International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 1(J); January 2018; Page No. 9377-9381
DOI: http://dx.doi.org/10.24327/ijcar.2018.9381.1548

Research Article

HYBRID IDS APPROACH TO DEFEND HYPERVISOR ATTACKS

Shreyal Gajare and Shilpa Sonawani

Maharashtra Institute of Technology, Pune

A R T I C L E I N F O

Article History:

Received 9th October, 2017
Received in revised form 10th November, 2017
Accepted 26th December, 2017
Published online 28th January, 2018

Key words:

Virtualization, Hypervisor, Hypervisor Attacks, Intrusion Detection System, Apriori, K medoids

A B S T R A C T

Cloud Computing is a newly emerged technology. It is a solution for next generation of IT enterprise which enables ubiquitous, on demand and convenient access to pool of configurable resources. Along with reduced cost & complexity of applications or resources, cloud enables flexibility and scalability making it one of the exciting technologies. Virtualization is the major paradigm of cloud technology making it robust and flexible. It creates virtual versions of device or resource known as virtual machines which are shared amongst the available users. In virtual machines, hypervisor is a key element that is more prone to attacks. So, to protect these hypervisors and virtual machines a technique known as Intrusion Detection System (IDS) is used on large scale. IDS defend the attacks mostly occurring on virtual machines. Hence Virtual Machine Hypervisor based Intrusion Detection System (VMHIDS) is developed that can protect both hypervisors as well as virtual machines. This helps in early detection of attacks and can take preventive measures as soon as possible. In IDS, Hybrid IDS is chosen which can detect known and unknown class of attacks. It leads to better performance and efficiency of the system.

INTRODUCTION

With the rapid growth of technology there is increase in cybercrime. Due to the distributed nature of cloud intruders are also attracted towards their target. Virtualization provides the ability to run multiple virtual machines on single platform thus reducing costs and on demand access to resources. In VMs hypervisor is responsible to manage and control the access of resources provided to the users. Virtualized environments are usually implemented with the use of a Hypervisor, which is a software layer that lies between the Virtual Machines (VMs) and the physical hardware.The Hypervisor allocates resources to the VMs, such as main memory and peripherals. Thus as the hypervisor is attacked whole system is under threat.

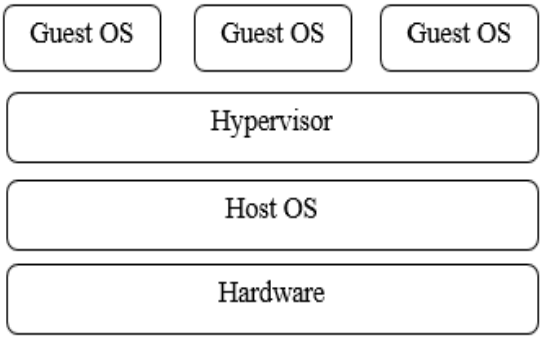

Fig 1 Hypervisor Overview

Corresponding author:* **Shreyal Gajare
Maharashtra Institute of Technology, Pune

Hypervisor is the single point of failure. Hence it should be carefully handled if any signs of compromise are observed. This work focusses on attacks on hypervisor and virtual machines.

The rise of the Cloud Computing paradigm has led to security concerns, taking into account that resources are shared and mediated by a Hypervisor which may be targeted by rogue guest VMs and remote attackers. The characteristic of cloud computing such as service transparency and flexibility have triggered the interest most of the organization to adopt the cloud services over storing their data information externally. Although the enormous researches about the common manners of the various malware have done in order to prevent vulnerabilities in the cloud computing. And yet the hypervisor attack is still concern by the cloud users.

The intent of this work is to find an approach which can defend hypervisor attack to a greater extent. Thus, IDS is used for early detection of attacks. In IDS methodologies are suggested which can be effective to mitigate the intruders.

Background

Hypervisor

Virtualization plays a vital role in the design of the cloud. However, there are many vulnerabilities existing in current virtualization technologies, which are inherent incloud implementations. These vulnerabilities allow an attacker to affect the securityand privacy of cloud resources as well as services. Thus, security and privacy aremajor concerns of the cloud. The hypervisor is the piece of software that

managesresources and isolates the VMs from each other. Hypervisor is known as virtualmachine monitor (VMM) that is responsible for managing the virtual machines inthe cloud environment. Hypervisor is a part of software that handles the resourcesshared among the virtual machines.

Hypervisor Attacks

A hypervisor attack is an exploit in which an attacker takes advantage of vulnerabilities in the program used to allow multiple operating systems to share a single hardware processor.If the intruder takes charge of single virtual machine, the other VMs running along with that attacked VM are affected thus affecting the hypervisor. The risks faced by hypervisors are VM sprawl, lack of visibility and control over virtual networks, resource exhaustion, unauthorized access to hypervisor, account or service hijacking through the self-service portal, risk due to cloud service provider API. In the end, all virtual machines will be affected gradually under the compromised hypervisor. The famous of the hypervisor attacks are BluePill, DKSM (Direct Kernel Structure Manipulation) and SubVirt.

Virtualization Attacks

In virtual environments, the attacker can take control of virtual machines installed by compromising the lower layer hypervisor. It is known that the Cloud Service Provider (CSP) is easily obtainable and this has beneficial for both cybercriminals and malevolent users. Without the virtualization, it is impossible for multiple users to communicate and share physical resources. Virtualization attacks can be of two types:

Insider Virtualization Attacks

Insider Attacker is the malicious user making wrong use of the knowledge regarding the cloud. This indirectly affects confidentiality, integrity and availability (CIA) of the CSP. These malicious usersalso lead to other types of insider attacks like communication within VMs, VM Escape etc.

External Virtualization Attacks

The external virtualization attacks can be caused due to any of the reasons like malicious attackers or the unauthorized access done by the intruders. The unauthorized access is obtained from cloud service provider. These include Breakout attack, hypervisor attacks, external alteration of VMs, etc.

Intrusion Detection System (IDS)

An IDS (Intrusion Detection System) is a software that automates the intrusion detection process and detects possible intrusions. The role of IDS in the security of cloud is very important since it acts as additional preventive layer of security and can detect various known attacks and unknown attacks. It is the process of monitoring the events taking place in the network and the system, and analyze the signs of intrusions. It captures data from the system or network under observation and notifies network manager by mailing or logging the intrusion event. The following figure depicts various IDS approaches in cloud system:

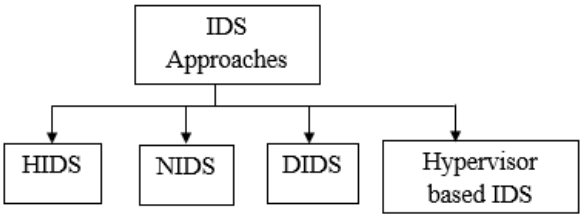

Fig 2 IDS cloud based classification

Host based Intrusion Detection System (HIDS)

HIDS is capable of monitoring and analyzing the internal computing of the system. This works for only host based sensors, and monitors only off host events. It records the new user entry and notifies unauthorized access.

Network based Intrusion Detection System (NIDS)

NIDS observes all the network based threats with network sensors. It reads all the network related packets i.e inbound packets and searches for any suspicious patterns. As the threat is found, based on its severity it takes possible actions notifying the administrator.

Distributed Intrusion Detection based System (DIDS)

DIDS is the self -monitoring system capable of detecting suspicious activity within the system by itself. It can contain many IDS combined together possessing detection component and correlation manager.

Hypervisor/VMM based Intrusion Detection System

HIDS is used to defend mainly hypervisor attacks in cloud. The layer between guest kernel and hypervisor is implemented by hypervisor based IDS. It observes the system metrics through cloud requests and detect any malicious events. The communication between VMs and hypervisor is observed by hypervisor and is effective in cloud.

Based on detection purpose IDS contains two major approaches which are widely used in network.

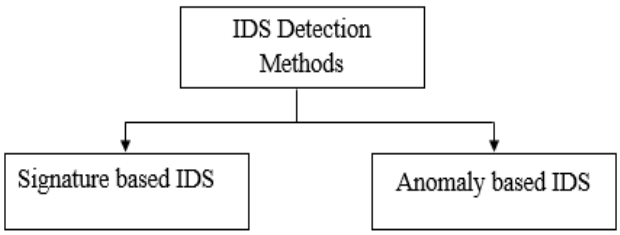

Fig 3 IDS approaches for detection

Signature based IDS

Signature based detection is performed by comparing the information collected from a network or system against a database of signatures. A signature is a predefined set of rules or patterns that correspond to a known attack. This technique is also known as misuse detection. It can efficiently detect known attacks with negligible false alarms. In Cloud environment, signature based intrusion detection method can be utilized at front-end (that is host) of cloud for detection of known attacks from external network.

Anomaly based IDS

Anomaly based detection compares current user activities against preloaded profiles of users or networks to detect abnormal behavior that may be intrusions. It detects intrusion by comparing observed activities with baseline profile without

signature database. The profiles may be dynamic or static and correspond to the expected or benign behavior of users.Anomaly based detection is effective against unknown attacks. In Cloud, unknown attacks can be detected at different levels by using anomaly detection technique.

Proposed Solution

Besides so many available methods in the market to protect cloud computing, they only protect cloud computing instead of hypervisors. Thus to develop an efficient tool to defend hypervisor attacks, IDS plays a vital role. Placement of IDS is an important phenomenon considered to define the level of defending the attacks. If IDS is placed on VMs it will only take care of external attacks and if it is placed on hypervisor it can defend only internal attacks. Thus by using hypervisor based IDS, IDS can be placed on both VMs as well as the hypervisor. This solution is known as Virtual Machine Hypervisor based Intrusion Detection System (VMHIDS).

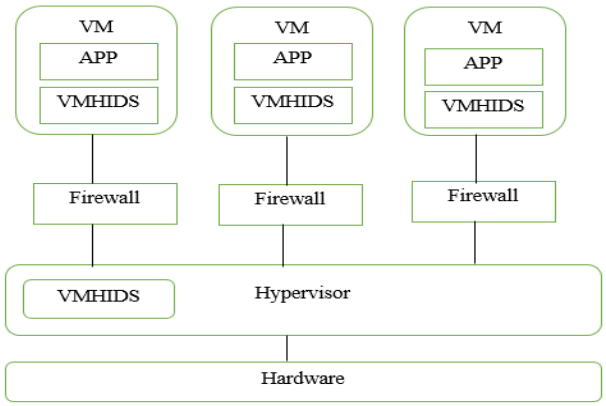

Fig 4 VMHIDS Architecture

Unlike Hypervisor-based IDS system, it isplaced on the hypervisor and its virtual machines to provide a more accurate detection of unsuspicious attacks. This approach protects both of the hypervisor and virtual machines from either insider or external attack on cloud environment. The continuous monitoring with VMHIDS from hypervisor or VMs enables to analyze real time events for automatic detect and block the malicious events. VMHIDS monitors and keep tracks on each file and process that communicate within the hypervisor in cloud computing.

In IDS, signature based and anomaly based techniques are used for detection of attacks. Both the methods have their advantages and disadvantages. For Signature method, signature database is mandatory thus cannot detect unknown attacks. In anomaly based detection process follows training and testing phases for real time attacks thus leading to generation of more false alarms. Hence Hybrid IDS is used for attacks detection in VMHIDS. It combines both, signature based & anomaly based methods with their advantages.

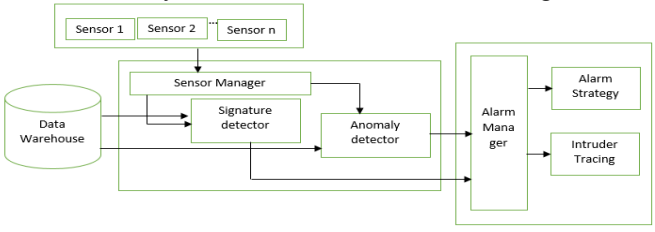

Fig 5 Hybrid Internal Implementation

A lot of research is going on in hybrid IDS methods. The need for a hybrid model contain the various attacks that can be used to create a data security breach must be considered. Common attacks that are utilized to carry out data breaches are SQL Injection (SQLI), brute-force, buffer overflows, Cross-Site Scripting (XSS), Remote File Inclusion (RFI), Directory Traversal (DT) and Cross-Site Request Forgery (CSRF).The efficiency of IDS can be significantly improved by combining signature based and anomaly based techniques which is called Hybrid detection technique.

Hybrid IDS model contains sensor manager which is responsible to sense the network for the data packets or audit data. After sensing the packets, it identifies whether it is known or unknown attack and then it forwards the attack to hybrid method containing both process signature and anomaly based within it. In Signature based method Apriori algorithm is considered and for anomaly K medoids is taken.

Apriori Algorithm

Apriori is an algorithm for frequent item set mining and association rule learning overdatabases. It proceeds by identifying the frequently items in the database and extending them to larger item sets as long as they appear sufficiently often in the database.The frequent item sets determined by Apriori can be used to determine associationrules which highlight general trends in the database: this has applications in domainssuch as market basket analysis. This algorithm helps in finding the accuracy of detected attacks for false positives and false negatives. This algorithm also improves thedetecting speed and accuracy and a more efficient approach to abnormal detectingattacks based on networking approach in the system and the knowledge base can beupdated automatically.

Algorithm

C_k : Candidate itemset of size k
L_k : frequent itemset of size k
L1 = frequent items;
for(k=1;L_k! = ϕ;k++) do begin
C_k+1 = candidates generated from L_{ki}
for each data packet p in database do
increment the count of all candidates in C_k+1 with min support that are contained in p
L_k+1 = candidates in C_k+1 with min support
end

K medoids Algorithm

The basic idea of this algorithm is to first compute the K representative objects which are called as medoids. After finding the set of medoids, each object of the data set is assigned to the nearest medoid. K-medoids algorithm is more robust to noise than K-means algorithm. A medoid can be defined as that object of a cluster, whose average dissimilarity to all the objects in the cluster is minimal.

Algorithm

Input: D dataset of n object
Output: Desired set of normal and abnormal clusters.
Begin

1. Standardize the dataset in order to make the feature value to appropriate range.

This is done because features with greater value dominate the features with lesser value.

2. Select initial medoids and for that the formula of Euclidean distance for dissimilarity measure has been used. It is given as under:

$dist_{ij}=\sum_{b=1}^{y}(zib - zjb)2$

Let x objects having y variables classifies into c clusters, compute,

$y_{ij} = \frac{distij}{\sum_{k=1}^{x} distik}$

After finding y_{ij} at each object and sorting them in ascending order, c objects are selected as the initial medoids having minimum value.

3. Associate each object to its closest medoid and calculate the optimal value as the sum of distances from all objects to their medoids.
4. Swap the current medoid in each cluster by the object which minimizes total distance to other objects in the cluster.
5. Again associate each object to the closest medoids and compute the new value as in step3. If the new value is same as previous one then stop the algorithm otherwise repeat step4.

Advantages of Apriori & K medoids algorithm

- Apriori enables usage of large itemset property i.e more number of data packetsof attacks can be considered for detection.
- Apriori algorithm works on association rules stored in the database and candetect the known type of attacks.
- K medoids reduces sensitivity to outliers. It minimizes the sum of dissimilaritiesbetween objects.
- K medoids is more robust in presence of noise and outliers.

Dataset Discussion

KDD-99 cup dataset is used to evaluate this work. This dataset contains 1000 connection records which consists of various attributes and their respective values. A few of the major attributes are duration, source bytes, destination bytes and protocol. These values are then checked for known or unknown sequence of bytes. If it is known then it is passed to frequent item set generation, otherwise passed to k medoids for finding out new patterns. K medoids calculates Euclidean distance to cluster the values and undergoes the training and testing phase.

Duration			Protocol		Service				Source bytes			
1	2	3	4	5	6	7	8	9	10	11	12	13
1	0	0	1	0	1	0	0	0	0	0	0	1
0	1	0	1	0	1	0	0	0	1	0	0	0
0	0	1	0	1	0	1	0	0	0	1	0	0
0	1	0	1	0	0	0	1	0	0	0	0	1
0	0	1	0	1	0	1	0	0	0	0	1	0
1	0	0	0	1	0	0	0	1	1	0	0	0

Fig 6 Network Data packets

1: Duration < 500
2: Duration < 1000
3: Duration >=1000
4: Protocol-TCP 5: Protocol-UDP
6: Service-FTP 7: Service-HTTP
8: Service-Telnet 9: Service-Others
10: Source bytes<10000
11: Source bytes<100000
12: Source bytes<280000
13: Source bytes>280000

IDS Placement Analysis

Hypervisor based IDS monitors the communications among VMs, between hypervisorand VM, and the virtual network. The table summarizes about the Cloud IDS types. As HIDS can be placed on only one node at once hence it provides good isolation but less variability. NIDS serves better as compared to HIDS in terms of deploying, efficiency, flexibility thus good in variability but no isolation at all. DIDS is able to detect the attacks over an entire network and reports to the centralized controller, thus increasing the loadon the controller. Hypervisor Based IDS can defend the attacks on both hypervisors and VMs (some extent). Only it possesses little complex design as it resides on the hypervisor.

Thus, there is an urgent need to take essential measures to prevent the data from getting exploited by applying any or a set of techniques with a clear view to seize or limit the attack or intrusion attempts. The need of the hour is that we should also achieve a highlevel of data security in all sorts of networks, among which there is still a huge group of static networks along with growing dynamic networks. Hence in this regard hybrid IDS is used that, providing a complete intrusion resistant package for a network.

CONCLUSION

Thus, Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS) is used for protecting from the hypervisor attacks. This approach ensures healthy state of virtual machine and hypervisor by detecting and eradicating intrusion in real time. It is followed that the hypervisor attack is categorized in the cloud infrastructure and external attack. Consequently, there are fiveexiting approaches such as virtual firewall, Intrusion Detection and Prevention Systems (IDPS), Network based IDS, Hosted-based IDS and Hypervisor-based IDS are used to compare along with their strength and weakness. An overview of Hybrid-IDS denotes the working on the anomaly based ids then it will generate a large no of false positive and false negative although it can detect unknown attacks but its performance is decreases due to large no of false positive and if we are working on signature based ids then it this is impossible to detect unknown attacks.So, to overcome this problem a hybrid ids isdeveloped which uses both anomaly and signature based ids to find out the unknownattacks and to raise the detection rate and lower false positive and false negative.Hence, Virtual Machines Hypervisor Intrusion Detection System is summarized toconquer the weakness found in the existing systems.

Future Scope

In the future, research should aim to provide new architectures, policies and techniques to maintain security on higher level for hypervisors. Newer hybrid IDS are being researched to ensure a more effective and efficient detection system. From the

comprehensive review, to extend existing solutions and to investigate new feasible solution different approaches can be used in hybrid intrusion detection systems at multiple end points of cloud. Even various hybrid techniques can also be compared for effective single solution. Along with attack detection, its prevention method can also be evaluated at different regions of cloud. Thus proper care should be taken to minimize the communication and computation overhead, while exchanging the intrusion evidences among multiple hosts in cloud.

References

1. C. Modi and K. Acha, Virtualization Layer Security Challenges and Intrusion Detection/ Prevention Systems In Cloud Computing: A Comprehensive Review, *the Journal of Supercomputing,* 2016.
2. A. Shameli-Sendi, M. Purzandi, M. Fekih-Ahmed and M.Cheriet, Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing, *Journal of Network and Computer Application,* vol. 58, pp. 165-179, 2015
3. J. Jabez and B. Muthukumar, Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, *Procedia Computer Science*, vol. 48,pp. 338-346, 2015.
4. W. Lin, S. Ke and C. Tsai, "CANN: An intrusion detection system based oncombining cluster centers and nearest neighbors", *Knowledge-Based Systems*, vol.78, pp. 13-21, 2015
5. E. Vasilomanolakis, S. Karuppayah, M. Mhlhuser and M. Fischer, "Taxonomy andSurvey of Collaborative Intrusion Detection", ACM Computing Surveys, vol. 47, no. 4, pp. 1-33, 2015.
6. S. Gautam and H. Om, Computational neural network regression model for Hostbased Intrusion Detection System, Perspectives in Science, vol.8, pp. 93-95,2016
7. S. Iqbal, M. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. Khan and K.Raymond Choo, On Cloud Security Attacks: A Taxonomy and Intrusion Detectionand Prevention as a Service, *Journal of Network and Computer Applications,* vol.74, pp. 98 120, 2016.
8. Muhammad S. Dildar, Nayeem Khan, J. Bin Abdullah, Adnan Khan, "Effective Way to Defend the Hypervisor Attacks in Cloud Computing", IEEE, 978-1-5090-5814-3, 2017.
9. O. Achbarou, M. Kiram and S. Bouanani, Securing Cloud Computing From Different Attacks Using Intrusion Detection System, *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, p. 61, 2016.
10. G. Nenvani and H. Gupta, "A survey on attack detection on cloud using supervised learning techniques", 2016 Symposium on Colossal Data Analysis and Networking (CDAN), 2016.
11. Bauman, G. Ayoade and Z. Lin, A Survey on Hypervisor- Based Monitoring ACM Computing Surveys, vol. 48, no.1, pp. 1-33, 2015.

How to cite this article:

Shreyal Gajare and Shilpa Sonawani *et al* (2018) 'Hybrid Ids Approach to Defend Hypervisor Attacks', *International Journal of Current Advanced Research,* 07(1), pp. 9377-9381. DOI: http://dx.doi.org/10.24327/ijcar.2018.9381.1548

****