iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4247

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secured Login Authentication on Key Attackers

K.Vanitha[1], M. Manikanta[2], M. Suresh Kumar[3]
[1,3] Assistant professor, [2]PG Student, Department of Computer Science
GIS, GITAM University Visakhapatnam

Abstract: ***An innovative solution is proposed to avoid the problem such as password security at application layer. For password security all lower case characters, upper case characters, special characters and digits in password could be encoded with a random single digit integer number and presented to the user through a Login input interface module. If a valid user enters his password in the form of the sequence code or numeric value from the login input interface module then that describes his password code in place of his actual password characters and for every time solution engine regenerates a new numeric value. When user enters password for each character each time the carriage return key is struck and this approach is known as key logger attack producing and this toughened password is more secure than a conventional password scheme.***
Keywords: Key Attackers, Authentication, Secure login interface.

I. INTRODUCTION

The password assists in ensuring that the authorized user only can access the resources and the unauthorized user not to access the resources. In the many resources the password length is inappreciable, which makes easier to spy and memorize them. The passwords can be monitored through keystrokes or eavesdropping. In an organization or company every user has unique password to use system resources and many employee presence around him. The Personal Identification Number (PIN) is always used by banks to allow their customers access to their online banking facility. Often banks provide users a small length PINS for the customers' convenience that is easy to remember but this advantage creates attacker to memorize the password. In this paper, we make a spy-resistant password entry module which looks as a Keyboard or virtual keyboard to improve more security on publicly observable. This approach gives a liberty to user and it is hard to guess and change them frequently. So the user enters a randomly generated single integer value in place of characters and this makes much difficult to crack through brute force attack and other attacks, because brute force attack attempt to discover/guess the correct password by trying every possible key combinations of letters, numbers and symbols that will unlock the encryption until the spy find the right one. It could take few minutes or hours or years to discover, since it is depended on the password's length and complexity and there could be trillions of possible combinations.

Figure 1: An Architecture For Password Authentication

II. LOGIN INTERFACE MODULE

The Login interface module was generated in secure login interface. The module shows the password characters with their corresponding single integer value (in black box). User enter the numeric input value according to his password in password text box area, if a user take too more time to enter password then login interface will be refresh and the randomly generated integer values corresponding to character, digits, special characters will be changed or user can do this itself by clicking on "Regenerate random number set " button. In this, first user registers his user id, password and mobile number and that will be stored in database in an encrypted form. The database DB, contains all the passwords of legitimate users. The database is designed to accept 200 and above characters length passwords but coder must restrict size of users' passwords to a reasonable length, for example 14 characters, for better security.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Figure 2. User Registration Form

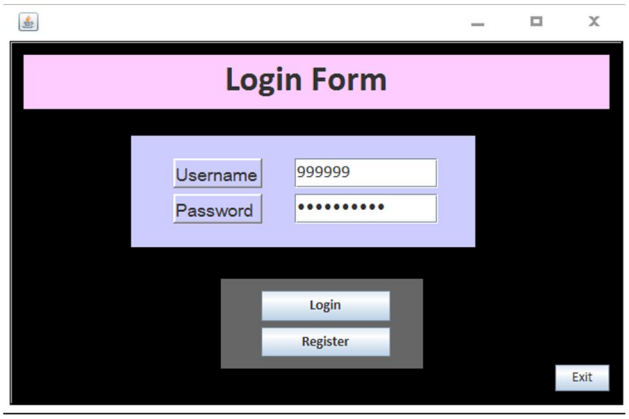


Figure 3. User Login Form

III. USER (SECURE) LOGIN INTERFACE

The user will login with a user id and password using secure login user interface as shown in figure 3. In this all characters will be printed in ASCII characters, which contain lower case, upper case, alphabets (A-Z, a-z), numeric digits (0-9), and special characters (+ - _ ^ , # % etc).

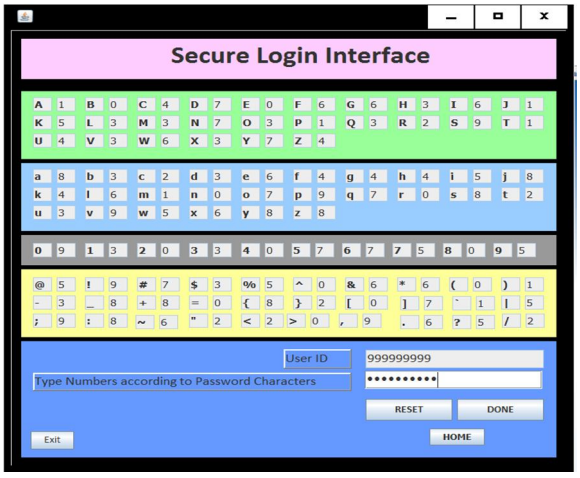


Figure 4. Secure login interface

User enters a single integer value corresponding to each character of his password. A new single integer value (0 to 9) will be generated corresponded to all characters, digits, special character etc. Whenever user needs to login he will enter password in the form of randomly generated single integer value correspond to valid password characters after studying the secure login user

interface, If user password length = = original password is false then a message is displayed as “incorrect password”. Else a message is displayed as “login success”. In this paper we use a jagged array[ ] in which all user input integer values stored and to create another array namely occurrence[ ] which is used to store each characters separately accordingly to their correspond single integer value from zero to nine to generate randomly. It means it may be assigned to more than one characters.

In this paper we match the user input value to the original password one by one character. For example the given password is “Gitam@123” and its corresponding user input value will be 678967899. As shown in above figure 4 first user input value 4 will be matched with actual password first character ‘G’ if it is success then it goes to next otherwise move out and a message is shown such as “ Password Not Matched ” and if first character is matched then this process move next character until we find actual password.

IV. CONCLUSION

In this paper an approach Randomly generated single integer input digits corresponding to password characters on login interface module makes it not possible for attackers to hack with any technique such as brute force attack at input level (at application layer). The implementation of this algorithm is presented in net beans.

REFERENCES

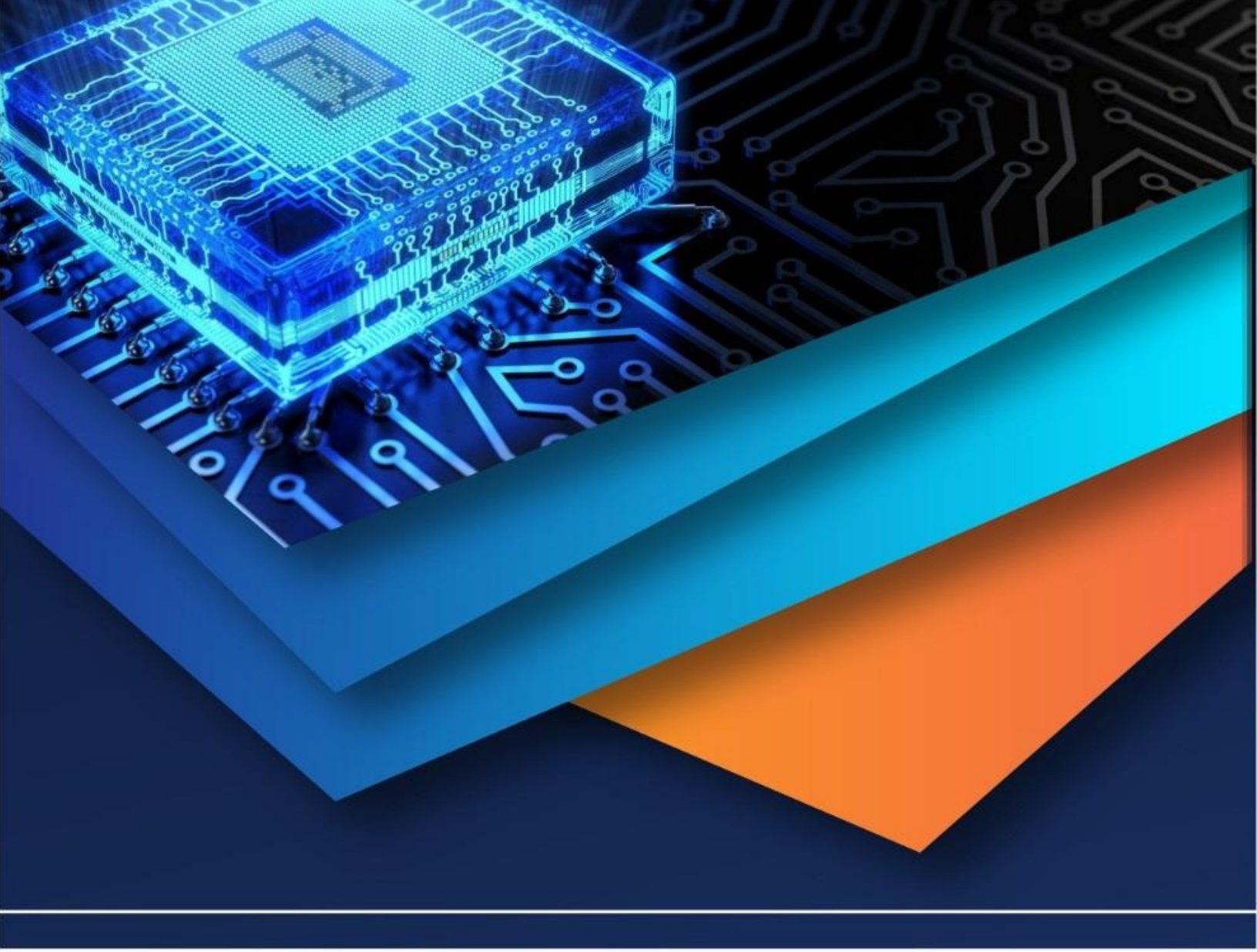
[1] Fujita, K. and Y. Hirakawa, 2008, “A study of password authentication method against observing attacks”,6th International Symposium on Intelligent Systems and Informatics, SISY 2008.
[2] Kessler, Gary C., 2002. Passwords - Strengths and Weaknesses. Jan-1996.
[3] G. Sowmya, D. Jamuna, M.Venkata Krishna Reddy, “Blocking of Brute Force Attack” International Journal of Computer Applications & Information Technology, Vol. I, Issue II, September 2012.
[4] Desney S. Tan, Pedram Keyani, Mary Czerwinski .“SpyResistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens”.
[5] Schneider, B., "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1996.
[6] Mathias Kolsch, Matthew Turk. “A Survey of Virtual Keyboards”, Dept. of Computer Science, University of California at Santa Barbara, CA.
[7] [Mark, 2005] Mark S., (2005), “Information Security, Principles and Practice”, Wiley Interscience.
[8] I. Scott MacKenzie, “KSPC as a Characteristic of Text Entry Techniques”, Dept. of Computer Science, York University Toronto, Ontario, Canada M3J 1P3.

BIOGRAPHY

K Vanitha is currently working as Assistant Professor in the Department of Computer Science, GIS, GITAM University. Her main areas of research include Cloud Computing and Data Mining.

M Suresh Kumar is currently working as Assistant Professor in the Department of Computer Science, GIS, GITAM University. Her main areas of research include Cloud Computing.

M. Manikanta Kumar pursuing Master of Computer Applications, GITAM Institute of Science, GITAM University, Visakhapatnam.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY