Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

"Emerging Technologies in the Computer World", January -2017

Honeyword :Encryption Mechanism in Network Security

Prof.P.S.Gaikwad[1] , Aishwarya Sonavane[2], Jeevan Jena[3], Pushpa Varsha[4], Megha Koul[5]

[1]*Computer Department, AISSMS IOIT*
[2]*Computer Department, AISSMS IOIT*
[3]*Computer Department, AISSMS IOIT*
[4]*Computer Department, AISSMS IOIT*
[5]*Computer Department, AISSMS IOIT*

Abstract — *Banking systems always needs escalated security solutions. In tradition websites security measures are very low resulting easily hack able server systems. We are proposing a new All in One architecture that will guard our banking system from various attacks. Main security threats such as SQL injection attack, URL injection attack, cross site scripting, brute force attack. We will build a system that will prevent all these type of attacks. Every time a hacker tries to launch any of these attacks our system will generate a log into database. Hacker will be banned for a certain of time period.*

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," Jules and Rivets pointed out. "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."

Our systems will have some unique features like user's password will be stored in encrypted format as a honeyword. This honeyword is shared with admin. If hacker use honeyword directly then system will ban access of hacker. System is complete Banking solution. User can transfer money to other accounts and perform other transactions.

Keywords-*Honeyword, Honeypot, Decoy, Authentication.*

I. INTRODUCTION

In today's real time modern industrialized world security systems place a vital role. Customers' personal information stored by the bank is also considered as private and should not be disclose to anybody with no authorization. The main motto of this application is to protect our banking system from various attacks.This system ha feature like password will be stored in encrypted format as a honeyword.

Banking systems always needs escalated security solutions. In tradition websites security measures are very low resulting easily hackable server systems. We are proposing a new all in one architecture that will guard our banking system from various attacks. Main security threats such as SQL injection attack, URL injection attack, cross site scripting, brute force attack. We will build a system that will prevent all these type of attacks. Every time a hacker tries to launch any of these attacks our system will generate a log into database. Hacker will be banned for a certain time period.

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.Our systems will have some unique features like user's password will be stored in encrypted format as a honeyword.

II. RELATED WORK

Honeywords are a defense against stolen password files. Specifically, they are bogus passwords placed in the password file of an authentication server to deceive attackers. Honeywords resemble ordinary, user-selected passwords. It's hard therefore for an attacker that steals a honeyword-laced password file to distinguish between honeywords and true user passwords. "Honey" is an old term for decoy resources in computing environments. To secure the account from various attacks such as DOS, Brute Force, Cross-Site Scripting .

2.1.Denial Of Service (DOS)Attack:

In computing, a **denial-of-service** (**DoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

2.2. Brute force :

Brute force (also known as **brute force** cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using **brute force**) rather than employing intellectual strategies.

2.3. Cross-Site Scripting:

Cross-Site Scripting (**XSS**) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web **sites**. **XSS** attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side **script**, to a different end user.

III. PROPOSED TECHNIQUE

3.1.

For each user ui, a list Wi of distinct words (called "potential passwords" or more briefly,"sweetwords") is represented:
Wi =(wi,1,wi,2,...,wi,k) .
The definition of the file F is changed so that it now contains an extended entry for each user ui, of the form:
(ui,H i) ,
where
$v_i,j = H(w_i,j)$
is the value of the hash of the user's j^{th} sweetword wi,j, and
H_i =(vi,1,vi,2,...,vi,k)
is the list of all these hash values.
We let Gen(k) denote the procedure used to generate both a list Wi of length k of sweetwords for user ui and an index c(i) of the correct password pi within Wi:
(Wi, c(i)) = Gen(k).

3.2. MATHEMATICAL MODEL

S={S, s, X, Y, T, fmain, DD, NDD, ffriend, memory shared, CPUcount}

- S(system):-Is our proposed system which includes following tuple.
- s(initial state at time T):-GUI of search engine. The GUI provides space to enter a query/input for user.
- X(input to system):-Input Query. The user has to first enter the query. The query may be ambiguous or not. The query also represents what user wants to search.
- Y(output of system):-List of URLs with Snippets. User has to enter a query into search engine then search engine generates a result which contains relevant and irrelevant URL's and their snippets.
- T (No. of steps to be performed):-These are the total number of steps required to process a query and generates results.
- fmain(main algorithm) :-It contains Process P. Process P contains Input ,Output and subordinates functions. It shows how the query will be processed into different modules and how the results are generated.
- DD (deterministic data):-It contains Database data. Here we have considered users Bank Transaction data.
- NDD (non-deterministic data):- No. of input queries. In our system, user can enter numbers of queries so that we cannot judge how many queries user enters into single session. Hence, Number of Input queries are our NDD.
- ffriend :- WC And IE. In our system, WC and IE are the friend functions of the main functions. Since we will be using both the functions, both are included in ffriend function. WC is Web Crawler which is bot and IE is Information Extraction which is used for extracting information on browser.

• Memory shared:-Database. Database will store information like list of receivers, registration details and numbers of receivers. Since it is the only memory shared in our system, we have included it in the memory shared.
• CPUcount:-In our system, we require 1 CPU for server and minimum 1 CPU for client. Hence, CPUcount is 2.

IV. ARCHITECTURE

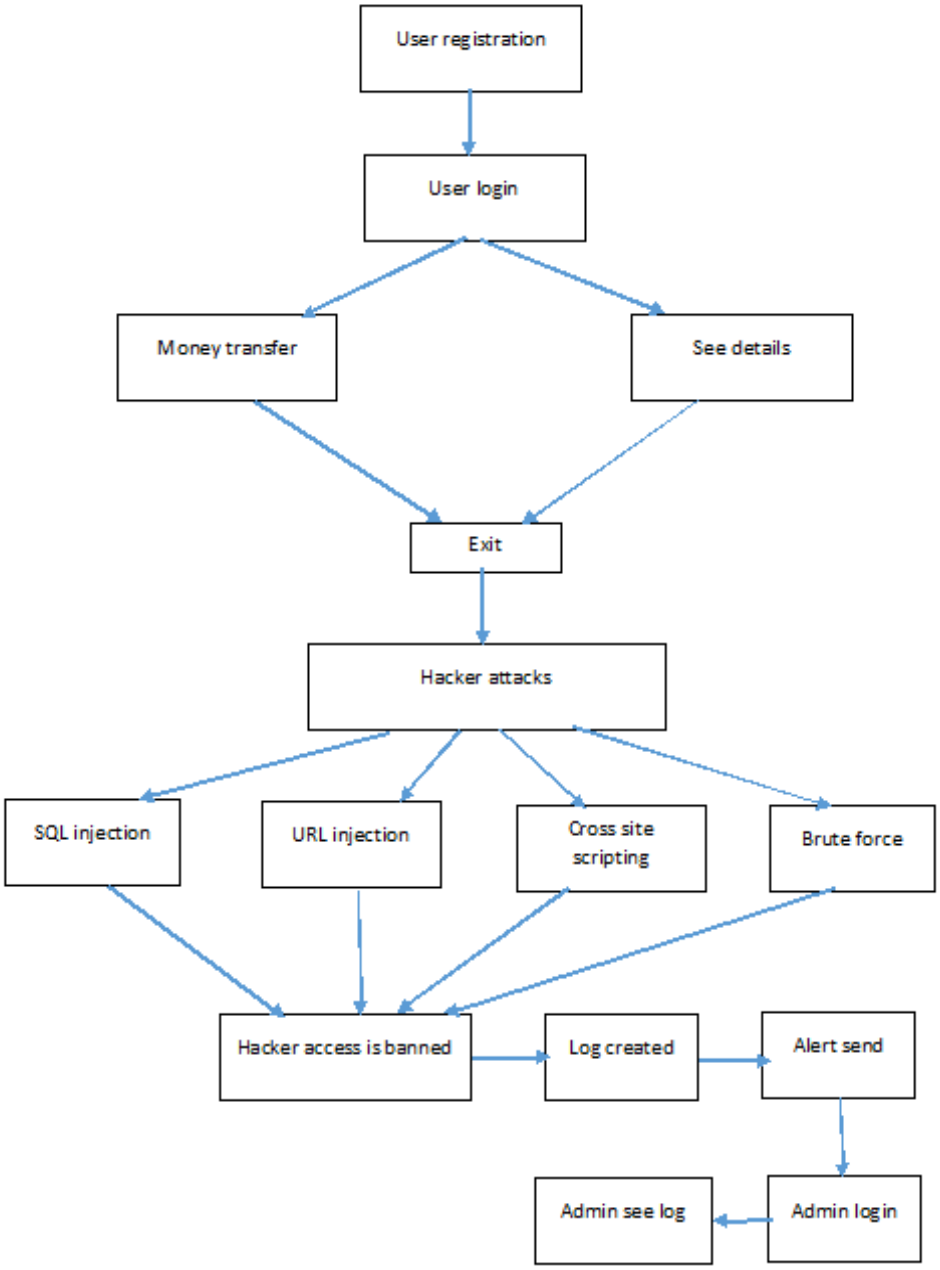

Figure 1. Architecture Diagram

V.CONCLUSION

This is a system which is to bring in a revolution in the bank security system. By making the procedure a little easy and more systematic for the bank officials. This is just a proposed model which when implemented would surely give very good protection from the hackers attack.In this system users password are saved in encrypted format as a honeyword. If hacker uses honeyword a fake account will be displayed to hacker. This system prevents unauthorized access.

VI.REFERENCES

[1] Luigi Catuogno, Aniello Castiglione, Francesco Palmieri," A Honeypot System with Honeyword-driven Fake Interactive Session", IEEE 978-1-4673-7813-0 ,45,2015

[2] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords" , IEEE Transactions on Dependable and Secure Computing 1545-5971,25, 2015

[3] Nilesh Chakraborty, Samrat Mondal "Few Notes Towards Making Honeyword System More Secure and Usable".

[4] Ziya Alper Genc*, Su¨leyman Kardas¸*,†, Mehmet Sabir Kiraz*,"Examination of a New Defense Mechanism: Honeywords".

[5] Ari Juels ,Ronald L. Rivest"Honeywords: Making Password-Cracking Detectable".

[6] Imran Erguler, TUBITAK BILGEM "Some Remarks on Honeyword Based Password-Cracking Detection.

[7] Nilesh Chakraborty, Samrat Mondal " A New Storage Optimized Honeyword Generation Approach for Enhancing Security an Usability.

[8] Prashant Dhas1, Ismail Mohammed," Efficient Approach for High Level Security Using Honeywords",IJARCSSE Volume 5 ,Issue 11 ,November 2015.

[9] Harish Reddy B, Beatrice Ssowmiya J,"Web Application:(with) Honeyword and HoneyEncryption",IJSR Volume 4 Issue 2,Februray 2015.

