Chapter 11 Enhancing Textual Password Authentication Using Typing Rhythm

Ferdinand Apietu Katsriku
University of Ghana, Ghana

Samuel Darko Abankwah
University of Ghana, Ghana

Edward Danso Ansong
https://orcid.org/0009-0001-5536-4667
University of Ghana, Ghana

Winfred Yaokumah
https://orcid.org/0000-0001-7756-1832
University of Ghana, Ghana

ABSTRACT

This chapter aims to enhance the security of textual passwords by adding a new layer that involves an individual's typing rhythm without requiring additional devices. It discusses authentication methods and develops a textual password authentication system, which takes advantage of the fact that every user has a distinct way of typing. Twenty participants, including novice and expert users, assessed the proposed system. The measuring metrics used were the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The flight time and typing rhythm were the biometric identification template. The results indicated low false rejection and acceptance rates, with the initial session registering 0.0 FRR and 0.1 FAR. Two weeks later, the second session recorded 0.25 FRR and 0.0 FAR. Using this model, users do not

DOI: 10.4018/979-8-3693-8014-7.ch011

need to select a complex password they might forget. Instead, they can utilize a good rhythm different from their natural typing rhythm, making it challenging to guess.

1. INTRODUCTION

Passwords are the most commonly used authentication method for digital systems, including email, social media networks, banking terminals, web and desktop applications, and network components like routers and switches (Pandey & Taffese, 2021). A password is a secret combination of characters that verifies the identity of a user accessing a system, device, application, or online account. The primary purpose of passwords is to provide security by ensuring that only authorized individuals can access protected resources (Salem et al., 2023). To enhance security, passwords must meet specific criteria, such as a minimum length and a combination of letters, numbers, and special characters, making them harder to guess or crack. Users must choose strong and unique passwords and avoid sharing them with others to protect their accounts from unauthorized access and potential security breaches (Cavus et al., 2023).

However, as internet services continue to expand, the security of passwords is becoming increasingly important. The amount of user identity information online is proliferating, and with it, the vulnerabilities of these systems (Lai & Arko, 2021). Unfortunately, as evidenced by the recent hacking of an online gaming company's servers (DiGiacomo, 2021), even sophisticated networks can still be compromised, putting sensitive information, such as Internet Protocol (IP) addresses, passwords, usernames, and email addresses, at risk. In many instances, individuals' accounts and reports document data have been breached. In the first half of 2022, the number of data breaches in the United States rose to 817, affecting over 53 million people (Verizon Report, 2023). While data breaches, data leakage, and data exposure are distinct events, they all share a commonality: unauthorized threat actors acquiring sensitive data. In 2016, Yahoo suffered the most significant data breach. Yahoo announced that hackers had taken user information linked to at least one billion accounts in 2013. In October 2017, the full scope of the breach was revealed when it was discovered that three billion accounts had been compromised (Haselton, 2017).

It is common for individuals with several passwords to forget them. Research has been conducted on how to manage numerous passwords. According to Verizon's 2017 Data Breach Investigations Report, weak or stolen passwords remain a primary cause of data breaches (Verizon Report, 2023). Hackers often rely on these types of passwords as they offer an easy, swift, and inconspicuous way to gain unauthorized access. Moreover, users can lose their passwords in several ways, including over-the-shoulder attacks, where someone steals a password by looking