Research Journal of Applied Sciences, Engineering and Technology 8(6): 755-759, 2014
DOI:10.19026/rjaset.8.1031
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: May 19, 2014 Accepted: July 01, 2014 Published: August 15, 2014

Research Article

Effective Data Security in Virtualization using Maize Routing Technique

[1]S. Anthoniraj and [2]S. Saraswathi
[1]Department of Computer Science and Engineering, Manonmaniam Sundarnar University, Thirunelveli 627 012, India
[2]Department of Information Technology, Pondicherry Engineering College, Puducherry 605 014, India

Abstract: Virtualization is a technology that combines or divides computing resources to present one or many operating environments using methodologies like hardware and software partitioning or aggregation, partial or complete machine simulation, emulation, time-sharing and others. The hackers are also making use of it for hiding their identity and to exploit the other machines. One more terminology, as port scanner for scanning the presence of hackers. It is also distorted by them in such a way for the analysis of open ports and also it provides a solution with the roll backing system and the Maize routing. So whenever the information loss occurs, the roll back mechanism is introduced and used as a secondary security. As a primary, the proposed concept of Maize Routing (MR) is used. Here we uses the Base Internet Protocol (IP) of the virtualized system as a reference and produce multiple duplicated IP's. Whenever the presence of the hacker is found, then the revealing mechanism sends a link to the virtual machine and directed to the Maize routing. Then the execution mechanism activates and diverts them in to a wrong direction. Hence the effective data security is achieved by using the mechanism of maize routing.

Keywords: Execution mechanism, hypervisor, internet protocol, Maize Routing (MR), Para-Virtualization (PV), private cloud, rollback system, virtualizations, Virtual Machine Monitor (VMM), XEN

INTRODUCTION

Virtualization is a popular technology that mainly becomes popular because it facilitates the day to day increases in the processing power and also it is aimed to increase the level of system abstraction. The hypervisor creates a fully virtualized environment so that one advantage is customization. Recently we make us of the virtualized environments for avoiding the direct loss of data from the machine. But at the same time the exploitation of the virtualized machine is always becoming a problem. We provide a virtual environment but also an introduction to the security measurements with it.

There are two approaches to enable virtualization. Para-Virtualization (PV) (Whitaker *et al*., 2002) requires OS modification to work cooperatively with VMM. We provide a virtual environment but also an introduction to the security measurements with it. The virtual environment is secured with a rollback system. Here whenever the data loss or the exploitation message is being passed into the system, the rollback system is being activated and hence protects from the data loss. There is an algorithm for the continuous inspection of the data security and make a reference to the storage system. Full virtualization requires no alteration, using hardware supports like Intel-VT (Uhlig *et al*., 2005). Xen (Barham *et al*., 2003) is an open source VMM, which supports both para-virtualization and full-virtualization. There is a time setting within that, whenever a new data is found, it will be passed into the storage reference and at the time of necessity it can be retrieved.

Port scanner can be considered as a technique used for measuring the presence of hackers or the malicious item. But it is being misused by the hackers in such a way that for finding the open ports that are available. There are more than 1000 open ports are available. It can identify the victim in an easy manner. Actually the port scanner is being designed for the detection mechanism, but apart from that mostly it is used for wrong purpose as a bad manner. In our current networking system we have limitations since the privacy policy of the service providers are putting restriction on us. Hence, there should be a new mechanism for resolving the existing problems. So here we introduce a new routing algorithm which hides the identity of the physical machine and from the virtual environment it derives duplicated IP's for the respective virtual machines.

Data security in various techniques: The security in the networking is becoming a serious issue. Most of the security mechanisms are exploited by the hackers,

Corresponding Author: S. Anthoniraj, Department of Computer Science and Engineering, Manonmaniam Sundarnar University, Thirunelveli 627 012, India

so that the introduction of a new mechanism to avoid the explosion is essential. Here we propose a new mechanism along with the existing techniques. In our system we introduce the data protection with two security mechanisms such as rollback system and the Maize routing.

Port scanner: Port scan attack refers to scanning all the open port number of the sufferer node, in order to get out all the services one can break into. In a port scan attack, the attacker mostly sends a message to each of the 65,535 ports or in some case just a few common ports, whichever is possible. Now depending on the reply, the attacker gets back from each of the ports, one can decide on which of the ports are open. However, there exist problems with such a port scan. It is that, some of the services in the destination node may create a log scan and if the service identifies the connection has been made but no data received in return, the log will report an error. But again in order to counter this many stealth scan techniques (Patterson, 2002) have been developed.

In this attack we propose an adversary, which exhibits the same behavior as an honest node during the route discovery process. It then launches a port scan attack on the Destination node, whose packets are to be intercepted. Once the Port Scan attacks become successful the adversary places itself in the routing path of the destination and launches our proposed attack. Patterson (2002) discusses a review or port scanning techniques. He discusses some of the stealth and indirect scanning techniques. In our system we have two security measures. We name it as primary and secondary security techniques. We set the Maize routing as the primary and the roll back system as the secondary one.

This method cannot be misused by the hackers like that of the port scanner. It also has a time limited setting over the network, so that after a particular time if the hacker is trying to get in and the limit exceeds, then the connection will be made into dead state and secures our system. Anonymity networks allow users to communicate while hiding their identities from one another and from third parties. We would like to design such networks with strong anonymity guarantees but without incurring high communication overhead or much added latency.

Many designs have been proposed to meet these goals to varying degrees (Oppenheimer *et al*., 2003). Of the many design proposals, Onion routing (Syverson *et al*., 2001) has had notable success in practice. Several implementations have been made (Chaum, 1985; Syverson *et al*., 2001; Rosenblum and Garfinkel, 2005) and there was a similar commercial system, Freedom (Boucher *et al*., 2000). As of September 2006, the most recent iteration of the basic design (Chaum, 1985), consists of over 750 routers, each processing an average of 100 KB/sec. Onion routing is a practical anonymity-network scheme with relatively low overhead and latency. It provides two-way, connection-based communication and does not require that the destination participate in the anonymity-network protocol. These features make it is useful for anonymzing much of the communication that takes place over the internet today, such as web browsing, chatting and remote login. Many Tor users communicate with web-based businesses and financial services. Goldschlag *et al*. (1996) was the first to note that even the best e-cash design fails to be anonymous if the network identifies the customer.

Roll backing system: The roll back system is to be considered as the secondary security measure. Here we call back the contents when the data loss occurs. At the extreme case of the primary security, if we lose our control over the system, then it erases the available data and there after call backs the data from the storage management system. Here we consider the storage management system as a private cloud. We make use of an algorithm in such a way that it inspects the data changes in machine and report it to the private cloud. At the same time it checks for the failure signal from the primary security and hence erases the whole content and protects our privacy. For this algorithm also we set an interval for the inspection for the changes and the signal establishment. There are many possible causes of network failures, one of the most significant is operator errors (Patterson, 2002; Oppenheimer *et al*., 2003). Furthermore, the majority of the operator errors, which we focus on throughout the paper, stems from configuration tasks (Oppenheimer *et al*., 2003). Consequently, the development of new network management schemes to tackle operator errors caused by configuration is important to make network more dependable.

METHODOLOGY

Maize routing implementation in virtualization environment: We propose an introduction to a new system which revolves the imaginary security into reality. In Fig. 1 We make use of a system with two security measures and the system is being connected to the cloud for ensuring the security. Multiple systems can have the access to the cloud but not from the external environment. We make use of the private cloud more over to give maximum security.

Here the physical machine refers to our system or the server that we are going to make use of whenever the hypervisor creates a fully virtualized environment. We are able to customize the configuration as per our wish and for future reference of the hypervisor to the physical machine. The internal architecture is done by the maze algorithm which governs the overall control. Open ports are the landmark for the hackers to identify the character of a system and to take its advantage.

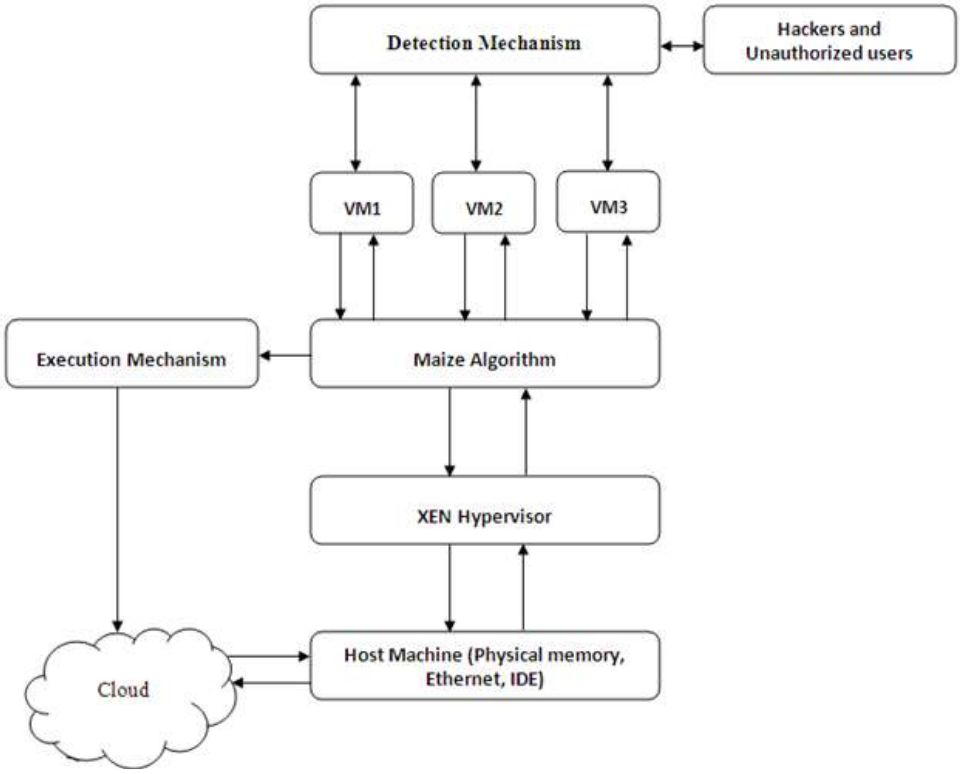

Fig. 1: Maize routing implementation in virtualization environment

While considering the existing mechanism if the ports are open the admin they have to close each ports individually which can be a difficult task and the other thing is scheduled scanning should be made as a routine. But scanning at every instant will affect the performance of the system. However the exploited methods like port scanner cannot be considered for the task management. According to the maize routing it solves all these confusions. If there occurs any crossings, then the automated system will notify and takes the relevant actions on it. And there is no need of continuous inspection and secure each ports. The overall makes the proposed system an effective one and to become a solution over the current scenario.

The hypervisor is having a link with the Maize routing. So, whenever the detection mechanism sends a request on alerting the presence of hacker or the malicious item and then the respective virtual machine forwards a request to the routing algorithm. Hence the algorithm is activated and hides the identity of the physical machine and from the hypervisor identity it creates duplicated IP's which denies the hackers attempt to get into the system. The execution mechanism is activated when the algorithm accepts the warning signal from the correspondent virtual machine. The whole is to be considered as our primary measure. At the extreme level of the primary security, we have secondary measure called rollback system. Here also we introduce an algorithm which inspects the system for any change in data or for the failure message from the primary system. It requires any change in the storage item, it will send a reference to the private cloud to ensure more security. When the failure message from the routing algorithm is received, then it erases the whole content from the system environment and sets the connection to a dead one. By the use of these techniques, we can able to make sure the security of our system.

Maize algorithm: r = 'V' IP; N = random IP; PC = Private Cloud; 1 = active; 0 = Inactive V_m = Virtual Machine; P_m = Physical Machine, M = Maize routing T1 = Temporary variable 1; DM = Detection Mechanism; H = Hacker:

1. Begin
2. Maize ( )
3. $\forall V_m \in P_m$
4. Set T1 = 'P' IP
5. Obtain 'V' IP from T1
6. Set T1 as inactive
7. If ((connection = True) && (Hacker == present)) do
8. Set DM = Active //Activate Detection Mechanism
9. If (Hacker present) then
10. DM send ALERT message to Vm
11. Vm send ALERT message to Maize
12. Maize routing get activated
13. If (Maize == Active) do

14. Set Timer = ON//Call EM ( )
15. If (Timer == OFF) then
16. DISCONNECT & RECONNECT
17. Else
18. Send CRASH message from Maize to P_m and PC
19. If P_m received CRASH message then do
20. Relocate Data from V_m to P_m
21. Relocate Data from P_m to Cloud
22. Set small Timer = ON
23. If (Timer == OFF) then
24. DISCONNECT & RECONNECT
25. If (Relocate == SUCCESS) then do
26. Vm = P_m = Inactive
27. End

RESULTS AND DISCUSSION

Compared to the existing security sectors we have more benefits in our system. During the measurement we will get more accurate value than the precursions that we are using today such as port scanner and cloud techniques. On this basic, we have some graphs which will explain the accuracy of our sectors. In the real world, the normal networking is not at all in a secure condition. Nowadays we are under massive attacks. Even though we make use of the existing security mechanisms it becomes a vain. Packet streaming is one of the main treat that we are facing now. It can cause the loss of important information to the external world. The word networking itself means establishment of the connection. If the denial of service occurs the concept will become a failure one. So, the necessity of a new system is essential. Port scanner can be considered as a crucial system in the computing sector. It has lot of verities and supervision techniques. As per the process administration it is not able to afford finest bandwidth due to the multifarious behavior techniques. Bandwidth decides significant aspects of networking, so conciliation in it won't be a fair one.

Maize avoids the entire confusions. It is an intelligent to offer most favorable bandwidth in view of the fact that the treatment techniques are done in a simple manner. In Fig. 2 While considering the TCP and window scan, port scanner is pitiable. Whereas in SYN and FIN it improves a slight but not to an adequate level. But in maize it can execute expected outcome in the case of FIN next to window scan and best possible in TCP and SYN scan. Therefore reasonably maize provides superior performance and simple to commence. Service establishment is surviving of the networks. There occurs certain denial case due to the misinterpretation and enforced crash as per Fig. 3. Due to the restricted view, port scanner is not talented to decide the service denial issues. It lags in organization and the reaction for the freeze circumstances will not make any outcome on it. Maize

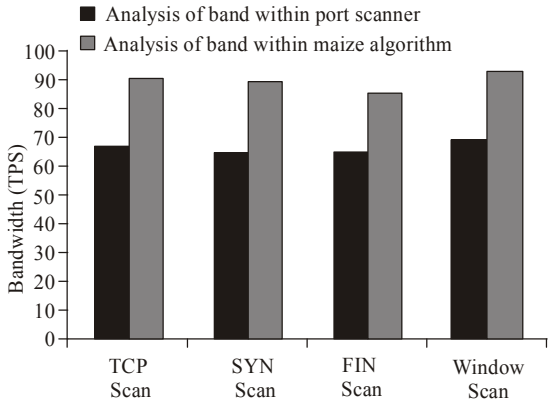

Fig. 2: Bandwidth analysis

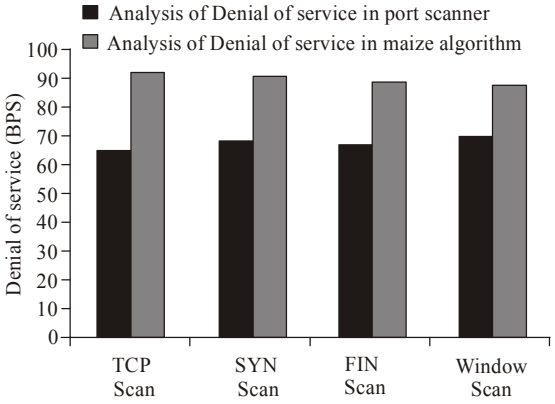

Fig. 3: Denial of service analysis

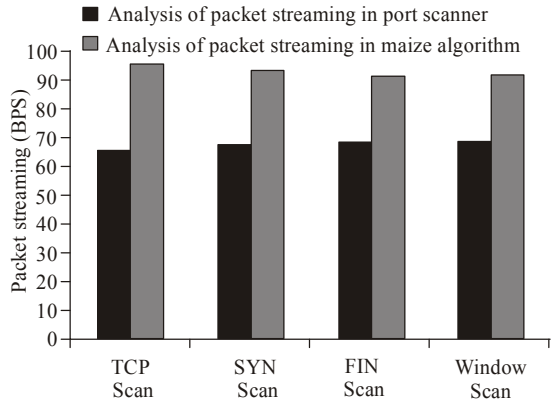

Fig. 4: Packet streaming analysis

is capable to direct this since it goes through threaded procedure, so that the consequential would be a fair state. In the case of different scans through port scanner it makes unfortunate result and causes dead locks. But gifted techniques in maize overcome the case and expectation of bypasses. In result, maize is in an adequate level and yields to the necessity of its introduction.

A packet governs the mode of transfer. The cases of streaming will origin vital changes in the end result. Port scanner is not stronger to control the approach and the provision of packets, as a result it fall short in treating the important aspect. At the same time as in view of maize, it proceeds as a breezy scheme thus the barriers are evaded. As per Fig. 4, the potential of port scanner is a condensed one in view of the fact that it has composite constitution. At the same time maize switches the issues through vigilant examination and cut down practices.

CONCLUSION AND RECOMMENDATIONS

Virtualization and the network security are the important terminologies that are being discussed in the field of computer science. We are always interested to stay in a secure environment. Here we made an establishment of a secure environment through the combination of both the rollback and port scanner concepts. The introduction of the maize routing makes tremendous changes in the cyber world. It hides the base IP of the hypervisor environment, through this we can ensure our security. The detection and management of the hackers an interesting factor in this study. This overall mechanism can be used along with a user id, for avoiding any illegal usage in future. It can be applied along with both client and server side and to ensure the security of two way verification passwords. We assure this as one of the best security mechanism that can overrule the current issues and make struggle to the exploiters to think about tomorrow.

REFERENCES

Barham, P., B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt and A. Warfield, 2003. Xen and the art of virtualization. Proceedings of the 19th ACM Symposium on Operating Systems Principles. Bolton Landing, NY, pp: 164-177.

Boucher, P., A. Shostack and I. Goldberg, 2000. Freedom Systems 2.0 Architecture. White Paper, Zero Knowledge Systems Inc., Montreal, Canada, December 2000.

Chaum, D., 1985. Security without identification: Transaction systems to make big brother obsolete. Commun. ACM, 28(10): 1030-1044.

Goldschlag, D., M. Reed and P. Syverson, 1996. Hiding Routing Information. In: Anderson, R. (Ed.), Information Hiding. LNCS 1174, Springer, Heidelberg, pp: 137-150.

Oppenheimer, D., A. Ganapathi and D.A. Patterson, 2003. Why do Internet services fail and what can be done about it. Proceeding of the 4th Conference on USENIX Symposium on Internet Technologies and Systems (USITS, 2003), 4: 1-1.

Patterson, D., 2002. Recovery Oriented Computing (ROC): Motivation, definition, techniques and case studies. Computer Science Technical Report UCB//CSD-02-1175, U.C. Berkeley.

Rosenblum, M. and T. Garfinkel, 2005. Virtual machine monitors: Current technology and future trends. Computer, 38(5): 39-47.

Syverson, P., G. Tsudik, M. Reed and C. Landwehr, 2001. Towards an Analysis of Onion Routing Security. In: Federrath, H. (Ed.), Designing Privacy Enhancing Technologies. LNCS, Springer, Heidelberg, 2009: 96-114.

Uhlig, R., G. Neiger, D. Rodgers, A.L. Santoni, F.C.M. Martins, A.V. Anderson, S.M. Bennett, A. Kagi, F.H. Leung and L. Smith, 2005. Intel Virtualization Technology. Computer, 38(5): 48-56.

Whitaker, A., M. Shaw and S.D. Gribble, 2002. Denali: Lightweight virtual machines for distributed and networked applications. Technical Report 02-02-01, University of Washington, Seattle.