ORIGINAL RESEARCH PAPER

Computer Science

Secure Graphical Authentication System for Web-Applications

KEY WORDS: .

Tushar R. Mahore PG Scholar, Government College of Engineering, Amravati, India.

A.V.Deorankar Associate Professor, Government College of Engineering, Amravati, India

ABSTRACT

Internet security is a trending concept in Computer Science, lots of researchers are working on solving these issues. In last few decades internet has grown in vast amount, with the increase of the users of internet, security issues also grows. One of the security aspect of the internet is the authentication, everywhere in case of accessing some services over internet, one needs to identify himself. The process of identification is known as the authentication. Authentication is one important process, if it gets compromised then there are few other security aspects which directly gets compromised. Various techniques have been developed in the way of making the authentication more secure. The most popular way for authentication used in today's web applications is the Text-Based passwords. This is the conventional way used for authentication from last few decades. The problem related in the text-based password scheme is that, it promises to be more secure when the user selects a strong password. To overcome the problems associated with the strong password, graphical passwords can be used. In this paper we have proposed a system which is simple and can promise security without any condition. In this paper we have discussed the different authentication schemes and from that a proposed system, which is safe and secure.

INTRODUCTION

Human authentication are of various types, such as knowledge based authentication, token based authentication, biometrics based authentication. Few of them have very basic requirements and few of them requires external hardware. Conventional technique, in which the combination of username and alphanumeric password is used for authentication is the basic way for granting access to the application. The problem associated with the conventional technique is the selection of alphanumeric password. Alphanumeric password is the combination of uppercase letters, lowercase letters, special symbols and numbers, for example "FJH6900@kert7" is considered as strong password. In many situations, according to the study by Ofcom, the UK communications watchdog, has putted in front some statistics which reveal just how badly the general public treat password security. According to Ofcom's "Adults Media Use and Attitudes Report 2013" report, a poll of 1805 adults aged 16 and over discovered that 55% of them used the same password for most websites [1].Especially remembering the strong passwords are very difficult for those who does not belong to the computer field [2].

Web applications provides various web services, to access these services one needs to be get identified, i.e. the one willing to get access to the services is supposed to be the person he is calming. For granting access the service provider is supposed to identify the person using some of his/her personal information. Now here is what the security comes in the focus, whenever the service provider wants to identify the user, he needs data, and the data is the asset. So in the prevention of such personal information, we are supposed to stay secure over the internet. Different ways are available in the computer world to stay secure, such as encryption techniques and the SSL for the network security. But still all these precautions are not enough, the attacker finds their way. To provide more security we can add such encryption technique to the database, from which the user credentials are never going to be on the network. There are three types of human authentication techniques present, as follows

- Knowledge based authentication
- Token based authentication
- Biometrics based authentication

Knowledge based passwords are those in which what you know is important, i.e. based on the knowledge possessed by the human the authentication has been done. Token based authentication is based what you have, i.e. any kind of card or device which can be used for the identification. For example, an ID card of an employee in the company, which is used for the attendance of the employee. And the third method is the biometric based, in which what you are is important, i.e. fingerprint or retinal scanner is used for the identification.

To solve the problems associated with the text-based passwords, graphical passwords gets more attention, this is because the capacity of human to remember images more than the text. It is found that human being can remember lots of things and in more efficient way by using the images. Lots of graphical authentication schemes have been developed in last few decades as shown in [3], [4], [5], [6].

LITERATURE REVIEW

Lots of research has been done in the field of authentication schemes, few of them promises more security over the others. Among all of the authentication schemes present out there, few are very basic, and few requires some additional hardware, like various sensors. There are other interesting techniques present such as shown in [7], [8], [9], [10], [11], [12] which are not graphical based but needs additional hardware such as audio, gyroscope, vibration sensor etc.

Blonder's Scheme is the very first graphical authentication scheme which has been proposed in 1996. In Blonder's scheme, in front of user an image is displayed which is predetermined image on any visual display device which user is using then user has to select one or more positions on image which are already known positions to user in a particular order to access the particular resource. After that the display quality of the devices gets better and new techniques has been proposed by the researchers, such as DAS (Draw-a-Secrete), PassFaces, PassPoints etc. These are the techniques which are more popular than the other, because of their simplicity and ease of use.

The following figures shows the overview of the above mentioned schemes.

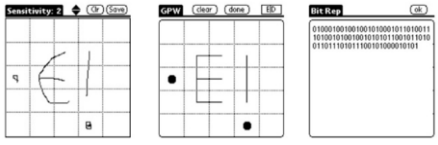

Figure 1: (a) User inputs desired Secrete, (b) Internal representation, (c) Raw bit string

Figure 2: Passfaces system. Left: sample panel from the original system [13]. Right: panel with decoys similar to the image from the user's portfolio [14].

All of the above images are directly extracted from the research papers. Based on the PassFaces and PassPoints schemes the researchers have developed the technique known as the PassMatrix technique for the graphical authentication. The PassMatrix technique is implemented on the android device. In the given proposed system the technique of PassMatrix is supposed to be implemented on the web application, and with few changes.

PROPOSED WORK

The proposed system is based on the PassMatrix scheme which has been recently developed by Hung-Min Sun, ShiuanTung Chen, Jyh-Haw Yeh and Chia-Yun Cheng in 2016. In this authentication scheme to make it shoulder surfing resistant scroll bars are used and one time password is generated. The following figure shows the components of the System. The system is proposed to be implemented on the web. The difference in this method and the earlier proposed method is that, the login indicator is generated once, and all\ the images for authentication is displayed on a single web page.

The modules of the proposed system are listed below;

- Image Discretization Module
- Login Indicator Module
- Horizontal and Vertical Axis control Module
- Communication Module
- Password Verification Module
- Upload/Download Module
- Database Module (Encryption with Homomorphic technique)

The system is mainly divided in two phases, these phases are registration phase and the login phase. In the registration phase the user has to input some basic information and have to select the image, and make one of the passimage as his/her password. The user can decide the grid of the images, and selects multiple images. Then in the login phase the login indicator has been generated and sent as an OTP to the user, then the user has to set the horizontal and vertical axis to the particular passimage and finally the user get authenticated. The main module is the Database which is encrypted by using the homomorphic encryption technique, in which encryption without decryption has used.

CONCLUSION

Graphical passwords can perform well on the web applications also. The proposed system is in future work can be implemented on the web application. Graphical authentication systems can be more useful than that of the conventional authentication schemes.

REFERENCES:

[1] "55% of net users use the same password for most, if not all, websites. When will they learn?" https://nakedsecurity.sophos.com/2013/04/23/users same-password most-websites/

[2] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[3] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[4] "Realuser," http://www.realuser.com/.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[6] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no.1-2, pp. 102–127, 2005.

[7] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[8] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.

[9] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.

[10] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference in Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.

[11] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.

[12] G. E. Blonder, "Graphical passwords", in Lucent Technologies, Inc.,Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.

[13] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.

[14] T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008.