DDSGA: A Data-Driven semi-global Alignment Approach for detecting masquerade attack

Miss.Choudhar Poonam R., Miss.Dhawade Pranita P., Miss.Khomane Shilpa I.
Guided By: Prof. Nale R.K.
Department of Information Technology, SVPM's College of Engg. Malegaon(BK),
Savitribai Phule, Pune University, Maharashtra, India

---***---

Abstract- A masquerade aggressor impersonates a legal user to utilize the user services and privileges. The semi-global alignment algorithmic program (SGA) is one in all the foremost effective and economical techniques to watch these attacks but it isn't reached nonetheless the accuracy and performance required by large scale, multiuser systems. to boost every the effectiveness and additionally the performances of this algorithmic program, we tend to propose the Data-Driven Semi-Global Alignment, DDSGA approach. From the protection effectiveness scan purpose, DDSGA improves the rating systems by adopting distinct alignment parameters for each user. Moreover, it tolerates very {little} mutations in user command sequences by allowing little changes among the low-level illustration of the commands utility. It collectively adapts to changes among the user behaviour by change the signature of a user in line with its current behaviour. To optimize the runtime overhead, DDSGA minimizes the alignment overhead and parallelizes the detection and additionally the update. Key words: Data-Driven Semi-Global Alignment Approach, Semi-Global Alignment, Full Parallelized Mode, Top Matching Based Overlapping.

1. INTRODUCTION

A participant is associate degree aggressor United Nations agency authenticates as a legal user by stealing its credentials or by violating the authentication service. Associate degree business executive participant may be a system user that misuses his/her privileges to access distinct accounts and perform unauthorized actions. Associate degree outsider aims to utilize all the privileges of a legal user. Different implementations of this attack do exist, like duplication or ex-filtration of user parole, installation of software package with backdoors or malicious code, eavesdropping and packet sniffing, spoofing and social engineering attacks. These attacks could leave some path in log _les that, when the very fact, is joined to some user. During this case, a log analysis by host-based IDS remains the state-of-the art to discover these attacks. Attacks that don't leave associate degree audit path within the target system could also be discovered by analyzing the user behaviors through masquerade detection. At first, masquerade detection builds a profile for every user by gathering data like login time, location, session period, CPU time, commands Issued, user ID and user information processing address.

2. LITERATURE SURVEY

A. "A detection-oriented classification of insider it misuses"[1]:

This though the matter of business executive misuse of IT systems is often recognized within the results of laptop security surveys, it's less wide accounted for in structure security practices and obtainable countermeasures. Indeed, the opportunities for business executive misuse, by perpetrators with licitly assigned privileges, square measure usually unnoted till a happening happens. A potential reason for this is often that the matter receives comparatively very little attention within the ordinarily recognized classifications of IT-related attackers and intrusions, with most focusing upon attacks and strategies involving some variety of system penetration and/or unauthorized access. This paper examines the potential styles of business executive misuse in additional detail, classifying them in keeping with the amount inside in an exceedingly target system at that the incidents can be detected. It's thought of that such associate degree approach might offer a relevant foundation in terms of later approaches to change business executive misuse detection strategies.

B. "Sequence alignment for masquerade detection"[2]:

The masquerade attack, wherever Associate in Nursing assailant takes on the identity of a legitimate user to maliciously utilize that user privileges, poses a significant threat to the safety of knowledge systems. Such attacks utterly undermine ancient security mechanisms as a result of the trust imparted to user accounts once they need been documented. Several makes an attempt are created at police investigation these attacks; however achieving high levels of accuracy remains Associate in Nursing open challenge. During this paper, we have a tendency to discuss the utilization of a specially tuned sequence alignment rule, generally employed in bioinformatics, to notice instances of masquerading in sequences of laptop audit knowledge. By victimization the alignment rule to align sequences of monitored audit knowledge with sequences notable to possess been created by the user, the alignment rule will discover areas of similarity and derive a metric that indicates the presence or absence of

Masquerade attacks. in addition, we have a tendency to gift many rating systems, ways for accommodating variations in user behavior, and heuristics for decreasing the machine necessities of the rule. Our technique is evaluated against the quality masquerade detection dataset provided by Schonlau et al. and therefore the results show that the utilization of the sequence alignment technique provides, to our data, the simplest results of all masquerade detection techniques so far.

C. “CIDD: A cloud intrusion detection data set for cloud computing and masquerade attacks” [3]

Masquerade attacks create a significant threat for cloud system attributable to the large quantity of resource of those systems. Lack of datasets for cloud computing hinders the building of economical intrusion detection of those attacks. Current dataset cannot be used attributable to the heterogeneousness of user necessities, the distinct operative systems put in within the VMs, and also the information size of Cloud systems. This paper presents a Cloud Intrusion Detection Dataset (CIDD) that's the primary one for cloud systems which consists of each information and behavior based mostly audit information collectedfrom each operating system and Windows users. With relevancy current datasets, CIDD has real instances of host and network based mostly attacks and masquerades, and provides complete numerous audit parameters to make economical detection techniques. the ultimate datum tables for every user are designed by Log instrument and Co-relator System (LACS) that parses and analyzes user's binary log _les, and correlates audits information in keeping with user information science address and audit time. we tend to describe in details the parts and also the design of LACS and CIDD, and also the attacks distribution in CIDD.

D. Predicting sequences of user actions[4]:

People show regularities in nearly everything they are doing. This paper proposes characteristics of Associate in Nursing idealized algorithmic rule that, once applied to sequences of user actions, would enable a computer program to adapt over time to Associate in Nursing individual’s pattern of use. we have a tendency to describe a straightforward prophetic methodology with these characteristics and show its prophetic accuracy on an outsized dataset of UNIX commands to be a minimum of nearly as good as others that are thought of, whereas victimization fewer procedure and memory Resources.

3. SYSTEM MODEL

DDSGA may be a masquerade detection approach based mostly upon Enhanced-SGA. It aligns the user active session sequence to the previous ones of a similar user and it labels the placement areas as abnormal. A masquerade attack is signaled if the share of abnormal areas is larger than a dynamic, user dependent threshold. DDSGA will tolerate tiny mutations within the user sequences with tiny changes within the low level illustration of user commands and it's rotten into a configuration part, a detection part and an update one. The configuration part, computes, for every user, the alignment parameters to be utilized by each the detection and update phases. The detection part aligns the user current session to the sig nature sequence. The procedure performance of this part is improved by 2 approaches specifically the Top-Matching based mostly Overlapping (TMBO) and therefore the parallelized approach. within the update part, DDSGA extends each the user signatures and user lexicon list with the new patterns to reconfigure the system parameters

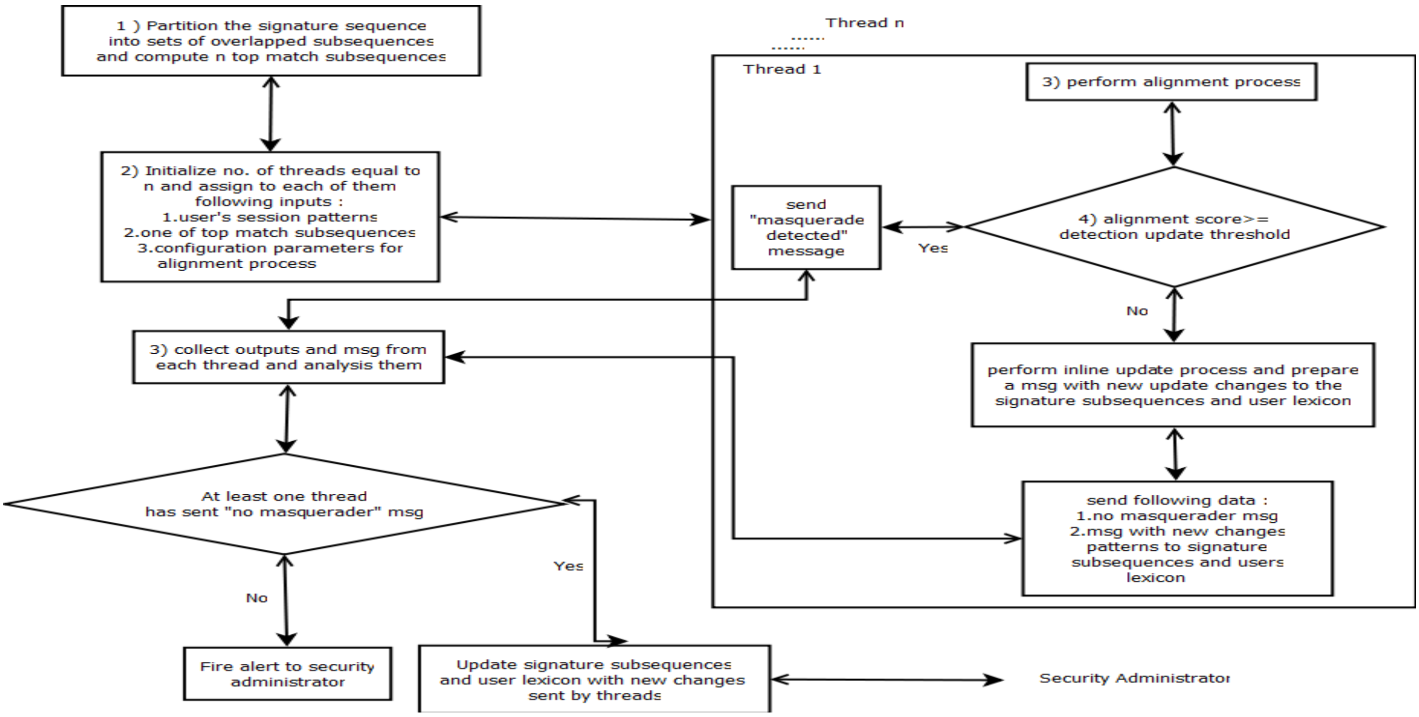
1) Partition the signature sequence into sets of overlapped subsequences and compute n top match subsequences
2) Initialize no. of threads equal to n and assign to each of them following inputs : 1.user's session patterns 2.one of top match subsequences 3.configuration parameters for alignment process
3) collect outputs and msg from each thread and analysis them
At least one thread has sent "no masquerader" msg
No
Yes
Fire alert to security administrator
Update signature subsequences and user lexicon with new changes sent by threads
Security Administrator
Thread n
Thread 1
3) perform alignment process
4) alignment score>= detection update threshold
Yes
No
send "masquerade detected" message
perform inline update process and prepare a msg with new update changes to the signature subsequences and user lexicon
send following data : 1.no masquerader msg 2.msg with new changes patterns to signature subsequences and users lexicon

Fig 1: System Architecture

4. CONCLUSION

Masquerading is far away one in every of the foremost vital attacks as a result of an aggressor which will with success logs to a system may also maliciously management it. The semi-global alignments (SGA) square measure based mostly upon sequence alignment and it's one in every of the foremost effective detection techniques which will be applied to distinct sequences of audit information. Whereas SGA might lead to low false positive and missing alarms rates, even its increased version has not however achieved the extent of accuracy and performance for sensible readying. This can be the rationale underlying the look of the info Driven Semi-Global Alignment Approach, DDSGA. From the safety potency perspective, DDSGA models additional accurately the consistency of the behavior of distinct users by introducing distinct parameters

REFERENCES

[1] H. Phyo and S. M. Furnell. A detection-oriented classi_cation of insider it

[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. 2433.

[3] S. E. Coulla and B. K. Szymanski, Sequence alignment for masquerade detection, J. Comput. Statist. Data Anal., vol. 52, no. 8, pp. 41164131, Apr. 2008.

[4] Monalisa 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. 1618.

[5] Yakov Amihud, Haim Mendelson, and Lasse Heje Pedersen. Liquidity and Asset Prices. Foundations and Trends in Finance, 1(4):269–364, August 2007.

[6] Brian D. Davison and Haym Hirsh, Predicting sequences of user actions, in Proc. Joint Workshop Predicting Future: AI Approaches Time Ser. Anal., 1998, pp. 512.