Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

Creating secure and dependable honey words to increase password security.

Ch V Sailaja[1], Dr. B. Tirapathi Reddy[2]
[1]M. Tech Student, Department of CSE (Cyber Security and digital Forensics), Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, sailajac99529@gmail.com
[2]AssociateProfessor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, tirapathireddyb@kluniversity.in

Abstract: Criminals have steadily used the internet to study, support, and perpetrate illegal activity in last few decades. Obtaining pertinent information about criminals in a timely manner is one of the substantial important ways that enforcement of the law can combat this expanding trend. The challenge gaining access to any device a criminal uses that are required authentication through the internet is a major impediment to this password. When generating passwords, password guessing techniques usually take into account typical user activity as well in addition to the password policy in place. When applied to a large/average population, such strategies may have a moderate success rate. When focusing on a single goal, however, they often fail – exceptionally when the latter is an educated consumer taking precautions as an agonizing criminal would. Law enforcement is constantly using open gather intelligence sources valuable information about a criminal, but nothing is being done to incorporate this data into password cracking in an automated way. The aim of this design is to look at the techniques that allow for the gathering of critical information about a suspect and to figure out how to utilize that Password guessing techniques contain information.

Keywords: Law Enforcement, Password Guessing, Password Policy and Password Cracking.

I. Introduction

The operate of the popularity of the cyberspace has skyrocketed in recent years, and it has become one of the most common means of communication among the general public.[1] The internet is now the primary means of communication, and data protection over the internet can be accomplished by data authentication, authorization, and encryption. The registration to the website is the first step in achieving good communication corresponding web page. The user's personal and financial information is recorded at the time of registration, and a password is one of the most significant measures in protecting the user's confidential information. [2] Passwords are used in a variety of areas, including banking, e-commerce, and online transactions. During the authorization process, all of the user's data, such as their email address and banking information, are checked by means of their respective websites In order to maintain confidentiality, all of the user's information is stored in a database.[3]
.
Password protection is currently a serious issue, but there is no acceptable metric for evaluating passwords. As a result, the main The purpose of this paper is to include a security time period for a user's password in an online system, enabling the user to before changing the password the security period expires, preventing[4] the perpetrator from identifying the password correctly. Based on the guessing entropy, we use the guessing chain to determine the approximate time it will take the perpetrator to correctly guess the target password. We assume the perpetrator employs a dictionary perpetrator, which is also a probability sequence, [5] with a non-ordered or ordered dictionary. Simultaneously, we examine the Rock you password dataset, which comprises approximately 32 million passwords. [6] We also assume that the password's probability of occurrence follows a long-tailed distribution in the ordered dictionary, which is arranged in descending frequency. When a unit is calculated, the table produced during pre-processing is used to convert it back into an alphabetic sequence. Experiments have shown that if the highest weight output is selected each time, the output wordlist would contain a large number of duplicates. [7] As a result, we sample the discrete distribution to determine the unit. Higher-weight candidates can be chosen with a higher likelihood, whereas lower-weight candidates can only be chosen after a large number of guesses.

II. Domain Overview:

Machine Learning is the major commonly used technique for forecasting the future or classifying data to assist people in making important decisions. Machine Learning designs are trained on examples or cases, from which they learn from past circumstances in addition evaluate historical information. As a consequence, as it trains over and over on the instance, it is able to recognise trends and make projections about the future.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

Machine learning algorithms rely heavily on data. We can generate more data by training these machine learning design with the aid of historical data. For example, Generative Adversarial Networks (GANs) are a kind of Machine Learning that grasp from previous images and uses that knowledge to generate new images. [9] This technique is also used in speech and text synthesis. As a result, Machine Learning has vastly enlarge the scope of data science applications.
Computer science, arithmetic, and statistics are all combined in Machine Learning. In order to draw inferences from data, statistics is needed. Computer science is used to implement computation, while calculus is used to create machine learning paradigm. [10]

However, merely creating models is insufficient. You must also properly refine and tune the model in order for it to produce accurate results. Optimization techniques include fine-tuning hyper parameters to achieve the best possible performance. [11]
Information is growing at an exponential rate, and in order to leverage the power of this input, Machine Learning has introduced a new dimension to the way we interpret knowledge, aided by enormous rises in computing power. Machine Learning is being used in a disparity of techniques. [12] Machine learning algorithms control the stereos you use and the requisition that are installed on them a part of your daily life.

III. Existing Work

The password has progressed into the most common form of authentication in today's world. After brute-force attack methods such as John the Ripper and Hash Cat were found to be ineffective, the study turned to password guessing. Statistical probability underpins state-of-the-art methods including the Transition Model and possibility context free grammar (PCFG). These methods prerequisite a significant amount of conjecture, which is time-consuming. In password guessing, neural networks have proved to be more peculiar and empirical than conventional approaches. A raw neural network delineation, on the other hand, is unsuitable for cross site attacks because each word processing has its own set of characteristics. Our research aims to generalise those leaked passwords and improve cross-site authentication efficiency.
We are not going to find a way to break a particular password when we talk about password guessing. We are attempting to increase the rate of matching in between the andragogy and examine sets. In password guessing, there are two types of tests. A one-site test is one in which the training and research sets are identical. A cross-site evaluation, on the other hand, is one in which the training and research sets are different. [13] As previously mentioned, all previous work can only train and create passwords using a single dataset, resulting in poor performance in cross- site tests. A cross-site attack, on the other hand, is the majority recognise way for a hacker to break into a database.

IV. Proposed System

Honey word (or fake password) based authentication is a well-known security method for protecting the original password from server-side attacks. However, there are a few fundamental problems with this detain that the security community is still concerned about. One major problem that needs more focus is achieving flatness or generating honey words that are similarly likely to the original password. [14] Despite the fact that recent studies have made significant advances, efforts to meet this flatness criterion, our research reveals that they still fall short.
First, we conducted a thorough investigation to identify the basic properties for achieving flatness in this paper. Then, in comparison to current state-of-the-art, we proposed a questionnaire-based authentication technique that can produce a substantially flatter list of honey words. Further research illustrate that the proposed methodology passes all of the other important honey word-based authentication technique evaluation requirements with flying colours.

A. Methodology Used:

An architecture diagram is a graphical representation of a collection of architectural concepts, including their values, elements, and components.

What exactly is a diagram? What are the opposed forms of architectural diagrams? The Dragon1 open EA Method makes it crystal clear: if a diagram does not depict a design, theory, or part of a principle, it is not an architecture diagram since it does not depict (a part of) the architecture.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

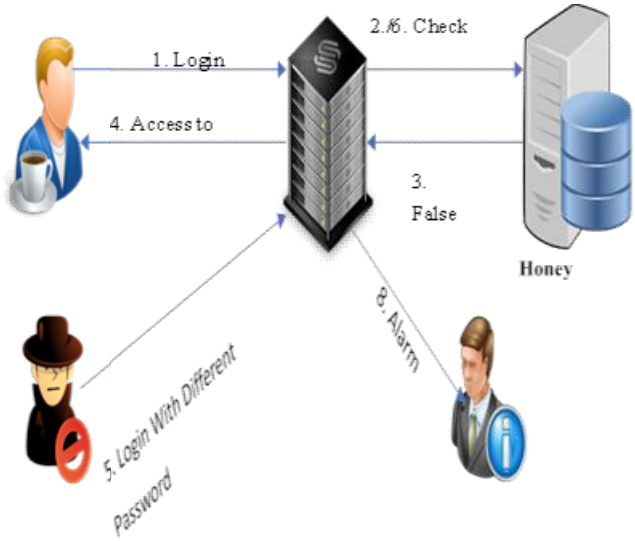

Fig 1: Architecture Diagram.

Software architecture diagrams, system architecture diagrams, device architecture diagrams, security architecture diagrams, and so on are all examples of architecture diagrams. System architects need system architecture diagrams in order to comprehend, explain, and convey ideas about the system cataloging and the user specifications that the mode must meet. It's a simple erection that can be used to help stakeholders understand the design, address changes, and clearly express intentions during the system planning process.

B. Modules:

Module 1 : Chaffing by tweaking Algorithm

Module 2 : Chaffing with a password model algorithm

Module 3 : Chaffing with ‘tough nuts’ Algorithm.

Module 1: Chaffing by tweaking Algorithm:

By “tweaking” certain characters from the user's original password, it creates false passwords. “Chaffing-by-tail-tweaking” is one of the major common variants of this form.

In this method, honey words are created by replacing each of the last t characters of pi with a random disposition of the same type: a letter is replaced by a rune, a digit is replaced by a digit, and a special character is replaced by a special character. If the pi is “Admins4 percent” and t = 3 is used, the honey words created could be “Adminw9@”, “Adminu1?”, “Adminr3*”, and so on.

Module 2: Chaffing with a password model Algorithm.

In this method, the generator algorithm takes the user's password and generates honey words using a probabilistic model of real passwords. The password is split into character sets in this model. For example, mice3blind is decomposed into four letters + one digit + five letters (L4 + D1 + L5) and replaced with gold5rings.

To begin, a password list L is created by combining a variety of real and random passwords of different lengths. Then, from the list of length d, a odd word is chosen. Furthermore, some honey words are created as "tough nuts"

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

with a probability of 0.8, which will be explained in the next section. Honey word characters are made by probabilistically removing characters from randomly selected L terms.

Module 3: Chaffing with 'tough nuts' Algorithm.

In this approach, the system injects some special honey words, dubbed tough nuts, into the system such that inverting their hash values is computationally impossible, e.g. fixed length random bit strings must be worn as a honey word's hash value. Furthermore, the number and locations of tough nuts are chosen at ra dom. The adversary will be unable to seize the entire sweet word assemblage as a reverberation of this, and some sweet words will be blank for her, preventing her from completing her assault.

V. Results

4.1 Home page of Application

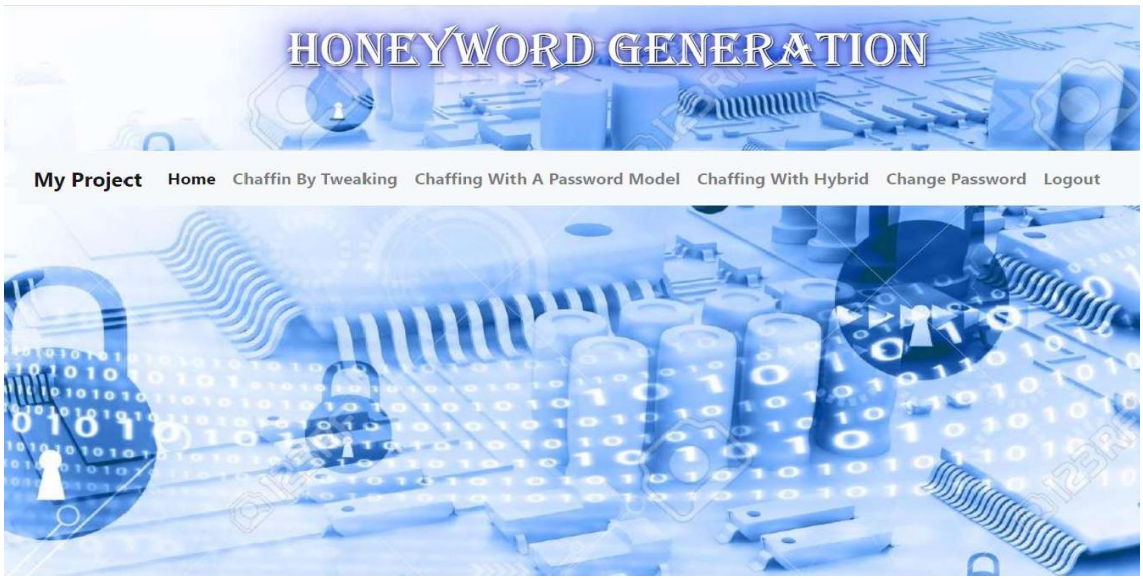

Figure 2 Home page of the generation.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

4.2 Generating password

Figure 3 Password generating.

Like this we have to generate the remaining modules these passwords will store in the honey words database.

4.3 Duplicate passwords

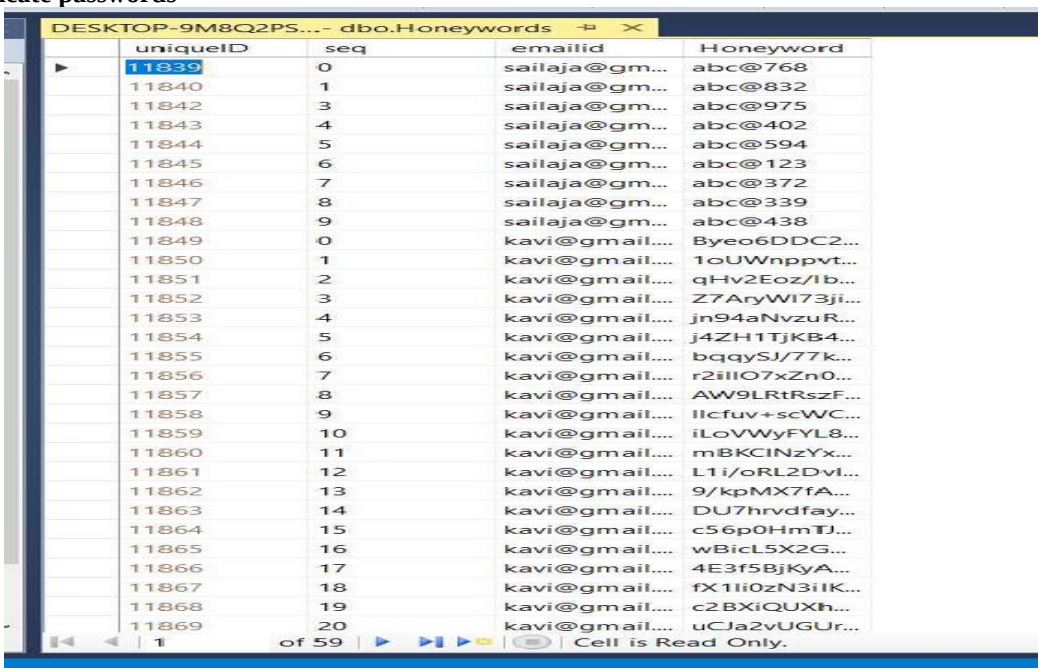

Figure 4 Creating duplicate passwords.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

In this we can see that if users create their own password then in honey word database will create duplicate passwords shown in *Figure 4*. By this the hacker can't hack user's password easily.

VI. Conclusion

Honey words are heavily used in modern research to detect password file breaches. While considerable progression has been made in developing honey word-based methods in recent years, the flatness criterion has not been satisfactorily addressed. We demonstrate from this paper that the lodge methodology overcomes majority of the key limitations of existing honey word-based authentication techniques, and, more importantly, produces a much flatter list of sweet words than the current state-of-the-art.

VII. Future Work

Any attacking methods may be used to test the flatness of honey words generation methods in the future. The user's actions in choosing passwords that are congruous with their private data is one of the important factors to consider when designing an attack (e.g. favorite band, phone number, etc.). The use of targeted guessing attacks to test the flatness of honey words generation methods would be important for future work based on the behavior.

VIII. References

[1].P.Heim.(2016,Aug.)Resettingpasswordstokeepyourfilessafe.[Online].Available:
https://blog.dropbox.com/topics/company/resettingpasswords-to-keep-your-files-safe

[2]. M. J. Schwartz. (2016, May) Linkedin breach: Worse than advertised. [Online]. Available:
https://www.bankinfosecurity.com/linkedin-breachworse-than-advertised-a- 9113

[3].R. Hackett. (2017, Oct.) Yahoo raises breach estimate to full 3 billion accounts, by far biggest known.
[Online].Available: https://blog.dropbox.com/topics/company/resetting-passwords-tokeep-your-files-safe

[4].Steve Ragan. Weebly data breach affects 43 million customers.
https://www.csoonline.com/article/3133031/security/weeblydata-breach-affects-43- million-
customers.html,Oct.2016.

[5].Richard Shay, SarangaKomanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. ACM Transactions on Information and System Security (TISSEC), 18(4):13,2016.

[6]. KristianSkraciˇc,PredragPale,andZvonkoKostanj´car.Authenti-ˇcationapproach using one-time challenge generation based on user behavior patterns captured in transactional data sets. Computers & Security, 67:107–121,2017.

[7]. NChakrabortyandSMondal,"Towards lowering the cost of storing and enhancing the security aspects of 21 honey word-based approaches," Procedia Computer Science, vol. 93, pp. 799–807, 2016.

[8]. Markus Durmuth, Fabian Angelstorf, Claude Castelluccia, Daniele Perito, and AbdelberiChaabane, "OMEN: Faster Attempting to guess a password using an ordered list Markov Enumerator," in International Symposium on Engineering Secure Software and Systems. Springer, 2015, pp. 119– 132.

[9]. Robert Hackett. Yahoo raises breach estimate to full 3 billion accounts, by far biggest known. http://fortune.com/2017/10/03/yahoobreach-mail/,Oct.2017.

[10]. Patrick Heim. Resetting passwords to keep your files

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 19588- 19594
Received 05 March 2021; Accepted 01 April 2021.

safe.https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-tokeep-your-files- safe/, August, 2016.

[11]. Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier, "Password strength: An experiential analysis," in 2010 Proceedings IEEE INFOCOM. IEEE, 2010, pp.1–9.

[12]. M. Durmuth, F. Angelstorf, C. Castelluccia, D. Perito, and A. Chaabane, ¨ "Omen: Faster Attempting to guess a password using an ordered list markov enumerator," in International Symposium on Engineering Secure Software and Systems. Springer, 2015, pp. 119– 132.

[13]. Avast.(2019,May)83%ofamericansareusingweakpasswords.[Online].Available: https://press.avast.com/83-of-americans-are-usingweak-passwords

[14]. BrilandHitaj,PaoloGasti,GiuseppeAteniese,andFernandoPerez-Cruz,"Pass GAN:Adeeplearningapproach for password guessing," in International Conference on Applied Cryptography and Network Security. Springer, 2019, pp. 217–2