International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Distributed Virtual Switch based Attack Detection and Countermeasure Selection for VM's

T. PUSHPAVATHI[*1] and D. ANUSHA[#2]

[*] *M.Tech (CSE), CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[#]*Asst Professor, Dept of CSE, CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[1]pushpa.thathireddy@gmail.com

[2]anureddyduddukunta@gmail.com

Abstract— Cloud computing provides service facilities to the consumers on demand. These services easily invite the attacker to attack by SaaS, PaaS,IaaS. Attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). At the SaaS level, the existing DDoS attacks uses analytical approaches to find the number of malicious packets thereby providing an impressive detection rate too. Though not optimal, many client puzzles are effectively defensive against the flooding attacks. At the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficultA defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. The patching known security holes in cloud data centers, have the privilege to control software installed on their managed VMs, might not work effectively and can violate the Service Level Agreement (SLA). Cloud users may install vulnerable applications on their virtual machines. In order to prevent the VM's in the cloud environment from being vulnerable, a multi-phase distributed vulnerability detection, measurement and counter selection measure selection mechanism called NICE is proposed. This scheme is based on a distributed programmable virtual switch to significantly improve attack detection and mitigate the attack consequences.

Keywords: Attack analysis, VM cloud security, Compromised machines, Spam zombies, DDoS attacks.

I. INTRODUCTION

As the technology is being emerged, Internet companies such as Google, Amazon, Microsoft and others, have acquired a considerable expertise in operating large data centers, the backbone of their businesses. Their know-how extends beyond physical infrastructure and includes experience with software, e.g., office suites, applications for process management and business intelligence, and best practices in a range of other domains, such as Internet search, maps, email and other communications applications.

Cloud Computing is the newly emerged technology of Distributed Computing System in which user concentrates on API security & provide services to its consumers in multitenant environment into three layers namely, Software as a service, Platform as a service and Infrastructure as a service, with the help of web services. It provides service facilities to its consumers on demand or pay-per-utility basis. In cloud computing, these services are hosted in a data center and commercialized, so that a wide range of software applications are offered by the provider as a billable service (Software as a Service, SaaS) and no longer need to be installed on the user's PC.

Cloud service providers gain an additional source of revenue, hence able to commercialize their expertise in managing large data centers.

The DDOS attacks such as HTTP & XML in this environment is dangerous & provides harmful effects for the consumer. For the intrusion detection systems that are introduced, the SOAP request is made between the communication between the client and the service provider. The proxy that marks the incoming packets with source message identification is used to identify the real client.

In the cloud environment, where the infrastructure is shared among millions of users, these attacks are more effective as the computing resources are shared using a switch, shared with data storage or files, etc.

In the proposed intrusion detection scheme, NICE (Network Intrusion detection and Countermeasure selection in Virtual network Systems), a framework for in-depth defence detection is implemented. This proposed work involves two phases:

1. A light-weight network intrusion detection agent to capture and analyze cloud traffic.

2. A Deep Packet Inspection for inspecting the VM's to make the behaviour of the potential attacks prominent.

This proposed work employs a novel attack graph approach for attack detection and prevention for correlating attacks and thereby suggesting the effective countermeasures for the same.

II. EXISTING SYSTEM

The major security challenge on the internet is the existence of large number of the compromised machines. These compromised machines are used to launch various attacks such as DDoS, spamming and Identity theft. Identifying and cleaning compromised machines in a network remain significant challenge with networks of various sizes.

The subset of compromised machines used for sending spam messages are referred to as spam zombies. The characteristics of the spamming botnets[4] is based on the sampled spam messages received at a large email service provider. The nature of the sequentially observing outgoing messages gives rise to the sequential detection problem. In order to monitor the outgoing messages, a spam zombie detection scheme named SPOT is designed, based on the Sequential Probability Ratio Test (SPRT). SPRT reaches to a decision based on the false positive and false negative probabilities bounded by a user threshold. SPRT mainly decides upon whether or not the host is compromised.

There are other existing schemes [5] which detect the compromised machines by allowing the correlated intrusion alarms that are triggered by the inbound traffic with resulting outgoing communication patterns. The well-defined stages including inbound scanning, exploit usage, egg downloading, outbound bot coordination dialog, and outbound attack propagation. Some of the other schemes exploit the spatial temporal behavior characteristics by grouping flows according to the server connections and search for the similar behavior. But when compared to Bothunter, SPOT does not need any support from the network intrusion detection system. Also SPRT is used to detect portscan activities; proxy based spamming activities, MAC protocol misbehavior in wireless networks.

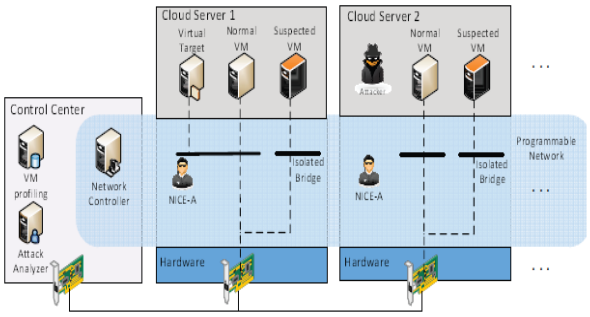
An attack graph is a modeling tool to illustrate all possible multi-stage, multi-host attack paths. An attack graph represents a series of atomic attacks that lead to an undesirable state where an attacker can obtain administrative access to a machine. In an attack graph, each node represents either a precondition or a consequence of an exploit. The attack graph provides the details of connectivity, all possible vulnerability information in a cloud system. If an event is recognized as a potential attack, we can predict or specify the countermeasures to mitigate the impact from contaminating the cloud system.

The existing attack-graph based correlation algorithm implements an alert dependency graph to group related alerts with multiple correlation criteria. But this consumes more power as it involves all pairs shortest path searching and sorting. For the cost benefit analysis several counter measures have been proposed. The first one is the attack countermeasure tree(ACT) to consider attacks and also the countermeasures in an attack tree structure. Several methods are also been designed based on greedy, branch and bound techniques to minimize the cost, number of countermeasures at the same time maximizing the benefit from implementing a counter measure set.

There are several other approaches [4] such as SDN programmed through software switch and open flow protocol, OVS and Open Flow switch (OFS) which supports fine-grained and flow level control for packet switching.

III. PROPOSED SYSTEM

The proposed model is a VM protection model based on a virtual network reconfiguration approach which utilizes attack graphs to model security threats and vulnerabilities.



.

Fig 1. Architecture of the IDS within one cloud server cluster

In the proposed system, the threat model assumes an attacker either located outside or inside of the virtual networking system. This work concentrates on virtual-network-based-attack detection and reconfiguration. This work can be deployed i n an IaaS cloud networking system where the cloud users are free to install whatever operating system and applications they want.

Two attack-based graphs are implemented say
1. Scenario Attack graph 2. Alert Correlation graph
1. Scenario Attack graph (SAG): SAG is a tuple where SAG= (V, E) such that V= NC ∪ ND ∪ NR
NC - conjunction node to represent exploit,
ND -disjunction node to denote result of exploit,
NR - root node NR for showing initial step of an attack Scenario.
E= Epre ∪ Epost denotes the set of directed edges.

2. Alert Correlation Graph (ACG): this is a 3-tuple ACG= (A, E, P) where A- set of aggregated alerts, E-set of directed edges, P-set of paths where Si ⊂ P in ACG.

The VM protection model consists of VM profiler, security indexer, and state monitor. The security index depends on various factors such as connectivity, number of vulnerabilities, impact scores. In this the connectivity metric of a VM is decided by evaluating incoming and outgoing connections. The VM states from the network controller can be defined as below:
1. Stable - does not exist any known vulnerability.
2. Vulnerable- presence of one or more vulnerabilities
3. Exploited - atleast one vulnerability is exploited and compromised
4. Zombie- a VM under the control of the attacker.

The framework is illustrated within one cloud server cluster. The core components network controller, attack analyzer and VM profiling server are kept under a centralized control that switches on each cloud server. NICE-A, a software agent in each cloud server controls the center through a dedicated and a isolated channel separated from the normal data packets using Open flow tunneling or VLAN approaches. This network intrusion detection engine can be installed either in a Dom0 or DomU of a XEN cloud server to capture and filter malicious traffic. The intrusion dtection alerts are sent to control center when suspicious or anomalous traffic is detected. Once the alert has been received, the attack analyzer evaluates the severity of the alert based on the attack graph. This attack graph derives the vulnerability information for both offline and real time attacks.

The NICE-A agent installed on either Dom0 or DomU in each cloud server scans the traffic going through Linux bridges that control all the traffic among VM's. The Snort technique used in Dom0 sniffs a mirroring port on each virtual bridge in the OpenvSwitch. Further the traffic generated from the VM's on the mirrored software bridge will be mirrored to a specific port on a specific bridge using SPAN,RSPAN,ERSPAN methods.

The major functions by attack analyzer includes procedures such as attack graph construction and update, alert correlation and countermeasure selection.

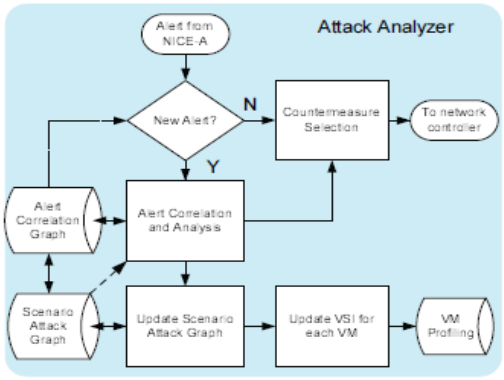


Fig 2: Workflow of attack analyzer

The attack analyzer handles alert correlation and analysis operations. From the above fig. after receiving an alert from the NICE-A, it matches with the alert in the ACG. If the alert already exists and matches with the attack signature, the attack analyzer then provides countermeasures and immediately notify the network controller to perform mitigate functions. If the alert is new then it updates the SAG and ACG and the countermeasure is applied based on the severity of evaluation results. If a severe alert is triggered and identifies some known attacks, or a VM is detected as a zombie, the network controller will block the VM immediately. And an alert with medium threat level is triggered by a suspicious compromised VM. In order to intercept the VM's normal traffic, suspicious traffic to/from the VM will be put into inspection mode, in which actions such as restricting its flow bandwidth and changing network configurations will be taken to force the attack exploration behavior to stand out.

Algorithm 1: Countermeasure selection

Require: $Alert, G(E,V), CM$
Let v_{Alert} = Source node of the $Alert$
if Distance_to_Target(v_{Alert}) $> threshold$ **then**
  Update_ACG
  return
end if
Let $T = Descendant(v_{Alert}) \cup v_{Alert}$
Set $Pr(v_{Alert}) = 1$
Calculate_Risk_Prob(T)
Let $benefit[|T|,|CM|] = \emptyset$
for each $t \in T$ **do**
  for each $cm \in CM$ **do**
    if $cm.condition(t)$ **then**
      $Pr(t) = Pr(t) * (1 - cm.effectiveness)$
      Calculate_Risk_Prob($Descendant(t)$)

$$benefit[t, cm] = \Delta Pr(target\_node).$$

    end if
  end for
end for
Let $ROI[|T|,|CM|] = \emptyset$
for each $t \in T$ **do**
  for each $cm \in CM$ **do**

$$ROI[t, cm] = \frac{benefit[t, cm]}{cost.cm + intrusiveness.cm}.$$

  end for
end for
Update_SAG and Update_ACG
return Select_Optimal_CM(ROI)

IV. CONCLUSION

The proposed IDS scheme detects and mitigates the collaborative attacks in the Cloud virtual network environment. The attack graph model conducts the attack detection and prediction. This solution explores the use of programmability of software switches based solution which improves the detection accuracy and strongly resist the collaborative attacks. The traffic can be handled for one cloud server and also can be extended to a large system. The implementation is based on mirroring and proxy-based attack detection agents. The NICE-A agent removes the traffic duplication and performs packet checking. The security status of a VM is also known such that the VM's with higher VSI values are to be monitored closely and the mitigation strategies need to be applied appropriately.

Host-based IDS solutions can be incorporated as a part of the future work. Also the future scope can be extended for a decentralized network control and an attack analysis model.

REFERENCES

[1] NICE: Network Intrusion Detection and CountermeasureSelection in Virtual Network Systems, Chun-Jen Chung, Student Member, IEEE, Pankaj Khatkar, Student Member, IEEE, Tianyi Xing, Jeongkeun Lee, Member, IEEE, and Dijiang Huang Senior Member, IEEE, IEEE transactions on Dependable and secure computing

[2] Cloud Security Alliance, "Top threats to cloud computing v1.0 "https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, March 2010.

[3] B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," IEEE Int'l Conf. computer Communication and Informatics (ICCCI '12), Jan. 2012.

[4] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J.Barker, "Detecting spam zombies by monitoring outgoing messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198–210, Apr. 2012.

[5] G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," Proc. of 5th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.