An analysis of the alternatives of using passwords for web-based user authentication

Son Mac and Kevin Gilman

I. Abstract

As web technologies continue to evolve and advance at a rapid rate, web-based systems have now enabled users to access vast amounts of information and knowledge with just a few clicks, but at the inevitable cost of trading personal data. Therefore, it is without any doubt that user authentication has become one of the most crucial aspects of contemporary web-based technology, which is traditionally operated with text passwords. However, it is also widely acknowledged that using passwords to authenticate and protect personalized data do have several shortcomings, including vulnerability to cyber-attacks and poor password management practices. As a result, alternative authentication methods have been proposed and implemented to enhance both security-related and user-experience aspects.

This literature review will first examine the current measures to improve the quality of passwords generation and management, then analyze some outstanding approaches to replace traditional password authentication which will provide insights into their strengths and weaknesses, and lastly discuss whether the use of passwords is still a secure and valid authentication technique for modern web-based systems despite their limitations.

II. Introduction

Ever since its first usage in the 1960s, text passwords have gone hand in hand with the development of the Internet which is the home to various web-based technologies, and have become one of the most common methods to authenticate human users in such environments. Generally, a password is required when an Internet user registers for a service that manages and provides a personalized experience in order to generate a secure layer of protection for these sensitive data, such as health records or financial transactions. In addition, the use of passwords as a layer of security also helps a system to filter out unauthorized access or intrusions.

One major problem with password-based authentication arises when cyber-attacks start to target the predictable nature of passwords. A study by Anne Adams and Martina Angela Sasse found that people, without feedback from security experts, often use easily guessable choices such as names or dictionary words, making the content of such passwords much less secure (Adams & Sasse, 1999). Furthermore, a recent investigation conducted by Cybernews on more

than 15 billion passwords collected from data breaches has shown that the three most common phrases are “123456”, “123456789”, and “qwerty” (Masiliauskas, 2023). These passwords are notoriously insecure and have been widely publicized as such, yet many Internet users still prioritize them at the cost of memorability. With a view to tackling this issue, many online platforms have implemented password composition policies upon registration or display a predefined metric that informs the users about the strength of their chosen passwords. These measures have been successful in making users adopt stronger passwords. For example, many websites require users to include a mix of uppercase and lowercase letters, numbers, and symbols, and also to make sure that the length of the password is at least 10 characters long.

With the proliferation of new online services every day, the average Internet user has to manage a sheer amount of accounts, each of which requires a complex password for security purposes. Unfortunately, this has eventually led to another major problem with password-based authentication: the tendency of people to share a single password, or to keep slightly modified versions, between separate platforms. Generally, repetitive but strong passwords do not directly lead to an insecure layer of security, but the risks of credential stuffing attacks caused by hacked accounts or unforeseeable data breaches do highly discourage the practice of reusing passwords regardless of complexity.

The continued dominance of password-based authentication across the Internet, coupled with the emergence of modern security threats, suggests that a solution to improve or replace the use of passwords is inevitable and of the utmost importance. However, determining the ultimate approach to enhance the current password system or to introduce a viable alternative is a complicated and challenging task. This is due to the tradeoff between simplicity and security in implementation, and different services require varying degrees of each. This literature survey aims to provide a comprehensive analysis of the current situation of password-based authentication methods. Moreover, it will examine some popular measures currently in place to strengthen these systems and evaluate potential candidates that may be adopted in the foreseeable future.

III. Problems

As previously noted, one common flaw of password-based authentication since its early days is the fact that users tend to create short and simple passwords using names, birthdays, or terms from dictionaries. On the bright side, employing this practice will provide users with a convenient experience when authenticating themselves to an online service since it will require less typing as well as little to no memorizing. Additionally, studies have found that a simple password also allows users to share it with their trusted ones more easily, and, at the same time, make the process of retrieving forgotten password significantly simpler (Tam, Glassman, & Vandenwauver, 2010). Although such insecure password habits will leave personal data and other privacy matters vulnerable to cyber attacks and fraudulent attempts, certain Internet users seem to lack understanding about how password cracking actually works, as revealed by the

study by Anne Adams and Martina Angela Sasse. More specifically, an employee from a construction organization who participated in the study believed that choosing a highly private word such as his wife's maiden name had already prevented the password from being maliciously interpreted (Adams & Sasse, 1999). In an attempt to explore this behavior even further, researchers have found that users of online platforms often hold an unrealistic optimism that the potential data breach, though bringing serious consequences, will not happen to them in the foreseeable future nor leave any immediate effects (Campbell, 2007), which eventually reduces the likelihood of those users adopting more secure password management practices.

Therefore, with a view to naturally encouraging users to employ stronger passwords, most online platforms have implemented a password composition policy on top of the ordinary authentication mechanism. The policy contains a set of rules that constrain password formation and length, making them more secure than ordinary passwords. An example of the password composition policy from one of Apple's applications is as follows:

- 8 or more characters
- Upper and lowercase letters
- At least one number

While this measure assures that all passwords will achieve a certain level of complexity and become less susceptible to cyber attacks, it does coexist with a tradeoff between security and usability due to the "password fatigue" that stems from a complicated policy. Indeed, "Password fatigue" is a natural behavior amongst users when they have to facilitate and memorize many passwords, especially complex ones, between different accounts. In fact, this behavior tends to reduce the security of the password system considering how users will attempt to write the passwords down, store them electronically, or reuse them across most websites (Das, Bonneau, Caesar, Borisov, & Wang, 2014). Supporting this, a study by Wash et al. reveals that passwords that are more complicated or have more entropy are more likely to be reused. Considering such shortcomings, most online platforms only implement simple password policies and leave it up to users to decide the actual complexity of their passwords.

Another traditional approach to ensure the complexity of passwords is to impose a "password meter" that automatically evaluates the strength of the chosen password. However, since this approach relies entirely on the designer of the meter for the evaluation of complexity, it would be difficult to counter the vulnerabilities that do not come from the lack of complexity. For instance, an adversary with certain knowledge about a user's habit of creating passwords will find it simple to break passwords that are considered secure by the password meter (Das, Bonneau, Caesar, Borisov, & Wang, 2014).

In general, it can be seen that most attempts to maintain traditional password-based authentication just by improving the complexity come with certain drawbacks, raising the need

for more effective solutions or potential replacements which will be discussed further in the next section.

IV. Body

This section will explore (1) the measures implemented to enhance the security of traditional password-based authentication, and (2) potential alternatives to this method with a brief analysis of the advantages and disadvantages of each approach. This provides insight into the challenges associated with implementation for particular use cases.

1. Approaches to enhance the security of traditional password-based authentication

Considering the known shortcomings of traditional password systems, which mainly result from the "human" factor as discussed previously, the approaches below concentrate on naturally eliminating the challenge of "password fatigue" while still maintaining a user-friendly experience.

a. Two-factor authentication (2FA):

This method is an enhanced authentication mechanism to protect users who lose control over their passwords either through a cyber attack, such as phishing, or a data breach event. The method requires access to an additional communication channel to provide the users with a short-lived one-time-generated token that will accompany the traditional password during the authentication process. Recently, the growth of personal cell phones has helped to facilitate the deployment of 2FA significantly. For example, after the user successfully provides the password to the online server, they need to input a one-time-generated code being sent to their phone via a text message. After that, the system will verify if the code is valid before granting access to the user. While it does not directly help the users protect the password, 2FA ensures that access to personal data is protected as long as the personal device, such as the user's cell phone, is not compromised, and allows the user to safely retrieve a new password to stop the attack completely. In addition to SMS texts with the one-time-generated token, the second factor in 2FA can also be other personal physical devices such as a key fob, a USB, or biological characteristics that are unique to the user, such as a fingerprint.

Although requiring a second layer of authentication makes 2FA extremely secure compared to just using the traditional password, the adoption of this method amongst users of modern web-based platforms remains relatively low. A study by a group of researchers at the Foundation for Research and Technology - Hellas on more than 100,000 Google accounts shows that only 6.4% of the population enable 2FA (Petsas, Tsirantonakis, Athanasopoulos, & Ioannidis, 2015). This may be due to the fact that 2FA users are required to have their second-factor device with them at all times, and in some cases, the device may not be readily available, causing delays or hindrances to accessing the service. Additionally, research has also shown that

personal cell phones are actually vulnerable to the interception of text messages (Zetter, 2016), putting SMS-based 2FA at risk.

b. Password management software

Password management software or password managers (PMs) are software applications that are designed to assist users in generating, saving, and organizing passwords. Usually, such applications will establish a connection to a local or a cloud database and use it to store all passwords from the user, which are securely encrypted to ensure an adequate level of protection. In order to operate a PM, users are required to keep a master password, typically a strong and secure one, which will be provided to the PM to grant access to all other passwords. Additionally, considering how users mostly interact with web-based applications, many modern PMs incorporate extra features to enhance user experience, including browser extensions that automatically complete sign-in/sign-up forms or cloud server storage that allows synchronization of the password database across multiple registered devices.

Since password managers are particularly designed and implemented to control the most sensitive data of any web user - passwords, the security of their architecture is evaluated based on two most important criteria: security of the master key and security of the credentials database. As shown in a study on 4 popular PMs by Arias-Cabarcos et al., they make sure that the master key is never stored, either in local storage or in cloud servers, but instead applied to a password-based key derivation function before being used on any of the PM actions. The function comprises a pseudorandom function, such as hash, and a salt value, and is being applied repeatedly to achieve a technique known as “key stretching” which reduces the vulnerability to cyber-attacks. Additionally, some PMs implement complex password composition policies to further strengthen the master password’s entropy. Regarding the security of the credentials database, most PMs employ Advanced Encryption Standard (AES) using a 256-bit key as the cipher, which is regarded as the algorithm with the highest security, while some others even go beyond by requiring users to update their passwords occasionally (Arias-Cabarcos et al., 2016).

Despite various advantages in terms of security that password managers bring about, the adoption of this method by the majority of web users remains unclear, and the problem seems to revolve around the usability of such systems. A usability study conducted by Chiasson et al. on a popular password management software in 2006, called PwdHash, has revealed that only 48% of users successfully sign in, and only around 20% of users can update their passwords with the password manager. More specifically, most users are reported to have “difficulty understanding when and how to activate each system, understanding how long it remains active once it is activated”, and are believed to be frustrated with the fact that they do not know about their passwords due to how the PMs are generating, encrypting, and inputting the passwords on behalf of the users (Chiasson, Oorschot, & Biddle, 2006). Although it has been 16 years since this usability study and improvements have been made to the new PMs, it’s always valid to question whether the incorporation of a password management system into the daily usage of an average

Internet user will be a suitable approach to enhance the security of password-based authentication. Eventually, people will be more likely to prioritize convenience and may be discouraged from adopting a quality password management solution.

Overall, both 2FA and PMs greatly improve the security of traditional password-based authentication by addressing the shortcomings of the human factor and adding extra security layers to the authentication system. On the one hand, in terms of security, while 2FA seems to provide stronger protection by operating on both computational and physical aspects, password managers, which primarily rely on a digital master password, will put all passwords at risk in the event of a well-prepared cyber attack. On the other hand, 2FA adoption might be less convenient due to the need for a second factor, while password managers can be easily installed into any computer with supporting features such as form auto-fill for online authentication. Ultimately, the choice between 2FA and PMs depends on the user's individual needs and preferences, and the specific applications and services being used.

2. Alternatives for text-based passwords

As the need for stronger security increases, the limitations of text-based passwords have become increasingly evident. There are several alternatives to traditional passwords that can provide stronger security and greater user convenience.

a. Physical tokens

One alternative to conventional passwords is the use of a physical token for authentication. This could include items such as USB drives, smart cards, RFID tags, or OTP tokens which are used as a physical key to authenticate a user. This adds a layer of security as users are required to physically possess the token to access their accounts. Physical tokens also provide the convenience benefit of not needing to memorize a long complicated text-based password. However, as with any security measure, physical tokens also have their own set of weaknesses that should be considered. To begin, there is a risk associated with physical tokens getting lost or stolen, which could result in compromised security. In addition, physical tokens often require specific equipment to authenticate users, which may not be practical for certain applications. These are important considerations before constructing an architecture for user authentication.

b. FIDO2

FIDO2 is a standard for providing stronger authentication methods for web services. FIDO2 utilizes hardware-based public key cryptography to provide greater security protection. The two main components are the Web Authentication API (WebAuthn API), and the client to authenticator protocol (CTAP). The WebAuthn protocol allows online services to authenticate users with public key cryptography. The CTAP protocol is used to provide secure communication between the client device, and the authenticator device. One weakness of FIDO2

is that it is not a universal authentication standard. Many major web browsers such as Google Chrome, Microsoft Edge, and Firefox support FIDO2, but it may not be feasible for all users to adopt the standard as their primary authentication method.

V. Conclusion

Through examination of the literature, it is evident that the continued reliance on text-based passwords for online authentication has led to numerous security issues. To address these problems, methods such as 2FA and PMs are used to provide stronger security and user convenience. However, there are other alternatives to conventional text-based password authentication including physical tokens, and FIDO2. Each approach of authentication has its own strengths and weaknesses which should be assessed before implementation. Text-based passwords are great to pair with 2FA as it adds the extra layer of security requiring a one-time authentication token without sacrificing too much convenience. Systems that use physical tokens for authentication have an added layer of security by requiring possession of a physical key. Consequently, physical tokens have a risk of being lost or stolen which could result in compromised security. Frequently a designer must balance user convenience with the security strength of the authentication system when choosing a method to implement.

VI. References

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

Masiliauskas, P. (2023, April 20). Most common passwords: latest 2023 statistics. Retrieved from https://cybernews.com/best-password-managers/most-common-passwords

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233-244. doi: 10.1080/01449290903121386

Campbell, J. (2007). Unrealistic optimism in internet events. Computers in Human Behavior, 23, 1273-1284.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. Proceedings of NDSS 2014. doi: 10.14722/ndss.2014.23357.

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: Is the world ready? Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 1-7. Doi: 10.1145/2751323.2751327.

Zetter, K. (2016, April). The Critical Hole at the Heart of Our Cell Phone Networks. Wired. Retrieved from https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure

Arias-Cabarcos, P., Marín, A., Palacios, D., Almenárez, F., & Díaz-Sánchez, D. (2016). Comparing password management software: Toward usable and secure enterprise authentication. IT Professional, 18(5), 34-40. doi: 10.1109/MITP.2016.81.

Chiasson, S., Oorschot, P.C., & Biddle, R. (2006). A Usability Study and Critique of Two Password Managers. USENIX Security Symposium.

VII. Roles and contributions

In this project, each team member played a critical role and made significant contributions towards research, and review. The areas of research were split into enhancement of text-based password authentication, and alternatives to conventional passwords.

Son worked on the problem section and the two approaches for the enhancement of text-based passwords. Kevin worked on the abstract, introduction, two alternatives for text-based passwords, and conclusion.