ISSN: 2278-4632
Vol-11 Issue-02 2021

Authentication & Key Agreement

[1]Neelamani Samal, [2]Debasish Pradhan, [3]Biswaraj Saheb

[1]Asst. Professor, Einstein Academy of Technology & Management, Bhubaneswar
[2]Asst.Professor, Einstein Academy of Technology & Management, Bhubaneswar
[3]Student, Einstein Academy of Technology & Management, Bhubaneswar

Abstract

The large audience demands online commerce, knowledge sharing, social networks etc., which grew exponentially over the past few years. Thus, it leads to the need for security and enhanced privacy. In recent days, fraud over the Internet constitutes one of the main drawbacks for the widespread of the use of commercial applications. Therefore, the three vital security issues take place every day in our world of transparent fashion, more precisely: identification, authentication and authorization. Identification is a process that enables recognition of an entity, which may be a human, a machine, or another asset such as a software programme.

1. Introduction

The nature of today's web threats is changing current attacks are much more covert than they were in the past. Decision makers need to understand the nature of the threat they face. This made web, network and application security extremely difficult issues. Despite the growing array of threats, many organizations are not taking appropriate steps to safeguard their corporate networks, applications or data. As the number of online services is increasing day by day, their usage is also increasing in the same ratio. Web based authentication mechanism which gained popularity for the reason it allows a simple registration and authentication of customers.

Authentication: Authentication means enabling the network to only admit the authorized users to have access to its resources. It provides the way where the claimed identifier is verified by the access control mechanisms through some means.

Security: The ability of a system to protect data, services and resources against misuse by un-authorized users.

Access control: The discipline in which mechanisms and policies are established that restrict access to the computer resources only to correct users.

Identification: It is a way where a resource claims (or is identified through other means) a specific and unique identifier.

Authorization: Which determines the privileges associated with authenticated identity.

Privacy: The ability of a system to protect the identity and location of its users from un-authorized disclosure.

Smart Card: A small pocket sized plastic card used to make payments and store personal information and which can be read when connected to computer system. It is widely used as hardware token in financial transaction systems especially in Internet based.

E-Voting: E-voting is also known as Electronic Voting, is electronic means of casting a vote and electronic means of counting votes. It can involve transmission of ballots and votes via telephone's private computer network or the Internet.

Authentication Attacks:

Attacks regarding authentication are those which target a web site's method of validating the identity of a user, service or application. These are of the following types.

Brute Force Attack: It is an automated process of trial and error used to guess a person's user name, password, credit card number or cryptographic key. A normal brute force attack uses a single user name against many passwords. A reverse brute force attack uses many user names against one password. When a guessed password allows access to the system, the brute force attack has been successful and the attacker is able to access the account.

Brute Force techniques are highly popular and often successful in systems with millions of user accounts.

ISSN: 2278-4632
Vol-11 Issue-02 2021

Weak Password Recovery Validation:
When a website permits to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password. The user should be the only person that knows the password and it must be remembered precisely. With the passage of time, a user's ability to remember a password fades. The complication increases further when the average user visits 20 or more sites requiring them to supply a password. A website is considered to have Password Recovery Validation when an attacker is able to foil the recovery mechanism being used. This happens when the information required to validate a user's identity for recovery in either easily guessed or can be circumvented. Password recovery systems may be compromised through the use of brute force attacks, inherent system weaknesses or easily guessed secret questions. Example of automated password recovery processes include requiring the user to answer a "secret question " defined as part of the user registration process. The second mechanism in use is having the user provide a " hint " during registration that will help the user remember his password.

Information Verification:
Many web sites only require the user to provide their e-mail address in combination with their home address and telephone number, which can be obtained from any number of online white pages easily.

Password Hints:
Password hint aids Brute Force attacks. An attacker can glean about user's password from the hint provided.

Secret Question and Answer:
A user's password could be "KARACHI" with a secret question of "Where were you born?" which helps an attacker to limit a secret answer Brute Force Attack to city names. Besides this, if the attacker knows a little about the target user, learning their birthplace is also an easy task.

Shoulder Surfing Attack:
It is that type of attack when the attacker tries to guess the password by direct observation or by using spy cameras to capture the user entering the password. International Journal of Video& Image Processing and Network Security.

Phishing Attack:
It is the attempt to criminally and fraudulently get/acquire sensitive information i.e. user name, password and credit card details etc.

Reconnaissance Attack:
The act of learning information about the target using publicly available information.

Schemes of Authentication

Usually user authentication involves confirming with a certain degree of confidence that the electronic form of user's identity represented in the IT System corresponds to the real life
Identity of the user. There are three factors of user authentication that may be used in combination to increase the level of confidence in the claimed identity of a user.

Two factor/Token based Authentication:
This scheme uses some physical items called tokens such as smart cards, passports and physical keys. Authentication token or simply a token may be a physical device that an authorized user of computer is given to aid in authentication. Such a token may be physically connected or plugged into the client system. The term may refer to software token as well. Hardware tokens are typically small enough to be carried out in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys such as a digital signatures or biometric data such as a fingerprint. Other may include small keypads to allow the entry of a PIN.
Token based authentication is based on " Something You Have " assumption, in which the user carries a wallet full of credentials (a driver's license, credit card, a university ID card) to certify his/her identity (as a driver, as a credit worthy consumer, or as a student). This system uses both forms of authentication. i.e. it involves using " Something You Know"(i.e. a PIN) and " Something You Have"(i.e. a token). Most widely used forms of two factor authentication are.
(i) Automated Teller Machine(ATM) or Cashpoint Machine Card and PIN.
(ii) Access Control Token and PIN. At an ATM, the user puts his/her Cashpoint/ATM card into
the ATM and the ATM requests the user to enter his/her PIN.
The information held on magnetic stripe of the card together with the PIN, encrypted in a secure block of data, is sent to the Bank's Central Authentication System, where the PIN entered by the user, is compared with the PIN held on file against the user's account number and details. However, in this scheme, personally designed unique information is used as token. Each user is registered against that unique token which becomes his identifying label of the token. Stored information is presented to the system (e.g. ATM card) as well as PIN code to authenticate a user.

One-time Password Token

The main drawback of static passwords is their lack of protection against replay attacks; hence, the purpose of the OTP mechanism is to annihilate the replay ability of passwords with the generation of a new password for each use. OTP systems can be considered as a bridge between a static password authentication and a better authentication method. It facilitates the migration of legacy applications that were designed to rely only on

ISSN: 2278-4632
Vol-11 Issue-02 2021

passwords (mainframes, websites, the IS of an organization. . .). The only impacted component is the monitor, and the IS does not need any change. An OTP token generally consists in a device with an LCD (Liquid-crystal Display) screen, which displays alphanumeric characters. It can have a button to generate OTPs, and some are locked by a PIN code (whose keyboard is either directly on the device either on the reader), so they can be considered as TF-A. As OTP generates a password, the verification requires synchronization between the token and the monitor. There are several categories of OTP, depending on counter synchronized, time synchronized, involving a secure channel, or with a shared list of passwords.

Cryptographic Challenge-Response based Authentication

PAP (Password Authentication Protocol) is a simple protocol for authentication over a network, which sends clear passwords and identifiers over the network. Subsequently, CHAP (Challenge Handshake Authentication Protocol) is an improvement of PAP, but it still requires transmitting a hashed password. The main idea of a challenge-response based authentication is that the claimant proves he/she knows the secret without sending it clear over the channel. Thus, CHAP is a challenge-based authentication protocol, but the transmission of a hashed password is still a problem due to brute force and dictionary attacks besides, hashed passwords still contain a lot of information about the secret password. The main response to solve that problem is the use of cryptography, either symmetric or asymmetric in order to implement a challenge-response authentication. Generally speaking, a challenge-response authentication system is a system that issues a "challenge" on the client request.

An example of a contactless smartcard for logical access control with an embedded fingerprint sensor for match on card (E-smart Technologies). Subsequently, a common means of authentication is by using the Radio Frequency Identification (RFID), which is a technology for transmitting data from devices called RFID tags to a specific reader. In the following subsection, we define how this method can help the users in communication capabilities, especially via Internet.

Conclusion

In this paper, I overviewed the authentication techniques and conclude that the authentication technique is convenient, safe and reliable. This system is pattern recognition system in which a person is recognized based on features derived from specific psychological or behavioral characteristics that the person possesses, which are harder to be theft or stolen

REFERENCES:

1. Authentication" Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, 2003
2. OXID (2011), "Caine & Abel", http://www.oxid.it/, (Accessed 25/3/11)
3. "Comparing Passwords, Tokens, and Biometrics for User", Rohs, M. (2004)
4. Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of
5. Applied Cryptography, CRC Press, pp.4-15, 516, 1996.
6. D. Bhattacharyya, R. Ranjan, Farkhod Alisherov A., and M. Choi. Biometric authentication: A review. International Journal of u- and e- Service, Science and Technology, 2(3):13–27, September 2009.
7. Modern Cryptography Theory and Practice ISBN 0-13-066943-1. An up-to-date book on cryptography. Touches on provable security, and written with students and practitioners in mind