ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

QR Code Resistant Key Logging Based Visual Cryptography

K.Udhayasurya [1], P. Kaliyamoorthy [2], T. Sivabalan[3]
M.E Student[1], Assistant professor & HOD [2], Assistant professor [3]
Department of Computer Science and Engineering
Cauvery College of Engineering and Technology, Trichy, India

Abstract:
The main aim here is to develop a combination of text and color QR Code based authentication mechanism passwords for session authentication instead of traditional textual passwords. Most existing methods have been subjected to lots of attacks. Even two factor authentication schemes have been proposed. The security of such systems is not always reliable. Key loggers are more troublesome for the users since a key logger records all the users' activity and when connected to the internet this data is sent to a remote hacker who then enters the client's application and thus breaches the security system. To mitigate the key logger attack, virtual or onscreen keyboards with random keyboard arrangements are widely used in practice. To overcome this problem a two factor visual authentication mechanism is proposed. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code.

Keywords: QR Code, Key Logger, Visual Cryptography.

I. INTRODUCTION

Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It has uses in the study of human– computer interaction. There are numerous key logging methods, ranging from hardware and software-based approaches to acoustic analysis. These are computer programs designed to work on the target computer's software. Key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Key loggers can also be used by a family (or business) to monitor the network usage of people without their direct knowledge. Finally, malicious individuals may use key loggers on public computers to steal passwords or credit card information. The key logger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example. A program on the machine 'gets root' and hides itself in the OS, and starts intercepting keystrokes (because they always go through the kernel). This method is difficult both to write and to combat. Such key loggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications who don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A key logger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system. The API based key loggers hook keyboard APIs inside a running application. The key logger registers for keystroke events, as if it was a normal piece of the application instead of malware. The key logger receives an event each time the user presses or releases a key. The key logger simply records it. The grabbing-based key loggers log web form submissions by recording the web browsing on submit events. These happen when the user finishes filling in the form and clicks on the "OK" or "Submit" or "Go" or anything that indicates that you're finished. This records form data before it is passed over the Internet. In the current scenario, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input. Systems are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these applications. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for all.The passwords are easily hack able. They are subject to attacks like shoulder surfing Keys are recorded and sent to the other users and hence not safe. In case of biometrics the users have to use sophisticated machines which are not user friendly.

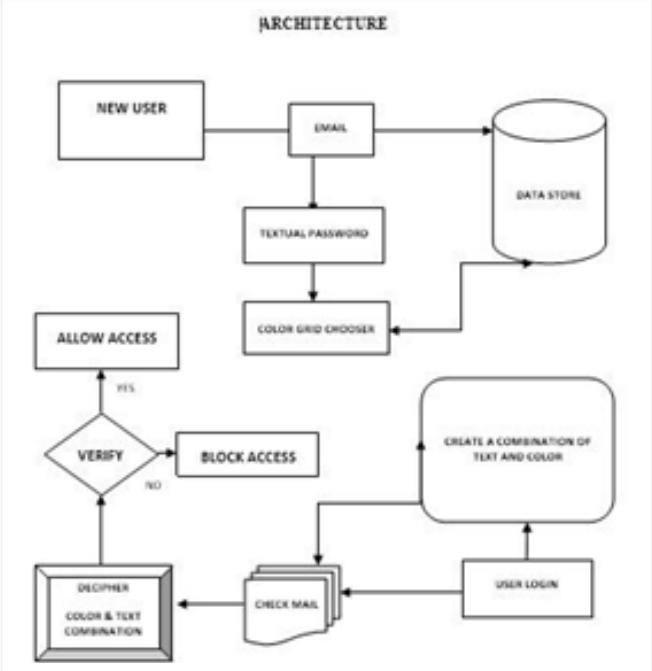
II. PROPOSED QR CODE MODEL

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites. The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that

users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels.

The following are advantages Resistant

to key logging attacks Is session Based and hence a new PIN for each and every login cannot be seen visually as it is visually encrypted. Is not hack able and will be foolproof.



III. USER REGISTRATION MODULE

Here the user registers his details. The user name should be unique. It is stored by an id in the database. Next a valid email id is procured. The user is redirected to the next screen. The generated unique identity is shown to the user for his login purposes. Then he is redirected to the next screen, where the user is shown the alphanumeric textual password.

TEXT GRID DEPLOYMENT

Here the user submits a textual password which should be having a minimum length of the 8 characters. This can be called as secret pass. The secret pass should contain even number of characters. This is validated and then stored in the user database. Next the users id redirected to the next screen, where the user is shown the color screen.

COLOR GRID DEPLOYMENT AND RATING

Grids of 8 colors are displayed to the user. The colors selected by the user. User should rate colors from 1 to 8 in any order. During registration, user should rate colors as shown in figure 9. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid. The login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, then get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider ratings and login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element.

QR CODE

The QR (Quick Response) code is generated based on the PIN generated and sent to the user. This causes the PIN to be successfully hidden by inside the QR code. The QR code is generated and sent to the user who has tried to login via email. A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image. The QR code system was invented in 1994 by Denso Wave. Its purpose was to track vehicles during manufacturing; it was designed to allow high-speed component scanning. QR codes are now used in a much broader context, including both commercial tracking applications and convenience-oriented applications aimed at mobile-phone users (termed mobile tagging). QR codes may be used to display text to the user, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), or to compose an email or text message. Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free QR code generating sites or apps. The technology has since become one of the most used types of two-dimensional barcode

EMAIL MODULE

The generated combination is sent to the users email id. The users then have to go to the corresponding mail id and find out the combination for the text and the appropriate color and enter it into the users login.

VERIFICATION MODULE

During this phase the system verifies if the combination is right for the text and color supplied for this session. If the password is accurate then the user is allowed entry into the system otherwise the login fails. As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. The QR Code is uploaded, matched and verified by the system. If the QR code is not matched then the user is sent an alert. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight

reading. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text. Normally, there is an expansion of space requirement in visual cryptography. The image has been split into two component images. Each component image has a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one, and the other. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match both. When these matching pairs are overlapped, they will appear light gray. So, when the two component images are superimposed, the original image appears. However, considered by itself, a component image reveals no information about the original image; it is indistinguishable from a random pattern of pairs. Moreover, if you have one component image, you can use the shading rules above to produce a counterfeit component image that combines with it to produce any image at all.

IV. RESULTS AND DISCUSSION

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data; extensions may also be used. The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing. Thus the generated QR code module consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns present in both horizontal and vertical components of the image, which is safe and secure for data transmission as in this case.

V. CONCLUSION

Two new authentication techniques based on text and colors are proposed for all existing text password based applications. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration, during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes even if new to the users they are very effective and the proposed authentication techniques are accurate.

VI. FUTURE ENHANCEMENTS

The project can be extended to be implemented as web services in the future. Such an innovation would make the services available as an alternative method to all the users of existing schemes in the future. The model can be used for mobile authentication as well. So if the QR Code module is used then the users of mobile applications like banking will be safe when using Visual Cryptography.

VII. REFERENCES

[1]. R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[2]. Real User Corporation: Passfaces. www.passfaces.com

[3]. Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[5]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[6]. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[7]. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127