OPTIMAL STRONG PASSWORDS AUTHENTICATION PROTOCOLS

[1]Sanya Jain, [2]Avani Kasat

Students
Vellore Institute of Technology

Abstract: The process or action of proving or showing something to be true, genuine, or valid is called authentication.
The proper functioning of OSPA (Optimal Strong Password Authentication) has been explained that how it functions and how the OSPA can improve the authentication process for obtaining mutual communication between user and server and the secure transfer of data between them.
Two major techniques can be used for the same — Hash Function and using USB Sticks.
Authenticating passwords using USB sticks is described with all the phases that are: Initialisation Phase, Registration Phase, Login and Authentication Phase and the Password change activity. These activities are described using proper notations and the diagrammatic representation.
As in Existing system only one hash function is used, so only the same value is passed every time during authentication. In multiple hash function will be used, so the values keep changing each time of authentication. So, the attacker cannot find the values.
The Proposed system is based on the cryptography. Cryptography plays a major role in computer security. It is a method of transferring private information and data through network communication, so only the receiver who has the secret key can read the encrypted messages. The messages could be in the format of images, texts or videos etc. Security issues in text-based password authentication are rarely caused by technical issues, but rather by the limitations of human memory, and human perceptions together with their consequential responses can be resolved using cryptography.

2. Introduction

Authentication can be described as the process or method which is used to recognize a true user's identity and the verification is done for the real user with the help of the credentials such as userid and password to avoid fake users.
This is done through a mechanism by taking the credentials from user and then verifying them using some protocols. The credentials are usually a userid and password, where password is a secret to everyone except the user and the system. The credentials that are being provided by the user are compared to those saved in a database where all user's credentials are being saved on a local operating system or an authentication server.
The weakness in this system is that passwords can often be stolen or forgotten and the person who stole the password could access the data of the user. When we are trying to protect our information online, passwords are the most used form of authentication for the websites and applications. Also, Cyber criminals can gain access to a system and steal information when user authentication is not secure. Authentication is important in security because it enables the organisations to keep their networks secure by permitting only authenticated users. Different organisations can use different methods to protect the data of the users.

3. Background and related work

Earlier, Lamport's One Time Signature Method was introduced. It is a method which is used for constructing a digital signature and it also typically involved the use of a cryptographic hash function. It is a type of one-time signature scheme; it can be used to securely sign one message. It was the first password authentication protocol introduced in this filed. This protocol was highly questionable by the community because it has a high hash overhead and the necessity to reset the password in addition to being vulnerable to the reply attack and the guess attacks by the fake users.
Later many algorithms and protocols have been introduced such as authentication using USB Sticks, single hash function, multiple hash based strong password authentication protocols. Some are resisting the fake users guessing attacks some are not able to resist them. Some protocols are also using One-time passwords but still strong authentication is not being done. So, the need for introducing a strong password authentication protocol became necessity to be introduced.

4. Existing system

The password authentication mechanism has three classifications which are: the password only PA protocols, the dedicated device aided protocols and memory device aided protocols.
The password only PA protocols does not use any external device, it simply uses a password that is memorised by the user and saved in the server. In dedicated device aided protocols, the user remembers a short password hold the special devices, for e.g., Smart Cards. The authentication information is stored in smart card and is not accessible to others except user and server.
In memory device aided protocols, the authentication information is stored in devices or drivers for the authentication by server.
We can also use Password authentication protocol. In this protocol the password created by the user is not encrypted and send to the server as plain text. This protocol is most likely to get a security threat, the user's data is not secure.
Hashing is also a technique for the authentication of real users. Hashing refers to the chopping of something into small pieces so that it looks like a mess and is difficult for anyone to guess. In this protocol we use encryption tools such as MD5, Secure Hash Algorithms (SHA) to encrypt the passwords which makes it difficult for a hacker to hack the password and get access to user's data.

5. Proposed system

In today's era, information/personal details are one of the most important and valuable assets that an organization or an individual can have. That is why keeping sensitive and private information away from prying eyes has the utmost importance in today's era. For this purpose, we are proposing authentication protocols using cryptography methods.

Cryptography is one of the most important fields in terms of computer security. Most importantly it plays an important method to be used for authenticating passwords. Cryptography is basically a method of transferring private information and data for example, credentials to sign in in any application or a software through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be in the form of documents, phone conversations, images or other form of data. To keep user's privacy simply by encrypting the information which should be hidden from everyone else can be achieved by using methods of Cryptography. The information must be crambled, so that the other users cannot access the actual information.

Cryptographic authentication is concerned with recognising an entity as the one that is in possession of a secret cryptographic key.

Cryptography provides following services:

1. Authentication of credentials, passwords or any user's entity.
2. It ensures the pure confidentiality of the user's data so that no one else can read it.
3. It keeps integrity and assurance that the information is same from source to destination. It never changes in between.
4. The information is secured 100%.
5. Only the authorized users and real users can get access to the data. It will be done after authentication only.

5.1 Classification of Cryptography

Now, depending on the type of keys and encryption algorithms, cryptography is divided into the following categories:

1. SYMMETRIC KEY
2. THE KEY TO ASYMMETRIC

A system in which the sender and recipient of a message share a single, common key used to encrypt and decrypt a message. The most popular equivalent system - key is the Data Encryption Standard (DES).

Also, a transposition cipher is a method of encryption where positions held by writing units (usually characters or groups of characters) are moved according to a standard format, so that the transcript is a written permission.

Asymmetric Key Encryption (or Public Key Cryptography) is an encryption process in which various keys are used to encrypt and decrypt data. Keys are different but mathematically related, such as finding clear text by deleting asymmetric text is possible. Asymmetric Key Encryption (also known as Public Key Cryptography) is a method of encryption where different keys are used to encrypt and delete text, messages or details. Keys are different but statistically related to permissions, such as retrieving explicit text by encrypting mathematical text can be easily done.

RSA is the most widely used encryption method for public keys, in this type of encryption Both public and private keys are interchangeable. Contains a Variable Key Size (512, 1024, or 2048 bits).

Identification and verification can be defined as a process that can be used to identify and authenticate users to their secure systems. In a secure system, the user must identify himself, then the system will verify their identity before allowing them to use the system. However, authentication confirms the user requesting the access process to determine who the user is a real user or not trying to access the system. The authentication and authentication process are successfully implemented using the following three methods:

1. Something known: With a password or ID number (PIN).
2. Something found: smart card or token identification.
3. Natural features: facial recognition or recognition, details of fingerprints, voice, retina, or risk features.

Procedures for identifying and authenticating can be seen as:

SMS-based verification

5. Symmetric-key authentication
6. Authentication of public keys

5.2 AUTHENTICATION ALGORITHMS:

1. Authentication with Symmetric Key Cryptography:

Authentication with Symmetric Keys mechanism that will help in protecting the application for integrity and confidentiality. Symmetric key cryptography is the method which relies on a single, shared, secret key that is used to both sign message and encrypt a message, and is usually faster as compared to public key cryptography.

In this Cryptography, the user is first authenticated by sending to the authentication server his/her username together with a randomly challenge message that is already encrypted by the secret key. And the user is considered as authenticated and real user if and only if the server can match the received encrypted message using its share secret key.

2. Public key authentication: Diffie-Hellman Authentication:

The key exchange is playing the role of an important method in public-key Cryptography for providing authentication cryptographic service. It was the very first public-key cryptographic method as developed by Whitfield Diffie and Martin Hellman, were the first who developed this key exchange algorithm that is called DH. In this method, keys are exchanged between the users according to various Cryptographic protocols which are based on the key exchange problem. They highlighted the most important method of exchanging the keys by using the discrete logarithm hard problem.

6. Results

In term of security, the use of password authentication is considered very weak, this is because of the software attacks. So, in our paper we have improved the process of authentication by using cryptography. In Existing system hash function is used, so only the same value is passed every time during authentication and also, we use USB Sticks for the authentication purpose. In Proposed system we use the cryptography method. Cryptography provides the data confidentiality, authentication and data integrity.

Conclusion

This paper summarises the method of cryptography for the optimal strong password authentication. It shows the possibility of using different methods which are password, public key sharing, symmetric key, token, and biometric authentication methods. The performance of these methods are actually different according to their tools cost, execution time and the security. Our main concern in this research paper was to find a solution for the issues regarding authentication. At the end we conclude that public key authentication method non cryptography is the best solution for the same problem.

References

1. International Journal of Network Security, Vol.2, No.3, PP.205–209, May 2006 (http://isrc.nchu.edu.tw/ijns/)
2. https://www.researchgate.net/publication/283672189_Cryptography_Based_Authentication_Methods
3. An Optimal Strong Password Authentication Protocol with USB Sticks by D.Vikram , M.E, Student