Password Cracking Detection System with Honeyword

Florita Sylvester Tuscano
M.E Student, Department of Computer Engineering,
L.T.C.O.E, New Mumbai

Abstract— Honeywords are the decoy words also known as potential password for a user which, when an attacker enters in the system, it is detected by the honeychecker. Honeyword is a technique that can be successfully used as a guard strategy which can be utilized against stolen secret key records. This technique is honed by putting bogus patterns of passwords inside the record that consist of passwords of authentication server to deceive adversary. Honeywords resemble ordinary, user-selected passwords. Various different password patterns make it troublesome for the attacker that steal a honeyword-laced password file to recognize the true user password and honeyword. ("Honey" is an old term for decoy resources in computing environments). In existing system honeywords (decoy passwords) are used to detect malicious attempter against hashed password database. While considering every single accessible record, the legitimate passwords are stored along with various patterns and different combinations of honeywords in order sense impersonation. While considering runtime scenario, a cyber-attacker hacked the file consisting of hashed passwords, but the attacker cannot make out whether the password that is available is authentic password or the honeyword any specific account. If the attacker tries to enter the dummy (honeyword) credentials, then an alarm will be triggered and that will notify the administrator regarding password file breach. Considering the present scenario of the expenses on the storage requirement for expanding the capacity prerequisite by ample amount, this technique is easy to adopt and implement efficiently to encounter the issues of password file disclosure events.
The aim of this research is to study honeyword generation system and techniques and compare the sub tasks using the literatures published in those areas finding out the research gaps in them and to analyses them to make password more secure using security hybrid generation method using triple hashing technique as perfectly flat honeyword gene ration method. The second aim is to make honeywords more realistic to trap adversary easily.

Keywords— *Honeyword, Attack, Password Salting, Hash function, Decoy Access*

*****

I. INTRODUCTION

Basically, any password is stored in encrypted form or in salted and hashed manner in database. All legitimate user details are stored in database file along with its respected password. While storing password there is facility to store password in more secure form. Still in many cases adversary can take over such accounts and hack internal information and required data. Adversary can misuse personal data and there are many examples of such cases. Many famous and most secure web sites are targeted previously like Yahoo, Indian Defense Website, etc. To make such adversary preventable there are many methods.

Honeyword generation methods divided into two groups and they are as follows:

1) The first category consists of legacy- UI (User Interface) procedure
2) The second category includes modified-UI whose password-change UI is modified for complex and better honeyword password generation.

Honeyword Generation Methods:

A. Chaffing-by-tweaking

The user password seeds the generator algorithm which tweaks selected character position of the real password to produce the honeywords. For instance, each character of a user password in predetermined position is replaced by a randomly chosen character of the same type:

Digits are replaced by digits,

Letters by letters

And special characters by special characters.

B. Chaffing-with-a-password-model

The generator algorithm takes the password from the user and relying on a probabilistic model of real passwords it produces the honeywords. In this technique password is spitted into characters set.

For instance,
Test1demos is decomposed as 4-letters+1-digit+5-latters => L4+D1+L5 and replaced with the same composition like gold5rings

C. Chaffin-with "Tough Nuts"

The system intentionally injects some special honeywords, named as tough nuts, such that inverting hash values of those words are computationally infeasible,
Example- Fixed length random bit strings should be set as the hash value of honeyword.
Nut would be like ''9,50PEe[KV.0?RIOtcL-:IJ"b+Wol¡*]!NWT/pb'.It is stated that number and

positions of tough nuts are selected randomly. By means of this, it is expected that the adversary cannot seize whole sweetword set and some sweetwords will be blank for attacker, thereby deterring the adversary to realize her attacker. It is discussed that in such a situation that adversary may pause before attempting login with cracked passwords.

1: procedure gen(k)

2: k ← k + ’9,50PEe[KV.0?RIOtcL-:IJ”b+Wol¡*]!NWT/pb’ adds tough salt to password

3: return k

4: end procedure

Comparative study- It adds certain random salted password with each honeyword. That named as nut which makes password inversion tough that is tough nut method

D. Hybrid Method

It is like combining the strength of different honeyword generation methods,

Example-Chaffing-with-a-password-model and chaffing-with-tweaking digits. By using this technique, random password model will yield seeds for tweaking-digits to generate honeywords.

II. LITERATURE SURVEY

Simple method for improving the security of hashed passwords: the maintenance of additional “honeywords” (false passwords) associated with each user’s account. 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. The attempted use of a honeyword for login sets off an alarm. An auxiliary server (the “honeychecker”) can distinguish the user password from honeywords for the login routine, and will set off an alarm if a honeyword is submitted. [1] A system model of the risks associated with password-based authentication is presented from a user centric point of view including the construct of user password memory aids. When confronted with too much data to remember, users will develop memory aids to assist them in the task of remembering important pieces of information. These user password memory aids form a bridge between otherwise unconnected systems and have an effect on system level security across multiple systems interconnected by the user. A preliminary analysis of the implications of this user centric interconnection of security models is presented. [2] It creates the situation where attacker attacks on wrong target meanwhile it gathers useful information of attacker for real user to detect actual attacker’s identity. Honeypots and similar sorts of decoys represent only the most rudimentary use of deception in protection of information system. [4] PolyPasswordHasher Honeypots are an indispensable tool for network and system security as well as for computer forensic investigations. They can be helpful for detecting possible intrusions, as well as for gathering information about their source, attack patterns, final target and purpose. Highly interactive honeypots are probably the most useful and enlightening ones, since they reveal much information about intruders’ behavior and skills, even though the implementation and setup of such tools might require considerable efforts and computational resources. Accordingly, they present architecture for highly interactive honeypots aiming at detecting password-cracking attacks by means of Honeywords and leveraging container-based virtualization to provide persistent sessions needed to capture attacker activities. [3] For Server stored password hashes, which were generated using special password-hashing functions, to slow down guessing attacks. The most frequently used functions of this type are PBKDF2, Bcrypt and Scrypt. [5] Password security is a major issue for any authenticating process and different researches in past have proposed different techniques like hashing, salting, honeywords to make the process most secured. [6] allows to add salt with hash with additional crash list generation formed by differential masking process.

III. PROPOSED SYSTEM

The purpose of design system is to make passwords more strong to make them difficult to get decrypted at attacker site. Here Hybrid Honeyword Generation method which includes tough nut technique is used to generate Honeywords on users entered personal details and all other passwords stored on database. Once the user enters his personal details to register on site, all the data get stored in database along with its password which will be used by our system to generate the honeyword. Using Hybrid Honeyword Generation method multiple honeywords are generated. In hybrid generation method it uses user entered details to generate multiple honeywords for single user which will make all honeywords more realistic. So attacker may get misguide or confuse because all honeywords look like same and relevant to users actual entered detail. In proposed system we are going to implement such encryption to password which will be difficult to attacker to inverse. Meanwhile, to generate Honeywords it uses following algorithms to make honeyword harder to crack for attacker.

SHA 512- The system will take a password (or honeyword) and apply SHA 512 algorithm to generate a single hashed password.

BCRYPT- To build a more secure password and for good strength of honeyword, a Bcrypt algorithm can be used. It

also utilizes Blowfish algorithm to improve the security further. In Bcrypt, hashing is increased by one more level and it became double hashing.

SCRYPT- It is introduced to make the system harder to crack by attacker. Such encrypted passwords will be difficult tasks for the attackers and almost impossible to invert and crack the system.

3.1 UI Based Pages

UI based approach says that being form are mandatory to implement this type of honeyword generation method. Some are mandatory to fill through which system will acquire required data which will be used to generate realistic honeywords.

3.1.1 Registration Form

It contains maximum fields which are needed to generate honeywords as system uses those fields in Honeywords. Maximum fields are used in honeyword generation method. It is simple as very important form for honeyword generation. Once registration is done all user personal data goes to generate honeyword generation system where all algorithms are applied on same details and secured password list get generated.

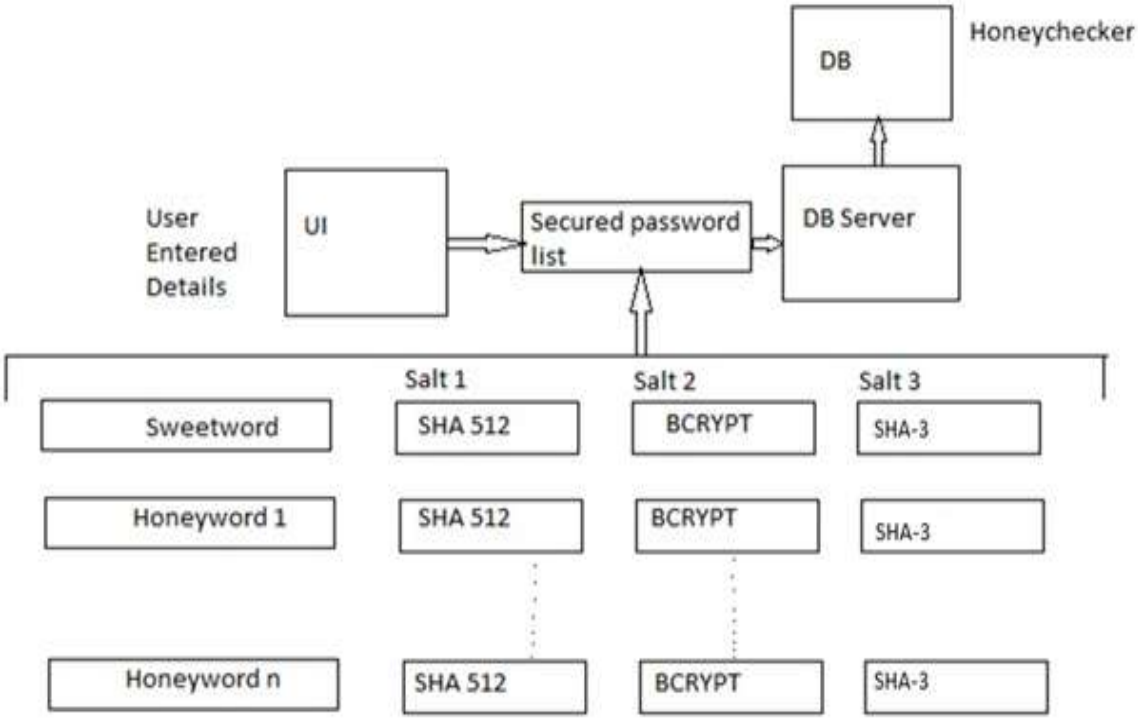

Figure 1: Architecture of System

3.1.2 Login Page

It is used to get access of respected site. If the user is legitimate then he will get direct access to real account. And if password file is already stolen then attacker will try to get access of that account by applying wrong passwords will could be from honeyword list.

3.1.3 Forget Password

Once suspicious access is started admin will notify real user to change password with message that someone is trying to login from your credentials.

IV. EXPECTED RESULTS

Proposed system is 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. Such Honeywords will lure the cracker to attempt frequently Honeywords which are realistic to Sugerword. Lured cracker gets trapped and alarm will buzz the real user. Using 'Tough Nuts' method normal honeyword generation is done which is included into Hybrid generation method. After applying triple hashing on honeyword it makes honeyword harder to crack. If in case attacker get database password file, then also it will be near to impossible to revert into its plaintext password.

The system finally will achieve the security by the following

1. Honeywords generated using hybrid method.

2. Three times hashing is applied to honeyword which makes it strong enough to make it impossible for attacker to revert its original form.

REFERENCES

[1] S A. Juels, R. L. Rivets, "Honeywords: Making Password-Cracking Detectable", IEEE International Conference on Computer, Communication and Control (IC4-2013).

[2] Art Conklin, Glenn Dietrich, Diane Walz, "Password-Based Authentication: A System Perspective", 37th IEEE Hawaii International Conference on System Sciences, 2004.

[3] Luigi Catuogno, Aniello Castiglione, Francesco Palmieri, "A honeypot system with honeyword-driven fake interactive sessions", IEEE International Conference on High Performance Computing & Simulation (HPCS),2015.

[4] Fred Cohen, "The Use of Deception Techniques: Honeypots and Decoys", University of New Haven, Handbook of information security: Threats, Vulnerabilities, Prevention, Detection, and management, Volume 3, Pg-09-15.

[5] Friedrich Wiemer, Ralf Zimmermann, "High-speed implementation of bcrypt password search using special-purpose hardware", IEEE International Conference on ReConFigurable Computing and FPGAs (ReConFig14), 2014.

[6] Seema Kharod, Nidhi Sharma, Alok Sharma, "An improved hashing based password security scheme using salting and differential masking", 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015.