A Review on Common Encryption Techniques to Brute Force Shielded Technique: Honey Encryption

Taunk Mayur[1] Laxmi Saraswat[2]
[1,2]Department of Computer Sci. and Engineering
[1,2]HJD Institute of Technical Edu. and Research Kera, Gujarat, India

Abstract— In today's era of information technology beginning from social network to most complex and secure transactions are going on the internet, when the internet technology begun it was accompanied by data threats and security breaches, then came the cryptography algorithms which were good enough to protect the treats and breaches, as the time elapsed we are in a era where straightforward mathematical cryptography techniques are not enough to secure our transactions/data on network, a new tricky technology is needed. This paper presents the straightforward algorithms and the attacks which they are vulnerable to and a review of a tricky cryptography algorithm Honey Encryption.

Key words: PBE (Password Based Encryption), Conventional Encryption Techniques, DTE (Distribution Transforming Encoders), HE (Honey Encryption), Brute Force, One-Time Pad.

I. INTRODUCTION

Cryptography is a technique which provides features such as confidentiality, authentication, non-repudiation and data integrity with techniques such as encryption, digital signatures, and hashing etc. cryptography was the conversion of information from a readable state to apparent non-sense [6]. But this concept seems to be vanished slowly as the attackers are smart enough to try the next key on non-sense information. A tricky technique of showing valid looking information is more beneficial than the some scrambled symbols like "Ŏ،£□", this technique is Honey Encryption where the information retrieved by a invalid key looks convincing to the attacker and may consider it as a valid information or on trying all the possible keys, attacker will be confused to select the valid information. Other vulnerabilities are the password selection by the users for protecting their data, users choose very weak passwords as a study conducted by Morris and Thompson examined attacks on UNIX system, A study on 3289 passwords were made and it was found that 86% of passwords were extremely weak; being too short, containing lowercase letters only, digits only or combination of the two, or being easily found in dictionaries or lists of names [3]. This paper is divided into five section where section one will describe the password selection habits of users, section two a quick review about some conventional encryption techniques which are simpler to complex and attacks they are suspectable to, section three will cover review of Honey Encryption, section four will describe Honey Encryption and section five will end up with the conclusion of this paper.

A. Password Selection Habits of Users

12345, 123456789, 1234 … are the most popular passwords selected by ordinary users. Among 32 million famously leaked passwords from a popular RockYou online service in 2009[1]. For a majority of users with many accounts online it is obvious to select a common password for all the accounts and which are very easy to remember, thus these passwords are the longstanding problem that they are easily brute forced [3]. As a study conducted average user has 6.5 passwords, each of which is shared across 3.9 different sites [3], A good password should be reasonably long, use a large character set, but still be easy to remember [5], but these password selection methods are not implemented until they are forced to be implemented, Thus users are left with the simple passwords which can be easily brute forced.

B. Conventional Encryption Techniques and attacks on them

1) Caesar Cipher

This technique uses simple substitution with alphabet [4]. That is it replaces each letter of the alphabet with the letter standing n places further down the alphabet [2].

There are only 25 keys to try; it can be easily brute forced

2) Mono Alphabetic Cipher

This technique uses arbitrary unique substitution of alphabets on key space of 26 letters.

The cipher text can be any permutation of 26 letters that is 26! Combination of key space, Thus bus using super computers this can be easily brute forced.

C. Play Fair Cipher

Use of pair of letter and substitute with 5x5 matrix designed with key and remaining alphabets [4] by following rules

1) Repeating letters falling in same pair are separated with letter 'x'
2) Letters in same rows are replaced by the letters on right
3) Letter on same column are replaced by letters beneath
4) Else letters are replaced by letter on own row and column occupied by other letter.
5) There are only 26 letters, thus there are 26x26 diagrams to be tried and the plain text will be with users.

D. DES

It is a block cipher technique where blocks of 64 bits are processed at a time with 56 bits of key and produce output of 64 bit block [7]. It consists of 16 Rounds of Feistel Structure, Left Circular Shift, Substitution 32-bit swap[4]. It was most secured method at the time of 19th century and was used in financial applications.

It is suspectable to brute force attack as there is only 56 bit length key.

E. The idea of Honey Encryption

The unbreakable cipher: One Time pad is the technique where the key length is of the same size of the plain text, other constraint involved in these techniques is that each new transmission requires a new key to be used, it produces random outputs that bear no statistical relation to the

plaintext [2]. The feature that was observed during the usage of one-time-pad, that same cipher text when decrypted with multiple keys it yield valid looking text but most of the keys fail to yield plausible plaintexts and instead correspond to random strings [1]. OTP used technique where each message of length ℓ-bit string and key with random selection of ℓ-bit length was chosen to be XORed, to computer the Cipher Text $C_i = M_i \oplus K_i$.

F. Honey Encryption (HE)

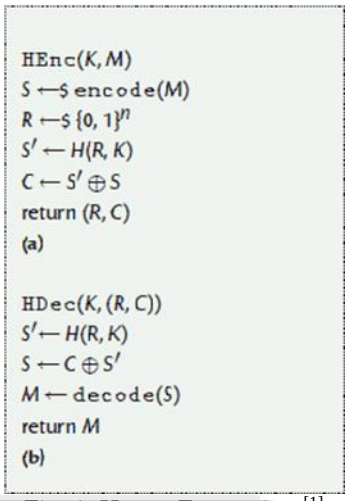

Fig. 1: Honey Encryption [1]

Honey Encryption is the technique which cannot be compromised by brute force attack which is the most possible attack on major encryption schemes. HE constructs a ciphertext which looks valid when decrypted with invalid key, it can be used to protect keys stored in wallets, it uses a specialized encoding technique and then the results are encrypted with any conventional password based scheme. This encoding technique is DTE (Distribution Transforming Encoder) and each message is encoded into seeds where each message can relate to multiple seeds. Figure 1 is the algorithm for the implementation of Honey Encryption.

G. Working

DTE encodes Messages to l-bit seed S, for example Credit Card Numbers as follows
5632125689563212 => 00,
5632125621457898 =>01,
5632125656874789 =>10,
5632125678859878 =>11,
Here all the text are valid Credit Card Numbers thus the correct Number is "5632125678859878" A DTE will encode this text to S=11 that is S=encode ("5632125678859878"). User A will now select a random number R= {0, 1}n bits and will find the Hash of R using Key K (suppose 0123) within the seed space, S'=H(R,K) (S'=11) and then computes C=S'⊕ S C=00 And will send R and C(00) to the opponent.

On receiving R and C (00) with knowledge of PBE Key (0123) opponent b computes S'=H(R,0123)=11 and then S=C⊕S'=00⊕11=11 which is equal to (5632125678859878).

While on the attacker side who doesn't have knowledge of key, Attacker may compute S'=H(R, 0012) =10 and then S=C⊕S'=11⊕10=01 which is equal to (5632125656874789).

Thus on every key attacker will get a plausible looking text which will confuse the attacker about the actual Credit Card Number, Thus even on the weakest password which are easily guessable, thought the attacker will not be assured about the text, that wether it is legitimate text or not. Thus this concept provides Security beyond the Brute-Force Bound.

II. Conclusion

In this paper we saw the trends of selecting weak passwords which can be easily breached by a brute-force attacked, we saw some conventional techniques which clearly shows how the only password based encryption (PBE) methods are vulnerable to attacks, We saw A naïve HE Attempt on study of One-Time Pad then HE with Distribution Transformation Encoders (DTE) were introduced with the example of using HE and its algorithm which provides security beyond the Brute-Force Bound.

Even though HE provides Security beyond the Brute-Fore Bound it goes thru some challenges as follows

1) Generating DTE with multiple plausible looking data is difficult as it involves complexities such as generation of plausible relative data to the original data.
2) Second Challenge is, what about the typo-safety? What if the actual user types a wrong PIN or Key, thus user may be misguided with the invalid message and may lead to issues.
3) HE works with different computer domains such as compression and human-language processing; implementing such a system would be a new task in information technology.
4) Currently it can work on Credit Card Number, PINS and RSA Keys.

References

[1] Honey Encryption, Encryption beyond the Brute-Force Barrier, IEEE Security & Privacy, July/August 2014
[2] William Stalling "Cryptography and Network Security" , Pearson Education,2009ss.
[3] A Large-Scale Study of Web Passwords Habits, Proc. WWW 2007, Banff, BC
[4] A review on symmetric key encryption techniques in cryptography, IJSETR, Volume 3, Issue 3, March 2014
[5] The memorability and security of passwords – some empirical results, Jianxin Yan, Alan Blackwell, Ross Anderson, Alasdair Grant Cambridge University Computer Laboratory
[6] https://en.wikipedia.org/wiki/ Cryptography
[7] A study of Encryption Algorithm AES, DES and RSA for Security, Global Journal of Computer Science and Technology Network, Web & Security Volume 13 15 Version 1.0 Year 2013
[8] A review paper on cryptography and significance of key Length, IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012
[9] Implementation of One-Time Pad Cryptography, K.V.O Rabh, Information Technology Journal 4(1): 87-95, 2005

