IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305382 |

Cross-VM Network Channel Attacks and Counter measures within Cloud Computing Environments Project

Prof. Rashmi K A[1], Abhishek B V[2], Abhishek K A[3], Gagan Kumar H M[4], Neeraj Y M[5]

Assistant Professor, Department of Computer Science and Engineering, S J C Institute of Technology,Chickaballapur, Karnataka, India[1]

U.G. Student, Department of Information Science and Engineering, S J C Institute of Technology, Chickaballapur, Karnataka, India[2,3,4]

ABSTRACT: Cloud computing, with its promise of cost-effective computational resources and storage, has become the cornerstone of modern data management. However, the centralization of data in third-party cloud servers exposes users to various security risks, including internal data tampering and external attacks on virtual machines (VMs). In this paper, we address the threat of cross-VM network channel attacks, wherein a compromised VM diverts traffic or overwhelms other VMs with excessive requests, jeopardizing user data. To counter such attacks, we propose the implementation of a Monitor Node, a controller responsible for scrutinizing the behavior of individual VMs within the cloud infrastructure. Leveraging the modular architecture of cloud platforms, our Monitor Node integrates seamlessly with existing components, including Compute and Network nodes. By continuously monitoring VM activities, the Monitor Node can detect anomalous behaviors indicative of potentialattacks, such as packet diversion or abnormal traffic patterns.

I. INTRODUCTION

Cloud computing has risen in prominence due to itsservice model enabling elastic on-demand access tocomputing resources and now underpins modern business operations. Cloud computing security is an important concern for enterprises when they shift critical information to geographically distributed cloud platforms that are directly not under their jurisdiction of control. There are many security concerns for cloud computing as it utilizes different technologies spanning networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management, which arepotentially vulnerable to attacks.

1.1 Overview: Despite the clear potential of cross-VM attacks for exploiting shared memory and disk, exhibition of cross-VM network- channel and privilege escalation that uses the ROP in conjunction with the network-channel attack has not been demonstrated. Currentnetwork-based attacks exploit existing vulnerabilities such as ARP spoofing and DNS poisoning that are difficult to use for VM- targeted attacks [14].

1.2 Problem Statement: Cross-VM Network Channel Attacks (CVNCA) refers to attacks where malicious actors exploit covert channels between virtual machines (VMs) in a cloud environment to compromise data confidentiality and integrity. The primary problem addressed by this project is how to detect, prevent, and mitigate CVNCA in cloud computing environments.

1.3 Objective:

- Investigate and categorize existing CVNCA techniques and vulnerabilities in cloud environments.
- To develop a method of privilege escalation by exploiting the Return Oriented Programming (ROP) method in conjunction with a network channel in the cross-VM setting of a virtualized system.
- To demonstrates two successful zero-day crossVM network attacks within a leading cloud platform (OpenStack).
- The prevention module block penetration ofany external device into the system and properly scrutinize the connection requestbefore granting the root connection.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305382 |

II. LITERATURE SURVEY

The landscape of cloud computing introduces new challenges in maintaining the security and isolation of co-located Virtual Machines (VMs). Researchers have extensively investigated the vulnerabilities associated with cross-VM attacks, specifically focusing on the exploitation of shared resources to extract sensitive information from co-residing VMs. This literature survey delves into various studies, attacks, and countermeasures proposed by researchers to address these security concerns.

Cross-VM Attacks:

1. **Categories of Co-Residency Attacks:** Zhang et al. [17] categorized co-residency attacks into three classes: access-driven side-channel attacks, time-driven side-channel attacks, and trace-driven side-channel attacks. Access-driven attacks exploit shared micro-architectural modules like caches, while time-driven attacks manipulate cryptographic operation execution times. Trace-driven attacks capture cache activity profiles [5] [18]. These findings challenge the assumption of trust between VMs sharing network interfaces due to the shared physical hardware in public clouds [16].
2. **Methods for Data Leakage:** Researchers [5] [18] demonstrated methods to leak sensitive data through TCP/IP. Timing channels, as presented by Ranjith et al. [19], utilize a timing channel for data leakage. These findings highlight the diverse avenues through which attackers can exploit shared resources to compromise data confidentiality.

Countermeasures and Hardening Techniques:

1. **Hypervisor Hardening:** Various methods are employed to harden hypervisors, such as Xen. Trustvisor [20] and Bitvisor [21] focus on code reliability, data privacy, and I/O device security, respectively. NOVA [22] leverages microkernel-like access to virtualization levels, minimizing performance overhead. However, there is room for improvement in the existing approaches.
2. **Protecting Commercial Hypervisors:** HyperGuard, HyperCheck [25], and HyperSentry [23] implement strategies to protect running commercial hypervisors like Xen and KVM. These methods involve placing the hypervisor measurement agent (MA) in the CPU System Management Mode (SMM) [25] and implementing non-bypassable memory lockdown techniques [24].
3. **Hypervisor for Control-Flow Hijacking Protection:** HyperSafe [24] is designed to protect against control-flow hijacking attacks, implementing hardware features for non-bypassable memory lockdown and fine-grained control-flow integrity.

Real-time Attacks and Vulnerabilities:

1. **ROP-Based Attacks:** The report discusses real-time attacks that manipulate Return-Oriented Programming (ROP) systems, exploiting vulnerabilities in applications like Adobe Flash Player and Adobe Reader [11]. The ROP technique is also appliedto escalate privileges in the Xen hypervisor [29].
2. **Offline Auditing Framework:** An offline automated framework for auditing consistent isolation between virtual networks in OpenStack is proposed in [27]. Additionally, Cloud Insider Attack Detector and Locator (CIADL) focuses on multi-tenantnetwork isolation in OpenStack [28].

Existing Attack Models and Vulnerabilities:

1. **Network Channel Attacks:** Researchers [14] categorized network channel attacks into spoofed ARP, virtual hub, and ARP poisoning. Various attacks, such as ARP spoofing and virtual hub sniffing, exploit vulnerabilities in different network configurations.
2. **ROP-Based Rootkits:** ROP-based rootkits targeting Windows and Apple iPhone are discussed, highlighting their ability to circumvent kernel integrity protection systems.
3. **Novel Attacks:** The literature survey also presents novel attacks like ZombieLoad [34], revealing a Meltdown-type effect ina processor's fill-buffer logic, and MemJam [35], exploiting aliasing for side-channel attacks.

III. METHODOLOGY

OpenStack

OpenStack is an open-source platform for cloud deployment. It attempts to provide sufficient compatibility to Amazon's external interfaces. It provisions scalability as well as a wide diversity of hypervisors, network infrastructures, and storage systems. The OpenStack section that is used in this research is neutron [39] that enables the

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305382 |

network component and is available under the Apache-2 license.

OpenStack Architectural Description

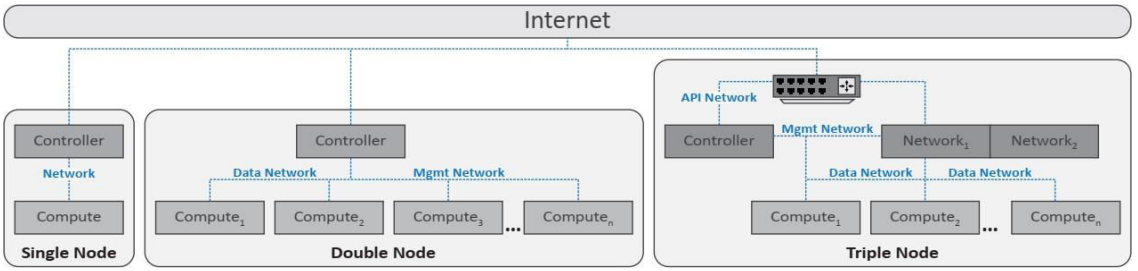


Figure: OpenStack Setups

Following are the node specifications and their descriptions used in OpenStack architecture.
Controller: Responsible for executing the services of management software that are needed for functioning of OpenStack platform. **Compute:** Compute nodes execute virtual machine instances in Open-Stack. KVM is used as a hypervisor in this node. This node is also responsible for providing firewall services. One can deploy more than one compute node in a setup.

Network: The responsibilities of network nodes ensure the creation of virtual networks needed by the customers to create public orprivate networks. It connects their virtual machines with the external networks, i.e. the Internet.

Deployment: All these nodes can be configured in the form of a single machine or multiple machines as shown in Figure 1. In a single node setup, all nodes are deployed within the same physical machine for facilitating all VMs and networking capability. In a multi- node setup, a single controller is responsible for system management of all compute nodes executing VMs.

Privileged and unprivileged domains: A number of VMs or domains can run on Xen. When the system boots, bootloader first loadsXen which loads its main domain called dom0. As Xen does not manage any device drivers, dom0 is used to access the hardware andcan handle device requests.

A **Linux bridge (L.B)** acts like a switch that follows the MAC learning principle. Multiple network interfaces devices can be connectedto such bridges. There are MAC caching tables.

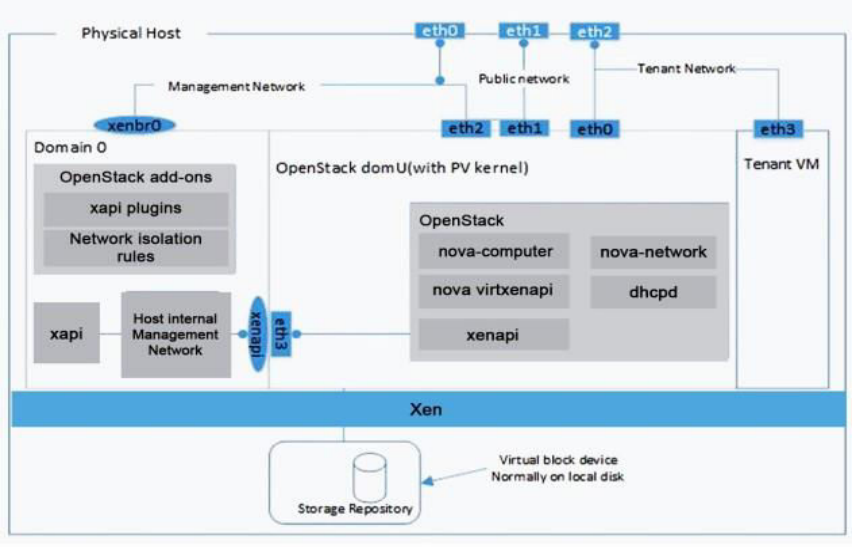


Fig. 3. OpenStack Xen Architecture [41]

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

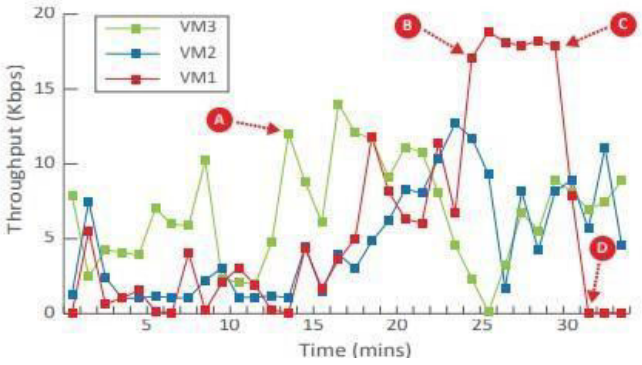
|| Volume 13, Issue 5, May 2024 ||

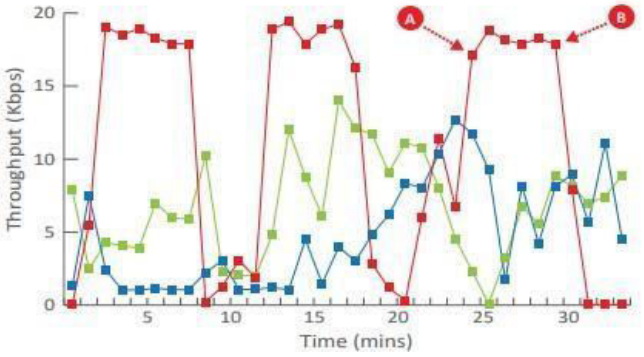
| DOI:10.15680/IJIRSET.2024.1305382 |

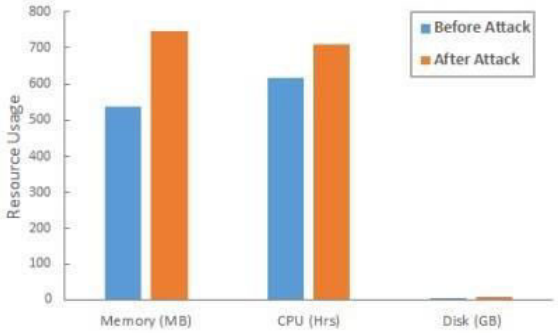
In these bridges that are used to keep records of which interfaces on the bridge are communicating with a host on the link. An Ethernet frame arrives at an interface connected to the bridge, the host MAC address and port on which the frame received is saved in a MAC caching table for a limited time. When the bridge needs to send a frame, it first looks up the table to see if the destination address of the frame is saved or not. If so, the Linux bridge in such a case will forward the frame only through port where the frame is received. If its record is not saved in a table, then the bridge will flood the frame to all network ports, with the exclusion of the port where the frame received.

IV. RESULTS

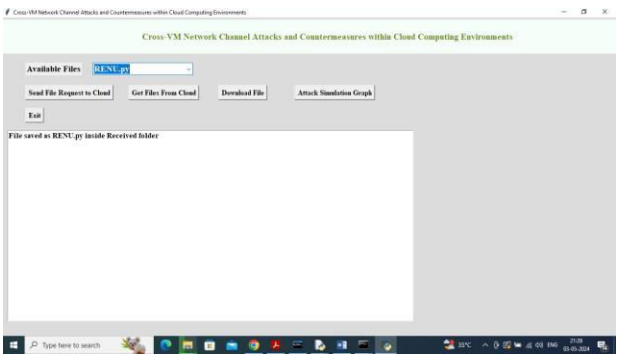
DEMO MODELS

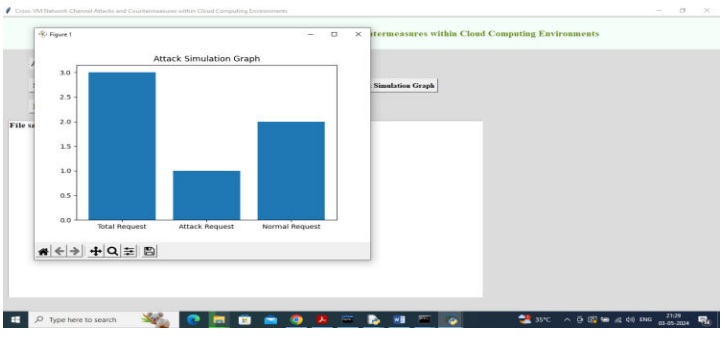






DISPLAY OF RESULTS





V. CONCLUSIONS

The project proposes a robust solution to mitigate cross-VM network channel attacks in cloud computing environments. By introducinga Monitor Node to actively monitor VM behavior and detect anomalies, the system enhances the security

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305382 |

posture of cloud servers, safeguarding user data integrity and service availability. Through simulations and experiments, the efficacy of the proposed solution has been demonstrated, showcasing its ability to detect and mitigate potential threats in real-time.

We have highlighted the challenge for cloud providers to observe and detect such attacks due to an attacking VM which neither violates assigned VM resource capacity nor it makes any illegal connection with the root user for privilege escalation. Future work will focus on improving the current heuristics that prevent penetration of external devices into the network and also observe the request for root-connection. Furthermore, we will investigate how to overcome the challenges of distinguishing between normal resource patterns andtarget attacks.

REFERENCES

1. A. Seshadri et al., "Secvisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity oses," in ACM SIGOPS Operating Systems Review, vol. 41, pp. 335–350, ACM, 2007.
2. http://cve.mitre.org/cgibin/cvename.cgi?name=CVE-2008-0923.
3. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security,pp. 199–212, ACM, 2009.
4. Z. Wu, Z. Xu, and H. Wang, "Whispers in the hyper-space: Highspeed covert channel attacks in the cloud.," in USENIX Security symposium, pp. 159–173, 2012.
5. J. Rutkowska, "Subverting vistatm kernel for fun and profit," Black Hat Briefings, 2006.
6. D. Hyde, "A survey on the security of virtual machines," Dept. of Comp. Science, Washington Univ. in St. Louis, Tech. Rep, 2009.
7. S. R. Kumari and V. Kathiresan, "Virtual environment securityconsiderations & practices," Networking and Communication Engineering, vol. 3, no. 2, pp. 87–92, 2011.
8. S. Zhang, "Deep-diving into an easily-overlooked threat: Inter-vm attacks," tech. rep., Technical Report). Manhattan,Kansas: Kansas State University, 2012.
9. Bates, Mood, et al., "On detecting co-resident cloud instances using network flow watermarking techniques," International Journal of Information Security, vol. 13, no. 2, pp. 171–189, 2014.
10. V. Varadarajan et al., "A placement vulnerability study in multitenant public clouds,"
11. Adobe, "Adobe systems. security advisory for flash player, adobe reader and acrobat: Cve-2010-1297.." http://www.adobe.com/support/security/advisories/apsa10 -01.html, 2010.
12. S. Ragan. http://www.thetechherald.com/articles/Adobeconfirms-Zero-Day-ROP-used-to-bypass-Windowsdefenses/11273/.
13. R. Hund, T. Holz, and F. C. Freiling, "Return-oriented rootkits: Bypassing kernel code integrity protection mechanisms," in USENIX Security Symposium, pp. 383–398, 2009.
14. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," The journal of supercomputing, vol. 63, no. 2, pp. 561– 592, 2013.
15. A. Saeed et al., "A cross-virtual machine network channel attack via mirroring and tap impersonation," in IEEEInternational Conference on Cloud Computing (CLOUD), pp. 606–613, IEEE, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details