ISSN 2348 – 9928
IJAICT Volume 7, Issue 1, January 2020 Doi:10.46532/ijaict-2020001 Published on 05 (01) 2020

THE SURFING ATTACKS SECURED PASSWORD AUTHENTICATION SYSTEM

P. Arulprakash Assistant Professor
K. Vidhya UG Scholar
E. Menaga priya UG Scholar
R. Abinisha UG Scholar
E. Manoj UG Scholar

**Department of Computer Science and Engineering,
RVS College of Engineering and Technology,
Coimbatore, Tamilnadu, India**

Abstract*— People enjoy the convenience of on-line services, but online environments may bring many risks. We propose a virtual password concept involving a small amount of human computing to secure users' passwords in on-line environments. We adopt 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 analyze how the proposed scheme defends against phishing, key logger, and shoulder-surfing attacks. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks together. In this work, we discussed how to prevent users' passwords from being stolen by adversaries. We proposed a virtual password concept involving a small amount of human computing to secure users' passwords in on-line environments.. We also implemented the system to do some tests and survey feedback indicates the feasibility of such a system. In this paper, we discuss how to prevent users' passwords from being stolen by adversaries in online environments and automated teller machines. We propose differentiated virtual password 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. Among the schemes, we have a default method (i.e., traditional password scheme), system recommended functions, user-specified functions, user-specified programs, and so on. A function/program is used to implement the virtual password concept with a tradeoff of security for complexity requiring a small amount of human computing

Keywords*—Authentication, Access Code, Surfing Attacks, Smudge Attacks.

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 so on. 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 [1].

The secure protocol SSL/TLS for transmitting private data over the web is well-known in academic research, but most current commercial websites still rely on the relatively weak protection mechanism of user authentications via a plaintext password and user ID. Meanwhile, even though a password can be transferred via a secure channel, this authentication approach is still vulnerable to the following attacks: 1) in phishing attacks, phishes attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication; 2) Password Stealing Trojan programs contain or install malicious codes. Examples include: a) key loggers capturing keystrokes in the machine; and b) Trojan Redirectors redirecting end-users network traffic to a desired location; and 3) Shoulder Surfing steals others' sensitive personal information by looking over victims' shoulders or capturing users' inputs and screens by taking pictures and videos using cameras and video recorders, respectively. Many schemes, protocols, and software have been designed to prevent users from some specified attacks [2].

However, to the best of our knowledge, there is not a scheme which can defend against all the attacks listed above at the same time. In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet-based environment or a ATM machine, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. We propose a virtual password concept involving a small amount of human computing to secure users'

passwords in online environments. We propose differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The tradeoff 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 a small amount of human computing [3].

We further propose several functions to serve as system recommended functions and provide a security analysis. We analyze 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. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks.

We believe that, for some sensitive accounts such as online bank accounts and online credit card accounts, users are likely to choose additional complexity which requires some degree of human computing in order to make the account more secure. 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 so on [4].

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 [5].

The secure protocol SSL/TLS for transmitting private data over the web is well-known in academic research, but most current commercial websites still rely on the relatively weak protection mechanism of user authentications via a plaintext password and user ID. Meanwhile, even though a password can be transferred via a secure channel, this authentication approach is still vulnerable to the following attacks: 1) in phishing attacks, phishes attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication; 2) Password Stealing Trojan programs contain or install malicious codes. Examples include: a) key loggers capturing keystrokes in the machine; and b) Trojan Redirectors redirecting end-users network traffic to a desired location; and 3) Shoulder Surfing steals others' sensitive personal information by looking over victims' shoulders or capturing users' inputs and screens by taking pictures and videos using cameras and video recorders, respectively [6].

Many schemes, protocols, and software have been designed to prevent users from some specified attacks. However, to the best of our knowledge, there is not a scheme which can defend against all the attacks listed above at the same time. In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet-based environment or a ATM machine, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. We propose a virtual password concept involving a small amount of human computing to secure users' passwords in online environments [7].

We propose differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The tradeoff 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 a small amount of human computing [8][9].

We further propose several functions to serve as system recommended functions and provide a security analysis. We analyze how the proposed schemes defend against phishing, key logger, [10] shoulder-surfing, and multiple attacks. In user specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions/algorithms. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks. We believe that, for some sensitive accounts such as online bank accounts and online credit card accounts, users are likely to choose additional complexity which requires some degree of human computing in order to make the account more secure.

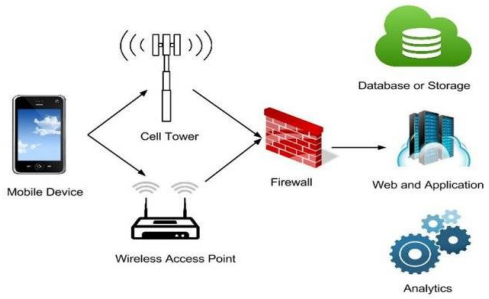

Fig 1: Authentication overview

II. PROBLEM FORMULATION

The proposed a virtual password concept involving a small amount of human computing to secure users' Passwords in online environments. We proposed differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The function/program is used to implement the virtual password concept with a tradeoff between security and complexity and requires small amount of human computing. However, since simplicity and security conflict with each other, it is difficult to achieve both.

We further proposed several functions serving as system recommended functions and provided a security analysis. We analyzed how the proposed schemes defend against phishing, key-logger, shoulder-surfing attacks, and multiple attacks. In user-specified functions, we adopted secret little functions in which security is enhanced by hiding secret functions/algorithms. In conclusion, user- defined functions (secret little functions) are better.

III. SYSTEM DESIGN

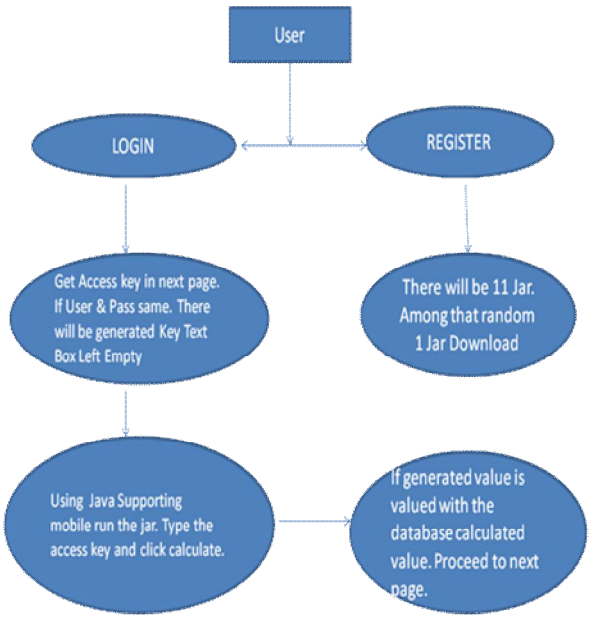

Fig 2 : Overall System Design

System analysis is a process of gathering the facts concerning the system breaking them into elements and relationship between elements. It provides a framework for visualizing the organizational and environmental factors that operate on a system. The quality of work performed by a machine is usually uniform, neat and more reliable when compared to doing the same operations manually.

IV. MAKING THE REGISTRATION

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.

V. SECRET LITTLE FUNCTION

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 eg a, b, c. Then a will be added with X variable b will be subtract 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.

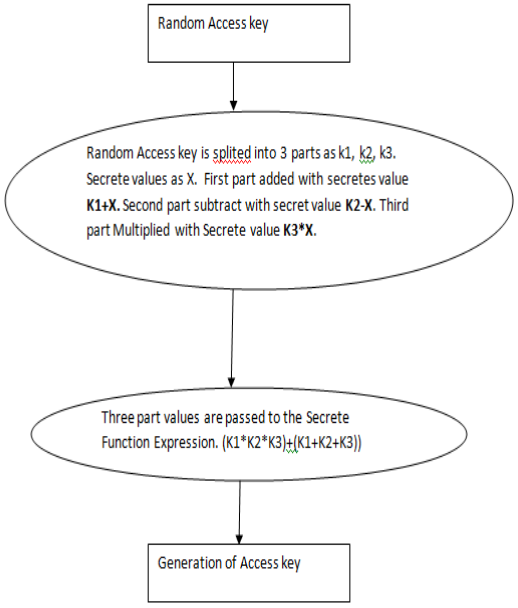

Fig 3 : Secret Little Function

VI. VIRTUAL PASSWORD

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

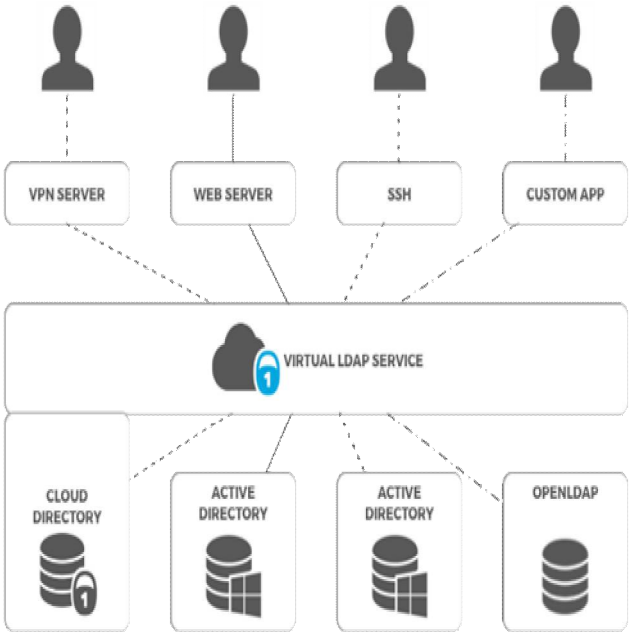

Fig 4 : Virtual Password

VII. RESULT ANALYSIS

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to

Authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones. To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. 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. Because of the design of the horizontal and vertical 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. Furthermore, we implemented a Pass Matrix prototype on Android and carried out user experiments to evaluate the memo ability and usability. The experimental result showed that users can log into the system with an average of 1:64 tries (Median=1), and the Total Accuracy of all login trials is 93:33% even two weeks after registration. The total time consumed to log into Pass Matrix with an average of 3:2 pass-images is between 31:31 and 37:11 seconds and is considered acceptable by 83:33% of participants in our user study. Based on the experimental results and survey data, Pass Matrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, Pass Matrix can be applied to any authentication scenario and device with simple input and output capabilities. The survey data in the user study also showed that Pass Matrix is practical in the real world.

VIII. CONCLUSION

Now days, the web services trending got increases day by day. so, authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones. In such case, we are providing efficient authentication mechanisms as access code .

References

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] 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.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

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

[5] 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.

[6] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

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

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

[9] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.

[10] B. Ives, K. Walsh, and H. Schneider, "The domino effect of password reuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78, 2004.