An Efficient Authentication Scheme using Mindmetrics and Two-Server Password Symmetric Protocol

[1]Ojaswi Pratulya, [2]Jayshree Ramteke, [3]Nisha Mahajan,
[4]Radhika Mahajan, [5]Prof. Mohini Devikar
[1, 2,3,4,5] Department of Computer Engineering,
[1, 2,3,4,5] Modern Education Society's College of Engineering, 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 a 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 both the phases 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 concept of two server password is implemented to prevent the password from getting hack. The proposed system does not make use of any hardware device and is cost effective.**

***Index Terms*— Authentication, Cryptography, Cyber Security, Hash Technique, Mindmetrics, Password Verification, User Identification.**

I. Introduction

Computer systems employ an authentication mechanism to allow access only to legitimate users. The authentication mechanism identifies the user through the login id and validates the password. If the login credentials are correct then the user gets access to the system. There are a number of ways to acquire other users' password for illegal access. Password can be hacked by trying password-guessing attack where the attacker tries possible values for the victim user. Some of the weak passwords can be even broken through a dictionary attack or a hybrid attack. When the attacker acquires the crack passwords, they can easily access the system using the known login IDs for the cracked passwords. In this paper the concept of two server and cryptography technique is used to secure the verification phase.

Password is a combination of random characters but login id formation has some pattern between the characters. Login Id is used for communication or accounting purposes, and hence should carry a meaningful pattern. Login Id can be a combination of users' first and/or 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. In other words, 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. Till today many systems are developed where great emphasis is given on verfication phase and less on identification phase. In this paper the concept of mindmetrics is used during the identification phase. The term "Mindmetrics" is coined with the concept of Biometrics as it is similar to biometrics. Biometrics is a field of study which aims to identify or recognize people based on traits they have. Biometrics is used in authentication schemes to identify a user with legitimate ID holder. Mindmetrics uses some secret data instead of human characteristics as a token to identify the user. It utilizes personal secret data instead of a login ID to identify a user uniquely, hence mindmetrics.

Thus by securing the identification and verification phase individually the overall security of the system is improved.

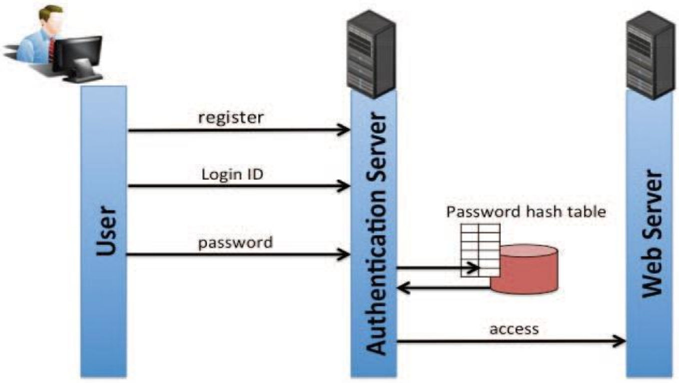

Figure 1. Conventional Password-based System

In figure 1, the architecture of conventional password based system is shown. The user register with the system. During registration user has to mention a login id and a valid password with all the other necessary details. All the details other than password are stored in the database. 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 to the user. The password-based system allows anyone to try publicly known login IDs without any restriction and it is more prone towards the password-guessing attack. Thus by studying the conventional password based system it can be concluded that there is a need to secure the identification phase and strengthen the security of password verification.

II. Proposed System

The proposed system has two servers. First is Identification Server and second is Verification Server. The proposed system separates the identification server and the verification server, thus it is scalable to a large system. Identification Server has its own local database. Verification Server is further connected to two more servers named Server 1 and Server 2. To establish a secure channel between verification server and server 1, verification server and server 2 a two way handshaking protocol named Deffie Hellman Key Exchange Protocol is implemented. The following figure 2 shows the detailed architecture of the proposed system.

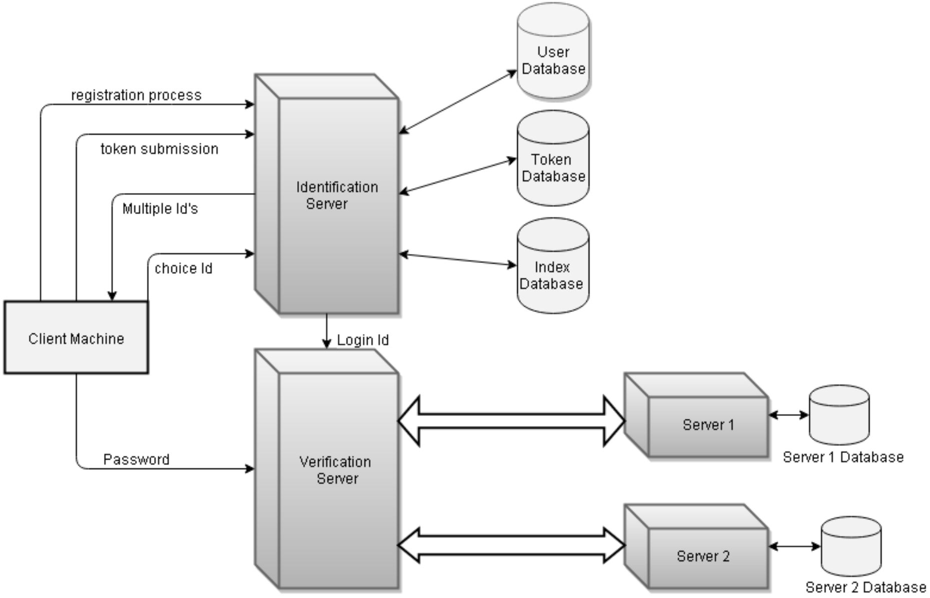

Figure 2. Proposed System Architecture

In the proposed system the login ID is not considered a secret. This is because it is impossible to keep the login ID secret as it is used for many other purposes such as accounting or email. So an alternative secret is needed for identification to recognize a user uniquely. This secret is referred as Mindmetrics token. During registration the user submits the token along with login id and other details. The hash value for token is generated and is stored in token database in the tuple format as {token hash value, index}. On the basis of login id, fake id's are generated and stored in the index database in tuple format as {index, fake login ID, fake login ID, true login ID, fake login ID}. All these functions are carried out at Identification Server. During registration, verification server accepts the password. It splits the password in two parts say part1 and part2. Each of the password part is encrypted using ElGamal Algorithm and is sent to the respective servers. Password part1 is sent to server 1 and part 2 is sent to server 2. Server 1 and Server 2 store their respective part of passwords in their local database.

During Login, system asks the user to enter the secret information required for identification. User submits the token. A new hash value is generated from the newly submitted token, and compared with the stored hash value in the token database. If the hash values match, token is validated and user enters in the next step of identification procedure. In this step multiple login id's are displayed to the user among which only one login id is correct. To enhance the security of this step the displayed login IDs are partially-obscured by replacing some characters in the login id with asterisks. If the user selects correct login id then only the user is allowed to enter the password. Thus the proposed 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. Once the user is identified as legitimate user the login id of user is sent to the verification server. The verification server requests for the password information from both servers. Both the servers decrypt their part of password information and send it to verification server. The password information is merged at verification server. If merged information and the password entered by the user matches then the particular user gets authentication to the system.

III. Algorithms Used

A. Deffie Hellman Key Exchange Algorithm

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

Consider two users Alice and Bob, who wish to exchange a secret key between them. Diffie-Hellman key exchange algorithm works as follows:
1. Alice and Bob agree on a cyclic group G of large prime order q with a generator g.
2. Alice randomly chooses an integer a from Z*q and
computes X = g^a. Alice sends X to Bob.
3. Bob randomly chooses an integer b from Z*q and computes Y = g^b. Bob sends Y to Alice.
4. Alice computes the secret key k1 = $Y^a = g^{ba}$.
5. Bob computes the secret key k2 = $X^b = g^{ab}$.
It is concluded that k1 = k2 and thus Alice and Bob have agreed on the same secret key, by which the subsequent communications between them can be protected.

Diffie-Hellman key exchange protocol is secure against any passive adversary, who cannot interact with Alice and Bob, attempting to determine the secret key solely based upon observed data.

B. ElGamal Algorithm

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. The algorithm consists of three phases: key generation, encryption, and decryption.
ElGamal Encryption Algorithm works as follows:
1. Key Generation:
Participant A generates the public/private key pair
a. Generate large prime p and generator g of the multiplicative Group Z*p of the integers modulo p.
b. Select a random integer a, $1 \leq a \leq p - 2$, and compute g^a mod p.
c. A's Public key is (p, g, g^a). A's Private key is a.

2. Encryption:
Participant B encrypts a message m to A
a. Obtain A's authentic public key (p, g, g^a).
b. Represent the message as integers m in the range
{0, 1, 2, ……….., p-1}
c. Select a random integer k, $1 \leq k \leq p - 2$.
d. Compute $\gamma = g^k$ mod p and $\delta = m * (g^a)^k$
e. Send ciphertext c = (γ, δ) to A.

3. Decryption
Participant A receives encrypted message m from B
a. Use private key a to compute (γ^{p-1-a}) mod p.
b. Recover m by computing (γ^{-a}) * δ mod p.

IV. Conclusion

In this paper, more efficient and secure authentication process is proposed. The proposed system overcomes all the drawbacks of conventional password based system. A new concept called mindmetrics is used to strengthen the identification process with the personal secret information. Mindmetrics is more advantageous than biometrics as it does not require any hardware device and is cost effective. It can be easily used on public e-commerce websites. The proposed system make 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. The involvement of more than one server increases the security of authentication process and prevents the system from active and passive attacks. As a whole, the proposed authentication system is made more powerful and effective by combining the concept of mindmetrics and two-server authentication protocol.

References

[1] Juyeon Jo, Yoohwan Kim, and Sungchul Lee, "Mindmetrics: Identifying users without their login IDs", IEEE 2014.
[2] Xun Yi, San Ling, and Huaxiong Wang "Efficient Two-Server Password-Only Authenticated Key Exchange", IEEE – 2013
[3] Vignesh Kumar K, Angulakshmi T, Manivannan D, Seethalakshmi R, Swaminathan P "Password Based Two Server Authentication System", JATIT – 2012
[4] Mihir Bellare, David Pointcheval and Phillip Rogaway "Authenticated Key Exchange Secure Against Dictionary Attacks".
[5] Michel Abdalla. David Pointcheval "Simple Password-Based Encrypted Key Exchange Protocols".

[6] Steven M. Bellovin, Michael Merritt “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”.

[7] Alon Schclar, Lior Rokach, Adi Abramson, and Yuval Elovici , “User Authentication Based on Representative Users”, IEEE November 2012.

[8] Anna Vapen, Nahid Shahmehri, “2-clickAuth: Optical Challenge-Response Authentication Using Mobile Handsets”, International Journal of Mobile Computing and Multimedia Communications, April-June 2011.

[9] Bob Zhang, Wei Li, Pei Qing, David Zhang, “Palm-Print Classification by Global Features”, IEEE March 2013.