A SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION SYSTEM.

AIM & OBJECTIVE

Aim of the project is to develop the application which resist Shoulder Surfing attacks in Graphical Authentication System, with a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images. Objective of the project is to resist Shoulder Surfing attacks in Graphical Authentication System.

ABSTRACT

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users’ credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the

experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

INTRODUCTION

Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.

EXISTING SYSTEM

In the Existing System Users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. Existing System is vulnerable to shoulder surfing attacks.

While logging into these services in public, they may expose their passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window . Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets. Shoulder surfing attacks have gained more and more attention in the past decade.