Computer Communications and Networks

For further volumes:
http://www.springer.com/series/4198

The Computer Communications and Networks series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

Siani Pearson • George Yee
Editors

Privacy and Security for Cloud Computing

Springer

Editors
Siani Pearson
Cloud and Security Laboratory
HP Labs
Filton, Bristol, UK

George Yee
Department of Systems
and Computer Engineering
Carleton University
Ottawa, ON, Canada

Series Editor
Professor A.J. Sammes, BSc, MPhil, PhD,
FBCS, CEng
Centre for Forensic Computing
Cranfield University
DCMT, Shrivenham
Swindon
UK

ISSN 1617-7975
ISBN 978-1-4471-4188-4 ISBN 978-1-4471-4189-1 (eBook)
DOI 10.1007/978-1-4471-4189-1
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012946924

© Springer-Verlag London 2013
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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
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.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

We live in a period where almost every member of the IT community argues about cloud computing and its security and trustworthiness, and very often does this in generic terms or, worse still, with statements based on false myths and a FUD (fear, uncertainty and doubt) approach. I was therefore very pleased to read through the pages of this book, with its excellent collection of ideas, concepts and criticisms of the current state of the art, as well as cutting-edge solutions to safe provision of cloud computing, performance of informed risk-based decision-making and architecting secure, reliable and legally compliant cloud services. The book comes with a perfect timing, as it supports the cloud-computing community during a period of crucial business and policy decision-making and action (e.g., with activities including the European Cloud Strategy, Governmental Clouds and the revision of the Privacy and Data Protection legislation in the EU, the USA and New Zealand).

In my view, this is a book written by thought leaders for thought leaders, critical minds and forward looking cloud strategists.

Managing Director, Cloud Security Alliance Europe — Daniele Catteddu

Preface

> … many still hesitate before the Cloud. They worry: how do I know what service I am buying? Will my data be protected? Which providers can I trust? If I don't like what I am getting, can I switch providers easily? Or, if I really don't like what I'm getting, can I easily enforce the contract through legal action?
>
> EU Commissioner Neelie Kroes – Setting up the European Cloud Partnership, World Economic Forum, Davos, Switzerland, 26th January 2012

Overview and Goals

Cloud computing has emerged to address an explosive growth of web-connected devices and to handle massive amounts of data. It is defined and characterized by massive scalability and new Internet-driven economics. Despite the enormous potential and rapid growth, privacy, security and trust for cloud remain areas of concern and uncertainty, and the risks need to be better understood. This is a major barrier to the switch to cloud models, due largely to lack of consumer trust and to regulatory complexity. New solutions need to be developed urgently. Of course, there is a strong business pull for this from regulators, governmental initiatives and companies. For example:

> The government will push ahead with … the shift towards cloud computing. It will mandate the reuse of proven, common application solutions and policies. These solutions must balance the need to be open, accessible and usable with the growing cyber-security threat and the need to handle sensitive information with due care.

from UK Government ICT Cloud Strategy, http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf

This book analyses privacy and security issues related to cloud computing and provides a range of in-depth cutting-edge chapters describing proposed solutions from researchers specializing in this area. It is a collection of papers on privacy, security, risk and trust in cloud computing that is loosely based upon selected papers from the International Workshop on Cloud Privacy, Security, Risk & Trust (CPSRT 2010)

at the IEEE 2nd International Conference on Cloud Computing Technology and Science, as well as some additional invited chapters from PC and steering committee members.

Addressing privacy issues in cloud computing is not a straightforward issue. Privacy laws both at the location of processing and at the location of data origin may need to be taken into account. Cloud computing can exacerbate this requirement, since the geographic location of processing can be extremely difficult to determine due to cloud computing's dynamic nature. Another issue is user-centric control, which can be a legal requirement and also something consumers want. However, in cloud computing, the consumers' data is processed in the cloud, on machines they do not own or control, and there is a threat of theft, misuse or unauthorized resale. Thus, the build-up of adequate trust for consumers to switch to cloud services can in some cases become an important necessity.

In the case of security, some cloud-computing applications simply lack adequate security protection such as fine-grained access control and user authentication. Since enterprises are attracted to cloud computing due to potential savings in IT outlay and management, it is necessary to understand the business risks involved. If cloud computing is to be successful, it must be trusted by its users. Therefore, we need to clarify what the components of such trust are and how trust can be achieved for security as well as for privacy.

Cloud business models can magnify privacy and security issues faced in subcontracting and offshoring. The cloud's dynamism renders inappropriate many traditional mechanisms for establishing trust and regulatory control. The cloud's autonomic and virtualized aspects can bring new threats, such as cross-virtual machine side-channel attacks, or vulnerabilities due to data proliferation, dynamic provisioning, the difficulty in identifying physical servers' locations or a lack of standardization. Furthermore, although service composition is easier in cloud computing, some services might have a malicious source. In general in the cloud, establishing risks and obligations, implementing appropriate operational responses and dealing with regulatory requirements are more challenging than with traditional server architectures.

As shown in the Trust Domains project,[1] business customers value high transparency, remediation and assurance, and if organizations can provide these, the customers will trust the organizations more and their brand image will be improved. If an organization is a cloud service provider or operator, this trust translates to a greater willingness for its customers to make the switch to cloud. This is particularly the case where business confidential or sensitive information is involved. Moreover, as customers shift to cloud models, they shift their focus from systems (which they used to control) to data and how that will be treated by other entities on their behalf. They require assurance that their data will be treated properly. This requires mechanisms to provide both adequate security for all data and also protection of

[1] Crane, S., Gill, M.: Framework and Usage Scenarios for Data Sharing. D1.3, Trust Domain Guide, March (2012). http://www.hpl.hp.com/research/cloud_security/TDoms_WP1_D1_3_-_Trust%20Domain%20Guide_-_Rel_1_0.pdf

personal data. By using these mechanisms, risk is reduced both for organizations and their customers. These risks are a top concern when moving to cloud computing. For example, the European Network and Information Security Agency (ENISA)'s cloud-computing risk assessment report states "loss of governance" as a top risk of cloud computing, especially for infrastructure as a service (IaaS). "Data loss or leakages" is also one of the top seven threats the Cloud Security Alliance (CSA) lists in its *Top Threats to Cloud Computing* report.

Organization of This Book

This book reports on the latest advances in privacy, security and risk technologies within cloud environments. It is organized into eight chapters across four headings. References are included at the end of each chapter, and a Glossary of terms is given at the end of the book.

A brief description of each chapter follows.

Part I: Introduction to the Issues

Chapter 1: "Privacy, Security and Trust in Cloud Computing"
This chapter begins by providing background information on cloud computing and on the relationship between privacy, security and trust. It then assesses how security, trust and privacy issues occur in the context of cloud computing and briefly discusses ways in which they may be addressed.

Part II: Law Enforcement and Audits

Chapter 2: "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent"
This chapter considers various forensic challenges for legal access to data in a cloud-computing environment and discusses questions of power raised by the exercise of legal access enforcement.

Chapter 3: "A Privacy Impact Assessment Tool for Cloud Computing"
This chapter discusses requirements for Privacy Impact Assessments (PIAs) for the cloud and explains how a PIA decision support tool may be constructed.

Chapter 4: "Understanding Cloud Audits"
This chapter discusses the use of cloud audits to attenuate cloud security problems, including an agent-based "Security Audit as a Service" architecture.

Part III: Security and Integrity

Chapter 5: "Security Infrastructure for Dynamically Provisioned Cloud Infrastructure Services"
This chapter discusses conceptual issues, basic requirements and practical suggestions for provisioning dynamically configured access control services in the cloud.

Chapter 6: "Modeling the Runtime Integrity of Cloud Servers: A Scoped Invariant Perspective"
This chapter proposes scoped invariants as a primitive for analyzing a cloud server for its integrity properties. A key benefit of this approach is that the confirmation of integrity can increase trust in the cloud server, and its capacity to properly handle customers' data.

Part IV: Risk Considerations

Chapter 7: "Inadequacies of Current Risk Controls for the Cloud"
This chapter examines the applicability (with respect to various service interfaces) to cloud-computing environments of controls that are currently deployed according to standards and best practices for mitigating information-security risks within an enterprise.

Chapter 8: "Enterprise Information Risk Management: Dealing with Cloud Computing"
This chapter discusses risk management for cloud computing from an enterprise perspective. The discussion includes decision-making and developments in trusted infrastructures, using examples and case studies.

Target Audiences

The target audience for this book is composed of business professionals, students and researchers interested in (or already working in) the field of privacy and security protection for the cloud and/or complex service provisioning.

This book would be of interest to an audience spanning a variety of disciplines. The broad range of topics addressed centres around privacy and security issues and approaches related to cloud computing including trust, risk and legal aspects. For newcomers to these areas, the book provides a solid overview of privacy, security and trust issues in the cloud. For experts, it provides details of novel cutting-edge research in inter-related areas as carried out by the various authors.

Acknowledgements

We would like to thank the authors for their excellent contributions to this book. In addition, we are grateful to Springer UK – and in particular Simon Rees – for helpful guidance throughout the book production process.

Our thanks are also due to our management within our respective institutions for supporting us in producing this material.

Siani Pearson
and George Yee

Contents

Part IV Risk Considerations

Contributors

Adrian Baldwin HP Labs, Bristol, UK

Andrew Charlesworth Centre for IT and Law, University of Bristol, Bristol, UK

Nathan Clarke Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, Germany

School of Computing and Security, Edith Cowan University, Perth, WA, Australia

Sadie Creese Cyber Security Centre, Department of Computer Science, University of Oxford, Oxford, UK

Yuri Demchenko University of Amsterdam, Amsterdam, The Netherlands

Cees de Laat University of Amsterdam, Amsterdam, The Netherlands

Frank Doelitzscher Cloud Research Lab, Furtwangen University, Furtwangen im Schwarzwald, Germany

Joan A. García-Espín I2CAT Foundation, Barcelona, Spain

Michael Goldsmith Cyber Security Centre, Department of Computer Science, University of Oxford, Oxford, UK

Paul Hopkins Security and Identity Management Department, Logica, Reading, UK

Martin Knahl Cloud Research Lab, Furtwangen University, Furtwangen im Schwarzwald, Germany

Diego R. Lopez Telefonica I+D, Madrid, Spain

Antonio Morales RedIRIS, Madrid, Spain

Canh Ngo University of Amsterdam, Amsterdam, The Netherlands

Siani Pearson Cloud and Security Lab, HP Labs, Bristol, UK

Calton Pu College of Computing, Georgia Institute of Technology, Atlanta, GA, USA

David Pym University of Aberdeen, Aberdeen, UK

Anand Rajan Corporate Technology Group, Intel Corporation, Hillsboro, OR, USA

Christoph Reich Cloud Research Lab, Furtwangen University, Furtwangen im Schwarzwald, Germany

Carlos V. Rozas Corporate Technology Group, Intel Corporation, Hillsboro, OR, USA

Simon Shiu HP Labs, Bristol, UK

David Tancock Department of Computer Science, University of Bristol, Bristol, UK

Ian Walden Centre for Commercial Law Studies, Queen Mary, University of London, London, UK

Jinpeng Wei School of Computing and Information Sciences, Florida International University, Miami, FL, USA

George Yee Carleton University, Ottawa, ON, Canada

Feng Zhu School of Computing and Information Sciences, Florida International University, Miami, FL, USA