ZOMBIE ATTACK DETECTION AND COUNTERMEASURE SELECTION IN CLOUD ENVIRONMENT

Rakshitha C M
M tech (computer networks), Department of Computer Science and Engineering,
Siddaganga Institute of Technology, Tumkur, Karnataka, India.
rakshitha.1si14scn11@gmail.com

Abstract

Cloud security is one of the most evolving sub domain of recent research and development in network security. attackers explore the vulnerabilities in cloud system intially, later it compromise the virtual network to deploy large scale Distributed Denial of Service(DDoS). Distributed Denial of Service attacks usually include multistep exploitation, low frequency vulnerability scanning and compromising vulnerable virtual machines as zombies. the detection of zombie attacks are extremely difficult in the Infrastructure as a Clouds(IaaS) since cloud user gets access to install the vulnerable applications to their managed virtual machines. proposed framework uses a multiphase vulnerability detection and counter measure selection to prevent zombie attacks, where proposed system incorporates attack graph analytical model and reconfigurable virtual networking techniques. this framework also exhibits the feature of Open Flow network programming APIs and open flow protocol manages both the control plane and forwarding plane efficiently

Index Terms: Network security, cloud computing, intrusion detection, attack graph, zombie detection.

I. INTRODUCTION

Cloud security is the most important factor so that the users can rely on cloud. Cloud Security Alliance(CSA) is an organization which gives the security measures for cloud usage. CSA survey shows that the iniquitous use of cloud computing is the top most security threat among all the security issues. System administrators had complete control over host machines in traditional data centers and they have handled the vulnerabilities in a centralized manner. where cloud users has privilege to control software installed on their Virtual Machines(VMs). So that the cloud user can install vulnerable software on their VMs, it may violate the Service Level Agreement(SLA) sometimes and there will be a security breach in Cloud. Attackers always try to attack and compromise multiple virtual machines. Proposed system has network intrusion detection and prevention measures for virtual network systems. It constructs a defense in depth intrusion detection framework. The design of proposed system does not intend to enhance the existing intrusion detection mechanisms, instead it employs the reconfigurable virtual networking approach for intrusion detection and counter measures to prevent it, hence the proposed mechanism prevents the zombie attack. This framework has less computational overhead over proxy based intrusion detection mechanisms.

Proposed framework has 2 main phases. It employs a light weight network intrusion detection agent on cloud server to monitor the cloud traffic and scans the vulnerabilities, attacks to establish Scenario Attack Graph(SAG). Based on how onerous the attack is, the framework decides that virtual network should be under inspection state or not. If a virtual network goes under inspection, Deep Packet Inspection is applied and virtual network reconfiguration takes place.

II. EXISTING WORK

Many existing counter attacks are there for zombie detection and prevention.

A. Securing Cloud Computing Environment Against DDoS Attacks

In this paper[1], they used Cloud trace back model[1] to verify the request coming from legitimate user, which is based on Deterministic Packet Marking algorithm(DPM). It marks the ID field and reserved flag within IP header and incoming packet will be marked, it also traverse the packet through out the network.CTB is placed at the edge routers, if no security services are there, the system becomes vulnerable to attacks.CTB does not directly eliminate DDoS attack instead it uses cloud protector which has virtual firewall. Where virtual firewall maintains white list and black list of source IP addresses**.** White list is used to tack the authenticated source IP addresses and this will be allowed to pass the firewall towards destined services and black list holds the unauthenticated source IP addresses and does not allowed to pass the firewall.

B. *Detecting spam zombies by monitoring outgoing messages(IEEE Trans 2012)*

Duan introduces SPOT[2] approach to detect the compromised machines in a network that are involved in spamming activities, by monitoring outgoing messages. SPOT is based on the powerful statistical tool called sequential probability ratio test(SPRT). SPRT is a random walk between false +ve and false –ve error rates, where these error rates are user defined. When walk reaches either of the boundaries for the first time, the walk will be terminated and corresponding hypothesis will be taken into consideration. SPRT requires large number of observations before it reaches smaller error rates. Evaluation studies shows that the SPOT is an effective system in automatically detecting compromised machines in a network. SPOT has 2 different algorithms to detect the zombie attack. one is Count Threshold(CT) detection algorithm which is based on the number of spam messages and another one is Percentage Threshold(PT) detection algorithm which is based on the number of spam messages sent from the internal machine.

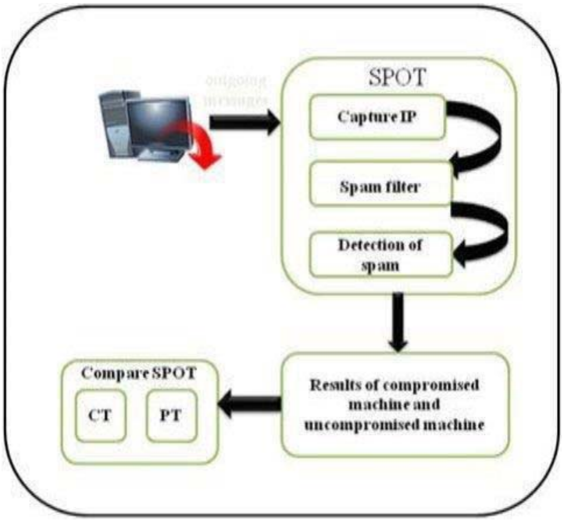

Fig 1: SPOT

C. MulVAL: A Logic-Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005:

MULVAL[3] is constructed by accumulating true facts of the monitored network system. Where Datalog is the modeling language of MULVAL. The reasoning engine consists of a collection of Datalog rules that captures the operating system behavior and the interaction of various components in the network. The reasoning engine in MulVAL goes well with the size of the network. Once the whole information is collected, the analysis can be performed with thousands of machines in a few seconds. But this process will terminate efficiently, because the facts are polynomial in nature, so proposed system approach modifies this and uses extended mulval.

D. *Automated generation and analysis of Attack Graphs:*

Attack graph[4] is able to represent a series of exploits called atomic attacks. There are many automation tools to construct an attack graph. And these attack graph can generate all possible attack paths but scalability is a big issue. To evaluate this we have *Dynamic security risk management using Bayesian Attack Graphs(BAG):*conventional network security planning and management starts with risk analysis, which decides threats to critical resources and the corresponding loss. But majority of the conventional models failed to achieve this by using attack graphs and attack trees. BAG selects the notion of Bayesian belief networks which gives the different security Conditions during the system compromise. This model includes the cause and consequence relationships between the different network states. It also gives the possible ways to exploit such relationships. The estimation mechanism has been proposed to evaluate the security risks from various vulnerability factors based on the metrics defined in the Common Vulnerability Scoring System(CVSS). This model has genetic algorithm. The algorithm comprises the mitigation plans for both single and multi objective analysis. At last this model provide a platform for both static and dynamic risk analysis in network. Above all these scalability is the issue here.

Disadvantages of Existing System:

But all these approaches concentrates on static attack scenarios and predefined solution for each attack. And these are inefficient to handle new vulnerabilities. No detection and prevention framework in a virtual networking environment.

No accuracy mechanism in the attack detection.

III. PROPOSED WORK

The proposed framework uses defence in depth intrusion detection, which incorporates attack graph analytical procedures. This framework is not improving any of the existing algorithms; instead it employs a reconfigurable virtual networking approach to prevent attempts to compromise virtual machines. Proposed system utilizes a new network control approach called Software Defined Networking(SDN). In SDN, networking functions can be programmed through software switch and open flow protocol[6]. Proposed system built on attack graph-based analytical models and reconfigurable virtual network using *Alert correlation*, *SAG* and *DPI*. It does not involve host based IDS. And it assumes that hypervisor is free of any vulnerabilities.

Proposed framework has 2 models.

Threat model: This model assumes that attacker can be located either outside or inside of the virtual networking system. Attacker's major concern is about exploiting vulnerable virtual machines and compromise them as zombies.

Attack graph model: This is a modelling tool to find all possible multistage, multiport attack paths and it is helpful to decide appropriate counter measures. This model extend the notation of MULVAL and construct it as Scenario Attack Graph(SAG).

Definition1: SAG is a 2 tuple structure i.e SAG=(V,E) where $V=N_C$ U N_D U N_R these 3 are set of vertices. NC is a conjunction node which represents exploit, N_D is a disjunction node which represents result of exploit, NR is a root node which represents initial step of attack.

$E=E_{pre}$ U E_{post} denotes the set of directed edges. These edges exist when N_c satisfied to achieve N_D and N_D can be obtained if N_c is satisfied.

Definition2: Alert correlation graph(ACG) is to correlate the alerts.ACG is a 3 tuple structure. i.e ACG=(A,E,P), where A is a set of aggregated alerts i.e a ϵ A is a data structure (src,dst,cls,ts). Contains source IP address, destination ip address, type of the alert and time stamp of the alert.

E is a set of directed edges which represents correlation 1 between two alerts (a,a). P is a set of paths i.e Si C P which represents set of related alerts in chronological order. There is a algorithm for alert correlation to keep track of new alerts, correlated alerts and paths.

Algorithm 1. Alert_Correlation Require: alert a_c, SAG,ACG

```
If($a_c$ is a new alert) then
    Create node $a_c$ in ACG
    n1<-Vc ϵ map(ac)
    for all n2 ϵ parent(n1) do
        create edge(n2.alert,$a_1$)
        for all $S_i$ containing a do
            if a is the last item in $S_i$ then
                append ac to $S_i$
            else
                create path $S_{i+1}$={subset($S_i$,a),$a_c$}
            end if
        end for
        add $a_c$ to $n_1$.alert
    end for
end if
return S
```

Mitigation strategies for zombie attack

Counter measure strategies: Attack analyzer initiates the counter measure selections for zombie attacks in cost effective manner. Proposed framework is able to construct the mitigation strategies in response to detected alerts. This strategy has countermeasure pool, which is defined as follows.

Countermeasure pool: A counter measure pool $CM=\{Cm_1,Cm_2,.....Cm_n\}$ is a set of countermeasures. Each cm £ CM is a tuple cm = (cost, intrusiveness, condition, effectiveness), where Cost is the unit that describes the expenses require to apply the counter measure, its value ranges from 1 to 5, and higher metric means higher cost.

Intrusiveness is the negative effect that a counter measure brings to the SLA and its value ranges from 1(least intrusive) to 5(most intrusive). Value of intrusiveness will be 0 if the countermeasure has no impacts on SLA.

Condition is the requirement for the corresponding countermeasure.

Effectiveness is the percentage of probability changes of the node, for the particular countermeasure is applied.

There are many counter measures that can be applied to the cloud environment. But our aim is to select optimal countermeasure. The optimal countermeasure selection is a multi-objective optimization problem, where it needs to find the MIN(impact, cost) and MAX(benefit). 1 to 5,and higher metric means higher cost.

Intrusiveness is the negative effect that a counter measure brings to the SLA and its value ranges from 1(least intrusive) to 5(most intrusive). Value of intrusiveness will be 0 if the countermeasure has no impacts on SLA. Condition is the requirement for the corresponding countermeasure.

Effectiveness is the percentage of probability changes of the node, for the particular countermeasure is applied.

There are many countermeasures that can be applied to the cloud environment. But our aim is to select optimal countermeasure. The optimal countermeasure selection is a multi-objective optimization problem, where it finds the MIN(impact, cost) and MAX(benefit) using Return of Investement(ROI) mechanism.

IV. SYSTEM ARCHITECTURE

This section describes the system design overview and detailed description of its components. The proposed framework is illustrated in the figure.

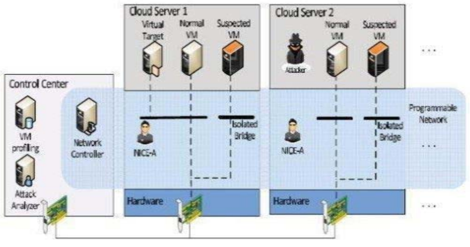

Fig 2: NICE

Network controller is responsible for deploying counter measures for attacks based on the decision made by the attack analyzer.

VM profiling in the cloud is there to get detailed information about the network state, services running, open ports and so on. Care must be taken for ports since port-scanning program can be used by attacker to check open ports.

Attack analyzer performs the major functions which includes constructing the attack graph, alert correlation and counter measures for particular attack.

The detection and mitigation of zombie attack can be achieved from the following scenario.

Network intrusion detection: Intrusion detection is a software agent implemented on each cloud server. It captures and filter malicious traffic.

Control centre : Intrusion detection alerts are sent to control centre. it deploys the counter measures for attack according to decision made by the attack analyzer.

Attack graph: Attack graph is established according to the vulnerability information.

Attack analyzer: Attack analyzer evaluates how dangerous the alert is, based on attack graph, It decides about the counter measure strategies, then invokes the strategies through the network controller.

Dynamic nature of attack graph: Attack graph will be reconstructed dynamically based on new vulnerabilities.

V. SYSTEM CONFIGURATION

Hardware requirements:

Processor	: Pentium –IV
Speed	: 2.4 GHz
RAM	: 500 MB(min)
Hard Disk	: 20 GB(min)

Software requirements:

Operating system	: Windows
Tool	: Eclipse
Platform:	Java/Swings
Database	: Oracle

VI. CONCLUSION

NICE framework is proposed to detect and mitigate the attacks in the virtual networking environment. The framework uses the attack graph model for attack detection and this framework uses the programmability of software switches to improve detection accuracy and defeat the attacks. hence proposed framework demonstrates the feasibility of NICE compared to other existing system and the framework has following contributions. Dynamic nature of attack graph is the most important feature in detecting new type of attacks. It captures and inspects the malicious cloud traffic without interrupting the ongoing user's cloud services. It also optimizes the implementation on cloud environment from minimized resource consumption.

REFERENCES

[1] Coud Sercurity Alliance, "Top Threats to Cloud Computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, Mar. 2010.

[2] B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf.Computer Comm. and Informatics (ICCCI '12), Jan. 2012.

[3] 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.

[4] X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic- Based Network Security Analyzer, " Proc. 14th

USENIX Security Symp., pp. 113-128, 2005

[5] Dynamic Security Risk Management Using Bayesian Attack Graphs IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012

[6] Open Networking Fundation, "Software-Defined Networking: The New Norm for Networks, " ONF White Paper, Apr. 2012.

.