ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (142-147), Month: April - June 2016, Available at: www.researchpublish.com

Color Combo: An Authentication Method against Shoulder Surfing Attack

[1]GOPIKA ANIL, [2]CHIPPY MARY JOHN, [3]PRADEEP P MATHEW

[1,2] Student, [3]Assistant Professor, Dept. of Cse, Mbccet, Peermade Idukki

***Abstract*: For authentication users mainly use PIN entry mechanism. Due to its usability and security aspects this scheme is popular. But one of the drawback of this scheme is that it suffers from shoulder surfing attack. An unauthorized user can fully or partially observe the login session in this attack. To get the actual PIN the attacker can record the activities of the login session and can use it later. In this paper,we propose an authentication method, known as Color Combo to resist the shoulder surfing attack so that user don't have to disclose the actual pin all he/she has to enter is the session pin. This scheme is based on a partially observable model. This scheme is user friendly and takes only less time to complete.**

General Terms: Authentication, shoulder surfing attacks, session pin.

***Keywords:* Feature table, color pins, partially observer model, one time paradigm.**

1. INTRODUCTION

We know that everyone in the world now uses internet and it includes both genuine and malicious users. Though there are many ways to find out malicious users, all these fail at some moment. To identify genuine users we use authentication technique. password based authentication scheme is the widely used authentication method as it is easy to use and have low cost. One of the disadvantages of this scheme is that it is prone to shoulder surfing attack.

The attacker can view the login session partially or fully . Hence it is classified into two categories fully observable and partially observable. If the attacker can view the login session fully then it is fully observable model and if the attacker can view the login session partially then it is partially observable model. This color pass scheme[1] is based on partially observable model. Here instead of using four digit as pin four colors are used.

This method uses one time pass paradigm. Four challenges questions are generated and user enters four responses with respect to each challenge. It has equal password strength as compared to normal pin entry mechanism and it is easy to use and doesn't require any pre requisite knowledge.

2. LITERATURE REVIEW

Personal Identification Numbers (PINs) are widely used to authenticate users. Unfortunately, classical PIN-entry methods are all vulnerable to observation attacks and it usually suffers from shoulder sufing attack. Some of the techniques against this are discussed below.

2. 1 PASSWORDS: IF WE ARE SO SMART, WHY ARE WE STILL USING THEM?

Passwords are used as a main weapon for authentication. User selects alphabetic,numeric and alphanumeric passwords yet it suffer from many problems like weak passwords,password guessing and brute-force dictionary[2]. Users also can have their passwords stolen through phishing, social engineering, man-in-the-middle, and keylogging attacks. Because of these cognitive challenges, users frequently store copies of their passwords and use the same password for multiple systems

As economic gain has emerged as a primary motivation for computer security exploits, there should be increased motivation to move beyond simple passwords. On the other hand, despite these signs of real need and a desire for change, adoption of authentication alternatives has been very slow. As the user types in a password, the obscured field responds to each character with an asterisk; this prevents another person from seeing the password over her shoulder. Password authentication is familiar to nearly all computer users; once you've learned how to log in to one system, you can apply the same method to others. The benefits of familiarity extend to administrators responsible for setting up and maintaining user security; the same general practices apply to all systems using password authentication.

ADAVANTAGES:

Password authentication is easy to implement To create them, a programmer creates an input form consisting of two text fields, one standard that accepts username and one obscured that accepts password. The cost is low Because software handles password authentication, the only cost comes from the minor effort required for programming. It easy to change a password, we can change it anywhere at any time.

DISADVANTAGES:

Computer programs, however, can launch brute force attacks on password systems. This means that a program literally reads through a provided dictionary of terms, trying each word until the correct combination of characters breaks the password. When you use password authentication, you must store passwords and usernames in a database to authenticate users. If you don't have strong server security, someone can break into the database and read the passwords. multiple security issues inherent to password authentication

2. 2 PASSPOINTS:

Sometimes it is difficult for users to remember all the passwords as a solution to this graphical passwords are introduced where user has to click on images rather than typing alphanumeric strings. It is important to not that graphical password users created stronger passwords with fewer difficulties than alphanumeric password users. Using images as password will lead to greater memorability and decrease the tendency to choose insecure passwords, which will in turn increase overall password security.

In a graphical password system[3], a user choosing click locations in an image needs to choose memorable locations. There are two issues in memorability: the nature of the image itself and the sequence of click locations. A user's password consists of any arbitrarily chosen sequence of points in the image. Since an intricate image easily has hundreds of memorable points, not many click points are needed to make a password hard to guess. At first, it seems that our graphical passwords cannot be hashed; indeed, when users log in they click close to their chosen click points, but not exactly on the chosen points. So, at the pixel level, the password that is entered changes all the time. Hashing does not allow approximation: two passwords that are almost identical will be hashed very differently.

ADVANTAGES:

The graphical password are easy to create. Graphical password are clear and simple for users. It is easy to obtain large passwords spaces, and allows safe storage and protection during file back-up. Most users can quickly learn to input graphical passwords without error, and even those who do make repeated errors can input them successfully given enough practice. Users remember graphical passwords as well as alphanumeric passwords over weeks without use.

DISADVANTAGES:

This scheme suffers from shoulder surfing attack and uses large password space on small images. Users have to enter graphical passwords to log in to various systems or to unlock a screen saver.

2. 3 PASS-GO:

Pass-Go,is also a graphical password scheme in which a user selects intersections on a grid as a way to in-put a password. This[4]scheme can be used inmost application environments and input devices, rather than being limited to small mobile devices (PDAs), and can be used to derive cryptographic keys Graphical passwords, which require a user to remember and repeat visual information, have been proposed to offer better resistance to dictionary attack.

Using a grid as background has several advantages: first, it eliminates the need to store a graphical database on the server side and removes the overhead to transfer images through network. Second, as a grid is a simple object, such schemes minimize the quality requirement for displays, which is an essential factor in image-based schemes. grid-based schemes do not impose a limit on the length of a password; a user can draw a password as long as desired.

ADVANTAGES:

Grid based passwords provide stronger security and better usability. It is n efficient and human readable encoding scheme. Dynamic password checking method identification of the need and a solution for keyboard input support.

DISADVANTAGES:

Users have to draw their input sufficiently away from the grid lines and intersections in order to enter the password correctly. Reduces the memorable password space

2. 4 MOD 10METHOD:

Here we describe a method and apparatus for secure entry and authentication of a multi digit personal identification number[5]. An authenticator generates a random number, and provides that number, or a function to a user. The user is exected to encode each digit of the PIN number, one digit at a time and this is done by performing a mathematical operation. The encoded PIN digit is provided to the authenticator which reverses the steps performed by the user to regenerate and verify the user's PIN. The user is prompted to encode subsequent digits of the PIN only after(1) a previous digit is encoded,(2) the encoded digit is provided to an input device for the authenticator, and(3)a new random number is generated and that random number, or a function there of, is provided to the user for encoding a subsequent PIN digit

User remembers a four digit PIN number from the set {0,1,. . . , 9}. User receives a challenge from the set {0, 1,. . . , 9} through a protected media. User will add the challenge digit with the corresponding PIN digit and will perform a modulo 10 operation. Finally he will enter back the obtained digit using a public keyboard. Suppose the first digit of the user chosen PINis 5. User now securely receives a challenge 7 from the system. So the valid response by user will be (5+7) modulo 10 (which is equal to 2). This invention relates to a method and apparatus for secure entry of a PIN in an environment in which the user may be subject to observation by adverse bystanders intending to obtain the number for fraudulent use.

ADAVANTAGES:

This method is easy to execute for math oriented people and gives good security againt guessing the password . This method reveals no information to the user as well as to the caller if telephones are used as the physical media for the transfer of generated numbers or function requires less login time and it is very user friendly.

DISADVANTAGES:

This method would posses so much difficulty to adopt for the non math oriented people. Problems arise when sum of the digits and the challenge exceeds 10.

2. 5 SHOULDER SURFING SAFE LOG-IN PARTIALLY OBSERVABLE MODEL:

Here we design a simple Table Lookup (STL) login method aimed at improving the Mod10 method. A simple table lookup has to be performed rathe[6]r. Our usability study shows that both Mod10 and STL login methods are user-friendly and have reasonably low login times. The results show that Mod10 has slightly lower login time at the cost of a higher error rate compared to the STL. Interestingly, the major source of errors with the Mod10 method are cases in which the sum of a challenge and the PIN digit exceeds 10,which indicates that non-math oriented people might need additional assistance when using the Mod10 method. Indeed, by extending this method with a simple lookup table ,the usability study reveals that older people prefer to use the Mod10-table method rather than Mod10. All the methods analyzed essentially implements one-time paradigm.

ADVANTAGES:

Needs to perform only a simple table look up**.** No need of higher mathematical assistance**.** Threats of side channel attacks were also considered.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (142-147), Month: April - June 2016, Available at: www.researchpublish.com

DISADVANTAGES:

Log in time goes high with the modulo 10 method. Error rate does not improve much wth the number of attempts.

2. 6 SHOULDER SURFING SAFE LOGIN:

This method Shoulder Surfing Safe Login (SSSL) [7]involves a protected channel through which a user receives challenges and the users are not required to perform any complicated mathematical or mentally demanding operation.

The SSSL scheme falls in the second class of PIN-entry methods, i. e. , it is designed to work in the partially observable model . Here the adversary can only partially observe the PIN-entry procedure. SSSL implements the challenge-response paradigm and comprises three major components: (i) a protected channel ensuring secrecy and integrity of challenge values, (ii) an SSSL table - a table of digits from 1 to 9 organized in such a way that each digit i is an immediate neighbor to the other 8 digits from the set{1. . 9}.

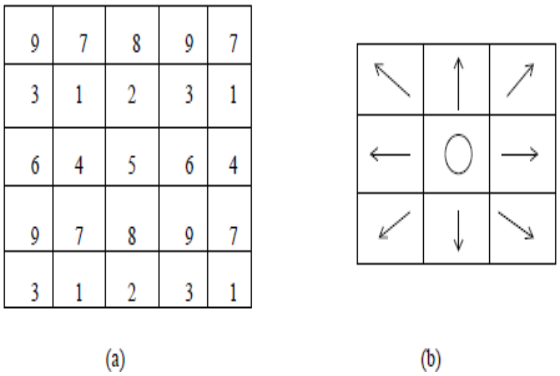

FIG (a)orientation of digits (b)keypad structure

ADVANTAGES:

The system is very user friendly with very low login rates and faster authentication schemes. It incurs very less cost. It is possible to integrate this system with the eisting login systems and it also provides a robust solution for shoulder surfing attacks. It is easy for non math oriented users and cheap to implement.

DISADVANTAGES:

Chances for brute force attack is very high in this system. Existence of correlation beween the digits can be easily tracked by a clever attacker and can be used for guessing the pins.

3. SYSTEM ANALYSIS

3. 1 EXISTING SYSTEM:

The traditional PIN entry mechanism is widely used for authentication. It is mainly used for authenticating user . It is widely used because of its usability and security. Even though it is considered as a secure method, it often leads to shoulder surfing attack. Here the unauthorized person may be fully or partially observe login session. This login session can be recorded and misused in future.

DISADVANTAGES OF EXISTING SYSTEM:

1. Shoulder surfing attacks: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder to get information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.

2. Brute-force attacks: A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (142-147), Month: April - June 2016, Available at: www.researchpublish.com

3. Side-channel attacks: A side-channel attack is a form of reverse engineering. Electronic circuits are inherently leaky – they produce emissions as byproducts that make it possible for an attacker without access to the circuitry itself to deduce how the circuit works and what data it is processing.

3. 2PROPOSED SYSTEM:

The proposed Color Pass interface is based on partially observable attacker model in which an attacker cannot see the challenge values generated by the system but can only see the response given by the user. Thus it is assumed that the media through which user gets the challenge should ensure security against man-in-middle attack.

3. 2. 1 PIN ENTRY MECHANISM:

Here, the user chosen PIN is four colors[1]. During the login procedure, when the Feature Tables appear in the screen then the system throws some challenge values to the user. Challenge values range from 1 to 10. Based on the challenge value the user has to select the corresponding Feature Table. For example, challenge value 4 indicates that the user has to look in the Fourth Feature Table. After listening to each challenge value, user selects a Feature Table. Then corresponding to the chosen color PIN, locates the color cell in that table. The user then finds the digit in that color cell and enters that digit as response to the challenge. Similarly user will respond to the other three challenge values and will complete the login process. Valid response to the challenge values will authenticate the user.

3. 2. 2 CHARACTERISTIC OF USER CHOSEN PIN:

In the conventional schemes it is required to remember either few digits or few characters as user PIN. But in our scheme the color is used to form a PIN. User can choose four colors from a set of ten different colors represented as {C0,C2,. . , C9}. User has the flexibility to choose one color more than once. So one possible instance of user chosen PIN might be C1C2C1C4. Each Ci denotes a specific color (say yellow or brown). As user chosen PIN is comprised of four colors so probability of guessing the PIN will be $1/10^4$.

3. 2. 3 STEPS OF LOGIN PROCEDURE:

• User enters his login id.

• Once system checks that the login id exists then it will generate Feature Tables.

• System then generates four random challenge values ranges from 1. . 10.

• Next user will have to give response to those challenge values.

• User response will be evaluated by system.

• Finally system will decide whether the user is legitimate or not

3. 2. 4 CHARACTERISTIC OF FEATURE TABLES:

Color Pass interface consists of 10 different Feature Tables which are numbered from 1 to 10. Each cell of a table is represented by a pair < Ci, Vi >. Here Ci denotes the color of the cell i and Vi indicates the digit corresponding to cell i.

	$C_0(0)$	
$C_1(1)$	$C_2(2)$	$C_3(3)$
$C_4(4)$	$C_5(5)$	$C_6(6)$
$C_7(7)$	$C_8(8)$	$C_9(9)$
	1	

Fig: Feature Table

ADVANTAGES:

The proposed system can prevent attacks such as shoulder surfing, guessing password, side channel attack, etc. This scheme is user friendly and takes very less time for login. The proposed methodology shows significant low error rate during login procedure

4. CONCLUSION

Here, we have proposed a novel scheme to authenticate a user using color PINS. The scheme is known as Color Pass scheme which provides an intelligent interface for users to login into system in a public domain. In this scheme, the user remembers four colors as his PIN. The scheme works on the framework of partially observable attacker model. From security point of view the scheme is quite robust against some possible attacks such as shoulder surfing, guessing password, side channel attack, etc. And from usability point of view the scheme is user friendly and takes very less time for login. Also the scheme can be used by both math and non-math oriented people. The proposed methodology shows significant low error rate during login procedure. In future we will explore how to extend this scheme for fully observable attacker model

REFERENCES

[1] Nilesh Chakraborthy and Samrat Mondal , Color pass:an intelligent user interface to resist Shoulder surfing attack.

[2] C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If were so smart, why are we still using them?," in Financial Cryptography, pg. 230–237,2009Nil

[3] Paivio, "Mind and its evaluation: A dual coding theoretical approach,",2006.

[4] G. E. Blonder, "Graphical passwords. in lucent technologies, inc. , murray hill, nj, u. s. patent, ed. united states," June 1996. [9]

[5] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," International Journal of Network Security, vol. 7,no. 2, pp. 273–292, 2008.

[6] G. Wilfong, "Method and appartus for secure pin entry. " US Patent No. 5,940,511, In Lucent Technologies, Inc. , Murray Hill, NJ, U. S. Patent, Ed. United States, 1997.

[7] Shoulder surfing safe-in login in a partially observer attacker model, Toni Perkovic´, Mario C˘ agalj and Nitesh Saxena, FESB, University of Split Polytechnic Institute of New York University

[8] Shoulder surfing safe login(SSL),Tony perkovic and Mrio Cagalj, research gate conference paper, October 2009.