IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

SecureOS: A Docker based Security OS

Akshat Roy and Vaishali Aggarwal
Department of Computer Science
Dronacharya College of Engineering, Gurgaon Haryana

Abstract: *The following research paper discusses the architecture, reasoning of systems implementation and components placement, discussion of performance metrics of Virtual Machines and Docker Containers, and implementation strategies for this modern-day Operating System.*
This architecture is designed keeping two major goals in mind: security and ease of use. As we observe the rise of AI and its misuse in the field of Security, the need for a modern system that can expand and grow for decades to come while being able to safeguard the data of its users becomes more and more important.
The following architecture aims at establishing a foundation for this type of Operating System and also presents sufficient reasoning and proofs to be laid for this type of OS to be realised one day.
**The paper follows a What?, Why?, and Achieved pattern for its sections..*

Keywords: Docker, Virtual Machine, Architecture, Security, Security OS

I. INTRODUCTION

This is a research paper that lays an account of a new type of Operating System that I have designed. The Operating system features the use of virtualization technologies as its base to host various types of services inside the system. Mainly the Operating system has been divided into two main sections namely the Application Section and the Storage Section, the application section is where all the applications of the Operating System are hosted, managed, and operated from, and the storage section of this operating system is where all the major bulk of the memory will be stored, managed and secured.

This architecture assumes that all the activity being performed by a user is harmful and vulnerable due to which these can cause a breach of the operating system by the use of viruses, malware, Trojan horses, specialized spearheaded attacks, etc, these attacks can lead to causing harm the host machine, corruption of data, and unauthorized access to the components of the machine like mic, camera, GPS, network devices and data stored. To prevent these types of attacks on a given system this operating system should be constructed. This architecture divides all the operations being performed by the OS into two main sections and these sections are further divided and controlled to provide the best possibility of maintaining the security of the system, to do this, activities are broken down into two sections Application Section and Storage Section, all the Applications and Softwares are places and runned in the Application system where they operate inside docker containers, the docker containers are modified to be able to host more than one application inside a single container, and the storage section is used to house all the data of the system and it is operated via virtual machine configured as a NAS type storage, these sections are further discussed in detail in the upcoming sections of this paper.

This Operating system plans to provide its users with a fast and secure space to house all their computing power and this paper aims to achieve this by laying the foundation of the architecture of this system

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

II. ARCHITECTURE

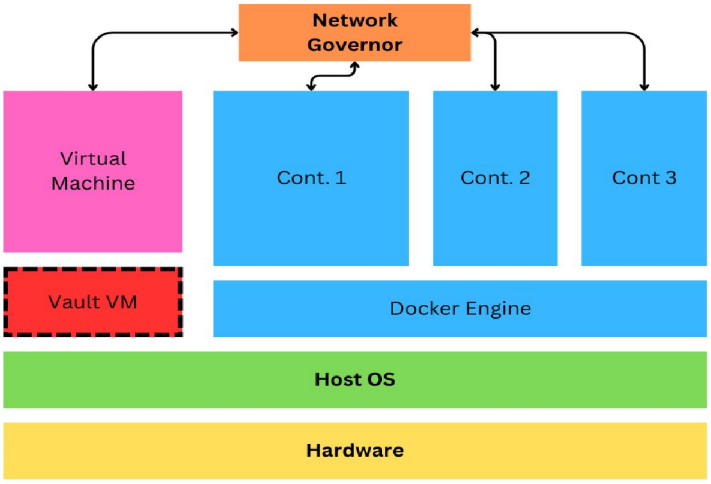

FIGURE 1. Architecture of the Operating System

Stated above is the architecture of this OS, representing how the various sections are all to be laid and constructed. As can be observed the structure has been divided into several sections handling various operations. The application section of the Operating system will be handled by the use of Docker containers represented with blue color in the architecture and the storage section of the operating system will be handled by a Virtual machine in NAS config represented with pink color in the architecture. All the communications between various containers and virtual machines are furnished by a network governor represented by an orange color in the architecture. The architecture also featured a Vault VM, which is a separate virtual machine that is designed to store all the important files of the operating system.

The various sections of the operating system are used to harness the main qualities and minimize the effects of their disadvantages as much as possible.

The Application Section

This part of the operating system is handled by various docker containers as docker provides a much better performance output as compared to virtual machines in common tests. Also, docker provides the functionality of placing applications in separate containers providing better resource utilization and security. Docker technology extensively uses namespaces in various areas for segregating various containers and their applications like the use of namespaces in differentiating processes id's and networks id's of these applications, these implications provide and strengthen the security of and from various apps being running inside the containers as if in case a malicious application even tried to bypass the security features and manipulate the host machines tasks it will not be able to do to that malicious application it will appear as if only one application is being run on the whole machine.

The Storage Section

This part of the operating system is run and managed by a virtual machine which is conferred as a NAS (Network Accessed Storage), this is because the docker containers communicate with each other over a network which allows segregation of the systems. The virtual machine is used for file storage and management as even though virtual machines are slower as compared to docker containers they are still more secure and robust than docker containers, this is because virtual machines use and establish a guest operating system which allows for further separate the machine from the operating system and provide a more secure environment. Viruses Malware and other types of malicious applications often traverse via the

storage of the machine therefore by using a virtual environment for storage of files enhances the security of the Operating System. Further enhancing the security of various applications can be done by creating partitions in the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

storage space for each container, this will create an added layer of security for the files stored and also limit the extent of exposure to viruses if one occurs. Since the virtual machine is configured as NAS it can be used to communicate with external devices like mobile phones, tablets, etc further improving and enhancing the usability of the Operating system.

Network Governor

Network Governor is used to regulate and restrict communications between various components of the operating system. Docker Containers communicate via the use of internal networks and this communication, if in plain text form, could be used to harm other containers in case one container is compromised, the network governor aims to restrict malicious activity by acting as a network firewall. Also as the operating system features a virtual machine configured as NAS the network governor will be used to safeguard the storage section of the operating system when communicating with external devices

Vault VM

Vault VM provides the user with a safe environment to store important files, passwords, documents, photos videos of importance, etc. Vault VM will be optimised for security, this can be achieved by not allowing any network connections like wifi, Bluetooth, Ethernet, internal bridges, etc, also to enhance the security of the VM it can be set up over a separate hypervisor this may reduce the speed of the whole operating system but will be able to provide the best security possible.

This arrangement and use of components provide the best possible performance, usability, security, and room for future growth of the operating system. The architecture is formed to harness the qualities of each component used. The application section is hosted by the use of docker containers providing the best performance and flexibility to applications being run on the system, the storage section hosted by a virtual machine provides a safe and secure place to store and manage all the files on the system while being secure, the network governor acts as a network firewall securing all the communications being carried out inside and outside the operating system, the vault VM gives a security-focused area to store all the sensitive information.

III. CONFIGURATION

To optimise the components being used in this operating system and ensure smooth working of various sections they have to be configured to allow smooth flow of data. The docker containers being used as per the architecture suggest the use of more than one application per container which is not recommended as per its design, The Virtual Machine being used as a NAS has to furnish all the containers with the data being demanded in a swiftly to allow for a smooth experience by the user, the vault must be secured and cause the least amount of hindrance to all the other functions of the operating system. These configurations will allow for a smooth and secure operating system to function properly.

Configurations allow to furnish and fulfil the goals set for the operating system to be attained.

Docker Containers

Docker Containers as per the architecture would be able to host more than one application inside a single container this would allow for faster and smoother inter-app connectivity, reduce the need for communication to and from other containers, increase response time, and improve the efficiency of the system as applications using the same bin files, libraries and are performing the same type of operations can be placed together in one container only. Placing more than one application inside a single container can reduce the flexibility of the containers, management of applications, keeping files up to date, and optimizing system resources can be difficult and may even cause errors, also applications placed inside a single container can interfere with each other and cause errors. To reduce these errors an Application management system can be used and placed inside each container the main goals of this system will be to ensure the smooth working of applications, application management, and updation and resource flexibility, this system will allow the use of more than one applications in one container and also ensure smooth working making the whole system more efficient.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

Virtual Machine

Virtual machines such as NAS allow for a more secure file storage system but due to this feature, the latency and speed of file retrieval will increase significantly causing the system to become slower. To improve the speed and efficiency of the system dedicated internal bridges can be used between the containers and virtual machines making it faster for containers to access data, but this feature can be exploited as malicious apps running on containers can reach and access all the system data making the system vulnerable. Solving this problem the virtual machine would be able to divide the given memory space and make partitions and then allow the containers to access only the sections assigned to them. The following figure explains this system clearly.

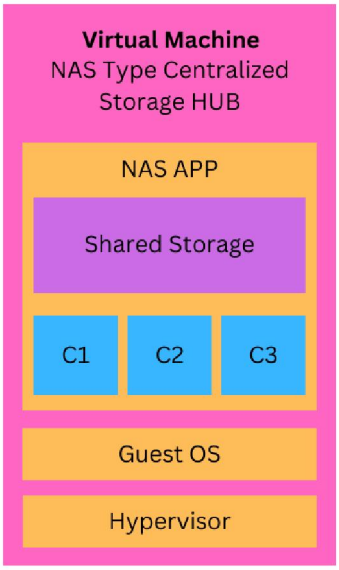

FIGURE 2. Virtual machine Internal architecture

As can be observed for 3 Docker Containers (C1, C2, C3) the memory space has been divided into 4 sections three sections for each container and one section for shared storage space, the containers would be able to freely communicate with their partition space and would require to go through network governor when wanting to access shared storage space or storage space of other containers. Since the Virtual machine is being configured as a NAS and has to actively manage and secure file systems the Guest operating system on the virtual machine must be light, flexible, smart, and secure to not burden the host operating system resources with its needs to fulfill these requirements. Operating systems such as Tiny Core Linux can be used as they are lightweight and are easy to configure as a NAS making the development process faster and easier.

The Vault VM

The Vault VM has the main responsibility of being secure and managing files to do this. A lightweight operating system that is security-centric like Alpine Linux or Arch Linux configured to keep security in mind can be used. These would allow for a security-based approach and also allow for more security features like password access and other methods to be set up. The security system must be made in such a way that it does not become too secure and reduce usability to an extent

IV. CONCLUSION

The designed architecture of the operating system needs further study and performance benchmarking to further strengthen and solidify the design details and goals set by the paper being attainable and the real-world practicality and implications of such an operating system, Comparison Tests must be made against popular operating systems in the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, April 2024

current time like Windows, Apple Mac, and Linux to understand how applicable this operating system is and also to identify and improve areas which can be further furnished to achieve the goals of this system.

V. FUTURE WORK

As this paper only describes the architecture of this operating system will be in the following order measure the performance metrics of this system, craft and modify various components of the system as per the needs and design of the architecture, measure all the metrics, and lay comparison to previous tests, compare the efficiency of this system with other popular systems and then finalize and working model of this Operating system.

REFERENCES

[1]. Author Cynthia E. Irvine, Michael F. Thompson, Michael McCarrin, and Jean Khosalim. Labtainers: "A Docker-based Framework for Cybersecurity Labs", (Naval Postgraduate School).

[2]. Babak Bashari Rad, Mohammad Ahmadi, Harrison John Bhatti. "An Introduction to Docker and Analysis of its Performance Article", (IJCSNS VOL 17 No. 3).

[3]. Thanh Bui. "Analysis of Docker Security". (Aalto University School of Science).

[4]. Amit M Potdara , Narayan D Gb , Shivaraj Kengondc , Mohammed Moin Mulla. "Performance Evaluation of Docker Container and Virtual Machine". (Procedia Computer Science 171 (2020) 1419–1428) . ·

[5]. Weichen Wang. "A cyber-security defence method using Docker Container". (Graduate School. Nashville, TN).

[6]. Emiliano Casalicchio, Vanessa Perciballi.Measuring Docker Performance: "What a mess!!! ".

[7]. (Blekinge Institute of Technology, University of Rome Tor Vergata).

[8]. Docker Documentation: https://docs.docker.com