International Journal of Research
International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Detecting Masquerade Attacks by Using a Data-Driven Semi-Global Alignment Approach

[1]KURRI SHIREESHA, [2]B. VENKANNA.

1.PG Scholar, Department of CSE, sphoorthy engineering college, Hyderabad

2.M-tech, Assistant professor, Department of CSE, sphoorthy engineering college, Hyderabad

ABSTRACT

A masquerade attacker impersonates a legal user to utilize the user services and privileges. The semi-global alignment algorithm (SGA) is one of the most effective and efficient techniques to detect these attacks but it has not reached yet the accuracy and performance required by large scale, multiuser systems. To improve both the effectiveness and the performances of this algorithm, we propose the Data-Driven Semi-Global Alignment, DDSGA approach. From the security effectiveness view point, DDSGA improves the scoring systems by adopting distinct alignment parameters for each user. Furthermore, it tolerates small mutations in user command sequences by allowing small changes in the low-level representation of the commands functionality. It also adapts to changes in the user behaviour by updating the signature of a user according to its current behaviour. To optimize the runtime overhead, DDSGA minimizes the alignment overhead and parallelizes the detection and the update. After describing the DDSGA phases, we present the experimental results that show that DDSGA achieves a high hit ratio of 88.4 percent with a low false positive rate of 1.7 percent. It improves the hit ratio of the enhanced SGA by about 21.9 percent and reduces Maxion-Townsend cost by 22.5 percent. Hence, DDSGA results in improving both the hit ratio and false positive rates with an acceptable computational overhead.

.1INTRODUCTION

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Diagram clearly explain the about the secure computing

Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. Physical security:

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

2 RELATED WORK IN MASQUERADE DETECTION

We briefly outline some masquerade detection approaches. The uniqueness approach [6] assumes that commands that have not been seen in the training data indicate a masquerader. Moreover, the probability that a masquerader has issued a command is inversely related to the number of users that use such a command. While uniqueness has a relatively poor performance, it is one of the few approaches that target false alarm rate of 1 percent. Na€ıve Bayes One-step Markov [13] is based upon one-step transitions from a command to the next. It builds two transition matrices for each user from, respectively, the training database and the testing one and it triggers an alarm when these matrices noticeably differ. The false alarm rate of this method is not satisfactory.

3 SGA AND THE ENHANCED-SGA

This section describes in some details SGA and some proposals to enhance it. SGA is more accurate and efficient than current approaches. It has low false positive and missing alarm rates and high hit ratio. It can be adopted in heterogeneous environment with distinct operating system because it can be applied to distinct audit data such as command line entries, mouse movements, system calls, registry events, file and folder names, sequence of opened windows titles and network access audit data. SGA aligns large sequence areas as in global alignments, while preserving the nature of local alignments. It can ignore both prefixes and suffixes and it only aligns the conserved area with the maximal similarity.

4 EXISTING SYSTEM:

Semi-global alignment (SGA) is one of the most efficient detection algorithms and its accuracy was improved by Coull et al.

Naïve Bayes One-step Markov is based upon one-step transitions from a command to the next. It builds two transition matrices for each user from, respectively, the training database and the testing one and it triggers an alarm when these matrices noticeably differ.

Schonlau et al. toggled between a Markov model and the simple independence one.

Dash et al. introduced an episode based Na€ıve Bayes technique that extracts meaningful episodes from a long sequence of commands.

DISADVANTAGES OF EXISTING SYSTEM:

The current detection approaches have not achieved the level of accuracy and performance for practical deployment in spite of the large amount of information they used to build a profile such as command line commands, system calls, mouse movements, opened files names, opened windows title, and network actions.

While uniqueness has a relatively poor performance, it is one of the few approaches that target false alarm rate of 1 percent.

The false alarm rate of this method is not satisfactory.

5 PROPOSED SYSTEM:

This paper introduces the Data-Driven Semi-Global Alignment (DDSGA) approach, which improves both the detection accuracy and the computational performance of the Enhanced-SGA and of HSGAA that is also based upon SGA.

The main idea underlying DDSGA is to consider 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 and 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 both the detection and 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 namely the Top-Matching Based Overlapping (TMBO) and the parallelized approach.

In the update phase, DDSGA extends both the user signatures and user lexicon list with the new patterns to reconfigure the system parameters.

ADVANTAGES OF PROPOSED SYSTEM:

DDSGA improves the security efficiency by using not only lexical matching such as string matching or longest common substring searches, but also by tolerating small mutations in the sequences with small changes in the low-level representation of the user commands.

To increase the hit ratio and reduce both false positive and false negative rates, DDSGA pairs each user with distinct gap insertion penalties according to the user behavior.

6 CONCLUSIONS

Masquerading is by far one of the most critical attacks because an attacker that can successfully logs to a system can also maliciously control it. The semi-global alignments (SGA) is based upon sequence alignment and it is one of the most effective detection techniques that can be applied to distinct sequences of audit data. While SGA may result in low false positive and missing alarms rates, even itsenhanced version has not yet achieved the level of accuracy and performance for practical deployment. This is the reason underlying the design of the Data-DrivenSemi-Global Alignment Approach, DDSGA. From the security efficiency perspective, DDSGA models more accurately the consistency of the behaviour of distinct users by introducing distinct parameters. Furthemore, 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 tolerates both permutation of its commands and changes in the user behaviour over time.

7 REFERENCES

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

[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.

[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.

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

[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.

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

[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.

AUTHOR'S PROFILE:

MALOTH RAJARAM

Pg Scholar , Department Of Cse. Gandhi Academy Of Technical Education, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206.

V RAMA RAO

Assistant Professor, Department Of Cse. Gandhi Academy Of Technical Education, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206