SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Mohammed M. Alani

Elements of Cloud Computing Security

A Survey of Key Practicalities

Springer

Mohammed M. Alani
Department of Information Technology
Al-Khawarizmi International College
Abu Dhabi
United Arab Emirates

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-41410-2 ISBN 978-3-319-41411-9 (eBook)
DOI 10.1007/978-3-319-41411-9

Library of Congress Control Number: 2016944339

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Foreword

Cloud computing has begun to revolutionize people lives, business, and services. The concept of cloud computing has emerged from virtualization and software design concepts. The emergence of service computing has revolutionized the software development methodologies. Cloud computing also offers different services (SaaS, PaaS, and IaaS) and deployment paradigms (private, public, and hybrid) that help business making relevant combinations that suit businesses and its impact on the global economy. In addition, there are also a number of advancements in the federation of clouds. However, challenges remain predominant to make cloud computing as a successful technology that will reach people and businesses. Such major challenges include cloud security, multitenancy, elasticity, secure and scalable service development and business sustainability.

This book has taken a major step in providing a breadth of knowledge on cloud security with elegance, examples, and comprehensive. This book has presented cloud security concepts in a simplified manner and elegant. Firstly, this book introduces the general concepts of cloud computing and then takes the reader very deeply into general concepts of cloud security techniques. This book has been well organized elegantly with five chapters.

Chapter 1 introduces the basic concepts and its underpinning technologies of cloud computing with simple illustration for all types of readers to understand. This chapter also explains the cloud's different service models and different deployment models. This chapter concludes with a discussion of cloud computing benefits to organizations.

Chapter 2 provides a brief introduction to cloud security. This chapter also discusses why cloud security is different from classical systems security.

Chapter 3 introduces to security threats in cloud computing very elegantly with detailed definitions of nine security threats such as data breaches, data loss, account or service hijacking, insecure interfaces and APIs, threats to availability, malicious insiders, abuse of cloud services, insufficient due diligence, and shared-technology vulnerabilities. In addition to the notorious nine, this chapter also explains additional threats such as lock-in, incomplete data deletion, and loss of governance among other threats along with their mitigation techniques.

Chapter 4 provides examples of cloud security attacks. A group of the most common attacks on the cloud was presented: denial-of-service attacks, hypervisor attacks, resource-freeing attacks, side-channel attacks, and attacks on confidentiality. This chapter also discusses mitigation techniques of those attacks.

Finally, Chap. 5 presents a short list of general security recommendations for the cloud adoption with emphasis given to good practice guidelines.

I am sure this book will make a huge impact on research as well as teaching and will add to a list of recommended books on cloud security. In light of the significant and fast emerging challenges that cloud computing face today, the author of this book has done an outstanding job in selecting the contents of this book. I am confident that this book will provide an appreciated contribution to the cloud computing and security community. It has the potential to become one of the main reference points for the years to come.

Leeds
June 2016

Muthu Ramachandran
www.soft-research.com

Preface

Network security is an ongoing effort full of challenges. It has become an integral part of any network service. With the rapidly increasing number of transactions happening on the Internet, security became a vital part of everyday life.

Network security becomes much more difficult to control when the environment becomes as dynamic and demanding as cloud computing.

Cloud computing aims at reducing costs. This reduction is not only in terms of computing resource, but also in terms of helping its users to focus on the business instead of the information technology enabling this business. Cloud computing has evolved from many different technologies such as virtualization, autonomic computing, grid computing, and many other technologies.

With every new technology, new challenges arise. A very important challenge is to provide adequate security to that cloud to perform as aimed.

This brief focuses on presenting cloud security concepts in a simplified way. After introducing the general concepts of cloud computing, the brief introduces the general concepts of cloud security by going through threats, attacks, and their mitigation techniques.

This brief starts by introducing the concepts and technologies underlying the cloud in Chap. 1. This chapter also explains the cloud's different service models and different deployment models. This chapter concludes with a discussion of cloud computing benefits to organizations.

Chapter 2 gives a brief introduction to cloud security. This chapter discusses why cloud security is different from classical systems security. This chapter also discusses the most famous cloud security incidents in the past few years.

Chapter 3 is devoted to security threats in cloud computing. This chapter discusses the nine most common security threats, referred to as the notorious nine: data breaches, data loss, account or service hijacking, insecure interfaces and APIs, threats to availability, malicious insiders, abuse of cloud services, insufficient due diligence, and shared-technology vulnerabilities. In addition to the notorious nine, this chapter also explains additional threats such as lock-in, incomplete data deletion, and loss of governance among other threats along with their mitigation techniques.

Security attacks on the cloud are discussed in Chap. 4. A group of the most common attacks on cloud was presented: denial-of-service attacks, hypervisor attacks, resource-freeing attacks, side-channel attacks, and attacks on confidentiality. This chapter also discusses mitigation techniques of those attacks.

Chapter 5 presents a short list of general security recommendations for the cloud.

Intended Audience of the Brief

- Researchers working in the cloud security field.
- Professionals in charge or involved in cloud computing.
- Graduate students.
- IT managers aiming to get basic understanding of cloud security challenges.

How to Use This Brief

If you are familiar with the general concepts of the cloud, its service models, and the underlying technologies, you can skip Chap. 1. If you have general knowledge about cloud security and how it is different from classic information security, you can skip Chap. 2 as well.

If you are new to the field of cloud computing, it is suggested that you start from Chap. 1 and go all the way up to Chap. 5.

Acknowledgments

Finally, I would like to thank my editors in Springer. You have made this project easy and simple. Thank you for believing in me. My final thanks go to my family, Marwa, little Aya and Mustafa, and mom and dad. Thank you all for enduring me during the time of working on this brief and all my life. I could not have been blessed more.

Abu Dhabi Mohammed M. Alani
April 2016

Contents

Acronyms

ABE	Attribute-based encryption
API	Application programming interface
AWS	Amazon Web Services
DDoS	Distributed denial of service
DoS	Denial of service
EC2	Elastic Cloud Compute
FTP	File Transfer Protocol
HSVM	Hierarchical secure virtualization model
IaaS	Infrastructure-as-a-Service
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LSM	Linux Security Module
MANET	Mobile ad hoc networks
NTP	Network Time Protocol
PaaS	Platform-as-a-Service
RFA	Resource-freeing attack
SaaS	Software-as-a-Service
SDN	Software-defined network
SETA	Security Educations, Training, and Awareness
SLA	Service Level Agreement
URL	Uniform Resource Locator
VM	Virtual machine
VPS	Virtual private server
VoIP	Voice-over Internet Protocol
WWW	World Wide Web