International Journal For Technological Research In Engineering
Volume 10, Issue 6, February-2023 *ISSN (Online): 2347 - 4718*

STUDY OF CONCEPT OF PROTECTING ACCESS OF SYSTEM: AN OVERVIEW

[1]Rahul Kumar, [2]Mr. Ramesh Kumar
[1]M.Tech Scholar, [2]Head of Department (H.O.D)
[1,2]Department of Computer Science & Engineering, K.K University, Nalanda (Bihar)

Abstract: ***By authorizing a human-to-machine transfer of credentials during interactions on a network, user authentication establishes the identity of a user attempting to gain access to a network or computing resource. The human-to-computer interactions on networks can either prevent or allow cyberattacks. We refer to this process where the application identifies the user as user authentication. It is necessary to secure your web application by recognizing and granting access only to authorized users. It is a security procedure that prevents unauthorized users from accessing your network or device. A user's authentication fails if they don't have the proper login rights to the network. It's a login procedure where an application asks for personalized passwords to authorize access to it.***

Keywords: Wireless Sensor Network, WSN Security, Nodes.

1. INTRODUCTION

The user authentication process covers all interactions between a human and a computer, such as registering and logging in. Simply put, authentication asks each user, "Who are you?" and verifies their answers. Users who register for an account are required to create a unique ID and key that will allow them to access their account later. The ID and key are generally a username and password, but other credentials can also be used. Essentially, User Authentication is a process that authorizes access to an online service, connected device, or other resource by verifying a person's identity. This allows them to access their own account, while preventing unauthenticated users from gaining access. [1]

Since business logic and risk profiles at enterprises can differ significantly, authentication occurs differently across services. The basic foundation for tying together authentication solutions is that the user must provide one, or more, of three authentication factors: knowledge (such as a PIN), possession, and inherence (biometrics). User authentication is also becoming increasingly based on contextual information from web browsers and mobile devices. These data points cover continuous authentication, as well as adaptive, dynamic, risk-based, and other authentication methods, with some overlap of terminology and meaning. [1]

It is the process of proving that something is genuine. The term authentication is often associated with proving a user's identity in computer science. In most cases, a user demonstrates their identity by providing their credentials, which are information that the system and the user have agreed upon. The most popular authentication mechanism is the username and password combination. [2]

A well-known example is accessing a user account on a website or a service provider such as Facebook or Gmail. Services typically present a screen that asks for your username and password before you can access your account. They then compare the data the user inserts with the values previously stored in an internal repository. [2] Your account will be accessible if you enter a valid combination of these credentials. Although the username may be public, like an email address, the password must be confidential. Because passwords are confidential, they must be protected from cybercriminals' stealing. Even though usernames and passwords are widely used on the internet, they are notoriously weak security mechanisms that are easily exploited by hackers. [3]

A strong password, that is, one whose complexity is sufficient to prevent malicious attackers from easily guessing it, is the first way to protect them. It is generally recommended to use a complex combination of lowercase and uppercase letters, numbers, and special characters to create a strong password. Otherwise, a weak password will result from an insufficient combination of characters. A report by SplashData, a security firm, identifies the 25 most common passwords used by end users. Millions of users use passwords like "123456" and "password" to authenticate, according to the list, which is derived from millions of passwords exposed by data breaches. [3]

Weak passwords are usually easier to remember. In addition, they often reuse the same password across multiple websites. Weak passwords are easy to guess, and leaked passwords can be used to access multiple services for the same account. A strong password, on the other hand, can withstand brute force attacks, but it can't withstand attacks like phishing, keyloggers, or password stuffing. In these types of attacks, the password is stolen directly from the user rather than guessing it. In a recent news report, Facebook was shown to have stored millions of Instagram passwords in plain text. Passwords should always be stored using best practices, such as hashing. [3]

2. WORKING OF USER AUTHENTICATION

To gain access, users must prove to the site that they are who they say they are. The user's ID and key are sufficient to confirm the user's identity. However, authorization is what determines what users can view and do when they log in. Although authorization and authentication are often used interchangeably, they work together to create a secure login process. [4]

User authentication consists of three steps:

- Provide a connection between the human (user) and the website's server (computer).
- Identify users and verify their identities.
- The system will proceed to authorizing the user once the authentication is approved (or declined).

On the website's login form, users input their credentials. That information is sent to the authentication server, where it is compared with all the user credentials available. The system will authenticate users and grant them access to their accounts if a match is found. If not, users will be asked to re-enter their credentials. After several unsuccessful attempts, the account may be flagged for suspicious activity or require alternative authentication methods such as a password reset or a one-time password.[5]

Types of User Authentication

When the word "technology" is uttered, authentication and security are unavoidable topics. Authentication is the first step to enhancing security due to the increasing demand for it. It manages user identification and grants them suitable access control for smooth operation and defense. Authentication should not be confined to usernames and passwords only; rather, Single Sign-On (SSO), Multi-Factor Authentication (MFA), Provisioning, Adaptive Authentication, and other Identity and Access Management (IAM) tools can reinforce conventional authentication methods. An array of authentication options are available when it comes to authentication and security. You should be aware of a few key factors before adopting or choosing any of the authentication methods for your Organization's employees or end users in order to choose the most appropriate authentication technique: [6]

Password Based Login: Password-Based Authentication is the most commonly used method for logging into online services. It involves entering a combination of a username/mobile number and password to gain access. However, as customers use more and more services, it becomes challenging to keep up with all their different usernames and passwords which can lead to bad behaviours such as forgetting passwords or using the same credentials across multiple sites; an opportunity for cybercriminals to exploit through activities like phishing or data breaches. This is why many companies are now shifting towards adding additional layers of security beyond traditional logins. [6]

Authentication with multiple factors: Authentication using multiple factors (MFA) is the process by which an individual must pass multiple factors to access a service or network. It adds another layer of security to the standard password-based login process. Additionally, individuals will be required to provide a second factor, a one-time code they will receive via phone or email along with their username and password. You can easily set up various Multi-Factor Authentication (MFA) methods to add an additional layer of security to your resources. Examples include OTP/TOTP via SMS, OTP/TOTP over Email, Push notification, Hardware Token and Mobile Authenticator (Google, Microsoft, Authy, etc.). Depending on your needs and requirements, you can select any MFA technique for enhanced security. To bolster security even further, both password-based traditional authentication and Multi-Factor Authentication are usually deployed together. [6]

Authentication using biometrics: Biometrics are used to authenticate individuals with the help of physical traits like fingerprints, palms, retinas and voice. This technology is primarily employed in places where security is a priority, such as airports, borders and private organizations. The method involves saving the person's data into a database for it to be matched against whenever they need to access any device or premises. It provides extra protection against unwanted access and makes user experience more pleasant. There are several popular biometric authentication systems that are used nowadays: fingerprint scans, retina scanning and facial recognition. [7]

Fingerprint authentication is one of the most popular biometric technologies for users, as it matches the unique pattern of an individual's print and is incredibly user-friendly and accurate. Some advanced systems even sense vascular structure too, elevating its level of security. It's not difficult to see why: fingerprint access has become commonplace, with people using it on their phones and businesses implementing it. [7]

Retina & Iris : The retina and iris are scanned using a strong light that looks for distinctive patterns around the pupil of the eye. In order to verify the identity, the scanned pattern is compared with data stored in a database. Eye-based authentication can be inaccurate when a person wears spectacles or contact lenses. [8]

In **facial authentication**, multiple aspects of an individual's face are scanned when they attempt to access a particular resource. The results of face recognition can be inconsistent when comparing faces from different angles or when comparing people who look similar, such as family members. [8]

Authentication based on certificates: Certificate-based authentication helps to identify people, servers, workstations, and devices by issuing an electronic digital identity. This is similar to the way a driver's license or a passport serves to confirm a person's identity. A certificate contains information like the user's public key and the certification authority's digital signature that verify the public key and its issuer are the same person. To access a server, one must present their

digital certificate which is then verified in terms of its identity and credibility through cryptographic validation of the accompanying private key. [9]

Authentication based on tokens: Using token-based authentication, users only enter their credentials once and receive an encrypted string exchange as a result. If you have a digital token, you won't have to enter your credentials every time you want to log in or gain access. The token ensures you already have access. Most use cases, such as Restful APIs that are accessed by many frameworks and clients, require token-based authentication. [9]

SSO (Single Sign-On): Using Single Sign-On authentication offers greater security and multiple advantages to your customers. With SSO, they will only need to enter their username and password once to gain access to all the configured applications. This saves them from having to remember multiple sets of passwords for different services and increases efficiency with fewer support calls for password and login issues. Moreover, it eliminates the risk of passwords being forgotten or written down on sticky notes. [10]

2nd Factor Authentication (Two-Factor Authentication): "Two-factor authentication" is an extra layer of security that requires two separate authentication steps before granting access to a certain resource. This type of protection can help ward off cyber assaults such as data breaches, phishing, and keylogging. With miniOrange, you can configure any application on any platform and enable 2FA with options like One Time Passwords (OTP via SMS/Email), Push Notifications, Biometrics, Authenticators (Google Microsoft,Authy), Yubikey and Hardware Token. Recent security surveys suggest that 2FA can prevent up to 80% of data breaches. [10]

Adaptive Authentication: Adaptive Authentication is a more sophisticated form of two-factor authentication (2FA) that adapts to the context. Administrators can authenticate users based on their applicable details such as IP address, device type, location, and time of access. When IP and location-based authentication are enabled, after entering their username and password, Adaptive Authentication will check for consistency between the user's IP address with that used by the administrator and whether he is in the assigned location. Should any discrepancy exist, access to the resources will be denied. This advanced authentication method is often employed by businesses to ensure their security. [11]

3. CONCLUSION

Keeping unauthorized users from gaining access to sensitive information requires a strong understanding of user authentication. A strengthened authentication process ensures that User A only has access to the information they need and cannot see the sensitive information of User B. Cybercriminals can access your system if your user authentication isn't secure, however, and steal whatever information the user is authorized to view. In the past, organizations have failed to secure their websites and suffered data breaches, such as Yahoo, Equifax, and Adobe. These companies serve as a warning about the negative consequences of insecure user authentication processes. These scenarios were not only costly for the organizations involved, but they also damaged their reputations and decreased user trust, among other things. This is why it's imperative that your organization does not become the next victim of such a cyber-attack. In order to avoid such a situation, it's a good idea to invest in high-quality authentication tools to help you secure your website..

REFERENCES

1. Seung-Hyun Kim Daeseon Choi and Seunghun Jin "Digital ID Wallet: Provide Selective Disclosure and Users Control of Identity Information" Security and Management pp. 457-462 2009.
2. S. -H. Kim and S. -H. Kim, "General authentication scheme in user-centric IdM," 2016 18th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 2016, pp. 737-740, doi: 10.1109/ICACT.2016.7423540.
3. Y. Lakh, E. Nyemkova, A. Piskozub and V. Yanishevskyi, "Investigation of the Broken Authentication Vulnerability in Web Applications," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 2021, pp. 928-931, doi: 10.1109/IDAACS53288.2021.9660889.
4. D. Stuttard and M. Pinto The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws John Wiley & Sons Inc. pp. 878 2011.
5. W. Du Computer & Internet Security: A Hands-on Approach USA Middletown DE pp. 690 2019.
6. L. Dostálek, "Multi-Factor Authentication Modeling," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 443-446, doi: 10.1109/ACITT.2019.8780068.
7. F. Alaca and P. C. v. Oorschot "Device fingerprinting for augmenting web authentication: classification and analysis of methods" ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications 2016.
8. Z. Yang R. Zhao and C. Yue "Effective Mobile Web User Fingerprinting via Motion Sensors" 2018 17th IEEE International Conference On Trust Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering 2018.
9. D. S. K. Putra, M. A. Sadikin and S. Windarta, "S-Mbank: Secure mobile banking authentication scheme using signcryption, pair based text authentication, and contactless smart card," 2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering, Nusa Dua, Bali, Indonesia, 2017, pp. 230-234, doi: 10.1109/QIR.2017.8168487.
10. Fenghui Liu "Efficient Two-Factor Authentication Protocol Using Password and Smart Card" in Journal of Computers Academy Publisher vol. 8 no. 12 pp. 3257-3263 Desember 2013.

11. M. Munandar and A. R. Hakim Analisis Keamanan pada Based Text Authentication pada Skema Login Surabaya:Seminar Nasional Sistem Informasi Indonesia 2013.
12. E. S. Nurcahyanto Penerapan Metode Pair Based Text Authentication Scheme pada Aplikasi Screen Lock sebagai Alternatif dalam Meningkatkan Keamanan Smartphone Android (Ice Cream Sandwich) Bogor:Sekolah Tinggi Sandi Negara 2015..