I.J. Wireless and Microwave Technologies, **2021, 4, 11-19**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.04.02

Pattern-based and Time-Synchronised Passwords

Mian Saeed Akbar[1,*], Asif Khan[2], Sara[3]
[1] Department of Computer Science, University of Engineering and Technology Mardan, Pakistan
[2] Department of Computer Science, Virtual University of Pakistan
[3] Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan
Email: [1] miansaeedakbar@uetmardan.edu.pk, [2] khn4524@gmail.com, [3] sarakareem9182@gmail.com

Received: 15 June 2021; Revised: 01 July 2021; Accepted: 25 July 2021; Published: 08 August 2021

Abstract: World has been changed; every person is using a number of software, websites, and other systems that are using text-based passwords as a method of authentication. These passwords need to be strong, hard to guess, and need to be stored in a secure environment. Major problems with passwords are caused by human limitations to remember passwords for different accounts. A trade-off between password security and human-memorability made it difficult to create passwords that are strong enough and easy to remember. No satisfactory solutions have been offered to problems associated with a password such as shoulder surfing, eavesdropping, keylogging programs, Trojan horse, brute force attacks, etc. This study suggests a new easy to use approach for creating a password that is easy to remember even for a large number of accounts. Here in this paper, we proposed two methods one is pattern-based passwords, a simple method that is solving the problem of memorability, another is the idea of Time-Synchronized Passwords (TSP), a novel method for creating passwords that are dynamic in nature and change with the passage of time. The novality of TSP is that instead of storing the passwords in database the patterns are stored, and these patterns are related linked with time. The significance of storing pattern instead of actual password is that at a specific time, the password will have only one instance known to the creator of the password, and this particular instance will be different from instances at other times and thus avoids shoulder surfing, eavesdropping, keylogging, and other problems associated with passwords. These methods are easy to implement and can be used in any system.

Index Terms: Pattern-based Passwords, Time-Synchronised Password (TSP), Password Memorability, Password Security.

1. Introduction

Every digital system that stores, communicate or processes information needs to be secure. Authentication needs to be done when accessing some useful resource for which passwords are the best, easy to use, and traditional choices to verify authenticity. Although, a password is the oldest mostly used method, possesses some drawbacks. Different alternative methods have been devised to replace text-based passwords including graphical password authentication, location-based authentication, and gesture-based authentication [1, 2, 3]. These methods of authentication look very strong but due to the natural user-friendly behavior of text-based passwords, no method overcomes the use of text-based passwords [4]. Traditional password authentication methods are the most dominant methods nowadays in the web and will be in the near future [5]. Traditional passwords need to be restricted in different aspects. Some methods recommend that passwords should not be short, should not match dictionary wordings, and should be changed frequently [6, 7]. Some suggest that a good password is one that has both upper and lower case letters, digits, special characters and should be easy to remember [8]. In [9] the author suggested that the password should not be the name of a friend/relative, or a dictionary word. These restrictions on passwords make their usability problematic. Wiedenbeck et al. [6] suggested that a good password should be easy to remember and hard to guess. Although, the passwords which are easy to remember are generally name of the person or friends name or dictionary words which are recommended not to use because these passwords can be easily cracked using a dictionary attack or easily guessable by people as personal information are known to others. On the other side, strong passwords are hard to remember, which ultimately leads to these problems of selecting weak passwords. These problems are called human factor problems [10].

Most of the time the people are aware of using strong passwords but they need few guidelines. Various websites provide guidelines and advice but most users ignore these guidelines and consequently choose weak passwords. Research shows that users commonly underestimate the risk associated with weak passwords [11, 12]. It is a good idea to warn users about the risk. So, more effective approaches are required to persuade users to adopt a secure manner in the password authentication domain. Rather than only telling them why they should choose strong passwords or restricting their choices with tedious password policy rules, showing how to create better passwords in efficient and fun ways is more convenient [13]. Password theft is also an important issue to be considered. Passwords can be stolen through social engineering, brute force, keylogging, and other methods. The organization of the system, on one hand, needs to encourage the users to keep strong passwords while on other hand need to devise mechanisms to prevent passwords from stealing. This is a great challenge. There exist softwares that store every key entered. These malicious softwares exist in the form of malware or trojan horse that sends back all the punched keys to its owner. Even if a user creates a very strong password but due to these keylogging programs the strong password has no meaning.

One main problem with password security is the memorability of different passwords. Every person is using different websites, mobile applications, ATMs, online banking accounts, and other systems that used passwords as a primary method of authentication. Memorizing passwords for all these accounts and systems is difficult for human and leads to some serious problems i.e. some people use a single password for multiple accounts, some write down their passwords and keep easy to remember passwords such as the name of friends or family or dictionary words which are not recommended. As described above human factors contribute a lot to creating strong passwords. In this paper, we briefly discussed the password creating policies recommended by different researchers in the password authentication domain. After that, we introduced a novel method for creating passwords which do not require human to remember strong password instead to create a pattern and remember that pattern.

One objectives of this research is to propose an easy to use methods that avaoid the problem of memorability while keeping the security of the password strong. Till date all the researchers who tried to increase password memorability decreased the password security. While those who tries to increase the password security decreased the memorability. In coming sections we are going to introduce the idea of pattern-based passwords which increases the password mamorabilty while keeping the security strong. Another main objective of this research is to propose a novel method for storing passwords in database. This method will actually store pattern instead of the passwords. The pattern are based on time, and at each instance of time the pattern will produce a distinct password which will avoid lots of problems associated with the storage, transfer and security of passwords.

The rest of the paper is organized as follows. In the next section, we discuss the background and some literature reviews. In section 3 we introduce the idea pattern-based password that overcomes the problem of memorability of a number of passwords. In section 4 we introduce the idea of Time Synchronise Passwords to avoid lots of problems and associated security issues for password creation, transfer, and storage. Finally, we conclude in section 5.

2. Background and Related Work

To increase password security strength, the users are normally required to have a set of rules which are known as guidelines for creating strong passwords. This will motivate the users to create strong and non-guessable passwords which will be difficult to crack using a dictionary attack. For example, the password must be 8 characters long and must contain a capital letter and small letter, a number, and some special characters and should not be the name of a user. Rules like these are used by organizations to make passwords as secure as possible [14, 10].

According to a study, a user has on average 25 online password-required accounts and uses eight passwords per day [15]. For a user to remember different passwords for different accounts it is extremely complex and human cannot remember all these passwords. as a result, the users use the same password for more than one account which is extremely vulnerable and ultimately undermine the security of the systems they are using. Various techniques have been adopted to replace this infelicitous behavior with appropriately suitable behavior for authentication [16]. These techniques aim to make user behavior by implementing strict password creation guidelines [17], proactive password checkers [18], or password expiry [19], to ensure a high-security level. Along with these, password management systems such as features in web browsers are used nowadays. These systems save different passwords along with usernames and websites, work as a solution to the problem of memorability but are also troublesome because if someone accesses the password management system he will get access to all passwords. Study shows that users do not like strict constraints and are more attracted by these type of weak and insecure methods because these avoid constraints from the users and provide easy to use environments [20, 21]. This study shows that the current text-base password policies are not able to resolve the socio-technical authentication problem and will be abandoned in the future [22]. Thus it is ineluctable to devise text-based authentication schemes that avoid these socio-technical problems.

Previous studies showed that strict password policy rules did not increase password security [17, 23, 10]. As stated previously that users cannot remember strong passwords, if they are forced to use strong policies then they wrote down these passwords which in turn makes the system policies unbeneficial. Grawmeyer and Johnson [24] conducted a study to scrutinize users' password generation behavior. All the passwords estimated as highly secure and secure in the study were in fact insecure passwords containing a single word. Therefore, the authors suggested that password guidelines contained in security policies should be devised and founded on a sufficient theoretical understanding of the users' task. In 2006, the National Institute of Standards and Technology (NIST) updated the “Electronic Authentication Guideline” [25] to be used by security system administrators for the implementation of electronic authentication. This guideline provides heuristics to measure the strength and efficiency of a password restriction policy considering bits of entropy to determine a password value's uncertainty. In this guideline, the estimation of Shannon's Entropy [26] was used for the entropy calculation. However, several studies [27, 28, 23, 29] have found that passwords created with particular password policies were more difficult to guess than the ones created with the NIST model suggestions [13].

Komanduri et al. [23] performed a large web-based study for the comparison of four different types of password creation policies. They found that passwords with a minimum of 16 characters provide the best security as compare to passwords with a minimum of 8 characters. They also found that users have less difficulty complying with creating 16 characters minimum password compared to 8 characters. Some researchers have claimed that password restriction policies do not improve password security [30]. There have been some laboratory [31] and field studies [32] conducted to test this claim. Results showed that when users are restricted to create strong passwords using some guidelines then they cannot remember these passwords. These password security policies also provide guidelines for crackers to guess the passwords more efficiently. Florencio and Herley [33] found in their web-based study that users only accept restriction policies if they have no other choice. The authors added that websites that typically users do not care too much in the creation of strong passwords are normally the most popular and most likely to be attacked because they possess lots of assets for hackers. If these websites impose strong password creation policies, then their security will be increased but usability will be decreased.

In 2017 NIST updated its guidelines, they highlighted that strict password creation rules are useless [34]. They recommended the organizations not to force the user to apply these rules anymore, also it is stated that the strength of the password is mostly affected by its length, so it is recommended to use long passwords. There is a trade-off between password security and usability. The most secure passwords are the more difficult to create and use due to the problem of memorability users either forget the password or write them down when they are forced to create strong, complex, and random passwords. On the other hand, simple and easy to remember passwords are susceptible to attacks. It seems more secure passwords mean less usable passwords or vice versa [35]. Some researchers investigated the relationship between password security and usability by conducting several studies [36]. The most important problem that affects the usability of strong passwords is memorability. Many studies stated that users face difficulty in remembering passwords [30]. Users typically follow copying strategies to avoid forgetting and resetting passwords. Vu et al. [31] conducted a memorability of text password tests. The passwords were generated using various password policy rules. They found that remembering five passwords are more difficult than remembering three passwords. Also, users follow some mechanisms to assist in memorizing passwords that are connected to the accounts. Chiasson et al. [37] conducted a study composed of both textbase passwords and graphical passwords. They found that passwords created graphically are easier to remember than text-based passwords. Chanda. K [38] in her paper designed a password strength checker that scores the user-entered password against a number of factors and returns the score along with the classification of `weak`, `fair`, 'strong`, and `invalid`. The author performed an analysis of various popular websites and concluded that flipkart.com has the least password security. The strongest rules enforced are by ebay.com followed by hotmail.com. Their restrictions force users to set passwords that are naturally hard to brute force.

These different researchers tried to increase the password security but on the other hand side the complexity of the password also increased. Some of them tried to avoid the problem of memorability but again these research shows that increasing mamorabiltiy in these ways decreases the password security. We aim to propose the methods which increase memorability as well as security of the passwords. In the next sections, we proposed solutions to the problem of memorability associated with text-based passwords and their security.

3. Pattern-based Passwords

Ways of existence in the world have been completely changed by the Internet. It has reshaped communications, and everyone prefers the Internet to be the medium for communication. Internet helps us in almost everything. We order food, buy products, share moments with relatives and friends, send images in instant messaging over the Internet. Before this revolution, if we wanted to keep updated on the news we needed to wait on the news stand for the news agent in the morning and buy a newspaper that reports what has happened in the day past. But due to the Internet today with a single click or two, we can read any newspaper and get any news from anywhere in the world and get updates up to the minute.

On the other way, the mobile application turned our existence up-down. We indeed wake up and thanks to the alarm app, manage our finances through mobile banking apps, get updates of our friends using social apps and do each activity of our daily lives using different apps. We use mobile apps so often that we use them without even thinking about them, a lot like breathing. Using different websites and different mobile apps has become part of our lives and our accounts in these websites and mobile apps are invaluable for us and need proper privacy and security. Most of the mobile apps nowadays use biometric security but these use password security as the first choice because biometric security has its own complications. While almost all websites used text-based password security for user accounts. According to a study, a user has on average 25 online password-required accounts and uses eight passwords per day [11]. As said before for a user to remember 25 different passwords for different accounts, is extremely complex and human beings cannot remember so many passwords, as a result, the users use a single password for more than one account which is extremely vulnerable and ultimately undermine the security of the systems they are using. Here we propose an efficient solution to this problem.

The proposed idea is to use pattern-based passwords. In this case, a person using different accounts needs to remember a single pattern instead of remembering lots of passwords for different websites and mobile apps. The pattern is chosen in such a way that for each account or mobile app the pattern produces a unique password. The pattern will include different number of parts depending from user to user. A user may generates a pattern having two parts or more. One or more part(s) of the pattern will be constant i.e. this/these part(s) will be the same for all accounts passwords. While the other part(s) of the password will vary depending on the websites, mobile apps or the system underuse. These are the information taken from the website title or website domain or some other information related to the website, mobile app, or the system that works as a clue and will be visible to the user at any time when he/she enters the password.

For instance, a person named `abc xyz' who has accounts in Facebook, Google, Yahoo, Bank account, University portal account, etc. and let the person use a very simple pattern as his name and then the last character of the domain name. He created the pattern for his passwords as

- First name
- Then @ the last character of the domain name in capital letters
- Then skip the first character in the last name
- Then $ first character of the domain name in small letters
- Then number of characters in the first word of the website title

According to this pattern his password for:

- Facebook is abc@Kyz$f8
- Google is abc@Eyz$g6
- Yahoo is abc@Oyz$y5
- Bank account is abc@Kyz$b4
- University portal is abc@Yyz$u10

So the user has to remember only this pattern and even if he has thousands of accounts in different websites or mobile apps he cannot forget his password in this way as it is easy to memorize the pattern only, this is the great beauty of pattern-based passwords. In all these passwords we see that there exist at least one digit, at least one special character, capital letter, small letter and hence follow almost all of the rules recommended by the researcher to create strong passwords. The user can add special characters to his pattern and at any position. The pattern is completely dependent on the will of the user. Each user will create the pattern in his own way and a major role in pattern creation is playing by the information from the title of the website or mobile app, or domain name, etc. and is not difficult to remember. Hence pattern-based passwords intelligently overcome the problem of memorization. Another benefit of pattern-based password is that the users will use a single pattern for different accounts and will need not to write it down and hence will excavate the security of the system they are using. Another advantage of pattern-based passwords is that all the existing systems can use them without modifying their security modules as it is dependent on the user side. What the website or mobile apps need to do is to display courteous messages that encourage the users to devise such patterns for their passwords.

4. Time-Synchronised Passwords (TSPs)

As discussed before almost every person in this world is using the Internet and mobile applications as a result the person is accessible to the whole world in which there exist lots of guys with bad intentions. It is enough to consider user name/id and password to protect the information, data, computer account from praying eyes. But there exist some bad people who are continuously trying to get access to others' accounts, data, or computers. It is therefore important to make the password security strong and tight. As said before if we make so strong passwords that are not possible to guess but if our system is infected and contains some keylogging programs or malware then the strong password will have no meaning. To avoid situations like these i.e. to protect passwords from keylogging programs, social engineering, and brute force, we introduced the idea of time-synchronized passwords.

Time-synchronized passwords (TSPs) are the passwords created in such a way that the password changes with time. It is a modification to the salted password hashing technique. At a specific time, the password will exist in one form and at another time the password will change automatically while the owner/creator of the password will know the exact password at any given time. This method removes lots of problems associated with the storage and transfer of passwords such as keylogging programs, eavesdropping, writing down passwords, and shoulder surfing problem. Shoulder surfing problem is the situation when a user type password and someone is seeing him and notes the password. A Time-Synchronised Password is logically divided into two parts. Part one is the part of the password that is used as a normal password (NP), the second part is a hashed key obtained by hashing a time part (TP) with a salt. Both parts of the TSP including the method of hashing, TP, salt is decided by the owner of the password.

$$TSP = NP + TimeHashing(TP, salt) \tag{1}$$

In this equation, NP is the normal password, + is used for concatenation. TimeHashing is a function that returns a specific hashed key of a constant length that is unique for each TP, TP is the part of the time after which the password will change automatically. It can be a minute, an hour, a day, a month, a year. Salt is the additional parameter to the hash function that is also decided by the owner of the password. The System uses TSP need to convince the users to create their password in this way by providing user-friendly interfaces. The general work flow for creation TSP is as shown in fig.1(a) is:

1. Ask the user to enter password NP
2. Then ask to select an operation for hashing TP with salt
3. Then ask to choose a TP
4. Then ask to select salt

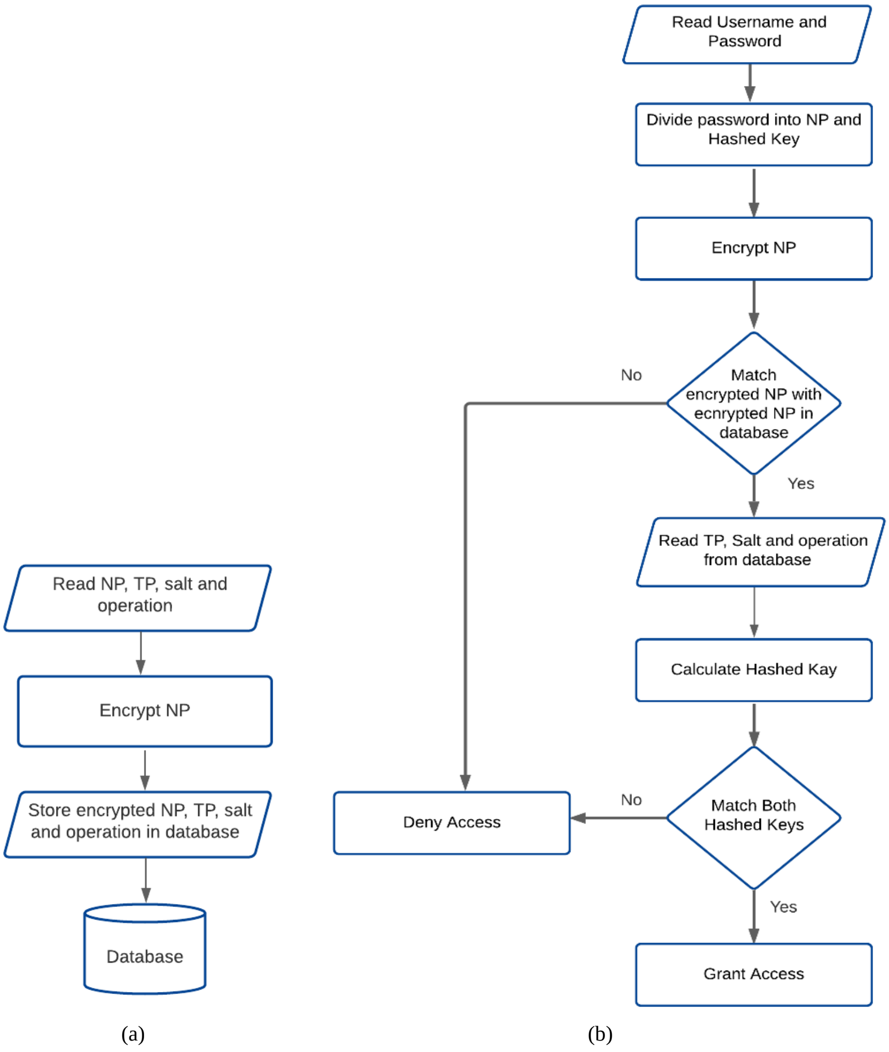
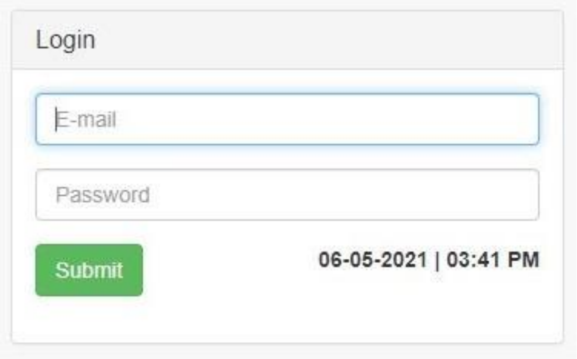

Read NP, TP, salt and operation
Encrypt NP
Store encrypted NP, TP, salt and operation in database
Database
(a)
Read Username and Password
Divide password into NP and Hashed Key
Encrypt NP
Match encrypted NP with ecnrypted NP in database
No
Yes
Read TP, Salt and operation from database
Calculate Hashed Kay
Match Both Hashed Keys
No
Yes
Deny Access
Grant Access
(b)

Fig. 1. TSP Creation and Checking

After submitting the above all parameters the system encrypts the NP using any of the known schemes i.e. MD5, SHA-1, SHA-2, SHA-3, SHA-256, SHA-512, RipeMD, WHIRLPOOL, etc. [39, 40]. And stores the encrypted NP, TP, and salt in the database. When the user logins to the system, the user knows the NP and TimeHashing function, enters NP, and hashed key at that specific time. The system performs the following steps as shown in fig.1(b):

1. Divides the entered password in NP and hashed key
2. Encrypts the NP and match it with the encrypted NP stored in the database
3. If a match occurs, then the system calculates hashed key from TP and salt stored in the database
4. The hashed key is generated and is matched with the hashed key part of the entered password
5. If a match occurs the user is granted access else access denied and the user gets the invalid username or password message.

For instance, a person named `abc xyz' is going to create a Time-Synchronised Password (TSP). He chooses the first part (NP) as his name i.e. abcxyz and the second part as TP = hour, salt = 3, and operation is multiply. The result is a hashed key that is concatenated with the first part and the result is stored as a password in the database. When the user logins to the system at a given time the user knows all the three parts of the password i.e. first part (NP) is his name and then the second part will be calculated as the current hour multiply by three as the user knows this. In this method the user password changes after each hour e.g. during 2:00 - 3:00 the hashed key is 6, during 3:00 - 4:00 the hashed key is 9, while during 11:00 - 12:00 the hashed key is 33. Using this mechanism, the password changes automatically and the owner of the password knows his exact password at any given time.



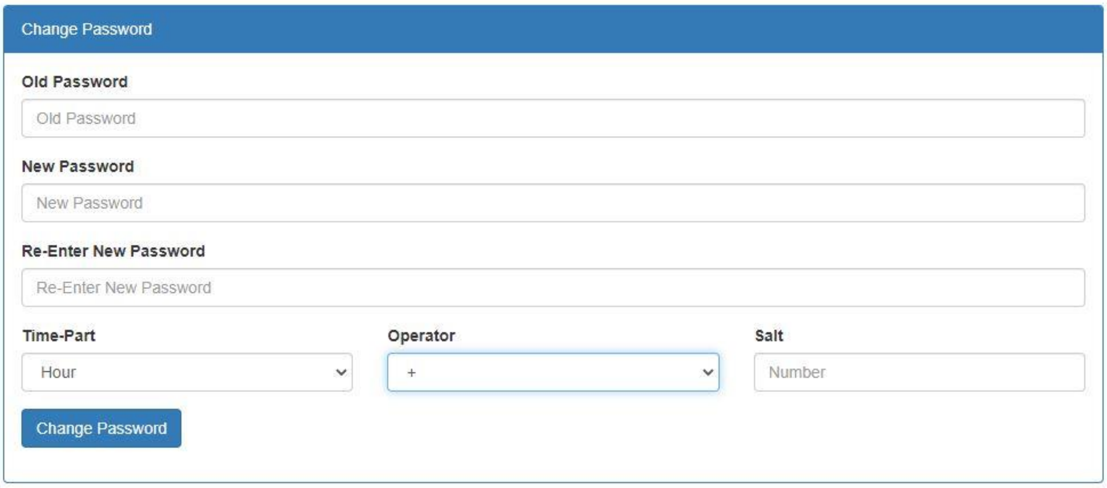
06-05-2021 | 03:41 PM

Fig. 2. Web Page showing TSP Login

We have implemented this idea in our website as shown in fig 2 and fig 3. Fig 4 and fig 5 show how TSP is stored in the database. The system using TSP must display the current time and date to users in order to evaluate their Hashed Key which is a part of the password. It is recommended to use such TP that changes frequently. TSP has overcome various problems associated with password security. First, it avoids shoulder surfing problems. During punching the password if someone is looking over the user's shoulder and notes down the password, the password will not work after its TP expires/passes. So it is highly recommended to use such TP that changes more frequently. In the same manner, if someone on the network catches the packet and reveals the password from the packet. The password caught will not work after its TP expires and hence provide a solution to minimize the problem of eavesdropping. It also minimizes the chances to get match using brute force attack. Consider and attacker started a brute force search for password and the password contain TP as minute, so after each minute the password will change and has a great chance not to be detected by the brute force search. In a similar way if someone's computer is infected that note down every punched key and then after some time sent these keys to its creator. When the creator gets the saved password the TP of the password saved will be expired and will not work. Hence in this way, TSP avoids lots of problems associated with password security.

5. Results and Discussion

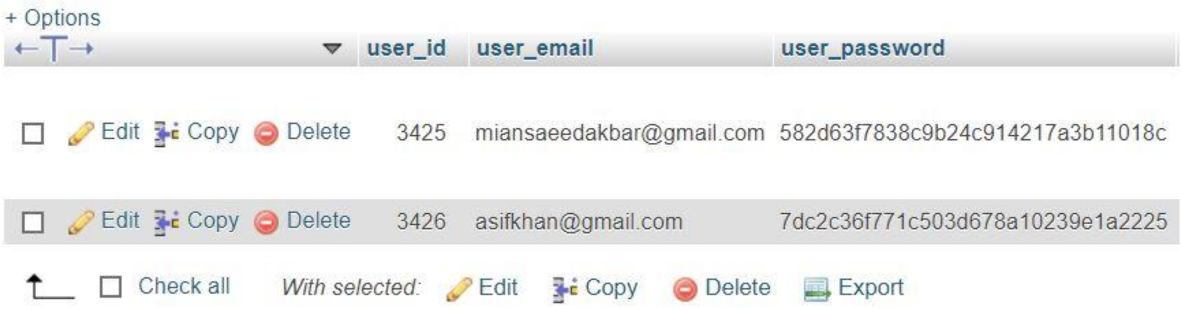
The need for this research was felt because of it was difficult to memorize multiple account passwords. All existing methods restricts users to use strong passwords which are not easy to remember. On the other hand if the users



Time-Part
Hour

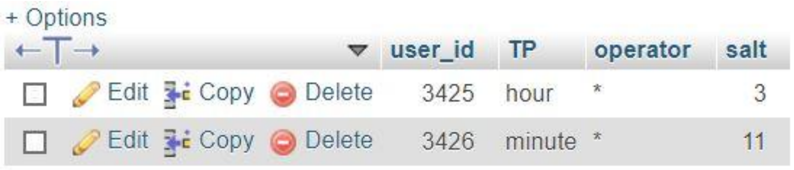
Operator
+

Fig. 3. Web Pages showing Changing TSP



	user_id	user_email	user_password
□	3425	miansaeedakbar@gmail.com	582d63f7838c9b24c914217a3b11018c
□	3426	asifkhan@gmail.com	7dc2c36f771c503d678a10239e1a2225

Fig. 4. Storing NP in Database



	user_id	TP	operator	salt
□	3425	hour	*	3
□	3426	minute	*	11

Fig. 5. Storing TP, Operator and salt in Database

use easy to remember password they are highly vulnerable to be catch by some one. Hence this papers resolve these problems upto a greate extent. Time-Synchronised passwords are actually patter-based passwords but these are dynamic pattern-based. In simple pattern-based password we existing systems do not need to be updated but the users shoud be advised to use password for different account in a pattern manner. While on the other hand in TSP the system database structure needs to be updated to accommodate the storage of pattern instead of single hashed strings of passwords as shown in fig.4 and fig.5.

6. Conclusion and Further Research

Although the use of a password as a means of authentication has been extensively studied in the past. No one in the previous research encouraged users to create easy-to-remember passwords because of its trade-off with security. One of the main contributions of this paper is presented in the form of pattern-based passwords that encourages users to create passwords that are easy to remember and contain a pattern, as a result, the user needs to remember only the pattern. In this way, a single user can remember hundreds and even thousands of passwords for different websites / accounts / mobile applications / systems. So this is one main contribution of this research that provides an easy way to use pattern-based passwords for a number of applications and hence avoid the problem of memorability.

One another main contribution of the paper is the idea of Time-Synchronised passwords. This provides a dynamic behavior to use passwords that changes with time automatically and as a result, avoid lots of problems associated with password security as mentioned by various researchers before. This method is very effective since that it is very simple to implement and easy to understand. The implementation of TSP requires that the back-end of the existing system should be modified to accommodate TSP logic while the front end of the system should be modified to advise the users to create TSPs.

So far, the main two ideas discussed in this paper are easy to implement. These techniques can be used in any type of website, mobile apps, or system to provide security to its users. This will make any kind of data more secure. TSPs can be further investigated to make their behavior more dynamic and encrypt all its parts like NP.

References

[1] A. Forget, A world with many authentication schemes, Ph.D. thesis, Carleton University, 2013.

[2] J. Goldberg, J. Hagman, V. Sazawal, Doodling our way to better authentication, in: CHI'02 extended abstracts on Human factors in computing systems, pp. 868-869.

[3] J. Thorpe, B. MacRae, A. Salehi-Abari, Usability and security evaluation of geopass: A geographic location-password scheme, in: Proceedings of the Ninth symposium on usable privacy and security, pp.1-14.

[4] J. Bonneau, C. Herley, P. C. Van Oorschot, F. Stajano, The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, in: 2012 IEEE Symposium on Security and Privacy, IEEE, pp. 553-567.

[5] C. Herley, P. C. Van Oorschot, A. S. Patrick, Passwords: If we're so smart, why are we still using them?, in: International Conference on Financial Cryptography and Data Security, Springer, pp. 230-237.

[6] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, N. Memon, Authentication using graphical passwords: E_ects of tolerance and image choice, in: Proceedings of the 2005 symposium on Usable privacy and security, pp. 1-12.

[7] E. F. Gehringer, Choosing passwords: security and human factors, in: IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293), IEEE, pp. 369-373.14

[8] S. Gar_nkel, G. Spa_ord, Practical UNIX security, O'Reilly & Associates, Inc., 1991.J. Yan, A. Blackwell, R. Anderson, A. Grant, Password memorability and security: Empirical results, IEEE Security & privacy 2 (2004) 25-31.

[9] W. C. Summers, E. Bosworth, Password policy: the good, the bad, and the ugly, in: Proceedings of the winter international synposium on Information and communication technologies, pp. 1-6.

[10] D. Florencio, C. Herley, A large-scale study of web password habits, in: Proceedings of the 16th international conference on World Wide Web, pp. 657-666.

[11] L. Zhang, W. C. McDowell, Am i really at risk? determinants of online users' intentions to use strong passwords, Journal of Internet Commerce 8 (2009) 180-197.

[12] M. Shahid, M. A. Qadeer, Novel scheme for securing passwords, in: 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, IEEE, pp. 223-227.

[13] D. Choi, S. Jin, H. Yoon, A user friendly internet identity management system, in: 2008 10th International Conference on Advanced Communication Technology, volume 2, IEEE, pp. 1163-1166.

[14] E.-J. Yoon, K.-Y. Yoo, Breaking a smart card based secure password authentication scheme, in: 2008 International Conference on Information Security and Assurance (isa 2008), IEEE, pp. 83-86.

[15] D. Wood, J. S. Bruner, G. Ross, The role of tutoring in problem solving, Journal of child psychology and psychiatry 17 (1976) 89-100.

[16] P. G. Inglesant, M. A. Sasse, The true cost of unusable password policies: password use in the wild, in: Proceedings of the sigchi conference on human factors in computing systems, pp. 383-392.

[17] J. J. Yan, A note on proactive password checking, in: Proceedings of the 2001 workshop on New security paradigms, pp. 127-135.15

[18] Y. Zhang, F. Monrose, M. K. Reiter, The security of modern password expiration: An algorithmic framework and empirical analysis, in: Proceedings of the 17th ACM conference on Computer and communications security, pp. 176-186.

[19] R. W. Proctor, M.-C. Lien, K.-P. L. Vu, E. E. Schultz, G. Salvendy, Improving computer security for authentication of users: Inuence of proactive password restrictions, Behavior Research Methods, Instruments, & Computers 34 (2002) 163-169.

[20] J. Roig, Do smarter people have better passwords?, arXiv preprint arXiv:1805.02931 (2018).

[21] M. Kotadia, Gates predicts death of the password, CNET News, February 25 (2004).

[22] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, Of passwords and people: measuring the e_ect of password-composition policies, in: Proceedings of the sigchi conference on human factors in computing systems, pp. 2595-2604.

[23] B. Grawemeyer, H. Johnson, Using and managing multiple passwords: A week to a view, Interacting with computers 23 (2011) 256-267.

[24] W. E. Burr, D. F. Dodson, W. T. Polk, et al., Electronic authentication guideline, Citeseer, 2006.

[25] C. E. Shannon, Prediction and entropy of printed english, Bell system technical journal 30 (1951) 50-64.

[26] C. Castelluccia, M. Du rmuth, D. Perito, Adaptive password-strength meters from markov models., in: NDSS.

[27] L. S. Clair, L. Johansen, W. Enck, M. Pirretti, P. Traynor, P. McDaniel, T. Jaeger, Password exhaustion: Predicting the end of password usefulness, in: International Conference on Information Systems Security, Springer, pp. 37-55.

[28] M.Weir, S. Aggarwal, M. Collins, H. Stern, Testing metrics for password creation policies by attacking large sets of revealed passwords, in: Proceedings of the 17th ACM conference on Computer and communications security, pp. 162-175.

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

[30] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, J. Cook, E. E. Schultz, Improving password security and memorability to protect personal and organizational information, international journal of human-computer studies 65 (2007) 744-757.

[31] M. Keith, B. Shao, P. J. Steinbart, The usability of passphrases for authentication: An empirical _eld study, International journal of human computer studies 65 (2007) 17-28.

[32] D. Flor^encio, C. Herley, Where do security policies come from?, in: Proceedings of the Sixth Symposium on Usable Privacy and Security, pp. 1-14.

[33] P. A. Grassi, M. E. Garcia, J. L. Fenton, Digital identity guidelines (), NIST special publication 800 (2017) 63-3.

[34] M. Ciampa, A comparison of password feedback mechanisms and their impact on password entropy, Information Management & Computer Security (2013).

[35] M. Hub, J. Capek, R. Myskova, Relationship between security and usability-authentication case study, Int. J. Comput. Commun 5 (2011) 1-9.

[36] S. Chiasson, A. Forget, E. Stobert, P. C. Van Oorschot, R. Biddle, Multiple password interference in text passwords and click-based graphical passwords, in: Proceedings of the 16th ACM conference on Computer and communications security, pp. 500{511.

[37] K. Chanda, Password security: an analysis of password strengths and vulnerabilities, International Journal of Computer Network and Information Security 8 (2016) 23.

[38] P. Sriramya, R. Karthika, Providing password security by salted password hashing using bcrypt algorithm, ARPN journal of engineering and applied sciences 10 (2015) 5551-5556.

[39] Al-Hammadi, Yousef Ali and Fadl, Mohamed Fadl Idris, Reducing hash function complexity: MD5 and SHA-1 as Examples, IJ Mathematical Sciences and Computing, 5 (2019) 1-17

[40] shi2012scheme, A Scheme of IBE Key Issuing Protocol Based on Identity-password Pair, International Journal of Engineering and Manufacturing, 2 (2012).

Authors' Profiles

Mian Saeed Akbar has got his MS degree from Institute of Management Sciences Peshawar in the filed of Computer Sciece. His research interest includes Web Security Graph Theory, Machine Learning, Web Sciences, Information Science and Information Security.

Mr. Asif Khan is currently enrolled at VU Pakistan. His qualifications are as mentioned. ADP.(Computer Science.), M.Sc(Electronics), Diploma.(Information Technology.). He has 5 years of teaching experience and his areas of interest include Cybersecurity, Ethical Hacking, Electronics (Hardware Based Programming).

Sara is a Ph.D student enrolled currently at Abdul Wali Khan University Mardan. She has got his MS degree from Sharhad University of Science and Technology. Her reseach intersest includes Web Security, Interner of Things and machine learning.

How to cite this paper: Mian Saeed Akbar, Asif Khan, Sara, " Pattern-based and Time-Synchronised Passwords", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.4, pp. 11-19, 2021.DOI: 10.5815/ijwmt.2021.04.02