Virtual Interface for Secure Password Creation Scheme

BHAWANA PARIHAR[1], KUBER SING[2], DR. POONAM CHHIMWAL[3]
[1, 2, 3] *Assistant professor BTKIT Drawahat*

Abstract— Password Authentication is the schema of verifying user credentials. There are different ways of authentications are proposed some of them are Textbased Passwords, Graphical passwords, Biometric password etc. But all techniques have certain limitations. Hence we propose a new technique of user Authentication which has capability of removing different type of attack. This new technique is based on real world simulation hence it is called Virtual interface. User is given a choice to interact with virtual interface and select his authentication method i.e textual based , graphical based , Biometrics,, Voice etc. This new scheme provides more options to user along with have higher password space and hence difficult to break and so it is safe from attacks.

Indexed Terms— Authentication, Virtual interface, Multi-password, SHA256

I. INTRODUCTION

Human factors are the often-considered weakest link in a computer security system. If we point out there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems.

In this paper we are protecting our system from different kinds of attacks.

Shoulder Surfing - This attack can be performed either at close range (by directly looking over the victim's shoulder) or from a longer range with, for example a pair of binoculars or similar hardware. Attackers do not need any technical skills in order to perform this method, and keen observation of victims' surroundings and the typing pattern is sufficient. However, the advent of modern-day technologies like hidden cameras and secret microphones makes shoulder surfing easier and gives the attacker more scope to perform long range shoulder surfing. A hidden camera allows the attacker to capture whole login process and other confidential data of the victim, which ultimately could lead to financial loss or identity theft.

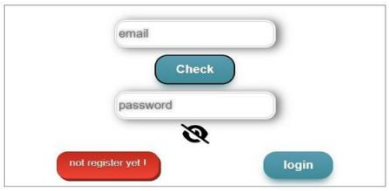
Brute Force - In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.A brute- force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

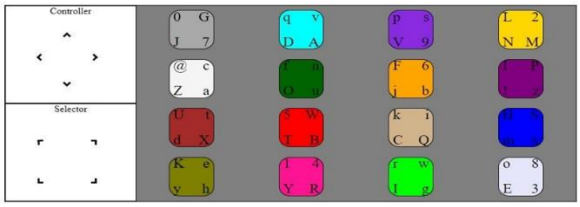
Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication methods, such as biometrics, virtual passwordhave been used. In this project, however, we will focus on another alternative: using color as our another entity, we will build a virtual password protection systems.

Objective of the scheme: We have so many passwords protection schemes, however most of them fell short at one area or other.As we know as our technologies are getting better, our password systems are getting outdated which is creating huge risks for privacy of our peoples and causing us millions of money.

We are trying to make a new improved system which will protect us from many cyber attacks including active and passive ones and we will be able to secure our proper system , which will eventually helps many other interfaces out there.

Design of the system: So our idea here is to implement another layer which is color that will make our system more secure from before and on top of that we are changing how we input our passwords. We basically have our own virtual keyboard there through which we will be entering our password.





with traditional username-password authentication methods, such as biometrics, virtual password have been used. In this project, however, we will focus on another alternative: using color as our another entity, we will build a virtual password protection systems. So in this keyboard as we have two areas for selection and controller by which we will be entering our password.

Firstly we will use controller which will select the color in virtual keyboard and then we will use the selector for selecting characters. As our boxes inside the keyboard changes randomly It will make the system more secure and will be hard to interfere with which will support our point of preventing attacks like active and passive ones

User Registration Phase: The user has to set his textual password K of length L characters, and choose one colour as his pass-colour from some colours assigned by the system. The remaining colours not chosen by the user are his decoy-colours. And, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed in an environment free of cyber attacks. The system stores the user's textual password in the user's entry in the password table, which should be encrypted by the system.

Login Phase: The user requests to login the system, and the system displays a virtual keyboard composed of numerous equally sized sectors. The colours of these sectors are different, and each sector is identified by the colour e.g., the red sector is the sector of red box. Initially, some characters are placed averagely and randomly among these sectors. All thedisplayed characters can be simultaneously rotated into either the adjacent sector by clicking the ‒arrow‖ button once or the adjacent sector by clicking the another ‒arro button once.

Testing: Security Testing is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.

In this paper we prevent our system from Shoulder Suffering, Brute Force and other active attacks.

We use combinations of all uppercase letters, all lowercase letters, digits from (0-9) and two special character for generate a password.

Which means we have total 64! Combinations of password, which it is very difficult to crack inBrute force manner.

We use virtual keyboard and different entity color for generating password which helps us to prevent form Shoulder suffering attack because we enter our password with the help of virtual keyboard.

Our System change the combinations of color and characters in each click in which it is very difficult to find any pattern for crack the password.

CONCLUSION AND FUTURE SCOPE

This paper has provided the interface for much more secured password protection. It provides a more convenient and accurate method for the password

security. In other words, this can provide solution to the many cyber attacks. So our paper basically proved how much we can provide security against these types of attacks and also with some future modifications it can also be applied to the real time heavy systems interface providing the conscious parameters to the system. With our color approach we added extra entity which basically improves the combinations and the virtual keyboard which shuffles the keys to that extent that even advance means will find our interface tough making it more secured.

REFERENCES

[1] Alsulaiman, F.A. and El Saddik, A. "Three- for Secure," IEEE Transactions on Instrumentation and measurement. 57(9) :1929-1938, 2008.

[2] Gadicha, A. B.; Gadicha, V. B.Virtual Realization using 3D Password. International Journal of Electronics and Computer Science Engineering. ISSN 2277-1956. 1(2) : 216-222.

[3] Dhamija, R.; Adrian, P. D. V. 2000. A User Study Using Images for Authentication. In Proceedings of USENIX Security Symposium, Denver, Colorado : 45-58.

[4] Alsulaiman, F. A. and A. El Saddik. “A novel 3D graphical password schema,” in Proc. IEEE Int. Conf. Virtual Environ., Human-Comput. Interfaces, Meas. Syst.: 125–128, 2006.

[5] Suo, X.; Zhu, Y. and Owen, G. S. “Graphical passwords: A survey”.Computer Security Appl. Conf.: 463–472, 2005.

[6] Weinshall, D. and Kirkpatrick, S. "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI).

[7] Alsulaiman, F. A. and El Saddik, A. A Novel 3D Graphical Password Schema, IEEE. International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, 2006.

[8] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, ―3D password, International Journal of Computer Applications (IJCA), pp. 6-10 2012.