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

Three Factor Authentication

Lakhansingh Jayramsingh Pardeshi
Keraleeya Samajam (Regd.) Dombivli's Model College

Abstract: In Spite of many efforts taken nowadays still security threats can be seen everywhere. And from the start we are using just single level password authentication factors, which is not sufficient to give more security.

In order to be more secure we can think of Three Level Password Authentication System.So this is an idea to implement three levels password authentication for true users. In short we can say, this is to implement three levels of security. The First level password consists of a simple text based password and this effort is taken to resist shoulder surfing attack through the text password. The Color Combination password there is basically three colors red green blue (RGB) where user can set different combination of colors according to their choice just by clicking on those colors forms the second level of authentication.Third level uses a Picture Password there at first user have to select an image in jpg format to use as a password and then the user can set the password by clicking on the image in different places. These three
levels of password in securing the resources from unauthorized use.

Keywords: Shoulder Surfing, Graphical Authentication, Text Based Authentication.

Introduction

This project gives more security to the user and validates users for accessing the system only when they have input the correct password. The the project involves three levels of user authentication. There are varieties of password authentication systems available nowadays but many of which have failed due to bot attacks while few have sustained it but to a certain limit. In short, almost all the passwords are authenticated .The system available today can be broken down easily. Hence this project is aimed to achieve the highest security in authenticating or validating correct users.This project contains three logins which include three different kinds of password systems. The password difficulty increases as the authentication level increases. Users have to enter Or input the correct password in order to successfully login. Users will be given privilege Or have rights to set passwords according to their wish. This project

comprises text password i.e. passphrase, color combination and graphical password for the three levels respectively. Along these lines there would be immaterial odds of bot or anybody to split passwords regardless of whether they have broken the principal level or second level, it is difficult to break the third one. Consequently while making The innovation of the accentuation was put on the utilization of inventive and non traditional techniques. Numerous clients locate the most broad text-based secret key frameworks hostile, so on account of three level secret key we had a go at making a straightforward UI and giving clients the best possible comfort in solving passwords.

Purpose, Needs, and Motivations for Multi factor Authentication .

There are typically three primary motivations for why people and organizations use MFA: security, compliance, and usability.

Security

The strength of authentication systems are largely determined by the number of factors or layers incorporated into the system. While each authentication method has strengths and weaknesses, systems that use two or more different factors are typically considered stronger than those that use only one factor.

Compliance

Almost every organization has some level of local, state, and/or federal compliance to which they must adhere. Many of these regulations specify that organizations must utilize MFA under certain circumstances, like when accessing particular types of data or connecting from certain locations. There is pressure for organizations to maintain compliance in order to mitigate audit findings and avoid potential fines and other penalties.

Usability

The key need regarding usability revolves around the concept that “passwords are dead.” This phrase commonly heard has two core meanings. First, people have too many passwords for their devices and applications, whether personal and/or professional. Furthermore, if you follow password best practices and make each one different and complex, most technical folks even struggle with the task. While password managers and IAM systems with single sign-on provide significantly reduced password-related headaches, with MFA, there are some opportunities to eliminate the use of passwords altogether by securely

authenticating users via other methods—a significant motivator on the usability front.

Multi factor Authentication Benefits

The benefits for MFA align very closely to the motivations for having multi factor authentication.

Improve Security the primary benefit of multi factor authentication is that it provides additional security by adding protection in layers. The more layers/factors in place, the more the risk of an intruder gaining access to critical systems and data is reduced.

Achieve Compliance

A second benefit of multi factor authentication is being able to achieve the necessary compliance requirements specific to my organization which in turn mitigate audit findings and avoiding potential fines.

Increase Flexibility and Productivity

And finally, being able to remove the burden of passwords by replacing them with alternatives has the potential to increase productivity and bring a better usability experience due to the increased flexibility of factor types. In the right environment and situation, there could even be an opportunity for a potential reduction in operational costs.

Multi factor Authentication Challenges

While there are well-known benefits for MFA, as with any technology, there will be potential challenges as well. Below we have listed common sticking points for MFA.

Usability

In most MFA implementations, passwords are still present. So, now in addition to having to manage the password, users have to manage an additional layer of security. But perhaps the biggest usability challenge is that your applications and systems often require different types of MFA. You may find yourself asking the question: How is this any better than having a different password for every application?

Cost

This is probably the number one challenge for multi factor authentication, but it is not a unique challenge. Most new technology deployments incur a cost increase, at least initially. MFA brings potential cost increases for things like additional support, training, maintenance, SMS Gateway or services, mobile app development, hardware and software tokens, and stipends for mobile phone expenses.

Technical Gaps

How do you blend MFA for local devices and cloud-based applications? Does your local device have MFA? What about your local email client or local devices?

Complexity

Some physical authenticators require additional drivers. adding another dimension of complexity for deployment, support, and maintenance. This also requires constant compatibility checking as environments change.

Backup Options

Do you have a backup plan in place for your multi factor solution? For example, what if a user loses his or her phone or token? Is there a way for users to gain emergency access?

Lack of Bandwidth

Technology roll-outs are time- and resource-draining. It can be difficult to balance an MFA implementation with existing priorities. MFA takes a significant amount of planning and training because it's critical that you research and understand any related compliance requirements and then figure out which solutions best align not only to those requirements, but also with your industry and user needs.

Varying Risks

Keep in mind, some methods are stronger than others (see AAL1-3) and each method has its own security risks. It is important to understand these risks and which will provide the right level of security for your organization.

Conclusion

The three level security approach applied for a framework makes it exceptionally secure alongside being more easy to understand. This framework will assist obstructing With bearing assault, Tempest assault and savage power assault at the customer side.3-Level Security framework is certainly is a tedious methodology, as the client needs to navigate through the three degrees of security, and should allude to his email-id for the one-time computerized secret word. In this way, this framework can't be a reasonable answer for general security purposes, where time intricacy will be an issue. Be that as it may, will be an aid in territories where high security is the principle issue, and time multifaceted nature is auxiliary, for instance we can take the instance of a firm where this framework will be open just to some higher assignment holding individuals, who need to store and keep up their pivotal and classified information secure. In not so distant future we will include more highlights as well as make our framework adjustable. The world is being automated and all the workplaces and establishments are being modernized. So the utilization and requirement for this product won't decrease. Additionally man consistently prefer to see all works getting increasingly secure and this undertaking does that.

References

[1] https://www.google.com