Proceedings

The Fourth International Symposium on Information Assurance and Security

IAS 2008

Proceedings

The Fourth International Symposium on Information Assurance and Security

September 8-10, 2008
Napoli, Italy

Edited by:
Massimiliano Rak, *Second University of Naples, Italy*
Ajith Abraham, *Norwegian University of Science and Technology, Norway*
Valentina Casola, *University of Naples Federico II, Italy*

Technically Sponsored by:

Dipartimento di Ingegneria dell'informazione – Seconda Università degli Studi di Napoli, Italy

ICST (International Communication Sciences and Technology Association)

Create-Net (Center of REsearch And Telecommunication Experimentations for NETworked communities)

CPS Conference Publishing Services

Los Alamitos, California

Washington • Tokyo

IEEE computer society

IEEE Computer Society Order Number P3324
BMS Part Number CFP0861C-PRT
ISBN 978-0-7695-3324-7
Library of Congress Number 2008928416

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Lisa O'Conner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

IEEE Computer Society
***Conference Publishing Services* (CPS)**
http://www.computer.org/cps

Table of Contents

IAS 2008

The Fourth International Symposium on Information Assurance and Security

---

Authentication and Access Control

Short Papers

Cryptographic Schemes and Applications

Data Security and Privacy

Intrusion Detection, Intrusion Prevention, Threat Modeling, and Analysis

Security Tools Design

Network Security and Sensor, Mobile and "ad hoc" Network Security

Chairs' Welcome Message

We are pleased to welcome our colleagues to The Fourth International Symposium on Information Assurance and Security (IAS 2008). The International Symposium on Information Assurance and Security aims to bring together researchers, practitioners, developers, and policy makers involved in multiple disciplines of information security and assurance to exchange ideas and to learn the latest development in this important field. The fourth conference will bring together the world's most respected authorities on Information assurance and security in networked and distributed information sharing environments. IAS 2008 addresses the following important themes:

Security Mechanisms for:

- Authentication and Identity
- Management Authorization and Access Control
- Trust Negotiation, Establishment and Management
- Anonymity and User Privacy
- Data Integrity and Privacy
- Network Security
- Operating System Security
- Database Security
- Intrusion Detection
- Security Attacks

Security and System Architectures

- Web Services Security
- GRID Security
- Ubiquitous Computing Security
- Mobile Agent Security
- Internet Security

Security Methodologies

- Security Oriented System Design
- Security and Performance trade-off
- Security Management and Strategy
- Security Verification, Evaluations and Measurements
- Secure Software Technologies
- New Ideas and Paradigms for Security

Security Application on Critical Environments

- Intellectual Property Protection
- E-Commerce Security
- E-Government Security
- E-Health Security
- Home System Security
- Sensor Network Security
- Ad hoc network security
- Biometrics Security and Applications
- Secure Hardware and Smartcards

Security Models

- Cryptography
- Cryptographic Protocols
- Key Management and Recovery

IAS 2008 is technically co-sponsored by “Dipartimento di ingegneria dell’Informazione”, Second University of Naples and the Second University of Naples CSI (Centro Servizi Informatici), by International Communication Sciences and Technology Association (ICST) and CREATE-NET, which is an International Institute, founded in Trento, Italy by major Universities and Research Centers in Europe. Each paper was peer reviewed by at least three or more program committee members and based on the recommendations of the reviewers, about 40 full papers and 20 short papers were included in the final Program.

The IAS 2008 Conference provided two special sessions, dedicated to specific topics:

- *Special Session on Quantum Cryptography* (Organized by Stamatios Kartalopoulos, University of Oklahoma, USA)

- *Special Session on Security in Critical Infrastructures* (Organized by Carlo Sansone, Federico II University of Naples, IT)

We would like to thank the IAS 2008 international program committee and the additional reviewers for providing the reviews in time. Our special thanks to Lisa O’Conner, of IEEE Computer Society Press, for all the support and help related to the production of this important scientific work. Finally, we would like to express our sincere gratitude to all the authors and local organizing committees that have contributed towards the success of this conference. We look forward to seeing you during IAS 2008, September 8-10, 2008.

IAS 2008 Chairs

Massimiliano Rak, Second University of Naples, Italy – *General and Program Chair*
Ajith Abraham, Norwegian University of Science and Technology, Norway – *General Chair*
Valentina Casola, University of Naples Federico II, Italy – *Program Chair*
Ning Zhang, School of Computer Science, University of Manchester, UK – *Program Co-Chair*

IAS 2008 Organisation

General Chairs

Massimiliano Rak, *Second University of Naples, Italy*
Ajith Abraham, *Norwegian University of Science and Technology, Norway*

Program Chairs

Massimiliano Rak, *Second University of Naples, Italy*
Valentina Casola, *University of Naples Federico II, Italy*
Ning Zhang, *School of Computer Science, University of Manchester, UK*

Steering Committee

Imrich Chlamtac (Chair), *Create-Net, Italy*
Melissa Ezell, *ICST Europe*

Local Organisers

Massimiliano Rak, *Second University of Naples, IT*
Valentina Casola, *University of Naples Federico II, IT*
Emilio Mancini, *RCOST, University of Sannio, IT*
Domenico Di Sivo, *Second University of Naples, IT*
Pasquale Cantiello, *Second University of Naples, IT*
Rosa Anna Micillo, *Second University of Naples, IT*
Flora Amato, *University of Naples Federico II, IT*
Andrea Gaglione, *University of Naples Federico II, IT*

Technical Program Committee (TPC) for IAS 2008

Dharma Agrawal, *University of Cincinnati, USA*
Flora Amato, *Federico II University of Naples, Italy*
Saxena Ashutosh, *SETLabs | Infosys Technologies Limited | Hyderabad DC, India*
Rocco Aversa, *Seconda Università degli studi di Napoli, Italy*
Youakim Badr, *National Institute of Applied Sciences, France*
Omaima Bamasak, *University of Manchester, Manchester, UK, UK*
Richard Chbeir, *Bourgogne University, France*
Yuehui Chen, *Jinan University, China*
Emilio Corchado, *Universidad de Burgos, Spain*
Marc Dacier, *Eurecom Institute, France*
Jan De Meer, *University of Applied Sciences Berlin, Germany*
Beniamino Di Martino, *Seconda Università degli studi di Napoli, Italy*
Danny Dresner, *National Computing Centre, UK*
Katrin Franke, *Gjøvik University College, Norway*
Deborah Frincke, *Pacific Northwest National Laboratory, USA*
Steven Furnell, *University of Plymouth, UK*
Amparo Fúster Sabater, *Institute of Applied Physics, Spain*
Andrea Gaglione, *Federico II University of Naples, Italy*
Ahn Gail-Joon, *University of North Carolina at Charlotte, USA*
George Ghinea, *School of Information Systems, Computing and Mathematics, UK*
Richard III Golden, *University of New Orleans, USA*
Stefanos Gritzalis, *University of the Aegean, Greece*
Crina Grosan, *University of Cluj-Napoca, Romania*
Lim Hyung-Jin, *Financial Security Agency, Korea*
Mauro Iacono, *Seconda Università degli Studi di Napoli, Italy*
Stamatios Kartalopoulos, *University of Oklahoma, USA*

Plenary Abstract 1

Why Selfishness in Wireless Mesh Networks

Dharma P. Agrawal

Computer Science Department
University of Cincinnati, Cincinnati, OH, 45221-0030
E-mail:dpa@cs.uc.edu
web: http://www.cs.uc.edu/~dpa

Abstract: Wireless Mesh Networks (WMNs) have revolutionized the provisioning of broadband wireless internet service to a community of users. A group of static mesh router automatically interconnect themselves to form a web of connection and employ multi-hop forwarding to connect to the Internet Gateway (IGW). Thus, we see that is critical to establish and ensure a collaborative framework at the MRs. All existing mesh routing protocols assume that each MR honestly participates in packet forwarding. But, this is valid only in a network managed by a single trusted authority such as University or Enterprise. Typically, mesh routers can be operated by different operators. Thus, a malicious user can erect a selfish MR that prioritizes treatment for the traffic originating from its mesh clients and drop's others traffic. This results in degradation of network performance. We discuss various existing schemes with respect to detect selfishness in WMNs, and highlight their relative advantages and deficiencies.

Plenary Abstract 2

A Look at Current Malware Problems and their Solutions

Tzi-cker Chiueh

Symantec Research Labs, USA
Computer Science Department, Stony Brook University, USA
Tzi-cker_Chiueh@symantec.com

Abstract: Malware is software that exhibits malicious behaviour, ranging from machine compromise to information stealing. Although there are a confusing array of names associated with malware, such as spyware, Trojan horse, or both, the fundamental principles underlying their operations are quite similar. The goal of this talk is to present the set of malware problems that the computer security industry is facing today, and describe how various solutions to them work at a high level. Hopefully it could inform the research community of the current concerns of the computer security industry and help shape future malware research directions.

Plenary Abstract 3

Trust, Security and Privacy in Service Oriented Architectures

David W. Chadwick

The Computing Laboratory, University of Kent,
Canterbury, CT2 7NF, United Kingdom
Email: D.W.Chadwick@kent.ac.uk

Abstract: Service oriented architectures are the modern paradigm for distributed computing. As long as all the services are under the control of a single organisation, there are no significant trust, security or privacy issues in sharing data between the services. But once several organisations come together to share their data between services in a virtual organisation, the trust, security and privacy issues become critically important. Today these are primarily addressed by creating signed legal paper contracts between the various parties, but this is a very time consuming and expensive process. Furthermore, there are no guarantees that breaches of contract won't occur, or that mistakes won't be made, and even if they are, the other parties may not be aware of them. Ideally, we need computer based technologies that will help to automate the creation and management of trusted infrastructures in order to reduce the set up and running costs of them. This talk will look at the various technologies that are being researched and developed in order to semi-automate the creation and maintenance of trust, security and privacy within service oriented VOs.

Plenary Abstract 4

Usage Control for Distributed GRID Systems Implemented in the Globus Toolkit

Fabio Martinelli

Information Security Group
Istituto di Informatica e Telematica - IIT
National Research Council - C.N.R.
Pisa Research Area
Via. G. Moruzzi 1 - Pisa, Italy
E-Mail: Fabio.Martinelli@iit.cnr.it

Abstract: We present an architecture and a prototype implementation for usage control for GRID services. The usage control model (UCON) is a new access control paradigm proposed by Park and Sandhu that encompasses and extends several existing models (e.g. MAC, DAC, RBAC, etc). Its main novelty, in addition to the unifying view, is based on continuity of usage monitoring and mutability of attributes of subjects and objects. We identified this model as a perfect candidate for managing access/usage control in GRID systems due to their peculiarities, where continuity of control is a main issue. Here we show how it is possible to adapt the original UCON model in order to develop a fully functional usage control system for GRID services. The implementation has been developed for the Globus Toolkit.

Short CV: Dr. Fabio Martinelli is a senior researcher of Institute of Informatics and Telematics of the Italian National Research Council (IIT-CNR). He is co-author of more than 80 papers on international journals and conference/workshop proceedings. His main research interests involve network and systems security, PKI & trust management, access and usage control policies and enforcing mechanisms as well as formal methods for security (including security protocols analysis and information flow study). He serves as PC-chair/organizer in several international conferences/workshops. In particular, He is the co-initiator of the International Workshop series on Formal Aspects in Security and Trust (FAST), one of the first events to recognize the necessity to consider trust and security issues altogether in new virtual and dynamic organizations/coalitions. He is serving as scientific co-director of the international research school on Foundations of Security Analysis and Design (FOSAD) since 2004 edition. He chairs the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM). He usually manages R&D projects on information and communication security and he is involved with several roles in the following FP6-FP7 projects: ARTIST2, BIONETS, CONSEQUENCE, GRIDtrust, S3MS, and SENSORIA.