INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY ON TRUST BASED AUTHENTICATION PROTOCOL

Sharmila .A

PG Scholar, Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Vattamalaipalayam, NGGO Colony (PO), Coimbatore, Tamilnadu, India.
sharmie.331@gmail.com

Abstract: - Text passwords are mostly preferred for authentication on websites due to its convenience and simplicity. However, user's passwords are prone to different threats and vulnerabilities. In the modern cryptographic methods the interruption by the third party is quite difficult but still the threats do exist. The user authentication protocol proposes the Opass enhancement to protect user identity. Opass is efficient and affordable compared with the conventional web authentication mechanisms. The Opass user authentication protocol performance have been enhanced of for accessing services. Online shopping is done in an efficient and secured manner in a website by adopting user authentication protocol.

Keywords: Password, Authentication, Opass, Security, Cryptography.

I. INTRODUCTION

People now-a-days rely heavily on the Internet since conventional activities or collaborations can be achieved with network services (e.g., web service). Widely deployed web services facilitate and enrich several applications, e.g., online banking, e-commerce, social networks, and cloud computing. But user authentication is only handled by text passwords for most websites and it is not safe at all occasions. So, user authentication is developed further to make online shopping and banking more secure.

Opass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider (TSP) in registration and recovery phases for the creation of the one-time password. Each time the user perform a login, a long-term password is used to generate a chain of one-time passwords. The generated password is used to find the authorized user and protect the system from the unauthorized users. The password is generated each time the user performs a login ensuring the authorization of the user.

User can recover Opass system with reissued SIM cards and long-term passwords. In case the authorized user forgets the password they can recover it. The Opass system is build considering the convenience and the information security of the client.

II. BACKGROUND STUDY

1. PASSWORD MANAGEMENT STRATEGIES

The paper [1] proposes Password security is an essential form of user authentication both on the Internet and for internal organizational computing systems. The FBI found in a recent survey that detected system penetrations from outside the organization were reported by 40% of the organizations surveyed, up from 25% a year earlier. Extensive literature on password security has evolved over the past 20 years.

In [10] the use of password authentication in on- line correspondence, subscription services, and shopping, there is growing concern about identity theft is proposed. When people reuse their passwords across multiple accounts, they in- crease their vulnerability; compromising one password can help an attacker take over several accounts. Our study of 49 undergraduates quantifies how many passwords they had and how often they reused these passwords. The majority of users had three or fewer passwords and passwords were reused twice. Furthermore, over time, password reuse rates increased because people accumulated more accounts but did not create more passwords. Users justified their habits. While they wanted to protect financial data and personal communication, reusing passwords made passwords easier to manage. They sometimes failed to realize that personalized passwords such as phone numbers can be cracked. We also present potential changes in website authentication systems and password managers.

In [4] the author report the results of a large scale study of password use and password re-use habits. The study involved half a million users over a three month period. A client component on users' machines recorded a variety of password strength, usage and frequency metrics. This allows us to measure or estimate such quantities as the average number of passwords and average number of accounts each user has, how many passwords she types per day, how often passwords are shared among sites, and how often they are forgotten. The data is the first large scale study of its kind, and yields numerous other insights into the role the passwords play in users' online experience.

2. GRAPHIC BASED PASSWORD

The underlying issues relating to the usability and security of multiple passwords are largely unexplored is proposed [3]. This reduces security since users reuse the same password for different systems or reveal other passwords as they try to log in. In a one-hour session (short-term), we found that participants in the graphical password condition coped significantly better than those in the text password condition. In particular, they made fewer errors when recalling their passwords, did not resort to creating passwords directly related to account names, and did not use similar passwords across multiple accounts. In our study, click-based graphical passwords were significantly less susceptible to multiple password interference in the short-term, while having comparable usability to text passwords in most other respects.

The paper [7] propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text- based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In this work we are primarily motivated by device such as personal digital assistants (PDAs) for graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm Pilot TM.

The passwords provide security mechanism for authentication and protection services against unwanted access to resources is proposed [11]. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart mobile devices (like smart phones i.e. iPod, phone, PDAs etc.) which are more handy and convenient to use than traditional desktop computer systems.

In the paper [9] proposed that the man-in-the middle attacks pose a serious threat to SSL/TLS based electronic Commerce applications, such as Internet banking. In this paper, we argue that most Deployed user authentication mechanisms fail to provide protection against this type of attack, even when they run on top of SSL/TLS. As a possible countermeasure, we introduce the notion of SSL/TLS session-aware user authentication, and present different possibilities for implementing it. More specifically, we start with a basic implementation that employs impersonal authentication tokens. Afterwards, we address extensions and

enhancements and discuss possibilities for implementing SSL/TLS session-aware user authentication in software.

The textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords [8]. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

3. PASSWORDS WITH COLORS AND TEXT

A highly severe menace to any computing device is the impersonation of an authenticate user. The most frequent computer authentication scheme is to use alphanumerical usernames and passwords. But the textual passwords are prone to dictionary attacks, eves dropping, shoulder surfing and social engineering. As such, graphical passwords have been introduced as an alternative to the traditional authentication process. Though the graphical password schemes provide a way of making more user-friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing [2]. To address this problem, text can be used in combination with the colors and images to generate the session passwords, thereby making a stronger authentication means. This method is most apposite to the PDAs besides other computing devices, as it is resistant to shoulder surfing.

In [12] the alphanumerical authentication systems nowadays always encounter the balancing problem between security and usability has been proposed. A weak password is easy be to remembered but it is also easy to be guessed while a strong password is harder to be guessed but it is also harder to be remembered. Thus, many automated attacks are designed to break the alphanumerical password. Graphical password system can overcome this problem by creating secure and memorable passwords. The basic idea of graphical password is that human can remember pictures better than an alphanumeric string. The primary objective of this project is to develop a graphical authentication system that is usable and secure. In addition, we applied fuzzy logic methods to enhance the usability by allowing certain degree of tolerance during authentication. Different types of pass images were also tested. From the implementation, the proposed scheme is able to provide larger password space and reduces registration and authentication time. Nature scene images that have the most key points are most suitable to be used in this scheme.

4. SCALABLE SHOULDER-SURFING

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder surfing. In this paper [6], a Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) is proposed. S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-camera and spyware attacks. It can replace or coexist with conventional textual password systems without changing existing user password profiles. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS shows significant potential bridging the gap between conventional textual password and graphical password. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical analysis of the security level using S3PAS is also investigated.

The Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session. In this paper, we propose and evaluate a new shoulder-surfing resistant scheme which has a desirable usability for PDAs. Our inspiration comes from the drawing input method in DAS and the association mnemonics in Story for sequence retrieval. The new scheme in [6] requires users to draw a curve across their password images orderly rather than click directly on them. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shoulder surfing. A

preliminary user study showed that users were able to enter their passwords accurately and to remember them over time.

III. CONCLUSION

Even though there are many proposals on text password, graphical password, It is been concluded that there can be chances of unsecure log in. So, to make a secured log in a user authentication protocol is been proposed and channelized.

REFERENCE

[1] Blake Ives, Kenneth R. Walsh, and Helmut Schneider, "The Domino Effect of Password Reuse", Communication ACM, vol. 47, no. 4, pp. 75-78.2004.
[2] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.VenkateswaraReddy,et al., "Authentication techniques for Engendering session passwords with colors and text", AITM, Vol. 1, No. 2, pp. 71-78, 2012.
[3] Chiasson.S, Forget.A, Stobert.E , Van Oorschot .P. C, and R. Biddle, "Multiple password interference in text Passwords and click-based graphical passwords" in CCS 09: Proc. 16th ACM Conf. Computer Communications Security, New York, pp. 500–511,2009ACM.
[4] Florencio.D and Herley.C, "A large-scale study of web password habits" in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, pp. 657–666, 2007ACM.
[5] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu, "A new graphical password scheme resistant to shoulder-surfing", 2010.
[6] Huanyu Zhao and Xiaolin Li, "S3pas: a scalable shoulder-surfing resistant textual-graphical password Authentication scheme", 2009.
[7] Ian Jermyn, Alain Mayer, Fabian Monrose,Michael K. Reiter, and Aviel D. Rubin, "The Design And Analysis Of Graphical Passwords" in SSYM'99:8th conf. USENIX security Symp., pp. 1-1, Berkeley, CA, 1999.
[8] M sreelatha M shashi , Manirudh , Md sultan ahamer , V manojkumar, "Authentication Schemes for Session Passwords using Color and Images" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011
[9] Rolf Oppliger, Ralf Hauser, and David Basin "SSL/TLS Session-Aware User Authentication Or How to Effectively Thwart the Man-inthe-Middle", 2007
[10] Shirley Gaw and Edward W. Felten, "Password Management Strategies For Online Accounts" in SOUPS'06: Proc. 2ndSymp. Usable Privacy. Security, pp. 44-55, ACM, New York, 2006
[11] Wazir Zada Khan, Mohammed Y Aalsalemand Yang Xiang, "A Graphical Password Based System for Small Mobile Devices" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.
[12] Woo Chaw Seng, Yong KokKhuenand Ng Liang Shing, "Enhance graphical password by using dynamic Block-style scheme", 2011.