CS-573-A – Introduction to Cyber Security

Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security

Link to Paper: https://www.ripublication.com/ijaer18/ijaerv13n10_46.pdf

By –
Prashant Pramodkumar Mall
CWID: 10459371

Introduction

Security breaches are always a threat to the confidentiality of personal data. Today, cybercriminals have more than 15 billion stolen credentials to choose from, and this stolen data is readily available to buy or download from the dark web. Passwords are the most common method to authenticate users. However, these passwords can be easily violated and even cracked with today's advanced technology. A long and complicated password may lower these chances, but a single layer of security is still not guaranteed to keep our accounts safe from online threats. The world was introduced with a two-factor authentication method, which involves typing in a second temporary password which can be received on your number or generated by an application. We want to expand this protection by introducing the idea of a three-level security system for users.

Authentication

Let's start with the fundamental reason – why do we even authenticate users? It is a way by which we can be sure the user is the person they are saying they are. There are multiple ways in which ownership can be verified. It can be with something only the user knows – like a unique password combination or something the user has to identify themselves – like a cellphone number or an identification card. We can also use things unique to human beings, like their retinal scan or fingerprint, to authenticate users. Usually, the more protection we implement to authenticate users, the more inconvenient the process becomes.

A New Approach to Authentication

An approach with a three-level protection method has been made to enhance the current two-factor authentication to be more secure but still convenient for the user. This is achieved with text as level one, which is our usual password and then on level two, a temporary generated password received by text or generated by an application and then finally, at level three, a random security question-based authentication which the user would have already set up earlier. This process can even further be optimised and enhanced by using biometrics. Biometrics will breed confidence and also develop dependability among the users. The proposed MFA scheme will take advantage of diversified authentication schemes. In an ideal scenario, the users should have absolute freedom to select the method from biometrics, picture recognition, etc., to complete their three-factor authentication. This is crucial as different people have different preferences and levels of comfort with technology. It should also appeal to users to make it a successful authentication method.

Most users repeat their passwords and have something predictable, nothing very complicated. Users invest heavily in computers, mobiles and other electronics but don't give many thoughts to the security aspect. Online password guesses have been going on forever, and there is little

education to users on how to prevent this. A simple multi-factor authentication has proven to be much more secure than a single layer complex password. Single-layer passwords can also be cracked with brute force attacks, and with the advancement in the processing power of machines, it has become easier than before to do this. A length of eight alphanumeric passwords with capital, small and numbers can be cracked within six minutes.

A combination of strong passwords and more layers of authentication can make the system almost unbreakable. The proposed model can authenticate the user into any target application or website. The first factor is a very familiar usual approach for users to type in their password. The second stage of a graphical or temporary generated password is easy to follow and not much hassle. The final stage is where the user can answer the security question or set up biometric authentication. If the user fails in any authentication steps, we can alert the user over email and block the login attempt. The features proposed are easy to use and follow, improving the security by a significant level. There are some negative points to this, as the entire system increases the time taken for the user to log in and get to the intended application or website. It also requires more memory to store the necessary login information, and of course, the user has to remember a few extra things to pass the validations. The idea is to protect from vulnerabilities today and in the near future. The standard of security will increase and become bothersome for some with time. Three-factor authentication has to be built up as a habit for the user and will take some time to adapt. We have to develop more ways to make this process convenient for users and provoke more vital security.

Recommendations

I am a firm believer in multi-layer factor authentication. I personally use 2MFA and highly recommend everyone to do so. As the paper briefly mentions, it is like a habit which needs to be developed among users. Users should realise how critical passwords are and treat them like it. People don't think about multi-factor authentications and even reuse their passwords. A breach on any one of the websites you have an account on can lead to financial and personal data loss if the password is reused. A simple multi-factor authentication can protect the user in such a case by blocking access to the application even if the password has been breached. I am very keen to look forward for the implementation of three-factor authentication where users can go through three layers of security without adding much hassle or difficulty to the existing system. If society learns to adapt to this method and design, the overall sense of security in the community will increase. There is no perfect solution to this, but generally, this idea brings us closer to safety in the world of cybersecurity. Many websites have started implementing this concept of MFA online and force the users to use some type of dual authentication at the minimum. They also use algorithms to check for suspicious attempts and prompt further verification. More methods are available, like using a password manager to generate strong, complicated passwords for user accounts. These, combined with MFA, reinforce the system even more.