Abstract

This paper presents a novel method for solving the shoulder surfing problem commonly found in the graphical password authentication system. Authentication of a user is the critical aspect required to gain access to secure and confidential data. Most of the current systems are using alphanumeric password for authentication purpose, however alphanumeric passwords have some disadvantages for example in terms of memorability. So a substitute to alphanumeric passwords, graphical passwords have been recommended. Graphical passwords have been planned to make passwords more unforgettable and effortless for the people to use. During a graphical password authentication, end users click on particular points on images rather than submitting alphanumeric characters. Graphical password schemes can be grouped into two general categories based on the type of cognitive activity required to remember the specific password: recognition and recall. Recognition is the easiest for human memory where on the other hand pure recall is most difficult since the information must be accessed from memory with no triggers. This paper focuses on Cued recall which falls somewhere between these two as it offers a cue which must establish a context and trigger the stored memory. Graphical
passwords generally suffer from shoulder surfing problem. The problem of shoulder surfing is solved using a fake cursor approach. This is a new approach in which two cursors are displayed during the login phase and only the authorized user is aware which is the original cursor and which one is the fake cursor.

References


Computer Networking | ISSN (online): 2321 – 0613.


**Index Terms**

Computer Science

Security

**Keywords**

Fake cursor, Graphical Password, Security, Authentication