Password Security: Authentication and Management

Vitaliy Tsytsyk

Northwest Missouri State University, Maryville MO 64468, USA
S533720@nwmissouri.edu tsytsyk.vitaliy@gmail.com

Abstract. Passwords are an integral part of the security, particularly user authentication. There have been many attempts to get rid of passwords, and come up with a better way to authenticate, however, to this day passwords stay essential. As computing power increases, so do the challenges associated with ensuring the level of protection passwords provide doesn't drop. Password managers emerged as an interesting solution to diversifying complex passwords (avoiding re-use and similarities). There are pros and cons to them, and they keep getting increasingly more popular. As an alternative, or additional type of authentication, governments and companies started using key cards or biometrics, which introduce a new perspective on security and authentication. However, even with them becoming more common as the time goes on, they still do not fully replace passwords. Therefore, password security is as important as ever, and should not be overlooked.

Keywords: Password · Security · Authentication · Management · Encryption.

1 Introduction

Password security is one of the many important aspects in the world of cybersecurity, and especially applications security. Password is the "gate" that protects users' data from being accessed by third parties. Therefore, making sure the authentication and management rules in place are top-grade should be one of the top priorities for the company. This paper will talk about the types of authentication, biggest threats associated with password authentication and management, and discuss best practices and rules to follow in order minimize the risks.

1.1 Goals of this Research

The goal of this paper is to provide a general overview of passwords and user authentication, and security associated with them. This will, hopefully, encourage people to seek additional, more in-depth information.

2 Related Work

The topic of password security is not a new one - there is a plethora of research papers regarding the topic. Researchers tend to focus on various aspects of password security - from the effects of the complexity, to the user's perception and training. This paper is based on many other works, and highlights the already made points.

3 Results and Discussion

There are several ways to authenticate a user: knowledge-based, possession-based, or inheritance based. Knowledge-based method refers to the traditional way of authentication – by using a password generated by the user as a means of verifying their identity. Possession-based method relies on the ownership component – for example using a unique key card or another e- mail address in order to successfully authenticate. Finally, inheritance-based way uses user's physical data – such as fingerprints or retina scan. For most instances, just the "basic" knowledge-based method is enough, therefore it will be the topic being focused on.

The number of web applications – which are responsible for the largest percentage of passwords used – grows every year, which is why it is of the utmost importance to look out and protect against potential threats concerning password management. The most common ones are brute force attack, shoulder surfing attack, sniffing attack, data breach, and login spoofing. Brute force attack might not be a sophisticated one, but without the protections set in place, can be effective in stealing passwords with the use of automated tools. Shoulder surfing and sniffing attacks are "sneakier" – they utilize micro-cameras (first one) or key loggers (second one) in order to get a correct password without bombarding the servers with all possible combinations. Data breaches can be devastating – if one happens, third parties might get access to login credentials and other confidential information from the databases. Login spoofing counts on user's complacency and lack of industry knowledge. Conceptually similar to phishing, this attack uses fake login web pages disguised as the real ones in order to capture the user's credentials.

Educating users on the topic of password security is incredibly important, as a majority of people not familiar with it, can not always accurately identify insecure practices. [4] One of the examples, is a users' inability to correctly identify the level of password's predictability. One online study looked into the inconsistencies in users knowledge regarding the topic. [10] Hence, as an organization, it is of a great importance to educate employees to raise their password security awareness. [3] This study analyzed the effectiveness of different types of online remote training for employees, and suggestions to increase it. [9]

Being aware of potential threats is important, however the crucial part is placing precautions in place in order to never have to fall victim to one of them. Users are often encouraged to make their passwords "secure" – long, random-like, complex as well as making sure not to write them down and store in easily

accessed places. [2] At the same time, unfortunately, an average person will not always choose security over comfort, therefore those rules should be made a requirement in order to create or change a password. Some other good practices for password authentication include scheduling password changes regularly, disallowing password re-use, disabling "remember me" option when logging in, re-authenticating user due to inactivity and prior to performing a major function, disabling an account after a set number of failed login attempts, obscuring password on the user's screen, logging all both failed and successful login attempts, and using multi-factor authentication. Using pass-phrases can be a great way to introduce length and complexity, while also making it easier for users to remember them. [8] In this specific case, grammar can play a role too. [6] In addition to the listed above authentication practices, another big part of keeping passwords secure is properly storing and managing them. This includes (but is not limited to) hashing and salting the passwords with a strong cryptographic algorithm, making the write-in table where they are stored write-only (for the application), implementing all of the listed above procedures only on trusted systems, validating the data only after both login and password have been submitted, using only POST requests to transmit credentials and storing authentication credentials used for external applications in a secure place on trusted systems (source code is not considered one).

Password managers have emerged as a popular tool for an easy and effective password managing for users. Both private users, and companies are adopting their use. They provide a way for people to create, store, and auto-fill passwords, which enables users to have a unique and strong password for each platform they are registered on. [7][5] On the surface, they seem like a brilliant idea. However, critics suggest that trusting a third party with all of one's passwords might be dangerous too, in addition to having all of their passwords behind a "master" password - a single point of failure.

4 Conclusion and Future Work

Password security is a large and complex topic that cannot be fully explained, but only summarized in a paper this size. However, it is a great overview of the main points: authentication types, most common vulnerabilities, and best practices to ensure safety. Some topics that would be a good follow-up are deeper analysis into each one of the vulnerabilities to understand how to prevent them on a more fundamental level as well as explanations with concrete examples about each of the best practices mentioned. Password managers and password cracking tools such as John the Ripper and Hashcat deserve another paper dedicated to them too. [1]

References

1. Gong, C., Behar, B.: Understanding password security through password cracking. J. Comput. Sci. Coll. **33**(5), 81–87 (may 2018)

2. Li, Z., Li, T., Zhu, F.: An online password guessing method based on big data. In: Proceedings of the 2019 3rd International Conference on Intelligent Systems, Metaheuristics amp; Swarm Intelligence. p. 59–62. ISMSI 2019, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3325773.3325779, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3325773.3325779
3. Mayer, P., Schwartz, C., Volkamer, M.: On the systematic development and evaluation of password security awareness-raising materials. In: Proceedings of the 34th Annual Computer Security Applications Conference. p. 733–748. ACSAC '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3274694.3274747, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3274694.3274747
4. Mayer, P., Volkamer, M.: Addressing misconceptions about password security effectively. In: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust. p. 16–27. STAST '17, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3167996.3167998, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3167996.3167998
5. Oesch, S., Gautam, A., Ruoti, S.: The emperor's new autofill framework:a security analysis of autofill on ios and android. In: Annual Computer Security Applications Conference. p. 996–1010. ACSAC, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3485832.3485884, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3485832.3485884
6. Rao, A., Jha, B., Kini, G.: Effect of grammar on security of long passwords. In: Proceedings of the Third ACM Conference on Data and Application Security and Privacy. p. 317–324. CODASPY '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2435349.2435395, https://doi-org.ezproxy.nwmissouri.edu/10.1145/2435349.2435395
7. Simmons, J., Diallo, O., Oesch, S., Ruoti, S.: Systematization of password manageruse cases and design paradigms. In: Annual Computer Security Applications Conference. p. 528–540. ACSAC, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3485832.3485889, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3485832.3485889
8. Singh, K.: On improvements to password security. SIGOPS Oper. Syst. Rev. **19**(1), 53–60 (jan 1985). https://doi.org/10.1145/1041490.1041496, https://doi-org.ezproxy.nwmissouri.edu/10.1145/1041490.1041496
9. Sterk, F., Heinemann, A.: It is Not as Simple as That: Playing out Password Security Trainings in Order to Nudge Password Changes, p. 20–25. Association for Computing Machinery, New York, NY, USA (2021), https://doi-org.ezproxy.nwmissouri.edu/10.1145/3487405.3487653
10. Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F.: Do users' perceptions of password security match reality? In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. p. 3748–3760. CHI '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2858036.2858546, https://doi-org.ezproxy.nwmissouri.edu/10.1145/2858036.2858546