ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Improved User Authentication Using Honeywords and Hybrid Generation Algorithms

Ramesh Kumar.B [1], Archana C [2]

Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India[1]

Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India [2]

ABSTRACT: Data access control and data authentication is an efficient way to ensure the data security in the internet. Online services are providing an effective solution for sharing information's through website. This proposal initiates the study of two specific security threats on online security based password authentication in distributed systems. Honey words-based password authentication is one of the most popular security mechanisms to keep the passwords safe and secure. Recently some authors were proposed honeywords, which is also known as decoy passwords to detect attacks against hashed password databases. The individual user's password is stored with several honeywords in order to sense imitation. 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. In addition, entering with a honeyword to login will trigger an alarm notifying the administrator about a password file breach. The proposal provides a hybrid generation algorithm with secure hashing technique. And the proposed system also consists of randomization technique, which frequently changes the honeywords according to the popularity.

KEYWORDS: password security, password guessing, password cracking attack, Honey words, authentication, login

I. INTRODUCTION

Data authentication and data privacy is a major aim of all applications, and recently several companies were affected by its security violations. The affected companies are LinkedIn, Adobe and Yahoo etc [1]. The leaked passwords create much more risk and there are huge possibilities for cyber attacks [2] [3]. Current systems are protecting the data from such attacks by asking for strong password selection, dynamic OTP (One Time Password) selection and verification, Captcha based security [3][4] etc., at the server side, companies are using some hashing and cryptographic functions to secure their clients passwords. Such security function follows MD5, SHA-1 algorithms [5] without a salt value. This increases the password stealing threats. Initially, we describe and discuses about the cyber attacks and its detection strategies and finally proposed a new security architecture for secure data management. The Cyber attacks are the malicious actions, which attempt to bypass security mechanisms of server. The detection of cyber attack can be performed only after the attack made. So effective prevention system should be detected and reviewed.

Cyber attacks are classified into different types such as eves dropping, man-in-middle attack, replay attack, brute force and dictionary attack, insider attack, key logger attack, phishing attack, Shoulder surfing attack and session hijacking attack. Every attack has dealt with different type of counter measures. The following fig 1.o shows the cyber attack type and its counter measures to handle those attacks [6][7][8].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Attack Name	Description	Counter measure
Eavesdropping Attacks	Un-authorized real time interruption	a) Standard encryption `techniques such as AES 128 bit or RC4 stream cipher b) single sign-on protocol can be included with SSL c) strong authentication protocol; like Kerberos can be used
Replay Attacks	An attacker copies the message, data, user credentials or key information transmitted between two hosts and then uses it for a nefarious purpose	a) OTP can be applied b) cookie timeout settings can protect users from replay attacks
Man-in-the-Middle Attack	Attacker simply monitors the data and may be reused. This can be active or passive type.	a) Use of SSL b) HMAC (Hashed message authentication code) can be used
Phishing Attacks	The attacker impersonates or copies the personal details such as email or phone call for nefarious purpose	a) Digital certificates can be used b) Source and URL verification c) HTTPS implementation
Brute Force Attacks	A computer program or ready-made software is commonly used for implementing brute force attack to crack the passwords.	a) Tarpitting methods are used b) honeypot mechanism c) CAPTCHA (Completely Automated Public Turing test) mechanism can avoid brute force attacks
Dictionary Attack	It is an attack attempted on authentication data by trying all the possible words in a dictionary.	a) Strong password can limit dictionary attacks impact.
Insider Attack	The system administrators or network managers steal the authentication data or exchange keys.	a) Intrusion Detection System (IDS) helps to mitigate such attacks b) Access control mechanisms
Keylogger Attack	It captures the keystrokes of the user for stealing their password	a) OTP (one-time password) b) virtual keyboard
Malicious Code Attack	advanced malicious Trojans may be used to gain control over the user's computer system	a) Antivirus can protect
Session Hijacking	attacker exploits the TCP session between a Web server and a Web browser and steals the session token to gain the unauthorized access	a) SSL combined with cookie management system b) Cryptography and secure protocol can be used.

Table 1.0 types of cyber attack and its counter measures

II. PROBLEM DEFINITION

III. Honeywords:

Honeywords which is also known as decoy passwords, which are created from users passwords to detect attacks against hashed database. This honey word helps to find the impersonate attacks. There are several methods were proposed to generate honey words, this chapter gives the overview about the methods and discuss some points that can cause some security problems. The following fig 1.0 shows the sample list of honey words.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

The authors in [9] categorize the honeyword generation methods into two groups. The first category consists of the legacy-UI (user interface) procedures and the second one includes modified-UI procedures whose password-change UI is modified to allow better password/honeyword generation.

From the analysis, we find several attacks are threatens web users by performing various types of cyber attacks. While considering and protecting from these security problems, there are two main issues arises. The first one is password protection process and second one is verifying the protection mechanism became successful or not. The details of the above issues are described below.

Password Protection: The passwords must be protected by taking appropriate precautions and storing with their hash values computed through salting or some other complex mechanisms effectively. The mechanism should be hard to acquire plaintext passwords by the attacker.

Password security and countermeasures: the second part of the problem is, the system should use appropriate counter measures. For performing the counter measures, the model should have all log files and event details.

This paper focuses on the above two problems with effective security mechanisms to thwart cyber security attacks. Honeypot is one of the methods to identify password database violations. So the proposed system has been developed from the above issues.

IV. PROPOSED SYSTEM

In modern scenario, a fundamental problem the literature often says is about leveraging the secrecy of a small piece of knowledge into the ability to perform cryptographic functions which is sampled as encryption and authentication multiple times. In this research, this introduces the concept of how to make an authentication key more powerful and reliable in the sense that it allows reliable verification against different attacks in the information domain without increasing its process. This aims to create a single set solution against different security threats. The followings are the major contribution of the proposed system.

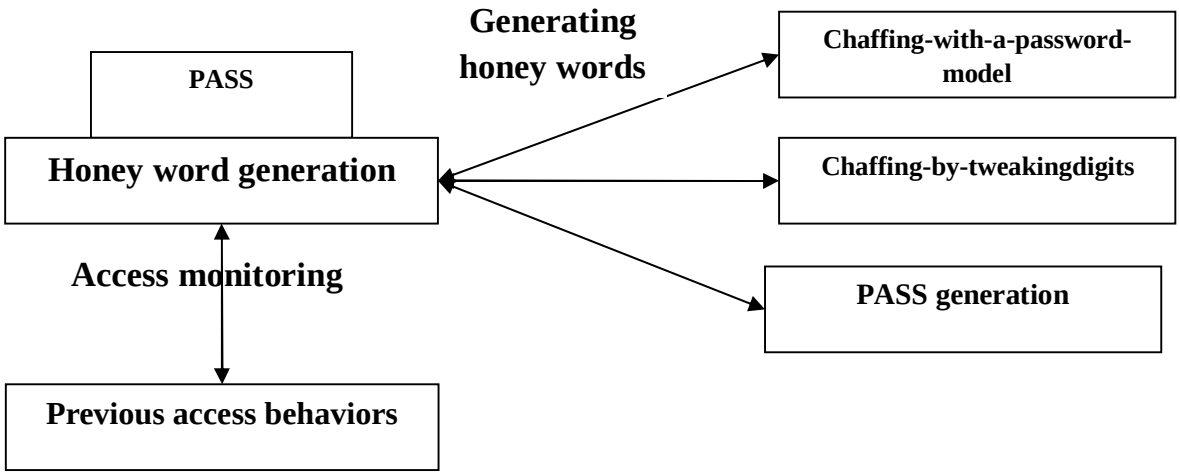

Fig 1.0 PASS framework architecture

This introduces a new authentication scheme which is named as **PASS (**Prompt Authenticated Single Session Protocol**)** technique, which creates a single session password embeds within the Honeywords and collects the keys from the user while performing authentication in a website.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Unlike the previous works, the average size and time of creating encrypted keys have been eliminated.

The proposal develops a five-step scheme for PASS implementation.

Step1: initial Honeyword set up and Honeyword generation process

Step2: single session key encryption process

Step3: Honeyword generator with respective encrypted keys

Step4: Honeyword verification

Step5: session based password verification

- The first one is initial Honey word selection, set up and Honey word generation for every user in the website. The first algorithm can generate a Honeyword using hybrid algorithm.
- The second step of the mechanism in PASS, is hash key creation with respective Honeyword using SHA-2 technique.
- The second scheme eliminates the existing key reuse problems and keylog attacks.
- The third step of the scheme is the SMS based authentication scheme, which helps to gather the encrypted keys from the device and verifies with the session details together for authentication.
- Finally this performs the session verification with the respective passwords of the user

The proposed work is the combination of the strength of different honeyword generation methods and made it as a new hybrid one, the proposed PASS framework performs chaffing-with-a-password-model and chaffing-by-tweaking digits. By using these two techniques, hybrid honey word generation model will yield seeds for tweaking-digits to generate honeywords. For example let the correct password be orange1903. Then the honeywords happy2562 and flower9137 should be produced as seeds to chaffing-by-tweakingdigits. For t = 3 and k = 4 for each seed, the sweetword table given in table 2.0 may be attained:

Table 2.0 honey word list

flower 9679	orange 1422	happy 2656
flower9757	orange **1903**	happy 2036
flower 9743	orange 1172	happy 2849
flower 9392	orange 1792	happy 2562

The paper has used C#.Net for developing the front end of this application and SQL Server for the back end. The reason for using C#.Net is its flexibility. This can add or remove any features without editing the whole code. This separated the standalone functions like user name matching and Honeyword matching in separate functions which are reused again and again. For the back end this needed a freely distributed and powerful database so SQL Server was a good choice. Whole of the games will be stored in the database.

Encrypted Honeyword:

The one-time encrypted hash key in PASS is generated by a secure one-way hash function. With a given input, the set of encrypted Honeywords is established by a hash chain through multiple hashing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

This helps to avoid the Honeyword reuse attacks in the data retrieval function on cloud storage. The next one-time encrypted has key is obtained by performing hashes Hence, the general formula and its steps is given as follows:

Steps:

1. The Honeywords is produced by performing N hashes on the input C
   a. $\delta = Hn - 1(c)$
   b. Where δ is the hash key which is derived from the input C.
2. Repeat the step 1.a until the value of 1 became i.
3. Return the hash key H.

Note that function is a hash which is irreversible in general cryptographic assumption. In practice, is realized by SHA-256 in proposed system. Therefore, the bit length of is 256.

In the *registration* phase, a user starts the program to register the new account on the website to utilize the shopping. Unlike traditional registration process the server requests for the user's unique id and phone number, instead of Honeyword. The program sets the user name and Honeyword for authentication. This secret key is used to generate a chain of one-time Honeywords for decryption key creation on the web server. Then, the program automatically sends a registration Email message to the client after completing the registration procedure.

V. RESULTS AND ANALYSIS

The proposed work is successfully implemented using C#.net. The performance of this proposed work PASS using Honeywords and new hybrid crypto scheme is compared with the existing approaches. The results prove the proposed system is outperformed than the existing techniques. This considered the hashing delay and Honeyword generation delay for deployed data on the web server in the process of authentication. Encryption and Honeyword verification and generation and verification delay are specified below.

Encryption Process	Honeyword generation time (ms)	Accuracy
Existing System	125	89
PASS	62	94

Table 2.0 compares between existing and proposed methods in the form of time and accuracy. The honey word generation delay has been compared with the existing technique. The existing system need more time to perform a 50 set Honey word generation. This is very high when comparing with our proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

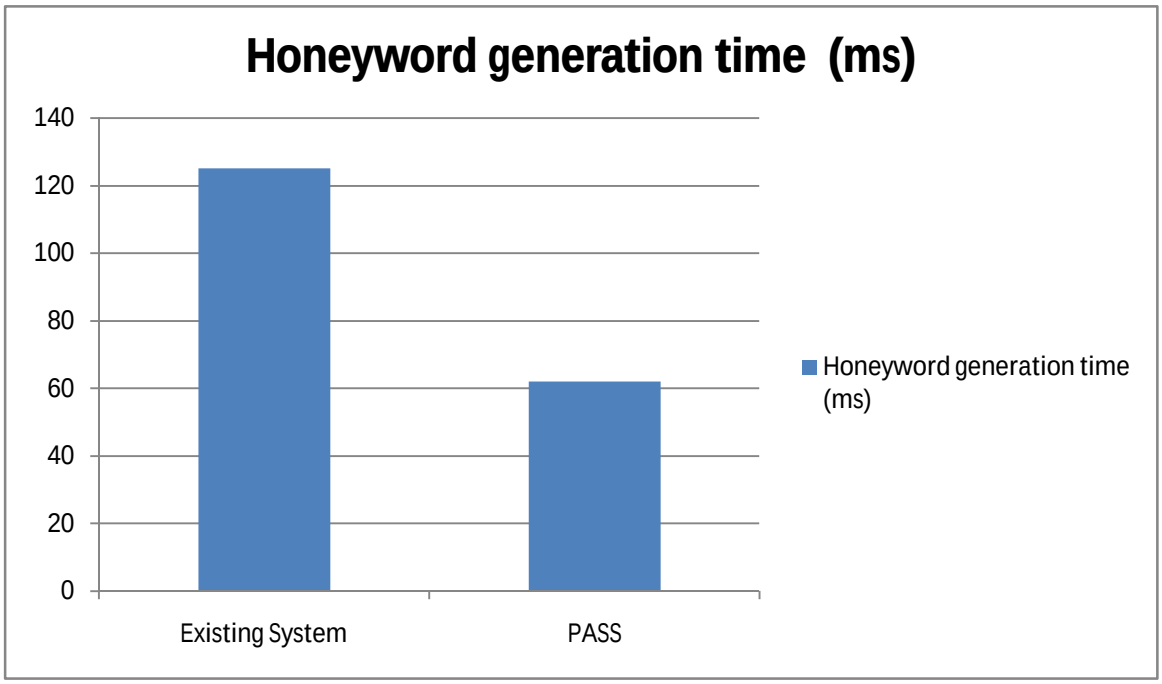

Fig 2.0 Delay Comparison Chart

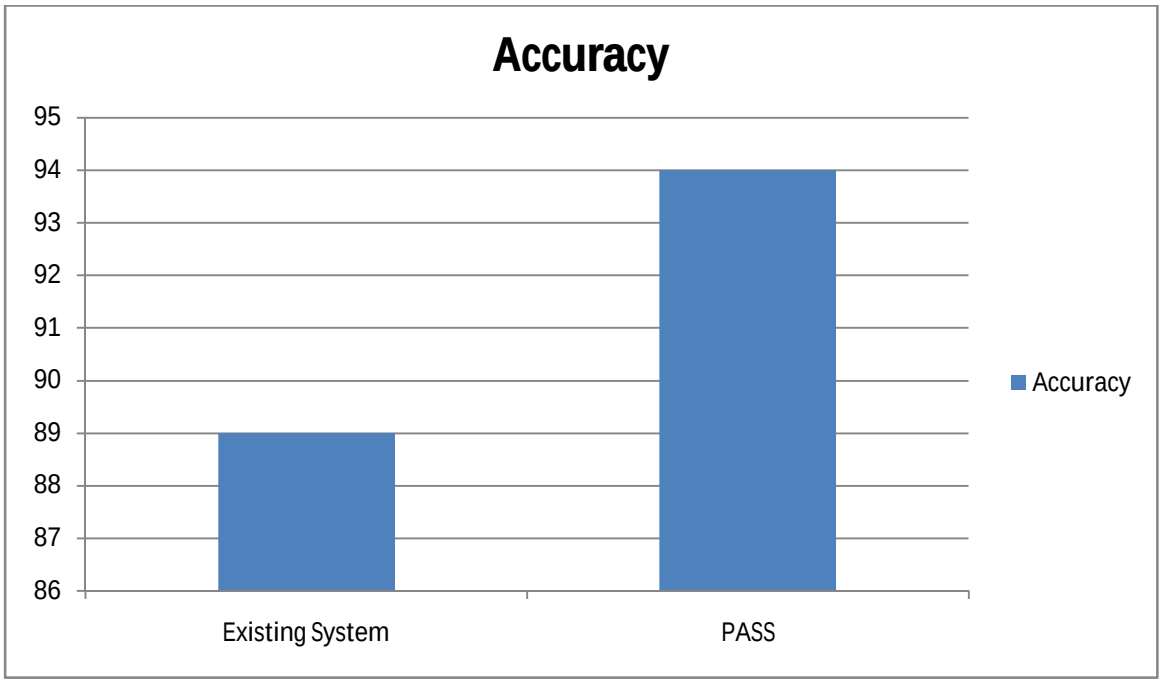

Fig 3.0 accuracy Comparison Chart

The above delay comparison chart indicates the execution time for the algorithm to produce cipher texts and corresponding keys before storing the data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

VI. CONCLUSION

The current study analyzed the security threats in the internet and introduction of the honeyword system. From the different analysis the system and addressed a number of defects that need to be handled before successful realization of the scheme. The proposed system creates strong honey word system directly depends on the hybrid generation algorithm, and it tracks the unauthenticated user by monitoring their behaviors. The system finds and proposed a new security framework named as PASS, which is a new password authentication scheme to fight against different security attacks in the real time scenario.

REFERENCES

1. D. Mirante and C. Justin, "Understanding Password Database Compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02, 2013.
2. A. Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times, vol. 20, 2010.
3. O'Shea, Kevin, and N. H. Hanover. "Cyber Attack Investigative Tools and Technologies." *HTCIA (Hanover, NH: Dartmouth College, 2003)* (2003).
4. Von Ahn, Luis, et al. "CAPTCHA: Using hard AI problems for security."*International Conference on the Theory and Applications of Cryptographic Techniques*. Springer Berlin Heidelberg, 2003.
5. Wang, Xiaoyun, et al. "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD." *IACR Cryptology ePrint Archive* 2004 (2004): 199.
6. Li, Xu, et al. "Securing smart grid: cyber attacks, countermeasures, and challenges." *IEEE Communications Magazine* 50.8 (2012): 38-45.
7. Bass, Tim, et al. "E-mail bombs and countermeasures: cyber attacks on availability and brand integrity." *IEEE network* 12.2 (1998): 10-17.
8. Gao, Zhiqiang, and Nirwan Ansari. "Tracing cyber attacks from the practical perspective." *IEEE Communications Magazine* 43.5 (2005): 123-131.
9. Erguler, Imran. "Achieving Flatness: Selecting the Honeywords from Existing User Passwords." *IEEE Transactions on Dependable and Secure Computing*13.2 (2016): 284-295.