Cybersecurity Mechanism and User Authentication Security Methods

Muhammad Mustafa Nabi[1] and Faisal Nabi[2]
(Corresponding author: Muhammad Mustafa Nabi)

Department computer Science, University of Sunderland, UK[1]
(mustafa.nabi2003@gmail.com)
School of Business, Department of Information System University of Southern Queensland, Australia[2]
(Received May 28, 2021; Revised and Accepted Nov. 27, 2021; First Online Dec. 15, 2021)

Abstract

New methods have come to secure user-defined password techniques, which often use traditional authentication-based security methods and user privacy. This paper has examined and reviewed user privacy and cybersecurity issues to deal with them. It is archived through conducting research based on a study of password incorporation with Brain-computer interface technique to understand the problem in-depth and classify the solution in the light of current authentication schemes and then proposed analysis to draw solution based conclusion.

Keywords: Authentication; Brain Bioinformatics; Cyber Security; Privacy; User Security Methods

1 Introduction

Usability is one of the most critical social concerns and problems currently in the area of cybersecurity. Supporting confidentiality, integrity, availability and other problems, security characteristics have become normal parts of the digital world that infiltrate our lives.

Required usage by both experts and novices. As security characteristics are exposed to broader organizational cross-sections, certain roles must be highly utilizable. This is particularly true because the poor usability of cyber security tools and functionality in that context usually translates into insufficient use, effectively restricting their performance and principles of user experience design in context of cybersecurity.

The classic example of these two principles is one of the most common safety measures used today when dealing with passwords authentication process. From a safety point of view, long and complicated (hard to guess). Special, frequently updated passwords are, however, ideal from a usability point of view; these criteria are also a major burden on users and, in turn, the usability of the system [16]. In the cyber safety sense, the focus is also on the digital world, a vast majority of these general security problems are also present. The problem of cybersecurity and comparable human-computer interaction and protection, especially in the case of principles of user experience design in context of cybersecurity system. Therefore, this conceptual and implementation gap is bridged and emphasized and stressed. It is important to combine these two principles to create functional interfaces and systems for cybersecurity.

Six types of usability studies are commonly available in the field principles of user experience design in context of cybersecurity. These include authentication, encryption, Public Key Infrastructure (PKI),

pairing of devices, security software and systems for security. In each of these areas, problems have been reported which affect the usability of cybersecurity interfaces and functionality. A crucial point to remember, apart from device usability being an issue in itself for users (in terms of uncertainty, annoyance, and so on), is that poor usability usually translates into incorrect or insufficient configurations of security tools and features in a cybersecurity context (e.g., access controls, firewalls, encryption mechanisms, routers) [9].

As the reflects on the issue of a lack of cybersecurity systems, Security functionality visibility in end-user applications. Popular failures include the fracturing of security options across Various menus and sub-options, security features that are classified as 'Advanced' (reporting that access should be granted only by advanced users), and lack visible system security status indicators.

Usability of cybersecurity issues faced by typical end-users. Such concerns include the proliferation of technical terms, Functionality, lack of obvious device, vague and confusing Informative feedback and status, forcing uninformed protection Decisions, and absence of security feature incorporation. The research Question that we deemed to be important to analyze authentication process in terms of password strength mechanism.

1) How can we determine the strength of strong scheme of authentication?

2) How one can evaluate authentication based password protection?

3) Usability and analysis of password mechanism through strong authentication method?

2 Background Based on Existing Research

The usability of cybersecurity should be evaluated or considered early. Cybersecurity, accessibility and their relationship with each other the ideas in the original should be explored and evaluated. Phases of the design and growth of a system. Bolting of Cybersecurity accessibility or retrofitting only at the end the growth of a scheme is likely to be harmful to Overall the device and lead to additional problems with usability and security.

Compatible for all forms of users: cybersecurity features should be designed to be versatile and accommodating for beginner and professional users. Although inexperienced users may often need support and step-by-step instructions, experienced users should be able to access the necessary features quickly through device shortcuts, hot keys and so on. In general, the need for different modes of device interaction is highlighted by this guidance [11].

Prevention, handling and recovery of failures: Systems should be built so that they foresee consumer Mistakes and avoid them from occurring. If mistakes do occur, they should be treated gracefully, however, and presented in instructive instructions and explain steps for recovery. This advice also indicates that the interface of cybersecurity Designs support functionality to undo and fast exit for when users make mistakes and enter unnecessary programme. Users should be able to rely on the application and not feel at a loss.

Make security measures available and accessible: Security, similar to other application features, should be easily accessed and visible. Hiding the features of cybersecurity inside sophisticated or different sections of an interface, it is likely to make the job of the consumer more challenging and more difficult. Ultimately, system usability is hindered. Authentication Mechanisms Come in a Variety of Forms. Researchers have been looking at how to design and build different types of authentication solutions using various methods, such as PIN, passwords, OTP, face, contact, and so on.

The need for effective computer security is growing in parallel with the rapid growth of networked systems and applications such as e-commerce. In general, there are three types of authentication: 1)

what you know (knowledge-based), 2) something you have (possession-based), and 3) something you are (identity based).

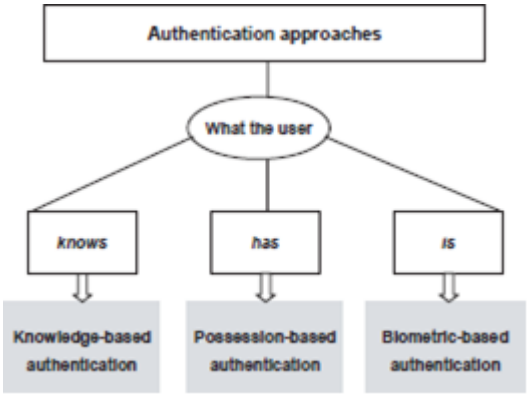

Figure 1: Methods of authentication approaches

Fist Method KBA is a security measure that distinguishes users by asking them to answer basic security questions. Authentication based on knowledge has become popular as users are asked to answer these questions in order to gain access to password-protected areas of their own. While this technique is useful, the learning of pins and passwords is still difficult for people. Computers will in future be able to devise these passwords [8, 15]. On the other hand, KBA may be an efficient way to handle individual user authorization, but there have been serious privacy concerns raised about using this type of personal information for online or network security.

Second, this method is often referred to as "token-based authentication." Its aim is to verify the legitimacy of the consumer. The token is created using the users' username and password. The user can then use the token at other locations to gain access to those locations without having to enter their usernames and passwords. This token, on the other hand, will grant them access for a set period of time. In short, users are given a token based on their login credentials. This token allows them to access their secure services for a set period of time without having to re-enter their credentials. The token is mainly made up of a string of 32 characters. The created token is associated with the database in some way after the user enters his login credentials. The token may be used to gain access to other sections of a related app. This is why the obtained token must be preserved after it has been retrieved. Since they keep the data for that person, tokens [7] are stateless and scalable.

This method ensures protection by ensuring that the token expires after a fixed period of time, requiring the user to re-login. This assists us in remaining healthy. There's also the concept of token revocation, which allows one to cancel a single token [5, 21] or even a group of tokens that share the same authorization allowance.

Third Method, A biometric system's architecture involves specialized hardware that is linked to processing hardware through a sensor. External attacks are vulnerable to the isolation of the pieces. Cryptography, on the other hand, may help protect the device. This is accomplished by dividing each system's private cryptography key, generating limited vectors from the system to be used as keys, and then computing a hash function for all of those keys. The process is repeated for each trait, and the hash functions are saved in an infinite database [13]. These hash values are primarily used to identify people.

The user would enter a biometric attribute that would thus be translated to the defined hash value

and the results tested accordingly. This approach is applied to all parts of the cryptographic key that correspond to various characteristics, and the resulting private key is then discarded after it has been used [14]. Although it is possible to use all of the traits at once, doing so reduces the risk of misuse and fraudulent attacks. Biometric authentication methods such as fingerprints, iris scans, and facial recognition are not yet commonly used because they are costly, the verification process is slow, and often inaccurate (i.e. it is unreliable because it is time consuming). The classification of the various authentication techniques.

3 Research Method

We have carried out an empirical research, review the most closely related research on passwords, and summarize related work exploring users' expectations of protection. The threats to password protection are then discussed, as well as methods for determining password power through the study of Brain Computer interface technique that would incorporate the password in dual biometric authentication process for strong authentication mechanism.

A recent research analysis of password formation using a think-aloud protocol indirectly relied on users' expectations of password protection in the password domain [19]. The study's emphasis, however, was not only on security perceptions. In addition, the previous research in literature was qualitative, while ours approach is primarily quantitative.

4 Empirical Research Study & Research Question Examine

The Password authentication suitability method among the discussed techniques for user and cyber security prospectus. A research from review of existing work-study explored users' impressions of the security and usability of computer unlock patterns [1], which is most closely related to our work. The technique compared two graphical and text unlock patterns and rated their relative security and

memorability (e.g., was the first pattern more safe but less memorable than the second). The analysis, unlike ours, did not compare the patterns' actual security.

A variety of attacks can compromise the authentication system. The effect of a password's protection on each form is different. The most serious threats are described in this section. The protection of a password is not always essential [3]. When a user's password is hacked, the attacker receives it in plaintext. In certain other instances, it is important that a password is not easily guessable. The attacker tries to authenticate to a running machine using guesses at the user's password in what is known as an online attack.

An offline attack, on the other hand, normally entails large-scale guessing. Passwords should be hashed using a cryptographically safe (irreversible) one-way mechanism, according to best practices. When a user logs in, the machine hashes the password and compares it to the value stored in its database. The type of hash function used to store the password as well as the resources available to the attacker determines the resistance of a password to an offline attack. Due to their speed, hash functions like MD5 were optimized for performance, making them ineffective for storing passwords.Modern hardware will attempt billions of MD5 guesses per second. The most serious security risk posed by an offline attack is password reuse [19]. Attackers will try the same username and password, or near variants, on other sites once, they have discovered a user's password in an offline attack. Passwords are often reused by users [4, 6, 19, 22], which can be dangerous and trigger significant harm.

Statistical approaches [2], which are mainly ideal for very large sets of passwords, or parameterized password guess ability [2, 10] can be used to obtain more precise password strength measurements.

Calculating a guess number for each password indicates how many guesses a specific password cracking method optimized and educated in a specific way would require to guess the password.

The below-mentioned Table 1 clearly illustrate the participants based data collection perception regarding cyber-attacks on systems and application that may cause of poor user adoptability strong password technique or other reasons of exploitation gap between the cyber security and user authentication process. Therefore, we have researched alternative approach to deal with these issues of cybersecurity and user authentication password process for a suitable secure defense.

Table 1: Participant demographics

Partidpant	Age	Sex	Experience
1	35–44	F	Career government information security (IS), academic IT researcher
2	>65	M	Career government IS officer, industry IS developer, IT educator
3	45–54	M	Security developer, academic IT security educator
4	35–44	M	Career government IS officer, academic IS researcher
5	<21	F	IT security student
6	35–44	M	Government network security researcher, academic IS researcher
7	35–44	M	Academic cybersecurity educator, IS developer
8	35–44	M	Industry mobile security researcher, university IS educator, industry IS developer
9	22–34	M	Academic IS researcher
10	45–54	M	Government IT security researcher
11	45–54	M	Government IT security researcher
12	22–34	M	Academic IT security researcher, government information security officer
13	35–44	M	Industry chief technology officer (CTO) and mobile IS researcher
14	>65	M	Military and government IS developer, academic IS educator, industry IS researcher and developer
15	55–64	M	Government and industry researcher and developer
16	22–34	M	Government IS researcher, academic IS student
17	45–54	M	Government IS developer, academic IS educator and researcher
18	22–34	F	Government IS researcher
19	>65	M	Government and industry IS researcher and developer
20	45–54	M	security app developer, academic IT security researcher

In this research, the primary data collection approach was open-ended discussion on a given set of questions, which we thought was better suited to the subject matter than other relevant qualitative methods like surveys and either informal or highly structured interviews . This in-depth questioning was thought to be essential for evaluating complex and variable authentication behaviours, as well as their underlying risk and technological functionality mental models. To eliminate duplication and endorse exploratory questioning, the query instrument's behavior and outlook were reordered.

The second approach is carried out through empirical analysis of data through the research study regarding cybersecurity and user perception to strong computer security methods, which leads to strong authentication process. The above table illustrate the research analysis data about the different category of cyber-attack and organizational risk impact of user perception leads to authentication and security risk management.

In the light of our research the suggested, another approach, the suitability of induced electroencephalograms (EEGs) for implementing high quality, functional biometric authentication systems is explored in depth through this research study. EEGs are difficult to fake because they represent an individual's inner self and are likely to vary from person to person even when performing similar mental tasks. EEGs, on the other hand, are dynamic and noisy signals that are influenced by a variety of brain and body movements.

During our empirical research, we have studied EEG signals in specific contexts, such as visual stimulations that result in very concentrated brain behaviours known as Visual Evoked Potentials (VEP). To our knowledge, this is the first research study of EEG-based authentication using VEPs, but

Table 2: Empirical analysis of data risk and cyber-attack on system and risk identification process

Common Vocabulary for Risk N	CESO	ONTIDS	CRATELO	OMG	M4D4	CORESEC	NRL	WALI	CycSecure
Alert		X			X			X	
Asset (⊂ tangible, untangible)	X		X	X		X	X		X
Benefit				X					
Configuration			X	X	X				
Consequence	X		X	X		X			X
Control				X					
Cost			X	X					
Countermeasure			X	X				X	X
Credential				X		X			
Cyber attack	X	X	X	X	X	X		X	X
Cyber defense			X	X					
Cyber exploitation		X	X	X	X				
Cyber incident				X		X			
Cyber operation			X	X					
Cyber response			X	X					
Cyber risk			X	X					
Cyber threat			X	X					
Cyber vulnerability		X	X	X	X	X			X
Dependability (⊂ attributes)				X	X				
Detection	X	X	X	X	X				
Fault			X	X					X
Failure			X	X					X
Impact			X	X	X	X			
Intent			X	X					
Likelihood			X	X		X			
Mission			X	X			X		
Network		X		X	X				
Origin/Source	X	X	X	X	X				
Payload			X	X					
Report				X	X				
Risk			X	X	X				
Risk assessment	X	X		X					
Risk factor			X	X			X		
Risk identification				X					
Risk metric			X	X		X			
Risk mitigation				X					
Risk monitoring				X					
Security/Risk policy				X	X		X		
Security protocol				X					
Situation			X	X					X
Service		X	X	X	X		X		
Stakeholder			X	X					
Target	X	X	X	X	X				X
Threat		X	X	X		X			
Treatment				X					

there have been other studies of EEG-based identification and EEG-based authentication using other brain activity stimuli (e.g. specific imagining tasks).This technique incorporating into password-based authentication makes this approach more secure as a dual security mechanism.

Therefore, we proposed a research study password based brain biometric authentication technique incorporating this scheme for strong authentication process of user protection as Brain Computer Interface method.

5 Research Analysis

We believe that this research is feasible to conduct through the process of data obtain as defined in methodology section. We will investigate the data obtained and analyzed it for research questions to justify the proposed research and timeline. The further details of data collection period is mentioned in the section of feasibility Targeted, data-driven input during password development is a promising way to help users better analyse their passwords in comparison to industry best practices. Password strength meters currently only inform users whether a password is strong or weak, not why [10, 18, 20]. Future research in this field may build on a recent study that revealed users' likely "auto completions" of the partially typed password [12].

There are no incentives for system administrators to allow users to create poor passwords for insignificant accounts or to write down their passwords. Users get oversimplified folk models and stereotypes. We demonstrated in this paper that users have a good understanding of the characteristics of strong and weak passwords by using correct authentication method, which can be used to assist users in creating stronger passwords, specially Brain Computer Interface technique incorporating password into it for strong authentication process.

6 Feasibility of Proposed Research

Our work entails comparing different methods for performing password-based authentication using and incorporating Brain Biometric authentication and demonstrating a realistic authentication scheme that can be used in security critical applications and computer security. For this purpose, research will expend to investigate the empirical research data and review of current research data relevant to above stated scheme. The time line for data collection is three weeks and research methodology helps out the gathering the data through empirical method rather than technology required hardware sensor of biometric detection and software for EEG signal reading for Brain biometric authentication mechanism.

7 Conclusion

The prevalence of bad passwords can appear to contradict characteristics that make passwords easier or harder for attackers to guess and compromise authentication process. This discrepancy, on the other hand, may be the product of a failure to educate users about the various types of password attacks and used authentication scheme. . For example, if a user reuses a password for other accounts or if the service provider fails to follow security best practices, the password's resistance to large-scale guessing is important. Users should defend themselves against all possible attackers using the defense-in-depth concept, which is why security experts often suggest using password managers to store unique passwords for each account. Moreover, our approach to password incorporating Brain Computer Interface technique would make the authentication process more secure.

Ethical Considerations

This research is involve human participation to conduct the interview and current research study in the field of cybersecurity and user interaction in terms of password authentication process strength and weakness.

References

[1] A. J. Aviv and D. Fichter, "Understanding visual perceptions of usability and security of android's graphical password pattern," in *Proceedings of ACSAC*, pp. 286–295, 2014.

[2] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proceedings of IEEE Symposium on Security and Privacy*, 2012.

[3] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Communications of ACM*, vol. 58, no. 7, pp. 78–87, 2015.

[4] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *Proceedings of NDSS*, 2014.

[5] H. Falaki, R. Mahajan, S. Kandula, *et al.*, "Diversity in smartphone usage," in *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys'10)*, June 2010.

[6] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[7] A. K. Jain, P. Flynn, A. ROSS, *Handbook of Biometrics*, Springer, USA, 2008.

[8] K. Jain, A. Ross, S. Prebake, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[9] R. Kainda, I. Flechais, and A. W. Roscoe, "Usability and security of outof-band channels in secure device pairing protocols," in *5th Symposium on Usable Privacy and Security (SOUPS'09)*, ACM, 2009.

[10] P. G. Kelley, S. Komanduri, M. L. Mazurek, *et al.*, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Proceedings of IEEE Symposium on Security and Privacy*, 2012.

[11] R. S. Kobsa, G. Tsudik, E. Uzun, and Y. Wang, "Serial hookups: A comparative usability study of secure device pairing methods," in *5th Symposium on Usable Privacy and Security (SOUPS'09)*, ACM, 2009.

[12] S. Komanduri, R. Shay, L. F. Cranor, C. Herley, and S. Schechter, "Telepathwords: Preventing weak passwords by reading users' minds," in *Proceedings of USENIX Security*, 2014.

[13] A. Kosse, "Do newspaper articles on card fraud affect debit card usage?," in *Conference on the Future of Retail Payments: Opportunities and Challenges*, No. 1389, Oct. 2011.

[14] I. A. Lami, T. Kuseler, H. Al-Assam, and S. Jassim, "LocBiometrics: Mobile phone based multi-factor biometric authentication with time and location assurance," in *Proceedins ogf 18th Telecommunications Forum*, IEEE TELFOR, 2010.

[15] K. Revett, *Behavioral Biometric A Remote Access Approach*, Wiley, UK, 2008.

[16] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest link' – A human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.

[17] M. F. Theofanos and S. L. Pfleeger, "Guest editors' introduction: Shouldn't all security be usable?," *IEEE Security and Privacy*, vol. 9, pp. 12–17, 2011.

[18] B. Ur, P. G. Kelly, S. Komanduri, J. Lee, M. Maass, M. Mazurek, T. Passaro, *et al.*, "How does your password measure up? The effect of strength meters on password creation," in *Proceedings of USENIX Security*, 2012.

[19] B. Ur, F. Noma, J. Bees, S. M. Segreti, *et al.*, "I added '!' at the end to make it secure: Observing password creation in the Lab," in *Proceedings of SOUPS*, 2015.
[20] D. Wheeler, *ZXCVBN: Realistic Password Strength Estimation*, 2012. (`https://blogs.dropbox.com/tech/2012/04/zxcvbnrealistic-password-strength-estimation/`)
[21] XMPP Foundation, *XMPP Standard*, June 21, 2011. (`http://xmpp.org/1`)
[22] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Survival of the shortest: A retrospective analysis of influencing factors on password composition," in *IFIP Conference on Human-Computer Interaction: Human-Computer Interaction (INTERACT'13)*, pp 460-467, 2013.

Biography

Muhammad Mustafa Nabi is studying Master of Cybersecurity at University of Sunderland UK in the School of Computer Science, Edinburgh Building, Chester Rd, Sunderland SR1 3SD, England. He has also received MSc degree in Information Technology from Preston University, Karachi, Pakistan. Interest: Cybersecurity & Networking.

Faisal Nabi is a PhD researcher at University of Southern Queensland. He has also received Honorary PhD in Computer Science from Brock University St. Catharine's, Ontario, Canada. Faisal's research interests are ecommerce security and software security.