International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Masquerade Attack Identification Via DDSGA-Based Anomaly Detection

Anusha Sivanandhan[1], Bibitha Baby[2], Dhanya G S[3]

[1]Assistant Professor, PG Department of Computer Science, Naipunnya institute of management and information technology (NIMIT),Pongam, Thrissur- 680308, Kerala, India
[21]Assistant Professor, PG Department of Computer Science, Naipunnya institute of management and information technology (NIMIT),Pongam, Thrissur- 680308, Kerala, India
[31]Assistant Professor, PG Department of Computer Science, Naipunnya institute of management and information technology (NIMIT),Pongam, Thrissur- 680308, Kerala, India

---

Abstract -To take advantage of the user services and privileges, a masquerade attacker poses as a legitimate user. The semi- global alignment algorithm (SGA) is one of the most effective and efficient techniques to detect these attacks but it has not yet reached the accuracy and performance required by large scale, multiuser systems. To improve both the effectiveness and the performances of this algorithm, the Data-Driven Semi - Global Alignment, DDSGA approach was proposed. By implementing unique alignment settings for every user, DDSGA enhances the scoring systems from the perspective of security effectiveness. Additionally, by permitting minor adjustments to the low-level representation of the instructions' functionality, it can withstand minor variations in user command sequences. It also adapts to changes in the user behavior by updating the signature of a user according to its current behavior. To optimize the runtime overhead, DDSGA minimizes the alignment overhead and parallelism the detection and the update.

Key Words: legal user, DDSGA approach, user services, SGA, DDSGA algorithm

1.INTRODUCTION

An attacker who poses as a legal user is known as a masquerader. This individual accomplishes this by either hacking the system that confirms the user's identification or by obtaining the user's login credentials. To put it another way, the masquerader fools the system into believing they are someone else who has access to specific resources. By exploiting a legitimate user's information, they can obtain illegal access to sensitive data or systems. Because the attacker can carry out tasks that should only be feasible for the authorized user, this can result in significant security breaches. The possibility of masquerading highlights how crucial it is to have robust security protocols and efficient authentication procedures in order to safeguard user identities and stop illegal access. Insider masquerading is a legitimate practice.

A legal system user who abuses their rights to get access to many accounts and carry out illegal activities is known as an insider masquerader. An outsider's objective is to exploit every right of a legitimate user (Phyo and Furnell, 2004). There are several ways to carry out this attack, including eavesdropping and packet sniffing, installing software with backdoors or malicious code, spoofing, social engineering, and duplicate or ex-filtration of user passwords. Log files may contain evidence of these attacks that can subsequently be linked to a particular user. The most advanced method for identifying these assaults in this situation is still log analysis by a host-based IDS. Analysing the target system can reveal attacks that don't leave an audit trail. By gathering information such as login time, location, session duration, CPU time, commands issued, user ID, and IP address, masquerade detection first builds a user profile. Computer infrastructure intrusions are becoming a bigger issue. Masquerading, in which an attacker poses as a genuine user on a computer system, is one of the most destructive intrusions or attacks in the real of computer security. Masquerade attacks typically occur when an intruder obtains a legitimate user password or when a user leaves their workstation unattended without a locking measure in place. Because the attacker looks like a regular user with legitimate authority and privileges, it is challenging to identify this kind of security compromise at the outset. The Data-Driven SemiGlobal Alignment (DDSGA) approach, which is presented in this research, enhances the computational performance and detection accuracy of the Enhanced-SGA and HSGAA, which are both based on SGA. The

main idea of DDSGA is to consider the best possible alignment between the user's recorded sequences and the sequence of the present session. Once the misaligned areas have been identified, we classify them as abnormal. A number of anomalous locations are very suggestive of a masquerade attack.

In addition to employing lexical matching techniques like string matching and longest common substring searches, DDSGA increases security efficiency by accepting minor sequence modifications. There have been some small adjustments made to the low-level representation of user commands. A command that performs the same functions can be matched for this purpose. 3 DDSGA assigns unique gap insertion penalties to each user based on their behaviour in order to improve the hit ratio and lower false positive and false negative rates. Additionally, it enhances Enhanced-SGA's alignment scoring mechanism and update phase to accommodate behavioural changes without appreciably lowering the alignment score.

2. Materials and Methods

DDSGA is an enhanced – SGA - based masquerade detection method. It classifies the misalignment areas as anomalous and aligns the user's current session sequence with their prior ones. A masquerade attack is signaled if the percentage of anomalous areas is larger than a dynamic, user dependent threshold. DDSGA has a unique ability to handle small changes in user sequences. These changes can occur in the low-level representation of user commands. This system is divided into three distinct phases: the configuration phase, the detection phase, and the update phase.

In the configuration phase, the system calculates the alignment parameters tailored for each user. These parameters are crucial as they guide both the detection and update phases. Proper alignment ensures that the system can accurately identify and respond to changes. Overall, this structured approach enables DDSGA to function effectively, even when faced with minor variations in user input. The detection phase aligns the user current session to the sig nature sequence. The computational performance of this phase is improved by two approaches namely the TopMatching Based Overlapping (TMBO) and the parallelized approach. In order to change the system settings during the update phase, DDSGA adds new patterns to the user lexicon list and user signatures.

ALGORITHM

A. The Enhanced-SGA developed by (Coulla ,Szymanski.2008) ,made significant changes to the SGA algorithm. It addressed shortcomings found in the standard Smith-Waterman alignment algorithm from two significant perspectives. The first perspective focuses on the fact that how legitimate users behave may change over time. This change can occur due to a shift in their roles or the introduction of new commands. Because of this, a static user signature may mistakenly identify these lawful variations as security threats. To minimize the occurrence of such false positives, the Enhanced-SGA updates the user signature as new behaviors are detected. This is achieved by utilizing the SGA's ability to find similarities in user actions.

B. Additionally, the authors presented two grading systems: command grouping and binary scoring. These systems are designed to align scores and balance penalties for gap insertions effectively. The binary grading system is particularly emphasized as it is the most effective. It updates the signature sequence to include new behaviours as well as incorporating the user lexicon, which records new commands used by the user. To enhance security, this method establishes a threshold for each user profile. This ensures that both the updated signature sequences and the user lexicon remain free from any compromised commands potentially linked to masquerade attacks. The threshold plays an essential role in both the detection and updating processes and is constructed based on an analysis of user signatures.

C. (Schonlau et al.2001),The second perspective addresses the computational challenges associated with the Smith-Waterman algorithm. This algorithm is often too expensive and impractical for use in detecting masquerade attacks, especially in multi-user environments. To tackle this, the Enhanced-SGA employs heuristic orientation that prioritizes user signature components with the highest likelihood of detection success. This approach significantly reduces processing demands while maintaining accuracy in identifying threats. These enhancements were tested against the ocean data set to compare effectiveness with other existing methods.

D. B. The Data-Driven Semi-Global Alignment approach, known as DDSGA, builds on the Enhanced - SGA framework. DDSGA aims to detect masquerade attacks by matching the current session of a user with

their historical session data. (Smith and Waterman,1981), If the number of identified abnormal areas exceeds a dynamically set threshold, a masquerade attack is indicated. DDSGA is capable of accommodating minor variations in user session data without compromising accuracy. It consists of three phases: configuration, detection, and updating.

E. During the configuration phase, DDSGA calculates the alignment parameters specific to each user. These parameters guide both detection and updating phases. (Dash et al.2005)In the detection phase, the current session of a user is compared with their signature sequence. The performance of this phase is enhanced through two techniques: Top-Matching based Overlapping (TMBO) and a parallelized processing method. The update phase then extends both the user signatures and the lexicon, integrating new patterns to adjust system parameters. The overall structure and the modules tied to these phases are elaborated upon in the following sections.

F.

3. CONCLUSIONS

Masquerading is a targeted attack strategy that poses a serious threat to information security. This method allows an attacker to secretly access and control a system with harmful intent. To combat such threats, a model known as the Sequence Alignment-based Audit (SGA) has been developed. This model analyses sequential audit data, which includes both the information that has been checked and information that has simply been observed. Although SGA is useful, it struggles with a low false positive rate. At the same time, it has a high rate of missed alarms, leading to problems with its accuracy. Even in its most recent version, SGA does not perform well enough to be reliable in real-world situations.

Recognizing these shortcomings, the Dynamic Data Sequence Alignment (DDSGA) model was created. This new model places an emphasis on improving security and accuracy. DDSGA achieves better consistency by assigning different parameters to each user. It also introduces a two-tier scoring system designed to reduce changes in how low-level user commands work. This system aligns commands within the same category while keeping the alignment score intact. Importantly, it takes into account how users execute commands and how their behaviours change over time.

The advancements in DDSGA result in significantly lower rates for false positives and missed alarms. It also enhances the detection hit ratio, leading to better overall performance. When comparing results using the SEA dataset, DDSGA consistently outperforms its predecessor, SGA. Additionally, DDSGA employs a Top-Matching Based Overlapping approach. This method reduces the computational load by simplifying the pattern sequence into a smaller set of overlapping subsequence. The system can also carry out detection and update processes at the same time, maintaining accuracy without any loss of effectiveness

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all individuals and institutions that supported this research. Special thanks are extended to resources and infrastructure significantly contributed to the successful execution of this study. We also acknowledge the valuable insights and constructive feedback provided by peer reviewers, which helped enhance the quality of this work. This research would not have been possible without the continued encouragement and support from our colleagues and academic mentors.

REFERENCES

1. H. Phyo and S. M. Furnell. A detection-oriented classification of insider it misuses, in Proc. 3rd Security Conf. 2004(2004).

2. S. E. Coull, J. W. Branch, B. K. Szymanski, and E. A. Breimer. Intrusion detection: A bioinformatics approach, in Proc. 19th Annu. Comput. Security Appl. Conf., Las Vegas, NV, USA, Dec. 2003, pp. 24–33(2003).

3. S. E. Coulla and B. K. Szymanski. Sequence alignment for masquerade detection, J. Comput. Statist. Data Anal., vol. 52, no. 8, pp. 4116–4131, Apr. 2008 (2008).

4. Hisham A. Kholidy and Fabrizio Baiardi. CIDS: A framework for intrusion detection in cloud systems, in Proc. 9th Int. Conf. Inf. Technol.: New Generations, Las Vegas, Nevada, USA, Apr. 2012, pp. 16–18(2012).

5. [Online].Available: http://www.schonlau.net/intrusion. html(2001).

6. M. Schonlau, W. DuMouchel, W. Ju, A. F. Karr, M. Theus, and Y. Vardi. Computer intrusion: Detecting masquerades, Statist. Sci. vol. 16, no. 1, pp. 58–74, (2001).

7. Greenberg: Using Unix: Collected traces of 168 users, Dept. Comput. Sci., Univ. Calgary, Calgary, Canada, Res. Rep. 88/333/ 45(1988).

8. T. Lane and C. E. Brodley. An application of machine learning to anomaly detection, in Proc. 20th Nat. Inf. Syst. Security Conf., 1997, pp. 366–380,(1997).

9. RUU data set:[Online] Available: http://sneakers.cs. columbia.edu/ids/RUU/data/,(2008).

10. Hisham. A. Kholidy and Fabrizio Baiardi. CIDD: A cloud intrusion detection data set for cloud computing and masquerade attacks, in Proc. 9th Int. Conf. Inf. Technol.: New Generations, Las Vegas, NV, USA, Apr. 2012, pp. 16–18,(2012).

11. R. A. Maxion and T. N. Townsend. Masquerade detection using truncated command lines, in Proc. Int. Conf. Dependable Syst. Netw., Washington, DC, USA, Jun. 2002, pp. 219– 228,(2002).

12. R. Posadas, J. C. Mex-Perera, R. Monroy, and J. A. Nolazco-Flores. Hybrid method for detecting masqueraders using session folding and hidden markov models, in Proc. 5th Mexican Int. Conf. Artif. Intell., 2006, pp. 622–631,(2006).

13. W. Dumouchel. Computer intrusion detection based on Bayes Factors for comparing command transition probabilities. Technical report 91, National Institute of Statistical Sciences, [Online]. Available: www.niss.org/downloadabletechreports. html (1999).

14. W. Ju and Y. Vardi. (1999). A hybrid high-order Markov chain model for computer intrusion detection. Nat. Inst. Statist. Sci. Research Triangle Park, NC, USA, Tech. Rep. 92(1999).

15. [Online].Available:www.niss.org/downloadablet echreports .html.

16. Brian D. Davison and Haym Hirsh. Predicting sequences of user actions, in Proc. Joint Workshop Predicting Future: AI Approaches Time Ser. Anal., 1998, pp. 5–12(1998).

17. T. Lane and C. E. Brodley. Approaches to online learning and concept drift for user identification in computer security, in Proc 4th Int. Conf. Knowl. Discovery Data Mining, New York, NY, USA, Aug. 1998, pp. 259–263,(1998).

18. Christopher. A tutorial on support vector machines for pattern recognition, Data Mining Knowl. Discovery, vol. 2, no. 2, pp. 121– 167,(1998).

19. Szymanski and Y. Zhang. Recursive data mining for masquerade detection and author identification, in Proc. IEEE 5th Syst., Man .Cybern. Inf. Assurance Workshop, West Point, NY, USA, Jun. 2004, pp. 424–431,(2004).

20. S. K. Dash, K. S. Reddy, and A. K. Pujari. Episode based masquerade detection, in Proc. 1st Int. Conf. Inf. Syst. Security, 2005, pp. 251–262(2005).

21. A.Sharma and K. K. Paliwal. Detecting masquerades using a combination of Na€ıve Bayes and weighted RBF approach, J. Comput. Virology, vol. 3, no. 3, pp, 237–245, (2007).

22. Subrat Kumar Dash, K. S. Reddy, and K. A. Pujari. Adaptive Naive Bayes method for masquerade detection, Security Commun. Netw., vol. 4, no. 4, pp. 410–417, (2011).

23. S. Malek and S. Salvatore. Detecting masqueraders: A comparison of one-class bag-ofwords user behavior modeling techniques, in Proc. 2nd Int. Workshop Managing Insider Security Threats, Morioka, Iwate, Japan. Jun. 2010, pp. 3–13,(2010).

24. A.S. Sodiya, O. Folorunso, S. A. Onashoga, and P. O. Ogundeyi. An improved semi-global alignment algorithm for masquerade detection, Int. J. Netw. Security, vo1. 12, no. 3, pp. 211–220, May 2011,(2011).

25. T. F. Smith and M. S. Waterman. Identification of common molecular subsequences, J. Molecular Biol., vol. 147, pp. 195–197(1981).

26. B. Christopher and T. D. Herbert. Receiver operating characteristic curves and related decision measures: A tutorial, Chemometrics Intell. Lab. Syst., vol. 80, pp. 24–38,(2006).

27. K. Wang and S. J. Stolfo. One class training for masquerade detection, in Proc. IEEE 3rd Conf. Workshop Data Mining Comput. Secur., Florida, Nov. 2003,(2003).