

A NOVEL APPROACH FOR COUNTERMEASURE SELECTION IN VIRTUAL NETWORK SYSTEMS WITH INTRUSION DETECTION

T. Veeraiah¹, N. Sharoon Kumar², B. Sai Krishna³, M. Sai Raghava⁴, S. Praneeth⁵,
S. K. M. Rao⁶, J. Amudhavel⁷

^{1,2,3,4,5,7}Department of CSE, K L University, Vaddeswaram A.P., India.

⁶Department of CSE, Gandhi Institute of Technology, Bhubaneswar, Odisha, India

Abstract: A New Multi-phase distributed identifying network intrusion and blockage framework in environment of networking. NICE scrutinize and identifies suspicious traffic of network system virtually without interrupting users virtual network system services and it's applications. NICE in-order for separation and inspects doubtful VMs for further investigation and protection organizes a particular solution. NICE develops the probability of attack detection and boosts the resiliency to VM exploitation attack without disturbing existing normal virtual network system services through the approach of programmable network. For the detection of attacks, NICE employs an approach of novel attack graph and also prevention through correlating attack behaviour and it also suggests effective countermeasures. In order to decrease the consumption of resources the application is optimized by NICE.

Our study depicts that NICE occupies least computational overhead when compared network intrusion detection solutions which is a proxy based. Ensuring the security of cloud computing is an important aspect in the environment of cloud computing, as users use cloud storage providers in order to store critical data providers but these may be untrusted. In this project we introduce NICE which is used for the detection of intrusions and also Countermeasure mechanisms.

The VMs that are not reliable from being compromised in the cloud are prevented. NICE detects and mitigates collaborative intrusions in the environment of cloud virtual network. The feasible nature of NICE is evaluated by demonstration of performance of system and exhibits that the solution that was introduced can significantly decrease the risk in Cloud system from being exploited and corrupt by internal and external attackers.

Keywords: Virtual Network System Computing, Intrusion Detection, Attack Graph, Zombie Detection.

1. Introduction

Cloud computing enables to provide an efficient method of computing resources management with relatively low cost. And it turns IT sector into ordinary commodities and services using pay-per-use pricing model.

A service provider rents Resources which are been taken from IT vendors as rents by the service providers to build Multi server systems that are relative and hence different applications are provided to the users. The result that were appropriate are received by the consumer with appropriate agreement by sending request to the service provider. The consumer's service pay depend up on the quality and the amount of service. To get many application domains service provider builds different multi server systems.

For data, cloud's storage system and system network's redundancy may not be reliable, it is concerned with score of security.

In cloud computing security is enormously improved due to the superior technology security system, that is currently simply obtainable and cheap. Applications not run on the desktop pc however run within the cloud. this suggests that the computer doesn't want the process power or magnetic disk area as demanded by ancient desktop software system. Powerful servers and therefore the like are not any longer needed. The computing endowment of cloud can be used to supplement or replace internal computing resources.

There is no want for the organisations to buy computing resources to handle the potential peaks. Expediently cloud computing is turning into an {efficient} good and efficient method of computing resources. Obviously, the necessity of profit maximization in the province of cloud computing atmosphere is required.

Today's the sixty billion servers square measure operating during this world in this service level agreement, outlined the standard of service

have to be compelled to offer for the user and also the most required execution time.

If the service supplier violates this service-level agreement no charge is provided for the particular service. Therefore there'll be the loss of the profit (IaaS) virtual network systems, the detection of zombie exploration attacks is extraordinarily troublesome. This is as a reverberation of virtual network system users might install vulnerable applications on their virtual machines. to forestall vulnerable virtual machines from being undermine within the virtual network system, we tend to adduce a multi-phase distributed network intrusion detection, measuring, and step choice mechanism known as NICE. NICE is formed on attack graph primarily based analytical models and reconfigurable virtual network based counter measures. The projected chassis ropes Open Flow schedule genus Apis to create a monitor and management plane over distributed programmable virtual switches so as to considerably improve attack exposure and mitigate attack consequences. The system and security evaluations demonstrate the potency and effectiveness of the projected solution.

2. Literature Survey

[1] **Mr. V.V.Prathap, Mrs.D.Saveetha, 2014** Detecting malware intrusion in network environment. In this model we have a propensity to undergone a study of 3 models, intrusion threat detection model, attack graph model and therefore the existing NICE model build the employment of attack graph to conduct prediction and detection of attack. NICE solely determines the IDS approach of network to counter zombie preliminary attacks.

[2] **Chun-Jen Chung, Tianyi Xing, Dijiang Huang, 2013** *NICE: network intrusion detecting and countermeasure selection in virtual network systems*. In this paper we have a proclivity to create study have studied the system and security evaluations demonstrate the potency and effectiveness of the projected resolution NICE, that is projected to find and mitigate cooperative attacks interior the cloud virtual networking surroundings. NICE solely investigates the network IDS approach to counter zombie exploratory attacks To improve the detection accuracy, host-based IDS solutions are required to be incorporated and to hide the absolute scope of IDS in reach the cloud system.

[3] **ShinaSheen, R Rajesh** network intrusion

detection mistreatment feature choice and call tree classifier. during this paper we've studied 3 totally different approaches for feature choice, Chi square, info gain and relief that is predicated on filter accession intrusion detection with detail choice was ready to trounce the choice tree algorithmic program. Without feature choice intrusion detection accession is extremely helpful for counter live.

[4] **Prof.D.P.Gaikwad, PoojaPabshettiwar, PriyankaMusale, PoojaParanjape, Ashwini S. Pawar, 2012A** submission for execution of signature based mostly IDS victimization multithreading technique In this paper we've mostly deliberated on signature based mostly IDS, exploitation multithreading technique. The diligent management of network security is crucial to the operation of networks, despite whether or not they have segments or not. Multithreaded technique for higher intrusion detection is concern to be distributed and cooperative by applying co-operative agents to the network.

3. Related Work

Network Intrusion Detection System In computer security:

A Network Intrusion Detection System (NIDS) is associate degree intrusion detection system that {attempts/makes associate degree attempt/tries} to find unauthorized access to a pc network by analyzing traffic on the network for signs of malicious activity Application protocol-based intrusion detection system associate degree application protocol-based intrusion detection system (APIDS) is an intrusion detection system that focuses its watching and analysis on a particular application protocol protocols in use by the automatic data processing system.

In the computing environment, the Graphical Desktop Sharing system utilizes Remote-Frame-Buffer (RFB) protocol for controlling other computer remotely. The system is named as VNC(Virtual Network Computing). It is done on a network by depending on screen updates that are graphical, back in the other direction and the transmission of mouse events and the keyboard are done from one computer to the other. This is platform independent system and to the most of the OS's there are clients and servers which are GUI-based and for Java.

Multiple no.of clients can get connected to this

server. The uses that are popular for this technique includes remote technical support and file accessing on one's work computer from one's home computer, or viceversa. By default this server (VNC) use 5900+N port, N is display number (usually: 0 to display physically) which is a TCP Port.

Many implementation techniques are also make a start over a basic HTTP server on 5800+N Port for providing a VNC viewer as Java applet, and connection is allowed in a easy way through any of the Java-enabled web browser, As far as the both the Client and Server are accordingly configured, the assignments of the port that are different can be used.

1. Security

By default, this isn't secure protocol because in this passwords aren't sent in Plain-text form as of telnet. If both i.e, the password that was encoded and key that was encrypted are sniffed from Network, then Cracking could be proven successfully.

For this, it is recommended that a password of atleast 8 Characters be used. On the other side, few versions of VNC support a Character of limit 8 i.e, if the sent password exceeds 8 characters then, the exceeded characters are deleted and the string that was truncated and the password are compared. UltraVNC support a plugin's use where complete session of VNC is been encrypted by that and which includes transfer of data and password authentication.

This plugin is Open-Source encryption plugin. Authentication that is to be performed based on NTLM and user accounts that are active directory are allowed. However, these encryption plugins make it incompatible with other programs of VNC.

2 Attack Analyzer

The functions that are majorly included in NICE system are done by the Attack analyzer which includes the procedures like construction of Attack Graph and selection of Countermeasure of Update, Alert Correlation.

The Constructing and Utilizing the Scenario Attack Graph (SAG) process contains 3 phases: Gathering of information, Constructing AttackGraph, and analysis of path that was exploited potentially. With the above information, using SAG these Attack paths are modeled. Attacker represent each node in the Attack Graph as an exploit. The attack that is successful is

represented by, each path that exists from initial node to the final node i.e, goal node.

3. Network Controller

Network controller is responsible for collecting network information and an input is provided to the attack analyzer to construct attack graphs.

The responsibility of the Network Controller's is also to apply Countermeasure. The countermeasures are choosed by the Attack analyzer and they are executed by Network controller which is based on risk probability and optimal investment return.

4. Countermeasure Selection:

For the attack scenario that is given algorithm-2 shows how to choose the countermeasure which is optimal.

Alert, Attackgraph G, and a countermeasures CM pool are the Inputs that are given to the algorithm Definition 3 (Countermeasure Pool). Countermeasures pool are shown as a set by $CM = \{ cm_1, cm_2, \dots, cm_n \}$ are called Countermeasure Pool. each cm_i CM is a tuple where $cm_i = (Cost, Intrusiveness, Condition, Effectiveness)$, where

1) Cost : Unit which describes the required expenses in the terms of operational complexity and resources in order to determine the Countermeasure, and it is of range from 1 to 5, and higher metric means higher cost;

2) Intrusiveness: The negative effect that is bought to the Service Level Agreement (SLA) by the countermeasure and value of it is ranging from least intrusive (1) to the most intrusive (5), On the SLA Countermeasure if there is no impacts then the value of intrusiveness is 0;

3) condition: It is need for the corresponding countermeasure; 4) effectiveness is the percentage of probability changes of the node, for which this countermeasure is applied.

Conclusion

In this, we proposed NICE model which is used for detecting and mitigating attacks which are collaborative in environment of Virtual Networking of cloud For prediction and detection it uses AttackGraph model.. The methos that was proposed determines how to use software programmability switches-based methods that improve accuracy of the detection and also to beat victim's phases that

are exploited of the attacks that are collaborative.

The performance of the system and its evaluation determines the feasibility of NICE and exhibits that the system and its proposed solution can significantly decreases the risk of cloud from being abused and exploited by external and also by internal attackers. NICE system only determines the IDS approach of network to the counter Zombie explorative attacks.

There is a requirement of host-based IDS solutions to improve accuracy of the detection, and are also required to include and to cover the entire spectrum of IDS in the Cloud. This future work is to be investigated. By investigating the control of Decentralized network control and Attack-analysis model the examination of the present NICE model is done to check scalability.

References

- [1] CloudSecurity Alliance, —Top Threats to Cloud Computing v1.0, <https://cloudsecurityalliance.org/topthreats/sathreats.v1.0.pdf>, Mar. 2010.
- [2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, —A View of Cloud Computing, *ACM Comm.*, vol. 53, no. 4, pp. 50-58, Apr. 2010.
- [3] 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.
- [4] H. Takabi, J.B. Joshi, and G. Ahn, —Security and Privacy Challenges in Cloud Computing Environments, *IEEE Security and Privacy*, vol. 8, no. 6, pp. 24-31, Dec. 2010.
- [5] Dhanalakshmi , R .Dhivyalakshmi , R.G. Gajalakshmi, Mrs.K.DeepaThilak, Scalability and the bandwidth efficiency of VoD Systems, *International Innovative Research Journal of Engineering and Technology*, vol. 2, no. 1, pp. 52-58, Sept.2016.
- [6] —Open vSwitch Project, <http://openvswitch.org>, May 2012.
- [7] 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.
- [8] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” *Proc. 16th USENIX Security Symp. (SS '07)*, pp. 12:1-12:16, Aug. 2007.
- [9] ISSN: 2305-0012, Sina Manavi, Sadra Mohammadalian, Nurlzura Udzir, Azizol Abdullah, 2012 secure model for virtualization layer in cloud infrastructure
- [10] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” *Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08)*, Feb. 2008.
- [11] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, “Automated Generation and Analysis of Attack Graphs,” *Proc. IEEE Symp. Security and Privacy*, pp. 273- 284, 2002,
- [12] “NuSMV: A New Symbolic Model Checker,” <http://afrodite.itc.it:1024/nusmv>. Aug. 2012.
- [13] P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable, graph based network vulnerability analysis,” *Proc. 9th ACM Conf. Computer and Comm. Security (CCS '02)*, pp. 217-224, 2002.
- [14] VOL. 10, NO. 4 Chun-Jen Chung, Tianyi Xing, Dijiang Huang, 2013 NICE: network intrusion detecting and countermeasure selection in virtual network systems.

