ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.7

Result Analysis on H2S Sholder Surfing improves Honeyword Encryption

Khushal Dalvi[1], Deepak Dharrao[2], Manjusha Tatyia[3]
Student[1], Professor[2], Assistant Professor[3]
Department of Computer Engineering
Indira College of Engineering & Management, Pune, India

Abstract:
When client contribution their passwords in a public place, they might be at danger of attackers stealing their password. An attacker can capture a password by direct observation or by recording the persons authentication session. This is referred to as shoulder-surfing and is identified threat of specific concern when authenticate in public areas. Till not too long ago, the only protection against shoulder-surfing was the alertness on the portion of the user. Shoulder surfing resistant password authentication mechanism promise shoulder-surfing resistant authentication to user. It makes it possible for user to authenticate by getting password in graphical way at unconfident locations, since users never ever have to click straight on password icons. It can be represented the honey word mechanism to detect an opponent who attempt to login with split passwords. New password is the combination of current user passwords known as honey words. Fake password is practically nothing but the honey words fundamentally for every username which is set of sweet words is constructing such that simply a one demanding part is the appropriate password and the other persons are honey words (decoy passwords). Therefore, when an opponent tries to enter into the mechanism with a honey word, an alarm is trigger to notify the manager about a password leakage. Honey words to detect attack next to hash password database. For every user account the real password stored as a type of honey words. In this study, system examine in detail with cautiously focus the honey word and present some comment to concentrate be utilized weak points. Also concentrate on practical password, minimize storage expense of password, and exchange way to select the new password from current user passwords.

Keywords: Tactile UI, security, PIN entry, user study, Security, Experimentation, Human Factors

I. INTRODUCTION

Mainly of the existing graphical password scheme are susceptible to known shoulder-surfing threat precisely where an attacker can capture a password by straight watching or by demo the authentication session. Due to the illustration border, shoulder-surfing becomes an exacerbate issue in graphical passwords. A graphical password is less difficult than a text mainly based password for most individuals to keep in mind. Suppose an 8- character password is required to achieve entry into a specific laptop network. Robust passwords can be developed that are resistant to guessing, dictionary attack. Essential loggers, shoulder-surfing and social engineering. Graphical passwords have been utilized in authentication for mobile phones, ATM machines, E-transactions. In this there are two problems that need to be deeming to conquer these safety issues: The second point is that a protected device must detect whether or not a password file discovery incident occur or not to take suitable actions. In this study, we concentrate on the latter problem and deal with fake passwords or accounts as an easy and price efficient resolution to detect compromise of passwords. When a user sends a login request, the login server will decide the order of her amongst the customers, and the order of the submitted password amongst her sweet words. The login server sends a message of the type to a safe server which is known as honey checker, for the user and her sweet word. The honey checker will make a decision whether or not the submitted word is a password or a honey word. If a honey word is submitted, then it will raise an alarm or take an action that is previously selected. The honey checker can't know something about the users password or honey words. It maintains a single database that consists of only the order of the accurate password amongst the users sweet words.

II. REVIEW OF LITERATURE

1.Multi-touch passwords for mobile device access.

Authors: I. Oakley and A. Bianchi
Description: Draw-a-Secret password scheme, like the Google robot prototype security device, involve stroke out a form on a stroke screen. This paper explores technique for increasing the wealth of this input modality (multitouch input, off-target interaction) in order to increase password entropy and confrontation to surveillance. A determining user study places of interest user perception and usability issue connecting to this intend space and suggest information for potential development of this concept.

2.The doodb graphical password database: Data analysis and benchmark results.

Author: M. Martinez-Diaz, J. Fierrez, and J. Galbally
Description: We there DooDB, a drawing database contain data from 100 users captured with touch screen-enabled mobile device under sensible situation following a methodical protocol.

The database contain two corpora:
1) doodles
2) pseudo-signatures, which are can be cut down finger-drawn versions of the handwritten signature. The dataset includes real samples and forgeries, produced under worst-case conditions, where attacker have visual access to the picture process. Statistical and qualitative analyses of the data are presented, comparing doodles and pseudo-signatures to

handwritten signatures. Time variability, learning curves, and discriminative power of dissimilar features are also studied. Verification presentation against forgeries is analyzed using state-of-the-art algorithms and benchmark results are provided.

3. Graphical Password-Based User Authentication With Free-Form Doodles.
Authors: M. Martinez-Diaz, J. Fierrez, and J. Galbally
Description: User verification using simple gesture is currently ordinary importable apparatus. In this function, verification with free-form sketch is calculated. Verification systems using dynamic time warp and Gaussian mixture models are suggested based on dynamic signature verification approaches. The most discriminate features are deliberate using the chronological forward floating selection algorithm. The effects of the time lapse between capture sessions and the impact of the preparation set size are also intentional. Development and validation experiment are performed using the DooDBdatabase, which contain passwords from 100 users capture on a smart phone touch screen. Equal error rates between 3% and 8% are obtainedagainst random forgeries and between 21% and 22% against skilled forgeries.

4.Covert attention shoulder surfing: Human adversaries are more powerful than expected
Authors: Dennis Mirante, Justin Cappos
Description: while a consumer interacts with a processor system to enter a secret password, shoulder surfing attacks are of great concern. To cope with this problem, previous methods presumed imperfect cognitive capability of a human opponent as a prevention, but there was a drawback with the supposition.

5.Understanding Password Database Compromises
Authors: T. Kwon, S. Shin, and S. Na
Description: Despite continuing advances in cyber security, website incursions, in which password databases are compromised, occur for high profile sites dozens of times each year. Dumps of recently stolen credentials appear on a regular basis at websites like pastebin.com and pastie.com, as do stories concerning significant breaches. As a result of these observations, we chose to examine this phenomenon. A study was undertaken to research information posted on the web concerning recent, high profile website intrusions, wherein user login credentials and other data were compromised. We searched for the party responsible for the incursion, the attack mechanism utilized, the format in which the login data was stored, and the location of any password dumps pilfered from the site. News stories from trade related journals, press releases from the victim company, hacker sites, and blogs from individuals and companies engaged in security analysis were, in particular, searched in order to find related information. A total of thirty four breaches were researched.

6.The Dangers of Weak Hashes
Authors: Kelly Brown
Description: There have been several high publicity password leaks over the past year including LinkedIn, Yahoo, and eHarmony. While you never want to have vulnerabilities that allow hackers to get access to your password hashes, you also want to make sure that if the hashes are compromised it is not easy for hackers to generate passwords from the hashes. As these leaks have demonstrated, large companies are using weak hashing mechanisms that make it easy to crack user passwords. In this paper I will discuss the basics of password hashing, look at password cracking software and hardware, and discuss best practices for using hashes securely.

III. SYSTEM REQUIREMENTS

- **Hardware Requirements:**

System : Pentium IV 2.4 GHz.
Hard Disk : 40 GB.
Ram:512Mb.

- **Software Requirements:**

Operating system : Windows XP/7.
Coding Language : JAVA/J2EE, Hibernate.
IDE : Eclipse Kepler
Web server : Apache Tomcat 7.
Front End : JSP, CSS etc.
Back End : SQLYog community/XAMPP Server.

IV. MATHEMATICAL MODEL

Let S be the Whole system which consists:
S= IP, Pro, OP. Where,
A. IP is the input of the system.
B. Pro is the procedure applied to the system to process the given input.
C. OP is the output of the system.

A. Input: IP = u, I, LI, ht,wt, pv , n,h.
Where,
1. u be the user.
2. I be set of images used for creating graphical password.
3. ht be the height of image.
4. wt be the width of the image.
5. pv be the pass values of the selected image for generating graphical password.
6. LI be the login indicator used at the time of login.
7. n be the number of images chosen for creating graphical based password from set of images I.
8. create 3 honey words.

B. Procedure:

- **Registration phase:**

i. In this stage, the user creates an account which contains a username and a password. The password consists of only one pass- quare per image for a sequence of n images.
ii. The number of images n is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account.
iii. Then the systems will Discretization the selected images by using pass matrix approach into x into y grinds by calculating ht and wt of images.
iv. Then system will create the graphical based password after clicking on the images selected from I.
v. At a time of registration, we create honey words.

- **2. Authentication phase:**

i. A login indicator LI is comprised of a letter and a number is created by the login indicator generator module.
ii. The LI will be shown when the user login with his email. In this case, the indicator is conveyed to the user by visual feedback. The indicator can also be delivered through a predefined image.
iii. Generating horizontal and vertical access control for login indicator based user selected images at the time of registration

this access control will change at every login time i.e. LI is defined for one time use only.
iv. The generated access control will be send to user registered email address.
v. User will enter the graphical password based on generated pass-values i.e. access controls.
vi. Multiple passwords created based on honey word.
vii. Honey checker disclosed the hacker information.

C. Output:

Secure and authenticated system based on Pass Matrix based graphical password system. Finally, to create honey words from existing user password. And also to detect attacks against hashed password databases. Reduce the storage cost while creating honey words.

V. SYSTEM ARCHITECTURE

In the proposed system, User first registers. In the registration, he will select 3 images as a password images and mention 3 sugar words which is co relevant to the original password. At the time of login, User first enters username and selects the images from image matrix (i.e. 9 images) that images same as a register time image. After that image will divide into 7*11 matrixes. On the basis of password (i.e. Secrete bit + random password) select the box w.r.t each images. After this honey word concept will apply to system. If user is fake user and they will not entered correct password or guess password or it will enter honey word as a password then honey checker check that password with some condition like:
1. If it is honey word then out of 3 chances 1 chance will increase.
2. If it is not a honey word or any sugar word then after 3 chance system automatic generate alert to owner.
After this condition user successfully login on system without shoulder surfing attack on user side. Here system also defines encryption technique called honey encryption for more security regards password on the server side. For that system used seed formation and many to many relationships with XOR binary operation. Through this technique, system failed hackers hacking on server.

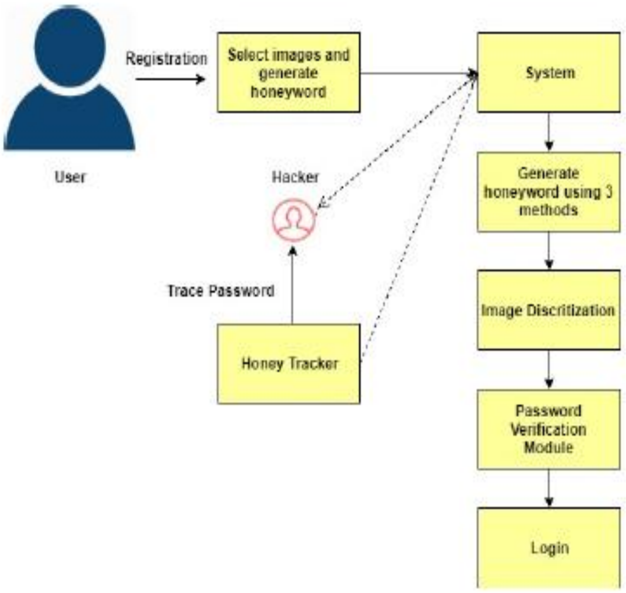

Registration
Select images and generate honeyword
System
User
Hacker
Generate honeyword using 3 methods
Trace Password
Image Discritization
Honey Tracker
Password Verification Module
Login

Fig. 1. Block Diagram of Proposed System

Table. I. Table name (write your table name)

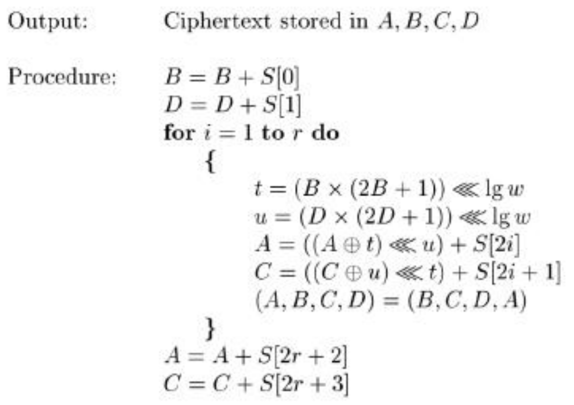
Parameters	Sholder Surfing (Existing)	Sholder+Honeyword (Proposed)
Efficiency	50.6	88.6
Availability	55.8	91.5
Accessibility	0.0359445	97.9
Robustness	89.3	93.02
Accuracy	95.4	98.9

VI. METHODOLOGIES AND ALGORITHM

Encryption Algorithm:

RC6:

In cryptography, RC6 (Rivest cipher 6) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and also was submitted to the NESSIE and CRYPTREC projects. It was a proprietary algorithm, patented by RSA



```
Output:      Ciphertext stored in $A, B, C, D$

Procedure:   $B = B + S[0]$
             $D = D + S[1]$
             for $i = 1$ to $r$ do
                 {
                     $t = (B \times (2B + 1)) \lll \lg w$
                     $u = (D \times (2D + 1)) \lll \lg w$
                     $A = ((A \oplus t) \lll u) + S[2i]$
                     $C = ((C \oplus u) \lll t) + S[2i + 1]$
                     $(A, B, C, D) = (B, C, D, A)$
                 }
             $A = A + S[2r + 2]$
             $C = C + S[2r + 3]$
```

Security:

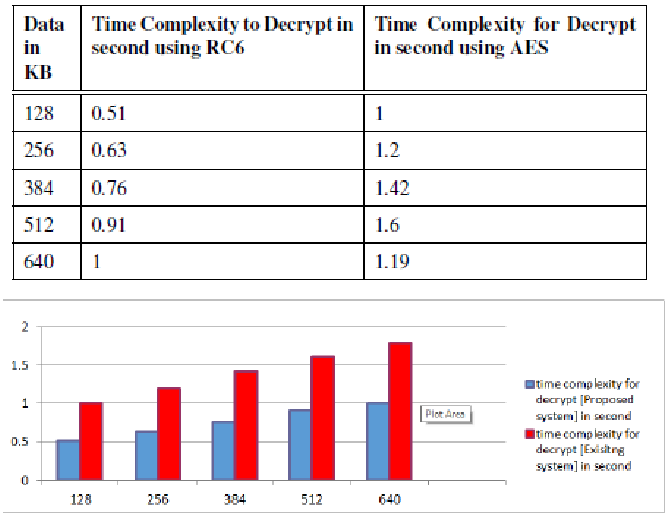
RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits up to 2040-bits, but, like RC5, it may be parameterised to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

Key eneration Algorithm: SPEKE:

SPEKE makes only one small change to the Diffie-Hellman Key Exchange. Rather than agreeing on a shared generator, each party will compute a generator (G; Step 2) by squaring the hash of some shared password. Because the generator (G) is now derived from a password, it is private. Note that in Step 5, Alices computation of K will be the same as Bobs computation of K if and only if the shared password used in Step 2 are the same. Hence, if only Alice and Bob know the shared password, then this algorithm is safe from a MitM attack. And since the generator (G) is private, no offline dictionary attack is possible. Note well, however, that no validation of K has occurred. So while Alice knows that data encrypted with K cannot be read by anyone but Bob, she still doesnt know whether the person on the other end of the exchange is, in fact, Bob. If it isnt Bob on the other end, K will contain a nonsensical value and any data encrypted by it will be irretrievable (assuming the security of the underlying cryptography system).

VII. PERFORMANCE ANALYSIS

Differentiate output results of encryption-decryption (Base 64, Hexadecimal) results are given in Fig. for Existing and Proposed System, Fig. shows the results at base 64 encoding while It gives the results of hexadecimal base encoding. We can notice that there is significant difference at both systems. The same method is applied for encryption with multiple sample; we can recognize that the two bars given as given



Data in KB	Time Complexity to Decrypt in second using RC6	Time Complexity for Decrypt in second using AES
128	0.51	1
256	0.63	1.2
384	0.76	1.42
512	0.91	1.6
640	1	1.19

Figure.1. Result Table with graph

VIII. CONCLUSION

We contain investigate carefully the safety of the honey word system and bring in a numeral of defect with the intention of require to be built-in with previous to victorious understanding of this strategy. We suggest monitor data access patterns by profile user behavior to decide if and when a malicious insider illegally accesses someone’s documents in a system service. trap documents stored in the system along with the user’s real data also serve up as sensors to detect illegal access. Once unauthorized information access or exposure is suspected, and after verified, with challenge for instance, we flood the malicious insider with fake information in to be able to thin or divert the uses data.

ACKNOWLEDGMENT

Improve authentication: It provides shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Security enhanced for user password: It will provide security and authentication for users password by generating honeyword.

IX. REFERENCES

[1]. D. Mirante and C. Justin, Understanding password database compromises, Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, New York, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.

[2]. A. Vance, If your password is 123456, just makes it hackme, New York Times, Jan. 2010.

[3]. K. Brown, The dangers of weak hashes, SANS Institute InfoSec Reading Room, Maryland US, pp. 122, Nov. 2013, [Online]. Available: http://www.sans.org/reading-room/ white papers/ authentication/dangersweak- hashes-34412.

[4]. M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, Password cracking using probabilistic context-free grammars, in Proc. 30thIEEE Symp. Security Privacy, 2009, pp. 391405.

[5]. F. Cohen, The use of deception techniques: Honeypots and decoys, Handbook Inform. Security, vol. 3, pp. 646655, 2006.

[6] M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, Improving security using deception, Center for Education and Research Information Assurance and Security, Purdue Univ., West Lafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013-13, 2013.

[6]. C. Herley and D. Florencio, Protecting financial institutions from bruteforce attacks, in Proc. 23rd Int. Inform. Security Conf., 2008, pp. 681685.