An Overview of Various Authentication Methods and Protocols

Dwiti Pandya
Student
Sinhgad Academy of Engineering
Pune, India

Khushboo Ram Narayan
Student
Sinhgad Academy of Engineering
Pune, India

Sneha Thakkar
Student
Sinhgad Academy of Engineering
Pune, India

Tanvi Madhekar
Student
Sinhgad Academy of Engineering
Pune, India

B.S. Thakare
Asst. Professor
Sinhgad Academy of Engineering
Pune, India

ABSTRACT
Nowadays, various online as well as offline activities have become an integral part of everyone's life. So, need for the security has increased drastically. For the secure communication, authentication of the connecting party is one of the prime factors. Many techniques and methods are available for authentication. This paper gives an overview of different methods and protocols of authentication, as well as their reliability in today's world.

General Terms
Authentication, finger prints, passwords, smart cards, credentials, cryptography, biometrics, information cards

Keywords
OTP, PAP, CHAP, Protocols

1. INTRODUCTION
The importance of authentication in today's world cannot be ignored because it plays a vital role and with so many different systems. The common example is internet as practically any action which is taken by user online begins with Authentication. Authentication is the process of giving the access to the system objects individually. It can be achieved in different ways. The most crucial decision in designing secure systems is the importance of selecting an environment appropriate Authentication Method. Authentication protocols are responsible for the authentication of connecting system. This overview describes several Authentication Methods and Authentication Protocols while designing a security system.

2. AUTHENTICATION BASICS
A variety of authentication technologies are available in the market over the years. For understanding these technologies, everyone should be familiar with the standard authentication factors such as something you know, something you have and something you are and how each technology contributes in giving strong authentication capabilities.

1) Something you know:It is specific, secret information, such as a password or an answer to a secret question which perhaps others do not know. These are Knowledge Factors.
2) Something you have:It is an item that is owned, such as a smart card or similarhardware device. These are Ownership Factors.
3) Something you are:It is a physical attribute like fingerprint or voice, which can be identified. These are Inherence Factors.

3. HOW DOES AUTHENTICATION WORK
A user provides credentials such as a password, smart card, fingerprint, digital certificate which identifies that user as the person who is authorized to access the system. The basic authentication process remains same for all methods. In authentication process, a user must have a valid user account with some authority that specifies the user's rights. User credentials account such as a password, a smart card certificate or a biometric scan must be associated with this account. These credentials are entered into the database against which future data will be compared. When the user wants to log in, he/she provides the credentials or passwords and the system checks the database and compares it with the stored one. If the credentials provided by the user match those in the database, access is granted.

4. AUTHENTICATION METHODS
Various methods for performing authentication are as follows:

(a) Password Authentication

(b) Public Key Cryptography

(c) Biometric Authentication

(d) Out of band

4.1 Password Authentication
The most widely used and oldest form of authentication is password. Users provide an id, a typed in word or name, along with a password. In majority of the systems the passwords are encrypted instead of storing it as a plain text. Password authentication does not require the support of hardware as authentication of this type is simple and does not require much processing power. This method has many drawbacks, some of which are:

1) Passwords are easy to guess.
2) Placing the password in a highly visible area.
3) Unsafe due to malpractice of eavesdropping.

Listening to anyone without permission can be managed by using digests. The connecting party sends a value generally

client's IP address or time stamp and any other additional secret information. Because this is unique for each accessed URL, no other documents can be accessed or viewed from other IP address or computers without detection. Because of hashing the password is also not vulnerable to eavesdropping.

4.1.1 One Time Password

To overcome the drawback of password reuse, one-time passwords were developed. A one-time password (OTP) is valid for only a single transaction on a computer system or any other device such as a smartphone. OTP's are generated using random values and hash functions. Types of one-time passwords are a challenge-response password and a password list [1]. The challenge-response password replies with a challenge value (e.g. a random number chosen by the authentication server) after getting a user identifier. The response is calculated using the response value (using a hardware) or from a table based on that particular challenge. A one-time password list makes use of previous passwords which are sequentially used by the user wanting to access a system. The values are generated such that it is very hard to predict the next value from the previously generated values. The time synchronization is also one of the approaches for generating OTP. In this approach, a security token is used. The clock in the token and authentication server is synchronized as generation of the password depends upon current time.

Working principle: User receives a password or some value through the SMS and enters that password or value to complete the process of authentication. Real life example: Use of OTP to login online shopping system.

4.2 Public Key Cryptography

Public key cryptography, which is an asymmetric cryptography, is a class of cryptographic protocols. The two keys are mathematically linked. The private key is kept as a secret and is used to decrypt and public key is used to encrypt messages between the clients. Encryption and verification of signature both is completed using public key.

Advantage of public-key cryptography is that the public key is easily available to the public. They are often published on the Internet so that they can be easily retrieved.

It is used to transfer a symmetrical encryption key by which the message is encrypted because of the computational complexity. It is based on simple algorithms and is much faster. A private key is kept by the user, while the corresponding public key is made available in a certificate digitally signed by a respective certification authority. This certificate is made available to users.

Real life example: Updating data of registered voters with the Registration and Electoral Office.

4.3 Biometric Authentication

Biometric is a common approach for the authentication. Many industries are using biometric as authentication mechanisms for accessing bank machines, door access control and general desktop computer access as well as attendance recording systems in various organizations. These systems recognize individuals based on their physical attributes (fingerprint, face, iris, voice) or behavioral attributes such as signature [2]. Because such characteristics are physically associated with a particular user, biometric recognition is a natural and more efficient mechanism for ensuring that only authorized users can access a system [2]. Biometric Authentication also proved useful in case of multiple identity cards (such as passports, Voter ID) for the same individual. This leads to higher security in the system. The biological pieces used in this process gives different authentication results.

Biometrics has following advantages:

1) Biometric measures do not contain personal information and are more difficult to steal.
2) Biometric measures can be used instead of a name or some number (such as ATM card number) to secure different transactions.

4.3.1 Types of Biometrics

A number of biometric methods are available, but few have gained wide acceptance.

1) Signature Dynamics**:**It is based on an individual's signature, but considered as unforgeable and unique because what is recorded isn't the final image but how it is produced that is. Differences in writing speed and pressure at various points in the signature are observed.
2) Eye scans:The hardware for eye scanning are expensive and specialized, but using it is rather slow and inconvenient and it may make the user uneasy. Two parts of the eye that is the retina and the iris can be scanned, using different technologies and hardware.
3) Fingerprint recognition: Fingerprints are unique. These fingerprints are easily accessible. They require small amount of memory either for the reading hardware or the stored data.
4) Hand or palm geometry:Use entire palm as identifier for the individual. The device that measures the length and angles of individual fingers is also available. These systems are user-friendly than retinal scans.
5) Voice recognition:This is just to verify the individual's voice against a stored voice, not to understand what is being said.
6) Facial recognition:Facial features such as upper portion of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes can be used as one of the attribute in biometric authentication. Areas of the face near the hairline are avoided so that hairstyle changes won't affect recognition.

4.4 Out of Band

Using an Out-of-band verification for authentication involves the bank organization calling a phone number that has been registered with it before and requesting that user to enter their password over the phone before allowing the user to login [3]. Similar to e-mail or SMS OTPs, this requirement is time consuming and requires that the user must be at the location specified by the registered phone number.

5. ONLINE AUTHENTICATION METHODS

5.1 Use of OpenID

It is an open source authentication protocol based on HTTP redirection. It allows users to login to an OpenID enabled site using their own OpenID login id and the respective password rather than having to create another set of id's and passwords [4].

5.2 Use of Information cards

Information cards are open industry standards for managing and sharing digital identities; popular example is Microsoft

Windows CardSpace. These cards are not privately owned by one vendor. An information card relies on someone to issue it and the issuing is done by the identity provider like the certificate authority, as with PKI (Public Key infrastructure) [4]. The identity provider can be any industry that needs to issue identities for its employees or customers and verifies personal data. "Claims" are the data points that are carried in information cards and they are cryptographically signed by the provider. "Relying parties" are responsible for obtaining digital signatures for authentication. These are basically type of services. "The subject" is anyone using a digital identity and they can choose which information from their digital identity to provide to that relying party. The advantage of information cards is its simplified encrypted authentication which means that it does not require a user name and password for website. Sites can operate other access methods at the same time: Customers having the information cards can use them, while others can authenticate themselves using a user name and password.

6. AUTHENTICATION PROTOCOLS

6.1 Secure Socket Layer

The SSL protocol is an Internet standard, which is often used to provide secure access to Web sites, and it uses a combination of public key and symmetric encryption technology. Symmetric encryption is faster, but asymmetric public key encryption provides a better authentication. SSL is designed in such a way that it takes the benefit from both. It is supported by Netscape, Microsoft and other majority of the browsers as well as by most of the Web server software's such as IIS and Apache. The Transport Layer Security (TLS) Internet standard is based on this SSL.

The SSL authentication is based on digital certificates that grant Web servers and clients to verify each other's identities

before establishing a connection. This is also referred to as mutual authentication. Two types of certificates are mainly used: client and server certificates

6.2 PAP

PAP is used for authenticating a user over a remote access control. The most important characteristic of PAP is that it sends credentials across the network to the authenticating or relying server in plain text. This gives a major haphazard, as an unauthorized or an unauthenticated user can also capture the data packets using a protocol analyzer to obtain the credentials. PAP is compatible with many server types running on different OS. This also serves as a major advantage. PAP is very useful in case of compatibility purposes.

6.2.1 SPAP (Shiva PAP)

This type of PAP sends user passwords in an encrypted format and the receiving remote server decrypts it.

6.3 CHAP and MS-CHAP

CHAP is also useful for remote access security. It uses MD5 which is a one-way encryption method. It performs a hash operation on the password and transmits that hash result instead of the password itself over the network. As the password itself does not pass through the network thus it cannot be captured and this becomes advantage over PAP/SPAP.

6.4 Kerberos

Kerberos is an efficient network authentication protocol. It was designed to provide strong authentication for client and server applications which uses secret-key cryptography. It was created by MIT. The Kerberos protocol is used so that a client can establish that it is a genuine user to the server and vice versa across an insecure network. After a client and server have used Kerberos to prove that they are genuine user, they can also encrypt all of their communications so that they can assure their privacy and data integrity [6].

7. AUTHENTICATION IN DIFFERENT SYSTEMS

7.1 Email Authentication

Email authentication basically means that it is a way to ensure that an email provider will be able to identify the sender of an incoming message and ignore the spam and abusive messages sent from unknown users. This authentication data is used to check the source of any message that is received. For example, if you receive a message from a well-known sender for example Hotmail, that isn't authenticated, this message is most likely a spam or may be forged [5]. Receivers can use authentication to verify them from where the incoming message has come and avoid phishing scams and other illegal activities by checking the signed by and mailed by headers in the mails.

7.2 Database Authentication

It is an act of verifying that a user who is about to log in to a database has the permission to do so, and is only awarded the rights to perform activities that he or she has been permitted to do. With related to databases, multiple authentications may be performed by the database itself, or the configuration may be changed to allow either the OS, or some other external method, to authenticate users. Take for example, while creating a database in SQL Server, a user is required to specify whether to use database authentication, OS authentication, or both. Other databases in which security plays an important role require inputs like fingerprint recognition, facial recognition, retinal scans etc.

8. CONCLUSION

With the working technology and times, the need to secure the personal data has increased to keep it safe from hackers and intruders who want to steal the data for their personal benefit. Thus, authentication evolved to make our life a little simpler. Identifiers and passwords first came in use. It was initially efficient but with passing time many drawbacks were realized. Thus, It gave way to newer and make efficient techniques such as biometrics protocols such as PAP,CHAP etc. and people still continue to look for methods to make sure the safety and security of data. Use of different authentication methods such as authentication using different devices or using particular location of your personal computers or laptops will prove useful.

9. REFERENCES

[1] overview-authentication-methods-protocols-118

[2] JainNandakumar_BiometricAuthenticationSystemSecurityUserPrivacy_IEEEComputer2012

[3] sevenstrongauthenticationmethods.htmlfromhttp://www.networkworld.com/article/2296774/access-control

[4] Online-authentication-methods-Personal-information-cardsandWebSSOfromhttp://www.computerweekly.com/tip

[5] understanding-and-selecting-authentication-methods from http://www.techrepublic.com/article

[6] Kerberos from http://web.mit.edu/