Constructing Invisible Boundaries: How Cloud Operating Systems Shield Themselves in a Growing Virtual Environment

Shane Snediker (ssnediker07@my.whitworth.edu)
Chad Ross (cross20@my.whitworth.edu)

May 22, 2019

Abstract

The marked transition from personal computer devices and local networks to the cloud necessitates a restructuring and evolution of traditional operating systems toward infrastructure that can adequately sustain cloud computing. This shift in system requirements has rendered cloud operating systems divergent in structure and core make up from their traditional operating system ancestors. While this transition toward portable computing has delivered many benefits, it has also introduced new challenges with regards to computing security. Internet hackers, thieves, and network attackers are relentlessly devoted to infiltrating computer systems and infrastructures to steal and/or corrupt data with malicious intent. This malice introduces a variety of threats to cloud operating systems. The current operating system measures that combat these unwanted intrusions must be improved and perfected and additional techniques will also need to be incorporated into future cloud operating systems.

1 Introduction

As the world relentlessly increases its reliance on the internet and information technology, humanity continues to push the envelope regarding platform infrastructures that can bolster this advancing online dependency. The exponential technological advancement ever since the first personal computer was invented in the 1940s has kept innovators on their toes and consistently has businesses struggling to keep up with the demand for faster, more efficient systems. Ever since the earliest batch operating systems (OS) of the 1950s and 1960s, aggregated improvements have compiled and improved the way an OS manages a computer's system resources, utilizes the processor, and makes a system more user-friendly. For several years, OS technology has focused on managing a single system's hardware and resources. The advent of cloud computing is dramatically altering the responsibility and expectations of OSs. OSs ten years from now will look nothing like the traditional OS that we have grown accustom to.

The cloud provides a virtual network, an ostensibly borderless arena for computing that can be accessed and utilized from any device almost anywhere in the world. But because cloud computing is technically still in its infancy, there are vulnerabilities within the infrastructure that lead towards security concerns. Cyberattacks endanger cloud systems in a variety of ways, including data breaches, cloud application programming interface breaches, pernicious insiders (legitimate cloud users with malevolent intentions), exploitation of the weaknesses of shared technologies (like virtualization and cloud orchestrations), attacks on weak cryptography, and attacks on vulnerabilities within the distributed systems of services within the cloud [5]. Traditional computing platforms focus security efforts on using a perimeter security model, because network perimeters are more readily defined [7]. But, with cloud computing, the networks are highly connected, and the boundaries are much less well defined [7]. This opens the door for traffic to more easily bypass traditional boundaries [7]. Cloud systems are forced to shift the balance of security from a perimeter boundary approach to a data-centric approach [7]. This involves instilling security measures at multiple levels surrounding the data, from encrypting the data, strengthening the authorization process, strengthening the password requirements and demanding two-factor authentication [7]. Cloud OSs enhance security in the cloud through security hardening tools, intrusion detection systems, and regularly updating the definition of computer viruses with the antivirus software that is downloaded onto the OS. In this way, cloud OSs provide an extra layer of protection from security invasions that take place on the cloud.

In this paper, we juxtapose the traditional OS with the cloud OS, discuss security concerns for cloud OSs and give an overview of how cloud OSs best combat such security concerns.

We begin in section two by analyzing conventional OSs and cloud-based OSs in order to provoke and develop a better understanding of the differences between the two. This section will highlight how remote computing has changed the operating system requirements and give an overview of what a cloud OS structure entails.

There is a wide gamut of potential security attacks that a cloud system faces, and in section three of this paper we give an overview of these different types of threats and explain how these unique threats manifest within the cloud community.

We will finish in section four, where we will outline the current security techniques in use by cloud-based OSs.

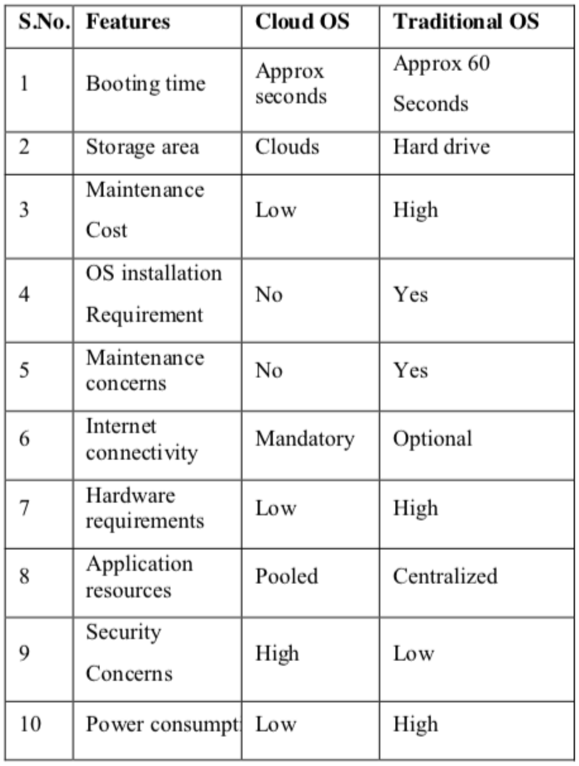
2 Differences Between Conventional and Cloud Operating Systems

The difference between a conventional and cloud OS may not be so obvious. This is due to the fact that virtual machines (VM), which run OSs in the cloud, “typically run the same conventional OSs that [are] used on physical machines” [4]. So, what is the difference then? To begin to understand, it is useful to know what a cloud OS is. A cloud OS focuses on delivering computing resources over the internet that a conventional OS provides directly [4]. It provides these resources through three separate platforms: infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) [3]. Each of these cloud platforms provide their own level of control over the main components of an OS. Certain components are controlled by a conventional OS and other components are controlled by the cloud OS [14].

To further understand the difference between a conventional and a cloud OS, it is vital to understand that the latter performs all of the same functions as the former and some additional functions as well. These additional functions include: management of the network, computing, and storage capacity; of the VM lifecycle; of the VM images; of the security; and of the remote cloud capacity [9]. Each of these must be managed with care as the cloud OS, facing the limitations of running remotely, must utilize resources more efficiently than a conventional OS.

Each of these functions have a significant impact on a cloud OS. The one that has the greatest impact is virtualization. According to [11], “virtualization allows multiple OSs to run on the same physical device at the same time.” [11] goes on to explain, “this allows several users to execute their applications on the same physical environment, but isolated from each other.” A conventional OS would never need to worry about managing multiple other OSs while a cloud OS does. The latter breaks these OSs down into two categories: host and guest [8]. The host OS, being the cloud OS, hosts all the other OSs. These other OSs are the guest OSs and are the client OSs running the client operations.

As a result of managing the VM and other functions, the cloud OS comes with many advantages and some disadvantages compared to a conventional OS. Figure 1 summarizes these with some notable effects being: a cloud OS reduces power consumption on a user's computer and a user's computer can contain lighter hardware and still run heavier OSs [9]. In the words of [9], a cloud OS is “modular, more portable, and convenient to expand” compared to a conventional OS.



S.No.	Features	Cloud OS	Traditional OS
1	Booting time	Approx seconds	Approx 60 Seconds
2	Storage area	Clouds	Hard drive
3	Maintenance Cost	Low	High
4	OS installation Requirement	No	Yes
5	Maintenance concerns	No	Yes
6	Internet connectivity	Mandatory	Optional
7	Hardware requirements	Low	High
8	Application resources	Pooled	Centralized
9	Security Concerns	High	Low
10	Power consumpt	Low	High

Figure 1: Conventional VS Cloud OS [4]

3 Security Dilemmas in Cloud Operating Systems

Now that we’ve taken a look at the key differences between conventional and cloud OSs, we move forward in our discussion to examine the security aspects of cloud OSs.

The allure of the cloud aligns perfectly with the pace of society. Humanity continues to quicken its clock, and with that comes a demand for quicker, more efficient computing. Cloud computing presumes to meet and exceed this demand by promising its clients the prospect of unlimited computing, network, and storage capacity. With this vast advance in responsibility taken on by the cloud comes substantial advantages for the users; however, it is not without a cost. The complexity of cloud computing networks increases the potential entry points for internet attackers to penetrate. And to compound the issue, the methods of these malicious individuals only continue to advance in sophistication.

This section will begin to explore the underlying patterns of attacks on cloud systems as well as describe many of the current methods employed by nefarious online assailants to compromise and obtain data and sensitive information from the cloud OSs. Security threats to cloud OSs generally fall under 7 basic categories: dishonest use of cloud computing, insecure APIs, malicious insiders, shared technology issues, data loss and leakage, account and service hijacking, and unknown risk profiles [2]. A brief description of these categories of security threats follows:

- Dishonest use of cloud computing is common and widespread. Perpetrators of these attacks take advantage of the fact that many cloud providers require very little information for registration. They exploit this relative anonymity to gain access into cloud networks and use such access for dishonest purposes. [2]

- Cloud providers rely on dynamic, multileveled APIs with varying levels of complexity. Cloud providers are still working to catch up their security measures and safeguards to the level of sophistication of the intrusion attempts being exacted against them. [2]

- Many cloud providers fail to adequately vet their employees and lack distinct policies and guidelines for who is allowed to access client's personal data leaving such data vulnerable to exploitation. [2]

- Cloud infrastructures act as a shared resource which provides consumers with a scalability that truly caters to each individual consumer's desired cloud experience. Unfortunately, many of the components of cloud host operating system infrastructures are not equipped to sustain multiple users. These weaknesses render infrastructure sharing systems vulnerable to cyberattacks. [2]

- The compromise of data is common across every platform of computing, and the cloud is definitely not immune from such intrusions. [2]

- Online predators attack by obtaining private information and credentials of innocent cloud consumers and once they obtain this information they commandeer their accounts to gain additional information, steal identities, and make unlawful computing decisions. [2]

- Despite the fact that we are living in a day and age where internet attacks are at an all-time high, many individuals and businesses still do not assume an accurate measure of understanding regarding the security risks and thus do not take sufficient means to protect themselves. Businesses don't realize the sense of urgency required to take security precautions in order to guard against cyberattacks and leave themselves exposed to being violated by cyber criminals. [2]

Now that we've addressed the general areas that cyberattacks fall under, we are going to examine some of the specific attacks rendered in the age of cloud OSs:

- Most cloud providers use the browser as the primary connection for I/O activities. The main drawback for browser-dominant computing is that most browsers lack the capability of accepting XML signatures and encryption methods. Within XML programs, data is sent with a specific XML signature that authenticates the data transmission and verifies that the data is reliable. Without the capacity to accept these XML encryption signatures, browser-led cloud OSs are left with Transport Layer Security (TLS). TLS is a basic level security measure that provides communication security between client and server applications that interact over the internet. The main drawback for cloud OSs that only employ TLS measures is that they are very susceptible to phishing. Once an attacker gains login information through phishing, the TLS model is wholly inept at protecting the user against further intrusions. [13]

- As we just mentioned, XML programs use special XML signatures to ensure authentic data transmission. An attack known as a wrapper attack is gaining momentum where the attacker essentially wraps the authentic XML signature around malevolent code. Because the code contains the authentic signature, it is often allowed transmission and then causes the computer to begin performing unwanted tasks. [13]

- There are a variety of intrusion implementations where attackers lure and deflect cloud users to malicious websites and once they've navigated to these websites they gain access to the user's computer and view their computing activities as well as steal their information and gain unauthorized access to their cloud platforms. [14]

- Most OS security software hooks into the data structures of the OS kernel and runs integrally with the kernel software allowing it to keep track of the computing operations that are particularly susceptible to security breaches, such as file creations and modifications, and network communications. Malicious malware infiltrates this security software and unhinges it from the kernel, rendering its services impotent. [10]

- Cyberattackers attempt to exploit the fact that cloud computing relies on distant data storage and web access because this unavoidably creates multiple levels at which access to the cloud can be interrupted or disrupted. In these attacks, data can be stolen from different servers and locations. [1]

- Another area of concern with regards to cloud security is called Distributed Denial of Service (DDOS). This unique attack happens when a cloud system is maliciously flooded with HTTP requests and XML messages to such an overwhelming extent that it paralyzes the system and blocks access from legitimate users to the system. [12]

- General data attacks on cloud servers are common. These include password and key cracking, phishing, and other code hacking attacks. Many cloud services lack adequate authentication measures and access control mechanisms giving intruders inspiration to attack. Because many services of the cloud are outsourced as opposed to the localized services of traditional systems, many of these services unfortunately circumvent the physical and logical security controls that are common in traditional OSs. [1]

Though there are many other potential security threats in cyberspace, this section has provided and overview of the central dilemmas facing cloud OSs today.

4 Security Solutions in Cloud Operating Systems

To combat the security threats outlined in Section three, a variety of security techniques have been designed. Each technique aims to be resilient to attack, which has resulted in some techniques being designed as preventative measures and others being designed as detective ones [14, 6].

The preventative measures act to prevent security breaches. Some of these techniques are simple and others are more complex. Regardless, none of these methods come without their flaws. There are a variety of breaches that can occur but each security measure is still valuable as, in the same way a fence keeps most intruders out, these techniques keep most attacks against cloud OSs from being successful.

Implementing this type of security, a cloud OS can cut-off its ability to contaminate others by following one simple rule. This rule is to never keep guest OS images that are not in use [8]. Without taking this precaution, contamination could easily infiltrate many cloud OSs. However, taking this precaution results in less guest OSs that could take control of the host OS. To extend this rule further, a host OS must never be migrated from one machine to another without the disks associated with it being wiped first [8]. This prevents any unauthorized physical access to the data stored on the disks and eliminates the possibility of any type of physical attack. Further, security measures such as XML signatures can be implemented to improve security of data. Using an XML signature, the integrity of data can be verified by the cloud OS as it is able to check for a signature and confirm that the data it is working with is safe [13]. Unfortunately, as was shown in section three, this isn't the most secure method of protecting the cloud OS. Therefore, more advanced security measures have created as well.

Protection of the hypervisor, which is the software in control of the VM, is where one of these more advanced security measures comes into play. To protect it, a system called Hypersafe was developed. Hypersafe is a system that maintains code integrity. It extends the hypervisor implementation and prevents its code modification by locking down the write-protected memory pages. As it does this, it secures the hypervisor against the control-flow hijacking attacks by protecting its code from unauthorized attacks. [8] This allows the OS to guarantee that the guest OS has not breached security and that the application code that it is working with is not malicious. Even so, more security measures should be taken to protect the hypervisor. [8] goes on to recommend "hardening the hypervisor" to improve its security. Such a measure can be taken by restricting the administrator functions of the cloud OS and by monitoring hypervisor logs heavily [8].

The virtual machine checkpoint is another method of preventing security breaches. Using this method, the cloud OS is capable of creating a copy of its current state [8]. This copy, called a snapshot, is useful for restoring a virtual machine to a state that is not compromised. It is also useful for finding the weak points in an OS as it works by capturing "the difference between the snapshot and the running state" [8]. This allows for all changes to be tracked so that malicious changes can be ignored.

Although preventing security breaches often works, when cloud OS security fails to prevent security breaches, detective measures work to recover from them. Many of these measures qualify as virtual security appliances, which, due to having more privileged access to the hypervisor, act to perform system and management functions [11]. Examples of these are firewalls, intrusion detection systems, and anti-virus systems [11]. While equipped with these functions, cloud OS security is able to fight against threats such as malware. Malware detection programs, such as Malaware, require signatures to verify that a process is authorized [6]. If a program attempts to run a process that it is not authorized to run, then the cloud OS will flag it as malicious. Malaware also uses techniques to stop attacks where a signature may be a faulty method of securing the cloud OS. Malaware, just as a bank teller memorizes the details of a dollar bill to verify if it is real, Malaware is able to check the page tables associated with a process to detect security breaches [6]. It can also check for "taint," which allow for a process to be flagged as malicious if changes are made to its instructions [6]. Each of these methods improves upon the ability for a cloud OS to detect security breaches and handle them properly.

One final method for securing the cloud has been developed by IBM. This development has resulted in an algorithm being produced which can start monitoring a guest virtual machine at any time and monitor it correctly [10]. To monitor it correctly, IBM has made two assumptions: that the hypervisor is correct and that there are virtual machines which no attacker can breach [10]. Figure 2 demonstrates how the algorithm determines the integrity of the guest kernel in three steps. Following these steps, IBM's system creates a whitelist which can be used later to continually scan the guest OS for unauthorized modifications [10]. If it finds a change that is not in line with the whitelist, then it adds it to a blacklist that tracks malicious processes.

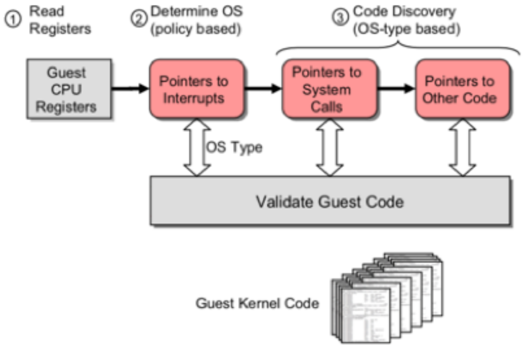


Figure 2: Malaware Security Steps [10]

5 Conclusion

In this work we have discussed the evolution of traditional computer OSs toward systems that are compatible with cloud networks. The cloud has transformed the way that an OS facilitates the use of computer resources and storage. We reviewed the core characteristics of a classical OS and juxtaposed them with emerging systems within the paradigm of cloud computing. After an introduction of the shift in OS structures, this paper explored one of the fundamental challenges facing cloud OSs, namely security. As outlined in section three, there are a wide variety of imminent security threats facing the cloud OS, from sophisticated hacking schemes that subdue system encryptions to corrupt individuals within cloud provider companies benefitting from unauthorized information access to entire system shutdowns due to collaborated, coordinated conspiracies that disrupt and derail cloud services for extended periods of time. We followed this by summarizing the methods that cloud providers employ to combat these security threats. As technology continues to advance at an alarming pace, the level of general information technology competence continues to rise. And with this rise inevitably comes a surge in cyber criminology. This is the unfortunate truth of the world we live in, and cloud providers will be perpetually hard-pressed to improve current security measures as well as evolve new technological strategies to stay ahead of cyberattacks and deliver cloud networks that people can fully trust in.

References

[1] M. I. Al Ladan, "A review and a classifications of mobile cloud computing security issues," 2016.

[2] C. S. Alliance, "Top threats to cloud computing," 2010. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3] O. I. Araoye and K. A. Akintoye, "Security and reliability issue in the deployment of cloud computing system," *Arabian Journal of Business and Management Review*, vol. 5, no. 2, pp. 1–7, 2015. [Online]. Available: https://www.researchgate.net/publication/298951997_Security_and_Reliability_Issues_in_the_Deployment_of_Cloud_Computing_System

[4] N. Bardhan and P. Singh, "Operating system used in cloud computing," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 1, pp. 542–544, 2015. [Online]. Available: ijcsit.com/docs/Volume%206/vol6issue01/ijcsit20150601121.pdf

[5] A. Bryk, "Cloud computing: A new vector for cyber attacks," February 2018. [Online]. Available: https://www.apriorit.com/ dev-blog/523-cloud-computing-cyber-attacks

[6] R. Denz and S. Taylor, "A survey on securing the virtual cloud," *Journal of Cloud Computing*, November 2013. [Online]. Available: https://www.researchgate.net/publication/273073449_A_survey_on_securing_the_virtual_cloud

[7] R. Hat, "What is different about cloud security," 2019. [Online]. Available: https://www.redhat.com/en/topics/security/cloud-security

[8] M. Kazim, R. Masood, M. A. Shibli, and A. G. Abbasi, "Security aspects of virtualization in cloud computing," in *Lecture Notes in Computer Science*, September 2013. [Online]. Available: https://www.researchgate.net/publication/273950406_Security_Aspects_of_Virtualization_in_Cloud_Computing

[9] O. Kumar, D. Rai, and V. Goel, "Cloud as an evolutionary operating system," *Interna-*

tion Journal of Computer Applications, pp. 11–14, November 2012. [Online]. Available: https://pdfs.semanticscholar.org/2aaf/8669e2956fa990000ef5905f31321395839f.pdf

[10] D. S. D. S. D. Z. Mihai Christodorescu, Reiner Sailer, "Cloud security is not (just) virtualization security," 2009.

[11] A. Mishra, R. Mathur, S. Jain, and J. S. Rathore, "Cloud computing security," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 1, no. 1, pp. 36–39, 2013. [Online]. Available: https://www.semanticscholar.org/paper/CLOUD-COMPUTING-SECURITY-Narula-Jain/34b8dd361329d636ce6f04eee2b58019f272d2c0

[12] D. K. Muhammed Abdulazeez, "Hierarchical model for intrusion detection systems in the cloud environment," 2015.

[13] J. C. Roberts and W. Al-Hamdani, "Who can you trust in the cloud? a review of security issues within cloud computing," *Proceedings of the 2011 Information Security Curriculum Development Conference, InfoSecCD'11*, 2011.

[14] V. O. Safonov, *Trustworthy Cloud Computing*. Hoboken, New Jersey: John Wiley and Sons, Inc., 2016.