ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (54-58), Month: October 2014 - March 2015, Available at: www.paperpublications.org

Multilevel Security and Authentication System

Pratik Anap[1], Sanjay Gholap[2] , Prasad Anpat[3], Abhijit Bhapkar[4]

[1,2,3,4] Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala, University of Pune, India

Abstract: **In an online security, authentication plays a crucial role in shielding resources against unauthorized and illegal use of information. Authentication processes may differ from simple password based authentication system to complex, costly and computation strengthened authentication systems. In recent days, increasing security has always been an important issue since Internet and Web Development came into actuality. Text based password is not enough to counter such problems, which is also an obsolete approach now. Consequently, this demands the need for something more secure along with being more user-friendly. Therefore, we have strained to rise the security by involving a multiple level security tactic, involving Text based using Cryptography, Grid Authentication and Image Based Password. The cryptography technique is very essential for the text based password while encrypting it with the principle of substitution method like Caesar Cipher. Session passwords are also necessary for eliminating the time factor attacks such as Brute Force attack. Grid Authentication makes the system more dynamic due ever changing nature. Image based authentication makes the system more user friendly, reliable and secure.**

Keywords: **Cryptography, Grid Authentication, Image Based Password, Shoulder Attack.**

I. INTRODUCTION

In Information and Network Security, authentication is an important term for dealing with the secure and confidential information which is of prime importance. Information can be protected with the help of passwords. These days' passwords are more than just a key. They serve several purposes. They safeguard our privacy, keeping our sensitive information sheltered. Passwords authenticate us to a machine to prove our identity-a secret key that only we should know. They also enforce non disclaimer, preventing us from later declining the legitimacy of transactions authenticated with our passwords. Our username identifies us and the password validates us. But passwords have some flaws: more than one person can possess its knowledge at one time. Moreover, there is a constant threat of losing your password to someone else with fatal intent. Password thefts can and do happen on a regular basis, so we need to protect them. Now merely using some random alphabets grouped together with special characters does not assure safety. We need something mysterious, something different along with being user friendly for our password, to make it secure. Besides being different it should also be light enough to be remembered by you and equally unbreakable to be hacked by someone else.

The study describes how the system works and how it eliminates the different attacks at client side, by employing the multilevel security system.

II. EXISTING SYSTEM

The existing security system consists of the simple level of authentication in which the rate of attacks can be at higher level. The system consists:

1. Simple Text Based Password

2. One Time Password

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (54-58), Month: October 2014 - March 2015, Available at: www.paperpublications.org

These are not sufficient to encounter the attacks or prevent them. Various attacks such as Shoulder Attack or Tempest Attacks may be possible in this system. To keep the information more secure we have introduced the different levels of security which would be essential to safeguard information.

III. PROPOSED SYSTEM

The unique and user-friendly levels in the multilevel security system are as follows:

- Text Based Authentication using Cryptography and Trusted Third Party Services.
- Grid Authentication
- Image Based Authentication

1. Text Based Authentication using Cryptography:

Security at this level has been imposed by using Text based password, which is a usual and now an anachronistic approach. For the text password to be more secure, use of Trusted Third Party can be done.

Cryptography: In modern science, cryptography is the study of techniques for secure communication in presence of Trusted Third Parties. We can construct and analyse the protocols that block the unwanted access to our system in any extreme cases. Two terms in cryptography are very much popular i.e. encryption and decryption. Modern cryptography is based on the mathematical models and scientific terms in computer science.

*Caesar Cipher***:** The action of Caesar Cipher is to replace each plain letter with a different one, a fixed number of places down the alphabet. The cipher illustrated here uses a left shift of three, so that each occurrence of E in the plaintext becomes B in the cipher text.

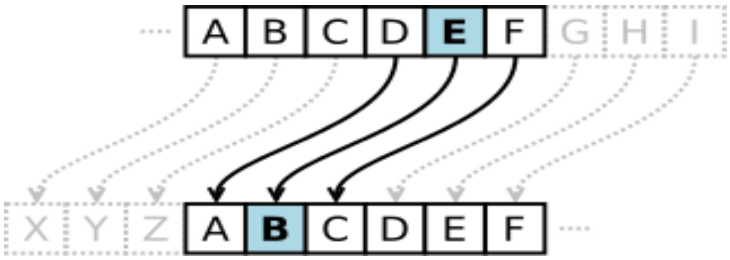

Figure 1: Caesar Cipher Technique

Technology: To implement this system, here we have used .Net framework 4.0 .NET Framework is Microsoft's comprehensive and consistent programming model for building applications that have visually stunning user experiences, seamless and secure communication, and the ability to model a range of business processes the .NET Framework 4 works side by side with older Framework versions. Applications that are based on earlier versions of the Framework will continue to run on the version targeted by default.

2. Grid Authentication:

In the Grid based authentication system we have grid structure of varying matrix sizes. For authentication system we have 6X6 Grid consisting of 26 alphabets and 0-9 numbers displaying in random manner. While registration, the user is asked to provide a private key which is basically a primary keyword for the grid structure. So, the password may be varying as the grid changes every time when user authenticates in the system. The pattern will be set for password to generate every time as grid shuffles the characters.

Grid based authentication is also an example of Session Based Authentication Technique.

What are Session Passwords?

Session passwords are passwords that are used only one time. Once the session is terminated, the session password is no longer useful. That means next time this password cannot work. For every login process, user's input different passwords.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (54-58), Month: October 2014 - March 2015, Available at: www.paperpublications.org

Algorithm: Pseudo Pair Matching Algorithm

Input: Row characters up to uses input and session user id Sid

Output: Session string for password matching

Step 1: Retrieve initial password from database of Xi user

Step 2: load grid GUI with 36 characters and numbers

Chars ={a,b,c,d……z},{0,1,2……..9}

Step 3: Take a two characters from Sid

sessionP $= \sum_{k=0}^{n}(k = 2)$

Step 4: Read the clickthrough from grid as r [] and c []

Step 5: foreach(j:r.length)

Foreach (k:c.length)

If(sessionP.equals(j,k))

Session follow;

Step 6: Repeat this step when Sid!=NULL.

Step 7: if all sessions==Sid then

Login success;

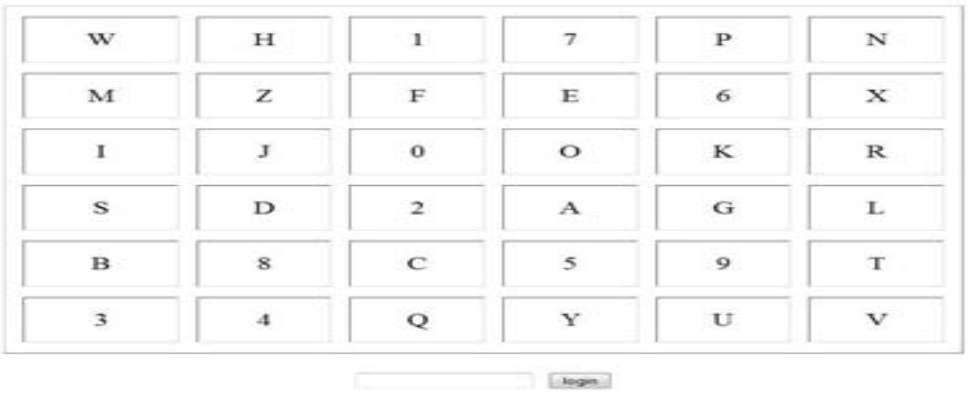

Figure 2: Login Interface

3. Image Based Authentication:

In the Image Based Authentication method, user is provided with the unique set of images at the time of registration. When the user selects the image, it is saved in the system as the default password for the next login session. In the image based authentication system, it doesn't mean to have a single image as password but another methods can also be implemented for registering the user by means of pattern recognition techniques or knowledge based authentication. By use of this technique the user can be prevented from different types of attacks, making the system more user friendly and reliable.

Image Based Authentication is performed by using the visual data to indicate that the data is not forgery, it should be ensured that the visual quality of the data is not damaged. At the same time the techniques must indicate the malicious modifications which include removal or insertion of certain frames, change of faces of some individuals, time and background.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (54-58), Month: October 2014 - March 2015, Available at: www.paperpublications.org

IV. SECURITY ANALYSIS

As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

Dictionary Attack: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In the text based authentication, resistance is provided by the fact that secret pass created during registration phase remains hidden so the user only knows the real key which is to be entered at the time of login session. Even if the other person views the password, it will not be the original password, as it is incremented or decremented during registration.

Guessing: Guessing can't be a threat to the grid based authentication because it is hard to guess secret pass and it is unknown. When the user enters grid password it is remembered on the specific pattern. As each time grid changes, the password key also changes, hence guessing is also prevented in this security system.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368.

V. ADVANTAGES

1. The cyber-attacks such as Shoulder Surfing can be prevented by the use of Cryptography in Text Based Authentication.

2. The use of Trusted Third Party Services is more secure method than having the One Time Password in the Authentication System.

3. Use of Session Password makes it more valuable by means of Security prevents from attacks such as Guessing or Dictionary attacks.

4. Image Based Authentication makes the entire security system more user friendly.

5. Various levels of Secure Authentication Techniques make the system more reliable.

VI. CONCLUSION

The Multilevel Security and Authentication System makes it highly secure along with being more user friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and Brute-force attack at the client side. It is somewhat a time consuming approach, as the user has to traverse through the multiple levels of security. Grid Passwords make the system more secure by the introduction of session passwords. Therefore, this system cannot be a suitable solution for general security purposes, where time complexity will be an issue. But will definitely be a boon in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be available only to some higher designation holding people, who need to store and maintain their critical and confidential data secure.

VII. FUTURE ENHANCEMENTS

In future, different security levels can be supplementary to the existing levels to increase the performance and security. More features can be added to make our system customizable and user friendly. Various new attacks are being generated time to time, so the Multilevel Security and Authentication System can prove a major encounter by introducing the newer techniques to safeguard the information.

REFERENCES

[1] Jean Bacon, David Eyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis, and Peter Pietzuch. "Grid Based Authentication System", IEEE Transactions on Security and Service Management, Vol. 11, No. 1, March 2014.

[2] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi, "Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication", 14th International Conference on Modelling and Simulation, 2012.

[3] Sonia Chiasson, Elizabeth Stobert, A. Forget, R. Biddle, P.C van Oorschot. "Persuasive Cued Click Points: Design, Implementation and Evaluation of Knowledge-Based Authentication Mechanism". IEEE Transactions on Dependable and Secure Computing. Vol. 9 No. 2; 2012.

[4] S. Singh, G. Agarwal. International Journal of Computer Applications (0975-8887). Vol. 12. No. 9; 2011.

[5] www.wikipedia.org/wiki/Caesar_cipher.