International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

GENERIC AUTHENTICATION SYSTEM

Veena Bhawani[1], Varsha Chaudhary [2], Pranav Lawate [3], Dr. D.V. Patil[4]

[1]Bachelor of Engineering, Department Of Computer Engineering, GESRHSCOE, Nashik, Maharashtra, India
[2] Bachelor of Engineering, Department Of Computer Engineering, GESRHSCOE, Nashik, Maharashtra, India
[3] Bachelor of Engineering, Department Of Computer Engineering, GESRHSCOE, Nashik, Maharashtra, India
[4] Assistant Professor, Department Of Computer Engineering, GESRHSCOE, Nashik, Maharashtra, India

---

Abstract - ***Since the beginning of era of personal computation there is growing need of security in ample number of fields. With increased number of devices per person, authentication becomes crucial. For providing solution to this issue, a new paradigm of security primitives emerged.***

In Today's world mostly alphanumeric passwords (string password) are used which are vulnerable to many types of attacks i.e. Dictionary attacks, DOS attacks ,Bot attacks etc. and graphical passwords suffer because of some vulnerabilities like Shoulder Surfing attacks. In this project we are designing an API which will be generic for authentication purpose provided to web application service providers named as "Generic Authentication System".

Our system accommodates and integrates legacy methods viz. string passwords and graphical passwords with abating drawbacks by collaboration and provides a novel and a better approach. GenAuth is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security..

Key Words: *Alpha Numeric password, Graphical password, Dictionary attack, shoulder surfing attacks, GenAuth.*

1. INTRODUCTION

In Today's world we deal with information. Information generally is, an answer to the question, as well as that which knowledge and data can be derived. This information may be personal information like bank account details, contact details, residential detail, etc. It may be social information like details sheared on social networking sites i.e. facebook, twitter, etc.

Putting your data on some website's server appears disconcerting to many provided. The website is legitimate and will not use your data without proper consent, there is a probability of leakage of your data because of compromised Security. As a Result, potentially sensitive data, bank details are at paramount risk. Authentication is the principal method to guarantee information security and the most common and convenient method is password authentication. Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to essentially all users. However, there are several inherent defects and deficiencies in alphanumeric passwords, which easily evolve into security issues. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember. Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack. Today users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security. Moreover, alphanumeric passwords are vulnerable to shoulder surfing attack, spyware attack and social engineering attack etc.

Motivated by the promise of improved password usability and security, the concept of graphical passwords was proposed in 1996. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words. Graphical passwords are vulnerable to shoulder-surfing attacks through direct observation or video recording.

Here we integrated string password and graphical passwords. So system provides better security and usability and appears to fit well with some practical applications. Our system aims at providing a novel and better way of authentication for web sites as well as applet supporting projects.

2. RELATED WORK

According to the taxonomy devised by L.Vasiu and I.Vasiu[1], password attacks can be grouped into three different categories: guessing, cracking, and harvesting.
If the password can easily be guessed, then this is a clear indication of a weak password set by the user. In some cases the password is set to be the same as the username, full name or birth date of the victim. If the password can be found using special software or algorithms, then that password is cracked. Finally, if the attacker manipulates their victims physically and/or psychologically so as to retrieve their passwords, this is referred to as password harvesting.

The authors believe the system is still vulnerable to shoulder-surfing attacks through direct observation or video recording. Man et al[2]. propose an alternative form of graphical passwords, where icons presented to the user have a number of variations (creating convex hulls)and thus limiting the attacker's ability to identify the correct password. A follow up study by the authors is still in progress, where they plan to mathematically prove the resistance of this system to shoulder-surfing.

Suo[3] proposed a shoulder surfing resistant scheme based on PassPoints. During login, the image is blurred except for a small focus area. Users enter Y (for yes) or N (for no) on the keyboard, or use the right and left mouse buttons, to indicate if their click-point is within the focused area. This process repeats 5 to 10 times. It is easily guessed by attackers if the click points are too few.

A similar technique, visKey[4], was developed by Sfr, and is a commercial version of PassPoints for the PPC (Pocket Personal Computer). This scheme is used for screen-unlock by tapping on a correct sequence of click-points with a stylus or finger. VisKey PPC combines easy handling with high security for mobile devices. Just a few clicks in a picture may offer a large theoretical password space.

To reduce hotspots and improve usability of click based graphical password schemes, Chiasson et al[5]. proposed Cued Click-Points (CCP), a variation of Pass-Points in which users click on one point per image for a sequence of images. The next image is displayed based on the location of the previous click-point, that is, each image after the first is a deterministic function of the current image and the coordinates of the user-entered click-point. If users click an incorrect point, a wrong image will be displayed. It is meaningless to attackers without knowledge of the correct password. However, analysis of user choice revealed that users tended to select click-points falling within known hotspots.

3. GOALS AND OBJECTIVES:

Objectives are as follows,

1. The main objective of our system is to offer reasonable security and usability.
2. Fit with practical online applications and improve online security.

4. PROPOSED WORK:

The proposed system uses combination of alphanumeric password (string passwords) and graphical password to provide better authentication. Proposed system provides a novel idea for authentication using image with traditional String Password. Co-ordinates of the image and alphanumeric keys will be stored at master record (Server). We keep mapping the credentials with users account. As per this mapping authenticity of logging user can be determined. Here we integrated string password and graphical passwords, So system provides better security and usability and appears to fit well with some practical applications.

5. SYSTEM ARCHITECTURE:

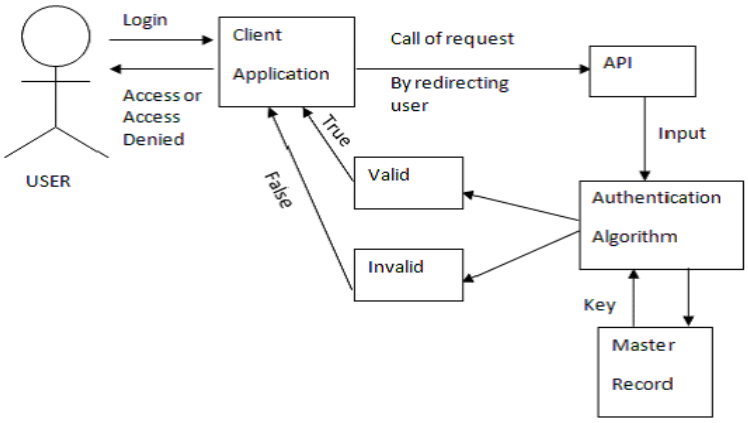

Fig -1: System Architecture

The Architecture diagram shows Client Application is Redirects the user to authentication server through provided API. Authentication Algorithm (Server) is checks further valid co-ordinates. Valid co-ordinate and alphanumeric keys stored in Master Record. When authentication is valid it returns true. When authentication is invalid it returns false.

5. CONCLUSIONS

We propose Generic Authentication System, a new novel and better security primitive relying on unsolved hard AI problems. Generic Authentication System is both graphical and an Alphanumeric password scheme. The notion of

Generic Authentication System introduces a new family of graphical passwords with together, which adopts a new approach to counter online guessing attacks which is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of Generic Authentication System can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack.

The proposed system is an API which will be Generic for Authentication purpose provided to web application service provided named as "Generic Authentication System". It offer reasonable security and usability. Appears to fit with some practical online application for improving online security. It also, defence against online attacks.

ACKNOWLEDGEMENT

We would like to take this opportunity to thank our guide **Dr. D.V. Patil** for giving us all the help and guidance we needed.

REFERENCES

[1] L. Vasiu and I. Vasiu, "Dissecting Computer Fraud: From Definitional Issues to a Taxonomy," presented at 37th Hawaii International Confernces on System Sciences, Hawaii, 2004.

[2] S. Man, D. Hong, B. Hayes, and M. Matthews, "A password scheme strongly resistant to spyware," presented at Int. Conf. on Security and Management, Las Vegas, NV, 2004.

[3] X. Suo, Y. Zhu, and G. Owen. "Graphical passwords: A survey". In Annual Computer Security Applications Conference (ACSAC), December 2005.

[4] "Sfr",www.sfr-software.de/cms/EN/pocketpc/viskey /index.html, site accessed in Oct, 2012.

[5] S. Chiasson, P.C. van Oorschot, and R. Biddle. "Graphical password authentication using Cued Click Points". In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[6] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems," in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[7] Haichang Gao, Wei Jia, Fei Ye and Licheng Ma, "A Survey on the Use of Graphical Passwords in Security," in Institute of Software Engineering, Xidian University, Xian, P.R.China, JOURNAL OF SOFTWARE, VOL. 8, NO. 7,JULY 2013.

BIOGRAPHIES:

Veena Bhawani is currently a student of GESRHSCOE, Nashik from the University of Savitribai Phule, Pune. Her main research interests include:
a)Web-Mining
b)Object oriented programming
c) Web-Designing.

Varsha Chaudhary is currently a student of GESRHSCOE, Nashik from the University of Savitribai Phule, Pune. Her main research interests include:
a)Data-Mining
b)Object oriented programming
c) Web-Designing.

Pranav Lawate is currently a student of GESRHSCOE, Nashik from the University of Savitribai Phule, Pune. His main research interests include:
a)Security
b) Java programming
c) Server Administration.