Grenze International Journal of Engineering and Technology, Special Issue

Practical Authentication Mechanism using PassText and OTP

V.Srividya[1], P.Swarnalatha[2] and L.Thirupathi[3]
[1] BE CSE Final year Student, Methodist College of Engineering & Technology /CSE Department, Hyderabad, India
Email: srividya.velupula@gmail.com
[2]BE CSE Final year Student, Methodist College of Engineering & Technology /CSE Department, Hyderabad, India
[3] Methodist College of Engineering & Technology /CSE Department, Hyderabad, India
Email: {swarnalaatha3576@gmail.com, thiru1274@gmail.com}

***Abstract*—Nowadays, especially with technology's fast development, password authentication mechanism is not enough anymore to provide complete security. This paper aims to implement a strong authentication mechanism with a practical reauthentication technique that answers the research question "how to increase the security of the authentication mechanism without sacrificing convenience?" The proposed solution is a combination of a text file that the user has to modify, "PassText", and a one-time password "OTP". This paper is based on achieving four main solution requirements: convenience, security, cost, and speed. Our proposed solution breaks the rules of security-convenience tradeoff by providing an intelligent authentication combination that provides security and convenience at the same time.**

***Index Terms*— One-time password, PassText, Reauthentication, Two-factors of authentication.**

I. INTRODUCTION

Security, convenience, and functionality are all essential factors for having an efficient authentication process. However, there is a tradeoff between these factors. When one increases, the others might decrease. There is an inverse relationship between security and convenience where organizations stand on a fine line between both. Therefore, there is an urgent need to find balance between security and convenience; otherwise, the organization will fall into either side. Unfortunately, nowadays, convenience keeps winning, which causes sacrificing security. Using passwords as an authentication method, despite the convenience, is full of security flaws [1]. One problem is that users may prefer passwords that are easy to remember, which makes them vulnerable to different types of attacks including guessing, dictionary, and brute force. Even if we suppose that the user was careful enough to set a strong password, he might fall a victim for a simple, yet smart, phishing attack. The increasing number of attacks on passwords has led organizations to force strict policies on how the user sets his password in order to provide an appropriate level of security. On the other hand, those policies have raised the inconvenience issue for the user, when the member needs to access his accounts frequently, not mentioning that the login session is relatively short in some systems.

The main contribution of our paper is improving the PassText mechanism through processing the whole text and not only a part of it. Then, hash it using bcrypt algorithm. Additionally, this paper focuses on increasing

Grenze ID: 01.GIJET.4.3.27

the security and convenience of the system that uses PassText by adding a second factor of authentication which is OTP and a reauthentication mechanism that requires PassText only as a one way of authentication during a certain session.

II. RELATED WORKS

This section first compares between different authentication methods, then, it illustrates some work related to our proposed solution.

The simplicity of using the password made it the dominant authentication method to authenticate users. Since passwords are the current authentication method used in most systems, it will be the reference of our comparison.

The comparison which is shown in Table I is conducted based on four different solution requirements: 1) Convenience: user's comfort and effort excreted in terms of memorizing or carrying objects [2]; 2) Security: how secure the system is based on four security measurements: resilience to physical observation, resilience to guessing, compromise detection and recovery from loss; 3) Cost-effectiveness: financial cost of implementing the authentication system; and 5) Speed: how fast is the authentication session from the starting point to the ending point [3].

A. Convenience

In this solution requirement, the techniques are compared using two sub criteria the memory-wise effort and the need to carry an external device. The result shows that all the techniques scored better than the password regarding the memorizing factor. In contrast, for the need to carry an external device, both types of biometrics are as the password offering the convenience for the user to not carry anything, while the NFC and Yubikey token offer less convenience than the password for this factor.

B. Security

The comparison of the authentication techniques security focuses on five security measures:

1) Resilience to Physical Observation

Physical observation here means that the authenticator can be stolen only from the observation; shoulder surfing attack is one example. What we can notice is that NFC, Yubikey and fingerprint are immune to these types of attacks. However, the voice recognition is vulnerable to them, because the voice can be recorded and then used for authentication.

2) Resilience to Guessing

Unluckily, guessing attacks are more successful than what people think. Due to the shortage of the human memory, some people might tend to choose passwords that are easy to remember, but on the other hand, easy to guess by the attackers. Nowadays, due to the increase of computing power and the availability of different dictionaries, the vulnerability for guessing attacks has increased too. Unlike the password, techniques such as NFC, Yubikey, fingerprint and voice recognition do not give the attacker the chance to try any predictable credentials.

3) Compromise Detection

It is important to deepen the defence line to exceed the front-line attacks. Therefore, compromise detection is essential to decide if an authenticator has been stolen or otherwise compromised, preferably before it is used illegally. For passwords and biometrics, the detection techniques are weak comparing to the detection methods of the NFC devices and Yubikey token. In the last two, the physical observation of the device's loss is deemed as physical evidence. In contrast, in case of the compromising of passwords and biometrics the user will not notice that, unless an authentication log is monitored and the user remembers when the last authentication activity occurred. Keeping in mind, that recently thefts of the token number have happened in this case the compromise is not detected; however, its effect will not last long because it is OTP, only viable for a session.

4) Recovery from Loss

As there is detection techniques there are also recovery techniques. The comparison here is different; the password has the best recovery methods among all the techniques. When a compromising is detected all what the user has to do is to change his password. Then come the NFC and Token recovery, in case of loss the user has to deactivate or deregister them from the system, but the same physical device will not be viable

anymore. The weakest recovery methods are for the biometrics, if the used algorithm does not employ the challenge-response concept and it only relays on the static biometric the compromise is deemed destroyable, because once user's biometric measures are exposed they cannot be recovered again.

C. Cost-effectiveness

The obvious result is that the password costs less than all other authentication techniques. And that because theses authentication techniques require special hardware or software to be implemented, deployed and maintained; therefore, they cost higher than the passwords.

D. Speed

The biometric techniques have similar processing speed level to the password. While NFC and the Token Yubikey have the highest speed among them all, because of the small size of their used code or signature that can be processed in short time.

TABLE I. COMPARISON BETWEEN EXISTING AUTHENTICATION TECHNIQUES

			Solution Requirements							
			Convenience		*Security*				*Speed -Cost-effectiveness*	
		References	*Memory wise-effort*	*Nothing to carry*	*Resilient-to-Physical observation*	*Resilient-to-Guessing attack*	*Compromise Detection*	*Recovery from Loss*		
Techniques	*NFC*	[4] [5] [6]	●	○	●	●	●	○	○	●
	Token (Yubikey)	[7] [8]	●	○	●	●	●	○	○	●
	Fingerprint	[9] [10]	●	=	●	●	=	○	○	=
	Voice Recognition	[11] [12] [13]	●	=	○	●	=	○	○	=

● offers a benefit over the password method; '○'the performance is worse than the password; '=' offers the same benefits as the password.

III. PROPOSED AUTHENTICATION SYSTEM

PassText is simply a text file contains certain meaningful text that is prompted to the user during registration. Then he must modify it by adding, deleting or changing characters. After that, each time the user wants to

access the system, the same original text file will be prompted to him and he must apply the exact modifications to the file. For our paper implementation, we decided to go with bcrypt which is a Blowfish based one-way hashing algorithm that is known for its slowness. Its slowness and multiple rounds ensure draining the attacker's resources, which prevents dictionary and brute force attacks. Furthermore, bcrypt has salts built-in, which helps in preventing rainbow table attack. It's noteworthy that bcrypt is considered slow compared to other hashing algorithms, however, its slowness is not considered an issue since 3 PassTexts could be hashed in one second. It's important to mention that bcrypt has a limit of 72 bytes, however, the PassText could be much longer than that. To overcome this issue, the PassText will be first hashed using SHA-256 hashing algorithm. After that, the resulting hash, which is only 32 bytes long, will be hashed again using bcrypt.

The main advantage of PassText over the password is that it provides a kind of visualization; users tend to remember what they can see and interact with it. To implement a strong authentication system, OTP will be used as a second authentication factor besides the PassText. For the practical reauthentication, the user must only modify the PassText whenever the session has been expired.

IV. Conclusions

After conducting a thorough research and comparison, we found out that most existing authentication methods suffer from drawbacks in one way or another, due to security-convenience trade-off. However, our proposed solution managed to stand out from other authentication methods by compensating for these drawbacks. In this paper, we introduced a new authentication method, PassText, which is based on modifying a text file and storing the hash of the modified file as a secret. This method enhances security on many levels since applying guessing attack on the PassText, unlike the password, is almost impossible. Furthermore, this method provides protection against brute force attacks since the PassText is longer than the password and has much more characters. Not forgetting to mention that the system is protected against dictionary attacks since the file modifications cannot be predicted easily. To enhance security even more, we combined OTP with PassText to provide a second factor of authentication. When it comes to convenience, we concluded that memorizing the changes made to PassText is easier than remembering a certain password, which length and security are affected by the shortage of human memory. Also, to make the user's life easier, we proposed that the user login with two factors at the beginning and reauthenticating with one factor only, which is PassText.

Future Work

We aspire to enhance our solution in the future by addressing some of the topics that were out of this papers scope such as ensuring that the transmission channels are encrypted in order to sustain complete confidentiality. Furthermore, we aspire to enhance the security of "Forgot PassText" function, since it only uses one authentication factor, which is OTP. To enhance security, more than one factor might be needed. It is important to note that user convenience should be considered as well.

References

[1] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 7(5), 95-107.

[2] Takahashi, T., & Nogami, H. (2001). U.S. Patent No. 6,332,025. Washington, DC: U.S. Patent and Trademark Office.

[3] De Luca, A., Hertzschuch, K., & Hussmann, H. (2010, April). ColorPIN: securing PIN entry through indirect input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1103-1106). ACM.

[4] Rahul, A., Krishnan , G. G., Krishnan, U. H., & Rao, S. (2015). NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY: A SURVEY. International Journal on Cybernetics & Informatics (IJCI), 133-144.

[5] Ali, A. H., RehamAbdellatifAbouhogail, I. F., & Youssef, M. I. Security Analysis of NFC Technology Compared with other Mobile Wireless Technologies.

[6] Alexiou, N., Basagiannis, S., & Petridou, S. (2016). Formal security analysis of near field communication using model checking. Computers & Security, 60, 1-14.

[7] Yubico, A. B. (2015). Kungsgatan 37, 111 56 Stockholm Sweden. The YubiKey Manual-Usage, configuration and introduction of basic concepts (Version 3.4).

[8] Künnemann, R., & Steel, G. (2012, September). YubiSecure? Formal security analysis results for the YubiKey and YubiHSM. In *International Workshop on Security and Trust Management* (pp. 257-272). Springer, Berlin, Heidelberg.

[9] J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano. (2012). "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". *IEEE Symposium on Security and Privacy, San Francisco, CA*. pp. 553-567
[10] Saini, R., & Rana, N. (2014). Comparison of various biometric methods. *International Journal of Advances in Science and Technology (IJAST) Vol, 2*.
[11] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, *2*(3), 13-28.
[12] Savchenko, A. V., & Savchenko, L. V. (2015). Towards the creation of reliable voice control system based on a fuzzy approach. *Pattern Recognition Letters*, *65*, 145-151.
[13] Matyáš, V., & Øíha, Z. (2002). Biometric authentication —security and usability. In *Advanced Communications and Multimedia Security* (pp. 227-239). Springer US.