International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

A Shoulder Surfing Resistant Graphical Authentication System

D. Ravi, I. S. Narmadha, L. Nivetha, R. Vijayalakshmi

Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

People enjoy the convenience of on-line services, but online environments may bring many risks. We propose a virtual password and QR code concept involving a small amount of human computing to secure users' passwords in on-line environments. We adopted user-determined randomized linear generation functions to secure users' passwords based on the fact that a server has more information than any adversary does. We propose differentiated QR code mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users' passwords. A functionis used to implement the virtual password concept with security for complexity requiring a small amount of human computing. For user-specified functions, we adopt secretlittle functions in which security is enhanced by to generate QR CODE.

Keywords : Graphical Passwords, Authentication, Shoulder Surfing Attack.

I. INTRODUCTION

Today, the Internet has entered into our daily lives as more and more services have been moved online. Besides reading the news, searching for information, and other risk-free activities online, we have also become accustomed to other risk-related work, such as paying using credit cards, checking / composing emails, online banking and soon. While we enjoy its convenience, we are putting ourselves at risk. Most current commercial websites will ask their users to input their user identifications (IDs) and corresponding passwords for authentication. Once a user's ID and the corresponding password are stolen by an adversary, the adversary can do anything with the victim's account, which can lead to a disaster for the victim. As a consequence of increasing concerns over such risks, protecting users' passwords on the web has become increasingly critical. In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet-based environment or an ATM machine, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. We propose a virtual password concept involving small amount of human computing to secure users 'passwords in online environments. The trade-off is that stronger schemes are more complex. Among the schemes, we have a default method (i.e., traditional password scheme), a system recommended function, a user-specified function, a user-specified program and so on. A function/program is used to implement the virtual password concept by trading security for complexity by requiring small amount of human computing. We analyse how the proposed schemes defend against phishing, key logger, shoulder surfing and multiple attacks. In user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions/algorithms.

II. METHODS AND MATERIAL

1. Existence Approaches

In the Existing system, the access code will be sent to the mobile using that user login to the website. Access code security is not there. We present a password protection scheme that involves a small amount of human computing in an Internet-based environment or an ATM machine, which will be resistant to phishing frauds, Trojan horses, and shoulder surfing attacks.

Disadvantages

- Attackers easily access our password
- In login time access code sent to user mobile and then user, login their account. Sometimes hacker can hack the database, see the access code, and then use our account.
- Website designed by a simple format.
- Not using special software using in virtual password creation and QR code.

2. Proposed System

In the proposed system, a QR code concept involving a small amount of human computing to secure users' Passwords in online environments is implemented. AQR code scheme ranges from weak security to strong security. The function/program is used to implement the QR code concept with a trade-off between security and complexity and requires small amount of human computing, hiding secret functions/algorithms.

Advantages

- It provides high security
- Hacker maybe knowing our password but he cannot access our account because he cannot create QR code
- Special jar was designed to create a virtual password.
- Any types of hacking method cannot implement our account.

3. Module

- Registration Module
- Login Module
- Secret Little Function Module
- Virtual Password Module
- Transaction Module

Registration Module

In the Registration Module, the users have to make registration here. As per the registration a jar will be downloaded as per the random value. User has to install the jar in the java supporting mobile. Using the jar only we will do the login form. In the jar there will be expression calculation. Expression varies for each jar. Expression will be stored in the database.

Login Module

In the login form the user will give the user name and password first. If the username and password is same means a random key will be sent to the access page. User has to install the jar and enter the random key contain in access page. As per the user expression calculation will be done and viewed in the access code text field. Please enter the value in the website if the value is correct means enter to the user's page.

Secret Little Function Modules:

There will be 11 jars the secret value and secret Function will vary for each jar. Calculation Part in the Secret Little Function module is as Follows: The access code values will be split into 3 parts. We split the value in 3 parts and assign to the 3 variables say a, b, c. Then a will be added with X variable b will be subtracted with x variable and c will be multiplied with x. Here x value will vary for each jar. Assign the value as a1, b1, c1. Secret Function will vary for each user. The expression calculation will be in a1 b1 c1 format only. The values will be passed to the expression and generated code will be generated.

Virtual Password Module:

In the Virtual Password module the Secret Function calculation will vary for different jar. The use gets the random value and generated value in dynamic format. Virtual means dynamic. Random numbers keep on changing so that Generated code will also keep on changing dynamically.

Transaction Module

The bankers have to rights for creating new bank accounts for user who wants to keep money on bank. Each user has provides user id and password by bank administrators for doing online transactions. In this module, Account holders are able to do online account transactions like Fund Transfer, With Draw and Deposits. Account holders have to register their personal information and send report their account transaction to Financial Intelligence. In addition, they

can view the summary of Transaction details and view balance of his account.

III. RESULTS AND DISCUSSION

1. Feasibility Study

Since the process of developing a system can be costly, the system investigation stage requires a preliminary study called a "Feasibility study". A "feasibility study" is a preliminary study, which investigates the information, needs of prospective users and determines the resource requirements, costs, benefits and feasibility of a proposed project. The goal of feasibility studies is to evaluate alternative systems and to propose the most feasible and desirable system for development. The feasibility of a proposed system can be evaluated in terms of the following major categories.

Types of Feasibility Study

Technical Feasibility

This method is used to evaluate the technical aspects of the proposed system. This can be demonstrated if reliable hardware and software capable of meeting the needs of proposed system. It can be acquired or developed in the required time. This project is technically feasible that satisfies the needs in the required time using the reliable hardware and software.

Behavioural Feasibility

This is the willingness and ability of the management, employees, end-user to operate and support for proposed system. This method is used for finding how much effort goes for education and training the staff for the system, which is to be developed. This project is operationally feasible because this is easy to operate and only need little knowledge.

Economic Feasibility

This is the method frequently used for evaluating the economic effectiveness of the system. The method is evaluated for benefits and costs that are accepted from the system are considered and reviewed. Further justification and alternation in the proposed system are incorporated .This project is economically feasible. The package being developed is definitely feasible from economic point of view because of software, Hardwar requirements and the number of operating personal required for operation of this project is Minimum.

Operational Feasibility

This is the willingness and ability of the management, employees, end-user to operate and support for a proposed system. This method is used for finding how much effort goes for education and training the staff for the system, which is to be developed. This project is operationally feasible because this is easy to operate and only need little knowledge.

2. Architecture Diagram

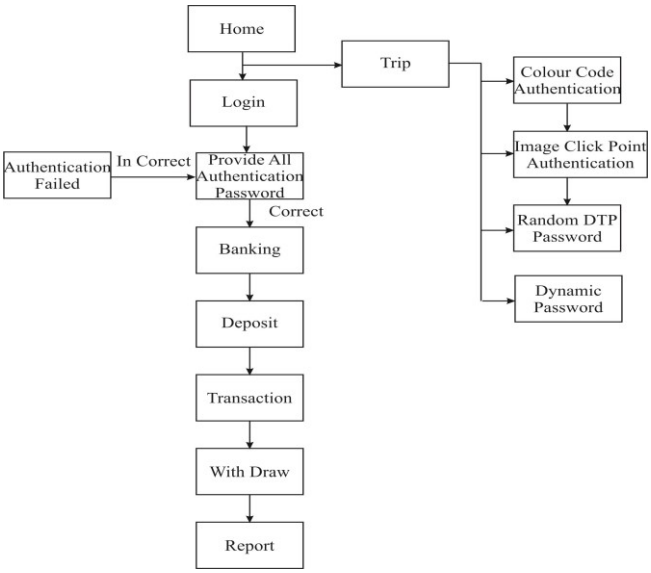

Figure 1. System Architecture

IV. CONCLUSION

To overcome the problem of shoulder surfing, we proposed a shoulder-surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. The design of all bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Based on the experimental results and survey data, PassMatrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks and the survey data in the user study also showed that PassMatrix is practical in the real world.

V. REFERENCES

[1]. A.Paivio, T.Rogers, and P.Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[2]. D.Nelson, U.Reed, and J.Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[3]. I.Jermyn, A.Mayer, F.Monrose, M. Reiter, and A.Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[4]. R.Dhamija and A.Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX SecuritySymposium-Volume9. USENIX Association,2000,pp. 4–4.

[5]. S.Brostoff and M. Sasse, "Are passfaces more usable than pass- words? a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.

[6]. K. Gilhooly, "Biometrics: Getting back to business," Computer- world, May, vol. 9, 2005.

[7]. S.Wiedenbeck, J.Waters, J.Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphicalpasswordsystem,"InternationalJournalof Human-ComputerStudies, vol. 63, no. 1-2, pp. 102–127, 2005.

[8]. S.Gurav, L.Gawade, P.Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[9]. "Realuser," http://www.realuser.com/.