International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 11 | Nov - 2021 ISSN: 2582-3930

RESEARCH PAPER ON TWO FACTOR AUTHENTICATION (2FA)

PARTHA MANISH VICHARE

Keraleeya Samajam's Model College , Dombivili East, Mumbai, Maharashtra, India

Abstract:

Two factor Authentication is been used to control access to sensitive system and data. It is implemented better protect both a user credentials and the resources the user credentials and the resources the user can access. It adds an additional layer of security to the authentication process by making it harder for attackers. First factor can be a biometer factor such as a fingerprint or facial scan.

Introduction:

With so much of our lives happening on mobile devices and laptops, it is obvious that our digital accounts have become a magnet for criminals. Especially in Banks, Goverment offices, Health Care industry, Defense organizations are setting standards, passing las and forcing organizations and agencies to comply with these standards with non compliance being met with wide ranging consequences.

Two factor authentications has been introduced in order to improve security in authentication systems. Different factors have been introduced , which are combined for means of controlling access. The increasing demand of high security applications has led to a growing interest for protecting confidential data using password, token, biometrics etc.

Two-factor authentication has long been used to control access to sensitive systems and data. Online service providers are increasingly using 2FA to protect their users credentials from being used by hackers who stole a password database or used phishing campaigns to obtain user passwords.

Two-factor authentication
Pick any two: Something you know, something you have, something you are
Username

What is two-factor authentication:

Something you have
Something you know
Something you are

Two-Factor Authentication has been introduced in order to enhance security in authentication systems. Two-factor authentication requires users to present two of the following types of authentication factors:

1. Something they know (traditionally a password)

2. Something they have (such as a phone or hardware token)

3. Something they are (referring to biometrics, such as a fingerprint)

A good example of two-factor authentication is **the withdrawing of money from an ATM**; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out.

Advantages of Two-Factor Authentication:

The main advantage of two-factor authentication is **the increased login security**. Two-Factor Authentication is an authentication mechanism to double check your identity is legitimate.

Benefits of multi-factor authentication

1. Improves user experience
2. Provides greater security
3. Protects against brute force attacks
4. Reduces cost in the long run

Two factor authentication works as an extra step in the process, a second security layer, that will re-confirm your identity. Its purpose is to make attackers life harder and reduces fraud risks. If you already follow basic password security measures, two-factor authentication will make it more difficult for cyber criminals to breach your account because it is hard to get the second authentication factor, they would have to be much closer to you.This drastically reduces their chances to succeed.

Disadvantages of Two-Factor Authentication:

As for the disadvantage, the main two being the increase in the time of entry into the system and the risk of losing the physical media serving to pass one of the authentication steps (mobile phone, U2F key, OTP-token

Other disadvantage are

1. Factors can get lost. There is no certainty that your authentication factors will be available when you need them.
2. False security. Two factor authentication provides a level of security, but its typically exaggreated.
3. It can be used against users.

How Does Two Factor Authentication Work:

Two-factor authentication is becoming increasingly used and support by a majority of companies, meaning you can set policies and two-factor authentication requirements for accounts such as gmail, microsoft office, and more. Social media accounts, banks, email clients, banking, and payment apps all allow to turn on two-factor authentication. On the user side, most forms of two-factor authentication feels just like entering two different password you just have to make sure you have access to your phone or email.

Two-Factor authentication protect your account with an extra layer of security by requiring access to your phone. Once configured you will be required to enter a code created by the Google Authenticatior or Duo Mobile apps in order to sign into your account.

Why Two-Factor Authentication

Two-Factor Authentication limits the ability of a cybercriminal to hack your account remotely using only a password. If you are not using two-factor authentication, your account could be compromised through a brute-force attack or your credentials might be stolen from your device via a malware attack. In any case, a strong password alone is not enough to protect your accounts. Two-factor authentication is one most effective steps you can take to improve your digital security. It can protect businesses, both large and small, against data loss when an employee’s computer or digital accounts are hacked remotely or via malware. In the vast majority of cases, two-factor authentication will protect accounts from cyberattacks and ensure personal or business data isn’t compromised or stolen.

Conclusion:

Two-Factor Authentication is one the most effective ways to protect your accounts from unauthorized access and improve data security within your household or business. Today most websites and apps offer some sort of two-factor authentication and we highly recommend making use of it. Whether you choose to use a one-time password, an authenticator app, or a security token, two-factor authentication will provide siginificantly enhanced security compared to using a password alone.

REFERENCE

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy Mag., vol. 1, no. 2, pp. 33–42, 2003

[2] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.

[3] M .Swathi, M. V. Jagannatha Reddy, Authentication Using Persuasive Cued Click Points International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July-2013 IJERT ISSN: 2278- 0181.

[4] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P.C. vanO or schot, Member, IEEE “Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points” IEEE Transactions on Dependable and Secure Computing, volume 03-No. 3. Issue 01 March 2012.

[5] L. Jones, A. Anton, and J. Earp, “Towards Under standing User Perceptions of Authentication Technologies,” Proc. ACM Workshop Privacy in Electronic Soc., 2007.

[6] Fatehah M.D., MohdZalishamJali&Wafa M.K., Nor Badrul Anuar, “Educating Users to Generate Secure Graphical Password Secrets: An Initial Study” 2013, IEEE.

[7] Muhammad Daniel Hafiz Abdul Hanan Abdullah, NorafidaIthnin, Hazinah K. Mammi, “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”, 2008, IEEE.

[8] Smita Chaturvedi, Rekha Sharma, “Securing text & image password using the combinations of Persuasive Cued Click Points with the help of Improved Advanced Encryption Standard, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[9] Madhuri Achmani, Radhika Dehaley, Anuja Gaonkar, Anindita Khad, Two Level Authentication System Based on Pair Based Authentication and Image Selection, IJRASET Volume 4 Issue IV, April 2016 ISSN: 2321-9653.