Honey Words “Detecting Password Cracking With Hacker Tracking”

[1] Ashwini Yele, [2] Pranali Pangerkar, [3] Prita Patil
[1][2][3] Department of Computer Engineer,
Mumbai University
Vidyalankar Institute of Technology, Mumbai
[1] ashwini.yele@vit.edu.in [2] pranali.pangerkar@gmail.com, [3] prita.patil@gmail.com

***Abstract*— For each user account, the legitimate password is stored with several honey words in order to sense impersonation. If honey words are selected properly, an adversary who steals a file of hashed passwords cannot be sure if it is the real password or a honey word for any account. Moreover, entering with a honey word to login will trigger an alarm notifying the administrator about a password file breach. At the expense of increasing storage requirement by 20 times, a simple and effective solution to detection of password file disclosure events. In this study, we advance the honey word system by introducing a concept of decoy files. Also, we suggest an alternative approach that selects honey words from existing user passwords in the system to provide realistic honey words – a perfectly flat honey word generation method.**

***Keywords*—honey word , decoy files ,access control , honey pot.**

I. INTRODUCTION

Use of malicious ways to access private data of users has rapidly increased these days. Internet is considered to be a boon to the 21st era but practice of some unwanted actions is turning out to be curse by unauthorised users . Honeywords are being introduced into the system so that even if any hacker has hacked the valid user password or his credential information the hacker will not directly get access to the information instead he will get access to the decoy details or files of the user. This can be achieved by implementing a concept called honeywords into the system. This system is mainly concerned with the security issues of the credential information. The use of decoy files is made so as to give the hacker a feel of accessing original data. This decoy file is a fake file which the hacker access considering it as the true file. Also after the hacker access files which are decoy files the valid user will easily come to know through notifications that some unauthorised user is trying to access his account.

A typical computer user today manages passwords for many different online accounts. Users struggle with this task —often forgetting their passwords or adopting insecure practices, such as using the same password for multiple accounts and selecting weak passwords. While there are many books, articles, papers and even comics which educating users about selecting strong individual passwords, there is very little work on password management schemes —systematic strategies to help users create and remember multiple passwords. Before we can design good password management schemes it is necessary to address a fundamental question: How can we quantify the usability or security of a password management scheme?

One way to quantify the usability of a password management scheme would be to conduct user studies evaluating each user‘s success at remembering multiple passwords over an extended period of time. However, these user studies would necessarily be slow and expensive and would need to be repeated for each new password management scheme. Our thesis is that user models and security models can guide the development of password management schemes with analysable usability and security properties. We present several results in support of this thesis. First, we introduce Naturally Rehearsing Password schemes. Notably, our user model, which is based on research on human memory about spaced rehearsal, allows us to analyse the usability of this family of schemes while experimentally validating only the common user model underlying all of them.

Second, we introduce Human Computable Password schemes, which leverage human capabilities for simple arithmetic operations. We provide constructions that make modest demands on users and we prove that these constructions provide strong security: an adversary who has seen about 100 10-digit passwords of a user cannot compute any other passwords except with very low probability.

Our password management schemes are precisely specified and publishable: the security proofs hold even if the adversary knows the scheme and has extensive background knowledge about the user (hobbies, birthdate, etc.). They do not require any significant server-side changes. In further support of our thesis, we show that user models and security models can also be used to develop server-side defences against online and offline attacks.

Disclosure of password files is a severe security problem that has affected millions of users and companies like Yahoo, RockYou, LinkedIn, eHarmony and Adobe[1,2], since leaked passwords make the users target of many possible attacks. These recent events have demonstrated that weak password storage methods are currently in place on many web sites. For example, the LinkedIn passwords were using the SHA-1 algorithm without a salt and similarly the eHarmony passwords were also stored using unsalted MD5 hashes [3]. Indeed, once a password file is stolen, by using password cracking techniques like the algorithm of Weir et al. [4] it is easy to capture most of the plaintext passwords. In this respect, there are two issues that should be considered to overcome these security problems: First, passwords must be protected by taking appropriate precautions and storing with their hash values computed through salting or some other complex mechanisms. Hence, for an adversary it must be hard to invert hashes to acquire plaintext passwords. The second point is that a system should detect whether a password file disclosure incident happened or not to take appropriate actions. In this study, we focus on the latter issue and deal with fake passwords or accounts as simple and cost effective solutions to detect compromise of passwords. Honeypot is one of the methods to identify occurrence of password database breach.

In this study, we analyse honeyword approach and give some remarks about security of the system. Furthermore, we point out that the key item for this method is the generation algorithm of honeywords such that they shall be indistinguishable from the correct passwords. Therefore, we propose a new approach that uses passwords of other users in the system for honeyword sets, i.e. realistic honeywords are provided. Moreover, this technique also reduces storage cost compared with the honeyword method in [9]. The rest of this paper is organized as follows. In Section 2, we review the honeyword approach and discuss honeyword generation procedures. Section 3 examines security of honeywords and Section 4 gives description of our proposed model. In Section 5 we analyze its security properties and we demonstrate a comparison between our approach and the original methods in Section 6. Finally, in Section 7 we conclude this paper.

II. LITERATURE REVIEW

1. Pinkas and Sander first proposed the use of reverse Turing Tests (RTTs, e.g., captchas) to restrict large-scale online password dictionary attacks. The protocol challenges users with RTTs for a small fraction of user-id password pair reduce server-load and impact while keeping the cost of launching a large scale guessing attack significantly high. They proposed the use of distorted images ciper/decipher machine to communicate small messages in human machine interaction.

2. Imran Erguler, in his paper _Achieving Flatness: Selecting the Honeywords from Existing User Passwords‘ researches Passwords are selected and checked if they match with honeyword or real password. This paper focuses on the various methodology used for carrying out the process of generation of hashed password like Chaffing by tweeking, Chaffing-with-a-password-model, Chaffing with Tough Nuts and hybrid model.

3. In this approach, the administrator purposely creates deceit user accounts to lure adversaries and detects a password disclosure if any one of the honeypot passwords get used [5,6]. This idea has been modified by Herley and Florencio [7] to protect online banking accounts from password brute-force attacks. According to the study, for each user incorrect login attempts with some passwords lead to honeypot accounts, i.e. malicious behaviour is recognized. For instance, there are 108possibilities for a 8-digit password andlet system links 10000 wrong password to honeypot accounts, so the adversary performing the brute-force attack 10000 times more likely to hit a honeypot account than the genuine account.

4. Use of decoys for building theft resistant is introduced by Bojinov et al. in [8] called as Kamouage. In this model, fake password sets are stored with the real user password set to conceal the real passwords, thereby forcing an adversary to carry out a considerable amount of online work before getting the correct information.

5. Recently, Juels and Rivest have presented the honeyword mechanism to detect an adversary who attempts to login with cracked passwords [9]. Basically, for each username a set of sweet words is constructed such that only one element is the correct password andthe others are honeywords (decoy passwords). Hence, when an adversary tries to enter with a honeyword, an alarm is triggered to notify the system about a password leakage.

III. PROPOSED WORK

In this section, we first briefly summarize the honeyword password model proposed by the Juels and Rivest in [9]. Then, we overview the methods on generation of honeywords given in the study and discuss some points that can cause some security problems.Basically, the simple but clever idea behind the study is insertion of false passwords – called as honeywords – associated with each user‘s account. When an adversary gets the password list, she recovers many password candidates for each account and she cannot be sure about which word is genuine. Hence, cracked password files can be detected by system administrator if a login attempt is done with a honeyword by the adversary.

This system will help the user to keep their personal data secured. This software will help the user from getting their data without being hacked by the hacker providing the safety of their private information by sending notifications to the actual user if any hacker is trying to get access to the actual user‘s account.

Algorithm for Honey Word Generator:

```
1. Take input as a Position(pos) and Password(pass).
2. Reverse the Password.
3. Apply for loop from 1 to 20.
4. if(i == position)
realPassword[i] = pass;
hashPassword[i] = generatorHash(pass);
5. else
realPassword[i] = replace(password1);
hashPassword[i] = generatorHash(pass);
6. passResult.put("real", realedPassword);
passResult.put("hash", hashedPassword);
passResult is HashMap.
7. return passResult;
```

Algorithm for Honey Word Checker:

```
if (honeyPassList[i].equals(passwordHash) && i != Integer.parseInt(pos))
{ }
```

Phase 1 : User registration and login

In this phase user can login into the system by simply entering their details and can logon into the system. This is the phase where user gets login into the system by once after doing registration.

Phase 2: Honeyword Generator

In this phase honeywords are generated by using chaffing with tweeking concept.Here honeywords are generated to ensure security of the system.There are total 20 honeywords are generated randomly and are stored in the some file.20 honeywords as in there are 19 honeywords generated randomly and 1 is the actual password is what user going to enter while logging into the system.So there are total 20 honeywords are generated and this honeywords are stored randomly. If any hacker is trying to get access into the valid user‘s account then he has given 3 attempts to get login into the system. If any of the password entered by hacker matches with the honeyword then he will get access to the system but system will show him the decoy files(dummy files)which are fake files and they are not the actual ones. Though hacker got fake files but the notification is sent to the valid user by mail that someone has tried to login into your account.

Phase 3: Implementation of Services like notification, performance evaluation and knowledge sharing point

Notification: A Notification Program is an additional service offered in our proposed System to notify the legitimate user about the hacker trying to access a file without his permission. Here the automated system notifies using techniques like SMS and Email. The permission to access this service is offered to all the users. The advantage of implementing our proposed service is to enhance the overall performance of the system and provides user satisfaction.

Knowledge Sharing Point : It is a special service provided in our proposed system. Here user can share their research work and knowledge gain from outside resources. During implementation we have used the concept of private user role. Each user can share their research work and knowledge gain and Delete and Edit permission access control is only assigned to that individual users and not getting inherited to upper user hierarchy.

Phase 4: Providing Central Repository for data storage

The present system involves scattered data across all the departments so integration and sharing for different purpose become difficult and time consuming. To overcome this difficulty we have proposed Central Repository for database system. with three-tier client server architecture.

Phase 5: Ensuring data security and data privacy

Last phase of this system in this phase, we have considered security aspect of our proposed system. We are going to secure our System by implementing IP based Security. In IP based security,we have assigned separate IP to our Proposed System and Data Repository which can be accessed only after proper authentication. Due to secured access the code future system modification is secured.

IV. IMPLEMENTATION AND ANALYSIS

The proposed system is implemented on three tier architecture in which the client interface is simply a web browser, XAMP 1.7.1 is configured as a web server, Java script is used as scripting language, MySQL Database connectivity.

After successful completion of all the mentioned in proposed system, we are able to achieve the following aspects related to access control in any organization:

❖ ***Services offered enhances overall performance :*** Notification service, GUI, and Knowledge Sharing Point enhance the overall performance of the system and provides satisfaction to the users.

V. EXPERIMENTAL RESULTS AND DISCUSSION VI.

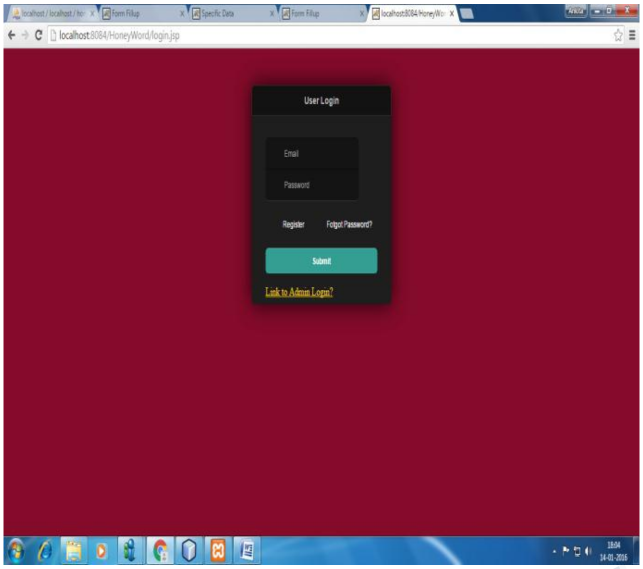


Fig. 1 User Registration

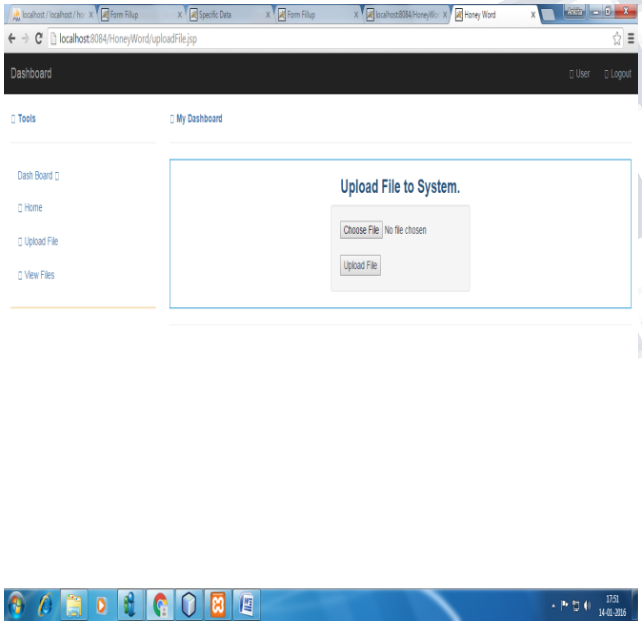
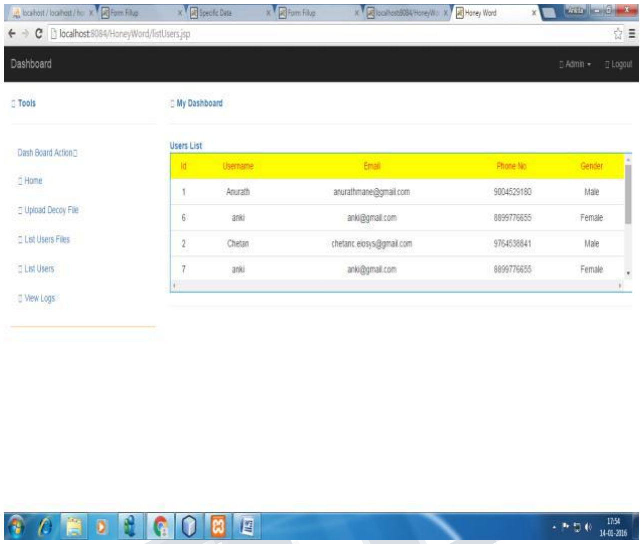


Fig. 2: User uploading a file



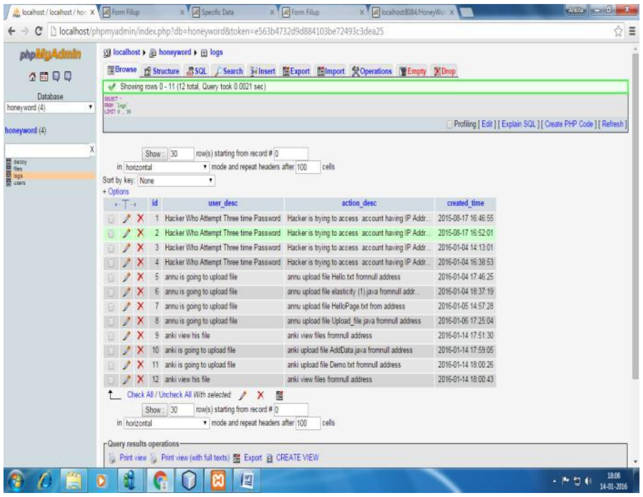
Users List

Id	Username	Email	Phone No	Gender
1	Anurath	anurathmane@gmail.com	9004529180	Male
6	anki	anki@gmail.com	8899776655	Female
2	Chetan	chetanc.eiosys@gmail.com	9764538841	Male
7	anki	anki@gmail.com	8899776655	Female

Fig. 4: User Files List Fig. 4

Parameter	Existing System	Proposed System
Duplicate User Role	Absent	Present
Notification	Using email	Using email as well as SMS
Speed of performance evaluation	Slower	Faster
Knowledge Sharing Point	Absent	Present
Speed of Administrative Actions	Slower	Fatser
Data Access	Slower	Faster

Table 2: Comparison between an Existing system and a Proposed system.


localhost/phpmyadmin/index.php?db=honeyword&token=e563b4732d9d884103be72493c3dea25
phpMyAdmin
localhost ▸ honeyword ▸ logs
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop
Database
honeyword (4)
Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]
Options
Check All / Uncheck All With selected:
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW

Showing rows 0 - 11 (12 total, Query took 0.0021 sec)

```
SELECT *
FROM `logs`
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None

id	user_desc	action_desc	created_time
1	Hacker Who Attempt Three time Password	Hacker is trying to access account having IP Addr...	2015-08-17 16:46:55
2	Hacker Who Attempt Three time Password	Hacker is trying to access account having IP Addr...	2015-08-17 16:52:01
3	Hacker Who Attempt Three time Password	Hacker is trying to access account having IP Addr...	2016-01-04 14:13:01
4	Hacker Who Attempt Three time Password	Hacker is trying to access account having IP Addr...	2016-01-04 16:38:53
5	annu is going to upload file	annu upload file Hello.txt fromnull address	2016-01-04 17:46:25
6	annu is going to upload file	annu upload file elasticity (1).java fromnull addr...	2016-01-04 18:37:19
7	annu is going to upload file	annu upload file HelloPage.txt from address	2016-01-05 14:57:28
8	annu is going to upload file	annu upload file Upload_file.java fromnull address	2016-01-06 17:25:04
9	anki view his file	anki view files fromnull address	2016-01-14 17:51:30
10	anki is going to upload file	anki upload file AddData.java fromnull address	2016-01-14 17:59:05
11	anki is going to upload file	anki upload file Demo.txt fromnull address	2016-01-14 18:00:26
12	anki view his file	anki view files fromnull address	2016-01-14 18:00:43

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Fig. 5: Log details of user action

VI. CONCLUSION

In this paper, a suitable model to avoid password cracking is designed. The principle idea of the System can be used as platform in Institutes .organisation anywhere where credential data is secured using password. It also helps upper user hierarchy to monitor administrative processes and evaluate the performance to take decision for improvement. System provides

Utilization of services like notification, improves overall efficiency of System and provides user satisfaction.

REFERENCES

[1] Ritvars Bregzis,Calvin Gotlieb,Carole Moore , *"The Beginning of Automation in the University of Toronto Library,1963–1972",* in IEEE Annals of the History of Computing, April–June 2002..

[2] Prof. Godswill Obioma , Prof. Ismail Junaidu , Dr. Grace Ajagun , ―The Automation of Educational Assessment in Nigeria: Challenged and Implications for Pre-Service Teacher Educaion‖,Annual Conference of the International Association for Educational Assessment (IAEA) held at the Dan Panorama Hotel, Tel-Aviv, Isreal October 20th – 25th, 2013

[3] M. Jou,J.K. Shiau and H.W. Zhang,‖Application of Web Technologies in Automationon Technology Education‖, International Journal of Computers and Applications, Vol. 31, No. 4, 2009

[4] Xiang Fu, Boris Peltsverger, Kai Qian, Lixin Tao, Jigang Liu,‖ *APOGEE – Automated Project Grading and Instant Feedback System for Web Based Computing*‖, Computer Science and Information Technology, 2nd IEEE International Conference 2009.

[5] Gerald Weber,‖ *Defining the Paperless Workplace with the Paper Metaphor -Not a Contradiction in Terms*‖,Conference: Proceedings of the Fourth Australasian Workshop on Health Informatics and Knowledge Management - Volume 120

[6] Ryan AusankaCrues,‖ *Methods for Access Control:Advances and Limitations",*Ryan Ausanka-Crues Harvey Mudd College 301 Platt Blvd Claremont, California ,2001

[7] Ravi S. Sandhu{, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youman*," Role-Based Access Control Models",* IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[8] Hamid Hatim, Hanan El Bakkali, Ilham Berrada,‖ *Workflow Access Control: From Role Engineering to Task Engineering*‖Internation Journal Internet Technology and Secured Transactions Vol 4, no.1, 2012

[9]Noorr Azah Samsudin,Shamsul Kamal Ahmad Khalid et.al. ,*"Procedure Automation with Immediate User Notification : A Case Study"*, IEEE Symposium on Buisness, Engineering and Industrial Applicatins, Malaysia, 2011.

[10] Andrew Rebeiro-Hargrave1, Hiroshi Nakajima, ―*Investigation into Blood Pressure Variability in Japan and Bangladesh by ICT based Healthcare Systems",* 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014.

[11] Reinhardt A. Botha, Jan H.P. Eloff,‖ *Designing Role Hierarchies for Access Control in Workflow Systems*‖, 0-7695-1372-7101 $10.00 *0* 2001

IFERP connecting engineers... developing research