HONEYWORD ENCRYPTION MECHANISM IN NETWORK SECURITY

Aishwarya Sonavane[1], Jeevan Jena[2], Pushpa Varsha[3], Megha Koul[4]
[1]Student,[2]Student,[3]Student, [4]Student
[1]Computer Engineering,
[1]All India Shri Shivaji Memorial Soc. Institute Of Information Technology, Pune,India

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 uses 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.

Index Terms— Honeyword, Honeypot, Decoy, Authentication.

I. INTRODUCTION (HEADING 1)

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 has features 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. WHAT ARE HONEYWORDS

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 .

Honeyword Generation Methods

Chaffing-by-tweaking :

Number of positions to be tweaked, denoted as t should depend on system policy.

Chaffing-by-tweaking-digits:

For the password 42hungry and t = 2, the honeywords 12hungry and 58hungry may be generated.

Chaffing-with-a-password-model :The password is splitted into character sets. For instance, mice3blind is decomposed as 4-letters + 1-digit + 5-letters ⇒ L4 +D1 +L5 and replaced with the same composition like gold5rings.

Hybrid Method:

It the combination of chaffing-with-a-password-model and chaffing-by-tweaking- digits.

III. ATTACKS

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.

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.

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.

IV. HONEYCHECKER

Honeychecer is A secure server which is used to assist with honeyword.
The system communicates with the honeychecker when a login attempt is made, or when a user changes the password.
In case of an irregularity, honeychecker is capable of raising an alarm.
Honeychecker maintains a single database value C(i) for each user Ui.
It accepts commands of exactly two types:

Set:Ci,Ui. Sets correct password index Ci for user Ui.
Check:Ui,j . Checks that C(i) = j .

V. MATHEMATICAL MODEL

S= {I, O, P,C,TC,D}
I = Input from user.
O = Output of the system.
P = Processes
P= {H, UA} where ,
H is Honeyword.
UA for User Authentication.
C= {U, MAX, TM} where,
U= User Login credentials.
MAX = {1, 2, 3, … , n}
TM is for Transfer Money.
TC = {M, G} where,
M is input which is taken from user.
G is a gateway through, TM will be sent to end user.
D = Database which contains
Number of users N,
User information Info.

VI. ARCHITECTURE

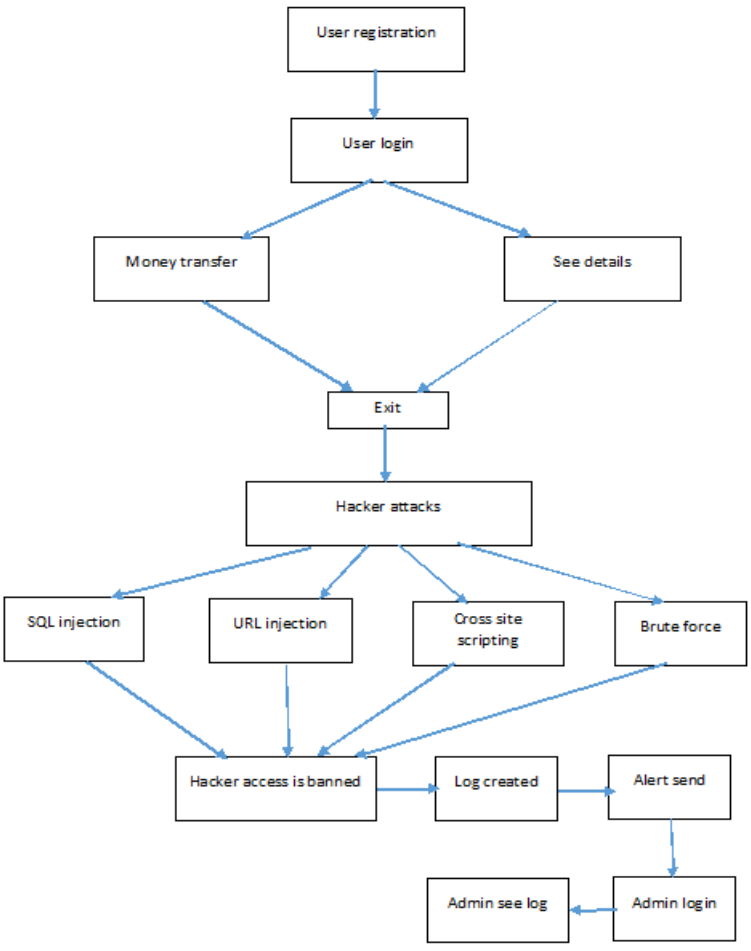

Figure 1 Architecture Diagram

VII. 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.

VIII. REFRENCES

[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.