Honeywords for Password Security and Management

Ms.Manisha Bhole

Student,Dept of Computer Science and Engineering,SSBT COET,Jalgaon,Maharashtra,India

---***---

Abstract - *With emphasis on Digital India and Government's encouragement for cashless transactions, it has become essential for organizations to maintain the secrecy of login credentials of their employees and clients. At the same time it is also necessary to monitor any suspicious activities/attempts to steal such data by hacker. There are many methods to achieve secure login like OTP and Token generators. But these methods require additional devices to be carried by the users. Loss or change of the additional devices can obstruct the user form logging in. Organizations can increase the customer comfort, while maintaining the secrecy, by storing bunch of decoy passwords or "honeywords" corresponding to the correct password in the hashed password database. A hacker hacking the hashed password database would not be able to identify the decoy password and an attempted use of honeyword can set off an alarm.*

In the proposed work, the Honeyword generation method i.e. chaffing-with-tweaking provides some improvements such as handling the brute force attack and social engineering attack and introduce an enhanced model as a solution to an open problem that also overcomes the drawbacks of previously proposed honeyword generation approaches like storage cost.

Key Words: Honeywords,Authentication,security, password

1. INTRODUCTION

1.1. 1.1 Background

Businesses should seed their password databases with fake passwords and then monitor all login attempts for use of those credentials to detect if hackers have stolen stored user information[2]. That's the thinking behind the "honeywords" concept first proposed in "Honeywords: Making Password-Cracking Detectable," a paper written by Ari Juels, chief scientist at security firm RSA, and MIT professor Ronald L. Rivest, who co-invented the RSA algorithm[2].

The term "honeywords" is a play on "honeypot," which in the information security really refers to creating fake servers and then learning how attackers attempt to exploit them in effect, using them to help detect more widespread intrusions inside a network.[1] "Honeywords are a simple but clever idea," said Bruce Schneier. "Seed password files with dummy entries that will trigger an alarm when used. That way a site can know when a hacker is trying to decrypt the password file."The honeywords concept is also elegant because any attacker who's able to steal a copy of a password database won't know if the information it contains is real or fake. An adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeyword[2]. The proposed mechanism can distinguish the user password from honeywords for the login routine and will redirect user to decoy data.

1.2. Motivation

Real passwords are often weak and easily guessed; either by sharing passwords, using names of loved ones, dictionary words, and brute force attacks. Motivation towards this project is to prevent the attacks and keep the adversaries away from the user accounts. Theft of password hash files are increasing. Therefore, this technique will give a break to hackers. Adversary compromises systems, steal password hashes, and cracks the hash. Adversary makes changes in the hash files, or misuse with the user accounts, eaves dropping and many more. Adversary succeeds in impersonating legitimate user and login.

1.3. Problem Definition:

Recently, Juels and Rivest proposed honeywords (decoy passwords) to detect attacks against hashed password databases. For each user account, the legitimate password is stored with several honeywords in order to sense impersonation. If honeywords are selected properly, a cyber-attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honeyword for any account. Moreover, entering with a honeyword to login will trigger an alarm notifying the administrator about a password file breach. At the expense of increasing the storage requirement by 20 times, the authors introduce a simple and effective solution to the detection of password file disclosure events. In this study, we scrutinize the honeyword system and present some remarks to highlight possible weak points. Also, we suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honeyword generation method – and also to reduce storage cost of the honeyword scheme..

1.4. Objective

Objective for this project is listed below:

- Monitoring data access patterns where system will generate honeywords to keep user data secure.
- Decoy data will be stored in the database, alongside the users real data also serve as sensors to detect illegitimate access or exposure is suspected.

- To validate the alerts issued by the anomaly detector that monitors user access behavior.
- Launch a disinformation attack by returning large amounts of decoy information to the attacker.

1.5. Proposed Solution

1. alphabets replaced by alphabets
2. digits replaced by digits
3. special character replaced by special characters
4. After producing this, the output of this should get stored in hashed password file with 19 honeywords+original password.
5. (Hashing used - SHA-256)
6. For wrong entry of password three times will give login as decoy user(Downloads dummy data).

1.6. Summary

In this chapter, an overview of the problem definition along with solution that work contained in this dissertation is provided. In the next chapter, Literature Survey is presented.

2. Literature Survey

Irjet Template sample paragraph .Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

2.2. The Science of guessing: analyzing an anonymized corpus of 70 million passwords

Authors: Joseph Bonneau 2012

This paper describes the evaluation of large password data sets by collecting a massive password data set legitimately and analyzing it in a mathematically rigorous manner. In previous paper, Shannon entropy and guessing entropy not worked with any realistically sized sample, therefore, they developed partial guessing metrics including a new variant of guesswork parameterized by an attacker's desired success rate. In their study most troublesome is how little password distributions seem to vary, with all populations of users.

2.3. A Large-Scale Study of Web Password Habits

Authors: Dinei Florencio and Cormac Herley

This paper describes the study of password used and password reused habits. They measured average number of passwords and average number of accounts each user has, as well as measured number of times user enters password per day. They calculated this data and estimated password strength, password vary by site and number of times user forgotten password. In their findings, it showed users choose weak password; they measured exactly how weak. They measured number of distinct passwords used by a client vs. age of client in days also, number of sites per password vs. age of client in days. They also analyzed password strength. We are able to estimate the number of accounts that users maintain the number of passwords they type per day, and the percent of phishing victims in the overall population.

2.4. An In-Depth Analysis of Spam and Spammers

Authors: DhinaharanNagamalai, Beatrice Cynthia Dhinakaran and Jae Kwang Lee

This paper describes the characteristics of spam and technology used by spammers. They observed that spammers use software tools to send spam with attachment. To track and represent the characteristics of spam and spammers they setup a spam trap in their mail server. The paper is discussed in two types i.e. first type spam with attachment and second type is spam without attachment. They concluded, for spam without attachment, senders use non sophisticated methods but for spam with attachment, senders use sophisticated software to spam end users.

2.5. Examination of a New Defense Mechanism: Honeywords

Authors: ZiyaAlperGenc, SuleymanKardas and Mehmet SabirKiraz

This paper describes hash passwords are used to improve security. For user authentication false passwords are added in hashed password file i.e. honeywords. They analyzed the honeyword system according to both functionality and the security perspective. They also elaborated how the system will respond to six password related attacks. Improvements for honeywords is described briefly i.e. number of honeywords, typo-safe honeyword generation and old passwords problem. Assumptions are illustrated to an active attack against honeyword system. They concluded that honeyword system is the powerful defense mechanism where an adversary steals the file of password hashes and inverts most or many of the hashes.

2.6. Explicit Authentication Response Considered Harmful

Authors: Lianying Zhao and Mohammad Mannan

This paper describes technology called Uvauth to hide authentication results from attackers to mitigate the risk of online password guessing. They propose the use of adapted distorted image as a computer-cipher/human-decipher channel to communicate short messages in human-machine interaction. The authors have discussed Uvauth and CAPTCHA for selfevidence of authentication that may make the scheme feasible. They have also elaborated possible attacks from attacker's perspective and some of them are limitations to current design. Limitations are they have not evaluated the server side load for generating and running a large number of fake sessions. They also have not tested how effectively users can detect implicit results from an authentication attempt, or whether messages via adapted distorted images can be used in practice.

2.7. Honeywords: Making Passwords Cracking Detectable

Authors: Ari Juels and Ronald L. Rivest

This paper describes honeywords technology to improve security level for authenticating fake users. The authors have also described briefly attacks on different scenarios, but have focused on stolen files of password hashes scenario. They have described various types of attacks on honeyword system that shows how it will manage and overcome it. The attacks are, namely, general password guessing, targeted password guessing, attacking the honeychecker, likelihood attack, DOS attack and multiple systems.The study shows to limit the impact of a DOS attack against chaffing-by-tweaking, one possible approach is to select a relatively small set of honeywords randomly from a larger class of possible sweetwords.

2.8. Kamouflage: Loss-Resistant Password Management

Authors: HristoBojinov, ElieBursztein, Xavier Boyen, and Dan Boneh

This paper describes kamouflage-based password manager a new technique to prevent theft-resistant. The study states to use salts and slow hash functions to slow down a dictionary attack on the master password but unfortunately these methods do not prevent dictionary attacks. Authors states the main difficulties to overcome to make kamouflage work are, human-memorable passwords, related passwords, relation to master password and site restrictions. The authors have done with a survey that shows how users choose passwords. Authors have also described threat model, decoy set generation and fingerprinting. They ended with the conclusion stating kamouflage and fingerprinting technique provides security at high level.

2.9. Passwords and Perceptions

Authors: Gilbert Notoatmodjo and Clark Thomborson

This paper describes users' perspective to their accounts and passwords. Authors described three main categories of attacks are, namely, attacks on the system end, attacks on the communication channel and attacks on the user end.

Summary

In this chapter, background and related work about password security, methods to protect them are described. In the next chapter, Proposed Solution is presented.

3: Problem Definition

Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attacker's capabilities to perform password cracking. An attacker steals a file of hashed passwords. To detect attacks against hashed password databases honeywords technology has been proposed. Honeywords means decoy passwords. Honeywords are used to detect attacks secured on hashed password databases. For each user account, real password is stored with several honeywords (required honeywords should be chosen properly), so that attacker who steals a file of hashed passwords should get confuse with the actual passwords and honeywords. Every user account will have three attempts to login, if not then invalid activity will be stored in log.

If any unknown/unauthorized attacker tries to access system or any individual data, then we need a smart system which can automatically identify such access and confirm the genuineness of the system/user.

A. *Proposed Solution*

- alphabets replaced by alphabets
- digits replaced by digits
- special character replaced by special characters
- After producing this, the output of this should get stored in hashed password file with 19 honeywords+original password.
- (Hashing used - SHA-256)
- For wrong entry of password three times will give login as decoy user(Downloads dummy data).
- User behaviour tracking based on ip address and download and upload pattern

B. If found invalid by behaviour tracking then logout.

4. Design Methodology

A. *Methodology*

The methodology proposed in this research work is based on Honeyword Generation Method/Algorithm using Honeychecker.

The above mentioned work is divided into various modules as follows:

1) Registration
2) Login

3) Hacker
4) File upload and view
5) Admin Login
6) Decoy file upload
7) Log creation
8) Valid user behavior tracking
9) User behavior analysis

The proposed architectural diagram is as follows:

B. Module-wise work breakdown

Registration: Here user is registered into system. At the time of registration, entering password, system will generate honeywords and their hash values and store into database. Along with hash values the real password's hash is also store at specific random position. User will get one key for uploaded file encryption and decryption.

Login: Here user is going to log in to the system. If password matches with the hash password, user is authenticated.

Hacker: Here hacker is loginto the system. If hacker tries to break the system and enters any honeyword then the alert is given to the Actual user. And if suppose he try combination of password and it goes more than three attempt and also entered password does not match with the honeywords then he get access the file but all files are decoy files.

File Upload and View: Authenticated user to the system can upload file into the System. And the uploaded file is encrypted by the encryption algorithm by the user encryption key. To view fie or download file user has to enter the decryption.

Admin Login: Here admin is loginto the system. Admin has the privileges to control over the mechanism. Admin has the authorization to maintain the user accounts.

Decoy File Upload: Here admin can add the decoy file of the uploaded file. If unauthorized user tries to attempt log in and fails to succeed three attempts, then he/she can get access to files but those fileswill bedecoy files.

Log Creation: Log creation is done for each user action to the system and which is store into the database.

Valid User Behavior Tracking: After user login, the system will track the user operations and track IP Address, MAC address and data size of resources downloaded by each user per session.

User Behavior Analysis: The parameters tracked above will be analyzed using similarity vector analysis to identify behavior of each user. If invalid detected, the user will be delivered decoy data for all downloads.

5. EXPECTED OUTCOMES

The research focuses on honeywords generation, i.e. the user passwords stored with sweetwords in hashed file and storing in random position as an encrypted file. User gets a key when account is created.

The users can use this key to encrypt/decrypt the files to view the files through their accounts.

Expected activities to be carried are as follows:

1) Authentication is done through log in to account
2) Create honeywords of saved password in database
3) Check whether the user is genuine or not, if yes
a) File upload/download rights
b) Can use key to encrypt/decrypt rights
4) If no, the hacker/spammer will beredirected to decoy data environment.

Honeyword Alphanumeric Algorithm

Steps:

1. Take input password
2. Take each character from that password string.
3. For each character
4. Check whether it is number, alphabet or symbol.
5. If it is number generate random number 48 to 57.
6. Then convert this ascii value to character and add it to new honeyword.
7. If it is alphabet.
8. Check whether it is in lowercase or uppercase.
9. If it is lowercase then generate random number between 97 to 122.
10. If it is uppercase then generate random number between 65 to 91.
11. If it is symbol
12. Then replace that symbol from list of all symbols.

Repeat steps 3 to 12 for 20 times

REFERENCES

[1] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-resistant Password Management," in Computer Security– ESORICS 2010. Springer, 2010, pp. 286–302.

[2] A. Juels and R. L. Rivest, "Honeywords: Making Password-cracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications

Security, ser. CCS ’13. New York, NY, USA: ACM, 2013, pp. 145–160. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516671

[3] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 538–552.

[4] L. Zhao and M. Mannan, “Explicit Authentication Response Considered Harmful,” in Proceedings of the 2013 Workshop on New Security Paradigms Workshop–NSPW ’13. New York, NY, USA: ACM, 2013, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/2535813.2535822

[5] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, “Guess again (and again and again): Measuring Password Strength by Simulating Password-cracking Algorithms,” in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523–537.

[6] J. Bonneau and S. Preibusch, “The Password Thicket: Technical and Market Failures in Human Authentication on the Web,” in WEIS, 2010.

[7] G. Notoatmodjo and C. Thomborson, “Passwords and Perceptions,” in Proceedings of the Seventh Australasian Conference on Information Security–AISC 2009. Australian Computer Society, Inc., 2009, pp. 71–78.

[8] D. Florencio and C. Herley, “A Large-scale Study of Web Pass-word Habits,” in Proceedings of the 16th international conference on World Wide Web. ACM Press, 2007, pp. 657–666.

[9] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password Cracking Using Probabilistic Context-Free Grammars,” in Security and Privacy, 30th IEEE Symposium on. IEEE, 2009, pp. 391–405.

[10] D. Malone and K. Maher, “Investigating the Distribution of Password Choices,” in Proceedings of the 21st International Conference on World Wide Web, ser. WWW ’12. New York, NY, USA: ACM, 2012, pp. 301–310. [Online]. Available: http://doi.acm.org/10.1145/2187836.2187878

[11] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using Hard AI Problems for Security,” in Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques–EUROCRYPT’03, ser. Lecture Notes in Computer Science, vol. 2656. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 294–311.

BIOGRAPHIES

Ms. Manisha Bhole B.E Computer, 2010 Mumbai University.

1. **Presented paper at National Conference Organized by Indira Gandhi College Of Science And Commerce on “Review on Cellular Wireless Communication: 5G”.On 21st&22ndDec 2013.**
2. **Presented paper at National Conference Organized by Indira Gandhi College of Science And Commerce on “Review on Data Warehousing andMining”. On 21 st Dec 2012.**