WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Password Guessing Resistance and Data Attacker Monitoring Using Honeypot Technique

Gopi S[1], Daniel V[2]

[1,2] BSc Computer Science, Rathinam College of Arts and Science, Coimbatore -641021
[1]gopis9898@gmail.com, [2]officialemailofdaniel@gmail.com

ABSTRACT:

Online banking applications are more popular nowadays; the e-banking transactions that are now becoming the dominant form of activity. In the internet banking application, many users may perform password guessing, stealing and hacking to gain the password. Sometimes this password guessing process blocks the account of the original user. In the banking application, the unknown IP login is intimate via email. But the motive of the attacker and their complete details are not gathered and informed to the original user.

So the proposed system develops a new banking security with the ability to handle password guessing attackers by navigating them to a fake page and knows their intention of hacking. Instead of avoiding the user, the application allows the attacker to a fake page and crawls all necessary data from them. The attacker activity will be capture and the image will send to the original user. Using this, the original user can know the attacker IP address, time, location and the activity after the login in detail.

The proposed system is used ASP.net and C#.net to develop a new attacker detection technique named as honeypot, which is a trick performed to detect and trace the attacker activity in the banking application.

Keywords: ***Password Guessing Attack, Honeypot Technique, Online Banking Security, Brute Force, Web Security***

1. INTRODUCTION

In today's digital age, online banking has become an integral part of our daily lives, offering a convenient and efficient means for financial transactions. However, with this increased reliance on digital platforms comes the ever-looming threat of cyber attacks. Password guessing, stealing, and hacking attempts pose serious risks to the security of online banking applications, not only compromising user data but also leading to frustrating disruptions such as blocked accounts.

While current security measures do notify users of suspicious activities, the information provided is often limited. Users are alerted about unknown IP logins, but the crucial details surrounding the attackers' motives and comprehensive post-login activities remain obscured.This gap in information leaves users vulnerable and unaware of the potential threats they face. To address this vulnerability, our research introduces an innovative security system designed to go beyond conventional defense mechanisms. We propose a proactive approach that not only resists password guessing attempts but also monitors attackers comprehensively. Central to our solution is the integration of a honeypot technique into the online banking application, offering a simulated environment that redirects attackers to a controlled page for observation.

Unlike traditional methods that merely block unknown IP addresses, our system actively engages with potential threats. By navigating attackers to a fake page, we collect vital data, including IP addresses, login times, geographical locations, and detailed post-login activities. This comprehensive information is then compile into a user-friendly report, empowering the legitimate user with the knowledge needed to counteract potential security breaches effectively.

This paper details the development and implementation of this advanced online banking security system, utilizing the robust combination of ASP.net and C#.net. Through the incorporation of the honeypot technique, our approach provides a novel and effective means of detecting and tracing attacker activities, contributing significantly to the resilience of online banking applications against evolving security threats. Our research aims to enhance the understanding and capabilities of the online banking industry, ensuring the continued safeguarding of user information and the preservation of the integrity of financial transactions in the digital realm.

2. RELATED WORKS

Honeypot Techniques in Online Banking:

"Honeywords for Password Security and Management" (IRJET, 2020): This paper explores the concept of "honeywords," fake passwords stored alongside real passwords to detect attackers accessing stolen password databases. While not directly using honeypots, it demonstrates the potential of deception techniques for online banking security.

"Intrusion Detection Using Honeypots and Honeywords" (IJTRA, 2019): This paper explores using honeypots and honeywords within an intrusion detection system for online banking. It discusses the benefits of combining these techniques for enhanced security.

Data Capture and Analysis in Honeypot Systems:

"Password Attack Analysis Over Honeypot Using Machine Learning" (DergiPark, 2021): This paper highlights the use of machine learning algorithms to analyze data captured from honeypots, specifically focusing on password attack patterns and detection. This could be relevant to analyzing attacker behavior captured through your honeypot.

3. OBJECTIVE:

1. The login protocol should make brute-force and dictionary attacks ineffective even for adversaries with access to large botnets (i.e., capable of launching the attack from many remote hosts).
2. The protocol should not have any significant impact on usability (user convenience). For example : for legitimate users, any additional steps besides entering login credentials should be minimal. Increasing the security of the protocol must have minimal effect in decreasing the login usability.
3. The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space.

The proposed system aims to reduce the possibility of cookie theft since a negative answer is expected if the user logs in from a public machine. The user account is set to be in non owner mode for a specified time window when a login is successful without receiving a valid cookie from the user machine; otherwise the account is set to owner mode.

4. Proposed System

In this proposed a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. We analyze the performance of PGRP with two real-world datasets and find it more promising than existing proposals.

Advantages:

- Easy to deploy and scalable.
- Minimum computational resources in terms of memory, processing time, and disk space.
- PGRP is more restrictive against brute force and dictionary attacks.

a. methodology

Modules:

1. User enrollment

The user enrollment process gets the user details and stores in the database. This initial registration process will be performed by admin and user. The application is created for the banking domain, which contains the basic registration process.

2. Account creation

The account details of the user will be saved in the database using this account creation module. The application receives the account holder name, address, branch and other details related to the account. Creation of a banking application with default security aspects is the main application interface of our project. Securing the banking transactions and improving the quality of service is the additional aim of the system. The application gives the security architecture by identifying and giving alert to the bank admin when the intruders try to hack the data.

3. Login

a. Login attempt calculation

This module will get the login attempt of the user and cookie information. This will get the information about the system while the user login from remote systems. If the user is first time then the cookie will store the data and can't verify things for access. This module keeps the copy of every single user login in the remote login as well the known machine, further it will helps to verify the data when wrong entry implies.

4. Fake page navigation

The input will be the username, password and the valid cookie. The cookie will store all the details from the browser history. These are identified by their IP addresses saved on the login server as a black-list, or cookies stored on client machines. If the user has more number of attempts, then the system will navigate them to a fake page.

5. Screen capturing

After fake page navigation, the system will start capturing the access of the intruder by applying honeypot techniques. Using this module, the real user can know the motive behind the intruder attack.

The screen capturing technique captures every activity for every 5 seconds and stores in a local cache. Finally the screens will be sending to the original user via email.

6. Improved honey pot based tracking

The alert about the intruder based on their failure count will be taken from the data stream i.e. the weblog. Using machine learning approach the details of the intruder will be gathered and grouped with the Meta alert schemes. The details about the system and relevant guessing data will be sending to the user.

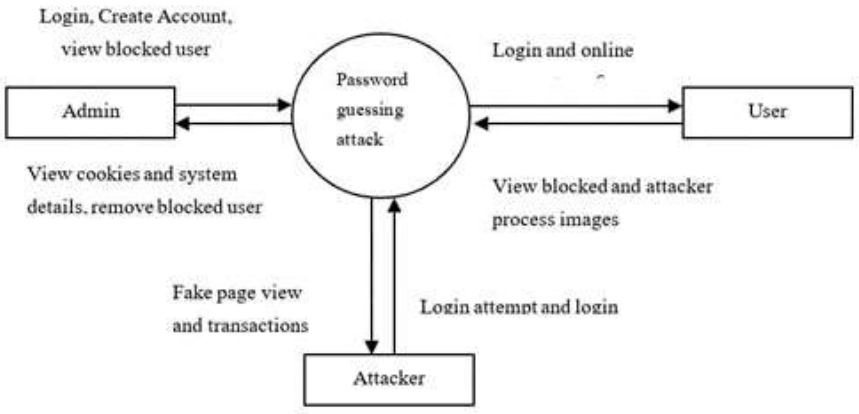
The user can view the logs and intruder details from the database. The admin also can view all the details about users, intruders through their web logs.

7. Transaction and report

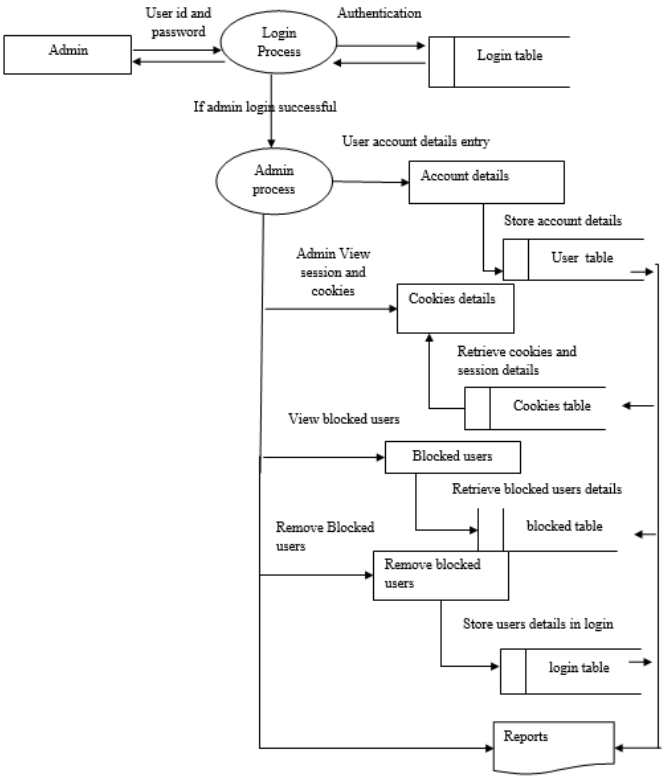
Finally the system allows the legitimate user to perform the transaction after successful login. The application allows all type of banking transaction after successful login.

5. Data flow diagram

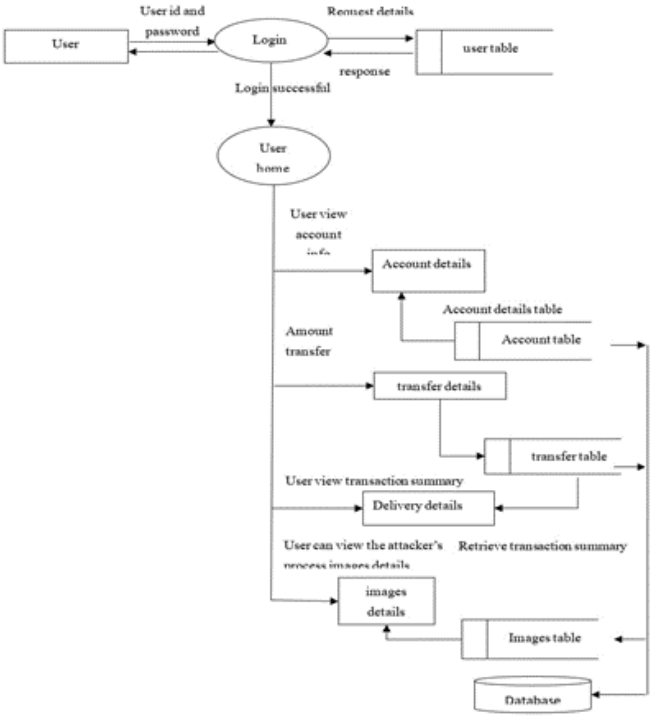
DFD depict hoe data interact with the system. DFD are extremely useful in modeling many aspects of a business function because they systematically subdivide a task into basic parts, helping the analyst understand the system that they trying to model data flow diagram models a system by using external entities from which data flow to a process which transmission the data and creates output data which goes to other processes on external entities of files. Data may also flow to process as inputs.



1.1 Data Flow Diagram

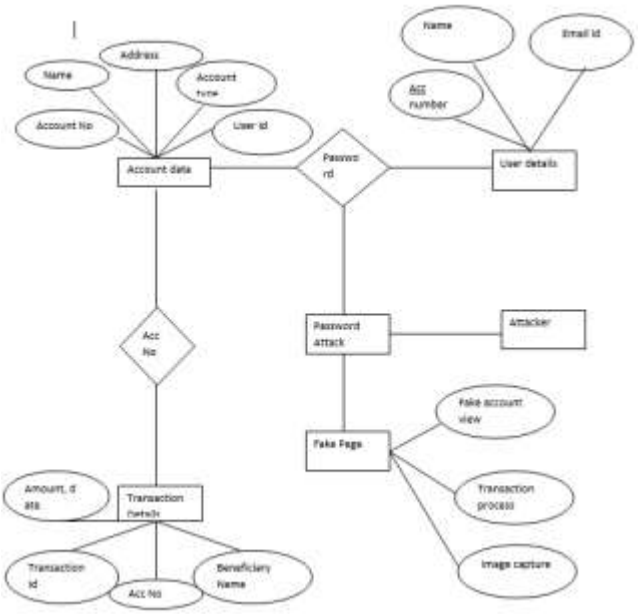


1.2 Admin Data Flow Diagram



1.3 User Data Flow Diagram

ERD



1.4 Architecture of the proposed system

6. Result and Discussion

a. Results

Implementation of Honeypot Technique:

Successfully developed and integrated the honeypot technique into the online banking application.

Implemented using ASP.net and C#.net technologies for seamless integration.

Data Collection:

Comprehensive data collected, including attacker

IP addresses, login times, locations, and post-login activities.

This data provides valuable insights into attacker behavior and intentions.

User Empowerment:

Users are provided with detailed information about attackers, empowering them to take proactive measures to safeguard their accounts.

This enhances user awareness and encourages a more proactive approach to security.

Discussion

Effectiveness of Honeypot Technique:

The honeypot technique proves to be effective in detecting and handling password guessing attacks.By redirecting attackers to a fake page, the system successfully gathers crucial information about their activities.

User Awareness and Proactivity:

Providing users with detailed information about attacker activities enhances their awareness and prompts them to take proactive security measures.

Users are better equipped to respond to potential threats and protect their accounts.

Future Development Opportunities:

While the current system demonstrates promising results, there is room for further refinement and enhancement.

Future research could focus on optimizing the honeypot technique and improving user interface design to enhance overall security and usability.

7. CONCLUSION

In conclusion, the development of this web application has been successful in integrating all modules, testing details, and deployment information seamlessly into the system. Rigorous testing procedures were undertaken, and any encountered errors were effectively debugged. The performance evaluation revealed satisfactory results, with all necessary outputs generated as expected.

This system offers a streamlined approach to automating various consumption functionalities, promising convenience and efficiency. Implementation of this application across multiple consumption scenarios could prove highly beneficial. Moreover, there is ample room for further enhancements to optimize the website's functionality, making it even more appealing and user-friendly.

Overall, it can be affirmed that the application meets the desired objectives and fulfills the identified needs. Through robust testing and debugging processes, it has demonstrated reliability and functionality. Additionally, it serves as a platform for the seamless sharing of files among valuable resources.

8. REFERENCES

[1] L. Spitzner, “Honeypots: definitions and value of honeypots,” URL: http://www.tracking-hackers.com/papers/honeypots.html, 2003.

[2] S. Baddar, A. Merlo, and M. Migliardi, “Anomaly detection in com- puter networks: A state-of-the-art review,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 5, no. 4, pp. 29–64, 2014.

[3] A. Kamra and E. Bertino, “Design and Implementation of an Intrusion Response System for Relational Databases,” IEEE Trans. Knowl. Data Eng., vol. 23, no. 6, pp. 875–888, 2011. [Online]. Available: http://dx.doi.org/10.1109/TKDE.2010.151

[4] A. Merlo, M. Migliardi, D. Raso, and E. Spadacini, “Optimizing Network Energy Consumption through Intrusion Prevention Systems,” in International Joint Conference SOCO’14-CISIS’14-ICEUTE’14, ser. Advances in Intelligent Systems and Computing. Springer International Publishing, 2014, vol. 299, pp. 505–515. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-07995-0_50

[5] F. Palmieri and U. Fiore, “Network anomaly detection through nonlinear analysis,” Computers & Security, vol. 29, no. 7, pp. 737 – 755, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404810000362

[6] M. Migliardi and A. Merlo, “Improving energy efficiency in distributed intrusion detection systems,” Journal of High Speed Networks, vol. 19, no. 3, pp. 251–264, 2013.

[7] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, “Network anomaly detection with the restricted boltzmann machine,” Neurocomputing, vol. 122, no. 0, pp. 13 – 23, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231213005547

[8] M. Curti, A. Merlo, M. Migliardi, and S. Schiappacasse, “Towards energy-aware intrusion detection systems on mobile devices,” in High Performance Computing and Simulation (HPCS), 2013 International Conference on, July 2013, pp. 289–296.

[9] F. Palmieri, U. Fiore, and A. Castiglione, “A distributed approach to network anomaly detection based on independent component analysis,” Concurrency and Computation: Practice and Experience, vol. 26, no. 5, pp. 1113–1129, 2014. [Online]. Available: http://dx.doi.org/10.1002/cpe.3061

[10] M. Migliardi and A. Merlo, “Energy Consumption Simulation of Different Distributed Intrusion Detection Approaches,” in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, March 2013, pp. 1547–1552.

[11] A. Juels and R. L. Rivest, “Honeywords: Making password-cracking detectable,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 145–160.

[12] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, and M. Herrb, “Lessons learned from the deployment of a high-interaction honeypot,” in De- pendable Computing Conference, 2006. EDCC ’06. Sixth European, Oct 2006, pp. 39–46.

[13] R. McGrew, “Experiences with honeypot systems: Development, deploy- ment, and analysis,” in System Sciences, 2006. HICSS’06. Proceedings of the 39th Annual Hawaii International Conference on, vol. 9. IEEE, 2006, pp. 220a–220a.

[14] G. Kontaxis, E. Athanasopoulos, G. Portokalidis, and A. D. Keromytis, "Sauth: Protecting user accounts from password database leaks," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 187–198.

[15] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss- resistant password management," in Computer Security–ESORICS 2010. Springer, 2010, pp. 286–302.

[16] I. Koniaris, G. Papadimitriou, and P. Nicopolitidis, "Analysis and visu- alization of ssh attacks using honeypots," in EUROCON, 2013 IEEE. IEEE, 2013, pp. 65–72.

[17] F. Cohen, "The use of deception techniques: Honeypots and decoys,"Handbook of Information Security, vol. 3, pp. 646–655, 2006.

[18] M. Kim, M. Kim, and Y. Mun, "Design and implementation of the honeypot system with focusing on the session redirection," in Computa- tional Science and Its Applications–ICCSA 2004. Springer, 2004, pp. 262–269.

[19] N. Chakraborty and S. Mondal, "Tag digit based honeypot to detect shoulder surfing attack," in Security in Computing and Communications. Springer, 2014, pp. 101–110.

[20] L. Zhao and M. Mannan, "Explicit authentication response consid- ered harmful," in Proceedings of the 2013 workshop on New security paradigms workshop. ACM, 2013, pp. 77–86.

[21] M. T. Qassrawi and Z. Hongli, "Deception methodology in virtual honeypots," in Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on, vol. 2. IEEE, 2010, pp. 462–467.

[22] I. Erguler, "Achieving flatness: Selecting the honeywords from existing user passwords," IEEE Transactions on Dependable and Secure Computing, 2015.

[23] I. Erguler, "Some remarks on honeyword based password-cracking detection," IACR Cryptology ePrint Archive, vol. 2014, p. 323, 2014.

[24] E. Bertino and R. S. Sandhu, "Database Security-Concepts, Approaches, and Challenges," IEEE Trans. Dependable Sec. Comput., vol. 2, no. 1, pp. 2–19, 2005. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2005.9

[25] Z. N. Peterson, R. C. Burns, J. Herring, A. Stubblefield, and A. D. Rubin, "Secure deletion for a versioning file system." in FAST, vol. 5, 2005, pp. 4–11.

[26] Z. N. Peterson, R. C. Burns, G. Ateniese, and S. Bono, "Design and implementation of verifiable audit trails for a versioning file system." in FAST, vol. 7, 2007, pp. 20–20.

[27] L. Catuogno, H. Löhr, M. Winandy, and A.-R. Sadeghi, "A trusted versioning file system for passive mobile storage devices," Journal of Network and Computer Applications, vol. 38, no. 1, pp. 65–75, 2014.

[28] V. Samar, "Unified login with pluggable authentication modules (pam)," in Proceedings of the 3rd ACM conference on Computer and communications security. ACM, 1996, pp. 1–10.

[29] S. Soltesz, H. Pötzl, M. E. Fiuczynski, A. Bavier, and L. Peter- son, "Container-based operating system virtualization: a scalable, high-performance alternative to hypervisors," in ACM SIGOPS Operating Systems Review, vol. 41, no. 3. ACM, 2007, pp. 275–287.

[30] P. B. Menage, "Adding generic process containers to the linux kernel," in Proceedings of the Linux Symposium, vol. 2. Ottawa Linux Symposium (OLS), 2007, pp. 45–57.

[31] Eric Biederman et al., "Linux containers," http://linuxcontainers.org.

[32] Odin Inc., "Openvz official site," http://openvz.org.

[33] X. Yi, M. G. Kaosar, R. Paulet, and E. Bertino, "Single-Database Private Information Retrieval from Fully Homomorphic Encryption," IEEE Trans. Knowl. Data Eng., vol. 25, no. 5, pp. 1125–1134, 2013. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/TKDE.2012.90

[34] A. Castiglione, A. De Santis, U. Fiore, and F. Palmieri, "An asynchronous covert channel using spam," Computers & Mathematics with Applications, vol. 63, no. 2, pp. 437 – 447, 2012, advances in context, cognitive, and secure computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0898122111006432

[35] A. Castiglione, B. D'Alessio, A. De Santis, and F. Palmieri, "New Steganographic Techniques for the OOXML File Format," in Availability, Reliability and Security for Business, Enterprise and Health Information Systems, ser. Lecture Notes in Computer Science,

A. Tjoa, G. Quirchmayr, I. You, and L. Xu, Eds. Springer Berlin Heidelberg, 2011, vol. 6908, pp. 344–358. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-23300-5_27

[36] A. Castiglione, B. D'Alessio, and A. De Santis, "Steganography and Secure Communication on Online Social Networks and Online Photo Sharing," in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, Oct 2011, pp. 363–368.

[37] A. Castiglione, A. De Santis, U. Fiore, and F. Palmieri, "E-mail- Based Covert Channels for Asynchronous Message Steganography," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on, June 2011, pp. 503– 508.

[38] A. Vance, "If your password is 123456, just make it hackme," The New York Times, vol. 20, 2010.