A Survey on Password Authentication Techniques

Ms.K.Usha Rani[1], Mrs.P.Rajeswari[2]
[1]Dept of Computer Science
[2]Assist.Professor,Dept of Computer Science,
[1, 2] Cauvery College for Women, Bharathidhasan University, Trichy, Tamil Nadu(India)

Abstract- *Nowadays, user authentication is an important topic in the field of information security. To enforce security of information, passwords were introduced. Text based password is a accepted authentication method used from early times. However text based passwords are flat to different attacks such as dictionary attacks, guessing attacks, brute force attacks, social engineering attacks etc. A password authentication schemes have been proposed so far as it recovers password usability and security. In this paper, we conduct a comprehensive survey of the existing password techniques. This survey will be particularly useful for researchers who are interested in developing new password Authentication techniques as well as industry practitioners who are interested in deploying password techniques.*

Keywords- Password, Authentication, attacks.

I. INTRODUCTION

In recent years, information security has been formulated as an important problem. Main area of information security is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method. A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and those wishing to gain access are tested and are granted or denied the access based on the password according to that. Passwords are used from ancient times itself as the unique code to detect the malicious users. In modern times, passwords are used to limit access to protect computer operating systems, mobile phones, and others.

A computer user may need passwords for many uses such as log in to personal accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc. Normal passwords have some drawbacks such as hacked password, forgetting password and stolen password. Therefore, strong authentication is needed to secure all our applications. Conventional passwords have been used for authentication but they are known to have problems in usability and security. Recent days, another method such as graphical authentication is introduced. Graphical password has been proposed as a different to alphanumeric password. Psychological studies have exposed that people can remember images better than text. Images are normally easier to be remembered than alphabets and numbers, particularly photos, which are even easier to be remembered than random picture.

II. RELATED WORK

Yang, [1] scrutinized the security requirements of smart-card-based password authentication schemes. They proposed a new scheme with a generic construction framework for smart-card-based password authentication and showed that a secure password based key exchange protocol can be efficiently transformed to a smartcard-based password authentication scheme provided that there exist pseudorandom functions and target collision resistant hash functions. They defined a set of desirable properties for secure smartcard-based password authentication schemes. The constructed secure two-factor framework smart-card-based password mutual authentication scheme transforms a proven secure one-factor password based mutual authentication protocol with pseudorandom functions and target collision resistant hash functions.

Gong [2] suggested a novel one-time Password (OTP) mutual authentication scheme based on challenge/response mechanisms. Their scheme used random sub-passwords and their corresponding hashes to be shared between the user and a server vice versa. The proposed scheme provided a robust and efficient OTP mutual authentication Calculation cost is low and resist for many attacks. But the scheme can only be applicable for ordinary applications and the work is so complex and hard to implement.

Zuo [3] criticized the weaknesses found in the existing password schemes SUN and LI and Suggested some solutions to avoid similar mistakes in future works. They also motivated to design more secure enhanced schemes. The system effectively identified the problems of the existing schemes. This paper reviewed the problems identified with two schemes. No new invention has taken place.

Bang [4] addressed the vulnerability of login credentials and also suggested a vulnerability measure of an individual's login credentials for analyzing the vulnerability of current Internet users. The obtained results are valuable not only to the research community but also to managers and policy makers striving to reduce security vulnerability. This work does not discussed the characteristics of individual login credentials determinants of Internet users' UID–PWD usages patterns need to be addressed more.

Nelson [5] conducted an experiment where the participants in this study were assigned to select one of three password generation groups: PPC(Proactive Password Checking) restrictions alone, image-based mnemonic, or text-based mnemonic to assess the vulnerability of password cracking. The participants were individually tested by

1. By assigning to the image-based mnemonic group.
2. Verbally informed mnemonic group.
3. Assigned PPC passwords.

The results were then analyzed and discussed in this paper. The image-based mnemonic technique was shown to be the most effective method for generating secure and memorable passwords. The use of mnemonic techniques resulted in the generation of longer, more complex and crack-resistant passwords as compared to those participants who only used the PPC restrictions. Passwords generated using PPC limitations alone were more simply beyond and susceptible to being cracked.

Cheong [6] offered a secure two-factor authentication Near Field Communication Smartphone access control system using digital key and proposed Encrypted Steganography Graphical Password (ESGP) validated the user view and behavioral purpose to use NFC ESGP Smartphone access control system during an experiment and user evaluation survey.

Their goal is to propose a new system to enhance the security of access control system without imposing undue technological efforts and inconvenience. Results specified that users weigh security as a leading attribute for their behavioral purpose to use NFC ESGP Smartphone access control system. Their findings offer a new insight for security scholars, mobile device service providers and expert systems to leverage on the two-factor authentication with the use of NFC-enabled Smartphone. The security and convenient level based on their personal preferences is to be determined. Requirements of the system went beyond the limits.

Vu [7] study evaluated the time and number of attempts needed to generate unique passwords satisfying different restrictions for multiple accounts, as well as the login time and accuracy for recalling those passwords. Recommendations for enhancing password security and memorability

1. There should be minimum length restriction
2. Inclusion of special characters and increase the security of passwords
3. Avoid using simple patterns
4. First letter sentence generation technique improve memory of passwords
5. Administrators should use a lock-out procedures after a certain number of attempts
6. Engaging user to login multiple times after generating the password will increase the memorability

The use of a technique for which the first letter of each word of a sentence was used and coupled with a requirement to insert a special character and digit that yielded more secure passwords those were more memorable. There need to be methods that help participants remember which passwords are associated with which accounts, for instance, making the participants generate sentences that they associate with the account they are trying to access

Duggan [8] designed security policy, task models of password behavior for different user groups—Computer Scientists, Administrative Staff and Students. Modeling revealed Computer Scientists viewed information security as part of their tasks and passwords provided away of completing their work. By contrast, Admin and Student groups viewed passwords as a cost incurred when accessing the primary task. This approach was to combine a diary study of password authentications with a debrief interview for each password used. In addition, one randomly selected participant from each group individually collaborated with model building. This combination of methods enabled detailed recording of in situ behaviour along with a more elaborate understanding of the individual passwords themselves and the rationale behind their selection. The diaries were used both to provide information about participant behaviour and as a prompt for the debrief interviews around each password. The recommendations suggested by the author are flexible and rely on the expertise of the security officer implementing them. The sample size of the dataset was not large and this limits the generalizability of the findings.

Wang [9] investigated two recent proposals in the area of smart-card-based password authentication for security-critical real-time data access applications in hierarchical

wireless sensor networks (HWSN). The two schemes were equipped with a claimed proof of security. They proposed lightweight operations, such as one-way hash functions and exclusive OR operations. They also pointed out that both protocols have various security flaws being overlooked. Provided a better understanding of the security challenges in designing two-factor user authentication schemes for HWSN, and may constitute a useful guidance to promote further development of more practical schemes. Public-key techniques are indispensable to resist against user anonymity violation attack under the non-tamper resistance assumption of the smart cards, finding/constructing a counter-example to this conjecture should be motivated.

Huang [10] proposed TSOTP(Time Stamp One Time Password) a new effective simple OTP method that generates a unique pass code for each use, since One-Time Passwords can provide complete protection of the login-time authentication mechanism against replay attacks. The calculation used both time stamps and sequence numbers. Simple one-pass authentication message exchange, no need for a third party, low computation cost and no cost for proprietary tokens using a mobile phone as the OTPs generator has the vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks.

Xie et al, [11] demonstrate that the protocol cannot resist impersonation attack and off-line password guessing attack. To overcome their security weaknesses, They proposed an improved chaotic maps-based 3PAKE protocol with the same advantages. Further, he applied the pi calculus-based formal verification tool ProVerif to show that the proposed 3PAKE protocol achieves authentication and security.

Farash et al. [12] showed that scheme is vulnerable to off-line password guessing attack, user impersonation attack and server impersonation attack, in the case that the smart card is stolen and the information stored in the smart card is disclosed. They proposed an improved smart card-based authentication scheme which not only conquers the security weaknesses of the related schemes but also provides a reduction in computational cost. This scheme provides the user anonymity and intractability, and allows a user to change his/her password without informing the remote server.

Zhang et al [13] pointed out that Mishra et al.'s scheme suffers from replay attacks; main in the middle attacks and fails to provide perfect forward secrecy. To defeat the weaknesses of this scheme, they proposed a three-factor authenticated key agreement scheme to allow the patient to enjoy the remote healthcare services via TMIS with privacy protection.

TABLE 1 Password Techniques comparison

S.No	Algorithm	Objective	Metrics	Protocol used	Demetrics
1	Two-factor mutual authentication based on smart cards and passwords.	The core feature of such a scheme is to enforce two-factor authentication in the sense that the client must have the smart-card and know the password in order to gain access to the server.	The constructed framework appears with provable security	A secure password based key exchange protocol	They showed that a proposed scheme does not satisfy some of the properties and some of their security claims are incorrect
2	A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords	A novel one-time password (OTP) mutual authentication scheme based on challenge/response mechanisms.	Robust and efficient OTP mutual authentication Calculation cost is low and resist for many attacks	Novel one-time password (OTP) mutual authentication scheme	Only be applicable for ordinary applications and the work is so complex and hard to implement
3	Improvements of Jung's password-authenticated key agreement scheme using smart cards	Inability of the password-changing operation; the session-key problem; and inefficiency of the double secret keys	The system effectively identified the problems of the existing schemes.	A password-authenticated key agreement scheme	Problems identified with two schemes. No new invention has taken place

4	Improving information security management: An analysis of ID–password usage and a new login vulnerability measure	As the e-commerce volume is increasing and various online services are becoming more popular, the number of sites to which an average Internet user subscribes is increasing rapidly	Managers and policy makers striving to reduce security vulnerability.	A vulnerability measure of an individual's login credentials and analyze the vulnerability of current Internet users	This work does not discussed the characteristics of individual login credentials
5	Effects of a mnemonic technique on subsequent recall of assigned and self-generated passwords	The impact of self-generated passwords on memory was discussed as well as the relative value of the mnemonic training strategy.	The image-based mnemonic technique was shown to be the most effective method for generating secure and memorable passwords	Self-generated passwords on memory	Passwords generated using PPC restrictions alone were more easily forgotten and susceptible to being cracked
6	Secure encrypted steganography graphical password scheme for near field communication smartphone access control system	Integration of both credentials provides higher security to access control system.	Their findings offer a new insight for security scholars, mobile device service providers	Secure two-factor authentication NFC smartphone access control system	Requirements of the system went beyond the limits
7	Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords	A notoriously weak security method because users tend to generate passwords that are easy to remember but also easy to crack	The use of a technique for which the first letter of each word of a sentence was used	Improve security at little cost to memorability scheme	There need to be methods that help participants remember which passwords are associated
8	Rational security: Modelling everyday password use		The recommendations suggested by the author are flexible and rely on the expertise of the security officer implementing them	Security policy, task models of password behaviour	The sample size of the dataset was not large and this limits the generalizability of the findings.
9	On the (in) security of some smart-card-based password authentication schemes for WSN	Investigate a temporal-credential-based password authentication scheme	Provided a better understanding of the security challenges in designing two-factor user authentication schemes	A temporal-credential-based password authentication scheme	Public-key techniques are indispensable to resist against user anonymity violation attack under the non-tamper resistance
10	A new one-time password method	The design of security policy, task models of password behaviour were	Simple one-pass authentication message exchange	New effective simple OTP method	Using a mobile phone as the OTPs generator has the

		constructed for different user groups			vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks
11	Improvement of a chaotic maps-based three-party password authenticated key exchange protocol without using servers public key and smart card	That their protocol cannot resist impersonation attack and off-line password guessing attack	This protocol is more efficient than Farash and Attari's protocol in terms of computation and communication costs.	Three-party password-authenticated key exchange (3PAKE) protocol	This protocol allows two users to establish a secure session key over an insecure communication channel
12	Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography	The session initiation protocol (SIP) has been receiving a lot of attention to provide security.	To show the security of this protocol, they prove its security the random oracle model.	Smart card-based authentication scheme	Their scheme is not secure against known security attacks
13	Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme	Telecare medicine information systems are more vulnerable to various types of security threats and attacks	Performance evaluation shows that the proposed scheme increases efficiency in comparison with other related schemes.	A biometrics-based authenticated key agreement scheme	Security analysis demonstrates that the proposed scheme not resists various attacks and provides several attractive security properties

III. CONCLUSION

In this work, different algorithms from password authentication are reviewed and surveyed. A different authentication method is presented above. Many researches on password techniques have to be done to reach higher levels of helpfulness. During our research, we recognize some drawbacks which can cause attacks. Therefore, it can be concluded that the general drawbacks on these graphical password methods and how to defeat these attacks. Then, we tried to survey on attack patterns and define general attacks in password authentication methods. Finally we make a comparison table among various password authentication techniques based on attack patterns.

REFERENCES

[1] 93. Yang, G.M., Wong, D.S., Wang, H.X., Deng, X.T.: Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences 74(7), 1160–1172 (2008)

[2] Gong, Longyan, et al. "A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords." Journal of Computer and System Sciences 79.1 (2013): 122-130.

[3] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, and Z. Y. Feng, "Improvements of juang et al.'s password-authenticated key agreement scheme using smart cards," IEEE Transactions on Industrial Electronics, vol. 56, no. 6, pp. 2284-2291, 2009.

[4] Bang, Youngsok, et al. "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure." international journal of information management 32.5 (2012): 409-418.

[5] Nelson, Deborah L., and Kim-Phuong L. Vu. "Effects of a mnemonic technique on subsequent recall of assigned and self-generated passwords." Symposium on Human Interface. Springer, Berlin, Heidelberg, 2009.

[6] Cheong, Soon-Nyean, Huo-Chong Ling, and Pei-Lee Teh. "Secure encrypted steganography graphical password scheme for near field communication smartphone access control system." Expert Systems with Applications 41.7 (2014): 3561-3568.

[7] Vu, Kim-Phuong L., Abhilasha Bhargav, and Robert W. Proctor. "Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords." Proceedings of the human factors and ergonomics society annual meeting. Vol. 47. No. 11. Sage CA: Los Angeles,

CA: SAGE Publications, 2003.

[8] Duggan, Geoffrey B., Hilary Johnson, and Beate Grawemeyer. "Rational security: Modelling everyday password use." International journal of human-computer studies 70.6 (2012): 415-431.

[9] Wang, Ding, and Chunguang Ma. "On the (in) security of some smart-card-based password authentication schemes for WSN." IACR Cryptology ePrint Archive 2012 (2012): 581.

[10] Huang, Yun, Zheng Huang, Haoran Zhao, and Xuejia Lai. "A new one-time password method." IERI Procedia 4 (2013): 32-37.

[11] Xie, Q., Hu, B.,Wu, T. “Improvement of a chaotic maps-based three-party password authenticated key exchange protocol without using servers public key and smart card,” Nonlinear Dynamics, Vol. 79, No.4, pp. 2345–2358, 2015.

[12] Farash, M.S., Kumari, S., Bakhtiari, M. “Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography,” Multimedia Tools and Applications, Vol. 75, No.8, pp. 4485–4504, 2016.

[13] Zhang, L., Zhu, S., Tang, S., “Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme,” IEEE Journal of Biomedical and Health Informatics, 2017.