A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

Haruna Adamu
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
harunaadamu1909@gmail.com

Abdulmalik Danlami Mohammed
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
drmalik@futminna.edu.ng

Solomon Adelowo Adepoju
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
solomon.adepoju@futminna.edu.ng

Abisoye Opeyemi Aderiike
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
o.abisoye@futminna.edu.ng

***Abstract*—Text passwords are the most extensively used technique of computer authentication. This approach has been found to have several flaws. Users, for example, typically select passwords that are simple to guess. A difficult-to-guess password, on the other hand, is also difficult-to-remember. Textual passwords are vulnerable to brute-force and keylogger attacks. Graphic passwords have been proposed in the literature as a possible replacement for alphanumerical passwords, based on the assumption that people remember pictures better than text. Existing graphical passwords, on the other hand, are vulnerable to a shoulder surfing assault. To solve these security flaws, this paper proposes an authentication method for online applications that uses a combination of one-time passwords, textual, and graphical passwords. The efficacy of the recommended solution was confirmed by usability testing and security analysis procedures. A total of thirty participants took part in the system evaluation. The security assessment found that the proposed system meets all its primary security requirements. The proposed system was found to be simple to use, friendly, and secure throughout the usability test. When compared to traditional authentication solutions, this study exhibited greater usability and security.**

Keywords—Textual Password, One-Time Password, Graphical Password, Shoulder Surfing, Key-logging

I. INTRODUCTION

User authentication is a method for a device to confirm the identity of a person connecting to network resources. Textual passwords are the most often used form of authentication for all websites and applications. Textual passwords are made up of a string of letters and numbers, with or without special characters or integers. Users can usually log into several accounts with just one username and password [1]. They are not, however, fully safe. As a result, strong passwords with numbers, uppercase, and lowercase letters should be used. These textual passwords are then considered strong enough to survive brute force attacks. On the other side, a strong textual password is difficult to memorize and recall. Password replay and keylogger attacks are also possible with textual passwords [2].

To address the struggle with alphanumeric authentication, a significant variety of graphical password schemes have been devised and tested [3]. The prevalence of graphical passwords can be explained by the fact that pictures, rather than strings of characters, are easier to recall [4]. Graphical passwords are passwords that are made up of pictures or drawings. Because people remember pictures better than text, graphical passwords are easier to remember. They are also more resistant to brute-force attacks because the search space is practically infinite. In conclusion, graphical passwords are a superior option for memorability and usability than text-based passwords [5].

One of the shortcomings of using a graphical password system is the likelihood of shoulder surfing [6]. A graphical passcode could be physically seen, particularly in public places, and if the adversary has a clear visual of the passcode being inserted numerous times, they can easily crack it, which is a severe flaw [7]. Another drawback of using a graphical password is that it is susceptible to guessing. Just like with a textual password, if the user simply registers a brief and predictable password, the chances of it being guessable grow [1]. Some researchers have proposed the use of passwordless use cases like fingerprint verification [8]. However, if one of the fingers is used as a password, for instance, and it is compromised, it cannot be used again since altering a fingerprint is nearly impossible, therefore it is irreversibly compromised. There are several ways to avoid keyloggers, shoulder surfing, and guessing attacks, but none of them are sufficient in and of themselves. A combination of strategies must be employed to effectively eliminate the problem [9]. This study uses a combination of one-time passwords, textual and graphical passwords to combat shoulder-surfing, replay, and key-logging assaults. As a result, the research's main contributions are as follows:

1. Development of a secure one-time password system.
2. Development of a secure textual password authentication system.
3. Development of a secure graphical password authentication system.

978-1-6654-7978-3/22/$31.00 ©2022 IEEE