ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Implementing Black hole Password Entry Technique For Mitigating Shoulder-surfing Threat

Yogesh Babu.B[1], Visvanathan.G[2]

M.E Computer science and Engg, IFET College of Engineering, Tamilnadu, India[1, 2]

ABSTRACT: Shoulder-surfing using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials.

I present Blackhole, a system that mitigates the issues of shoulder surfing via a novel approach to user input. With user enters sensitive input (password, PIN, etc.) by filling up four boxes from the randomly selected six password blocks with the missing letters that fills the original password. In this technique, the user has to enter different letter combinations from his original password each time he/she logs in, making eavesdropping by a malicious observer largely impractical, developing more sophisticated methods to enhance our project in all possible ways.

Categories and Subject Descriptors
[Security and Protection]: Authentication.
[User Interfaces]: Input devices and strategies.

KEYWORDS: Security, Human Factors, Shoulder surfing, password entry, Random Password entry.

I. INTRODUCTION

Passwords remain the dominant means of authentication in today's systems because of their simplicity, legacy deployment and ease of revocation. Unfortunately, common approaches to entering passwords by way of keyboard, mouse, touch screen or any traditional input device, are frequently vulnerable to attacks such as shoulder surfing and password snooping. Current approaches to reducing shoulder surfing typically also reduce the usability of the system; often requiring users to use security tokens, interact with systems that do not provide direct feedback or they require additional steps to prevent an observer from easily disambiguating the input to determine the authentication methods do not support traditional password schemes. I present Blackhole, a similar approach to password entry that retains the ease of use of traditional passwords, while mitigating shoulder-surfing and acoustics attacks. Blackhole password entry makes gleaning password information difficult for the unaided observer while retaining the simplicity and ease of use for the user. In spite of all the limitations with the traditional method of password entry, we have come up with a new methodology to use the same traditional method in a different way. A twenty(20) character long password is entered the first time when a new user signs up, the password gets stored and different combinations from the original 20 character long password, each of six character long is generated every time. Thus the user needs to enter different passwords (of 4 characters long) each time he wants to access his/her account. Thus making no use of shoulder surfing and eaves dropping.

II. BACKGROUND AND RELATED WORK

Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. It can be done remotely using binoculars and cameras, using keyboard acoustics, or electromagnetic emanations from displays. Access to the user's password simply by observing the user while he or she is entering a password undermines all the effort put in to encrypting passwords and protocols for authenticating the user securely. To some extent, the human actions when inputting the password are the weakest link in the chain.

In general, approaches to overcoming shoulder surfing rely on "increasing the noise" for the observer so that it becomes difficult for the observer to disambiguate the user's actions/input. Rothetal present an approach for PIN entry which uses the philosophy of increasing the noise for the observer. In their approach, the PIN digits are displayed in two distinct sets colored black and white. For each digit the user must make a series of binary choices as to which set (black or white) the PIN digit appears in. The correct PIN digit is identified by intersecting the user's set choices. The approach requires users to make multiple binary selections in order to correctly input each digit of the PIN.

Wiedenbeck et al introduce a shoulder-surfing-resistant graphical password scheme. The user selects a number of icons as his or her pass icons. When logging in, the user is presented with a random assortment of icons. The user must find the pass icons previously identified, create a mental image of the convex hull formed by these icons and then click inside this convex hull. The scheme again relies on multiple challenge response passes in order to successfully authenticate the user. This approach requires the user to learn a new approach and also increases the length of the authentication process.

Weinshall introduces an approach that uses a set of machine generated pictures as the user's password. The user must memorize the pictures. When presented with the login screen, the user must mentally trace a path which includes the password pictures and answer a multiple choice question. A series of challenge-response sets result in authentication. Since only the user knows which path was traced, a human or software observer (spy-ware) would be unable to determine the correct password. However, as the author states, "the benefit is obtained at the cost of a relatively long login time of a few minutes." The approach has been shown to be insecure against an eavesdropping adversary.

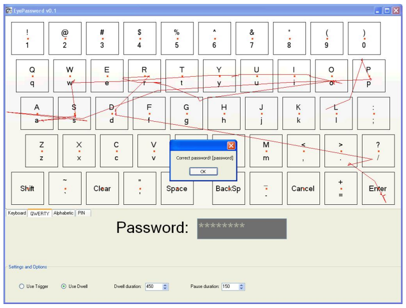
Tanetal propose a spy-resistant keyboard, which uses a level of indirection to prevent the observer from guessing the password. Their approach adds sufficient ambiguity for the observer to be unable to determine the user's choice without remembering the layout of the entire keyboard. However, to enter the password, users must use an unfamiliar keyboard layout and complex interaction technique. While there are other approaches to prevent shoulder surfing [16], it is sufficient to note that all the approaches have the common theme of increasing the noise/ambiguity for the observer.

In this Black hole system, the tradition shoulder-surfing technique is used with modification that over comes the drawback of tradition shoulder-surfing, Instead of having fixed order password, which an intruder can observe, since the password is fixed. In this Black hole system we apply a password sequence in a box, during registration and while logging in, the software selects random sequence of character highlighted but hidden according to the given program.

While logging we need to authenticate giving this highlighted character, if highlighted hidden character can be entered in any order irrespective of the password sequence given in the password box during registration. While logging in for the first the password character will be four letter length and they have to select the highlighted hidden character, in case of incorrect password for more than three times the password length becomes seven character and seven hidden highlighted character will be shown in the password box.

III. EYE TRACKING SYSTEM

Eye tracking technology has come a long way since its origins in the early 1900's [18]. State of the art eye trackers offer none cumbering, remote video-based eye tracking with an accuracy of 1° of visual angle. Eye trackers are a specialized application of computer vision. A camera is used to monitor the user's eyes. One or more infrared light sources illuminate the user's face and produce a glint – a reflection of the light source on the cornea. As the user looks in different directions the pupil moves but the location of the glint on the cornea remains fixed. The relative motion and position of the center of the pupil and the glint is used to estimate the gaze vector, which is then mapped to coordinates on the screen plane.



Correct password! [password]

Password: ********

○ Use Trigger ● Use Dwell Dwell duration: 450 Pause duration: 150

Figure 2: Gaze-pattern when the user enters "password" as the password. Each key has a bright red dot at the center of it. This focus point allows the user to focus their gaze at the center of the target there by increasing the accuracy of eye tracking data

Commercial eye-trackers are currently very expensive, varying in price from US $5,000 to US $40,000. However, the underlying technology is straightforward and other than recovering the cost of research and development, there is no reason why an eye tracker should be so expensive. Technology and research trends indicate that the cost of eye tracking systems should decline rapidly in the near future, making eye tracking a viable form of augmented input for computer systems. Devices such as Apple's MacBook laptops include a built-in Sight camera and hardware trends indicate that even higher resolution cameras will be embedded in standard display devices in the future. Using such a camera for eye tracking would only require the addition of inexpensive IR illumination and image processing software. ATMs are equipped with security cameras and the user stands directly in front of the machine. Since ATM pins typically use only numbers, which need fewer distinct regions on the screen, the quality of the eye tracking required for tracking gaze on an ATM keypad does not need to be as high as the current state-of the- art eye trackers. Current generation eye trackers require a onetime calibration for each user. We envision a system where the calibration for each user can be stored on the system. Inserting the ATM card identifies the user and the stored calibration can be automatically loaded. Gaze-based password entry has the advantage of retaining the simplicity of using a traditional password scheme. Users do not need to learn new way of entering their password as commonly required in the techniques described in the previous section. At the same time, gaze-based password entry makes detecting the user's password by shoulder surfing a considerably harder task, thereby increasing the security of the password at the weakest link in the chain – the point of entry. Gaze-based password entry can therefore provide a pragmatic approach achieving a balance between usability and security.

BLACK HOLE SYSTEM IS ADVANCED FROM EYE TRACKING SYSTEM?

HOW?

Gaze-based system is advance login system, which have sensor and which can track the character that the eye observes and enters the character and very difficult to the intruder observe the password, since the intruder has no clue about the password.

Eye tracking system has some draw backs like, Contrary to gaze-based typing techniques, gaze-based Password entry technique should not provide any identifying visual feedback to the user (i.e. the key the user looked at should not be highlighted). In black hole password entry system, we are using the traditional system to enter the password, So that there is no chance for this type of feedback. Black hole technology in complex and architecture in complex and difficult to understand and the cost of implementing technology is high.

Black hole uses traditional system for the login process and the technology can be modified on the cost of the old tradition shoulder surfing method. The black hole is simple and easier to implement whereas the gazed based system is difficult to implement is certain area, like ATM ,computers because it needs more advancement in the technology but the black hole can be easily implemented in any sectors , ATM etc., with no additional cost but still having high security assured.

MOTIVATION FOR BLACKHOLE DESIGN

From the evolution of computer there has been always threat to the important information for the protection of information use login system, but since the evolution of computer, the traditional login system is in still for general authentication but the hackers are understood the process of ethical hacking and can break in the user login system.

This black hole password entry system is similar to our traditional system with little modification. In this system without prior permission of the user the intruder cannot login to it as in the system the newer and newer password will be generated from the existing one and this will be known to the user alone.

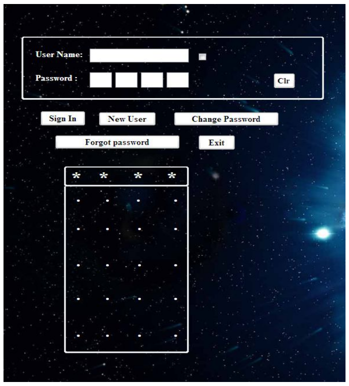
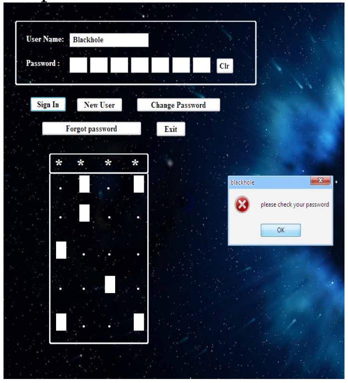


Fig (a) .Shows the login page of the black hole system

The black hole system uses the traditional system but in this system the user enters the new password sequence, when the users logs in the mechanisms for black hole uses traditional password system but while the user registrant, during that time user enter 5*4 matrix password a sequence and while the user logs in the password, the highlight character from 5*4 matrix password sequence is given and the user enters the highlighted characters in the password box and again when the user logs into account the user have enter new sequence of password.


User Name: Blackhole

blackhole

please check your password

Fig (c). When the password gets wrong above three times

When any other unauthenticated user tries to observe our password for the four character password, the authenticated user may try to enter the password to login but since the password sequence has changed row the authenticated enter the wrong sequence or may enter the previous password sequence, which is not the same for the next login time so, if the unauthenticated person tries hit and trail method for login, the password field, changes from the four character password field since he may all the combination of four characters to the user account, but this changes make impossible tasks for the authenticated user to break the password to login and makes the security login system more safer.

IV. THREAT MODEL

I modeled a shoulder surfer as an adversary who observes the user's keyboard and screen. Moreover, the adversary can listen to any sound emanating from the system. Our goal is to build an easy to use password-entry system secure against such adversaries.

Our system allows easy login technique with high security involved because since the password with every time the user logs in and it becomes difficult to access the user password by any other intruder, even if the intruder observes the password carefully, he cannot login into the system, since the sequence password going to change during next login session. The purpose of our system is to propose a random generation of password sequence interaction which eliminates the vast majority of the shoulder-surfing attacks. It is indeed difficult for a shoulder surfer to determine the user's password.

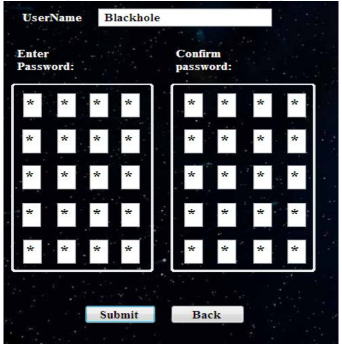
V. DESIGN & MECHANISM

The basic architecture of the black hole is same as traditional system, in the design section we will try to explain the design of the working mechanism of the design of the black hole, first we can explain the working principle of the registration of the login page. The Fig (d) password creator demonstration the registration page.

Here, in the black hole system the registration is same as the traditional system, the difference lies in the password selection area. It contain two (4x5) matrix containing password field in each textbox should be filled and other matrix checks whether the user is entering the correct password and then the user can sign up the black hole system.

Black hole system can be logged as similar to the traditional system except the trick lies in the password entry. It contains four character password box and the password. Character should be selected accordingly to the highlighted hidden character which drives login process.

In case of wrong entry of password more than three consecutive attempts the four character password changes to seven character so the hacker cannot break into the account and after that if the user enters the correct password than it comes four character password, again if the user gives the wrong password then it again changes the password entry length.



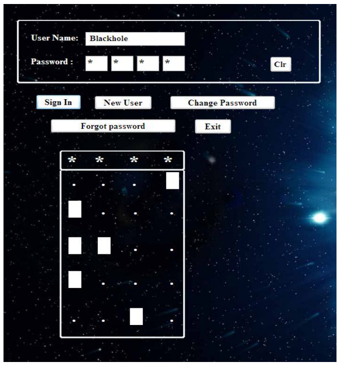
UserName Blackhole

Fig (d). Password creation

The Black hole provides change password option but in this system we need not to give the entire password an given during the registration, instead the user can enter the four character password and select the change password and change the password by providing the new password as like during the registration

5.2 Random Keypad Layout

While typing the password by the user during that time random generator will present on the screen.



User Name: Blackhole

Password : * * * *

Fig (b).Randomly generated password sequence

It will generate the password from the user password. In this keypad will be made up of dots, each and every dots will represent the user password because while creating the password each textbox contain the character later that will be highlighted during in the login session.

When the user opens his password, he has to type the password using the selected random highlights from the random generator. It will be in the form of (4*5 matrix) 5 rows, 4 columns totally twenty dots will take the entire screen.

5.3 Trigger Mechanism

In the multi-modal method, the user uses the QWERTY keypad or numpad for logging in the password in this system the user hits the keyword and it trigger the password and the user an login, but in multi-modal a simultaneous observer a can observe the password can login by the multimodal system, other drawback is when the password is transfer from atm machine to server during that time there is some possibility to hack the password.

Black hole system does not have this demerits since whenever the user have to login it will send different sequence every time the user logs. So, there is less possibility for the hacker to intrude into the system because every time the user logs in he gets a new sequence to enter.

5.4 Feedback

Contrary to black hole password entry system, first it will take some time for the users to get used to the password for accessing.

Since the password coding is done in the form of 4*5 matrixes, it will take six to seven times for the users to identify the words in the matrix.

But after frequent usage of the code it will become an easy task for the user and thus they will obtain privacy.

VI. IMPLEMENTATION

I implemented Black hole on Windows using .Net framework. Back end process: sql server 2000. Can be installed and used on any platforms and for all types of services of the study, subjects were asked to provide their subjective opinions on the techniques used.

VII. TESTS AND RESULTS

I tested our project for its robustness on security; by various experts, from our tests we found our method successful in our experiment and our technique stood on top. Contrast analyses between other techniques showed that the differences between the keyboard and all other systems including gaze based techniques are significant.

VIII. DISCUSSION

While the time difference between using other new high security systems such as Gaze-based system is very high when compared with that of our 'black hole' security system which is comparatively less. And our method follows the traditional password entry technique and hence can be implemented in any of the security services including ATM's, internet services such as mails etc. as our system follows the traditional method, it will be readily accepted by almost all kinds of users globally.

While other systems involves new practices and usage to new hardware and cannot be readily accepted.

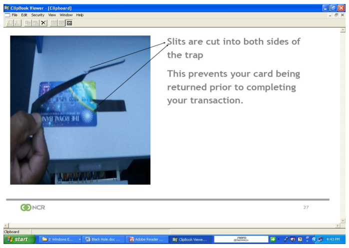
I have heard news about the stealing of account cash through different password recovery techniques. They are almost useless with our black hole security systems. I provide a entirely different and optimized way of protecting our private datas.

The equipment used to capture your ATM card number and PIN is cleverly disguised to look like normal ATM equipment. A "skimmer" is mounted to the front of the normal ATM card slot that reads the ATM card number and transmits it to the criminals sitting in a nearby car. At the same time, a wireless camera is disguised to look like a leaflet holder and is mounted in a position to view ATM PIN entries.

The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM."

This activity has been around for a few years. In the past, it was primarily done in small retailers, where the skimming device was behind the counter and the camera was over the keypad. It was also done by setting up ATM machines that were completely fake.

Also another way of getting your ATM hacked is a modern sophisticated technique in which the thief will prepare a tape made of a magnetic film which will fit into the card slot in an ATM. The thief will fix the card into the slot which is almost out of sight for any observer. When a victim enters his original card, the details get saved in the tape and the card gets stuck into the slot, the thief waiting for the right time enters into the ATM room as a helper and gets the PIN details from the victim. Once the victim leaves the taking his money, the thief gets the chance and from the tape he enters the PIN as well and gets the money from the victim's account. This is impossible in our method.

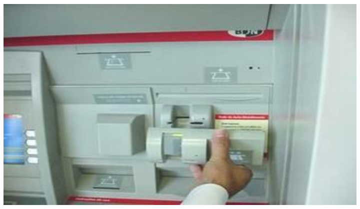


Slits are cut into both sides of the trap

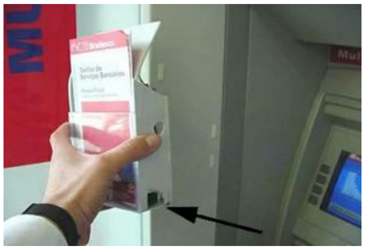
This prevents your card being returned prior to completing your transaction.

It's always a VERY GOOD IDEA to implement our technique in such cases, where the stealing of passwords through hidden cameras is of no use to the thieves. They can try as many times as they wish with the stolen password to unlock our system and fails in all those attempts. Our system will only accept new combinations every single time. Here is a picture of a ATM Machine after being compromised.

They attach a device over the card slot on the legitimate ATM, which reads the magnetic information. Using the latest wireless technology, it is normally transmitted to fraudsters in a nearby vehicle.



Your ATM is protected by a PIN, but these criminals have a solution for this too. They install a hidden camera, again using the latest technology (wireless) and the PIN is digitally recorded.



Here is a picture of the compromised ATM with the camera installed.

IX. FUTURE WORK

I can even improve the effective security of this technique by employing certain algorithms and increasing the probability of recurrence of the same combination of sequences to a mere infinite number. This assures the 99.9% reliability on our security. Our team is working on the algorithms and on the improvement of the systems.

X. CONCLUSION

Passwords possess many useful properties as well as widespread legacy deployment; consequently we can expect their use for the foreseeable future. Unfortunately, today's standard methods for password input are subject to a variety of attacks based on observation, from casual eavesdropping (shoulder surfing), to more exotic methods. Many alternative approaches to password entry, based on different techniques, which deters or prevents a wide range of these attacks are also introduced but with improved tediousness and additional costlier hardware requirements. We have demonstrated through user studies that our approach requires a little marginal additional entry time.

REFERENCES

1. Miklos Santha, Umesh V. Vazirani (1984-10-24). "Generating quasi-random sequences from slightly-random sources". Proceedings of the 25th IEEE Symposium on Foundations of Computer Science. University of California. pp. 434–440. ISBN 0-8186-0591-X. http://www.cs.berkeley.edu/~vazirani/pubs/quasi.pdf. Retrieved 2006-11-29.

2. John von Neumann (1963-03-01). "Various techniques for use in connection with random digits". The Collected Works of John von Neumann. Pergamon Press. pp. 768–770. ISBN 0-08-009566-6.

3. Adam Young, Moti Yung (2004-02-01). Malicious Cryptography: Exposing Crypto virology. sect 3.2: John_Wiley_&_Sons. pp. 416. ISBN 978-0-7645-4975-5. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0764549758.html.

4. Handbook of Applied Cryptography, Alfred Menezes, Paul van Oorschot, and Scott Vanstone, CRC Press, 1996, Chapter 5 Pseudorandom Bits and Sequences (PDF).

5. Brown, George W (June 1949), History of Rand's Million Digits, papers, RAND Corporation, http://www.rand.org/pubs/papers/P113.

6. Brown, Bernice (October 1948), Some Tests of the Randomness of a Million Digits, Papers, RAND Corporation, http://www.rand.org/pubs/papers/P44 .

7. "Tube type 6D4", Electron Tube Data handbook, Sylvania, 1957 .

8. A Million Random Digits with 100,000 Normal Deviates, RAND Corporation, http://www.rand.org/publications/classics/randomdigits/ .

9. Galton, Francis (1890), "Dice for statistical experiments", Nature (42): 13–4, http://www.mugu.com/galton/statistician.html .

10. (PDF) Randomness and Genuine Random Number Generator with Self-testing Functions, Japan: LE Tech RNG, http://www.letech-rng.jp/SNA+MC2010-Paper.pdf.

# ^ http://mlawire.blogspot.com/2009/07/linux-password-generator.html

# ^ http://docs.python.org/py3k/library/random.html

# ^ http://docs.python.org/py3k/library/os.html#os.urandom

# ^ a sample PHP secure random program

# ^ http://php.net/manual/en/function.openssl-random-pseudo-bytes.php

# ^ Levine, John R., Ed.: Internet Secrets, Second edition, page 831 ff. John Wiley and Sons.

# ^ Schneier, B: Applied Cryptography, Second edition, page 233 ff. John Wiley and Sons.

# ^ "Electronic Authentication Guideline" (PDF). NIST. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Retrieved March 27, 2008.