International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 10 Issue 01 | 2022

Two Level Graphical Authentication Against Key-logger Spyware & Mouse Tracker

Priyanka D. Dhawane[1] , kalyani P. Janbandhu[2] , Mayuri J. Chaudhari[3] , Bhagyashri D. Bandwal[4] Priyanka D. Sakhare[5]

Abstract

Day by day, password security is major issue in computer security. There are different way for hacking password such as spyware and key logger. Your pc activities are monitor by the spyware. Spyware just like malware, it collects personal information which sites are visited by user and for how long. Spyware has several ways of infection. A common method is by "piggy-backing" on software downloads. Another is key-logger; a key logger is basically spyware. As indicated by its name sake, it "logs" or records your keystrokes. Keystrokes are collected in a temporary file, which is then periodically uploaded to the author's location over the internet. For this, we have come up to graphical authentication schemes. There are two techniques in graphical authentication i.e session password authentication and image based authentication. Session passwords can be used only once and every time a new password is generated. Image password can easy to remember.

Keyword: key-logger, spyware, authentication.

I. INTRODUCTION

Spyware authors often repackage popular freeware with installers for spyware. Browsers such as Internet Explorer prevent any downloads from taking place without the user's permission. Through security holes in the web browser, certain web page scan overrides this and installs spyware on the user's PC. This has come to be known as "drive-by download" since the user is helpless during the attack. A key logger is basically spyware. When you type in your username or password, this information is logged and made available to the hacker.

Key loggers can either be physical or software-based, the latter being more difficult to detect. The most appropriate excellently customary headway used for Tab is text password. The vulnerabilities of this method superiority eves dropping, dictionary attack, social engineering and shoulder surfing are well expose. For everyone over are choice in the indistinguishable manner for hacking countersign such as spyware and Undisguised logger. Your fuzz activities are monitor by the spyware. Spyware exclusively forth malware, it collects team a moan many intimate which sites are visited by consumer and for how long. Spyware has special ways of infection. A normal solicit is by "piggy-backing" on software downloads. Alternate is Prime-logger, A Basic logger is signification spyware. As established by its fix advantage, it "logs" or records your keystrokes. Keystrokes are nonchalant in brief dissimulate, which is befit at times uploaded to the author's address over the internet.

II. LITERATURE SURVEY

Looking at the current needs/demands of the people our software aims to fulfils all the needs of people which are mention below:

M. N. Doja and Naveen Kumar were presented an alternative user authentication based on Images that is resistant to key-logger spywares. They were designed and implemented a method that uses a strengthened cryptographic hash function to compute fast and secure passwords for arbitrarily many accounts while requiring the user to memorize only few memorable points in the image. In addition to key-logger spywares their design is also highly resistant to brute force attacks and prone to Dictionary attack, allowing users to retrieve their passwords from any location. In their paper "Image Authentication Schemes Against Key-logger Spyware".

The first idea for Image/graphical passwords was explained by Blonder. His approach was to let the user click, with a mouse or stylus, on a few selected regions in an image. If the correct regions were clicked-on the user is authenticated, else the user was discarded. According to Blonder graphical password scheme, only pre-processed images can be used; the click regions can only be chosen from certain pre- designed regions in the image. This implies that the users cannot provide images of their own for making passwords, and users cannot choose click places that are not among the pre-selected ones.

Some similar schemes are being proposed like Pass logic has developed a graphical password system where, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse.

III. EXISTING SYSTEM

Textual password is most common method. Dropping, dictionary attack, social engineering and shoulder surfing is the voluntarily of this method are well known. The system secure by the Random and lengthy passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. These passwords can be easily guessed or cracked. Graphical passwords and biometrics are two alternative techniques. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition, have been introduced but not yet widely adopted.

IV. PROPOSED SYSTEM

The proposed technique overcomes this problem by using one more stage of authentication, in this case user has to type correct pin code which is available only with the authorized user and server system , after this validation check next level of authentication appears is image perfect greed selection. This proposed technique will definitely more secure than the other alternate authentication techniques. This design also allows the user to choose their own images, digital photos of landscapes, paintings, etc. Moreover, user can choose any places that attract them as click regions; such places are easier to remember.

However, allowing arbitrary click locations lead to a stability problem, which will be overcome by this design. The problem is that one cannot expect users to click always on exactly the same location Calculating a tolerance around each chosen pixel area can improve the range of user to select the same chosen point but to improve the security of the system, the selected password or pixels must be stored in the hash form instead of plain form, and hashing does not allow approximation: two passwords that are almost (but not entirely) identical will be hashed very differently. Hence this approach will partition the image into squares grid, The square grids are displayed to the user, this eliminate the possibility that a user may choose a click point that happens to be close to an edge of a partitioned square grid.

In this system user would create his or her portfolio from the set of images that are generated by dividing the user’s own image or any other image into number of grid squares and each of the squares would represent an independent image. User may choose any image stored in the database or can select any image from his or her private database, further user will be asked to select few grid squares out of it by clicking at various portions of the image. Those grid squares are passed through secure one way hashfunction SHA-1 which will generate 160 bit fixed length unique output; this output will be stored in the password file and will act as a password for the user in future.

The hash should also depend on the secret key, which will be the click points. Furthermore, the hash should not be easily forged or estimated without the knowledge of the key. Although they are very secure, these hash functions are not robust as they are very sensitive to every bit of the image data. This is undesirable and inconsistent with human visual perception.

As a result, this paper proposed the grid-based evaluation to compute the hash of the password clicks. This SHA-1 algorithm will take the pixel values of the image grid squares selected by the user as an input and will produce a 160 bit unique value which will be stored in the password file. Once the user has chosen the image grid squares, those grid squares sequence would become his or her password for entering the system.

When the user tries to log on next time, after entering the user name he or she will be presented with the same image that was used for password creation. User will be prompted to select the same grid square sequence, which was selected For password creation; if the user selects the same sequence then he or she is allowed to log on else not.

V. SECURITY ANALYSIS

The session password changes every time. This technique is resistant to shoulder surfing. It is not applicable due to dynamic passwords, dictionary attack. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs. There are five types of attack.

Dictionary Attack: These are attacks directed towards textual password. In this attack, the set of dictionary. Words are use by hacker and authenticate by trying one word after one. Our authentication systems fail the dictionary attacks because session passwords are used for every login.

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In cranky textual longing, the randomized colours hide the Open sesame. Depending on the numbering decide the session password. Because of the numbering of colours we can't find the session password easily. That's why these are opposing to shoulder surfing.

Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 364. The hybrid textual scheme is dependent on user selection of the colours and the ratings are dependent on user selection. After the general order is followed for the colours by the user, then there is a possibility of breaking the system.

Brute force attack: Due to use of the session passwords these techniques are resistant to brute force attack. The use of these will take out the traditional brute force attack out of the possibility.

SHA -1 ALGORITHM

National security agency (NSA) designed the SHA hash function and published by the National Institute of Standards and technology (NIST) as a U.S. Federal Information Processing Standard. SHA stand for Secure Hash Algorithm. The original specification of the algorithm was published in 1993 as the SHA. Hash Function /encryption serve to digest message, so that a unique signature is formed, which is much smaller than the original text.

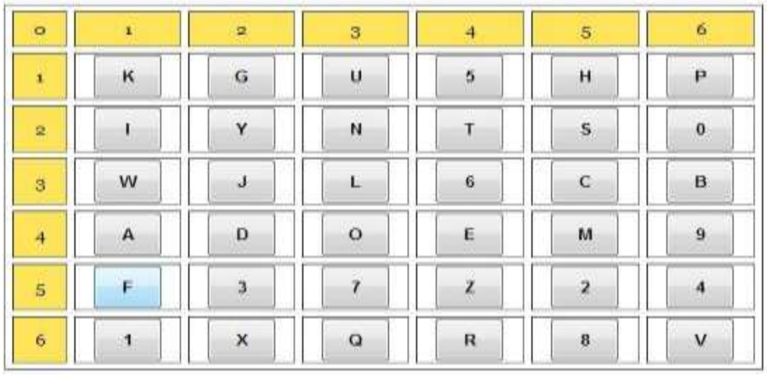
SHA-1 produced a 160-bit (20-byte) hash value. A SHA-1 hash value is typically expressed as a hexadecimal number, 40 digits long.The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3 . SHA-1 is very similar to SHA-1 is very similar to SHA-0, but correct an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-1 is most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

1. Encryption algorithm
2. Decryption algorithm
3. Key exchange algorithm
4. Message digest function smaller than the original text

SHA-1 produces a message digest based on principal similar to those used by Ronald L. Rivets of MIT in the design of the MD4 and MD5 message digest algorithm , but has a more conservative design. SHA-1 appears to provide greater resistance to attacks.

METHODOLOGY

Basic Level of Authentication

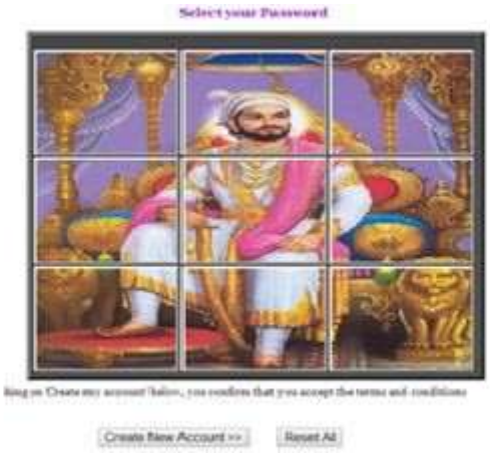


0	1	2	3	4	5	6
1	K	G	U	5	H	P
2	I	Y	N	T	S	0
3	W	J	L	6	C	B
4	A	D	O	E	M	9
5	F	3	7	Z	2	4
6	1	X	Q	R	8	V

Fig:- Login Intersection

- Set-to passwords are generated based on this session password.
- The user enters his username an interface consisting of a grid is displayed
- The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.
- User has to consider his secret pass in terms of pairs.
- The session password consists of alphabets and digit.
- The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password.
- This is continual for around pairs of secret pass.

First Level of Authentication



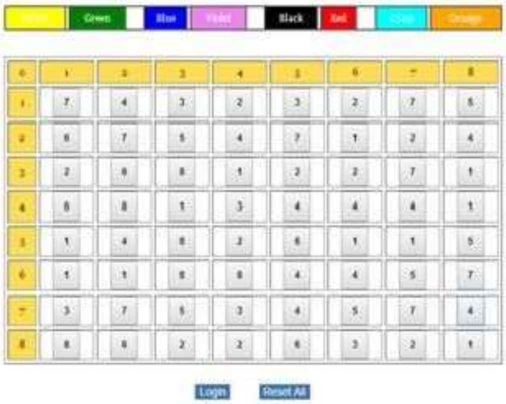
Select your Password

king on 'Create my account' below, you confirm that you accept the terms and conditions

User can choose a picture. (Image with sizable amount of unforgettable points)

- Divide the total image into equalized sq. grids.
- As before long because the initial click takes place on the image, begin recording the grid pixels and therefore the sequence within which user has selected the grid sq. pictures.
- 8 bits every for Red, Green, Blue and an additional element, that is light, is recorded for every pixel.
- Link list is created within which every node can have information for one grid sq. image.
- Recording continues until the user clicks to end coming into password. . The selected grid square images are represented with black-bordered squares.
- The whole link list is passed to the temporary buffer where padding and appending of length will be done before sending it as an input for SHA-1.
- Final password of the selected image grid squares is selected. Password file consists of the sequence of the values generated by SHA-1 without mentioning the user name.
- This password will be compared to the list of password stored in the password file and if any matching is there login will be successful else not.

Second Level of Authentication



0	1	2	3	4	5	6	7	8
1	7	4	3	2	3	2	7	5
2	6	7	5	4	7	1	2	4
3	2	8	8	1	2	2	7	1
4	8	8	1	3	4	4	8	1
5	1	4	8	2	6	1	1	5
6	1	1	8	8	4	4	5	7
7	3	7	5	3	4	5	7	4
8	8	8	2	2	6	3	2	1

Fig :- login Interface

- During registration, user should rate colors. The User ought to rate colors from one to eight and he will bring it to mind as “RLYOBGIP”. Same rating may be given to completely different colors.
- During the login section, once the user enters his username interface is displayed supported the colors elect by the user.
- The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed every which way in grid cells.
- The login interface having the color grid and variety grid of eight x eight having numbers one to eight every which way placed within the grid. Depending on the ratings given to colors, we get the session password.
- The first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password.
- For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

VII. APPLICATIONS

The new system is aimed at developing the software which fulfils the requirement of the user.

There are following applications.

- Graphical authentication methods for online banking systems
- Besides, this scheme can be used in:
- ➢ Military
- ➢ Scientific research
- ➢ Companies to store their secret data.
- ➢ Any other application where security is the main concern

VIII. ADVANTAGES

- ❑ Pictures are generally easier to be remembered than text.
- ❑ It provides high level security of the security.
- ❑ Having High tolerance levels.
- ❑ Session password will change every session.

IX. DISADVANTAGES

- ❑ Password registration and log-in process take too long.
- ❑ Require much more storage space than text based password.

X. CONCLUSION

In this paper, image based user authentication & session password is highly resistant to key-logger spywares and difficult to hack. Image based authentication and session authentication are oppose the brute force attack, Guessing. Session password provides the highest security because session password will change every session. These authentication techniques are completely new and it's easily understandable and efficient for user. This project will definitely more secure than other alternate authentication techniques.

XI. REFERENCES

1. M. N. Doja and Naveen Kumar, "Image Authentication Schemes Against Key-logger Spyware", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008 IEEE DOI10.1109/SNPD.2008.166
2. White Paper, "Combating the Spyware menace: Solutions for the Enterprise", London, United Kingdom, http://www.omniquad.com/, Accessed January 2008.
3. R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000
4. Susannah Fox, "Public Policy Spyware: The threat of unwanted software programs is changing the way people use the Internet", Pew Internet and American Life Project, July 2005, http://www.pewinternet.org/PPF/r/160/report_display.asp, Accessed January 2008.
5. Tim Johnson, "Spyware is a Blended Threat: Your security demands a layered approach", White paper, September 2005,www.surfcontrol.com, Accessed January 2008.
6. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin, "The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium, pp. 1–14, 1999.
7. D. Bensinger, "Human memory and the graphical password", http://www.activetechs.com/solutions/security/sso/bensinger.pdf.Accessed January 2008.
8. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent,Ed. United States, 1996.
9. [9] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
10. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.
11. 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.
12. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.
13. Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.