www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11491-11495

A Password authentication in social Networking sites

MR. Praveen Kumar[1], S.Sirisha2, N.Breetha[3], M.Lakshmi[4]
[1]Assistant professor, VITech,, Anna University, vitpraveenkumar@gmail.com,
[2]Under Graduate Student, Computer science and Engineering, Velammal Institute of Technology
siri.sikha@gmail.com, breetha29@gmail.com, lakshmisrispet@gmail.com.

***Abstract*—Early we use Plain Textual passwords as a security. A password is a word or string of characters used for user authentication. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, networks, web sites, and reading the newspapers online. The common method which we used is a Textual password which is lengthy and consider as secured but difficult to remember thus the user pick short password but short password are easily crack or hack. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable for security, initially proposed, is an exciting new paradigm. So we proposed new password authentication technique is Session password and color password. Where it gives the options for user to select the password as a color or alphanumerical grid.**

***Index Terms*—Color password, session password, Novel attacks.**

I. INTRODUCTION

Textual password is a very simple password scheme. It was used in old days. The textual password is easy to trace so system access easily. Because user gives the password that is easy to remember, like pet name, birth day date, mobile number etc. So textual password scheme is unreliable. For more security practices a new technology is invented that is Graphical password. It uses a very expensive system like a biometrics, thumb recognition, speech recognition, digital signature etc .But it was a very expensive so it is not affordable for user. Both the textual password and Graphical password having some drawbacks hence to remove such drawbacks the newely security scheme is implemented or invented that is session password. It is very secure compares to remaining systems.

II. ONLINE SHIPPING WEBSITE

Online Shipping Application helps to book a ticket to send a parcel. It provides express shipping rates. These applications also support the customer with their customs expertise, variety of shipping solutions and wealth of knowledge in international shipping. Web Shipping is the online shipping solution that helps us to manage express shipments. We can print labels, schedule courier pickups, store addresses, track your shipments and much more. If we need speed and accuracy, Web Shipping will streamline your shipment process and eliminate manual paperwork. This solution is ideal for small to medium-sized companies, office managers, receptionists, business travellers or anyone on the go.

Web Shipping is easy to use and requires no training to use. The account holders can register and start shipping online. It only takes a minute to schedule a shipment.

III. ONE TIME PASSWORD

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has as well as something a person knows.

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details.

IV. CARP TECHNOLOGY

CaRP (Captcha as graphical Passwords).This is the present technology used in today's world. CaRP is challenging and click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login

attempt. But this system can suffer attacks such as malware attacks. Malware (Spyware attack) is a major anxiety for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker. So in order to overcome this Novel attacks we overcome with an special methods of color and session passwords respectively.

V. COLOR PASSWORD

The color password is highly secured process of protecting ones information. This is mainly used in online shopping websites. The implementation side includes giving ratings to the corresponding colors. Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration. It contains the following contents.

VI. PAIRED BASED AUTHENTICATION SCHEME

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 8 x 8 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.

Fig 1: The login interface

User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets, digits and special characters. 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 repeated for all pairs of secret pass. Fig 3.1 shows that x is the intersection symbol for the pair "xn". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system.

VII. HYBRID TEXTUAL AUTHENTICATION SCHEMES

Define During registration, user should rate colors The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

Fig 2: Rating Of Colors' By User

Shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, 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 col.umn of the grid is part of the session password. Consider the figure 9 ratings and figure. Login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e 5. The same method is followed for other pairs of colors. For figure 3.3 the password is " 5121".

Fig 3: Intersection letter for pair AN

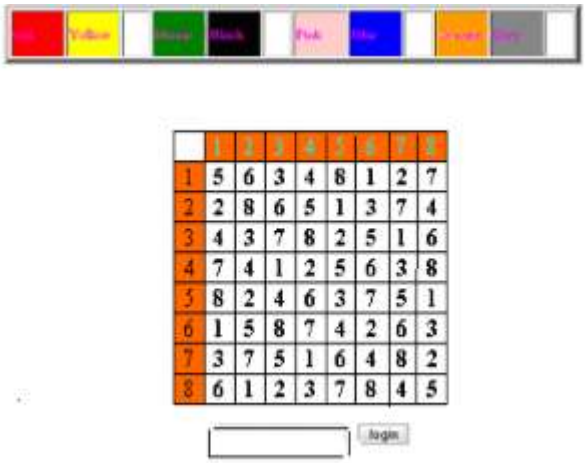

Fig 4: Login interface

VIII. SALT (CRYPTOGRAPHY)

In Cryptography, a salt is random data or string that is used as additional input to a function that hashes a password. The main function of salt is to protect against dictionary attacks and rainbow table attacks. A salt is randomly generated string for each password. The generated salt and User's password are concatenated and processed with the Cryptographic hash function and result is stored with salt in a Database. Hashing allows for late authentication while defending against compromise of the plaintext. Cryptographic salts are used in many Computer systems like UNIX system and Internet security.

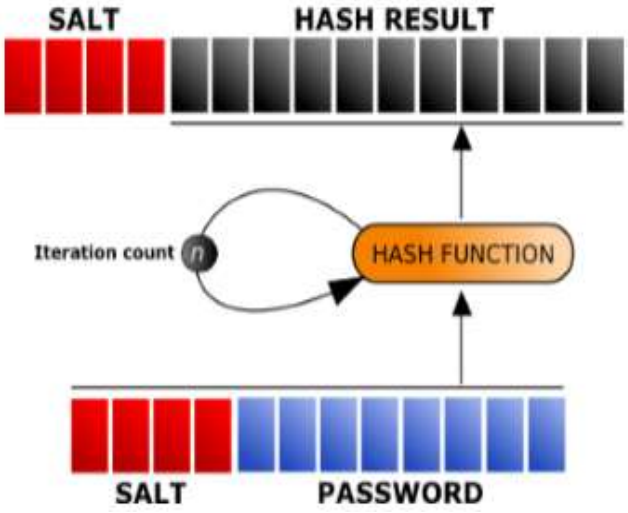

Fig 5: Generating Salt hash password

There are two types of salt first is fixed salt and second is Variable Salt. Fixed salt is a sequence of bytes which is used for concatenating with every password. We can keep this salt hidden and consider its providing security but it makes our system more vulnerable. The Variable salt is safer option as compare to the fixed salt because this is generated or computed separately for each password for concatenation with original password. It allows each stored password decoupled from the others and improving security against attacks. Steps for generating Salt Hash password:

1. Get password.
2. Generate Salt using random function.
3. Append salt to original password.
4. Generate Salt Hash password using appropriate hash function.
5. Finally store Salt and Salt Hash in the Database.

According to above steps Hash Password is generated. First original password is taken from the user and using Random function Salt is gets generated. After this generated Salt is appended to the original user's password. Then this Salt appended password is passes to Hash function. This Hash function is used to generate Salt Hash Password. Finally this generated Salt Hash Password and Salt is stored in database.

In this iteration count is used which is refers to the number of time that the hash function with which we are digesting is applied to its own this means that, once we generate a salt and concatenated with the password then apply the hash function, get the result and again pass that result as a input to the same hash function .This process is repeated again and again a number of times. The minimum number of iteration is 1000 for more security.

IX. PBKDF2 (Password Encryption)

Pseudorandom function such as cryptographic hash, cipher is applied by PBKDF2 to the user password along with salt value. This process repeated multiple times to produce derived key. This key is used as cryptographic key in subsequent operations. Having a salt added to the password reduces the ability to use recomputed hashes for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

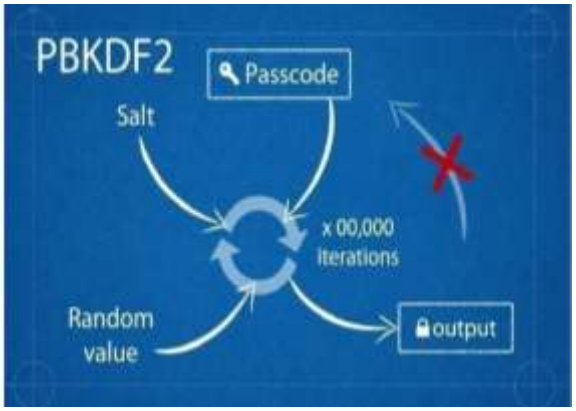

Fig 6: Password Encryption

PBKDF2 is used for generating derived key along with value of salt. So PBKDF2 algorithm takes an salt, Random function which gives random value, original user's password. Then this algorithm using number of iterations again and again Derived Key is generated which is final output. Derived key that conations salt, some random values and original password. This is for the login passkey which is makes cracking or hacking of password is quite slow and makes password more secure and protected.

5.1 Key derivation process of PBKDF2 in this key derivation function has five parameters:

$$DK = PBKDF2(PRF, Password, Salt, c, dkLen)$$

Where:

- PRF is a pseudorandom function
- Password is the master from which a derived key is generated.
- Salt is a generated cryptographic salt.
- c is the number of iteration in hash function.
- dkLen is the desired length of derived key.
- DK is the generated derived key.

X. CONCLUSION

Existing techniques does not have that much capability to secure password from hackers or third party location .because in this techniques only one password is used for each and every session and password is transfer for authentications of users. So these passwords are easily hacked by hackers. We proposed a system called Session password, in this it provides a new

password for each session and need not to transfer password form server each time for authentication purpose that's why Session password scheme provides more security than the other existed.

.

REFERENCES

[1] Jermyn, I., Mayer A., Monrose, F., Reiter, M.,and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[2] Haichang Gao, Zhongjie Ren, Xiuling Chang,Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant To Shoulder Surfing.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal valuation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, (2005), pp. 102-127.

[4] D. Weinshall, "Cognitive Authentication Schemes Safe against Spyware", (Short Paper), IEEE Symposium on Security and Privacy, (2006).

[5] S. Chiasson, R. Biddle and P. C. van Oorschot, "A Second Look at the Usability of Click-based Graphical Passwords", ACM SOUPS, (2007).

[6] L. F. Cranor and S. Garfinkel, "Security and Usability", O'Reilly Media, (2005).

[7] R. N. Shepard, "Recognition memory for words, sentences, and pictures", Journal of Verbal Learning and Verbal Behavior, vol. 6, (1967), pp. 156-163.

[8] 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).

[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, (2004), pp. 1399-1402