International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 4 ǁ 2022 ǁ PP. 33-36

Color Matrix based Virtual Password System: A Review

Adwait Padhye[1], Anik Mukherjee[1], Himanshi Darvekar[1], Akash Zalke[1]
[1]Student, Department of Computer Engineering, Government college of Engineering Nagpur, India.

Abstract: *- Shoulder surfing attacks have proven to be a great bane for information and technology systems since their very inception. While great strides have been taken to improve the security of systems internally against hacks and viruses, the same progress has not been made to circumvent the very basic intrusion made by human eyes. While there are no reliable statistics on the prevalence of shoulder surfing attacks, a 2016 study conducted by Memon and Nguyen found that 73 percent of mobile device users surveyed reported that they had observed someone else's PIN (although not necessarily with malicious intent), and a 2017 study of shoulder surfing awareness presented at the ACM Conference on Human Factors in Computing Systems reported that 97 percent of those surveyed claimed awareness of a shoulder surfing incident in everyday life, and that in the majority of cases, victims were unaware that they were being observed. Password authentication systems form the basis of most of the contemporary businesses, medical, financial, entertainment, and technological industries. A simple glance from an onlooker can give away the login details of an individual or an organization. Incidents such as this can prove extremely costly, but at the same time, are extremely difficult to avoid. As a result, having such an underwhelming solution to an extremely serious security risk is far from ideal.*

Key Words— Password, Shoulder Surfing, Random matrix, Authentication.

Date of Submission: 13-04-2022 Date of acceptance: 29-04-2022

I. INTRODUCTION

In today's highly technological environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing.

Today's information system the security is largely supported by password for authentication process. The most of password contains alphanumeric and special characters it is highly vulnerable. To overcome the drawbacks of traditional method we propose new authentication method to abolish well known Security threats like brute force and shoulder surfing attacks.

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder. Unauthorized users watch the keystrokes inputted on a device 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. 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.

Irrespective of how cautious a person is when entering their password, or how quickly they try to do it, it is almost impossible to avoid being shoulder surfed if the intruder so desires.

In an attempt to overcome this issue, and reduce the paranoia around entering passwords in public, the Color Matrix based Virtual Password System finds a novel way around this problem by completely eliminating the risk of giving away your password to an unwanted observer. Color Matrix Based Virtual Password System uses a color matrix which is randomly generated on each login attempt. This color matrix maps a single color to multiple characters which are supported in a password. This basic functionality of this app allows an added layer of protection by introducing an additional layer of abstraction between the user and the onlooker.

II. DRAWBACKS WITH EXISTING SYSTEMS

A. Pattern based unlocking system:

- While patterns are quite a lot more difficult to shoulder surf than traditional passwords by eye, they can still be easily copied with the use of a camera.
- It can often be quite difficult for individuals to remember complex patterns.
- Older people or those with special needs often find it difficult to draw intricate patterns.

B. One-Time Password Protection:

- This is not really a replacement for traditional password systems, but a supplement to it. This system can also be used in conjunction with our Matrix based system for greater security.
- It causes difficulties in logging in if a user does not have his mobile phone on hand.

C. Face Detection:

- Not very secure, as a person may have his face scanned by another individual without being aware of it.
- Not very reliable as sometimes it may unlock devices or applications unintentionally.
- Only work if a device has a camera.

D. Fingerprint locks:

- Only work if a device has a fingerprint sensor.
- Not very secure, as a person may have his finger scanned by another individual without being aware of it.
- Fingerprints of an individual can change overtime, and may also get damaged in an accident.

III. Methodology

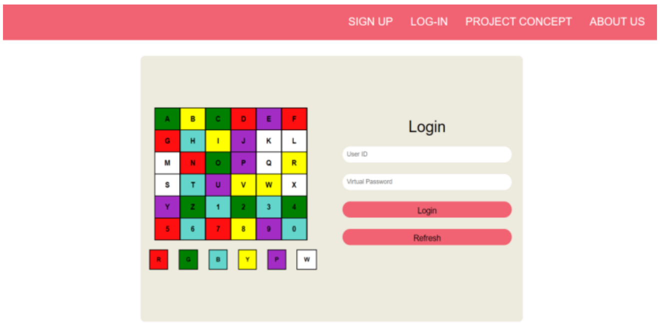
Color Matrix Based Virtual Password System uses a color matrix which is randomly generated on each login attempt. This color matrix maps a single color to multiple characters which are supported in a password. The matrix that is generated with each iteration is displayed on the screen at each refresh.

When an individual is trying to enter their password using this virtual password system, instead of entering their actual password, they would enter the color associated with the corresponding characters by the color matrix. As the user only inputs the color associated with a character, and not the character itself, the actual password would not be exposed to any observers as each color has multiple characters associated with it. As each color is mapped to multiple characters, and multiple such colors are entered during password verification, the probability of an onlooker finding out the correct password becomes very low, and the password would be protected.

As the color matrix is randomized at each login attempt, even after multiple attempts of password theft, any malicious individuals would be unable to correctly identify the password as the mapping of colors to characters in the back-end changes with each attempt. So, the characters mapped to a color are always different. This basic functionality of this app allows an added layer of protection by introducing an additional layer of abstraction between the user and the onlooker.

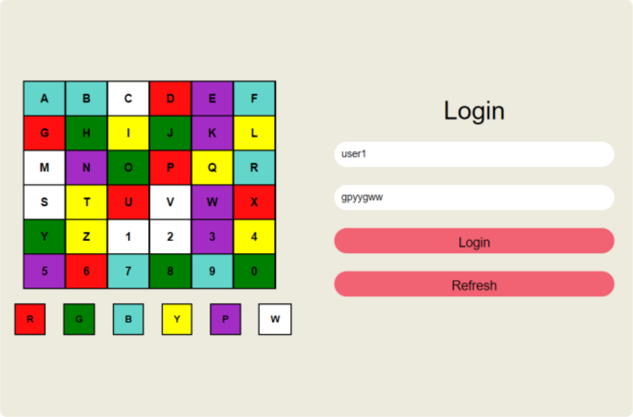
The development of the user interface of this project for the web application was undertaken using Flask framework developed using HTML, CSS and Jinja2 templating programming language. The coding for the application was done on Microsoft Visual Studio Code also called VSCode, configured with python plugin. Additionally, a Local Host server was put up to test the application without running it on an actual Internet which worked as a testing environment. The development of the user interface of the website was undertaken using flask framework and JavaScript programming language. Visual elements of the website were developed using Hypertext Markup Language (HTML), Cascading Style Sheets (CSS) and Bootstrap framework Microsoft Visual Studio Code also called VSCode was used for the writing and editing the code for the website. Mozilla Firefox was the web browser of choice for testing the website.

The SDLC model that the team selected is the Waterfall SDLC model.



A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

Fig.1. UI corresponding to the color matrix page



🟦 A	🟦 B	⬜ C	🟥 D	🟪 E	🟦 F
🟥 G	🟩 H	🟨 I	🟩 J	🟪 K	🟨 L
⬜ M	🟪 N	🟩 O	🟥 P	🟨 Q	🟦 R
⬜ S	🟨 T	🟥 U	⬜ V	🟪 W	🟥 X
🟩 Y	🟨 Z	⬜ 1	⬜ 2	🟪 3	🟨 4
🟪 5	🟥 6	🟦 7	🟩 8	🟦 9	🟩 0

🟥 R 🟩 G 🟦 B 🟨 Y 🟪 P ⬜ W

Login

user1

gpyygww

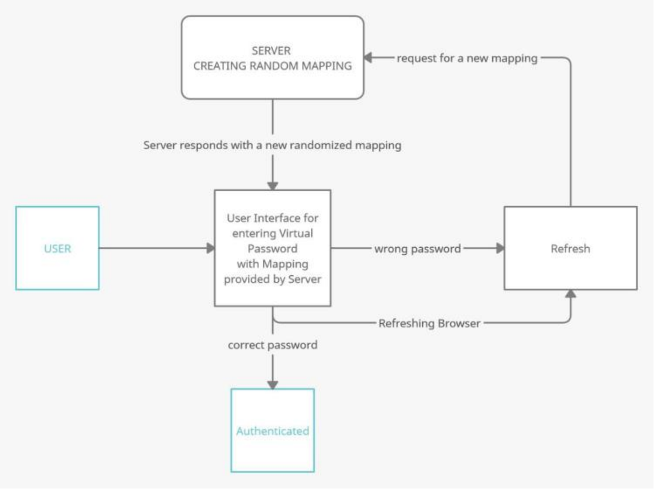
Fig.1. Inputting color codes for the password "hello12"

IV. RESULTS AND DISCUSSION

The introduction of unique passwords in order to protect our data was a revolution in the computer security field. However since then every step taken in order to enhance security only proved to be an iterative improvement over the system already in place. This has left a gaping hole in many security systems as most systems still use some version of the age old password protection system that has proven to be less than secure at stopping shoulder-surfing attacks and key stroke capturing attacks.

Although the Color Matrix based Virtual Password system is not a revolution in Computer system security, it builds on the presently used password security mechanism and adds an additional layer of security or abstraction on top of it by using the randomized color matrix. The number of colors chosen in this example is 6, but that can be varied according to the application deployers convenience. In this example, i.e., with 6 colors each color is assigned 6 characters or numbers. So, even if a would be code breaker gets a glimpse of the users' inputted password, there would be 6 characters corresponding to each of the 'n' colors inputted in the password field. So, for the code breaker to input the correct password, the task would be mathematically overwhelming as when he tries to brute force the password in the next refresh, the mapping of the colors would be completely different, and possibly 6 completely different characters would be assigned to a single color as compared to the previous attempt.

The data flow diagram of this application in order to make it function properly is as follows:


SERVER
CREATING RANDOM MAPPING
request for a new mapping
Server responds with a new randomized mapping
USER
User Interface for entering Virtual Password with Mapping provided by Server
wrong password
Refresh
Refreshing Browser
correct password
Authenticated

The user interacts with the User Interface module to enter Virtual Password based on the mapping provided by the server for this refresh. If the wrong password is entered or if the user refreshes the browser manually, a new mapping is requested to the server, which runs the algorithm in the back-end to generate a new mapping for the color matrix. This is then displayed on the User Interface. When the correct password is entered, the password is authenticated and the user is redirected to the appropriate page.

Although not foolproof, this application provides much more security against shoulder surfing attacks as compared to regular password authentication systems.

V. CONCLUSION

In the proposed system, we have implemented a password authentication system which makes use of a randomized color matrix in order to prevent the danger of shoulder surfing attacks by ensuring that the potential victims never have to actually enter the password, and that the password to color mapping changes for each refresh.

REFERENCES

[1]. H. Gao, X. Guo, X. Chen, L. Wang and X. Liu, "YAGP: Yet Another Graphical Password Strategy," 2008 Annual Computer Security Applications Conference (ACSAC), 2008, pp. 121-129, doi: 10.1109/ACSAC.2008.19.

[2]. H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing," 2010 International Conference on Cyberworlds, 2010, pp. 194-199, doi: 10.1109/CW.2010.34.

[3]. https://www.researchgate.net/publication/224229789_A_graphical_password authentication system

[4]. AVI '06: Proceedings of the working conference on Advanced visual interfaces May 2006 Pages 177–184 https://doi.org/10.1145/1133265.1133303