International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Detection of Masquerade Attacks by using DDSGA: Data-Driven Semi-Global Alignment Approach with CIDS Framework

Shital Rajabhau Ghuge[1], Sandip Satav[2]

[1]Department Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

[2]Professor, Information Technology, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

Abstract: ***Masquerade attackers embody a genuine user to get the user services and advantages. The SGA is very effective as well as especially techniques to find out this attack but it has not stretched the accuracy and executions required by large scale, multiuser systems. To increase whole effectiveness as well as the execution of this algorithm, we suggest the Data Driven Semi-Global Alignment, DDSGA approach. As per the view point of security operative, DDSGA update the scoring systems by adopting various alignment arguments for every user. more ever, it allow small change in user command series by allowing little becoming different in the low-level showing of the command to ability to perform a task . It makes suitable changes in the client using technique by updating the pattern of a user according to its current using technique. For perfecting the runtime located, DDSGA to make as tiny the alignment overhead and parallelizes the find out and the update. After representing the DDSGA phases, we represent the experimental results. This output shows that DDSGA get the high hit ratio of 88.4 % with a low false positive rate. It increases the hit ratio of the enhanced SGA as well as reduces Maxion-Townsend cost. Hence, DDSGA results in increasing all the hit ratio and false positive rates with an capable calculation overhead.***

Keywords: Masquerade detection, sequence alignment, security, intrusion detection, attacks

1. Introduction

Masquerader is an attacker who find easily the genuine user who accesses the services as well as immunity of the user. This problem can be overcome by proposing SGA (Semi Global Alignment) algorithm. It is very efficient as well as operative algorithm. Meanwhile the limitation is that it is not too accurate for the multiuser systems. As per this point of view, the DDSGA algorithm can be proposed. It can easily find and detect the attacks. It improves the effectiveness as well as efficiency as compare to SGA algorithm. For the security system DDSGA improves the scoring system. The scoring system is improved for each and every user by adopting distinct alignment. DDSGA minimizes the overhead of alignment as well as detects parallel, also update it. After describing the phases of DDSGA, we can get the results. This result also shows that the DDSGA can find the high hit ratio of 88.4% with low false positive ratio too. DDSGA improves false positive rate as well as reduced Marion Townsend cost.

2. Related Work

Hisham A. Kholidy and Fabrizio Baiardi In this paper, They have presented the architecture of a distributed system for intrusion detection called CIDS, which employs multiple elementary detectors and combination of their alerts to make an accurate determination of intrusion. Then we presented an instantiation of this architecture with three elementary detectors and a manager with a graph-based and a Bayesian network based inference engine. They evaluated the system under a real-world web based e-commerce application and three classes of attacks. CIDS was found to bring down the incidence of missing alarms and false alarms with negligible impact on the performance. They are currently exploring how to set up the Rule Objects for different attack classes in an automated manner. The approach uses a feedback control loop to adjust the weights or probabilities in the rules. They are developing a larger set of test cases to carry out statistically large set of experiments to measure false positives and false negatives in CIDS. We are adding a timing module to estimate the speed of propagation of attacks and augmenting the Response Engine to have a choice of responses which will be decided based on the timing information. [1]

Brian D. Davison and Haym Hirsh We have presented a method that fulfills the requirements of an Ideal Online Learning Algorithm. Incremental Probabilistic Action Modeling has an average predictive accuracy at least as good as that previously reported with C4.5. It operates incrementally, will remember rare events such as typos, and does not retain a copy of the user‟s action history. IPAM can generate top-n predictions, and by weighing recent events more heavily than older events it is able to react to „concept-drift‟. Finally, its speed and simplicity make it a strong candidate for incorporation into the next adaptive interface. [2]

Christopher In this paper**,** SVMs provide a new approach to the problem of pattern recognition (together with regression estimation and linear operator inversion) with clear connections to the underlying statistical learning theory. SVM training always finds a global minimum. The simple geometric interpretation of SVM provides fertile ground for further investigation. An SVM is largely characterized by

the choice of its kernel, and SVMs thus link the problems they are designed for with a large body of existing work on kernel based methods. I hope that this tutorial will encourage some to explore SVMs for themselves.[3]

Szymanski and Y. ZhangIn this paper, we show how to apply recursive data mining to solve the masquerade intrusion detection and author identification problems. Compared to the results from other researchers, our results are very promising. [4]

Subrat Kumar Dash, K. S. Reddy, and K. A. PujariWe propose, in this paper, a method that takes into consideration this aspect of user behavior while detecting masquerade attacks. Our scheme is based on the premise that the commands used by a legitimate user or an attacker may differ from the trained signature. But the deviation of the legitimate user is momentary whereas that of an attacker persists longer. By introducing this novel concept in the detection mechanism, the performance improves. We show this empirically using several benchmark datasets [5]

A. S. Sodiya, O. Folorunso, S. A. Onashoga, and P. O. OgundeyiIn this work, an improved semi-global alignment called Crosssemiglobal algorithm, is designed to improve the efficiency of masquerade detection. In the previous pair-wise algorithms, a fix value is always assumed as the gaps score. In Cross-semiglobal algorithm, the scoring function on which the algorithms based their scores is constructed from legitimate users‟ sequence of commands. This principle was implemented using platform independent C/C++ framework. The designed was tested using a systematically generated ASCII coded sequence audit data from Windows and UNIX operating systems as simulations for standard non-intrusive and intrusion data. The result shows a reduction in false positive rate from 7.7% using semi-global alignment to 5.4% using cross-semiglobal. The detection efficiency was also improved by 7.7%. [6]

3. Proposed Work

From the security efficiency perspective, DDSGA models more accurately the consistency of the behavior of distinct users by introducing distinct parameters. Furthermore, it offers two scoring systems that tolerate changes in the low-level representation of the commands functionality by categorizing user commands and aligning commands in the same class without reducing the alignment score. The scoring systems also tolerate both permutations of its commands and changes in the user behavior over time. All these features strongly reduce false positive and missing alarm rates and improve the detection hit ratio. In the experiments using the SEA data set, the performance of DDSGA is always better than the one of SGA. From the computational perspective, the Top-Matching Based Overlapping approach reduces the computational load of alignment by decomposing the signature sequence into a smaller set of overlapped subsequences. Furthermore, the detection and the update processes can be parallelized with no loss of accuracy.

4. Architectural View

The architecture diagram of the system shown below helps us to understand the system.

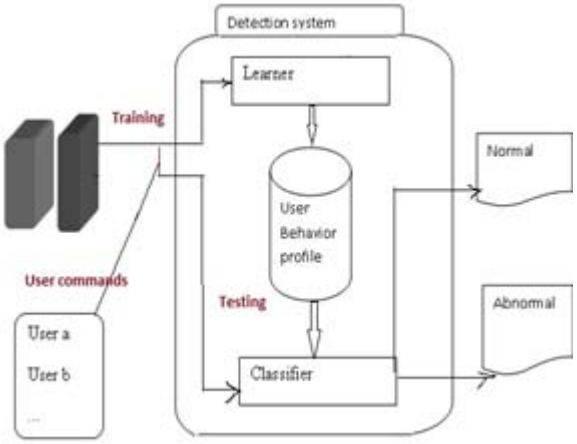

Figure 1: System Architecture

- This paper is introducing the Data-Driven Semi-Global Alignment (DDSGA) approach. The DDSGA which improves the detection accuracy as well as the computational performance of the Enhanced-SGA and of HSGAA which is also based upon SGA.
- The main idea of DDSGA is of considering the best alignment of the active session sequence to the recorded sequences of the same user. After discovering the misalignment areas, we label them as anomalous. The several anomalous areas are a strong indicator of a masquerade attack.
- DDSGA can tolerate small mutations in the user sequences with small changes in the low level representation of user commands and it is decomposed into a configuration phase, a detection phase and an update one.
- The configuration phase, computes, for each user, the alignment parameters to be used by the detection as well as update phases.
- The detection phase aligns the user current session to the signature sequence. The computational performance of this phase is improved by two approaches. One is the Top-Matching Based Overlapping (TMBO) and second one is the parallelized approach.
- In the update phase, DDSGA extends both the user signatures and user lexicon list with the new patterns. It get done to reconfigure the system parameters.

Sr No.	Paper	Technique	Advantages	Disadvantage
1	Intrusion detection: A bioinformatics approach	Detection Algorithm, Alignment Algorithm	sequence alignment algorithm for the detection of masqueraders	initial false positive rate is somewhat lackluster, often misidentifies user subsequences as an intruder
2	Sequence alignment for masquerade detection	Sequence Alignment Algorithm	offers the level of accuracy necessary for practical deployment	Sometimes fail to detect masquerade attacks
3	CIDS: A framework for intrusion detection in cloud systems	Algorithm for processing a new event at the Graph-based Inference Engine	employs multiple elementary detectors and combination of their alerts to make an accurate determination of intrusion.	measure false positives and false negatives in CIDS not done
4	Computer intrusion: Detecting masquerades	exponential weighting algorithm, The compression algorithm builds compression rules from the beginning of the file.	statistical methods can detect intrusions	Unable to deal with complex intruder behavior
5	An application of machine learning to anomaly detection	selection algorithm based on the least-recently-used (LRU) page replacement policy	highly optimizable	Unable to examine the tradeoff between adapting to legitimate change and protecting against hostile training
6	Masquerade detection using truncated command lines	The Naive Bayes classification algorithm	careful data collection, attention to experimental methodology, and error analysis	Masquerade detection remains among the most challenging of classification problems.
7	Predicting sequences of user Actions	Incremental Probabilistic Action Modeling Ideal Online Learning Algorithm	this method generates a list of commands with associated probabilities for prediction	problems, including text compression, dynamic program optimization, and predictive caching
8	Approaches to online learning and concept drift for user identification in computer security,"	detection algorithms described in the security literature	updating hypothesis parameters and selecting instances for insertion into the user profile	Unable to track and predict the complete envelope of the classification region

5. Conclusion

Masquerading means the attack intentionally. It is one of the most critical attacks. So attacker can easily enter into the system with wrong intension and can control the system.SGA is a model based on sequence alignment and it is used to detect the different sequential audit data means checked and observed data but the SGA has very low false positive rate and missing alarm rates .low accuracy even its new version or achieved the correct accuracy and also not given the performance for practical deployment .So the overcome from SGA problem we have DDSGA model this model is security perspective and with more accuracy .DDSGA keep the consistency by providing different parameter to different user and then it offers two level scoring system that tolerate means avoids change in the low level commands functionality of user command and aligning commands in the same class but without reducing the alignment score . The scoring systems also allow all to carry out of its commands and changes in the user behavior extra time. All features strongly degrade false positive and missing alarm rates and increase the detection hit ratio. In the SEA data set, the performance of DDSGA is always better as compare to the one of SGA. Top-Matching Based Over-lapping approach reduces the computational load of alignment by reducing the pattern sequence into a smaller set of overlapped subsequences. Furthermore, the detection and the update processes can be parallel with no loss of accuracy.

References

[1] W. Dumouchel. (1999). "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.
[2] 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. [Online]. Available: www.niss.org/downloadabletechreports.html
[3] 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.
[4] 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.
[5] B. Christopher, "A tutorial on support vector machines for pattern recognition," Data Mining Knowl. Discovery, vol. 2, no. 2, pp. 121– 167, 1998.
[6] B. 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.
[7] 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.

[8] 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.
[9] 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.
[10] S. Malek and S. Salvatore, "Detecting masqueraders: A comparison of one-class bag-of-words user behavior modeling techniques," in Proc. 2nd Int. Workshop Managing Insider Security Threats, Morioka, Iwate, Japan. Jun. 2010, pp. 3–13.
[11] T. F. Smith and M. S. Waterman, "Identification of common molecular subsequences," J. Molecular Biol., vol. 147, pp. 195–197, 1981.

Author Profile

Mrs. Shital .R. Ghuge currently pursuing M.E (Computer) from Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. SavitribaiPhule PuneUniversity, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from Shivnagar vidhya prasark mandal malegaon(bk) , Baramati, pune, University, Pune, Maharashtra, India - 413115. Her area of interest is network security, WSN.

Asst Prof. Sandip Satav received the M.E (CSE/IT) degree from Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, MAH, India in 2004. He is currently working as Asst. Professor with Department of Information Technology, Jayawantrao Sawant College of Engineering, Pune, MAH, India. His research interests include Image Processing, Networking.