INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3239 - 3244
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018
April 11, 2018

# LINKAGE INTERFERENCE FINDING AND COUNTER MEASURE RANGE IN SIMULATED NETWORK

K.Naresh[1],T.Vinoth Kumar[2],K.Sankar Ganesh[3]

Department of Computer Science and Engineering, Students[1, 2], Assistant Professor[3], Kingston Engineering College, Vellore, India.

## ABSTRACT

Network security is one of most important issues that have attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a system and compromise machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as exploitation, low frequency scanning, and turning off the servers, and finally DDoS attacks through the entire system. Within the system the detection of intruder exploration attacks is extremely difficult. This is because users may install vulnerable applications on their systems. To prevent this we propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable network-based countermeasures. The proposed system is used to build a monitor and in order to significantly improve attack detection and overcome the attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

## I.INTRODUCTION

Network security is one of most important issues that have attracted a lot of research and development effort in past few years. The challenge is to establish an effective vulnerability attack detection and response system for accurately identifying attacks and minimizing the impact of security breach. Therefore in this article, we propose NICE (Network Intrusion detection and Countermeasure sElection) to establish a defense-in-depth intrusion detection framework. For better attack detection NICE incorporates attack graph analytical procedures into the intrusion detection processes. The main objective of the NICE is not to improve any of the existing intrusion detection algorithms but a efficient way to detect and counter the attempts to prevent from the intruders.

## II. EXISTING SYSTEM

The network and the server users can install vulnerable software on their systems which essentially contributes to loopholes in the security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to the users. Almost all the networks are protected by the firewalls and however these firewalls are not always effective against the emerging intrusion attempts . In the system the infrastructure is shared potentially by millions of users, abuse and also use the shared infrastructure benefits attackers to exploit vulnerabilities of the server and use its resource to deploy attacks in more efficient ways. Such attacks are

more effective in the networking environment since users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. Although data mining in intrusion detection is a fairly new method of maintaining the network security. It involves both legitimate users and malicious intentions by hackers who are trying to breach the network security. And also in the existing system it supports nearly 24 different types of attacks so it is very much difficult to find the intruder into the server or into the system.

## III. DISADVANTAGES

No detection and prevention framework in the networking environment.Not accuracy in the attack detection from the attackers.The number of real attacks are far below the number of false alarms.Encrypted packets are not processed in this system.When an attacker gains access due to weak authentication mechanisms then it cannot prevent the adversary from any malpractice.By sending the fragmented packets the attacker will be under the radar and can easily bypass the detection system's ability to detect the attack signature.The TCP port utilized by a protocol does not always provide an indication to the protocol which is being transported. If an attacker had reconfigured it to use a different port, the IDS may not able to detect the presence of the Trojan.The attackers can increase the difficulty of the ability of the Security Administrators to determine the source of the attacks by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server, it makes very difficult for IDS to detect the origin of the attack.The IDS generally rely on the pattern matching to detect an attack by changing the data used in the attack slightly it may be possible to evade the evade detection.

## IV. LITERATURE SURVEY

[1] B. Joshi and A. Vijayan have proposed the securing cloud computing environment against the DDos attacks. They proposed in their paper that Cloud Computing is the freshly emerged technology of Distributed Computing system. Cloud Computing user concentrate on API security and 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 their demand. These services provided can easily invites attacker to attack by SaaS, PaaS and IaaS. Since the resources are gathered at one place in data centers.The DDoS attacks such as HTTP and XML in this environment is dangerous and provide harmful effects and also all the consumers will be affected at the same time. The Detectors are used to monitor and filter the DDoS attacks such as HTTP and XML DDoS attack. Finally the filtered real client message is transferred to the cloud service provider and the corresponding services are given to the client in the secured manner.

[2] P. Chen, F. Sanchez, Y. Dong, M. Stephenson and J. Barker proposed detecting spam zombies by monitoring outgoing messages. Here they focus on to detect the compromised machines in a network that are used for sending spam messages which are commonly referred to as a spam zombies. Given that spamming provides a critical economic incentive for the controllers of the compromised machines to recruit these machines, it has been nearly observed that many compromised machines are involved in

spamming.A number of recent research efforts have studied the aggregate global characteristics of spamming compromised machines in the network**.**

[3] H. Takabi, J.B. Joshi and G. Ahn is proposed the security and privacy challenges in the cloud computing environment. They mentioned that Cloud computing has generated significant interest in both academia and industry, but it's still an evolving prototype. Essentially, the goal is to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications and information infrastructures consisting of pools of computers, networks and storage resources. Confusion exists in IT communities that how can a cloud differs from existing models and how these differences affect its adoption. Some consider the cloud as a novel technical revolution, while other consider it as a natural evolution of technology and economy. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several review of potential cloud adopters indicate the security and privacy is the primary concern hindering its adoption.

[4] In M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G.Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia has addressed that Business continuity and service availability from the service out stages is one of the top concerns in cloud computing systems. In a system where the infrastructure is shared by potentially millions of users use the shared infrastructure benefits the attackers to exploit vulnerabilities of the system and share the computing resources.

[5] O. Sheneyer, J. Haines, S. Jha, R. Lippmann and J.M. Wing in automated generation and analysis of attack graphs have proposed a technique based on a modified symbolic model checking and Binary decision diagrams to construct all possible attack paths and however the scalability is a big issue for this solution.

[6] Many attack graph based alert correlation techniques have been proposed by L. Wang, A. Liu and S. Jajodia devised an in-memory structure called queue graph to trace alerts matching each exploit in the attack graph. However the implicit correlations in the design make it difficult to use the correlated alerts in the graph for analysis of similar attack scenarios.

[7] S. Roschke, F. Cheng and C. Meinel 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 to group related alerts with multiple correlation criteria.After knowing the possible attack scenarios applying countermeasure is the next important task. Several solutions have been proposed to select optimal countermeasures based on the likelihood of the attack path and cost benefit analysis. A. Roy, D.S. Kim and K. Trivedi proposed an attack countermeasure tree to consider attacks and countermeasures together in an attack tree structure. probability assignments to the model.Therefore we take the advantage of the Network controller to apply the selected network countermeasures in the solution.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3239 - 3244
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018
April 11, 2018

## V. PROPOSED SYSTEM

Network security is one of most important issues that have attracted a lot of research and development effort in past few years. Therefore we propose NICE (Network Intrusion detection and Countermeasure selection in network systems) to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable networking approach to detect and counter the attempts to compromise the systems, thus preventing the Intruders. The Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and system activities for malicious activity. The Intrusion prevention systems(IPS) can take some actions such as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.

## VI. ADVANTAGES

We devise NICE, a new multi-phase distributed network intrusion detection and prevention framework in the networking environment that captures and inspects suspicious traffic without interrupting users applications and services.NICE incorporates a software switching solution to quarantine and inspect suspicious system for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to the exploitation attack without interrupting existing normal services.NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.It also shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions. The network based IDS systems can detect the attacks which are host-based sensors which fails to detect. A network based IDS checks for all the packet headers for any malicious attacks. The proposed system constantly monitors the network for the invasion or abnormal activity.NICE significantly advances the current network IDS/IPS solutions by using programmable networking approach that allows the system to construct a IDS.NICE optimizes the implementation on the servers to minimize the resource consumption . The system architecture diagram enables you to graphically model the applications of a system, and the externals that they interface with and data stores that they use or provide information to.

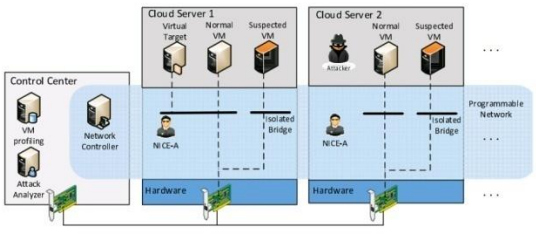


**Figure 5.1 System Architecture diagram**

## VII. FUTURE ENHANCEMENT

The proposed system 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. This should be investigated in the future work. We will investigate the scalability of the proposed solution by investigating the network control and attack analysis model.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.The system and the security evaluations has to demonstrate the efficiency and effectiveness of the proposed solutions. The performance results provides us a benchmark for the given hardware setup and shows how much traffic can be handled by using a single detection domain. To scale up to a data center level intrusion detection system ,a decentralized approach must be devised ,which is scheduled in our future research .

## VIII. CONCLUSION

In this paper, we presented NICE, which is proposed to detect and mitigate collaborative attacks in the networking environment. NICE 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.The system performance evaluation demonstrates the feasibility of NICE and shows that the proposed solution can significantly reduce the risk of the system from being exploited and abused by the attackers. The scalability of the proposed NICE solution will investigate by researching the network control and attack analysis model has been increased .

## REFERENCES

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

[2] P. Chen, F. Sanchez, Y. Dong, M. Stephenson, J. Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages", *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[3]H. Takabi, J.B. Joshi, G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Security and Privacy*, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A View of Cloud Computing", *ACM Comm.*, no. 4, pp. 50-58, Apr. 2010.

[5] O. Sheyner, J. Haines, S. Jha, R. Lippmann, J.M. Wing, "Automated Generation and Analysis of Attack Graphs", *Proc. IEEE Symp. Security and Privacy*, pp. 273-284, 2002.

[6]L. Wang, A. Liu, S. Jajodia, "Using Attack Graphs for Correlating Hypothesizing and Predicting Intrusion Alerts", *Computer Comm.*, vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[7]S. Roschke, F. Cheng, C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph", *Proc. Fourth Int'l Conf. Computational Intelligence in Security for Information Systems*, pp. 58-67, 2011.

[8]A. Roy, D.S. Kim, K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees", *Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12)*, 2012-June.

[9]N. Poolsappasit, R. Dewri, I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74, Feb. 2012.

[10]E. Keller, J. Szefer, J. Rexford, R.B. Lee, "NoHype: Virtualized Cloud Infrastructure without the Virtualization", *Proc. 37th ACM Ann. Int'l Symp. Computer Architecture (ISCA '10)*, pp. 350-361, 2010-June.