ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 55 - 58 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

WEB BASED SECURITY ANALYSIS OF OPASS AUTHENTICATION SCHEMES USING MOBILE APPLICATION

K.Shruthi
Dept, College:**MRIET**
Hyderabad

L. Naresh Babu
Dept, College:**MRIET**
Hyderabad

ABSTRACT

Graphical password, text password are authentication of users on websites because of its simplicity and easy. User's passwords are easy to hack by using different malicious programs and threats. First, Users select easy to remember password because nowadays they using many accounts on different websites. To login to websites they need to remember all passwords. So users would choose easy to remember passwords, but these passwords are not safe. Reusing passwords across different websites may cause users to lose their information which is stored in websites once the password hacked or compromised by attacker. Second, hackers can install malicious software to get the passwords, when user typing their username and password into unknown public computers. In this paper, developing web based security analysis of one Time password authentication schemes using mobile application. A user authentication protocol which involves user's cell phone and short message service to prevent password stealing and reuse attacks. User's only need to remember a long term password for login on different websites.

Keywords: Authentication, Hacking, Analysis, Stealing

INTRODUCTION

Password-based user authentication has a problem that humans are not able to remember all passwords. Because, most users would chooseeasy-to-remember passwords even if they know the passwords might be unsafe. Another crucial problem is that users reuse passwords across various websites . For online accounts, users are at the same machine but access many different accounts . The average user has 6.5 passwords, each of which is shared across 3.9 different websites. Each user has about 25 accounts that require passwords, and types an average of 8 passwords per day. Users would choose weak passwords to remember easily. Users forget passwords a lot: we estimate that at least 1.5% of Yahoo users forget their passwords each month..Graphical passwords are an alternative to text passwords, whereby a user is asked to remember an image (or parts of an image) instead of a word. Humans have difficulty remembering complex or meaningless passwords. PassPoints involves a user creating a five-point click sequence on a background image. Scalable attacks require that the attacker collect sufficient"human-computed" data for the target image, which is morecostly for systems with multiple images. This leads to ask whether more scalable attacks exist, and in particular, effective fully automated attacks. An attacker may install a malicious program such as a keystroke logger that can observe and modify a

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 55 - 58 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

legitimate software environment, compromise modifiable software such as the BIOS, or add malicious hardware such as a USB sniffer. Each of these attacks poses password stealing attacks.

EXISTING SYSTEM

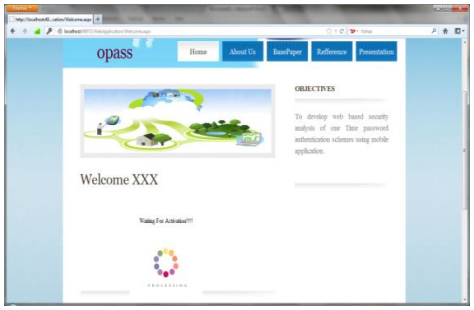
People have access to a computer and the Internet when logging into online accounts, able to show the technology they used did not help them with recalling their passwords. The nature of online accounts and tools for managing passwords in online accounts enable poor password practices rather than remembering them . The data allows us to measure for the first time average password habits for a large population of web users. A Large Scale Study of Web Password Habits able to estimate the number of accounts that users maintain the number of passwords they type per day, and the percent of phishing victims in the overall population.Graphical passwords are more robust than text passwords against multiple password interference (assuming distinct background images). Users could more easily remember multiple graphical passwords than multiple text passwords. Graphical passwords is at least part of the reason for better user performance and that cueing should be part of any recall based authentication scheme.Purely Automated attacks could be used to help inform more secure design choices in implementing Pass Points-style graphical passwords. Proactive checking rules for Pass Points style graphical passwords might be created based on the click order pattern attacks.A user can perform the majority of browsing interactions from the PC and only perform very sensitive interactions from the PDA (Personal Digital Assistant). Session Magnifier enables a user to fully take advantage of the convenience of using a Pc.

PROPOSED SYSTEM

The Objective of web based security analysis of opass authentication schemes using mobile application is free users from having to remember or type any passwords into untrusted public computers for authentication. A user authentication protocol which involves user's cell phone and short message service to prevent password stealing and reuse attacks. The cell phone, which is used to generate one-time passwords and SMS, which is used to transmit authentication messages between web server and trusted mobile devices. Users only need to remember a long-term password for login on all websites.A user authentication protocol has to develop mainly for overcoming below two major problems. First, Forget the Password so the user didn't Login any one Website and he/she can't access any information from that's website. Second Reusing passwords causes a domino effect, when an adversary compromises one password, adversary will exploit it to gain access to more websites. Hacker Applying Random-Key Functional Method for Hacking the user password.Users are able to log into web services without entering passwords on their computers. Thus, malware cannot obtain a user's password from untrusted computers. opass schemes achieves one-time password approach. The cell phone automatically derives different passwords for each login. The password is different during each login. Under one-time password approach, users do not need to remember any password for login. They only keep a long-term password for accessing their cell phones.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 55 - 58 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India



RESULT

The Registration and login performance is quite important for web authentication. Table I shows performance that the average time of login is 21.62 s, and the SMS delay time is 8.9 s.

TABLE

Registration		Login	
SMS delay	total	SMS delay	total
Avg time 9.1	21.g	8.9	21.6
min, max(6, 12)	(11, 59)	(7, 12)	(17,32)
a 1.72	14.05	1.45	4.05

CONCLUSION

A user authentication protocol which involves user's cell phone and short message service to prevent password stealing and reuse attacks. User's only need to remember a long term password for login on different websites. Web based security analysis of opass authentication schemes using mobile application is acceptable and reliable for users. The performance of login of opass schemes is better than graphical and text password schemes. In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authenticating the user referring to credentials presented by the user. This protocol applied in many security areas such as, Networking, Online business, Government sectors, Military sectors. password recovery is also considered and supported when users lose their cell phones.

FUTURE WORK

To make a user authentication protocol fully functional, password recovery is also considered and supported when users lose their cellphones. They can recover the system with reissued same SIM cards and long-term passwords.

REFERENCES

[1] B.Ives, K. R.Walsh, and H.Schneider, "The domino effect of password reuse," Commun. vol.47, no.4, pp.75-78,2004, ACM.

[2] s. Gawand E. W. Felten, "Password management strategies for onlineaccounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy SecuritY,New York, pp.44-55,2006,ACM.

[3] D. Florencio and C.Herley, "A large-scale study of web password habits," inWWW·07:Proc.16thlnt. Co.!!World Wide Web., New York, pp.657-666,2007, ACM.

[4] S. Chiasson, A. Forget, E. Stober!, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in CCS '09: Proc. 16th ACM Con! Computer Communications Security, New York, pp.500-511,2009,ACM.

[5] I.Jermyn, A.Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, 'The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Co,!! USENIX Security Symp., Berkeley, CA, 1999, pp. 1-1, USENIX Association.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 55 - 58 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

[6] P. van Oorschot, A. Salehi-Abari, and .I. Thorpe, "Purely automated attacks on passpoints-stylegraphical passwords," IEEE Trans. Information Forensics Security, vol.5, no.3, pp.393-405,Sep.2010.

[7] N.Provos, D. Mcnamee, P.Mavrommatis, K. Wang, and N.Modadugu, "The ghost in the browser: Analysis of web-based malware," in Proc.1st Co,!! Workshop Hot Topics in Understanding Botnets, Berkeley, CA,2007.

[8] s. Garriss, R. Caceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang,"Trustworthy and personalized computing on public kiosks," in Proc. 6th Int. Conf Mobile Systems, Applications Services, pp. 199-210, 2008,