IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-3, May 2016 E-ISSN: 2347-2693

Advance Security for Identifying Users without Their Login Ids

Manjunath R[1], Suresha T G[2], Ashok kumar P S[3]

[1 2]Computer Science & Engineering, City Engineering College, Bangalore, India
3 Professor & Head, Dept. of CSE AIems, Bengalore

Available online at: www.ijcseonline.org

***Abstract*—**Authentication to a computing system is composed of two parts, identification and verification. Traditionally, login IDs have been used for identification and passwords for verification. The method that can augment the current password-based system by strengthening the identification process. It utilizes personal secret data instead of a login ID to identify a user uniquely. It then asks the user to choose a correct login ID among multiple choices of partially obscured IDs. Since it does not accept a login ID during the authentication process, a stolen or cracked password cannot be used for gaining an access to the computing system unless the attacker provides a correct identification material. Hence in this paper, provide more security in the system. The security can be provided using user authentication, device authentication and captcha as a protocol step.

Keywords- Cybersecurity, authentication, identification, Password.

I. INTRODUCTION

Computer systems employ an authentication mechanism to allow access only to legitimate users. The authentication procedure is composed into two parts, identification& verification. The identification process is for answer the question, and the verification is for answering. Traditionally the identification is performed with a username and the verification is done with a password. In a password-based system, the plaintext passwords are transformed into hash values with a one-way hash function, and stored in a password hash file. During the verification process, a new hash value is generated from the newly entered password, and compared with the stored hash value in the password hash file. If the hash values match, access is granted. This password verification process is the heart of the most authentication systems. The number of ways to acquire other users' password for illegal access. Plaintext passwords can be captured from the network, by malware or by key logging software. When the plaintext password is not available, the attackers can try password-guessing attack where they try possible values for the victim user. In the password cracking attack, the attackers obtain a password hash file and try different inputs to find an input that produces the same hash value as the victim user's hash value.

Password hash files are stolen quite often and cracked by hackers. Password cracking attack is a statistical attack, and some of the weak passwords can be broken through a dictionary attack or a hybrid attack. After the attackers crack some passwords, they can access the system using the known login IDs for the cracked passwords. The attack against passwords is a serious threat to current authentication systems, and additional security measures are needed to mitigate this threat. Once an account is breached, the cost from the damage is high for both victims and the companies. The passwords are supposed to be random characters, login IDs are not random. They are used for communication or accounting purposes, and must carry a meaningful pattern. It may be part of users' first and last names, part of social security number, combination of names and numbers, account number, or email addresses. Thus login IDs are publicly known or can be guessed easily. Obtaining the login ID is generally not a barrier for the attackers, and the success of an attack depends on the difficulty of the password. While a great emphasis was given to the verification, i.e., password system, less attention was given to the identification, i.e., login ID. By fortifying the identification part, the overall authentication system can be stronger. The goal of these research is to provide more security in the system. The security can be provided using three way handshaking scenario. In proposed approach user authentication, device authentication and captcha as a protocol can be used. For user authentication three techniques are used namely hybrid, colour and text and pattern matching for detailed interaction between client and server. Rest of the paper is organised as follows: Section 2 gives an overview of the related work; Section 3 presents the proposed approach and Section 4 concludes the proposed approach.

II. RELATED WORKS

Authentication is any process by which a system verifies the identity of a user who wishes to access it. Since access control is normally based on identity of the user who requests access to a resource, authentication is essential to effective security. The different work done is discussed in this section.

Joseph Boneau, in [1], presents comprehensive approach leads to key insights about the difficulty of expected to replacing passwords. The two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty five usability, deploy ability and security benefits that an ideal scheme might provide. The comprehensive approach leads to key insights about the difficulty of replacing passwords. Many academic proposals have failed to gain traction because researchers rarely consider a wide range of real-world constraints. The framework provides an evaluation methodology and benchmark for web authentication proposals.

Nikos Komninos, in [2], presents a novel graphical password scheme, NAVI, wherethe credentials of the user are his username and a password formulated by drawing a route on a predefined map. Graphical password systems, based on visual information such as the recognition of photographs and pictures, have emerged as a promising alternative to mitigate reliance on text passwords. In this paper, a novel knowledge based authentication scheme that belongs to the recall based graphical passwords family is introduced.

Chao Shen et al. in [3], presents User Authentication through Mouse Dynamics. In this paper, mouse dynamics aims to address the authentication problem by verifying computer users on the basis of their mouse operating styles. A simple and efficient user authentication approach based on a fixed mouse operation task is given. A mouse-operation task, consisting of a fixed sequence of mouse operations is designed. Holistic features and procedural features are extracted from the fixed mouse-operation task to accurately characterize a user‘s unique behaviour data. AloneSchclar et al. in [4], presentsa novel approach for user authentication based on the keystroke dynamics of the password entry is introduced. Also the cluster representatives (CR) and Inner cluster representatives (ICR) strategies introduced to select the representatives. A common problem in user authentication is theacquisition of data. Hence the approach selects representative users, a dataset with a large enough number of users was required.

Bin B. Zhu et al. in [5], presents a novel family of graphical password systems built on top of Captcha technology. Captcha and graphical password addresses a number of security problems together, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shouldersurfing attacks.A password is more valuable to attackers than a free email account that Captcha is typically used to protect. Bob Zhang et al. in [6], proposed Three-dimensional (3-D) palm print tobe a significant biometrics for personal authentication. Three dimensionalpalm prints are harder to counterfeit than 2-D palmprints and more robust to variations in illumination and serious scrabbling on the palm surface. Three novel global features of 3-D palm prints which describe shape information and can be usedfor coarse matching and indexing to improve the efficiency of palm-print recognition, particularly in very large databases. The three proposed shape features are maximum depth of palm center, horizontal cross-sectional area of different levels, and radialline length from the centroid to the boundary of 3-D palm-printhorizontal cross section of different levels. Jaeseok

Yun et al. in [7], proposed a biometric user identificationmethod based on user‘s gait. The obtainable features fromuser‘s gait divided into two categories: walking pattern and steppingpattern (dynamic footprints), and considers an approachof identifying user with dynamic footprints. A software module is developed to extract dynamic Footprints from the samples acquired, and PCA (Principal Component Analysis) and neural network technique are employedto identify the user with extracted features.

JozeGuna et al. proposed an intuitive and very easy to use implicit gesture based identification system that is especially suited for security-wise noncritical applications, such as the user login inthe multimedia services. Performance of the proposed system is comparable to results ofother respectable related works when using explicit identification gestures, while also showing that implicit gesture based user identification is possible and viable.

Feng Zhang et al. presents location based authentication and authorization scheme for mobile transactions using smart phones. A solution that uses GPS technology provided by smart phones for location-based authentication and authorization. It is easy and flexible to integrate our solution with any existing authentication and/or authorization systems.

MariuszRybnik et al. presents two extracted keystrokes features: _flight‘ and _dwell. Without the need for analysis of many features and with the use of relatively simple classification techniques the keystroke dynamics proved to be very promising biometrics for identification of keyboard users. Alternative methods to replace the password based authentication system have been developed and some are widely used at this time. When two methods from two different categories are combined, it is considered two-factor authentication. The user authentication techniques can provide more security in the system.

II. PROPOSED WORK

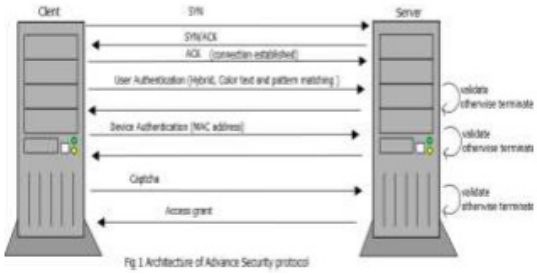

Fig 1 Architecture of Advance Security protocol

Step1: First client make a connection with server.

Step2: User Authentication. User send request to server. Using hybrid, colour & text and pattern matching mechanism, if Validate access is granted. Otherwise connection is terminated.
Step 3: Device Authentication. Access to peer can be granted using MAC address.
Step 4: Captcha can be used to authenticate user. If validates access is granted. Otherwise connection is terminated.
Step 5: If above things are validates access is granted.

User Authentication with Hybrid Mechanism:-

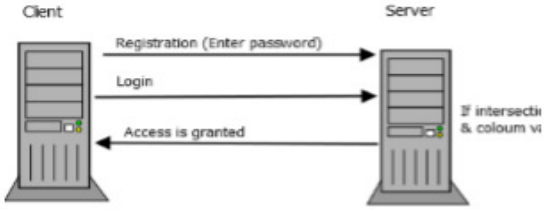

Fig 2: User authentication with hybrid mechanism.

Step 1: User make registration i.e. enter password.
Step 2: User make Login. If intersection of row and column valid, access is granted.
Step 3: Otherwise terminated.

During the phase of registration, the user submits the secret pass. The minimum length of the secret pass is8 and it should contain even number of characters. During the primary level authentication, when the user chooses the pair-based authentication scheme, an interface consisting of 6X6 grid is displayed. The grid contains both alphabets and numbers which are placed atrandom and the interface changes every time. The mechanism involved in the pair-based authentication scheme work as: Firstly, the user hasto consider the secret pass in terms of pairs. The first letter in the pair is used to select the row and the second letter is used to select the column in the 6X6 grid. The intersection letter of the selected row and column generates the character which is a part of the session password. In this way, the logic is reiterated for all other pairs in the secret pass. Thus, the password n putted by the user i.e. the session password is now verified by the server to authenticate the user.


Figure 6: Hybrid Textual Login Screen

In this scheme, the session password is generated for the color password. This scheme considers the ratings given to the color pattern at the time of registration phase. During login phase, once textual authentication is done then, the user has to do the color authentication. At the time of color authentication, new color pattern is displayed. This pattern consists of randomly placed colors (not "RGBY"). Then the user has to set the range for newly pattern according to registered color password. Lets understand with the example. Consider the ratings given during registration phase is 4213 for "RGBY". Then at the login time,if suppose following pattern is displayed then according to registered color password, the user will rate the color as follows:

From the above figure it shows that at the registration time the rating for yellow is 3, for red it is 4, for blue it is 1 and for green it is 2.So based on the registered ratings, we have set the ratings for this color pattern which is displayed during login time. This newly given rating is called as rated password. Thus in our example, 3412 is the rated password. This pattern changes for every login phase and thus the rating also changes for every login phase. Now, the 4x4 matrix is displayed which consists of digits numbered from 1 to 4. This digits are also placed randomly such that no two elements are placed in one row and colomn and changes for every login session as shown below:

	1	2	3	4
1	3	4	2	1
2	2	1	3	4
3	1	2	4	3
4	4	3	1	2

Once we have rated the colors, the next step is to divide the ratings into a pair of two such that first digit is row element and the second digit is the column element. The intersection of these two element is the session password.

So, in our example, the rated password 3412 is broken into a pair of two as 34 and 12. Now, as per previous statements, 3 is the row element and 4 is the column element. Now, we will search for the intersection element for 3 and 4 in the above color matrix. After searching, we get 3 as intersection digit which is the session password for

34. Likewise,we will generate session password for the remaining pairs. Hence, for another pair i.e 12, we get 4 as session password. Thus , by combining , we get final session password as 34 for rated password "3412".

User Authentication with Colour & Text Mechanism:

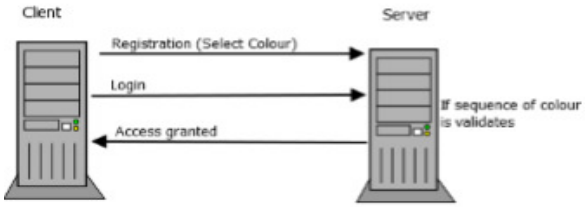

Fig 3: User Authentication with Colour & text mechanism

Step 1: User make registration i.e. select colours.
Step 2: User make Login. If sequence of colour is valid, access is granted.
Step 3: : Otherwise terminated.

During registration, the user gives rankings (1to8) to colours in the colour grid which is considered as the hybrid textual password. In primary authentication, when the user selects the hybrid textual authentication scheme, an interface is displayed. The interface consists of 8X8 number grid in which numbers from 1 to 8 are placed erratically. In addition to this, a colour grid is also displayed containing 4 pairs of colours. Both these grids changes for every session. The logic involved in this scheme is that the rating given to the first colour of every pair represents a row and the rating given the second colour in that pair represents a column of the 8X8 number grid. The number in the intersection of the row and column of the grid is the part of session password. This procedure is repeated for the remaining colour pairs in the colour grid. In both the cases, if the session password entered by the user is correct, then he is permitted to face the secondary level authentication. Otherwise, the user is prompted to re-enter the session password according to the secret pass and hybrid textual password.

User Authentication with Pattern Matching Mechanism:-

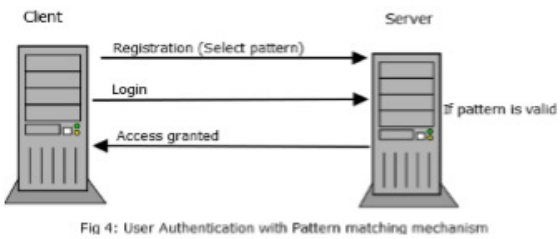

Fig 4: User Authentication with Pattern matching mechanism

Step 1: User make registration i.e. select pattern.

Step 2: User make Login. If pattern is valid, access is granted.

Step 3: Otherwise terminated.

The user has to draw a sequence, as draw-a-secret joining the dots. For normal registered user, if the sequence drawn during authentication matches with the sequence drawn during the registration phase, then the user is given the permission to access the confidential files. If the draw-a-secret is wrong, then a message sequence doesn't match is indicated to the user.

III. CONCLUSION

Authentication is any process by which a system verifies the identity of a user who wishes to access it. Since access control is normally based on identity of the user who requests access to a resource. To improve online data security captcha, authentication protocols, identification protocols, data encryption can be used.Generally, there are many drawbacks associated with the textual passwords such as brute-force and dictionary attacks. Similar is the case with the graphical passwords which includes shoulder-surfing and are very expensive to implement. As such, we have proposed the idea of utilizing session passwords for authentication. For this purpose, we had made use of both the textual and graphical password techniques. In this paper, we have implemented two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Associated with these techniques is the draw-a-secret graphical method employed for security issues.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User StudyUsing Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[3] A. F. Syukri, E. Okamoto, and M. Mambo, "A User identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[4] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang.Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing."

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy,,N.Memon, "Design and longitudinal evaluation of a>graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

[6] H. Zhao and X. Li, "S3PAS: A Scalable ShoulderSurfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[7] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme,,"in Proceedings of International conference on security and management. Las Vegas, NV, 2003.