

*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*

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

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*New York University, NY, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Sushil Jajodia Duminda Wijesekera (Eds.)

# Data and Applications Security XIX

19th Annual IFIP WG 11.3 Working Conference on  
Data and Applications Security  
Storrs, CT, USA, August 7-10, 2005  
Proceedings



Springer

## Volume Editors

Sushil Jajodia  
Duminda Wijesekera  
George Mason University  
Center for Secure Information Systems  
Fairfax, VA 22030, USA  
E-mail: {jajodia,dwijesek}@gmu.edu

Library of Congress Control Number: 2005929872

CR Subject Classification (1998): E.3, D.4.6, C.2, F.2.1, J.1, K.6.5

ISSN	0302-9743
ISBN-10	3-540-28138-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-28138-2 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media

[springeronline.com](http://springeronline.com)

© IFIP International Federation for Information Processing 2005  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 11535706 06/3142 5 4 3 2 1 0

# Preface

The 19th Annual IFIP Working Group 11.3 Working Conference on Data and Applications Security was held August 7–10, 2005 at the University of Connecticut in Storrs, Connecticut. The objectives of the working conference were to discuss in depth the current state of the research and practice in data and application security, enable participants to benefit from personal contact with other researchers and expand their knowledge, support the activities of the Working Group, and disseminate the research results.

This volume contains the 24 papers that were presented at the working conference. These papers, which had been selected from 54 submissions, were rigorously reviewed by the Working Group members. The volume is offered both to document progress and to provide researchers with a broad perspective of recent developments in data and application security.

A special note of thanks goes to the many volunteers whose efforts made the working conference a success. We wish to thank Divesh Srivastava for agreeing to deliver the invited talk, Carl Landwehr and David Spooner for organizing the panel, the authors for their worthy contributions, and the referees for their time and effort in reviewing the papers. We are grateful to T. C. Ting for serving as the General Chair, Steven Demurjian and Charles E. Phillips, Jr. for their hard work as Local Arrangements Chairs, and Pierangela Samarati, Working Group Chair, for managing the IFIP approval process. We would also like to acknowledge Sabrina De Capitani di Vimercati for managing the conference's Web site.

Last but certainly not least, our thanks go to Alfred Hofmann, Executive Editor of Springer, for agreeing to include these proceedings in the Lecture Notes in Computer Science series. This is an exciting development since, in parallel to the printed copy, each volume in this series is simultaneously published in the LNCS digital library ([www.springerlink.com](http://www.springerlink.com)). As a result, the papers presented at the Working Conference will be available to many more researchers and may serve as sources of inspiration for their research. The expanded availability of these papers should ensure a bright future for our discipline and the working conference.

August 2005

Sushil Jajodia and Duminda Wijesekera

# Organization

General Chair	T. C. Ting (University of Connecticut, USA)
Program Chairs	Sushil Jajodia and Duminda Wijesekera (George Mason University, USA)
Organizing Chairs	Steven Demurjian and Charles E. Phillips, Jr. (University of Connecticut, USA)
IFIP WG11.3 Chair	Pierangela Samarati (Università degli Studi di Milano, Italy)

## Program Committee

Gail-Joon Ahn	University of North Carolina at Charlotte, USA
Vijay Atluri	Rutgers University, USA
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Steve Demurjian	University of Connecticut, USA
Roberto Di Pietro	University of Rome “La Sapienza”, Italy
Csilla Farkas	University of South Carolina, USA
Eduardo Fernandez-Medina	Univ. of Castilla-La Mancha, Spain
Simon N. Foley	University College Cork, Ireland
Ehud Gudes	Ben-Gurion University, Israel
Carl Landwehr	National Science Foundation, USA
Tsau Young Lin	San Jose State University, USA
Peng Liu	Pennsylvania State University, USA
Sharad Mehrotra	University of California, Irvine
Ravi Mukkamala	Old Dominion University, USA
Peng Ning	North Carolina State University, USA
Sylvia Osborn	University of Western Ontario, Canada
Brajendra Panda	University of Arkansas, USA
Joon Park	Syracuse University, USA
Charles Phillips	U.S. Military Academy, USA
Indrakshi Ray	Colorado State University, USA
Indrajit Ray	Colorado State University, USA
Pierangela Samarati	University of Milan, USA
Sujeet Sheno	University of Tulsa, USA
David Spooner	Rennselaer Polytechnic Institute, USA
Bhavani Thuraisingham	University of Texas at Dallas, and The MITRE Corp., USA
T.C. Ting	University of Connecticut, USA
Ting Yu	North Carolina State University, USA

## **Sponsoring Institutions**

Center for Secure Information Systems, George Mason University

Department of Computer Science and Engineering, University of Connecticut

Dipartimento di Tecnologie dell'Informazione, Università degli Studi di Milano

# Table of Contents

Streams, Security and Scalability <i>Theodore Johnson, S. Muthukrishnan, Oliver Spatscheck, Divesh Srivastava</i> .....	1
Towards Privacy-Enhanced Authorization Policies and Languages <i>C.A. Ardagna, E. Damiani, S. De Capitani di Vimercati, P. Samarati</i> .....	16
Revocation of Obligation and Authorisation Policy Objects <i>Andreas Schaad</i> .....	28
Role Slices: A Notation for RBAC Permission Assignment and Enforcement <i>J.A. Pavlich-Mariscal, T. Doan, L. Michel, S.A. Demurjian, T.C. Ting</i> .....	40
Designing Secure Indexes for Encrypted Databases <i>Erez Shmueli, Ronen Waisenberg, Yuval Elovici, Ehud Gudes</i> .....	54
Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases <i>Jun Li, Edward R. Omiecinski</i> .....	69
Verified Query Results from Hybrid Authentication Trees <i>Glen Nuckolls</i> .....	84
Multilevel Secure Teleconferencing over Public Switched Telephone Network <i>Inja Youn, Csilla Farkas, Bhavani Thuraisingham</i> .....	99
Secrecy of Two-Party Secure Computation <i>Yi-Ting Chiang, Da-Wei Wang, Churn-Jung Liao, Tsan-sheng Hsu</i> .....	114
Reliable Scheduling of Advanced Transactions <i>Tai Xin, Yajie Zhu, Indrakshi Ray</i> .....	124
Privacy-Preserving Decision Trees over Vertically Partitioned Data <i>Jaideep Vaidya, Chris Clifton</i> .....	139
Privacy-Preserving Collaborative Association Rule Mining <i>Justin Zhan, Stan Matwin, LiWu Chang</i> .....	153

Privacy-Preserving Distributed $k$ -Anonymity <i>Wei Jiang, Chris Clifton</i> .....	166
Towards Database Firewalls <i>Kun Bai, Hai Wang, Peng Liu</i> .....	178
Complete Redundancy Detection in Firewalls <i>Alex X. Liu, Mohamed G. Gouda</i> .....	193
A Comprehensive Approach to Anomaly Detection in Relational Databases <i>Adrian Spalko, Jan Lehnhardt</i> .....	207
An Authorization Architecture for Web Services <i>Sarath Indrakanti, Vijay Varadharajan</i> .....	222
Secure Model Management Operations for the Web <i>Guanglei Song, Kang Zhang, Bhavani Thuraisingham, Jun Kong</i> .....	237
A Credential-Based Approach for Facilitating Automatic Resource Sharing Among Ad-Hoc Dynamic Coalitions <i>Janice Warner, Vijayalakshmi Atluri, Ravi Mukkamala</i> .....	252
Secure Mediation with Mobile Code <i>Joachim Biskup, Barbara Sprick, Lena Wiese</i> .....	267
Security Vulnerabilities in Software Systems: A Quantitative Perspective <i>Omar Alhazmi, Yashwant Malaiya, Indrajit Ray</i> .....	281
Trading Off Security in a Service Oriented Architecture <i>G. Swart, Benjamin Aziz, Simon N. Foley, John Herbert</i> .....	295
Trusted Identity and Session Management Using Secure Cookies <i>Joon S. Park, Harish S. Krishnan</i> .....	310
Security Issues in Querying Encrypted Data <i>Murat Kantarcioğlu, Chris Clifton</i> .....	325
Blind Custodians: A Database Service Architecture That Supports Privacy Without Encryption <i>Amihai Motro, Francesco Parisi-Presicce</i> .....	338
<b>Author Index</b> .....	353