ISSN: 2321-7782 (Online)

Volume 3, Issue 4, April 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Network Intrusion Detection and Countermeasure Selection in Virtual Private Network Systems

Sanjana B.G[1]
Dept. of CSE
BMSCE
Bengaluru, India

Anjali Vats[2]
Dept. of CSE
BMSCE
Bengaluru, India

Suriya Fathima[3]
Dept. of CSE
BMSCE
Bengaluru, India

Shruthi Shetty[4]
Dept. of CSE
BMSCE
Bengaluru, India

Madhavi R.P[5]
Associate Professor,
Dept. of CSE
BMSCE
Bengaluru, India

***Abstract:** There is an increasing demand nowadays to connect to internal networks from different regions. Employees often connect to internal private network over the insecure Internet from home, hotels or from any other external network. When business partners have constant access to internal networks from insecure external locations,security is the major factor. VPN (Virtual Private Network) technology provides a way of protecting information being sent over the Internet, to securely enter in a network by allowing users to establish a virtual "tunnel" for accessing resources, data and communications via insecure network such as the Internet [1]. VPNs carry sensitive information over an insecure network.*

In order to enable VPN use in real and large scale environments,It is necessary to provide protection to VPN infrastructures. The networking systems are under threat from network attackers. Denial-of-service (DoS) attack is one of the most common type of attack which causes serious impact on these computing systems.Attackers can explore vulnerabilities of the system and compromise virtual machines which leads to the large-scale Distributed Denial-of-Service (DDoS). DDoS attacks involve early stage actions which include low frequency vulnerability scanning, multi-step exploitation and identifying zombies.

An Intrusion detection system (IDS) pertains to the methods used to identify an attack on a computer or computer network. To prevent vulnerable virtual machines from being compromised, we have proposed Network intrusion detection system .It is multi-phase distributed vulnerability detection and countermeasure selection mechanism built on attack graph based analytical models and reconfigurable virtual network-based countermeasures. The security and system evaluations demonstrate the efficiency and effectiveness of the proposed solution. We discuss the potential security risks as well as the security considerations that need to be taken into account when implementing a virtual private network.

***Keywords:** VPN, Network Security, Intrusion Detection system, DOS, Attack Graph, Zombie Detection.*

I. INTRODUCTION

A VPN is a private network that uses a public network(usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site[2]. VPN are very flexible in terms of growing with the company and adding new user to the network. VPNs can be broadly categorized into firewall-based VPN , software based VPN , hardware based VPN and SSL VPN[3,4,5]. We are currently implementing the firewall based VPN that makes use of the security mechanisms in firewalls to restrict access to an internal network.

Businesses have lost productivity and millions of dollars for not having a secure network. In contrast to the benefits brought by VPN, the shared use of routing devices and communication channels introduces a series of security related concerns. Without an adequate protection, users from a network might be able to access or even interfere with traffic that belongs to other virtual networks, violating security issues such as confidentiality and integrity[6,7] . Additionally, the infrastructure could be a target for denial of service attacks (DOS), causing availability issues for virtual networks instantiated on top of it [8]. Therefore, it is of great importance that network virtualization architectures offer protection against these and other types of threats that might compromise security.

DENIAL-OF-SERVICE attack is one of the most common types of attack on servers. DoS attacks, usually reduces the availability of resources to the victim. Large computation tasks are imposed by the attackers by flooding it with huge rate of duplicate packets[9] resulting in the victim being forced out of network service for several days. This leads to serious problem. There are many types of DoS attacks [10]. Network level, Application level and Data level attacks are dealt with in DoS attack detecting system.

A variety security product such as firewalls, scanners to conduct vulnerability assessment and intrusion detection systems are available for businesses to protect their VPN from attackers. Protection is not provided by the firewalls for the malicious activities happening inside the network[11]. The purpose of an intrusion detection system is to build normal patterns of a normal system and triggers an alert when abnormal patterns or anomalous activities are detected. An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer system and networks. An IDS inspects all the inbound and outbound activities of the network along with detecting suspicious patterns that indicate an attack which can lead to zombies. Intrusion Detection Systems are configured to send an alert to a human being when they detect suspicious activity[12]. Various types of alerts can be used, from the entries in log files to e-mail or text messages sent by SMS.

There are two different Intrusion Detection Systems :

» Host Based - Intrusion Detection System is installed on a host in the network. It collects and analyzes the traffic that is originated or is intended to that host.

» Network Based - Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host or network. And it has the capability of monitoring the network and detecting the malicious activities intended for that network.

In this article, we propose Network Intrusion detection and Countermeasure selection in virtual private network systems to establish a defense-in-depth intrusion detection framework. For attack detection, It incorporates attack graph based on analytical procedures into the intrusion detection process. We must note that the design of Network Intrusion detection and Countermeasure selection in virtual private network does not intend to improve any of the existing intrusion detection algorithms. Indeed, It makes use of reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, hence preventing zombie VMs.

In general, It includes two main phases: (1) deploy a lightweight mirroring-based network intrusion detection AGENT on each server to capture and analyze traffic. An AGENT periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability towards the collaborative attack goals, Network Intrusion detection and Countermeasure selection in virtual private network will decide whether to put a VM in network inspection state. (2) Once a VM enters into inspection state, Deep Packet Inspection (DPI) is applied, virtual network reconfigurations can be deployed to the inspecting VM to make the potential attack behaviors prominent.

This model significantly advances the current network IDS/IPS solutions by employing programmable virtual networking approach. It constructs a mirroring-based traffic capturing framework to minimize the interference on users traffic compared to traditional (i.e., proxy-based) IDS, by using software switching techniques [13]. The programmable virtual networking architecture of Network Intrusion detection and Countermeasure selection in virtual private network enable the VPN to establish inspection and quarantine modes for suspicious VMs based on the current SAG. Depending on the collective behavior of VMs in the SAG, Network Intrusion detection and Countermeasure selection in virtual private network decides on appropriate actions. It does not need to block traffic flows of a suspicious VM in its early attack stage. The advantages of are presented below:

» We construct, a new multi-phase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious traffic without interrupting users applications and services.

» It incorporates a software switching solution to inspect suspicious VMs for further investigation and protection of the VMs. It can also improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal services through programmable network approaches.

» It makes use of a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.

» It enhances the implementation on servers to minimize resource consumption. Study shows that this model consumes less computational overhead compared to proxy-based network intrusion detection solutions.

II. Survey

1. Related work

we concentrate on literatures of several highly related research areas to Network Intrusion detection and Countermeasure selection in virtual private network, including: zombie detection and prevention, attack graph construction and security analysis, and software defined networks for attack countermeasures.

Effective detection of DDoS attacks is mandatory for the protection of network services to prevent DoS attack. There are various types of detecting systems , they are network based detecting system and host based detecting system. Network based detecting system is better to use. Generally, network-based detection systems can be classified into two main categories, namely, misuse-based detection systems [14] and anomaly based detection systems [15]. We are addressing the network based detection system. The area of detecting malicious behavior has been well investigated. work by Duan et al. [16] focuses on the detection of compromised machines that have been recruited to serve as spam zombies. To tackle with this, SPOT is used which is based on sequentially scanning outgoing messages while employing a statistical method Sequential Probability Ratio Test (SPRT), to quickly determine whether or not a host has been compromised.

An attack graph is able to represent a series of exploits called atomic attacks, that signals to an unappealing state, for example a state where an attacker has acquired administrative access to a machine. There are various automation tools to construct attack graph. O. Sheyner et al. [17] recommends a technique based on a modified symbolic model checking NuSMV [18] and Binary Decision Diagrams (BDDs) to construct attack graph. Also this model can generate all possible attack paths, though, the scalability is a big issue for this solution. P. Amman et al. [19] tabled the assumption of monotonicity, in which states that the precondition of a given exploit is never invalidated by the successful application of another exploit. In simple words, attackers never need to backtrack. With this theory, they can procure a concise, scalable graph representation for encoding attack tree. X. Ou et al. come up with an attack graph tool called MulVAL [20], which adopts a logic programming approach and uses Data log language to model and analyze network system. The attack graph MulVAL is designed by accumulating true facts of the monitored network system. The process of attack graph construction will terminate efficiently because the number of facts is polynomial in system. In a way to provide the security assessment and alert correlation feature. In this paper, we have modified and extended MulVAL's attack graph structure.

Intrusion Detection System (IDS) and firewall are widely used to monitor and detect suspicious events in the network. Yet, the false alarms and the large volume of raw alerts from IDS are two major problems for any IDS implementations. In order to identify the target of the intrusion in the network, mainly to detect multi-step attack, the alert correction is an important tool. The prime goal of alert correlation is to provide system support for a global and condensed view of network attacks by analyzing raw alerts [21].

Many attack graph based alert correlation techniques have been proposed recently. L. Wang et al. [22] devised a queue graph (QG), to trace alerts matching each exploit in the attack graph. Yet, the implicit correlations in this design makes it difficult to use the correlated alerts in the graph for analysis of similar attack scenarios. Roschke et al. [23] proposed a modified attack-graph-based correlation algorithm to create explicit correlations only by matching alerts to specific exploitation nodes in the attack graph with multiple mapping functions and devised an alert dependencies graph (DG) to group related alerts with multiple correlation criteria. Each path in DG signifies a subset of alerts that might be part of an attack scenario. Still, their algorithm involved all pairs shortest path searching and sorting in DG, which consumes considerable less computing power.

After knowing the possible attack frameworks, applying countermeasure is the next important task. Several solutions have been tabled to select optimal countermeasures based on the likelihood of the attack path and cost benefit analysis. A. Roy et al. [20] tabled an attack countermeasure tree (ACT) to consider attacks and countermeasures together in an attack tree structure. They devised several functions based on greedy and branch and bound techniques to minimize the number of countermeasures, reduce investment cost and maximize the benefit from implementing a certain countermeasure set. In this design, each countermeasure optimization problem could be solved with and without probability assignments to the model. Although, the solution focuses on a static attack scenario and predefined countermeasure for each attack. N. Poolsappasit et al. [22] tabled a Bayesian attack graph (BAG) to address dynamic security risk management problem and applied a genetic algorithm to solve countermeasure optimization problem.

Our solution utilizes a new network control approach called SDN [23], where networking functions can be programmed through software switch and Open Flow protocol [24], plays a major role in this research. Flow- based switches, such as OVS [5] and Open Flow Switch (OFS) [23], support fine-grained and flow-level control for packet switching [25]. With the help of the central controller, all Open Flow-based switches can be examined and configured. We take an advantage of flow based switching (OVS) and network controller to apply the selected network countermeasures in our solution.

2. Network Intrusion Detection Models

Here, we describe how to utilize the attack graphs to model security threats and vulnerabilities in a virtual networked system, and propose a VM protection model based on virtual network reconfiguration approaches to prevent VMs from being exploited.

2.1 Threat Model

In our attack model, we assume that an attacker can be located either outside or inside of the virtual networking system. The attacker's primary goal is to exploit vulnerable VMs and compromise them as the zombies. Our protection model focuses on virtual-network-based attack detection and reconfiguration solutions to improve the resiliency to zombie exploration attacks. Our work doesn't involve host-based IDS and neither does it address how to handle encrypted traffic for attack detections.

The service users are free to install whatever applications they want, even though such action may introduce vulnerabilities to their controlled VMs. Physical security of server is out of scope of this paper. We assume that hypervisor is secure and free of any vulnerabilities.

2.2 Attack Graph Model

An attack graph is a modeling tool .It illustrate all the possible multiple stage, multiple host attack paths that are crucial to understand threats and then to decide appropriate countermeasures [28]. In an attack graph, each node represents either precondition or consequences of an exploit. The actions need not necessarily be active attack since normal protocol interactions can also be used for the attacks. Attack graph is helpful in identifying possible attacks, potential threats and known vulnerabilities.

Since the attack graph provides details of all known vulnerabilities in the system and the connectivity information, we will get a whole picture of current security situation of the system where we can predict the possible threats and attacks by correlating detected events. If an event or activity is recognized as a potential attack, we can apply countermeasures to mitigate its impact or take actions to prevent it from contaminating the systems. To represent the attacks and the result of such actions, we extend the notation of MulVAL logic attack graph as presented by X. Ou et al. [24] and define it as Scenario Attack Graph (SAG).

2.3 VM Protection Model

The VM protection model of Network Intrusion detection consists of a state monitor, a security indexer and a VM profiler. We specify security index for all the VMs depending upon various factors that include connectivity, the number of vulnerabilities present and their respective impact scores. As defined in the CVSS guide the impact score of a vulnerability [27], helps judge the confidentiality, integrity, and availability impact of the vulnerabilities being exploited. Incoming and outgoing connections to the VM's are evaluated to decide on connectivity metric of a VM.

III. CONCLUSION

In this paper, we presented Network Intrusion detection and Countermeasure selection in virtual private network, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. It utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. It only investigates the network IDS approach to counter zombie explorative attacks. In order to improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the system. This should be investigated in the future work. Additionally, as indicated in the paper, we will investigate the scalability of the proposed Network Intrusion detection and Countermeasure selection in virtual private network solution by investigating the decentralized network control and attack analysis model based on current study.

ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

References

1. Chowdhury NMMK, Boutaba R (2012) A survey of network virtualization.Comput Newt 54(5):862–876
2. Fernandes N, Moreira MD, Moraes I, Ferraz L, Couto R, Carvalho HT,Campista M, Costa LK, Duarte OB (2011) Virtual networks: isolation, performance, and trends. Ann Telecommun 66(5–6):339–355
3. Anderson T, Peterson L, Shenker S, Turner J (2013) Overcoming the internet impasse through virtualization. Computer 38(4):34–41
4. Bays LR, Oliveira RR, Buriol LS, Barcellos MP, Gaspary LP (2014) A heuristic-based algorithm for privacy-oriented virtual private network embedding. In: IEEE/IFIP Network Operations and Management Symposium (NOMS). IEEE, Krakow, Poland

5. Cabuk S, Dalton CI, Ramasamy H, Schunter M (2011) towards automated provisioning of secure virtualized networks. In: ACM Conference on Computer and Communications Security. New York, USA

6. Yu S, Zhou W (2010) Entropy-based collaborative detection of ddos attacks on community networks. In: IEEE International Conference on Pervasive Computing and Communications. IEEE Computer Society, Washington, DC, USA

7. Oliveira RR, Macron DS, Bays LR, Neves MC, Buriol LS, Gaspary LP, Barcellos MP (2013) No more backups: Toward efficient embedding of survivable virtual networks. In: IEEE International Conference on Communications.IEEE, Budapest, Hungary

8. Karig, David and Ruby Lee. Remote Denial of Service Attacks and Countermeasures, Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2010.

9. “OpenvSwitchproject,’’http://openvswitch.org, May2012

10. Karig, David and Ruby Lee. Remote Denial of Service Attacks and Countermeasures, Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2001.

11. M. Tavallaee, E. Bagheri, L. Wei, and A.A. Ghorbani, “A Detailed Analysis of the KDD Cup 99 Data Set,” Proc. IEEE Second Int’l Conf. Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.

12. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting spam zombies by monitoring outgoing mes- sages,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198–210, Apr. 2012.

13. “NuSMV: A new symbolic model checker,” http://afrodite.itc.it:1024/∼nusmv. Aug. 2012.

14. S. H. Ahmadinejad, S. Jalili, and M. Abadi, “A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs,” Computer Networks, vol. 55, no. 9, pp.2221–2240, Jun. 2011.

15. X. Ou, S. Govindavajhala, and A. W. Appel, “MulVAL: a logic- based network security analyzer,” Proc. of 14th USENIX Security Symp., pp. 113–128. 2013.

16. R. Sadoddin and A. Ghorbani, “Alert correlation survey: frame- work and techniques,” Proc. ACM Int’l Conf. on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST ’06), pp. 37:1–37:10. 2012.

17. L. Wang, A. Liu, and S. Jajodia, “Using attack graphs for corre- lating, hypothesizing, and predicting intrusion alerts,” Computer Communications, vol. 29, no. 15, pp. 2917–2933, Sep. 2011.

18. S. Roschke, F. Cheng, and C. Meinel, “A new alert correlation algorithm based on attack graph,” Computational Intelligence in Se- curity for Information Systems, LNCS, vol. 6694, pp. 58–67. Springer,2011.

19. A. Roy, D. S. Kim, and K. Trivedi, “Scalable optimal countermea- sure selection using implicit enumeration on attack countermea- sure trees,” Proc. IEEE Int’l Conf. on Dependable Systems Networks (DSN ’12), Jun. 2012.

20. N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic security risk management using bayesian attack graphs,” IEEE Trans. Depend- able and Secure Computing, vol. 9, no. 1, pp. 61–74, Feb. 2012.

21. Open Networking Foundation, “Software-defined networking: The new norm for networks,” ONF White Paper, Apr. 2012.

22. “Openflow.” http://www.openflow.org/wp/learnmore/, 2012.

23. X. Ou, W. F. Boyer, and M. A. McQueen, “A scalable approach to attack graph generation,” Proc. of the 13th ACM conf. on Computer and communications security (CCS ’06), pp. 336–345. 2006.

24. P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system (CVSS), ”http://www.first.org/cvss/cvss-guide. html,” May 2013.