Chapter 80
Cyber Security Aspects of Virtualization in Cloud Computing Environments: Analyzing Virtualization-Specific Cyber Security Risks

Darshan Mansukhbhai Tank
https://orcid.org/0000-0002-5138-8979
Gujarat Technological University, Ahmedabad, India

Akshai Aggarwal
School of Computer Science, University of Windsor, Canada

Nirbhay Kumar Chaubey
https://orcid.org/0000-0001-6575-7723
Gujarat Technological University, India

ABSTRACT

Cybercrime continues to emerge, with new threats surfacing every year. Every business, regardless of its size, is a potential target of cyber-attack. Cybersecurity in today's connected world is a key component of any establishment. Amidst known security threats in a virtualization environment, side-channel attacks (SCA) target most impressionable data and computations. SCA is flattering major security interests that need to be inspected from a new point of view. As a part of cybersecurity aspects, secured implementation of virtualization infrastructure is very much essential to ensure the overall security of the cloud computing environment. We require the most effective tools for threat detection, response, and reporting to safeguard business and customers from cyber-attacks. The objective of this chapter is to explore virtualization aspects of cybersecurity threats and solutions in the cloud computing environment. The authors also discuss the design of their novel 'Flush+Flush' cache attack detection approach in a virtualized environment.

DOI: 10.4018/978-1-7998-8954-0.ch080

INTRODUCTION

Cybersecurity in today's connected world is a basic component of any establishment. Weak security policies result in major service interruption and data breaches (Michelle, 2018). Cyberspace refers to the environment in which communication occurs over computer networks. The future of cybersecurity is firmly associated with the future of information technology and the advancements of the cyberspace. Cyberspace has become the most popular carrier of information exchange in every corner of our life. With the continuous development of science and technology, especially the virtualization technology, cyberspace security has become the most critical problem for the cloud computing environment (Zhou, Shen, Li, Wang, & Shen, 2018).

As an integral part of most of the business, virtualization is becoming more prevalent in various sectors of society. The virtue of virtualization rests on its ability to cut down operational costs and to provide an effective means of managing Information Technology (IT) resources (Francia, Garrett, & Brookshire, 2013). Virtualization has changed the landscape of technology and revolutionized computing capability. Virtualization has been widely adopted. An enterprise runs most of its workloads in a virtualization environment. A virtualized system has many advantages compared to traditional computing systems. The key benefit of virtualization is to reduce the overall operational cost.

Virtualization is a technique to separate multiple users on a single machine. Virtual Machines (VMs) share the underlying hardware and rely on the software level isolation provided by the hypervisor. The Hypervisor provides virtualization of hardware resources and thus enables multiple computing stacks called VMs to be run on a single physical host (Chandramouli, 2018). The sharing of hardware resources between multiple guest systems optimizes resource usage (Agarwal, 2018). However, it has been discovered and proved that this isolation is not impenetrable (Paundu, 2018).

The objective of this book chapter is to explore virtualization aspects of cybersecurity threats and solutions in the cloud computing environment. The rest of this book chapter is organized as follows. First, we provide some background information on cryptography, cybercrime, and cyber-attacks in the context of cybersecurity. Second, we define cybersecurity and discuss why cybersecurity should be the biggest concern. Third, we narrate the importance of cybersecurity in the cloud computing environment. Fourth, we discuss guidelines and recommendations on the security aspects of virtualization provided by standard security agencies and present taxonomy of virtualization security issues. Fifth, we analyze virtualization specific cybersecurity threats, vulnerabilities, and mitigation techniques. Sixth, we compare various defense mechanisms pertaining to virtualization security. Next, we outline our proposed '*Flush+Flush*' cache attack detection approach. Finally, we conclude this book chapter and discuss future research directions.

BACKGROUND

Cryptography can be defined as a technique of securing private messages by using codes so that only those for whom the message is destined can read and process it. It converts ordinary plain text into impenetrable text and vice-versa. The concept of cryptography has been widely used for secure communication in computer networks. Current cryptographic techniques may be easily defeated by increasing computing power and thus not likely to be more secure.