NAME: Naveen Kumar
NAME OF SUPERVISOR: Prof. M. N. Doja
DEPARTMENT: Department of Computer Engineering
TITLE OF THE THESIS: Improving the Graphical Password Scheme to Provide Secure Authentication

ABSTRACT

All user authentication schemes are based on three fundamental pieces of information: what you know, what you have, and who you are, which also corresponds to token-based (smart cards, ATM, etc), knowledge-based (alphanumeric) and biometric authentication. Alphanumeric Password is the leading mechanism for verifying the identity of computer users, even though it is well known that people normally choose passwords that are vulnerable to different attacks. The motivation for addressing the security and shortcomings of alphanumeric password authentication is that users tend to choose passwords that are easy to remember. However, secure passwords should be random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text. Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. Moreover, passwords are susceptible to dictionary attack, brute-force attack and are easy to steal though spywares. Further, social engineering practices like Phishing and Snooping are emerging problems for alphanumeric password schemes. One such improvement is graphical passwords, i.e. passwords that are based on pictures or images rather than simple alphanumeric strings. The primary reasoning is that, using images will lead to greater memorability and decrease the tendency to choose insecure passwords, as human being's ability of visual memory is much more powerful than the textual memory.

OBJECTIVES AND SCOPE

This research aims to study the existing graphical password schemes and to design and develop an improved graphical password scheme, to empirically test its security & usability, and to compare it with existing alphanumeric and graphical password schemes. The extent of previously discussed problems and their effect on individuals and organisations give raise to a number of research questions:

- What is the security and usability performance of graphical password schemes in actual use? How can the performance of graphical password schemes be measured?
- Are graphical password schemes as secure as alphanumeric passwords? What are the causes of good or bad performance of alphanumeric and graphical password schemes?
- What are the major design and implementation issues for graphical password schemes? And ultimately,
- What interventions can be made to improve the security and usability performance of graphical password schemes?

This research provides secure, usable and cost effective user authentication mechanisms to help mainly the computer users those are working on untrustworthy computers, Internet, and unsafe networks. However, we have also focused towards the ATM machines, palmtop, and mobile and other handheld device authentication.

COMPARATIVE ANALYSIS

To study different user authentication schemes that are more reliable, affordable, and more secure than traditional password approaches, we have conducted a comparative analysis of the existing graphical password schemes. These schemes are classified into three categories: Cognometric, Locimetric and Drawmetric. We discussed the strengths and limitations of each scheme and pointed out the future research directions in this area.

SURVEY EVALAUTION

A questionaire based evaluation of alphanumeric and graphical password is conducted, to decide and understand the security and usability issues related to these schemes. Both schemes are in the category of knowledge-based passwords, and suffer from the problem of memorability. We have compared the memorability of both the schemes and found that the alphanumeric passwords are more difficult for people to remember and the consequence is that one has to write them down.

SYSTEM DEVLOPEMNT

We have developed two graphical password schemes named *Grid based Locimetric Graphical Password* and *Virtual Password*, and shown that it overcomes most of the limitations of the existing graphical password schemes and offers stronger security and better usability. We conducted detailed system evaluation on *Grid based Locimetric Graphical Password* and provided detailed statistics about the characteristics of user-chosen passwords. *Virtual Password* has an enormous password space as users navigate a non-immersive virtual environment and interact with objects inside the virtual environment for password creation and verification. User password is a combination of user interactions, actions and inputs towards the objects and towards the virtual environment. System repeats the reverse process for verifying the user identity. Implementing the familiar virtual environments, objects and actions for the multiple users is a critical task and is a part of study. Also, there is a need to explore the other attacks on the system like shoulder surfing attack. The virtual password is now in its infancy. A study on a large number of users is required. We have categorised some of the application development areas that require further research and enhancement. Generally, graphical password schemes are prone to shoulder surfing attacks. Hence, the Virtual Password scheme can be improved in terms of users actions and behaviours towards virtual objects so that users can be identified. In addition, if immersive virtual environment based password scheme can be developed, it will be very useful, specifically for visually and physically challenged people.

.