Ma et al. showed that entropy is conducted on a model of n-order Markov process, which is an extension of Shannon's entropy formula and is, therefore, fundamentally inapplicable when one attempts to use is as a measure of password quality. The authors' premise is that there is no statistic distribution for passwords, password guessing is not a Markov process because knowing few characters cannot help in knowing the rest, and guessing entropy only provides a lower boundary for cracking a password.

The solution proposed by the authors is based on Levenshtein's editing distance formula and is as follows:

$$\lambda = (D, L)$$

where D is Levenshtein's editing distance between the chosen password and the words in a password dictionary and L is the length of the password. Ma et al.'s scheme for a strong password requires that the password be at least eight characters long, contains at least three special characters and other alphanumeric characters.

Since passwords are not based solely on words in a language, where one character may depend on the previous character (as in a Markov process), we agree with the authors that entropy cannot provide a measure of password quality. Password quality can be measured by the difference between a password and dictionary words, the length of the password, and the magnitude of the password character set [13]. Based on this understanding, it can be seen that Levenshtein's editing distance, which provides a measure of similarity between two strings, is a better approach to measure the quality or strength of a password than Shannon entropy formula that is better used to measure information gain.

3.3 Password-Based Authentication: A System Perspective

In this paper, Conklin, Dietrich, and Walz examined security and password security techniques and practices. The paper started off by summarizing the beginnings of computing and origins of the password security paradigm. In former times, there were only a single mainframe computer and perhaps one or two accounts that were protected by passwords. However, nowadays with the advent of cheap and affordable home computing as well as the evolution of computer networking and the Internet, users can have at least half a dozen passwords to remember to be able to conveniently access things on line. With so many new applications and services being moved to and created on line, people need to keep track of all of their account information. Thus, the authors stated that not only is this a huge usability issue but also a huge potential security risk. They claimed that the current security model is very vulnerable to the three typical password attacks, which are brute force, discovery and social engineering.

For a solution, Conklin, Dietrich, and Walz proposed that designers start thinking about security differently before starting to design computing systems. The authors made an appeal to modern day developers to consider a more user-centric approach to scientific problems and perhaps change the way they design their systems. A very good argument brought up by the authors is the fact that most older systems have a a reductionist view of their systems and thus often carry problems such as this one. If more developers had an emergent approach to their system design (where the security is thought of before hand and built along the system instead of being tacked on at the end) then we would have a much more secure platform for personal computing.

We agree with the arguments raised in this paper, but are not sure whether the implementation and lack of any specific proposed solution actually help. Raising awareness about certain issues is certainly very important, but proposing a viable and feasible solution is just as, if not more important. Keeping the users and general user experience in mind is of course very important and should always be at the forefront of every design decision. There are of course differing requirements for usability and security for different applications, but password security refers to our everyday use of everyday products and services that we have all become familiar with today.

3.4 Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment

Vance et al. examined the influence of interactive password strength meter, static fear appeal, interactive fear appeal, and their effectiveness in motivating users to increase the strength of their passwords in their paper entitled *Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment*. By way of a controlled field experiment, the authors employed the services of 354 users from 65 countries to register on Socwall.com via their new registration system. Their claim is that results show that interactive fear appeals motivate users to increase password strength whereas interactive password strength meter and static fear appeal do not motivate users to increase the strength of the passwords they select.

While we agree that the paper provides significant depth to support the authors' use of Fear Ap-

peal Theory especially since it was used in other studies to motivate users to install anti-spyware, we do not agree that instilling fear in a user is the way to achieve an acceptable level of security in password authentication. A user could become annoyed if upon entering a password, a dynamic warning constantly appears that the selected password makes the account prone to attacks. If this is the case, the organization will need to employ better techniques to protect users' accounts. Additionally, due to the fact that a controlled field experiment was done and users were paid for their time, it could be concluded that users only selected strong passwords in order to please the researchers, and this is in no way a representation of their behavior in everyday life.

3.5 Do Strong Web Passwords Accomplish Anything?

In this paper, Florêncio, Herley, and Coskun argued that strong passwords provide very little benefit and weak passwords can withstand up to ten years of sustained brute-force attack on an account. This is due to the fact that the main threats to a user's password are phishing and keylogging. Best practices, such as choosing strong passwords, changing passwords frequently, and not writing down passwords, do not offer any real protection against phishing or keylogging. Comparatively, there is not much difference in the theft of strong and weak passwords by phishers or keyloggers, and changing passwords frequently helps only if the attacker is extremely slow in exploiting stolen credentials.

Other prevalent attacks that may be attempted on accounts protected by passwords include brute-force attack, bulk guessing attack, and access attack (e.g. shoulder surfing and console access). Employing a "three strikes" type lockout rule when using a weak password can help a system withstand a brute-force attack on the user's account. Shoulder surfing does not appear to be common because humans are good at taking note of people in their personal space. Additionally, password strength does not play a role when an attacker gains access to a console application on a machine where password auto-fill is enabled or a password manager is being used.

We agree with the authors that the best practices enumerated by experts do not offer any strong protection against the most well-known attacks. We take such stance due to the fact that it is a burden for users to adhere to practices such as changing passwords frequently and the authors demonstrated mathematically that strong userIDs could achieve stronger authentication than passwords.

3.6 Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol

In their paper, entitled *Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol*, Jeong, Won, and Kim made reference to a number of authors who attempted to design a secure hash-based password authentication scheme and the weaknesses that other researchers found in the proposed schemes plus suggested improvements. They made reference to Sandirigama's Simple and Secure (SAS) password protocol that was proposed in 2000, but was found to be vulnerable to replay and denial of service attacks by Lin et al, who then proposed Opti-

mal Strong Password Authentication (OSPA). This chain of proposals and improvement continued through to 2009, when Kim-Koç proposed a fix to Yoon, Ryun, and Yoo (YRY) password scheme.

Jeong, Won, and Kim demonstrated that Kim-Koç's fix is vulnerable to impersonation attack, guessing attack, and stolen-verifier attack [9]. In their paper, they proposed a fix to Kim-Koç's protocol. Due to the comprehensive nature of the fix—from registration to password-reset—we will only show the fix they propose for the registration step, which we have shown in Figure 3.1. We agree based on the added RSA optimal asymmetric encryption padding that the authors' proposal is a secure fix to Kim-Koç's protocol. It can be seen from the image that adding encryption to hashing and the XOR cypher provides a more secure level of encryption.

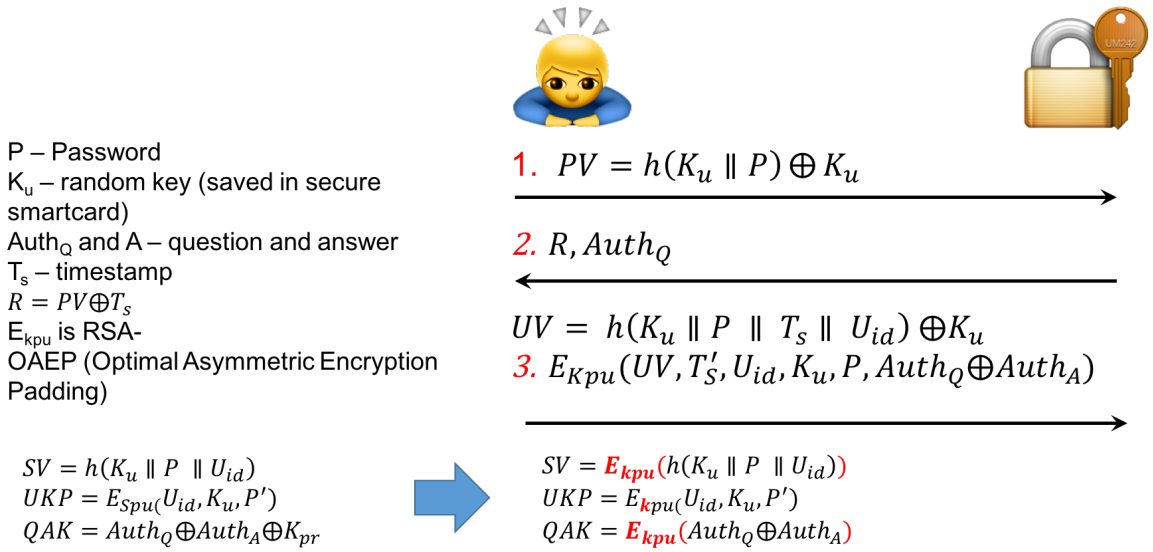

Figure 3.1: Jeong, Won, and Kim proposed fix to Kim-Koç's registration protocol.

3.7 Password Authentication with Insecure Communication

This is one of the first, most important and most fundamental papers related to remote password-based security. Lamport presented the issue of securely communicating between client and server especially over an insecure communication medium. The author outlined three key issues and vulnerabilities associated with this problem: gaining access to information stored inside of the system, intercepting user's communication with system and user's inadvertent disclosure of the password. She concentrated on the first two issues and stated that the last one cannot be as easily fixed. To thwart these issues, people have tried using a one-way function (such as hashing), but this has the disadvantage of storing the password hashes. Another solution they relied on was storing sequences of passwords instead, but this had similar issues of storing a giant password table. So for the solution, Lamport proposed a new way of password hashing and chaining known today simply as hash chaining.

Given this solution and the date of the publication, we agree with it and comprehend its limitations. Hash chaining is an incredibly useful technique for remote password based authentication, especially in situations where the communication medium is insecure. This is an important distinction since if we look at our computing world today, a lot of networks are insecure and the data could be easily collected by anyone on the network. This is an excellent solution and a wonderful basis for the rest of basic password computer security.

3.8 A Comparison of Password Techniques for Multilevel Authentication Mechanisms

Zviran and Haga examined several different password authentication techniques based on primarily objective memorability and subjective user preference. The authors began by outlying all the known issues with password-based security and how they relate to human cognitive abilities and thus their usability factor. To empirically find out which of these techniques were easier to remember, use and were most preferred by the users, they conducted a research survey with a questionnaire and follow up questionnaire 3 months later. The factors mentioned and at least partially examined were memorability, convenience, amount of time it takes to authenticate, ease of use, user preference, security, familiarity and error proneness. The five different password techniques examined in the paper are self generated passwords, system generated passwords, associative passwords, cognitive passwords and pass phrases. To test the memorability of each of these techniques the authors simply had the users remember all of these password types in the first questionnaire and have them recite it in the second survey three months later.

The results of the study are very interesting and show once again how most people do not like the current password security scheme and how impractical and insecure it can be. Of the 101 participants in the study only 27% were able to recall their original password that they themselves chose. The study also found that of the system generated passwords, their length didn't matter much when it came to memorability and only the ones that resembled real words or were easily pronounceable were good. For the pass phrase technique only 21% were able to recall the entire phrase which was on average 23 characters long. Overall, the two best password techniques were self generated passwords and associative passwords. The self generated passwords were obviously the most familiar to the users and rated as number for subjective ease of use for probably this reason, and number one for memorability which surprised us. However associative passwords were the best all rounder as they were number two for both memorability and ease of use and this is considering the fact that none of these users used this type of password before. Out of these two techniques we prefer the associative passwords since we feel like they offer better usability for actually better security. The issues with traditional passwords still stand and using this technique could possibly alleviate a lot of these issues.

3.9 Improved Visual Preference Authentication

In their paper entitled *Improved Visual Preference Authentication*, Jakobsson and Siadati proposed a password reset scheme that is based on a three-class classification system and can be used to authenticate users. The proposed scheme allows users to choose two sets of images—one set they like and one set that they dislike—from a displayed gallery of images during online registration and authentication. The images that do not fall into any of the two classes are then placed in a third no-opinion class, and all three classes of images are used by the authentication system to help users reset their passwords when needed.

The authors discussed the weaknesses of using security questions as part of a password reset scheme, the challenge of using a two-class preference-based reset scheme, and other features of authentication systems that rely heavily on memorability. Based on the comparison they provided, which we have summarized in Table 3.2, we agree with the authors' results that such a system would be ideal for inclusion in online registration systems. It can be seen that their password reset scheme that uses a tertiary classification system outperforms the existing two class visual preference authentication systems in all selected measures.

Two-Class Visual Preference	**Three-Class Visual Preference**
Classes: likes and dislikes	Classes: likes, dislikes, no-opinion
Registration: 170 seconds Authentication: 60 seconds	Registration: 100 seconds Authentication: 40 seconds
To attain FPR[2] of 1% and FNR[3] of 2.5%, it takes 12 likes and 12 dislikes to authenticate users	For an FPR of 0.5% and FNR of 0.9%, it takes 3 likes and 3 dislikes to authenticate users

Table 3.2: Comparison of two and three class visual preference authentication schemes [8].

3.10 New Remote User Authentication Scheme Using Smart Cards

This paper examined the current industry for password security and smart cards and the authors came up with their own method to thwart certain attacks while maintaining usability and availability. Kumar based his smart card scheme on the El-Gamal public key encryption protocol made in 1985, which in turn was based on the Diffie-Hellman protocol. This method relied on the computational complexity of discrete logarithms to exchange a pair of keys for easy, convenient and secure communication. The authors decided to combine the smart-card device infrastructure with El-Gamal's cryptosystem for a "best of both worlds" solution. The first step is associating a certain user account with a smart-card and input device. During the login phase, the user would input his ID and password while the smart-card performs the following operations: It would first generate a random number, which it would use as part of the calculation as specified in the protocol. After all the necessary parameters have been computed, a message can be encoded and sent off for authentication to the remote system.

[2]False Positive Rate
[3]False Negative Rate

Kumar proposed a very interesting scheme for authentication, but one we do not entirely support. We do not think that smart cards are the future of password based security if authentication security at all. Not only that, but this scheme has many problems with it and is prone to a number of different attacks including but not limited to masquerading attacks, impersonation and quantum computing. As is made evident by Jiang et al. in their paper, this is an interesting scheme but is not entirely secure against man-in-the-middle type attacks. And since the El-Gamal cryptosystem relies on the computational complexity of discrete logarithms, it vulnerable to attacks that could be carried out on quantum computers. Albeit, this is not a present and significant threat. It will become one in the future and there is no point in relying on a temporary broken system.

3.11 Improvement of Robust Smart-card-based Password Authentication Scheme

Jiang et al. looked at Kumar's paper and analyzed it for its weaknesses and attempted to fix them while still maintaining the efficiency and convenience of the original system. The main vulnerability the authors found and tried to fix was the offline password guessing attack. Their methodology included observing the power draw of the smart card to analyse the collected data and figure out the secure key and ID information stored on the smart card. To fix this they proposed that only a minor change in the login and authentication phases that changed the way the authentication token was getting passed and used. In the original model the scheme was vulnerable to an offline guessing attack if the adversary was able to eavesdrop on the communication and retrieve the necessary authentication parameters from the smart card. With this old scheme the adversary was able to check the validity of each candidate password by computing the key with a different set of parameters each time.

The new and improved method proposed by Jiang et al. replaces the validation step parameters to use a new parameter alpha instead of the actual user credentials. This new alpha parameter is based on the computational Diffie-Hellman problem which is similar to the original El-Gamal scheme. The authors also claim that there are no significant differences in computational time or resources as they were able to measure and compare both the old and new systems. Once again we do not think that smart cards are the future of authentication and are weary of the new fix to the old problems since it is still just as vulnerable to ubiquitous quantum computing as the original protocol is. There is no point on relying on an old and out of date cryptosystem especially since it has gone through so many revisions and people are still able to find issues with it.

3.12 Password authentication using Keystroke Biometrics

The authors of Password authentication using Keystroke Biometrics started off with the old premise that traditional passwords are bad and should not be used as the sole source of security in a secure system. D'Lima and Mittal proposed to use the natural typing pattern of the user as an additional layer of security on top of the old password authentication scheme. They stated that biometrics are more robust than unique keys and physical security of which there are three modalities: biological

such as DNA, behavioural such as keystroke dynamics and morphological such as a fingerprint or retina scan. However the biggest issue with most current biometrics is the fact they usually have a high set up cost and can be considered as more intrusive than a traditional password. Their methodology for this study was using a multitude of sensors to measure the keystrokes, typing speed, use of the tab key, mouse movement and keystroke pressure. On top of this the authors propose using an artificial neural network (ANN) for user modelling and a machine learning algorithm for behaviour classification. They also provide an alternative to this in case the user fails all three pattern matching cues.

D'Lima and Mittal have a multistage system that creates a new user and models his behaviour based on a prompt of a sample English sentence that contains all the characters. The users do this 10 times to train the system which re learns with every new entry. During the authentication stage the authors use a Gaussian probability density function for threshold check with a minimum threshold value of 90%. The retraining is simply done by taking the average of the last user model and the current one. This seems like an interesting scheme for improved password security and we would agree with it if there were no other options available. There are obviously issues with this scheme like still relying on the passwords and all of their vulnerabilities.

3.13 Passwords are Dead: Alternative Authentication Methods

Bachmann started off with, once again, the well known issues and problems of traditional passwords. The authors proposed to consider using a number of different newer methods. These new methods and techniques include but are not limited to biometrics, image authentication, authentication without preset passwords, electronic tattoos and electronics edibles. The main method presented and proposed is using authentication without preset passwords such as the brand new services provided by PINgrid and SlickLogin (which was recently acquired by Google). This is basically using the natural pattern matching skills of most people and using the fact that they're extremely memorable and just as secure as old password schemes. The way this would work is a user would, for example, choose a pattern of six keys on a 6x6 grid of numbers. Then whenever the user would want authenticate he would just have to enter his pattern the auto-generated new password based on the grid numbers would activate and check against the user pass pattern. If these thing match then the user is able to access the service or data he requested.

Another new and interesting method proposed by Bachmann is image authentication of which there are three main types. These are searchmetric which is selecting a set of images from a certain predetermined subset, locimetric which is picking out specific points on an image and drawmetric which is drawing lines from certain points to certain others on an image. Out of these three types drawmetric and searchmetric are probably the most common. We have differing opinions on all of these alternative authentication methods as they are largely quite subjective due to their complete difference in security, usability, familiarity and comfort creating a whole spectrum for the both of us. However we can both agree that the old password model needs to go and should be replaced by one, if not more than one, of these alternative schemes. Although much more research will need to be done on the usability and acceptance of the brand new methods such as tattoos and edibles due to their bizarre and intrusive natures.

3.14 A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems

In *A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems*, Huang et al. investigated the use of three-factor authentication (password, smart card, and biometrics) to authenticate users of distributed systems and proposed a generic framework to transition from two-factor authentication (smart-card-based password authentication) to three-factor authentication. They argued that text-based passwords can be cracked in a short time by simple dictionary attacks and smart-card-based password authentication can fail if the password and the data on the smart card gets into the hands of an attacker. Further, they showed that existing approaches to three-factor authentication have followed a chain of fixes and improvements and claimed that their authentication scheme is more secure than those of their existing counterparts. Their proposed three-factor authentication comprises five steps, which can be summarized as follows[4]:

1. 3-Factor-Initialization$(k) \rightarrow (SK, PK)$
2. 3-Factor-Registration $C[PW, bioData) \overset{\text{3-factor-registration}}{\Longleftrightarrow} S[SK] \rightarrow SC$ (smart card)
3. 3-Factor-Login-Authorization $C[PW, SC, bioData) \overset{\text{3-factor-authorization}}{\Longleftrightarrow} S[SK]\{1, 0\}$
4. 3-Factor-Password-Changing
5. 3-Factor-Biometrics-Changing

We agree with the authors that the proposed framework adds an extra layer of security to the existing two-factor authentication. The authors discussed the use of cancellable biometrics to preserve privacy but excluded it from their framework upon the grounds that secrecy is a requirement in biometric salting and it is challenging to design a noninvertible transform [7]. Consequently, we do not believe their proposed solution can be adopted on a large scale until research is done on the practical threats to three-factor authentication and the generic framework in converted into a practical one with better performances.

3.15 Passwords: If We're So Smart, Why Are We Still Using Them?

In 2009, Herley, Oorschot, and Patrick argued in their paper (*Passwords: If We're So Smart, Why Are We Still Using Them?*) that passwords have been used for many years, but due to the number of problems they involve, their use should be coming to an end. They suggested that users' selection of weak passwords increases the feasibility of guessing, brute-force dictionary and exhaustive attacks [6]. Moreover, by utilizing password reset schemes, users make expensive customer support phone

[4]where k is a system security parameter, C represents the client, S represents the server and the information in square brackets indicates secret data.

calls or utilize automated backup authentication schemes, which often involve very weak forms of authentication such as insecure challenge questions.

The authors suggested further that while there are concerns with passwords, there are at least six barriers to moving beyond their use. These barriers are as follows: (1) *Diverse requirements* - there is a wide range of services, such as financial transactions and social networking sites, so one solution will work; (2) *Competitive technical proposals* – there are different (dis)advantages, cost, etc, when employing a new system; (3) *Competition among stakeholders* – people hold different views that cause challenges; (4) *fear of losing data* – it is difficult to make trade-off decisions about known loss incidents versus future costs of employing new authentication schemes; (5) *reluctant users and usability concerns* – new solutions often require additional user effort and buy-in; (6) *Individual control of end-user platforms* – e.g. banks cannot tell users how to secure their personal computer; [6]

Based on the above barriers and the authors' suggestion that users are satisfied with resetting their passwords when required, we believe that text-based passwords will be in use for quite a few more years. It may take a catastrophe or government regulation to push organizations to adopt newer forms of authentication techniques.

4 COMPARISON

Three of the papers [2, 5, 13] that we reviewed above dealt with challenges involving passwords, [15] presented a comparison of password techniques, and [12] discussed the use of passwords in insecure authentication. Three papers [8, 9, 14] focused on strengthening password authentication schemes and one paper [4] questioned whether strengthening passwords actually accomplish anything. [1, 3, 7, 10, 11] proposed alternatives to text-based password authentication and [6] attempted to answer why organizations have not transitioned to new authentication schemes.

We now compare the ideas and solutions proposed in the papers. All the papers that dealt with password challenges emphasized that weak passwords can cause systems to be more vulnerable to attacks. [5] compared rules in 1991 with 2001 and stated that they have gotten more stringent due to the technical capabilities of attackers (See Table 3.1). The author of [5] proposed using delays between user attempts to enter their password and introduce a larger numbers of attempts to discourage them from writing down their passwords. However, if users are given more attempts to enter their passwords, this also allows attackers more time to carry out brute-force dictionary attacks. Therefore, we do not believe this is an ideal solution. Further, Both [4] and [6] showed that strong passwords may not accomplish much since the most prevalent attacks on passwords are phishing, keylogging, and brute-force attack. [4] proposed that strong userIDs could achieve better security than passwords, which we agree with based on the mathematics they provided.

In [12] and [15], both papers agree that there are issues with traditional password based security but largely have differing views and proposed solutions. This is mostly because of the large difference in the publication date of each paper and the awareness of the problems of traditional passwords. In [12], we see a unique and robust solution to an essential problem in early secure, remote com-

puting and authentication whereas in [15] we see a comparison of the already established password authentication techniques and the differences and similarities between them mainly in terms of memorability and subjective user preference.

If we employ the solution of improving password authentication as proposed in [8, 9, 14], we think a combination of solutions would be ideal. First, instead of using a large number of rules that annoy users, [13] offered a better solution than [5] that only requires three rules to achieve a strong password, and the author proposed a good way (PQI that utilizes Levenshtein's editing distance) to determine the strength of a password. Improved visual preference authentication as a password reset scheme [8] could be combined with Jeong, Won, and Kim's improved hash-based strong-password authentication protocol. While Vance et al. achieved ideal TPR and FPR in [14], we do not believe instilling fear in users is a good way to achieve secure authentication. Moreover, this technique could be further utilized as a test in online registration systems to see how users respond instead of doing a controlled field experiment as done by the authors.

Finally, if we opt for alternatives to text-based password authentication then we have a wide range of options available as presented in [3, 15] and [1]. Out of all of these options, a mix of the best two or three might be ideal. As proposed by the authors of [3] is probably a better idea to use a combination of password authentication techniques to grasp all aspects of these issues like usability and security. So we could possibly use theses keystroke biometrics in combination with an alternative like associative passwords as analyzed in [15]. We could of course also use the brand new methods such as edible pills and electronic tattoos, proposed in the same paper, but there has not been enough research done on these methods in terms security or usability and most users would be freaked out by these new and intrusive methods anyway, including ourselves. We believe that the three-factor authentication proposed in [7] could be a very secure means of authentication when compared with [1, 3, 10, 11]. However, due to its generic stage, it cannot be used as an authentication technique until further research and analysis is done.

5 DISCUSSION

In this section, we discuss our findings and lessons learned from the review.

In terms of the challenges with passwords, most of the papers we reviewed mentioned some challenges with text-based passwords such as the potential of brute-force, keylogging, and phishing attacks. However, [4] showed that a relatively weak password (e.g. a 6-digit pin) could withstand a brute-force attack of up to ten years and strong passwords do not protect against keylogging, phishing, attacks that result from special knowledge about a user, and social engineering. We agree with this understanding and think that solutions such as those proposed in [5] fix one challenge, but are prone to other attacks. Additionally, the password quality indicator proposed in [13] is more useful than the existing entropy-based technique in the literature.

In terms of the second class of papers that dealt with strengthening password authentication schemes, each paper proposed an improvement to a unique aspect of password authentication and, therefore, has its its own merit and disadvantages. Due to the challenges with the use of security questions

as part of a password reset scheme, we believe the improved visual preference solution proposed in [8] is novel and better than the existing two-class visual preference scheme as shown in Table 3.2. Jeong, Won, and Kim demonstrated that their improvement to Kim-Koç's protocol proposed in [9] is very secure. We think this solution is ingenious due to their redesign of Kim-Koç's entire scheme plus the added layer of encryption.

Finally, in terms of alternatives as listed in [1] and of these that have been analyzed by Zviran and Haga there are a few alternatives that stand out and present themselves to be viable for most users in the near future. The associative passwords discussed and analyzed in [15] have a promising score in terms of memorability and user preference and could be used in conjunction with the method of keystroke biometrics as proposed in [3]. However we also really like the method of using people's natural ability of pattern matching and its inherent memorability as another alternative as proposed by PINgrid in [1]. This method has two inherent advantages over other methods since it utilizes the natural human ability that we all share of being easily memorable and creative thus secure.

6 CONCLUSION

Text-based password authentication has been around for a long time and many scholars and users hope its reign is coming to an end. In this paper, we reviewed several papers about the challenges surrounding the use of text-based password authentication, improvement of password authentication schemes, and the design and adoption of alternative authentication techniques. While we agree with the premise that text-based password authentication has its weaknesses, we believe that due to differing requirements in organizations, no one solution will replace it in the near future. Alternatives such as biometrics, graphical passwords, two-factor and three-factor authentication will be adopted gradually until the barriers preventing the death of text-based passwords are torn down.

References

[1] M. Bachmann. “Passwords are Dead: Alternative Authentication Methods”. In: *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint*. 2014, pp. 322–322.

[2] Art Conklin, Glenn Dietrich, and Diane Walz. “Password-Based Authentication: A System Perspective”. In: *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS’04) - Track 7 - Volume 7*. HICSS ’04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 70170.2–. URL: http://dl.acm.org/citation.cfm?id=962755.963150.

[3] N. D’Lima and J. Mittal. “Password authentication using Keystroke Biometrics”. In: *Communication, Information Computing Technology (ICCICT), 2015 International Conference on*. Jan. 2015, pp. 1–6.

[4] Dinei Florêncio, Cormac Herley, and Baris Coskun. “Do Strong Web Passwords Accomplish Anything?” In: *Proceedings of the 2Nd USENIX Workshop on Hot Topics in Security*. HOTSEC’07. Boston, MA: USENIX Association, 2007, 10:1–10:6. URL: http://dl.acm.org/citation.cfm?id=1361419.1361429.

[5] Edward F. Gehringer. *Choosing Passwords: Security and Human Factors*. 2002.

[6] Cormac Herley, P. C. Oorschot, and Andrew S. Patrick. “Passwords: If We’re So Smart, Why Are We Still Using Them?” In: *Financial Cryptography and Data Security*. Ed. by Roger Dingledine and Philippe Golle. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 230–237. URL: http://dx.doi.org/10.1007/978-3-642-03549-4_14.

[7] Xinyi Huang et al. “A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems”. In: *Parallel and Distributed Systems, IEEE Transactions on* 22.8 (Aug. 2011), pp. 1390–1397.

[8] M. Jakobsson and H. Siadati. “Improved Visual Preference Authentication”. In: *Socio-Technical Aspects in Security and Trust (STAST), 2012 Workshop on*. 2012, pp. 27–34.

[9] Hanjae Jeong, Dongho Won, and Seungjoo Kim. “Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol”. In: *Journal of Information Science and Engineering,* 26.5 (Aug. 2010), pp. 1845–1858. URL: http://www.iis.sinica.edu.tw/page/jise/2010/201009_18.html.

[10] Qi Jiang et al. “Improvement of Robust Smart-card-based Password Authentication Scheme”. In: *International Journal of Communication Systems* 28.2 (2015), pp. 383–393. URL: http://dx.doi.org/10.1002/dac.2644.

[11] M. Kumar. “New Remote User Authentication Scheme Using Smart Cards”. In: *Consumer Electronics, IEEE Transactions on* 50.2 (May 2004), pp. 597–600.

[12] Leslie Lamport. “Password Authentication with Insecure Communication”. In: *Commun. ACM* 24.11 (Nov. 1981), pp. 770–772. URL: http://doi.acm.org/10.1145/358790.358797.

[13] Wanli Ma et al. “Password Entropy and Password Quality”. In: *Network and System Security (NSS), 2010 4th International Conference on*. 2010, pp. 583–587.

[14] Anthony Vance et al. “Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment”. In: *2014 47th Hawaii International Conference on System Sciences* 0 (2013), pp. 2988–2997.

[15] M. Zviran and W. J. Haga. “A Comparison of Password Techniques for Multilevel Authentication Mechanisms”. In: *The Computer Journal* 36.3 (1993), pp. 227–237. URL: `http://comjnl.oxfordjournals.org/content/36/3/227.abstract`.