

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Nora Cuppens-Boulahia
Frédéric Cuppens
Joaquin Garcia-Alfaro (Eds.)

Data and Applications Security and Privacy XXVI

26th Annual IFIP WG 11.3 Conference, DBSec 2012
Paris, France, July 11-13, 2012
Proceedings

 Springer

Volume Editors

Nora Cuppens-Boulaia

Frédéric Cuppens

Joaquín García-Alfaro

Télécom Bretagne, Campus de Rennes 2

rue de la Châtaigneraie

35512 Cesson Sévigné Cedex, France

E-mail: {nora.cuppens, frederic.cuppens, joaquin.garcia} @telecom-bretagne.eu

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-31539-8

e-ISBN 978-3-642-31540-4

DOI 10.1007/978-3-642-31540-4

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940756

CR Subject Classification (1998): C.2.0, K.6.5, C.2, D.4.6, E.3, H.4, C.3, H.2.7-8, E.1

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

© IFIP International Federation for Information Processing 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

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

Preface

This volume contains the papers presented at the 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2012). The conference, hosted for the first time in Paris, France, July 11–13, 2012, offered outstanding research contributions to the field of security and privacy in Internet-related applications, cloud computing and information systems.

In response to the call for papers, 49 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty and technical quality. Each paper was reviewed by at least three members of the Program Committee. The Program Committee meeting was held electronically with intensive discussion over a period of one week. Of the papers submitted, 17 full papers and 6 short papers were accepted for presentation at the conference. The conference program also included two invited talks by Patrick McDaniel (Pennsylvania State University) and Leon van der Torre (University of Luxembourg).

Several trends in computer security have become prominent since the beginning of the new century and are considered in the program. These include the proliferation of intrusions that exploit new vulnerabilities, the emergence of new security threats against security and privacy, the need to adapt existing approaches and models to handle these threats and the necessity to design new security mechanisms for cloud computing infrastructure. Reflecting these trends, the conference includes sessions on security and privacy models, privacy-preserving technologies, secure data management, smart card, intrusion, malware, probabilistic attacks and cloud computing security.

The success of this conference was the result of the effort of many people. We would especially like to thank Joaquin Garcia-Alfaro (Publication Chair), Said Oulmakhzoune (Web Chair), Ghislaine Le Gall (Local Arrangements Chair) and Artur Hecker (Sponsor Chair). We also thank EADS/Cassidian and the Institut Mines Télécom for their financial support.

We gratefully acknowledge all authors who submitted papers for their efforts in continually enhancing the standards of this conference. It is also our pleasure to thank the members of the Program Committee and the external reviewers for their work and support.

Last but not least, thanks to all the attendees. We hope you will enjoy reading the proceedings.

July 2012

David Sadek
Frédéric Cuppens
Nora Cuppens-Boulahia

VIII Organization

Jason Crampton	Royal Holloway, UK
Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Bouhahia	Télécom Bretagne, France
Mourad Debbabi	Concordia University, Canada
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Eduardo B. Fernandez	Florida Atlantic University, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Simon Foley	University College Cork, Ireland
Sara Foresti	Università degli Studi di Milano, Italy
Alban Gabillon	University of French Polynesia, France
Ehud Gudes	Ben-Gurion University, Israel
Ragib Hasan	University of Alabama at Birmingham, USA
Sushil Jajodia	George Mason University, USA
Wael Kanoun	Alcatel-Lucent, France
Sokratis Katsikis	University of Piraeus, Greece
Adam J. Lee	University of Pittsburgh, USA
Yingjiu Li	Singapore Management University, Singapore
Peng Liu	The Pennsylvania State University, USA
Jorge Lobo	IBM T.J. Watson Center Research, USA
Javier Lopez	University of Malaga, Spain
Emil Lupu	Imperial College, UK
Martin Olivier	University of Pretoria, South Africa
Stefano Paraboschi	Università di Bergamo, Italy
Wolter Pieters	University of Twente, The Netherlands
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Kui Ren	Illinois Institute of Technology, USA
Mark Ryan	University of Birmingham, UK
Kouchi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Anoop Singhal	NIST, USA
Traian Marius	Truta Northern Kentucky University, USA
Leon van der Torre	University of Luxemburg, Luxemburg
Vijay Varadharajan	Macquarie University, Australia
Jaideep Vaidya	Rutgers University, USA
Lingyu Wang	Concordia University, Canada
Meng Yu	Virginia Commonwealth University, USA
Xinwen Zhang	Samsung Information Systems, USA
Jianying Zhou	Institute for Infocomm Research, Singapore
Zutao Zhu	Google Inc., USA

Additional Reviewers

Massimiliano Albanese
Damià Castellà-Martínez
Tom Chothia
William Fitzgerald
Xingze He
Deguang Kong
Meixing Le
Min Li
Giovanni Livraga
Santi Martinez-Rodriguez
Takashi Nishide
Adam O'Neill
Ruben Rios
Georgios Spathoulas
Xiaoyan Sun
Emre Uzun
Duminda Wijesekara
Jia Xu
Lei Zhang
Yufeng Zhen

Sergiu Bursuc
Ramaswamy Chandramouli
Nicholas Farnan
Nurit Gal-Oz
Masoud Koleini
Kostas Lambrinoudakis
Younho Lee
Jia Liu
Luigi Logrippo
Dieudonne Mulamba
David Nuñez
Thao Pham
Jordi Soria-Comas
Chunhua Su
Isamu Teranishi
Guan Wang
Lei Xu
Shengzhi Zhang
Yulong Zhang

Table of Contents

Invited Paper

Logics for Security and Privacy	1
<i>Leendert van der Torre</i>	

Access Control

A User-to-User Relationship-Based Access Control Model for Online Social Networks	8
<i>Yuan Cheng, Jaehong Park, and Ravi Sandhu</i>	
Automated and Efficient Analysis of Role-Based Access Control with Attributes	25
<i>Alessandro Armando and Silvio Ranise</i>	
A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC	41
<i>Xin Jin, Ram Krishnan, and Ravi Sandhu</i>	

Confidentiality and Privacy

Signature-Based Inference-Usability Confinement for Relational Databases under Functional and Join Dependencies	56
<i>Joachim Biskup, Sven Hartmann, Sebastian Link, Jan-Hendrik Lochner, and Torsten Schlotmann</i>	
Privacy Consensus in Anonymization Systems via Game Theory	74
<i>Rosa Karimi Adl, Mina Askari, Ken Barker, and Reihaneh Safavi-Naini</i>	
Uniform Obfuscation for Location Privacy	90
<i>Gianluca Dini and Pericle Perazzo</i>	

Smart Cards Security (Short Papers)

Security Vulnerabilities of User Authentication Scheme Using Smart Card	106
<i>Ravi Singh Pippal, Jaidhar C.D., and Shashikala Tapaswi</i>	
Secure Password-Based Remote User Authentication Scheme with Non-tamper Resistant Smart Cards	114
<i>Ding Wang, Chun-guang Ma, and Peng Wu</i>	

A Friendly Framework for Hidding *fault enabled virus* for Java Based Smartcard 122
Tiana Razafindralambo, Guillaume Bouffard, and Jean-Louis Lanet

Privacy-Preserving Technologies

Approximate Privacy-Preserving Data Mining on Vertically Partitioned Data 129
Robert Nix, Murat Kantarcioglu, and Keesook J. Han

Security Limitations of Using Secret Sharing for Data Outsourcing 145
Jonathan L. Dautrich and Chinya V. Ravishankar

Privacy-Preserving Subgraph Discovery 161
Danish Mehmood, Basit Shafiq, Jaideep Vaidya, Yuan Hong, Nabil Adam, and Vijayalakshmi Atluri

Data Management

Decentralized Semantic Threat Graphs 177
Simon N. Foley and William M. Fitzgerald

Code Type Revealing Using Experiments Framework 193
Rami Sharon and Ehud Gudes

From MDM to DB2: A Case Study of Security Enforcement Migration 207
Nikolay Yakovets, Jarek Gryz, Stephanie Hazlewood, and Paul van Run

Intrusion and Malware

XSS-Dec: A Hybrid Solution to Mitigate Cross-Site Scripting Attacks... 223
Smitha Sundareswaran and Anna Cinzia Squicciarini

Randomizing Smartphone Malware Profiles against Statistical Mining Techniques 239
Abhijith Shastry, Murat Kantarcioglu, Yan Zhou, and Bhavani Thuraisingham

Probabilistic Attacks and Protection (Short Papers)

Layered Security Architecture for Masquerade Attack Detection 255
Hamed Saljooghinejad and Wilson Naik Bhukya

k-Anonymity-Based Horizontal Fragmentation to Preserve Privacy in Data Outsourcing..... 263
Abbas Taheri Soodejani, Mohammad Ali Hadavi, and Rasool Jalili

Reconstruction Attack through Classifier Analysis	274
<i>Sébastien Gambs, Ahmed Gmati, and Michel Hurfin</i>	
Cloud Computing	
Distributed Data Federation without Disclosure of User Existence	282
<i>Takao Takenouchi, Takahiro Kawamura, and Akihiko Ohsuga</i>	
Improving Virtualization Security by Splitting Hypervisor into Smaller Components	298
<i>Wuqiong Pan, Yulong Zhang, Meng Yu, and Jiwu Jing</i>	
Enforcing Subscription-Based Authorization Policies in Cloud Scenarios	314
<i>Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, and Giovanni Livraga</i>	
Author Index	331