World Applied Sciences Journal 19 (4): 439-444, 2012
ISSN 1818-4952;

DOI: 10.5829/idosi.wasj.2012.19.04.1837

A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication

Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider

Comsats Institute of Information Technology, Wah Cantt., 47040, Pakistan

Abstract: Passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. The major aim for using passwords is to restrict unauthorized users to access the system. Passwords are necessary but, still they are not considered much safe to provide the security to the users because of many flaws in the conventional password systems. A large number of attacks on many systems are related to the passwords. This paper describes password attacks and comparative analysis of different authentication methods for awareness of attacks and selection of authentication method in a particular scenario.

Key words: Brute force · Dictionary · Key Loggers · Security · Keystroke

INTRODUCTION

There are a number of passwords attacks and few of them are described here, so that any person can understand and be aware of unauthorized access or passwords attacks. Many contributors presented password methods for a secure authentication. Some contributors as [1-4] have surveyed on authentication philosophy, attacks and graphical password methods. In this paper authentication methods are classified and comparatively analyzed. The purpose of this research is to highlight the advantages and disadvantages of different secure authentication methods and provide awareness to persons about password attacks and suitability of authentication method in a particular scenario. The part I of the paper describes password attacks, part II describes classified password methods of different contributors and part III presents comparative analysis of different authentication methods which are described in part II. At the end of the paper conclusion is presented to guide contributors for the development of more secure authentication method.

Password Attacks

Brute Force Attacks: In this type of attack, all possible combinations of password apply to break the password [5]. The brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted text. Early Linux systems use MD5 hashing schemes for storing the passwords. There is a password file in the operating system which contains the user's passwords with user names. If the file is stolen by the attacker then the password can be caught. The original password is not in the file but it is encrypted in the form of MD5 Hash. The encrypted password seems to be safe but in fact it is also vulnerable to brute force attack. For this, the attacker first converts all combinations of passwords into their MD5 Hashes. In order to break the password the attacker first extracts the MD5 hash of suspected password from the password file placed in the system. The hash is then matched with all MD5 hashes one by one. When the hashes are matched, the corresponding password is selected [6].

Brute force attacks are very time consuming as searching a hash from all possibilities is a time taking process. For example a user enters a password of 8 characters and all characters are lower case letters then to break the password using the brute force attack it requires $(26)^8$ combinations which is equal to 208827064576. If a single computer takes 1000 passwords to check in one second then total time will be 208827064576 / 1000 = 208827064.576 seconds which is equal to 58007.52 hours. This shows that brute force attack is effective for smaller passwords.

Corresponding Author: Mudassar Raza, Comsats Institute of Information Technology, Wah Cantt., 47040, Pakistan.

Fig. 1: Shoulder Surfing

Dictionary Attack: This type of Attack is relatively faster than brute force attack [7]. Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage. Many users generally write passwords related to the names of birds, familiar places, famous actors names [8] etc. These passwords can be judged by the dictionary attack. The attacker makes the dictionary of most commonly used words that might have been be used as a password. The attacker then applies all these words to break the password. Although the dictionary attack is faster than brute force attack, it has some limitations too i.e. brute force attack contains limited words and sometimes it is unable to crack the password because it remains a possibility that password to be cracked may not be present in the dictionary itself.

Shoulder Surfing: Shoulder Surfing is an alternative name of "spying" in which the attacker spies the user's movements to get his/her password. In this type of attack, the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed.

There are many variations of shoulder surfing [9] i.e. the attacker can use binoculars to see the user entering the password from a distance. The attacker can use the hidden close circuit TV camera to observe the password entering from a remote location. The attacker can listen that how many keys the user has pressed and then the attacker uses all the possibilities related to the password length to break it.

Replay Attacks: The replay attacks [10] are also known as the reflection attacks. It is a way to attack challenge response user authentication mechanism (Same type of protocols by each sender and receiver side for challenge and response). The method for this type of attack is that the attacker first enters his/her name in first login connection. To authenticate the user, the receiving device sends the challenge to the sender (in this case attacker). The attacker opens another login at the same time with its own valid user name and replies the receiving device as challenge of previous connection. The receiving side accepts the challenge and responds to it. The attacker then sends back that response through the account to be hacked and thus it gets authenticated. Then the attacker gets access to that account.

Phishing Attacks: It is a web based attack [3, 11] in which the attacker redirects the user to the fake website to get passwords/ Pin Codes of the user. To explain Phishing, suppose a user wants to open website say "www.yahoo.com". The attacker redirects the user to another website e.g. "www.yah0o.com" whose interface is similar to that of the original website to disguise the user. The user then enters the login information which is retrieved by the attacker. The attacker then redirects the user to the original website and logins the user with the original website. Different phishing control filters are used nowadays but still they are not much reliable.

Key Loggers: The attacks through key loggers are similar to the login spoofing attacks discussed above [7, 12, 5]. They are also called the Key Sniffers. The key loggers are the software programs which monitors the user activities by recording each and every key pressed by the user. The attacker installs the key logger software into the user system, either by installing that software himself or by tricking out the user to click to install that file into his (user) system. The key logger makes the log file of the keys pressed by the user and then sends that log file to the attacker's e-mail address. The attacker then gets the password and can access to the target system.

Video Recording Attack: In such type of attack the attackers with the help of camera equipped mobile phone or miniature camera, analyzes the recorded video of users which enters password. In it user's password entry operations are recorded once or twice [5].

Authentication Methods Based on Password

Conventional Password Scheme: The Conventional Password Scheme is an old and most widely used password scheme. In this scheme the user enters or logs in into the system through his username and password. The system first authenticates the user from the user database and on the basis of authentication of the user and then grants the access to the system is granted.

The advantage of conventional password scheme is that it provides the security of data by allowing only authenticated users to access the system. However, such scheme is vulnerable to attacks like Shoulder Surfing, Key loggers, Phishing Attacks and Login Spoofing etc.

Keystroke Dynamics: The key stroke dynamics [13-19] (also called the typing dynamics) records the key press and key timings. It does not deal with "what" the user has entered the password; it deals with "how" the user has entered the password. The Key Stroke Dynamics stores the following time patterns of the user along with the conventional password.

- Time between the key pressed and release
- Time between the two keys pressed.
- The name of the key pressed
- Biometric password entering rhythm of individual users

The Keystroke Dynamics originated from the word telegraph which is an electronically message passing system through unique click patterns of key clicks. Telegraph machine was invented in 1884 in which the user clicks the different timing patterns to generate a message. The message is then sent to the destination through the electric wires.

Advantages of key stroke dynamics include that no need of extra hardware, only good programming skills are required to implement such authentication system. It resists to password attacks like shoulder surfing, phishing, key loggers etc. Also the attacker cannot get into the system even if he/she gets the password. Disadvantages of Key Stroke Dynamics include that password rejection rate is high due to different levels of typing speed of users and User feels it as an extra overhead. It can be effective in different mental conditions of the user (i.e. happiness, sadness, hypertension etc.).

Click Patterns: Click Patterns is a type of mouse based password entering scheme described by [20, 21]. In this type of password scheme, the user is provided with a click pad on the screen. The click pad can contain different color grids or it can be the combination of different symbols. The user can mislead the attacker by using the click pattern as a password. Along with the patterns, the click pattern scheme also tracks the user clicking rhythm.

Advantages of Click Patterns include that it does not require extra hardware and it is resistant to password attacks like shoulder surfing, phishing, key loggers etc. Also the attacker cannot get into the system even if he/she gets the password. The disadvantages include that the Password rejection rate is high due to different mental levels of users i.e. the system often cannot recognize the user. It gets affected by different mental conditions of user (i.e. happiness, sadness, hypertension etc.)

Graphical Passwords: Graphical passwords have many variations described by different authors [1, 2, 22, 23]. In this scheme, the user first enters the user name to login. After that some graphical objects are displayed, which are necessary to be selected by the user. These selected objects are then drawn by the user using mouse, touch screen, stylus or touch pad etc. The system performs preprocessing on the user drawn objects and converts the sketches into hierarchical form. At last hierarchical matching is performed for user authentication.

Advantages included reduced shoulder surfing and it is a more secure authentication. Disadvantages include that the system verifies the user only if proper sketch is drawn by the user and touch sensitive screens are required for sketching. Also it depends upon the ability of the user to draw sketches and its authentication processing time is much longer than other schemes.

Biometrics: Biometrics is also used as authentication procedure in which the recognition is based upon image processing. In this case to verify an image, it is first preprocessed to extract features from it and then the image based on these extracted features is matched with the database.

There are many types of biometrics based authentication [24-26] i.e.

- Finger print authentication
- Face Recognition
- Signature Verification
- Speech Recognition
- Iris recognition etc.

Advantages of such schemes include that it involves real and unique signatures and it cannot be stolen. The disadvantages includes that, it is costly and difficult to implement. It is still not mature and can be bypassed. Also it is time taking process.

Authentication Panel: In these password schemes instead of pressing exact button for password, user is prompted to select the location of the password words from given panel [5, 27, 28].

It provides resistance against brute force, dictionary, shouldering and video recording attacks. It does not required extra hardware and it is fast.

Reformation Based Authentication: In such scheme the password is shifted to new form before storing and whenever the password has to be read then it must be required to apply reform mapping to verify the user given password [29, 30]. As it provide a layer above the original stored password. The reformation that is applied at the time of authentication of a user is dynamic in nature. Hence the hacker is unaware of the real password string even if the stored password is hacked. The main advantage of this scheme is as it resist strongly against dictionary attacks, shoulder surfing, video recording and brute force attacks.

Moving Balls Based Security Scheme: In this novel scheme the user click the mouse, then a user have number of balls moving in different columns and it all seen on screen, now the user just has to remember the number of columns and the respective balls [31].

Expression Based Security Scheme: This novel scheme provides two level securities as password on password. The user has to remember both the password and generated key by the system [31].

Virtual Password: This Novel password scheme offers secure user's password in on-line environments [32, 33]. It can provide protection against different online attacks as phishing and password file compromise attacks.

Time Signature: Time signature is a novel technique proposed in [20] "Time Signatures - An Implementation of Keystroke and Click Patterns for Practical and Secure Authentication". It is a new and hybrid password scheme with the combination of conventional password, Keystroke Dynamics (KD) and Click Patterns (CP). The purpose of such hybrid password technique is to provide better security of data for end users.

Time signatures provide more security than the conventional password systems [20]. Time signatures can be the good answer to the attacks like shoulder surfing attacks, dictionary attacks key loggers and replay attacks etc. Even if the attacker knows the password, he cannot enter into the system because he is unable to enter the password with the prescribed time sequence by the original user. It is also observed that whether the original user tells the password to the attacker along with the time sequence, it is still impossible for the attacker to remember the time sequence which is in the original user's mind. This provides the security of the passwords.

Comparative Analysis of Authentication Methods: In Table 1 different password methods are comparatively highlighted in which it is tried to show that which password method or authentication scheme could resist against what type of attacks. The table also highlights method's additional requirements, cost, processing time, protection level and method's effect towards person's metal condition.

Table 1: Analysis of authentication methods

Method	Resistance to attacks	Additional Hardware Requirement	Cost	Mental attitude effects	Protection level	Processing Time
Conventio-nal password scheme	No		Normal		Low	Fast
Key stroke dynamics	Shoulder surfing, pishing, key loggers	No	Normal	Yes	Medium	Medium
Click patterns	Shoulder surfing, pishing, key loggers	No	Normal	Yes	Medium	Medium
Graphical passwords	Shoulder surfing	Yes	High	Yes	Medium	Slow
Biometrics	Shoulder surfing, pishing, key loggers etc	Yes	High	No	High	Slow
Authentication Panel	Video recording, shouldering	No	Normal	Yes	High	medium
Reformation Based	Brute force, video recording, shoudering and dictionary attacks	No	Normal	No	Medium	Fast
Moving Balls Based	Dictionary attacks, shouldering	No	Normal	Yes	High	medium
Expression Based	Brute force, video recording, shoudering and dictionary attacks	No	Normal	Yes	High	Fast
Virtual Passwords	Pishing, key loggers and all other online attacks	May be	May be high	No	Medium	Fast
Time Signature	Shoulder surfing, dictionary attacks, replay attacks, key loggers etc	No	Normal	Yes	High	Slow

CONCLUSION

Through this survey several things are concluded as before adopting any password or authentication method, user must know the password attack and then user should apply appropriate solution. The user should apply the authentication method according to scenario because some of the methods are applicable at stand alone system and some are applicable at online environments as over ATM and several internet services. Although several novel schemes described here provide protection against dictionary attacks, brute force attacks, video recording attacks, spyware, shoulder surfing, phishing etc but in order to secure the system. Also different password schemes can be merged together to form a single and more secured password scheme. Such scheme can be the combinations of passwords schemes such as:

Conventional Passwords
Conventional + Keystrokes Dynamics
Conventional + Click Patterns
Biometrics + Conventional + Keystrokes
Conventional + Memorable

REFERENCES

1. Anand Sharma and Vibha Ojha, 2010. Password based authentication: Philosophical Survey. IEEE.
2. Martinez-Diaz, M. and C. Martin-Diaz, 2010. A comparative evaluation of finger drawn graphical password verification methods. 12th international conference on frontiers in handwriting recognition 2010 Spain.
3. Ilkka Uusitalo and Josep M. Catot, 2009. Phishing and countermeasures in Spanish online Banking. 3rd International conference on emerging security information, System and Technologies.
4 Ali, M. Eljetlawi and Norafia Ithnin, 2008. Graphical password: Comprehensive study of the useability features of the recognition base graphical password methods. 3rd International conference on convergence and Hybrid Information Technology.
5. Fujita, K. and Y. Hirakawa, 2008. A study of password authentication method against observing attacks. 6th International Symposium on Intelligent Systems and Informatics, SISY 2008.
6. Muhammad Sharif and Aman Ullah Khan, 2007. Benchmarking of PVM and LAM/MPI Using OSCAR, Rocks and Knoppix Clustering Tools in ICCISSE 2007, XXI. International Conference on Computer, Information and Systems Science and Engineering May 25-27, 2007 Vienna, Austria.
7. Arvind Narayanan and Vitaly Shmatikov, 0000. Fast dictionary attacks on passwords using time-space tradeoff, Conference on Computer and Communications Security, Proceedings of the 12th ACM Conference on Computer and Communications Security, pp: 364-372.
8. Kessler, Gary C., 2002. Passwords - Strengths and Weaknesses. Jan 1996. URL: http:// www.garykessler.net/library/password.html.
9. Huanyu Zhao Xiaolin Li, 2007. A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme, Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference, 2(s): 467-472.
10. Syverson, P., *et al*., 1994. A taxonomy of replay attacks [cryptographic protocols], Proceedings of Computer Security Foundations Workshop VII, CSFW, 7(s): 187-191.
11. Fahad Ikram, Muhammad Sharif and Mudassar Raza, 2008. Protecting Users against Phishing Attacks in 7th CIIT Workshop on Research in Computing June 23, 2008 CIIT, Lahore - Pakistan.
12. Baig, M.M. and W. Mahmood, 2007. A Robust Technique of Anti Key-Logging using Key-Logging Mechanism, Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES, Feb 2007, (s): 314-318.
13. Haider, S., A. Abbas and A.K. Zaidi, 2000. A Multi Technique Approach for User Identification through Keystroke Dynamics, 2000 IEEE International Conference on Systems, Man and Cybernetics, 2(s): 1336-1341.
14. Nick Bartlow and Bojan Cukic, 2006. Evaluating the Reliability of Credential Hardening through Keystroke Dynamics, 17th International Symposium on Software Reliability Engineering, 2006. ISSRE apos06 Nov.(s): 117-126.
15. Jarmo Ilonen1, 2003. Keystroke Dynamics, Advanced Topics in Information Processing 1 - Lectures, Wed Dec 10, 2003, http:// www.it.lut.fi/ kurssit/ 0304/ 010970000/lectures.html.
16. Enzhe Yu Sungzoon Cho, 2003. GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification, Proceedings of the International Joint Conference on Neural Networks, 2003. 3(s): 2253- 2257 Vol. 3 ISSN: 1098-7576.
17. Tai-Hoon Cho, 2006. Pattern Classification Methods for Keystroke Analysis, SICE-ICASE, 2006. International Joint Conference Oct. 2006, (s): 3812-3815.

18. Attila Mészáros, Zoltán Bankó and László Czúni, 2007. Strengthening Passwords by Keystroke Dynamics, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany.
19. Dalia Abdul Hadi Abdul Ameer and Ahmed Abdulhakim Al-Absi, 2010. Anywhere On-Keyboard Password Technique. IEEE Student conference on Research and development 2010 Putrajaya Malaysia.
20. Muhammad Sharif, Tariq Faiz and Mudassar Raza, 2008. Time Signatures - An Implementation of Keystroke and Click Patterns for Practical and Secure Authentication, The third International Conference on Digital Information Management (IEEE ICDIM 2008), 13-16 November, 2008, University of east London, London UK.
21. Abdurazzag Ali Abura and Manal I. Al Fallah, 2008. Password generator based on mouse clicks signal and screen cursor position. IEEE Proceedings of the International Conference on Computer and Communication Engineering.
22. Qurat-Ul-Ain Arshad, Muhammad Sharif, Mudassar Raza and Aman Ullah Khan, 2007. Secured and Handy Graphical Password System, National Conference of Information and Communication Technologies (NCICT-2007), June 09, 2007, at Main Campus University of Science and Technology, Bannu, NWFP, Pakistan.
23. Mohd Ali Bin Mohd Isa and Mohd Nor Hajar Hasrol, 2008. User perception towards the use of colour as Authentication method: focus on FTMSK lecturer. Proceeding of the International Conference on Computer and Communication Engineering Malaysia.
24. Varun Kacholia and Shashank Pandit, 2003. Biometric Authentication Using Random Distribution (BioART), Canadian IT Security Symposium (CITSS)
25. Ahmed, A.A.E. and I. Traore, 2005. Anomaly Intrusion Detection Based on Biometrics, Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IAW '05.
26. Fadhli Wong Mohd Hasan Wong Supian, A.S.M. Ismail and A.F. Lai Weng Kin Ong Cheng Soon, 2001. Enhanced User Authentication through Typing Biometric with Artificial Neural Networks and K-Nearest Neighbour Algorithm, Thirty-Fifth Asilomar Conference on Signals, Systems and Computers, 2001. 2(s): 911-915 Vol. 2, ISBN: 0-7803-7147-X.
27. Manabo Hirano and Tomohiro Umeda, 2009. T-PIM: Trusted password Input method against data stealing Malware IEEE 6th International Conference on IT.
28. Hirotaka Tazawa and Takashi Katoh, 2010. A user authentication scheme using Multiple Passphrases and its arrangements. ISITA Taiwan.
29. Safdar, S., M.F. Hassan, M.A. Qureshi, R. Akbar and R. Aamir, 2010. Authentication model based on reformation mapping method " International Conference on Information and Emerging Technologies (ICIET).
30. Shakir, M. and Abdul Ayaz Khan, 2010. S3TFPAS: Scalable shoulder surfing resistant Textual-Formula base Password Authentication system. IEEE.
31. Shahid, M. and M.A. Qadeer, 2009. Novel scheme for securing passwords". IEEE 3rd International Conference on Digital Ecosystems and Technologies, DEST '09.
32. Mohammadi, S. and S.Z. Hosseini, 0000. Virtual password using Runge-kutta method for internet banking. IEEE 2nd International Conference on Communication Software and Networks.
33. Qiang Wang and Zhiguang Qin, 2010. Stronger User authentication for web browser. 3rd International conference on advance computer theory and engineering (ICACTE) China.
34. http://www.datadoctor.ws/disk-data-recovery/keylogger.html.
35. http://newsdesk.si.edu/images_full/images/museums/nmah/treasures/morse_telegraph_ key. jpg.