International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-2 Issue-4, March 2013

A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices

Kailas I Patil, Jaiprakash Shimpi

Abstract*— Passwords provide security mechanism for authentication and protection services against unwanted access to resources. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart mobile devices (like smart phones i.e. ipod, iphone, PDAs etc) which are more handy and convenient to use than traditional desktop computer systems.

Index Terms*— Authentication, Graphical Passwords, Network Security.

I. INTRODUCTION

One of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of a use and accessibility. Current secure systems suffer because they mostly ignore the importance of human factors in security . An ideal security system considers security, reliability, usability, and human factors. All current security systems have flaws which make them specific for well trained and skilled users only. A password is a secret that is shared by the verifier and the customer. ”Passwords are simply secrets that are provided by the user upon request by a recipient.” They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists. Passwords are the most common means of authentication because they do not require any special hardware. Typically passwords are strings of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being hard to remember .

Manuscript published on 30 March 2013.
***Correspondence Author(s)**
Prof. Kailas I Patil, Information Technology, NMU/G.H.Raisoni Engg College, Jalgaon, Maharashtra, India.
Prof. Jaiprakash Shimpi, Computer Engineering, NMU/Gulabrao Deokar Engg College, Jalgaon, Maharashtra, India.

II. CLASSIFICATION OF CURRENT AUTHENTICATION METHODS

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication . Currently the authentication methods can be broadly divided into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication , also shown in the Figure 1.

A. Token Based Authentication:

It is based on “Something You Possess”. For example Smart Cards, a driver’s license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site.
Many token based authentication systems also use knowledge based techniques to enhance security.

B. Biometric Based Authentication:

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits . It is based on “Something You Are”. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify.

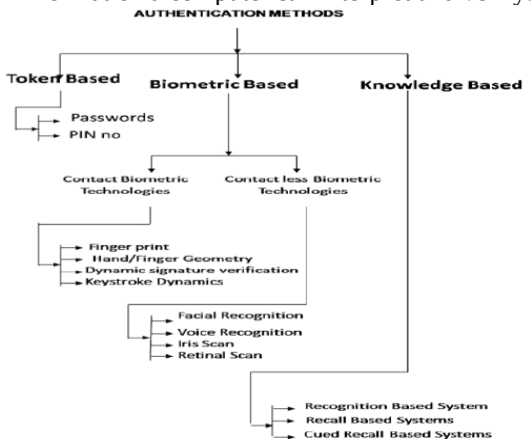

Fig. 1 Classification of Authentication Methods

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics . Biometric identification depends on computer algorithms to make a yes/no decision. It enhances user service by providing quick and easy identification .

C. Knowledge Based Authentication:

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge-based authentication (KBA) is based on "Something You Know" to identify you For Example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question . KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics .

III. CLASSIFICATION OF GRAPHICAL PASSWORD BASED SYSTEMS

Graphical based passwords schemes can be broadly classified into four main categories: First is **Recognition based Systems** which are also known as Cognometric Systems or Searchmetric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is **Pure Recall based systems** which are also known as Drwanmetric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is **Cued Recall based** systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Fourth is **Hybrid systems** which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes. Detailed classification of systems, involved in these four categories is shown in Figure2.

IV. PROPOSED SYSTEM

Taking into account all the problems and limitations of graphical based schemes, we have proposed a hybrid system for authentication. This hybrid system is a mixture of both recognition and recall based schemes.

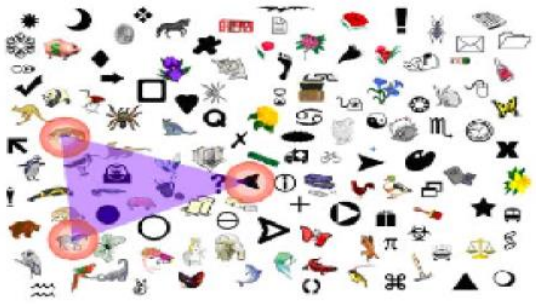

Fig. 2 A shoulder surfing resistant graphical password scheme

Our proposed system is an approach towards more reliable, secure, user-friendly, and robust authentication. We have also reduced the shoulder surfing problem to some extent.

A. Working of Proposed System:

Our proposed system comprises of 9 steps out of which steps 1-3 are registration steps and steps 4-9 are the authentication steps.

Step 1 The first step is to type the user name and a textual password which is stored in the database. During authentication the user has to give that specific user name and textual password in order to log in.

Step 2

In this second step objects are displayed to the user and he/she selects minimum of three objects from the set and there is no limit for maximum number of objects. This is done by using one of the recognition based schemes. The selected objects are then drawn by the user, which are stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Examples are shown in Figure 4.

Step 3

During authentication, the user draws pre-selected objects as his password on a touch sensitive screen (or according to the environment) with a mouse or a stylus. This will be done using the pure recall based methods.

Step 4

In this step, the system performs pre-processing

Step 5

In the fifth step, the system gets the input from the user and merges the strokes in the user drawn sketch.

Step 6

After stroke merging, the system constructs the hierarchy.

Step 7

Seventh step is the sketch simplification.

Step 8

In the eighth step three types of features are extracted from the sketch drawn by the user.

Step 9

The last step is called hierarchical matching.

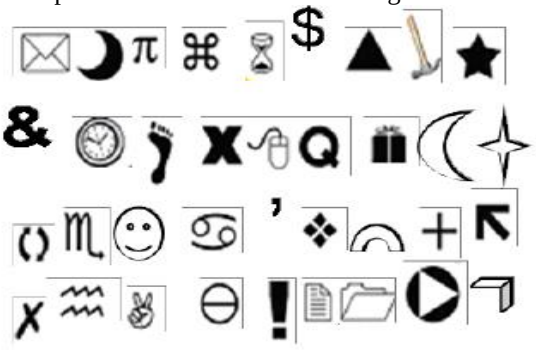

Fig. 3 Some examples of objects shown to the user

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

V. CONCLUSION & FUTURE WORK

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password be more secure, reliable and robust as there is always a place for improvement. Currently we are working on the System Implementation and Evaluation. In future some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.

VI. ACKNOWLEDGMENT

The authors wish to acknowledge the anonymous reviewers for valuable comments.

REFERENCES

1. Roman V. Y., "*User authentication via behavior based passwords*," Systems, Applications and Technology Conference. Farmingdale, NY. 2007.
2. Rachna Dhamija and Adrian Perrig, "*Deja Vu: A User Study. Using Images for Authentication*" In Proceedings of the 9th USENIX Security Symposium, August 2000.

AUTHOR PROFILE

Mr. Kailas I Patil, Teaching Exp.-3Yr Qualifications-BE (IT), ME (CSE pursuing) International Paper-5, National Paper-3

Mr.Jaiprakash Shimpi, Qualifications-BE (Computer), MBA (Marketing), M.TECH (CSE pursuing) Teaching Exp.-5yr

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)