

SPRINGER BRIEFS IN COMPUTER SCIENCE

Tatiana Galibus

Viktor V. Krasnoproshin

Robson de Oliveira Albuquerque

Edison Pignaton de Freitas

Elements of Cloud Storage Security

Concepts, Designs
and Optimized
Practices



Springer

SpringerBriefs in Computer Science

Series editors

Stan Zdonik, Brown University, Providence, Rhode Island, USA

Shashi Shekhar, University of Minnesota, Minneapolis, Minnesota, USA

Jonathan Katz, University of Maryland, College Park, Maryland, USA

Xindong Wu, University of Vermont, Burlington, Vermont, USA

Lakshmi C. Jain, University of South Australia, Adelaide, South Australia, Australia

David Padua, University of Illinois Urbana-Champaign, Urbana, Illinois, USA

Xuemin (Sherman) Shen, University of Waterloo, Waterloo, Ontario, Canada

Borko Furht, Florida Atlantic University, Boca Raton, Florida, USA

V.S. Subrahmanian, University of Maryland, College Park, Maryland, USA

Martial Hebert, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

Katsushi Ikeuchi, University of Tokyo, Tokyo, Japan

Bruno Siciliano, Università di Napoli Federico II, Napoli, Campania, Italy

Sushil Jajodia, George Mason University, Fairfax, Virginia, USA

Newton Lee, Newton Lee Laboratories, LLC, Tujunga, California, USA

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

Tatiana Galibus • Viktor V. Krasnoproshin
Robson de Oliveira Albuquerque
Edison Pignaton de Freitas

Elements of Cloud Storage Security

Concepts, Designs and Optimized Practices

 Springer

Tatiana Galibus
Belarusian State University
Minsk, Belarus

Viktor V. Krasnoproshin
Belarusian State University
Minsk, Belarus

Robson de Oliveira Albuquerque
University of Brasília
Brasília, Brazil

Edison Pignaton de Freitas
Federal University of Rio Grande do Sul
Porto Alegre, Brazil

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-44961-6 ISBN 978-3-319-44962-3 (eBook)
DOI 10.1007/978-3-319-44962-3

Library of Congress Control Number: 2016955170

© The Author(s) 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Abstract

This book is a result of scientific and industrial collaboration in the field of cloud protection. It provides guidelines for the practical implementation of security architecture in a particular corporate cloud. The authors are mathematicians and specialists in data modeling and security. The scientific collaboration with the industry inspired the authors to attempt to conceptualize the common processes and strategies in cloud security in order to make the security system deployment as simple and transparent as possible. The deployment is broken in several essential steps that allow splitting the functionality of the security architecture of any cloud into a set of modules. The first step is the level of architecture where the authentication and key establishment procedures are identified. The second step provides the support of the authorization and other additional security mechanisms for each component of the cloud. The continuous verification of security support on all levels (data, processes, and communication channels) allows avoiding the common security breaches and protecting against the most dangerous attacks at maximum. Additionally, it is proposed to perform the optimization of the selected set of mechanisms in order to intensify the efficiency of the security system.

Preface

Cloud-based systems are gaining importance due to the number of companies that are adopting them as the IT support for their core activities. With this increase in the number of cloud users, the visibility of these systems is also increasing, which calls the attention of cybercriminals to expend time trying to attack them. The goal of these criminals is to have access to valuable data of individual or corporate users. In this context, the cloud security is an important current issue in IT. The list of problems related to cloud security is large [1], inheriting all sorts of network attacks usually performed against corporate servers, but it also includes brand new types of attacks tailored to the new cloud environment. However, in the other end, IT security professionals are working hard to create solutions for these problems, which makes the list of solutions as big as the list of problems or even larger [2].

The Cloud Security Alliance (CSA), an organization that promotes the best practices for providing security assurance within cloud computing, provides a list of problems and currently available countermeasures, besides those that are being developed. The list of problems released by CSA in March 2016, known as the “Treacherous 12” [3], describes the 12 top security threats organizations face in the cloud computing environment. The problems covered by this list summarize the concerns about cloud security organizations have to care about. Its goal is to present knowledge about the most important problems so that companies can prevent them and properly get the benefits of cloud computing, without incurring in the drawbacks raised by the possible vulnerabilities.

Despite an active community sharing information about the problems organization may face in the cloud environment, an important problem is still an absence of a strategic approach in this field to face these problems. In other words, a practitioner, i.e., an IT security professional, incurs the risk to become lost among the several possible methods of protection. In light of this fact, it is possible to state that

there is a clear need for a straightforward guide able to provide an understanding of the placement and the need for specific security mechanisms. The basic set of questions asked by these professionals is as follows:

1. How to implement a security system for a cloud? This is a very general question, which in fact involves several others. The very first one is related to the type of the cloud that it is taken into concern, i.e., which is the adopted cloud model (private, public, hybrid, community)? What is the volume of data stored in this cloud? Are there confidentiality concerns? If so, in which level? What are the possible threats and vulnerabilities a given company must care about? In summary, before trying to answer the main question about how to implement a security system for a given cloud, there is a need for a well-defined characterization of the cloud environment and the involved risks that specific cloud will face. Only after this characterization is it possible to start thinking about a concrete implementation of a security system.
2. Where to start? Okay, the IT personnel in charge of the cloud security have done the characterization of the cloud environment that has to be secured and started thinking about its implementation. However, where should they start? Which part of the cloud should be handled and in which order? Is there any requirement to be considered beforehand?
3. How to select the necessary mechanisms? From the myriad of available security mechanisms that can be adopted, which one should be selected and why? Which one is the most suitable? Informed decisions must be taken, and after taken, they have to be justified.
4. How to verify that the system is optimal? Mechanisms are finally selected and implemented, that's all? Not at all! How to verify the adopted security solution is optimal? This concerns not only the optimality in terms of covering all identified possible threats and vulnerabilities but also in allowing the system perform its activities without performance degradation due to the security mechanisms' overhead.
5. How to verify its security? Fine, the security system was finally implemented covering the requirements presented by the characterization, taking into account performance issues and other concerns. At this point in time, personnel in charge of the security can rest, right? Unfortunately, the answer is a sounding no! After all the work that was done, the security team has to perform exhaustive penetration tests. They have to check every possible breath that may still exist, as well as be diligent and continuously verify if the adopted security solution is really the most suitable one.

It is possible to conclude that in the field of cloud security, there is a demand for specific practice-oriented models. Such models should help practitioners to understand the cloud environment they have to protect, what are the alternatives they have to implement this protection, and how to verify that a given adopted alternative is

really the most suitable one. Understanding this need, this book approaches the problem of cloud security in a concrete and straightforward way. It proposes a transparent protection system model based on a cryptographic approach that can be easily verified for security requirements. The proposal is based on a modular approach, i.e., on a set of interdependent mechanisms oriented toward solutions for specific tasks. The modular structure of a proposed model allows adjusting and optimizing the system according to the required needs. This means that it is able to scale according to the size of the cloud, but also is able to tackle specificities of the different types of cloud models. Additionally, the book answers the question about how to start by proposing an iterative two-step method of constructing a security system for a cloud environment.

The advantages of the proposed approach are transparency, adjustability, and the systematic construction. This allows adapting the solution for different needs, providing a step-by-step method to build up and run a security system for clouds.

With the aim to address the abovementioned topics, the content of this book is pedagogically organized in order to facilitate the readers' understanding. Following this principle, the book is structured as follows:

The first chapter presents the current cloud storage landscape. It describes the basic types of cloud from the point of publicity as well as the important characteristics concerning security. The main concepts and characteristics of cloud-based systems are also revisited in order to provide a comprehensive background to the reader. The chapter describes the main processes, components, and services of the cloud storages. The chapter also discusses a set of requirements for the cloud system life cycle and the appropriate set of requirements for cloud security system. These requirements provide the basis for a specification of the goals of a cloud protection system.

The second chapter classifies the basic vulnerabilities and attacks on the cloud. The types of attacks are specified according to the type of cloud, component, and process, and the vulnerabilities are also specified according to the component or process. The chapter formulates the basic security problem for the cloud, i.e., the set of security requirements for the security system in the cloud. The details provided in this chapter complement to more generic and high-level ones discussed in the previous chapter.

The third chapter specifies the basic mechanisms of the security system. It gives the definitions and the strategies in mobile security, authentication and key distribution, authorization, and threat intelligence. The mechanisms are specified in accordance with attacks they neutralize. This chapter is organized so that the reader can easily refer to the definition and basic functionality of a specific mechanism and go further on the details, according to his/her needs.

Finally, the last chapter provides the practical recipe to solve the security problems that affect cloud storage systems. It contains the best practices and their analysis from the point of security and optimization. As it was highlighted above, it is

important to analyze the suitability of a given security solution, not only in terms of how well it addresses a given security problem but also in terms of the overhead it imposes to the system. This aspect refers to the suitability of the security solution under consideration. An illustrative example is provided in order to make clear for the readers how to address the studied security problems. This example describes a practical solution to protect cloud storage, referring to the detailed content presented through the book content.

Minsk, Belarus

Brasília, Brazil

Porto Alegre, Rio Grande do Sul, Brazil

Tatiana Galibus

Viktor V. Krasnoproshin

Robson de Oliveira Albuquerque

Edison Pignaton de Freitas

References

1. US Department of Defense. Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 2, 18 March, 2016
2. Cloud Security Alliance.
3. Cloud Security Alliance. “The treacherous 12 – cloud computing top threats in 2016” Available online:https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Contents

1	Cloud Environment Security Landscape	1
1.1	Cloud Computing Model Background	1
1.2	Cloud Service Models	3
1.3	Deployment Models	6
1.4	Cloud Storage Classification	8
1.4.1	Corporate Cloud Storage Types	9
1.4.2	Corporate Cloud Storage Components.....	10
1.4.3	Centralization Features.....	11
1.4.4	Basic Scenarios	11
1.5	Cloud Security Requirements	12
1.5.1	Top Cloud Security Threats.....	14
1.5.2	Cloud Security Requirements Recommendation	17
	References.....	18
2	Common Cloud Attacks and Vulnerabilities	19
2.1	Types of Attacks in Cloud Systems.....	19
2.2	Classification of Attacks According to General Security Mechanisms	25
2.3	Classification of Vulnerabilities According to General Security Mechanisms	27
2.4	Threats Applied to Cloud Solutions	27
2.5	Classification of Threats According to General Security Mechanisms	31
2.6	Adversary Types Related to Cloud Solution Providers.....	31
	References.....	34
3	Cloud Storage Security Mechanisms	37
3.1	Authentication and Tokenization.....	37
3.1.1	Definition and Specific Characteristics	37
3.1.2	Types of Authentication	38
3.1.3	Usage of Tokens in the Cloud Storage	40

- 3.2 Key Distribution and Data Encryption..... 41
 - 3.2.1 Encryption in the Cloud 42
 - 3.2.2 Additional Methods..... 44
 - 3.2.3 Key Distribution..... 45
 - 3.2.4 Key Storing and Using 45
- 3.3 Authorization and Access Control Support..... 49
 - 3.3.1 Definition and Implementation of Access Control..... 49
 - 3.3.2 Access Control Models and Policies..... 50
 - 3.3.3 Access Control Methods 51
 - 3.3.4 Key Renewal and Revocation..... 53
 - 3.3.5 Authorization Vulnerabilities, Attacks, and Requirements ... 53
- 3.4 Threat Intelligence 54
- 3.5 Cloud Storage Component Security..... 58
 - 3.5.1 Server-Side Protection..... 59
 - 3.5.2 Client-Side Protection 61
 - 3.5.3 Mobile Device Protection..... 62
 - 3.5.4 Channel Protection Mechanisms..... 65
- References..... 66
- 4 Cloud Storage Security Architecture 69**
 - 4.1 General Model of the Security System 69
 - 4.2 Step-by-Step Security System Construction 71
 - 4.3 Identification of the Identity Management Infrastructure 74
 - 4.3.1 Formal Model of Identity Management Infrastructure 74
 - 4.3.2 Types of IMI in Relation to Cloud Storages 75
 - 4.3.3 Proposed Authentication Solutions 77
 - 4.4 Identification of Access Control Framework 78
 - 4.4.1 Setting Up Security Policies..... 78
 - 4.4.2 Configuring the Data Encryption 81
 - 4.4.3 Configuring Key Management 83
 - 4.5 Identification of Threat Intelligence Unit..... 86
 - 4.6 Identification of the Component Security Framework..... 86
 - 4.6.1 The Basic Strategies to Organize the Server Protected Storage 87
 - 4.6.2 The Basic Strategies to Secure the Client Application..... 90
 - 4.7 Security Optimization and Verification 91
 - 4.7.1 Attack Prevention Verification 91
 - 4.7.2 Component Security Testing 91
 - 4.7.3 Security Optimization 91
 - 4.8 The Practical Implementation 94
 - References..... 100
- Afterword..... 101**
 - Reference 101