Original Research Paper

Volume-9 | Issue-7 | July - 2019 | PRINT ISSN No. 2249 - 555X

Computer Science

RECALL BASED TEXTUAL PASSWORDS AUTHENTICATION SYSTEM

Yashaswini B M — M.Tech student, Computer Science & Engineering, BIT, Bengaluru, Karnataka, India

Madhuri J* — Assistant Professor, Dept. of Computer Science & Engineering, BIT, Bengaluru, Karnataka, India *Corresponding Author

ABSTRACT Textual passwords remain the most commonly employed user authentication mechanism, and potentially will continue to be so for years to come. Despite the well-known security and usability issues concerning textual passwords, none of the numerous proposed authentication alternatives appear to have achieved a sufficient level of adoption to dominate in the foreseeable future. Password hints, consisting of a user generated text saved at the account setup stage, are employed in several authentication systems to help users to recall forgotten passwords. However, users are often unable to create hints that jog the memory without revealing too much information regarding the passwords themselves. The proposed method involves rethink of password hints by introducing a novel cued recall-based textual password method that reveals no information regarding the password, requires no modifications to authentication servers, and requires no additional setup or registration steps. This will make use of users' contact lists, so that mapped password hints extracted from a user's contacts are automatically generated while the user is typing the password.

KEYWORDS : Textual passwords, Password hints, contact lists, user authentication, forgotten passwords.

1.INTRODUCTION

In the vast majority of authentication systems, textual password schemes are the dominant choice for authenticating end users, despite the well-known security issues concerning passwords, and the inconvenience incurred by end users in remembering multiple passwords for different accounts. Typically, users tend to choose easy-to-remember passwords that are also easy for adversaries to guess. In addition, security vulnerabilities, phishing of credentials, and poor security practices in storing password-related files have led to large-scale security breaches and an ongoing online trade of hundreds of millions of stolen usernames and passwords belonging to various accounts End users are often compelled to choose “strong” passwords (e.g., through password meters). However, security and usability trade-offs (e.g., password strength vs. memory and password strength vs. reuse) limit not only the ability of users to create unique and strong passwords for their accounts , but also increase the likelihood that users find such processes burdensome and irritating.

1.1 Problem Statement

To recall forgot textual passwords with the help of the password hints. The main dilemma concerning such password hints is that the more information a user's chosen hint provides regarding the password, the more likely it is that an attacker can guess the password by reading the password hint.

1.2 Proposed System

The work proposes a novel password hint scheme, which makes use of a user's contacts list, which constitutes an available and familiar information source to the user, to automatically generate an on the- fly, easy-to-remember password hint that is learned upon the first login. To use, a user must only mentally associate contact names from her contact list with the correct passwords. Other than setting up application at the installation stage, no additional setup or registration steps are required for a new user account.

2. LITERATURE SURVEY

In [1], the authors has compared and evaluated the effectiveness of currently known attacks using various datasets of the known passwords. The datasets concerning password hints are stored in the database. Then by accessing those databases the user will guess the password for the authentication to the system.

In [2], the authors have worked on comparing the recall of multiple textual passwords with the help of recalling the multiple click – based graphical passwords. The pass points marked in the figure will help in remembering of the password. This will help by connecting the dots with the help of user memory.

In [3], the authors worked in accomplishing the task by modeling the success rate of current password cracking techniques against real user passwords i.e., by determining the effectiveness of using entropy, as defined in NIST SP800-63, as a measurement of the security provided by various password creation policies.

In [4], the authors have worked on the need to underscore for more realistic evaluations of the use of multiple graphical passwords. In this study they have employed the multiple person's images in the form of set of 9 pictures in one grid. There can be any number of grids. User has to choose one picture from each grid that he had registered while authentication. When correct pictures are chosen the he will get an access to the system.

3. SYSTEM ARCHITECTURE

The system architecture is as shown in figure 1.

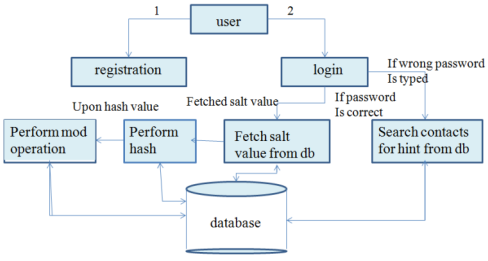


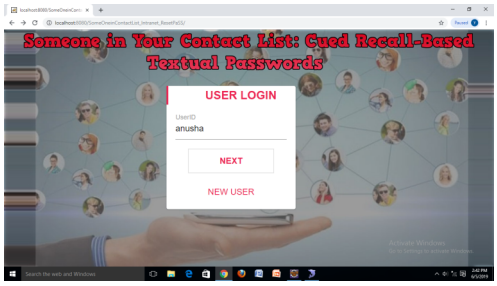
Fig -1: System Architecture

The architecture diagram depicts the overall picture of the process that has been take place. First the user has to register himself into the account by providing his details. Then on the successful creation of the registration, the password along with the salt value has been sent to the user through SMTP services. The salt value is generated at random and can be any length, in this case the salt value is 16 bytes long. The salt value is appended to the plain text password and then the result is hashed, this is referred to as the hashed value. Both the salt value and hashed value are stored Then by referring the above the user needs to enter the same when he first login into his account. Then the second time onwards there will be no need to type the salt value as it will be stored in the database and fetched from it. If the wrong password is typed then the relevant hint will be displayed to the user. Then again wrong password has been typed then the relevant next field will be displayed as hint to the user and so on until all fields are over then the message will be typed as invalid password.

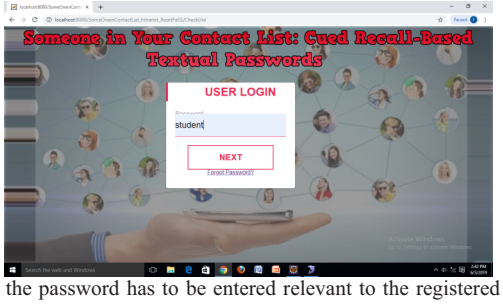
This will be used to authenticate into the user accounts. Many of the authentication systems uses text as passwords and it is the very popular nowadays. But many of them will ask the questions regarding to provide users with the hint password. But the adversaries can easily guess the password with the maximum number of hint answers provided by the user while authenticating into the account. This attempts will be reduced as the current method uses user contact

information as the hint for the password where the user only knows the proper information regarding his contacts. When someone else tries to authenticate he can't able to identify clearly about the displayed hint fetched from database.

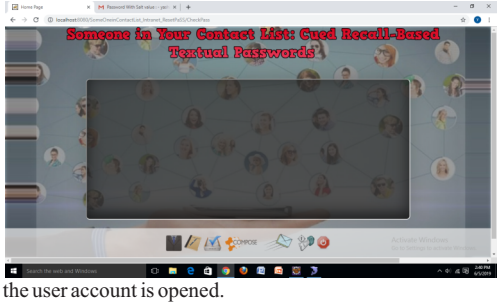
4. RESULT SNAPSHOTS



The registered name has to be entered in the login page.



Then the password has to be entered relevant to the registered user name.



Then the user account is opened.

When the user types the wrong password the relevant hint name is displayed which is fetched from the database.

5. CONCLUSIONS

The proposed system minimized the number of invalid login attempts, and improves the memory recall for textual passwords. Here the users' ability to recall passwords will improve over time after they begin to utilize password hints each time they enter their login credentials. But the work has to be made on minimizing users' need to resort to other verification methods to regain access to blocked accounts. Also the effort should be made on improving the accuracy and speed of recalling randomly generated passwords.

REFERENCES

[1] Matteo Dell'Amico, Pietro Michiardi and Yves Roudier, "Password Strength: An Empirical Analysis," in IEEE communication Society , IEEE, 2010.

[2] Sonia Chiasson , Alain Forget , Elizabeth Stobert , P.C. van Oorschot , Robert Biddle, "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords", page no. 500 – 511, ACM, 2009.

[3] Matt Weir, Sudhir Aggarwal, Michael Collins, Henry Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords", page no. 162 -175, ACM, 2010.

[4] Katherine M. Everitt, Tanya Bragin, James Fogarty, Tadayoshi Kohno, "A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords", page no.889 – 899, ACM, 2009.