Lecture Notes in Computer Science 3919

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
University of California, Los Angeles, CA, 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
Digital Rights Management

Technologies, Issues Challenges and Systems

First International Conference, DRMTICS 2005
Sydney, Australia, October 31 – November 2, 2005
Revised Selected Papers
Preface

The First International Conference on Digital Rights Management: Technology, Issues, Challenges and Systems (DRMTICS – pronounced ‘dramatics’), took place in Sydney, Australia on 31st October - 2nd November, 2005. It was organized by the Centre for Information Security of the University of Wollongong and in cooperation with the International Association of Cryptologic Research (IACR) and IEEE Computer Society’s Task Force on Information Assurance.

DRMTICS is an international conference series that covers the area of digital rights management, including research advancements of an applied and theoretical nature. The goal is to have a broad coverage of the field and related issues and subjects as the area evolves. Since the Internet and the computing infrastructure has turned into a marketplace for content where information goods of various kinds are exchanged, this area is expected to grow and be part of the ongoing evolution of the information society. The DRM area is a unique blend of many diverse disciplines that include mathematics and cryptography, legal and social aspects, signal processing and watermarking, game theory, information theory, software and systems design and business analysis, and DRMTICS attempts to cover as much ground as possible, and to cover new results that will further spur new investigations on the foundations and practices of DRM. We hope that this first conference marks the beginning of a fruitful and useful series of future conferences.

This year, the conference received 57 submissions out of which 26 were accepted for presentation after a rigorous refereeing process. In addition to the regular program, the program also included invited talks and a panel discussion. Renato Ianella gave an invited talk describing “A Brief History of Right Expression Languages,” Moni Naor gave a talk entitled “Humans, Computers and Cryptography,” and Karen Gettens gave a talk on “DRM– the Legal Issues.” The panel was chaired by Bill Caelli and was entitled “Is Reliable and Trusted DRM Enforcement Realistic or Even Possible?”

We wish to thank all the authors of submitted papers for providing the content of this year’s workshop; their high quality submissions made the task of selecting a program hard. We would also like to thank the program committee members as well as the external reviewers, who helped in the refereeing process. We wish to thank our sponsors: Smart Internet Technology CRC, Motorola, DigiSensory Technologies, The Telecommunications and Information Technology Research Institute of the University of Wollongong, Research Network for a Secure Australia, Infosys and Markany. We further wish to thank the attendees, speakers and the participants, as well as Susan Branch, Debbie Farrelly, Harikrishna Vasanta, Wenming Lu, Liang Lu, Rungrat Wiangsripawan, Siamak Fayyaz-Shahandashti, Angela Piper and Martin Surminem, who helped with the organization of the conference.
Last but not least, we would like to thank Wanqing Li and Nicholas Sheppard, general co-chairs of the conference, for their relentless effort in organizing the event and paying attention to every detail, which made DRMTICS a good drama, but one without unnecessary, unexpected dramatic moments! Without the help of the above bodies and individuals this inaugural conference would not have been a possibility.

November 2005

Rei Safavi-Naini
Moti Yung
Organization

General Chairs

Wanqing Li University of Wollongong, Australia
Nicholas Sheppard University of Wollongong, Australia

Program Chairs

Rei Safavi-Naini University of Wollongong, Australia
Moti Yung Columbia University and RSA Security, USA

Program Committee

Feng Bao Institute for Infocomm Research, Singapore
Stefan Bechtold Max Planck Institute for Collective Goods, Germany
Jong Uk Choi MarkAny, Korea
Christian S. Collberg University of Arizona, USA
Ingemar Cox University of London, UK
Ezzy Dabbish Motorola Labs, USA
Jana Dittmann University of Magdeburg, Germany
Yevgeniy Dodis New York University, USA
Brian Fitzgerald Queensland University of Technology, Australia
Susanne Guth ODRL Initiative, Austria
Greg Heileman University of New Mexico, USA
HweeHwa Pang Singapore Management University, Singapore
Hideki Imai University of Tokyo, Japan
Sushil Jajodia George Mason University, USA
Ton Kalker Hewlett-Packard Labs, USA
Stefan Katzenbeisser Technical University of Munich, Germany
Aggelos Kiayias University of Connecticut, USA
Kwangjo Kim Information and Communication University, Korea
Kaoru Kurosawa Ibaraki University, Japan
Jeff Lotspiech IBM Almaden, USA
Stefan Nusser IBM Almaden, USA
Josef Pieprzyk Macquarie University, Australia
Bin Zhu Microsoft Research Asia, China
External Reviewers

Yongdong Wu  Christopher Peikert  Dinesh Dhanekula
Yuichi Kaji  Prashant Puniya  Pramod Jamkhedkar
Takao Nishizeki  Kevin Kloker  Fabricio Ourique
Tomoyuki Asano  David Kravitz  Angela Piper
Katsunari Yoshioka  Tom Messerges  Wenming Lu
Goichiro Hanaoka  Kohich Kamijoh  Nicholas Sheppard
Carl Bosley  Deepa Kundur  Harikrishna Vasanta
Nelly Fazio  Jong W. Kim

Sponsoring Institutions

DigiSensory Technologies, Australia
Infosys, India
MarkAny, Korea
Motorola, USA
Research Network for a Secure Australia, Australia
Smart Internet CRC, Australia
Telecommunications and Information Technology Research Institute, University of Wollongong, Australia
# Table of Contents

## Assurance and Authentication Issues

A Novel Framework for Multiple Creatorship Protection of Digital Movies  
*Yu-Quan Zhang, Sabu Emmanuel* ........................................ 1

TIVA: Trusted Integrity Verification Architecture  
*Mahadevan Gomathisankaran, Akhilesh Tyagi* ......................... 13

## Legal and Related Issues

The Australian Sony PlayStation Case: How Far Will Anti-circumvention Law Reach in the Name of DRM?  
*Brian Fitzgerald* ............................................................. 32

Downloading vs Purchase: Music Industry vs Consumers  
*Supriya Singh, Margaret Jackson, Jenny Waycott,*  
*Jenine Beekhuysen* .......................................................... 52

Digital Rights Management: Merging Contract, Copyright and Criminal Law  
*Yee Fen Lim* ................................................................. 66

## Expressing Rights and Management

User-Attributed Rights in DRM  
*Milan Petković, R. Paul Koster* ........................................... 75

AVS-REL—A New Right Expression Language  
*Ying Sha* ............................................................................. 90

A Comparative Study of Specification Models for Autonomic Access Control of Digital Rights  
*K. Bhoopalam, K. Maly, R. Mukkanama, M. Zubair, D. Agrawal,*  
*D. Kaminsky* ................................................................. 102

## Watermarking

The Effect of Fidelity Measure Functions on the Capacity of Digital Watermarks  
*Yanjun Hu, Xiaoping Ma, Linming Dou, Ying Chen* .................. 113
A MPEG-2 Video Watermarking Algorithm with Compensation in Bit Stream
   Hongmei Liu, Fenglian Shao, Jiwu Huang .......................... 123

Reversible Semi-fragile Image Authentication Using Zernike Moments and Integer Wavelet Transform
   Xiaoyun Wu, Xiaoping Liang, Hongmei Liu, Jiwu Huang,
   Guoping Qiu .......................................................... 135

Software Issues

Software Tamper Resistance Through Dynamic Program Monitoring
   Brian Blietz, Akhilesh Tyagi ....................................... 146

Call Tree Transformation for Program Obfuscation and Copy Protection
   Valery Pryamikov .................................................. 164

Algorithms to Watermark Software Through Register Allocation
   William Zhu, Clark Thomborson ................................. 180

Fingerprinting and Image Authentication

An Efficient Fingerprinting Scheme with Secret Sharing
   Seunglim Yong, Sang-Ho Lee ...................................... 192

Worst-Case Optimal Fingerprinting Codes for Non-threshold Collusion
   Takaaki Mizuki, Satoshi Nounin, Hideaki Sone, Yousuke Toyota .... 203

Secure Remote Fingerprint Verification Using Dual Watermarks
   Taehae Kim, Yongwha Chung, Seunghwan Jung, Daesung Moon ..... 217

Supporting Cryptographic Technology

Security Weaknesses of Certain Broadcast Encryption Schemes
   Miodrag J. Mihaljević, Marc P.C. Fossorier, Hideki Imai .......... 228

A Broadcast Encryption Scheme with Free-Riders but Unconditional Security
   Andre Adelsbach, Ulrich Greveler ................................ 246

A Novel Broadcast Encryption Based on Time-Bound Cryptographic Keys
   Miodrag J. Mihaljević, Marc P.C. Fossorier, Hideki Imai .......... 258
# Table of Contents

## A Vector Approach to Cryptography Implementation

*Jacques J.A. Fournier, Simon Moore* .................................................. 277

## P2P Issues

A Novel Privacy and Copyright Protection Enforced Peer-to-Peer Network

*Xiaoming Wang, Bin Zhu, Shipeng Li* ................................................ 298

Design of a Secure Digital Contents Delivery System in P2P Networks

*Young-Ho Park, Jung-Hwa Shin, Kyung-Hyune Rhee* ......................... 311

## Implementations and Architectures

Real-Time Implementation of Broadcast Switching System Using Audio Watermark

*Jongwoon Kim, Dongwan Shin, Jonguk Choi* ............................... 322

Enforcing Regional DRM for Multimedia Broadcasts With and Without Trusted Computing

*Ulrich Greveler* .................................................................................. 332

A DRM System Supporting What You See Is What You Pay

*Bin B. Zhu, Yang Yang, Tierui Chen* .................................................. 341

## Author Index

*................................. 357*