J. Appl. Environ. Biol. Sci., 4(9S)298-302, 2014

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Efficient Position Based Operation Code Authentication

Hashim Ali, Sheheryar Khan and Shazia Tabassum

Department of Computer Science Abdul Wali Khan University Mardan, KPK, Pakistan

Received: September 12, 2014
Accepted: November 23, 2014

ABSTRACT

Security for application/s is always been a keen issue of concern. In general, safety is to allow access of grant to authorized user or to deny non-authorized access to the system. Shoulder surfing is an observation technique to hack an account or to enter into a system. When a malicious observer is capturing or recording the fingers of a user while he is entering sensitive inputs (PIN, Passwords etc.) and might be able to observe user's password credential. It is very rigorousfor a novice user to prevent himself from shoulder surfing or unaided observer in a public place while accessing his account. In order to secure the user account, there are five factors of authentication; they are: i. "Rather You have, ii. Rather you are, iii. Rather you know, iv. Somebody you know and v. Rather you Process". A technique has been developed of fifth factor authentication "Rather you process" to provide novel approach to the user. In this paper, we have applied position based operational code authentication in such a way to more easy and user friendly to the user.

KEYWORDS—shoulder surfing; malicious observer; sensitive inputs; authentication.

1 INTRODUCTION

In recent days, world IT provides a lot of services to secure application especially for those we need a conventional and easy technique. Traditionally a password is an appropriate and easy mechanism in computer's security system. Unfortunately, this method is vulnerable to spyware and key-loggers [1]. Password Authenticated Key agreement method is an interactive method to establish cryptographic keys based on the knowledge of, one or more parties, about password [2].The system only needs the user to present something he knows as evidence. That's he is actually who he claim to be. Password is easily executed but at the same time the password methodology is subject to a number of security threats. Shoulder attack and brute force attack are public security hazard where a genuine user can lose his sensitive information (PIN, password etc.). Users tend to choose simple and easy to remember passwords as opposed to strong alphanumeric passwords which weakens their account security [3]. For example the first letters of the words of a sentence or phrase or proverb, e.g. my name is Sheheryar Khan, so the password will be *mnisk*. In some cases passwords use are only numeric e.g PIN (personal identification number), briefcase numbers. Sometimes people use short and easy passwords, so that they can remember and type easily. Password rests the most common feature of computer safety, to know that how much the password is strong; it should be analyzed that how much it can resist against the different attacking techniques, applied by hackers like guessing attacks, shoulder attacks, brute force attacks. Password strength depends upon three main factors, i.e. complexity, randomness and length. As the online services are increasing to avail the service the user must need a secure way. Identification of a legitimate user is the demand of computing society. Well, the term "security" has lots of meanings. There are certain places where security needs to be addressed according to the demand of organization.
Some of them are listed below:

A. Workplace Security

Nowadays, almost every individual works under rather hazardous for health conditions. Computers that influence eyesight, poor light, etc. All this may be discussed in workplace security research papers.

B. Business Security

What laws protect businessmen? What documents should be signed to start your own business? What requirements should be met?

*** Corresponding Author:** Hashim Ali, Department of Computer Science Abdul Wali Khan University Mardan, KPK, Pakistan. hashimali@awkum.edu.pk

C. Computer Security

Computers play a really important role in the life of every person. People work and communicate via computers, store important documents and private letters, and so on. This is why the matter of computer security is rather urgent. Computer security plays an important role in the security of an industry which is dependent on computer. Term computer safety is also used as computer security. Computer security is always in the headlines of an organization which operates through computers.

Shoulder surfing is an observation technique to hack an account or to enter into a system. When a malicious observer is capturing or recording the fingers of a user while he is entering sensitive inputs (PIN, Passwords etc.) and might be able to observe user's password credential. It is very hard for a novice user to prevent himself from shoulder surfing or unaided observer in a public place while accessing his account. These attacks can be very dangerous for companies and organization and has been creating a lot of problems. Recent authentication techniques have been moving forward to prevent hackers and shoulder attackers from hacking. Authentication, is the process of validating who you are to whom you claimed to be [4]. Many researchers have provided the techniques against shoulder attacks using graphics and formula based authentication. While alphanumeric passwords systems are vulnerable to shoulder-surfing if the attacker can see the keyboard, graphical password systems may be more vulnerable in certain settings. This makes it necessary that such techniques should be developed by which these attacks can be prevented, provided with the easy to use.

In crowded effective areas, shoulder surfing becomes easy and effective, because it is easy to observe when:

a) User is filling a form.
b) User uses a POSS terminal or automated teller machine and enter the PIN codes.
c) User use the calling card at a public pay phone.
d) User enters passwords at a cybercafé, public and university libraries, or airport.
e) User enters a code for a rented locker in a public place such as a swimming pool or airport.

Most of the people think that the process of shoulder surfing is a straight forward process, by simply peering over someone's shoulder and getting the require result.

It is important to note that the process of shoulder surfing is not as straight forward as it may sound. It really isn't simply a case of peering over someone's shoulder and then writing down the information, there is a lot more to it.

Binoculars or other vision-enhancing devices are also used for shoulder surfing attacks. Low-cost, tiny closed circuitry television cameras may be cloaked in ceilings, side walls or equipment to witness password or any data entry. It is directed to protect paper work or the key pad, from sight, by means of cupping one's finger or one's physique to thwart shoulder attack.

Shoulder attackers can be prevented by using sophisticated display, i.e. it discourages the shoulder suffers from viewing the screen; recent automated teller machines have used this technique. This gives a darker view of the screen at a particular viewing angle, thus the screen gives the good look, when the user is standing in opposite of it. Though this stops a viewer finding nearly some statistics, e.g. account and its balance, but it does not shield the PIN, as the PIN is normally not exposed for the duration of entry. Unsure models of credit-card bibliophiles have the key pad dipped, and employ an elastic protection that environs a substantial part of the initial towards the key pad. This marks shoulder-surfing meaningfully stiffer, as sighted the key pad is restricted to a plentiful added shortest angle than older models.

The security system must be intended in such a method that it provides shield against all the attacks i.e. prevention from malicious data , man in the middle attacks, shoulder attacks, guessing attacks, brute force attacks and like that. Passwords should be selected so that they are tough for an attacker to predict and tough for an attacker to discover using any (and all) of the available automatic attack schemes. The security of a password-protected system depends on several factors.

Section II gives detailed study related to the work presented. Problem definition is given in Section III. Proposed solution is applied in Section IV and lastly conclusion is given in Section V.

2. RELATED WORK

Susan wieden beck and jim [6] water propose convex hull scheme. They used graphical element in their authentication system. Many windows presented by the system in a specific order, contain different icons. The user has to select the correct icon password for authentication. The user must locate three or more of his password icon visually. The technique is easy to remember because of its graphical elements. The icons randomly changing its positions in a specific time. The users have to click on the right icon every time.

For multi-server environment using java based smart based on two factor authentication concepts have been explained by Mr. Misbah ud Din, et'al [3]. They propose image based login authentication. During signup the user have to give a username and upload an image or the user can select the default image provided by the server for setting the password. If the user selects the default image then he has to select an image from the given set. Each picture have a password on its back which is then written on his java based smart card. During login time the user has to insert the smart card and type hi ID. The ID will be checked on smart card initially then at the server. If the ID is genuine then the server provide images where the user has to enter the matching password to avoid shoulder attack the image randomly presented in 3x3 grid.

"Pass shape – stroke based shape passwords" by Alexander Deluca, et'al [7]. In the paper they evaluate different PIN entry for ATM's. They noticed that many user remember their PIN as a shape on the number pad not as a combination of number. They present an idea to use shape as a password. The shape consist of different numbers but it should not be connected to each other which allow unlimited possible.

In the research paper, "secure graphical code word system for high traffic public area" by Bogdan Hoanca [8]. They suggest a camera built eye tracing system that functions as a watched built mouse. The user solely guises at an item on the screen and choice via obsession or by unrelenting a button. To lessen shoulder surfing no "ON screen feed-back" is on condition that as to which image/location was to be selected. Their experiment indicate reasonable cell size 10x10 pixels. The direction of extent of password space of a picture cell is at most stronger than 8 character/s text based password. They likewise extant a scheme that reason for systematics error/s. This kind of error/s is once projected observation position and actual observation position differs by a continual translation vector.

In the paper "fourth factor authentication" by john Brained [9] explored fourth category of authentication "somebody you know" they vouching system for hardware token and describe a prototype implantation for secure ID token.

Mr Shakir Ullah, et'al [10] in "New factor/s authentication some-thing you may process" proposed a formula based authentication system. During registration each manipulator will partake a different formula assigned by the system and each manipulator will partake dissimilar value/s of the variables from A-Z. At login time the user will process the formula and calculate the accurate result to authenticate.

The fifth factor authentication explored by Syed shabih ul islam, et'al [7] in "operation code authentication". They explored the fifth factor in such a way to prevent shoulder surfing. By the period of sign up the manipulator will be enquired to give in to two things i. PASSCODE it isa 3 to 6 digit number and ii. FOUR LETTER WORD like iron, lion etc. this four letter word represent four basic airthematic operator in BADMOS sequence and OPS DIGIT . The user will also upload two picture of his own choice. At login time the system will give a formula to the user randomly every time. If the user calculates the formula accurately he will be authenticated to the next step which is crises pictures. If the user feels he is in danger or at gun point he should select his own uploaded picture if he is safe then he can select the any pictures among the others.

3. PROBLEM DEFINITION

From the very beginning computer passwords are the mostly used methods by users to prevent their data and other sensitive information from unauthorized users. Passwords are considered as a double edge sword to repudiate the unauthorized person/s to access the data. They are also one of the most sought after pieces of information by malicious crackers and other nefarious individuals Passwords should be set in such a way, that the information should be secure from invalid and unauthorized access, but comfortably accessible for authorized and legitimate users.

There have been known five factors for authentication. The fifth factor of authentication "something you process" explored by Syed Shabih ul Islam, et'al [5]. In their technique the user will enter two things during registration apart from username. Pass Code (3 to 6 digit number) and Four Letter Word (like, lion, Iran etc.) which represent four basic operator (/,*, +,-) in BODMOS sequence. At login time the system gives formula (op code) if user calculates accurately he will be authenticated to the next Step Graphical

Security Box. For example a user 321 as a Pass Code and lion as Four Letter word and the Op code (formula) is N4 at login time. In this case N stand for – (subtraction)

L i o n
/ * + -

The user has to calculate 321-4 the password will be 317. If the user enters NINE as Four letter word then the scenario will be totally confusing. For example the OP Code is N4. In this case N stand for both Division and Addition.

N I N E
/ * + -

So the user has no idea from which position the N is picked up by the system. To solve this issue in this paper we propose Efficient Position Based Operation Code Authentication.

5. **PROPOSED SOLUTION**

In this paper we explored "operation code authentication"[7]. We proposed position based technique in such way which would be more efficient and user friendly. In this technique, besides, the username, user will submit two things firstly, pass code (3 to 6 digit number) and secondly, any kind of four letters word (lion, nine, aaaa, aabb) during registration like previous technique. Four letter word represent four basic arithmetic (/, *, +, -) in bodmas sequence.

During Login after the username the user will select a Position for operator from his Four Letter Word. For example the Pass Code is 123 and Four Letter Word is NINE.

At login user will asked to select a position (0 to 3) to select his corresponding operator from his Four Letter Word. If the user select 2 as position so in this case

N I N E
/ * + -

N corresponding to + (addition) is picked up for OP Code (formula) with a random number from 1 to 9. Let's suppose the system gives the OP Code N8. So this mean the user has to add 8 with 123 i.e. 123+8 so the password for the next step is 131.It is showed that in fig.1,The system checks the username if it is false it will go to the failed option if it is true then the user need to enter a position number for his operator and a random number is generated by the system itself. Then the system shows the Op code after it the user need to enter Live pass. System will check the Live pass if it is false the user will repeat the process if true the user will get authentication. Based on Fig1, the algorithm of the system is as followed:

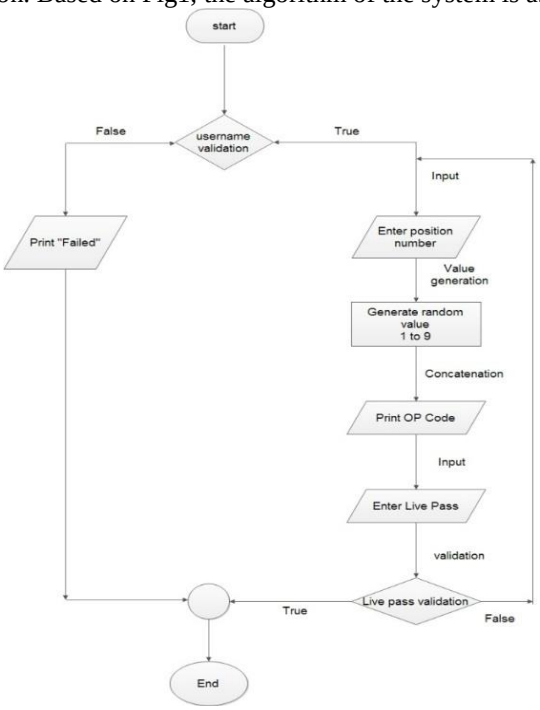

Fig 1 Flow Chart.

Algorithm Authentication (username)

1. q-result ⟵ "username from the data base"
2. If !q-result then
3. print wrong username
4. exit
5. else
6. passcode ⟵ q-result [passcode]
7. letter word ⟵ q-result [letter word]
8. pos ⟵ "get position from user"
9. process ⟵ process(pos, passcode, letter word)
10. If process then
11. "Authenticate"
12. else
13. "go to step no 8 "

5. CONCLUSION

This paper introduces the concept of position based operation code authentication to overcome shoulder surfing or to prevent users from malicious observer. This research work focus on efficiency from the user perspective which is easier for a novice user to use the authentication system. In the previous technique ambiguities were present in Opcode calculation. That resulted very complex issue for a user to solve the Opcode when a user have repetition of word in Four Letter Word. The same vary remains focus of our paper and later it is easily solved it through position based operation code authentication. In this methodology the user needs to enter a username, Pass code, and a four letter word. After entering username the user enter a position number for operator from his four lettered word. The system will generate an OP code formula which is the combination of given position number and a random value from 1 to 9. So the user has to solve the Op code to get authentication.

Future Work: In the future we can provide more flexible way for the calculation of the OP Code from the user perspective. Randomization of the four lettered word can be more efficient in some other ways. Modification in the technique can be a future research paper.

REFERENCES

1. Madoka Hasegawa, et al, 2009 "A Study on an Image Synthesis Method for Graphical Passwords".
2. Federal Financial Institutions Examination Council, 2007 "Authentication in an Internet Banking Environment",.
3. Mohammed Misbahuddin, et al, 2009. " A User Friendly Password Authenticated Key Agreement for Multi Server Environment" ICAC3'09
4. Fawaz A. Alsulaiman and Abdulmotaleb El Saddik " Three-Dimensional Password for More Secure Authentication".
5. Syed Shabih ul Hasan Naqvi and Samiullah Afzal "operation code authentication".
6. Susan Wiedenbeck, et al, 2006. "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme" AVI'06
7. Alexander De Luca, Roman Weiss, Heinrich Hussmann, 2007. "Pass Shape - Stroke based Shape Passwords" OZCHI '07
8. Bogdan Hoanca, Kenrick Mock, "Secure graphical password system for high traffic public areas"
9. John Brainard, Ar. Juels, Ronal L. Rivest, Michael Szydlo and Moti Yung, 2006. "Fourth Factor Authentication: Somebody You Know", CCS '06
10. Shakir Ullah Shah, Fazal-e-Hadi, Abid Ali Minhas, 2009. "New Factor of Authentication: Something You Process" ICFCC '09.