An Efficient Authentication Scheme based on the concept of "Mindmetrics"

Dhanashree Ambawle[1], Dilpreet Singh Gill[2], Resham Wadhwa[3], Shehjar Kilam[4]
[1, 2, 3, 4] AISSMS IOIT, Pune, India

Abstract- *User Authentication in computer systems is an important cornerstone in today's computer era. The concept of a login id and password is one of the easiest ways for authentication. It is not only the easiest way, but also cost effective and highly efficient. Authentication process to an any computing system is composed of two parts i.e. identification and verification. Login Id is used for identification and password is used for verification. It is very important to secure both the phases of authentication process. In this paper, a system is proposed where security is provided to the identification phase of authentication process without the involvement of any specialized devices. In identification phase, concept called mindmetrics is implemented where personal secret data instead of login id is used to identify the user. In verification phase, the old traditional concept of password verification is used. The proposed system does not make use of any hardware device and hence it is cost effective.*

Keywords- Authentication, Cryptography, Cyber Security, Hash Technique, Mindmetrics, Password Verification, User Identification.

I. INTRODUCTION

"Mindmetrics" idea is like biometrics. Biometrics is a field of study which means to distinguish or perceive individuals in light of qualities they have. Given these qualities, a framework can be prepared to perceive certain individuals, with a specific likelihood. Biometrics alludes to measurements identified with human attributes. Biometrics confirmation is utilized as a part of software engineering as a type of recognizable proof and get to control. Mindmetrics utilizes some mystery information rather than human qualities as a token to distinguish the client. It uses individual mystery information rather than a login ID to recognize a client particularly, thus mindmetrics. The idea of biometrics or mindmetrics is utilized as a part of validation plans to recognize a client with true blue ID holder.

Examination between Biometrics and Mindmetrics

1] Some extraordinary equipment gadget (e.g.: thumb scanner) is required in biometrics. Then again no unique equipment is required in mindmetrics and can be effectively actualized. So mindmetrics can be utilized for getting to nearby or remote figuring frameworks from any customary private or open PCs.

2] Biometrics is expensive and can't be effortlessly actualized on open e-business sites. Mindmetrics is savvy and can utilized for open e-business sites.

Mindmetrics is a deterministic procedure, and therefore there is no vulnerability. Hence mindmetrics is more user friendly, less expensive, and can be utilized by any open sites, for example, e-business sites.

II. PREVIOUSLY WORK DONE

The paper presented by Alon Schclar and Lior Rokach Describes that the User authentication based on username and password is the most common means to enforce access control[1]. The paper introduces a novel approach for user authentication based on the keystroke dynamics of the password entry. A classifier is tailored to each user and the novelty lies in the manner by which the training set is constructed. This concept reduces the possibility of over fitting, while allowing scalability to a high volume of users. Specifically, only the keystroke dynamics of a small subset of users, which we refer to as representatives, is used along with the password entry keystroke dynamics of the examined user. The contribution of this approach is twofold: it reduces the possibility of over fitting, while allowing scalability to a high volume of users. We propose two strategies to construct the subset for each user. The first selects the users whose keystroke profiles govern the profiles of all the users, while the second strategy chooses the users whose profiles are the most similar to the profile of the user for whom the classifier is constructed. Results are promising reaching in some cases 90% area under the curve. In many cases, a higher number of representatives deteriorate the accuracy which may imply overfitting. An extensive evaluation was performed using a dataset containing over 780 users[1].

The paper presented by Bin B. Zhu and Jeff Yan focuses on Using hard AI problems for security. The paper presents that many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-explored. In this paper, we present a new security primitive

based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security[2].

The paper published by Mariusz Rybnik and Marek Tabedzki mainly describes that On-the-fly keyboard user authorization is certainly an interesting option for standard security procedures for high-security computer systems. Unauthorized access to logged-in workstation could threaten the security of data and systems. Conventional authorization methods (passwords, fingerprint scans) verify user identity only during logging process, leaving system vulnerable to user replacement afterwards. Procedures overcoming this peril are often invasive (constant visual monitoring) or uncomfortable (frequent identity verification with user cooperation). A possible solution for constant authorization without these drawbacks is to identify the keyboard user while typing. The approach we propose is based on two extracted keystrokes features: 'flight' and 'dwell'. We have tested the suggested solutions on individual group resembling a medium-sized company. The obtained results are promising[3].

The paper presented by Bob Zhang, Wei Li, Pei Qing and David Zhang focuses on authentication system based on Palm-Print Classification by Global Features. Three-dimensional (3-D) palm print has proved 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. Previous work on 3-D palm-print recognition has concentrated on local features such as texture and lines. In this paper, we propose three novel global features of 3-D palm prints which describe shape information and can be used for 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 radial line length from the centroid to the boundary of 3-D palm-print horizontal cross section of different levels. We treat these features as a column vector and use orthogonal linear discriminant analysis to reduce their dimensionality. We then adopt two schemes: 1) coarse-level matching and 2) ranking support vector machine to improve the efficiency of palm-print recognition. We conducted a series of 3-D palm-print recognition experiments using an established 3-D palm-print database, and the results demonstrate that the proposed method can greatly reduce penetration rates[4].

The paper presented by Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano focuses on The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. It presents that they evaluate 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 scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals[5].

III. PROPOSED SYSTEM

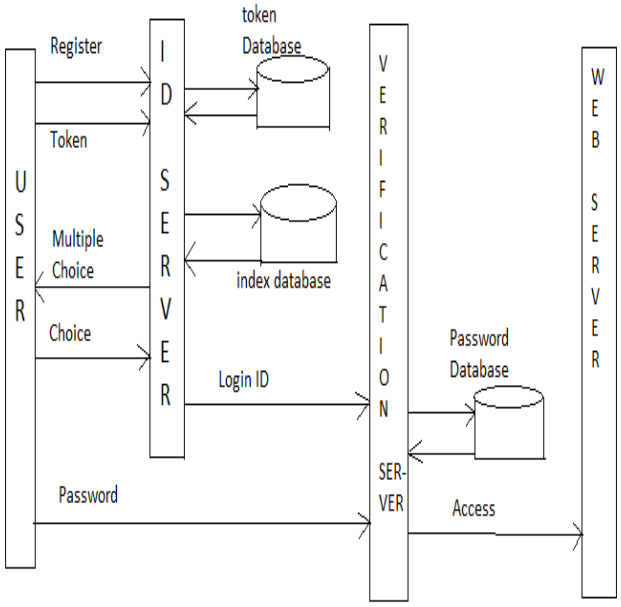


Figure 1. System Architecture

There are two parts in the mindmetrics-based authentication process:-

1] Mindmetrics token is requested in the login page. A user specifies the token with which a computing system can identify a user account. Then the identification server looks up the registered access tokens to find a matching token and login ID.

2] The server presents multiple login IDs to the user, with one of the login IDs being the correct login ID for the user account and some more real or fake IDs. To prevent the attackers from recognizing the login IDs, the login IDs are partially obscured. Among these partial login IDs, a legitimate user can still recognize the correct login ID and choose it.

Above two steps are carried out in the identification phase. Once the server is identified then the conventional password verification method is used for granting the access.

Mindmetrics based system allows only the legitimate users to pass the identification stage. Here the password verification server is kept hidden, and users cannot access it unless they pass the identification server.

The proposed system makes use of hashing algorithm Message Digest 5 to generate hash values of tokens. MD5 processes a variable-length user token into a fixed-length output of 128 bits. Following are the steps of MD5 algorithm.

1. The input message is broken up into chunks of 512-bit blocks, the message is padded so that its length is divisible by 512.
2. The padding works as follows: first a single bit, 1, is appended to the end of the message.
3. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512.
4. The remaining bits are filled up with a 64-bit integer representing the length of the original message, in bits.
5. The MD5 algorithm uses 4 state variables, each of which is a 32 bit integer (an unsigned long on most systems). These variables are sliced and diced and are (eventually) the message digest.

The variables are initialized as follows:
A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325476.

6. Now on to the actual meat of the algorithm: the main part of the algorithm uses four functions to thoroughly goober the above state variables. Those functions are as follows:

F(X,Y,Z) = (X & Y) | (~(X) & Z)
G(X,Y,Z) = (X & Z) | (Y & ~(Z))
H(X,Y,Z) = X ^ Y ^ Z
I(X,Y,Z) = Y ^ (X | ~(Z))

Where &, |, ^, and ~ are the bit-wise AND, OR, XOR, and NOT operators

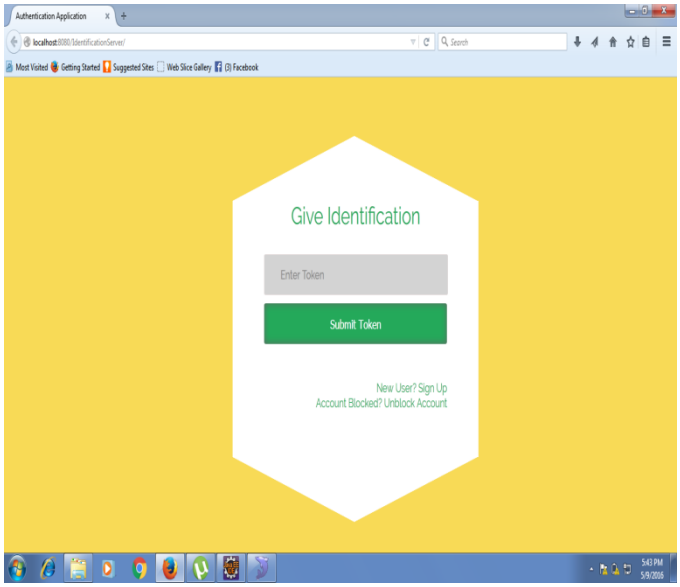
7. These functions, using the state variables and the message as input, are used to transform the state variables from their initial state into what will become the message digest. For each 512 bits of the message, the rounds performed (this is only pseudo-code, don't try to compile it) After this step, the message digest is stored in the state variables (A, B, C, and D). To get it into the hexadecimal form you are used to seeing, output the hex values of each the state variables, least significant byte first. For example, if after the digest:
   A = 0x01234567;
   B = 0x89ABCDEF;
   C = 0x1337D00D
   D = 0xA5510101
   Then the message digest would be:

67452301EFCDAB890DD03713010151A5 (required hash value of the input value).

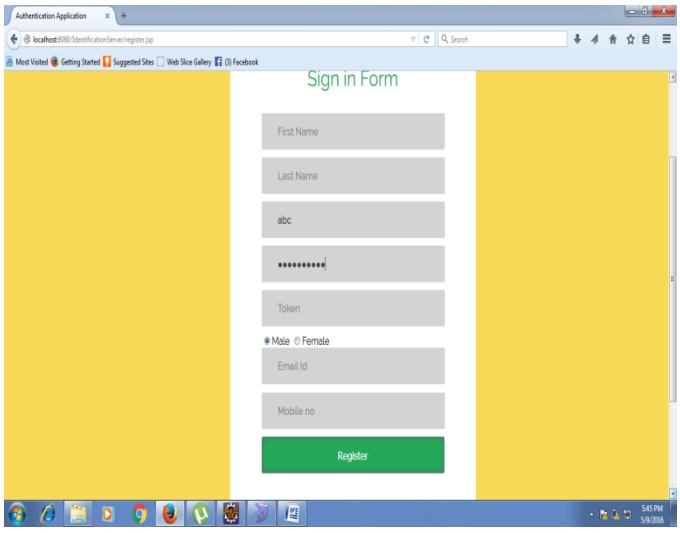
IV. SYSTEM RESULTS

Following are some system results:

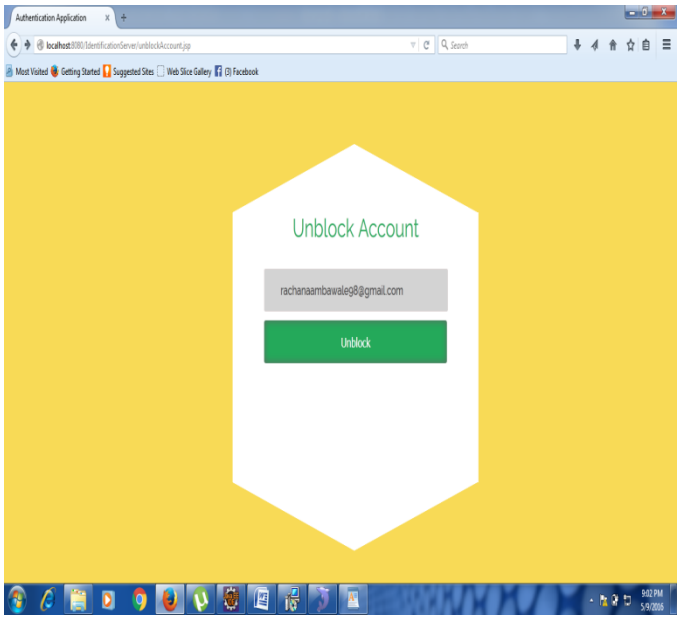
1] Screenshot showing token identification screen



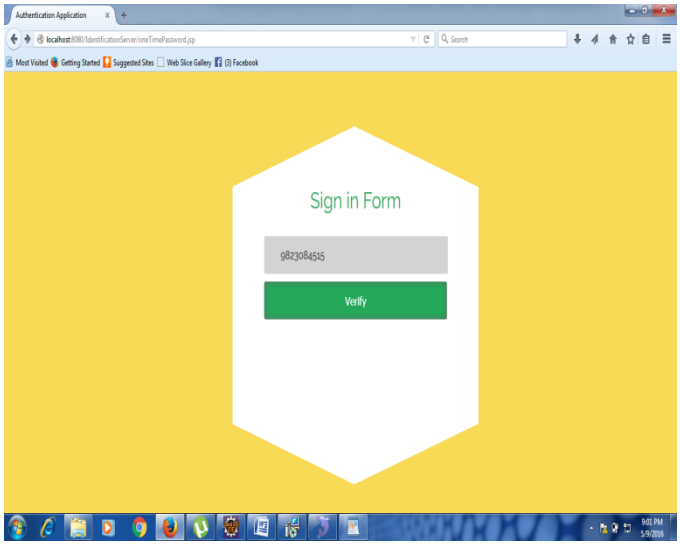
2] Screenshot showing registration form



3] Screenshot showing unblock account functionality



4] Screenshot showing one time password (OTP) procedure



V. CONCLUSION

User authentication is done in two steps, identification and verification. The traditional password-based verification system has been challenged by sophisticated attacks, but new schemes are being made to cover the weaknesses of the password-based systems. However, the identification part is still done based on a public login ID. We are going proposed a new scheme called mindmetrics to strengthen the identification process with personal secret information. In mindmetrics systems, a login ID will not be asked. Instead a user must provide the correct token to pass the identification stage. In case the password file gets stolen,

the login attempts by attackers will be blocked by the identification server. Thus it may stop or slow down attackers, and account holders can change their account credentials before attackers can gain access. Mindmetrics can simulate biometrics with its high security level where true two factor authentication with biometrics is not feasible. It is very simple, and it does not require any specialized devices or any mathematical algorithm. So, it will be more practical than other methods and can be used by any public web sites. We will implement a proof-of-concept system and evaluated it with test users. The survey indicates that mindmetrics system is intuitive and easy to use, and users are willing to use it to have extra protection.

REFERENCES

[1] Joseph Bonneau, cormac Herley, Paul C van Oorschot, and Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", 2012 IEEE Symposium on Security and Privacy, pp. 553 – 567

[2] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu,"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

[3] Anna Vapen, David Byers, and Nahid Shahmehri, "2-clickAuth – Optical Challenge-Response Authentication", 2010 International Conference on Availability, Reliability and Security, pp. 79 – 86

[4] Dileep Kumar, Yeonseung Ryu, and Dongseop Kwon, "A Survey on Biometric Fingerprints: The Cardless Payment System" 2008 Int'l Symposium on Biometrics and Security Technologies, pp. 1-6

[5] 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

[6] Jaeseok Yun, Gregory Abowd, Woontack Woo, Jeha Ryu, "Biometric User Identification with Dynamic Footprint", 2007, 2nd Int'l Conference on Bio-Inspired Computing: Theories and Applications, pp. 225-230

[7] Alon Schclar, Lior Rokach, 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

[8] Mariusz Rybnik, Marek Tabedzki, and Khalid Saeed, "A Key stroke dynamics based system for user identification, 7th Computer Information Systems and Industrial management Applications, 2008 pp. 225 – 230.