Improved CAPTCHA based Authentication for E-mail ID

K. Naveen1*, S. Saravanan1, M. Lavanya1 and V. Vaithayanathan2

1School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; krishnamoorthi.naveen@gmail.com, saran@core.sastra.edu, m_lavanyass@ict.sastra.edu
2SASTRA University, Thanjavur - 613401, Tamil Nadu, India; vvn@it.sastra.edu

Abstract

This article aims to present the importance of authentication for E-mail ID through improved CAPTCHA based method. The structure of the CAPTCHA has to be reorganized to suit the user requirements to facilitate the authentication for E-mail ID. CAPTCHA is achieved by rearrangement of alphabets randomly on the buttons and it is very easy to frustrate by simple keyloggers. The motive of improving E-mail authentication is done by incorporating two factor visual authentication mechanisms. It is targeted to CAPTCHA based human interaction with sophisticated user friendly protocol. All the intermediate interaction is visualized by the user with better CAPTCHA code. It provides only one time (or) one session valid authentication through color grid rating method. This two layer authentication promises more secure in accessing any secure information based portal.

Keywords: Authentication, CAPTCHA, E-mail, Hacker Attack, Keyloggers

1. Introduction

The earliest user authentication mechanism through the Internet is based on password. The security of such systems is not always reliable. For example, poor password selections, the password capture Trojans, and the reuse of passwords could break the security. One popular attack is called dictionary attack, which targets to find the correct password by trying a large amount of likely possibilities, such as words in a dictionary or the likely combination of words. But even more sophisticated attacks like keyloggers are more troublesome for the users since a keylogger records all the users’ activity and when connected to the internet this data is sent to a remote hacker who then enters the clients application and thus breaches the security system. The user then logs in for a transaction from the terminal. The password is verified in the server.

2. Existing Methods

Several research works has been already carried out in this field, particularly user information authentication and security. In paper1 authentication is provided by using Images. It focuses on the fundamental weakness based on knowledge-based schemes, which shows human limitation to remember authenticated password. Recall-based authentication method hides users from choosing poor passwords and makes it very difficult to share passwords with others.

In paper2 graphical password schemes was proposed. It exploits the fundamental features of graphical input information displays to achieve proper authentication and security than basic text-based authentication of passwords. The given graphical input devices always enable the user profile to decouple the position (or) state of the given inputs from temporal data and it shows that this decoupling method can be used to produce authenticated password schemes with huge memorable password.

In paper3 it focuses on user identification system and it protects information from illegal way of access. Each system has its own identification standard for keyboard or mouse. Mouse is used as a user to identification system and proposed a complex figure object and signature. This includes making normalization of the given input data,
with new signature adaptation, evaluation of verification data using geometric average value and its dynamic update of database. Still this method has various disadvantages of authentication of user profile.

In paper 4 Graphical password survey is presented with various authenticated usernames and passwords. This paper addresses this problem and forces the researchers to develop new authentication methods for privacy information authentication. Graphical Password Scheme for resistant to shoulder-surfing is proposed in paper 5. Authentication based password is used as direct observation or by recording the session. Visual interface based graphical password is adopted in this paper. But this method has significant usability drawbacks in time and effort time of log in. So curve based password images were used.

Longitudinal evaluation 6 password system is discussed about clicking on images is proposed rather than typing alphanumeric letters/strings. Two groups of longitudinal trials were used. But using graphical information will take more time in given protected password.

In paper 7,8 user authentication for mobile device through image selection is proposed. Analyzing several visual techniques for authentication of mobile device users is focused in this method. In paper 9 it is focused on phenomena as potential certificates of identity. Zero-knowledge protocols is used and it is used to minimize the amount of secret information which is store in the memory. This provides a better module to human-computer interfaces.

Doodling method 10 is focused about how user searching recalls all visual elements of the doodle, and also recalls alphanumeric passwords. Scalable based paper 11 shoulder surfing password authentication is proposed. The advantage of the textual password authentication is well known method. It replaces conventional textual input password systems into changing of earlier existing user password profiles. Brute-force attack through various dynamic and volatile passwords is also discussed.

3. Proposed System

This proposed system overcomes various demerits of earlier existing systems by modifying user terminal in its intermediate state with comfortable user-friendly protocol. Keylogging attack is prevented by legacy authentication. So no retrieval of information is needed. Mail based augmented reality is proposed in this work.

The visual involvement of users in a security protocol boosts both the security of the protocol and is re-assuring to the user because she feels that she plays a role in the process. Smartphone device can be used for visual security protocol. Basic design method is shown in Figure 1.

4. Advantages

Basically two techniques are proposed to generate session passwords. They are text, colors and a CAPTCHA Code. These above methods are suitable for all system to prevent attack against keylogging and malware.

Second visualization can enhance not only security but also usability by proposing two visual authentication protocols: One for password-based authentication, and the other for one-time-password. Through rigorous analysis, we show that our proposed protocols protect from information attacks. This proposed system also useful in real-world deployment which addressing user’s shortcomings and limitations.

5. Algorithm Steps

- To generate key
  Declare an integer variable ran
  Declare an double variable x
  Declare an integer variable secnum
  Set ran to r1.nextInt()
  Set x to (double)ran/integer.MAX_VALUE × 6999
  Set secnum to absolute value
  End.

Figure 1. Data flow diagram for proposed method.
To generate a key with less than 4 digits we use the formula random number divided with the maximum value of the integer multiplied with 6999. This will result a value which is assigned to the x. Since the key generated will be in an absolute value we convert the double to absolute value

- To generate the CAPTCHA file
  Declare a string variable s
  Declare s2
  Set s to secnum
  Set s to integer value
  For
  {  
    I is assigned to 0
    I < length-1
  Declare a string s1
  Set s1 to capfile from database
  {  
    Assign s2 to cap
    S2+=capfile
  }
  Print s2
  }
end
In this we generate the CAPTCHA file. The key is assigned to s. Then based on the key generated we select each CAPTCHA file from the database then it is assigned to string s2.

- To generate password combination
  Declare the string variable com
  For
  {  
    I assigned to 0 and I to I < length–1  
    While (key.next())
    {  
      Set tt to string value of pw
      {  
        For
        {  
          Set I to 0 and I < len–1
          Set cc to col
        }
        Pass=tt+cc
      }
    }
  }
In the above pw is the password. cc is the color code value. Pass is the password value. It is the textvalue. In this we combine the color code and the text password and we generate the new password every time for the key generated.

6. Modules

6.1 User Registration Module
Here the user registers his details. The user name should be unique. It is stored by an ID in the database. Next a valid email id is procured. The user is redirected to the next screen. The generated unique identity is shown to the user for his login purposes. Then he is redirected to the next screen, where the user is shown the alphanumeric textual password. Here the user submits a textual password which should be having a minimum length of the 8 characters and it is called as secret pass. It contains always even number of characters. This is validated and then stored in the user database. Next the user's id redirected to the next screen, where the user is shown the color screen.

6.2 Color Grid Deployment and Rating
Grids of 8 colors were displayed to the user and it can be selected by the login user. From 1 to 8 in any order the user can use. The user can remember it as "R-L-Y-O-B-G-I-P". User information provides unique color rating which depends of various grid sizes like 8×8 matrix. Random digits value from one to eight is placed properly in grid cells. Four pair of colors represented by row and column is used for user login. It also have two basic grids. One is color grid and another one is number grid, with 8×8 numbers and with 1 to 8 randomly placed in the grid. Row and column number grid will provide password.

6.3 CAPTCHA Module
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a one type of testing to determine whether the user is human or machine (or) automated tool. Distorted image is presented in the form of CAPTCHA. Obscured way of sequence letters and digits also appears in the login screen. Testing can be proved by attempting the authenticated user to login the system. CAPTCHAs are basically defined by fully automated and requires little human administration. This is authenticated by three separate abilities such that invariant recognition, segmentation, and parsing and it is used to correctly complete the task with any consistency.
6.4 E-mail Module
The generated CAPTCHA combination is sent to the users email id. The users then have to go to the corresponding mail id, login and find the CAPTCHA letters. This login is another step in user security. The person has to authenticate with the email and then only be able to use the CAPTCHA code. Next they have to find out the combination for the text and the appropriate color and enter it into the user login.

6.5 Verification Module
During this phase the system verifies if the combination is right for the text and color supplied for this session. If the generated session and decoded color text combination is accurate then only the user is allowed entry into the system otherwise the login fails. Due to dynamic session based passwords, dictionary attack is not applicable and other forms of phishing are also not possible. The system is resistant to a variety of attacks.

Figure 1 shows data flow diagram of proposed method. Table 1 shows the comparison of various methods with proposed method in terms of attack and security. This shows our proposed method can be more adoptable for E-mail ID authentication purpose.

7. Conclusion
In this paper two new authentication based techniques were proposed. They are based on text, colors and CAPTCHA text password based applications. These techniques authenticated passwords sessions and resistant to brute force attack, shoulder-surfing and dictionary attack. All the above said techniques uses grid of session passwords generation. In pair based method, no special type of registration is required. During login time, the grid displayed a session password and it is generated for authentication. To make hybrid textual CAPTCHA scheme, it is given and rated by various colors. Based on these key ratings, corresponding CAPTCHA is generated and it is sent via E-mail ID. During login, the session passwords are authenticated and the user is allowed access.

8. References
1. Dhamija R, PerrigA. Deja Vu: A user study using images for authentication. 9th USENIX Security Symposium; 2000. p. 4.
2. Jermyn I, Mayer A, Monrose F, Reiter M, Rubin AD. The design and analysis of graphical passwords. Proceedings of USENIX security symposium; 1999. p. 1.
3. Syukri AF, Okamoto E, Mambo M. A user identification system using signature written with mouse. 3rd Australasian Conference on Information Security and Privacy (ACISP); 1998. p. 403–41.
4. Blonder GE. Graphical passwords. Murray Hill, NJ: Lucent Technologies Inc. U. S. Patent; 1996.
5. Gao H, Ren Z, Chang X, Liu X, Aickelin U. A new graphical password scheme resistant to shoulder-surfing. International Conference on Cyberworld; 2010. p. 194–9.
6. Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N. Design and longitudinal evaluation of a graphical password system. International J of Human-Computer Studies. 2005; 102–27.
7. Jansen W. Authenticating Mobile Device User through Image Selection. Data Security. 2004. p. 1–10.
8. Jansen W. Authenticating users on handheld devices. Proceedings of Canadian Information Technology Security Symposium; 2003. p. 1–12.
9. Weinshall D, Kirkpatrick S. Passwords you’ll never forget, but can’t recall. Proceedings of Conference on Human Factors in Computing Systems (CHI); Vienna: Austria. 2004. p. 1399–402.
10. Goldberg J, Hagman J, Sazawal V. Doodling our way to better authentication. CHI ’02 Extended Abstracts on Human Factors in Computer Systems; 2002. p. 868–9.
11. Seng LK, IthninN, Mammi H. An anti-shoulder surfing mechanism and its memorability test. International Journal of Security and its Applications. 2012; 6(5):87–96.