Various Approaches in Secure Password Authentication and Secondary Authentication Methods

Dr.Lalitha.R[1], Kamali.B[2]

Professor, Computer science, Rajalakshmi institute of technology, Chennai, India [1]
UG scholar, Computer science, Rajalakshmi institute of technology, Chennai, India[2]
lalitha.r@ritchennai.edu.in kamaliboji39@gmail.com

Abstract: A password is the main player in authenticating user accounts in multiple digital accounts like social media, banking websites etc., It mainly lets only the creator or user of that particular account to access and utilize the same. But password based security works on the assumption that only the user knows the password and also anyone who enters the wrong password is not the user. This might prove difficult in the event that the user picks a password that can be easily guessed or if the user forgets the password. This paper addresses the various methods to set secure passwords that overcome the above mentioned issues.

Keywords: Authentication, Cognitive Password, Graphical Passwords , Biometrics, Click pattern , Salts and Security

I. Introduction

Password Authentication works similar to locks and keys of the real world in digital platforms. It works on the principle that the authorised user is the only person with the knowledge of the password. This might prove to be highly inefficient since humans are prone to errors or forgetting the passwords. Long et all., [1] describes humans as the weakest link in most human-computer interactions. But this may not only factor affecting generic password authentication systems. Due to various technological advancements there are various new attacks that work on predicting the password or hack into the account protected by the password, fortunately a number of new techniques have emerged to counter these attacks. Also, when it comes to users forgetting their passwords, there are several secondary authentication methods that help the user regain access of the account. But these methods also become a liability if someone pretends to be the actual user who has forgotten the password. These secondary authentication methods highly rely on data that the user may easily recall and is only known by the user, it assumes the user has not made this information public knowledge which might not be true, for example the user may have posted on social media platforms, the name of his first pet. This data is accessible to any of his friends and can be misused. Lately, many methods have been proposed to overcome this issue.

This paper discusses the various password attacks in subdivision II, a survey on security measures to counter password attack in subdivision III and secondary authentication methods and their drawbacks in subdivision IV.

II. TYPES OF PASSWORD ATTACKS

A. *Brute force attack*

It is a method which uses a trial and error approach to find the password of an account.[11] Since the possibilities are endless even for an eight-character password, automated software’s which try out all possible combinations are used

B. *Shoulder surfing.*

It is basically looking over a user’s shoulder while they enter the password. This attack can be performed in both short and long range by using a pair of binoculars or a hidden camera and secret microphones. Using technology makes shoulder surfing much easier for the attackers to perform long range shoulder surfing.[12]

C. *Dictionary Attack*

Similar to brute force attack, this method tries to crack the password by using all the strings or words from a possible topic. The strings can be derived from available databases according to topic like sports database, music database etc., This method works on the assumption that the user selects a short text based password.

D. *Hybrid Password Guessing Attack*

A hybrid attack is a blend to both dictionary and brute force attack. This means that while dictionary attack would include a word list of passwords, the brute force attack would apply to each possible password in that list[8].

E. *Password Resetting*

This is a method that involves direct interaction between the attacker and the user[10]. The attacker creates a service that the user is persuaded to sign up. The details collected in this process is used by the attacker pretending to be the user who has forgotten the password, in the "forgot password" secondary authentication method to access the account[15].

F. *Password Cracking*

This is a process that utilises the data stored in and transmitted by the computer system.[14] These data can be obtained from the systems communication network, system cache, etc.,[16]

G. *Rainbow Tables.*

Hashed passwords are difficult to crack than plaintext passwords. Here rainbow tables are required to crack passwords.[17] A hash function maps plain text to hashes. the reduction function maps hashes to plain text. Hashes and reduction functions are one way functions. A Rainbow table is a precomputed table for reversing cryptographic hash functions.[19] The chains which makes up rainbow tables are chains of one-way hash and reduction function starting at a certain plaintext and ending at a certain hash[18]

H. *Phishing*

It is a method that deceives the user into believing the malicious website as a trustworthy source. It works by email spoofing or instant messages and it often directs the user to enter personal information at a fake website which looks just like the original site with only a difference in the URL of the website.[20]

III. LITERATURE SURVEY

Text based passwords have been the primarily used authentication method for many years now. It is solely based on the text or alphanumeric passkey set by the user itself.
This method has been lacking in providing secure authentication due to being very prone to multiple attacks even after evolving from just text passwords to case sensitive alphanumeric passwords which are marginally difficult than the previous versions.

Gaze based password authentication [] was proposed to prevent shoulder surfing[1]. In this method a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using only the orientation of their pupils.

CaRP[] as a graphical password paper proposed various protection schemes to combat diverse security attacks[2]. The strategies implemented leveraged the use of cryptology primitives that reduced the bottlenecks of traditional systems. The proposed authentication process involves graphical password scheme that solved different types of attacks both relay and dictionary to a great extent.[1]

In the present scenario, information systems are subject to password stealing and use attacks[4]. Therefore, this paper proposed a secure password authentication technique to overcome such challenges on a regular basis[3]. The new technique authenticated the user handling the system through one-time password generated randomly and communicated to the user via electronic communication system or email service[5].
Text based passwords have been traditionally used as an authentication technique but unfortunately it is associated with various usability and security issues. Parallel to that, tokens and biometric systems also had some bottlenecks.[6]Therefore, to counteract such techniques, a new method called graphical passwords – Zero Knowledge Based and Genuine Knowledge Based was proposed to minimize the security attacks.[7]

TABLE I
COMPARISON OF MAJOR PASSWORD AUTHENTICATION TECHNIQUES

Technique Used	Operation method	Possible attacks
Text based password	Type in user	Dictionary attack, brute force search, guess, spyware, shoulder surfing.
Perrig and Song [2]	Pick several pictures out of many choices. Takes longer to create than text password	Brute force search, guess, shouldersurfin g

Sobrado and Birget [3]	Click within an area bounded by pre-registered picture objects, can be very fast	Brute force search, guess
Man, et al.[4] Hong, et al.[5]	Type in the code of preregistered picture objects; can be very fast	Brute force search, spyware
Passface [6]	Recognize and pick the preregistered pictures; takes longer than text-based password	Dictionary attack, brute force search, guess, shoulder surfing

IV.CONCLUSION

We have analyzed the available security measures used in the way of protecting user's information. The analysis included many methods studies such as perring song, sobrado and birget, Man, et al hong, et al, Passface and the possible deficiencies in the method. From, these findings we conclude that the methods used individually may be vulnerable to various attacks, so we propose the usage of multiple combine methods such that each method, cancels the deficiencies of the other methods, for improving security

REFERENCES

[1] A. C. Long, A. S. Patrick, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale,

[2] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999

[3] L. Sobrano and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002

[4] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[5] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003

[6] Real User, "www.realuser.com," last accessed in June 2005.

[7] Namita Raghuwanshi, Prof. Amit "Namita Raghuwanshi, Prof. Amit Saxena Truba "A Survey of Two-Party Password Authentication Key Exchange" in International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 1078

[8] Sonia Chiasson,Alain Forget,Robert Biddle,P. C. van Oorschot," User interface design affects security: patterns in click-based graphical passwords",in international journal journal of information security , December 2009

[9] *Preethi. D, Priya. J, Saranraj. G,"* Enhancing Security Using Graphical Patterns Selection (ENSUGPS), in november 3 2013

[10] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd," Reducing Shoulder-surfing by Using Gaze-based Password Entry"
[11] Duchowski, A. T., Eye Tracking Methodology: Theory and Practice: Springer. 227 pp. 2003.

[12] Golle, P. and D. Wagner, Cryptanalysis of a Cognitive Authentication Scheme, International Association for Cryptologic Research, July 31 2006.

[13] Hansen, D. W., D. MacKay, and J. P. Hansen. Eye Tracking off the Shelf. In Proceedings of ETRA: Eye Tracking Research & Applications Symposium. San Antonio, Texas, USA: ACM Press. pp. 58, 2004. 14. Hansen, J. P., K. Torning, A. S. Johansen, K. Itoh, and H. Aoki. Gaze Typing Compared with Input by Head and Hand. In Proceedings of ETRA: Eye Tracking Research & Applications Symposium. San Antonio, Texas, USA: ACM Press. pp. 131-38, 2004.

[14] 1Manjunath D, 2Nagesh A S,3Sathyajeeth M P, 4Naveen Kumar J R, 5Syed Akram," A Survey on Knowledge-Based Authentication",july 3,2008

[15] Ms Sayali .P Shinde 1, Prof J.S Raghatwan 2," A Survey Paper on Secure User Authentication using CaRP a security primitive based on Hard AI Problems",may 5,2016

[16] ArunKumar.Kasa1, Sai Ashritha.K2,, "A Survey Paper On User Authentication", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 4, Aug-Sept, 2013

[17] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[18] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[19] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[20] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.