

SECRYPT₂₀₀₆

International Conference on Security and Cryptography

SECRYPT is organized by INSTICC - Institute for Systems and Technologies of Information, Control and Communication and technically co-sponsored by IEEE and in cooperation with IACR - International Association for Cryptologic Research.

SCOPE

The purpose of the International Conference on Security and Cryptography (SECRYPT-2006) is to bring together researchers, mathematicians, engineers and practitioners interested on security aspects related to information and communication. Theoretical and practical advances in the fields of cryptography and coding are a key factor in the growth of data communications, data networks and distributed computing. In addition to the mathematical theory and practice of cryptography and coding, SECRYPT also focus on other aspects of information systems and network security, including applications in the scope of the knowledge society in general and information systems development in particular, especially in the context of e-business, internet and global enterprises.

Information theory and information security are hot topics nowadays, ranging from statistics and stochastic processes to coding, from detection and estimation to Shannon theory, from data compression to data networks and systems security, cryptography as well as many other topics that can be listed, as indicated below. SECRYPT is mainly interested in contributions related to ideas on how to analyze and approach security problems by combining information and communication technologies with the appropriate theoretical work including information theory and communication theory, either in the scope of R&D projects, engineering or business applications, are welcome. Papers describing new methods or technologies, advanced prototypes, systems, tools and techniques and general survey papers indicating future directions are also encouraged.

Papers describing original work are invited in any of the areas listed below. Accepted papers, presented at the conference by one of the authors, will be published in the Proceedings of SECRYPT, with an ISBN. Acceptance will be based on quality, relevance and originality. Both full research reports and work-in-progress reports are welcome. There will be both oral and poster sessions.

The best papers will be selected to appear either in an international journal or in a book to be published by Springer.

Special sessions, case-studies and tutorials dedicated to technical/scientific topics related to the main conference are also envisaged: researchers interested in organizing a special session, or companies interested in presenting their products/methodologies or researchers interested in holding a tutorial are invited to contact the conference secretariat. Additional information can be found at <http://www.secrypt.org>.

CONFERENCE AREAS

Each of these topic areas is expanded below but the sub-topics list is not exhaustive. Papers may address one or more of the listed sub-topics, although authors should not feel limited by them. Unlisted but related sub-topics are also acceptable, provided they fit in one of the following main topic areas:

- Access Control and Intrusion Detection
- Network Security and Protocols
- Cryptographic Techniques and Key Management
- Information Assurance
- Security in Information Systems

Area 1: Access Control and Intrusion Detection

- Authentication and Non-repudiation
- Identification and Authentication
- Insider Threats and Countermeasures
- Intrusion Detection & Prevention
- Identity and Trust Management
- Biometric Security
- Trust models and metrics
- Regulation and Trust Mechanisms
- Data Integrity
- Models for Authentication, Trust and Authorization
- Access Control in Computing Environments
- Multiuser Information

Area 2: Network Security and Protocols

- IPsec, VPNs and encryption modes
- Service and Systems Design and QoS Network Security
- Fairness Scheduling and QoS Guarantee
- Reliability and Dependability
- Web Performance and Reliability
- Denial of Service and other attacks
- Data and Systems Security
- Data Access & Synchronization
- GPRS and CDMA Security
- Mobile System Security
- Ubiquitous Computing Security
- Security in Localization systems
- Sensor and Mobile Ad Hoc Network Security
- Wireless Network Security (WiFi, WiMAX, WiMedia and others)
- Security of GSM/GPRS/UMTS systems
- Peer-to-Peer Security
- E-commerce protocols and micropayment schemes

Area 3: Cryptographic Techniques and Key Management

- Smart Card Security
- Public Key Crypto Applications
- Coding Theory and Practice
- Spread Spectrum Systems
- Speech/Image Coding
- Shannon Theory
- Stochastic Processes
- Quantum Information Processing
- Mobile Code & Agent Security
- Digital Rights Management

Area 4: Information Assurance

- Planning Security
- Risk Assessment
- Security Area Control
- Organizational Security Policies and Responsibility
- Security Through Collaboration
- Human Factors and Human Behaviour Recognition Techniques
- Ethical and Legal Implications
- Intrusive, Explicit Security vs. Invisible, Implicit Computing
- Information Hiding
- Information Systems Auditing
- Management of Computing Security

Area 5: Security in Information Systems

- Security for Grid Computing
- Secure Software Development Methodologies
- Security for Web Services
- Security for Databases and Data Warehouses
- E-Health
- Security Engineering
- Security Information Systems Architectures
- Security requirements
- Security Metrics
- Personal Data Protection
- XML Security
- Workflow and Business Process Security

KEYNOTE SPEAKERS

Manu Malek, Stevens Institute of Technology, USA

TUTORIALS

SECURITY 2006 may include one or more tutorials, depending on the submitted proposals, to be lectured the day before the conference opening. If you would like to propose a tutorial for SECURITY 2006, please contact the secretariat as soon as possible. Proposals should specify the topic and scope of the tutorial, the background knowledge expected of the participants, and a short CV of the instructor(s).

SUBMISSION OF PAPERS

Authors should submit a complete paper in English of up to 8 A4 pages, using the submission procedure indicated below. The program committee will review all papers and the contact author of each paper will be notified of the result, by email. Each paper should clearly indicate the nature of its technical/scientific contribution, and the problems, domains or

environments to which it is applicable. Authors must also indicate the conference track to which the paper is submitted. The paper must be carefully checked for correct grammar and spelling.

Paper submission procedure

1. A "blind" paper evaluation method will be used. To facilitate that, the authors are kindly requested to produce and provide the full paper, WITHOUT any reference to the authors. The manuscript must contain, in its first page, the paper title, an abstract and a list of keywords but NO NAMES OR CONTACT DETAILS WHATSOEVER are to be included in any part of this file.

2. The contact author will then use the SECRIPT web-based submission facility available at the conference web site, <http://www.secrypt.org/> to enter the contact information of all paper authors plus the file indicated in point 1, above. The facility will automatically send a submission acknowledgement, by email, to the author indicated as "contact author". Please contact the secretariat if no acknowledgement is received.

If the author is unable to use the web-based procedure then he/she can send the paper by e-mail to the secretariat attaching an additional file containing: the title, author(s), affiliation(s), contact details, a list of keywords and an abstract. Authors must also indicate the conference area (including the topics), to which the paper is submitted.

The camera-ready format will be enforced only for accepted papers, but authors are encouraged to use it also for paper submissions, in order to reduce extra work later. Two templates are provided at the conference web site: one for Latex and another for MS Word. Due to space limitations in the Proceedings, the camera-ready version will be limited to 8 (eight) pages for full papers, 6 (six) for short papers (progress reports) and 4 (four) for poster presentations. If absolutely needed, the number of pages may be increased up to a maximum of 12 (long presentations), 8 (short presentations) and 6 (poster presentations). However, for each page in excess of the maximum allowed, the author will have to pay an additional fee.

PUBLICATIONS

SECRIPT 2006 papers will be indexed by DBLP.

All accepted papers will be published in the conference proceedings, under an ISBN reference, in paper and in CD-ROM support.

A book including a selection of the best conference papers will be edited and published by Springer.

The Journal of Network and Systems Management will publish a selection of ICETE - SECRIPT 2006 best papers.

IMPORTANT DEADLINES

Full Paper Submission: **deadline expired**

Author Notification: 24th May 2006

Final Paper Submission and Registration: 8th June 2006

Conference Date: 7-10 August 2006

SECRETARIAT

SECURITY Secretariat
Av. D.Manuel I, 27A 2ºesq, 2910-595 Setúbal - Portugal
Tel.: +351 265 520 185
Fax: +351 265 520 186
E-mail: secretariat@secrypt.org
Web: <http://www.secrypt.org>

PROGRAM CHAIR

Manu Malek (Stevens Institute of Technology, USA)
Eduardo Fernández-Medina (UCLM, Spain)
Javier Hernando (Polytechnic University of Catalonia, Spain)

PROGRAM COMMITTEE

Kamel Adi, University of Quebec, Canada
Gail-Joon Ahn, University of North Carolina at Charlotte, U.S.A
Ali Akhavi, University of Caen, France
Jörn Altmann, Seoul National University & International University Bruchsal, Korea
Farooq Anjum, Telcordia Technologies, U.S.A
Giuseppe Ateniese, Johns Hopkins University, U.S.A
Dan Bailey, RSA Laboratories, U.S.A
Anthony Bedford, RMIT University, Australia
John Black, University of Colorado at Boulder, U.S.A
Carlo Blundo, Università di Salerno, Italy
Xavier Boyen, Voltage Inc., U.S.A
Emmanuel Bresson, CELAR, France
Rahmat Budiarto, National Advanced IPv6 (NAv) Center, Malaysia
Roy Campbell, University of Illinois, U.S.A
Rui Costa Cardoso, University of Beira Interior, Portugal
Eurico Carrapatoso, FEUP/INESC Porto, Portugal
Pascale Charpin, INRIA - Rocquencourt, France
Mathieu Ciet, Gemplus, France
Miguel Correia, LASIGE, Faculdade de Ciências da Universidade de Lisboa, Portugal
Véronique Cortier, Loria, CNRS, France
Paolo D'Arco, D.I.A - University of Salerno, Italy
Sabrina De Capitani di Vimercati, DTI, Università degli Studi di Milano, Italy
Falko Dressler, University of Erlangen, Germany
Robert Erbacher, Utah State University, U.S.A
Serge Fehr, CWI Amsterdam, Netherlands
Eduardo B. Fernandez, Florida Atlantic University, U.S.A
Marc Fischlin, Emmy Noether Fellow, Germany
Mário Freire, University of Beira Interior, Portugal
Mariagrazia Fugini, Politecnico di Milano, Italy
Steven Furnell, University of Plymouth, U.K
Luciano Gaspary, Universidade do Vale do Rio dos Sinos, Brazil
Paolo Giorgini, University of Trento, Italy
Dieter Gollmann, TU Hamburg-Harburg, Germany
Carlos Goulart, Federal University of Vicosa, Brazil
Lisandro Granville, Federal University of Rio Grande do Sul, Brazil
Stefanos Gritzalis, University of the Aegean, Greece
Vic Grout, University of Wales, U.K
Cynthia Irvine, Naval Postgraduate School, U.S.A
Hamid Jahankhani, University Of East London, U.K
Nigel Jefferies, Vodafone Group R&D, U.K
Willem Jonker, Philips Research / Twente University, Netherlands
Elias P. Duarte Jr., Federal University of Parana, Brazil
Aggelos Kiayias, University of Connecticut, U.S.A
Seungjoo Kim, Sungkyunkwan University, Korea

Paris Kitsos, Hellenic Open University (HOU), Greece
Lars Knudsen, Technical University of Denmark, Denmark
Cetin Koc, Istanbul Commerce University, Turkey
Christopher Kruegel, Technical University Vienna, Austria
Kaoru Kurosawa, Ibaraki University, Japan
Tanja Lange, Technical University of Denmark, Denmark
Victor Peral Lecha, France Telecom R&D, U.K
Albert Levi, Sabanci University, Turkey
Chae Hoon Lim, Sejong University, Korea
Javier Lopez, University of Malaga, Spain
Olivier Markowitch, Université Libre de Bruxelles, Belgium
Alexander May, TU Darmstadt, Germany
Madjid Merabti, Liverpool John Moores University, U.K
Ali Miri, University of Ottawa, Canada
Atsuko Miyaji, Japan Advanced Institute of Science and Technology, Japan
Edmundo Monteiro, University of Coimbra, Portugal
Haralambos Mouratidis, University of East London, U.K
Yi Mu, University of Wollongong, Australia
Volker Müller, University of Luxembourg, Luxembourg
Juan Gonzalez Nieto, Queensland University of Technology, Australia
Kaisa Nyberg, Helsinki University of Technology and Nokia, Finland
Tatsuaki Okamoto, NTT, Japan
José Luis Oliveira, University of Aveiro, Portugal
Martin Olivier, University of Pretoria, South Africa
Rolf Oppliger, eSECURITY Technologies, Switzerland
Elisabeth Oswald, Graz University of Technology, Austria
Guenther Pernul, University of Regensburg, Germany
George Polyzos, AUEB, Greece
Atul Prakash, University of Michigan, Greece
Jean-Jacques Quisquater, UCL, Louvain, Belgium
Indrakshi Ray, Colorado State University, U.S.A
Indrajit Ray, Colorado State University, U.S.A
David Samyde, FemtoNano, France
Susana Sargento, Instituto de Telecomunicações - Universidade de Aveiro, Portugal
Damien Sauveron, University of Limoges, France
Erkay Savas, Sabanci University, Turkey
Berry Schoenmakers, Technical University of Eindhoven, Netherlands
Bruno Schulze, LNCC, Brazil
Alice Silverberg, University of California, Irvine, U.S.A
Nicolas Sklavos, University of Patras, Greece
Jose Neuman de Souza, Federal University of Ceará, Brazil
Mark Stamp, San Jose State University, U.S.A
Lily Sun, The University of Reading, U.K
Berk Sunar, Worcester Polytechnic Institute, U.S.A
Willy Susilo, University of Wollongong, Australia
Tsuyoshi Takagi, Future University-Hakodate, Japan
Robert Tolksdorf, Freie Universität Berlin, Germany
Ambrosio Toval, University of Murcia, Spain
Wade Trappe, WINLAB, Rutgers University, U.S.A
Wen-Guey Tzeng, National Chiao Tung University, Taiwan
Ulrich Ultes-Nitsche, University of Fribourg, Switzerland
Guillaume Urvoy-Keller, Institut Eurecom, France
Huaxiong Wang, Macquarie University, Australia
Yongge Wang, University of North Carolina, U.S.A
Susanne Wetzel, Stevens Institute of Technology, U.S.A
Duminda Wijesekera, George Mason University, U.S.A
Chaoping Xing, National University of Singapore, Singapore
Shouhuai Xu, University of Texas at San Antonio, U.S.A
Mariem Yagüe, University of Malaga, Spain
Jeff Yan, University of Newcastle, U.K
Alec Yasinsac, SAIT Laboratory, FSU, U.S.A
Sung-Ming Yen, National Central University, Taiwan
Meng Yu, Monmouth University, U.S.A
Moti Yung, RSA Labs and Columbia University, U.S.A

Yuliang Zheng, UNC Charlotte, U.S.A
André Zúquete, University of Aveiro, Portugal