# Mindmetrics : An Appraoch For Upgrading Security

Prajakta Y. Patil
Computer engineering
SSBT COET
Jalgaon, India

Bhushan R. Badgujar
Computer engineering
SSBT COET
Jalgaon, India

Anil P. Chaudhari
Computer engineering
SSBT COET
Jalgaon, India

Shraddha V. Patil
Computer engineering
SSBT COET
Jalgaon, India

Kuldipsinh A. Rajput
Computer engineering
SSBT COET
Jalgaon, India

***Abstract*—Disclosure of the password hash files is a critical security concern making millions of user prone to cyber-attacks. Most of the time the attacker tries to steal the password hash files and then he tries to crack them. In this type of password cracking attack the weak passwords are broken through a dictionary attack or hybrid attack. After the attackers crack some passwords, they access the system using the known login IDs for the cracked passwords. The attack against passwords is a serious threat to current systems [2]. Many methods have been proposed to stop these types of attacks but they require specialized devices. The method presented in this paper magnifies the traditional password based system by enhancing the identification process. For this purpose the proposed method accepts personal secrete data instead of a login ID to identify a user uniquely, called as "mindmetrics" [2]. It then asks to choose the correct login ID form given ID's. After the several login attempts attacker will be blocked by the identification server. Thus it stop or slow downs attacker.**

***Keywords— Password, cyber attack, identification, verification***

## I. Introduction

An authentication is mechanism which is employed by computer system to allow access to the legitimate users. Generally the authentication procedure comprises of two parts, identification & verification. Generally the identification process is carried out with a username and the verification is done with a password. In a traditional password-based system [2], any one hash function is used to transform the plaintext password into the hash values then these values are stored into a password hash file accordingly.

Once the identification part is completed, the verification process begins in which a new hash value is generated from the newly entered password, and is compared with the stored hash value in the password hash file for particular login ID [2]. If the match is found then the access is granted. In most authentication systems verification process plays a vital role. There are numerous ways to acquire other user's password for illegal access. Malwares or key logging software can easily capture the plaintext passwords. The attacker uses the different types of attacks to get the password which are as follows.

*1) Password Guessing attack:* Password guessing attack may seems silly but this can easily help one to get information and details in seconds. This attack happens only when the user is well known to the attacker and the attacker will be able to guess the information using the information that he knows such as date of birth, date of joining etc.

*2) Brute Force Attack:* In this method, the attacker tries every possible combination of numbers, characters [4], special characters and alpha-numeric combinations till the correct combination of pass¬word is obtained. It is a very long process and it takes more time as it is totally depends on the complexity of the password.

*3) Dictionary attack:* Dictionary attacks are based on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary [4].

The traditional password-based system is which very much vulnerable to the attacks that have been discussed above.

In this system the login IDs are used for identification and password is used for verification. As we know login ID's are used for communication or accounting purposes, and must carry a meaningful pattern. Login ID's may be made up of user's 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 and can be guessed easily. Obtaining the login ID is not a difficult task 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 [2]. By focusing only on the identification part, the overall authentication system can be made stronger.

The goal of this research is to provide more security to the authentication system.

## II. Literature Survey

To verify the identity of user (person willing to access the system) a process called "authentication" is used. 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 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 [1], presents a novel graphical password scheme, NAVI, where the 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 [4], 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 behavior data.

Alon Schclar et al. in [5], presents a 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 the acquisition of data. Hence the approach selects representative users a dataset with a large enough number of users was required. Authentication scheme that belongs to the recall based graphical passwords family is introduced.

Bin B. Zhu et al. in [6], 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, shoulder surfing 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 [3] proposed Three-dimensional (3-D) palm print to be a significant biometrics for personal authentication. Three dimensional palm prints are harder to counterfeit than 2-D palm prints 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 recognition, particularly in very large databases.

## III. Existing System

The existing system is the traditional password based system. As we know in this system user has to enter the User ID along with the password. The User ID accepted by this system is known to all and password is unique and secret in this login system. As the user ID of the system is known to all. Once the hacker gets the password hash files then he can use the password files for the known login ID's. Traditional password-based system shown in figure is vulnerable to the attacks. In the traditional password-based system everyone is allowed to try openly with known Login IDs without any restriction. An attack on the password hash table will turn out to be dangerous. This attack will harm not only to the user but also to the entire system. The security analysts are trying their best to stop the attacks which are made from the attackers. Therefore there is need to provide the security to various aspects of system and it should be started from fundamental i.e. from the user itself. There are a numerous ways by which the user account is harmed either by using technical or non-technical methods. All of these things lead to the discovery of method which is robust and can protect the user credentials in secure manner. The method used for identification is referred to as Mind metrics token. The title "mind metrics" is coined due to its similarity to the biometrics' [2]. In the case of biometrics, only the legitimate user possessing the physical character can pass through the identification stage. Similarly, with the mind metrics identification technique, a user can pass through the identification stage [2] in an authorized and a secured manner, subjugated to the overall security of the system in use.

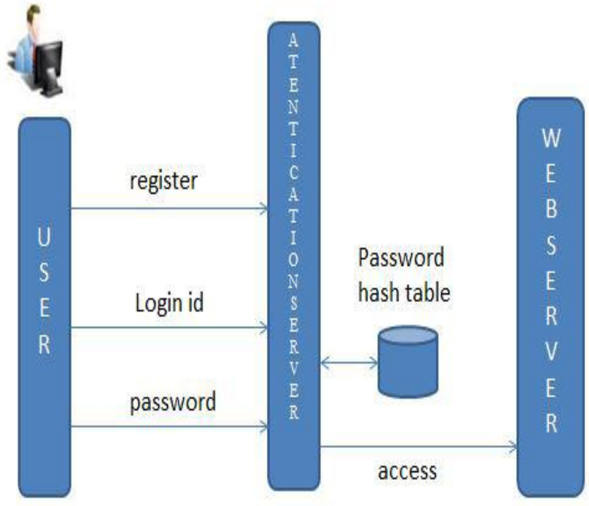

Fig. 1. Traditional password based system.

Without the use of mind metrics secret key, the user can’t pass the identification stage and move on to the next process, i.e. verification stage.

## IV. Proposed System

A schematic view of the mindmetrics system architecture is shown in figure 2. The architecture consist of two server first is identification server and second is verification server. Both of these performs authentication process by dividing it in two parts i.e. identification and verification. Proposed system is developing for secure communication between client and server.

Detailed procedure of mindmetrics based system is described in the following steps:

Step 1: Users Register to system by giving mindmetrics token, email id and password. The user creates the token which user can remember and it acts as its secret key. The login ID may be created by user or given by the server. After the user has entered them, the user selects the Create Account option. Then the authentication server validates the entered information. For this server ensures that the login Id is unique [2] and password satisfies all the constraints. If it does not satisfies the constraint then server may prompt the user to enter another login ID or password.

Step 2: User Information will then be split into two parts on two different servers i.e. identification server and verification server.

Step 3: The identification server receives user input specifying a token, and determine whether the token matches a token stored for a user account [2].

Step 4: The user logs in with the original credentials. Then server looks up for the matching token that the user has supplied. After the matching token is determined, the server will not display login id instantly because an attacker can contrive the token and the matching login ID [2]. It presents multiple login IDs in partially obscured form and then allows user to select one. The numbers of choices are either decided by identification server or the user [2]. Several strategies are employed to enhance the security in this step.

Step 5: After selecting a single login ID, the user types the password which matches the login ID. Then login ID and password is given to the verification server. If the credentials [2] supplied at the time of login are matched with original credentials then the access is granted otherwise access is not granted and mail will be send to the original user.

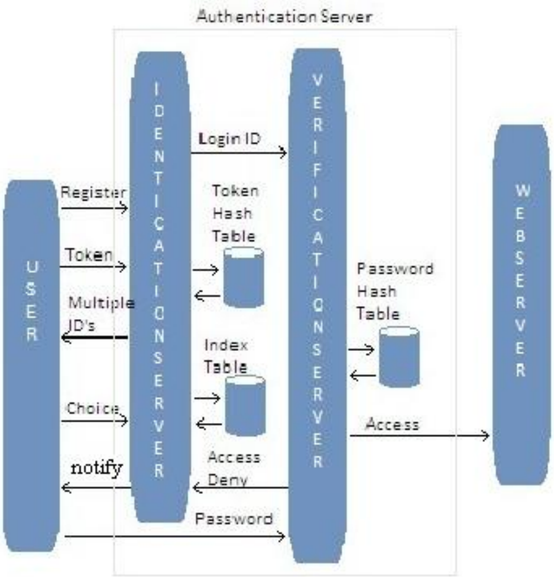

Fig. 2. Mindmetrics based system.

## V. Analysis

The main aim of mindmetrics system is to improve the security of the authentication process by providing it with a secure identification process. By making token sophisticated and long, the higher level of protection can be achieved. Token complexity is increased by using special keys and intentional misspelling.

Mindmetrics system may look like a double-password system where a user provides two independent passwords. However, it has a significant advantage over the conventional password system as it makes a targeted attack on a particular user account nearly impossible. The first line of defense comes from the storage of multiple files. The authentication system stores the token hash file, index file, and password hash file separately in order to mitigate the risk of theft. Unless the attacker obtains them altogether, a successful cracking attack is very difficult [2].

Mindmetrics authentication system can be used either for a local or a remote machine. Existing password systems can be easily upgraded to mindmetrics system by adding the identification server without any change in the existing password system [2].

## Conclusion

The proposed system overcomes all the drawbacks of traditional password based system. A new concept called mindmetrics is used that strengthen the identification process with the personal secret information [2]. Mindmetrics is more advantageous than biometrics as it does not require any hardware device and is cost effective. System makes false login attempts difficult and increase in login attempts by attackers is blocked by identification server. The user is not allowed to enter the verification phase till it clears the identification phase. The proposed system makes use of symmetric protocol for two-server password authentication and key exchange. The proposed system is very efficient as compared to the traditional authentication protocols implemented on single server [5].

The future work will have to be concentrated on providing additional security to verification server through honey words or by encrypting the passwords.

## REFERENCES

[1] Joseph Bonneau, Paul C van Oorschot, and Frank Stajano, ―The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes‖, 2012 on Security and Privacy, pp. 553 – 567, Christos Douliger ―NAVI: Novel with Visual Information on Computers and Communications, 2012, pp. 588 – 595.

[2] Juyeon Jo, Yoohwan Kim, and Sungchul Lee, Mind metrics: Identifying users without their login IDs, IEEE International Conference on Systems, Man, and Cybernetics, 23-October -2015, vol. 5-8, PP. 448-161.

[3] Bob Zhang, Wei Li, Pei Qing, and David Zhang, ―Palm-Print Classification by Global Features, Ieee Transactions On Systems, Man,And Cybernetics: Systems, Vol. 43, No. 2, March 2013, pp. 370 – 378

[4] Juyeon Jo, Yoohwan Kim, and Sungchul Lee, Mind metrics: Identifying users without their login IDs, IEEE International Conference on Systems, Man, and Cybernetics, 23-October -2015, vol. 5-8, PP. 448-161.

[5] Chao Shen, ZhongminCai, Xiaohong Guan, Youtian Du, and Roy A. Maxion, ―User Authentication Through Mouse Dynamics‖, IEEE Trans on Information Forensics and Security, v. 8, no. 1, Jan 2013, pp. 16 – 30.

[6] Alon Schclar, LiorRokach, Adi Abramson, and Yuval Elovici, ―User Authentication Based on Representative Users, IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews,Vol. 42, No. 6, November 2012, pp. 1669 – 1678

[7] Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu,‖Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems, IEEE Transactions on Information Forensics And Security, Vol. 9, No. 6, June 2014, pp. 891 – 904.

[8] D. B. K. Kamesh, K. Rama Krishna and J. K. R. Sastry] - Authenticating Clients without using their Login IDs through Mind Metrics, Indian Journal of Science and Technology, Vol 9(30), DOI: 10.17485/ijst/2016/v9i30/98715, August 2016.