

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
April 2016

Mohammed M. Alani



<http://www.springer.com/978-3-319-41410-2>

Elements of Cloud Computing Security

A Survey of Key Practicalities

Alani, M.M.

2016, XI, 55 p. 7 illus., Softcover

ISBN: 978-3-319-41410-2