Efficient Authentication System using Mind metrics and PAKE Protocol

Shital Bhise¹, Sujata Chaudhari², Pradnya Pujari³, Mayuri Shinde⁴
Department of Computer Engineering,
P.E.S. Modern 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 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. 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 mind metrics is implemented where personal data instead of a login ID to identify a user uniquely. 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, i.e., mind metrics token. This additional step raises the security of an authentication system. In verification phase, the concept of two server Password Authenticated Key Exchange (PAKE) protocol, a client splits its password and stores two shares of it in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. In these system two compilers that transform any two-party PAKE protocol to a two server PAKE protocol on the basis of the identity based cryptography, called PAKE protocol. By the compilers, we can construct PAKE protocols which achieve implicit authentication and implemented to prevent the password from getting hack. The proposed system does not make use of any hardware device and is cost effective.

1. Introduction

Computer systems use an authentication mechanism to allow access only to legitimate users. The authentication process is consisting of two parts, identification and verification. Identification is a process to recognize an unknown individual out of many (1:N relationship) and verification process, the system asks a proof of the ID since the system does not know whether the user is the legitimate ID holder (1:1 relationship). Traditionally the identification was performed by a “username” or login ID and the “password” for verification. The passwords are supposed to be a random characters, login IDs are not random. They are used for communication or accounting purpose, and must carry a meaningful pattern. It may be part of user’s first and/or last names, part of social security number, combination of names and numbers, account number or email addresses. Thus login ID’s 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. The term “Mind metrics” 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. Given these traits, a system can be trained to recognize certain people, with a certain probability. Biometrics refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. Mind metrics 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 mind metrics. The concept of biometrics or mind metrics is used in authentication schemes to identify a user with legitimate ID holder.

In a password based system, the plaintext passwords are transferred into hash values is generated from the newly entered password, and compared with the stored hash values in the password hash file. If the hash value matches, access is granted. This password verification process is the heart of the most authentication systems. There are number of ways to stole the user’s password for illegal access.

In password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication system. The two secure channels are established for all two-server PAKE protocols, where a password is
split into two parts, which are securely distributed to the two servers. We refer to the concept of public key cryptosystem; the encryption key of one server should be unknown to another server. PAKE protocol is symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

2. Proposed System

A system is proposed where security is provided to both the phases of authentication process without the involvement of any specialized devices. 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. 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.

In the proposed system the login ID is not considered a secret. The concept of mind metrics is implemented where personal data instead of a login ID to identify a user uniquely. 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, i.e., mind metrics token. This additional step raises the security of an authentication system. 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, true login ID, fake login ID\}. All these functions are carried out at Identification Server.

In verification process, the concept of two server Password Authenticated Key Exchange (PAKE) protocol, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. Each of the password part is encrypted using ElGamal Algorithm and is sent to the respective 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.

We propose a new symmetric solution for two-server PAKE. The password pw is secret unless the two servers collude. Although we use the concept of public key crypto system, our protocol follows the password-only model. The encryption and decryption key pairs for the two servers are generated by the client and delivered to the servers through different secure channels during the client registration, as the client in any two-server PAKE protocol sends two halves of the password to the two servers in 4secret, respectively. In fact, a server should not know the encryption key of another server and is restricted to operate on the encryption of the password on the basis of the homomorphic properties of ElGamal encryption scheme. Security analysis has shown that PAKE protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

3. Algorithms

3.1 Diffie-Hellman key Exchange Protocol

The Diffie-Hellman key exchange protocol was invented by Diffie and Hellman in 1976. It was the first practical method for two users to establish a shared secret key over an unprotected communication channel.

Consider two users Alice and Bob, who are totally unaware of each other, but want to establish a secure communications between them.
Diffie-Hellman key exchange protocol can be used 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 $\mathbb{Z}_q$ and computes $X = g^a$, while Bob randomly chooses an integer $b$ from $\mathbb{Z}_q$ and computes $Y = g^b$. Then Alice and Bob exchange $X$ and $Y$.
3. Alice computes the secret key $k_1 = Y^a = g^{ab}$, while Bob computes the secret key $k_2 = X^b = g^{ab}$.

It is obvious that $k_1 = k_2$ and thus Alice and Bob have agreed on the same secret key, by which the subsequent communication 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.

### 3.2 ElGamal Encryption Scheme

ElGamal encryption scheme was invented by ElGamal in 1985 [3] on basis of Diffie-Hellman key exchange protocol. It consists of the key generation, encryption, and decryption algorithm.

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

#### 3.2.1 Key Generation

The key generator works as follows:

1. Alice generates an efficient description of a cyclic group $G$ of order $q$ with generator $g$. See below for a discussion on the required properties of this group.
2. Alice chooses an $x$ randomly from $\{1, \ldots, q-1\}$.
3. Alice computes $h := g^x$.
4. Alice publishes $h$, along with the description of $G, q, g$, as her public key. Alice retains $x$ as her private key, which must be kept secret.

#### 3.2.2 Encryption

The encryption algorithm works as follows: to encrypt a message $m$ to Alice under her public key $(G, q, g, h)$.

1. Bob chooses a random $y$ from $\{1, \ldots, q-1\}$, then calculates $c_1 := g^y$.
2. Bob calculates the shared secret $s := h^y$.
3. Bob maps his secret message $m$ onto an element $m' \in G$.
4. Bob calculates $c_2 := m'. s$.
5. Bob sends the cipher text $(c_1, c_2) = (g^y, m'. h^y) = (g^y, m'. (g^x)^y)$ to Alice.

Note that one can easily find $h^y$ if one knows $m'$. Therefore, a new $y$ is generated for every message to improve security. For this reason, $y$ is also called an ephemeral key.

#### 3.2.3 Decryption

The decryption algorithm works as follows: to decrypt a cipher text $(c_1, c_2)$ with her private key $x$.

- Alice calculates the shared secret $S := c_1 x$ and then computes $m' := c_2 . s^{-1}$ which she then converts back into the plaintext message $m$, where $S . i$ is the inverse of in the group $G$. (E.g. modular multiplicative inverse if $G$ is a subgroup of a multiplicative group of integers modulo $n$).

The decryption algorithm produces the intended message, since

$$C_2 . s^{-1} = m'. h^y . (g^x)^{-1} = m'. g^{xy}. g^{-xy} = m'.$$

### 4. Related Work

In Identification process the main focus is improving the security of the authentication system by supplementing it with a secure identification process. To make false login attempts difficult, our method does not use a publicly known login ID for identification. Instead it uses private information known only to the computer system and the user. This process makes the stolen password files unusable for the attackers.

In Verification process traditional system have drawback of the password that passwords are stored in a hash table using a cryptographic hash value of the password over a public channel which makes hash value accessible to an attacker. This was because the password was stored in a single server in hash table, it is not very difficult for a attacker to get the password from a hash value to over increase the strength the two secure channels are necessary for all two-server PAKE protocols, where a password is split into two parts, which are securely distributed to the two servers, during registration. Although we refer to the concept of public key crytosystem, the encryption key of one server should be unknown to another server and the client needs to remember a password only after registration.

### 5. Conclusion

User authentication process is done in two steps, identification and verification. The traditional password-base verification system are been challenged by sophisticated attacks, but the new schemes are being made to cover the weakness of the password-based systems. Proposed system is more efficient and secure. The proposed system overcomes all the drawbacks of conventional password based system. We concentrated on adding extra security to
identification as well as verification processes. A new concept called mind metrics 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 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. 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 mind metrics and two-server authentication protocol. In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

6. References


