SECRYPT 2007

International Conference on Security and Cryptography

SCOPE

The purpose of SECRYPT 2007 the *International Conference on Security and Cryptography* 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

- Intrusion Detection and Vulnerability Assessment
- 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 Responsability
- 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

SECRYPT 2007 will have several invited keynote speakers, who are internationally recognized experts in their areas. Their names are not yet confirmed.

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 SECRYPT 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

SECRYPT 2007 papers will be indexed by ISI, INSPEC and 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.

IMPORTANT DEADLINES

Full Paper Submission: 4th April 2007 (new)
Author Notification: 21st May 2007 (new)
Final Paper Submission and Registration: 31st May 2007 (new)
Conference Date: 28-31 July 2007

SECRETARIAT

SECRYPT 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**

VENUE

The conference will be held in Barceló Hotel Sants. The Barceló Hotel Sants is a deluxe hotel located in the heart of Barcelona. It stays about 15 minutes from the airport, 4 minutes to Plaza de Catalunya and 500 meters to the Fira de Barcelona. Considering the hotel is exactly above the train station, it allows traveling to anyplace. Most important is the fact that all the noise from the train station is undetected because the hotel is soundproofed. The Barcelo Hotel Sants also offers on site dining and is convenient to many shopping and entertainment venues.

CONFERENCE CO-CHAIRS

Joaquim Filipe (Polytechnic Institute of Setúbal / INSTICC, Portugal)
Javier Hernando (Polytechnic University of Catalonia, Spain)
Mohammad S. Obaidat (Monmouth University, U.S.A.)

PROGRAM CHAIR

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

PROGRAM COMMITTEE

Michel Abdalla, Ecole Normale Supérieure & CNRS, France
Kamel Adi, University of Québec in Outaouais, Canada
Gordon Agnew, University of Waterloo, Canada
Gail-Joon Ahn, UNC Charlotte, United States
Luiz Carlos Pessoa Albini, Federal University of Parana, Brazil
Jörn Altmann, Seoul National University & International University of Bruchsal, Korea
Farooq Anjum, Telcordia Technologies, United States
Joonsang Baek, Institute for Infocomm Research, Singapore
Dan Bailey, RSA Laboratories, United States

Lejla Batina, Katholieke Universiteit Leuven, Belgium
Anthony Bedford, RMIT University, Australia
Carlo Blundo, Università di Salerno, Italy
Emmanuel Bresson, DCSSI Crypto Lab, France
Rahmat Budiarto, National Advanced IPv6 (NAv) Center, Malaysia
Roy Campbell, University of Illinois at Urbana-Champaign, United States
Rui Costa Cardoso, University of Beira Interior, Portugal
Kim-Kwang Raymond Choo, Australian Institute of Criminology, Australia
Edward Chow, University of Colorado at Colorado Springs, United States
Christophe Clavier, Gemalto, France
Debbie Cook, Alcatel-Lucent Bell Labs, United States
Mads Dam, KTH - Royal Institute of Technology, Sweden
Paolo D'Arco, University of Salerno, Italy
Falko Dressler, University of Erlangen, Germany
Orr Dunkelman, Katholieke Universitiet Leuven, Belgium
Iwan Duursma, University of Illinois at Urbana-Champaign, United States
Robert Erbacher, Utah State University, United States
Eduardo B. Fernandez, Florida Atlantic University, United States
Mário Freire, University of Beira Interior, Portugal
Steven Furnell, University of Plymouth, United Kingdom
David Galindo, Ecole Normale Superieure, France
Luciano Gaspary, Federal University of Rio Grande do Sul, Brazil
Paolo Giorgini, University of Trento, Italy
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, United Kingdom
Javier Herranz, IIIA-CSIC, Spain
Amir Herzberg, Bar Ilan University, Israel
Min-Shiang Hwang, National Chung Hsing University, Taiwan
Cynthia E. Irvine, Naval Postgraduate School, United States
Hamid Jahankhani, University Of East London, United Kingdom
Christian Damsgaard Jensen, Technical University of Denmark, Denmark
Willem Jonker, Philips Research Europe, The Netherlands
Elias P. Duarte Jr. , Federal University of Parana, Brazil
Pascal Junod, Nagravision, Switzerland
Kwangjo Kim, ICU, Korea, Republic Of
Seungjoo Kim, Sungkyunkwan University, Korea, Republic Of
Paris Kitsos, Hellenic Open University (HOU), Greece
Cetin Koc, Istanbul Commerce University, Turkey
Steve Kremer, ENS Cachan & CNRS & INRIA Futurs, France
Christopher Kruegel, Technical University Vienna, Austria
Ralf Kuesters, ETH Zurich, Switzerland
Tanja Lange, Eindhoven University of Technology, Netherlands
Victor Peral Lecha, France Telecom R&D UK Ltd, United Kingdom
Albert Levi, Sabanci University, Turkey
Yingjiu Li, Singapore Management University, Singapore
Chae Hoon Lim, Sejong University, Korea
Javier Lopez, University of Malaga, Spain
Olivier Markowitch, Université Libre de Bruxelles, Belgium
Alexander May, TU Darmstadt, Germany
Breno de Medeiros, Florida State University, United States
Madjid Merabti, Liverpool John Moores University, United Kingdom
Ali Miri, University of Ottawa, Canada
Atsuko Miyaji, Japan Advaned Institute of Science and Technology, Japan
Edmundo Monteiro, University of Coimbra, Portugal
Haralambos Mouratidis, University of East London, United Kingdom
Yi Mu, University of Wollongong, Australia
Volker Müller, University of Luxembourg, Luxembourg
Juan Gonzalez Nieto, Queensland University of Technology, Australia

José Luis Oliveira, University of Aveiro, Portugal
Martin Olivier, University of Pretoria, South Africa
Rolf Oppliger, eSECURITY Technologies, Switzerland
Elisabeth Oswald, University of Bristol, United Kingdom
Carles Padro, Universitat Politecnica de Catalunya, Spain
Daniel Page, University of Bristol, United Kingdom
Guenther Pernul, University of Regensburg, Germany
Marinella Petrocchi, IIT-CNR, Italy
Raphael C.-W. Phan, EPFL, Switzerland
George Polyzos, AUEB, Greece
Joachim Posegga, University of Hamburg, Germany
Atul Prakash, University of Michigan, Greece
Indrakshi Ray, Colorado State University, United States
Indrajit Ray, Colorado State University, United States
Srinivas Sampalli, Dalhousie University, Canada
David Samyde, Intel, United States
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 R. Schulze, LNCC, Brazil
Alice Silverberg, University of California, Irvine, United States
Nicolas Sklavos, Technological Educational Institute of Messolonghi, Greece
José Neuman de Souza, Federal University of Ceará, Brazil
Mario Spremic, University of Zagreb, Croatia
Mark Stamp, San Jose State University, United States
Aaron Striegel, University of Notre Dame, United States
Lily Sun, University of Reading, United Kingdom
Willy Susilo, University of Wollongong, Australia
Michael Szydlo, RSA, the security division of EMC, United States
Tsuyoshi Takagi, Future University-Hakodate, Japan
Ferucio Laurentiu Tiplea, "Al.I.Cuza" University of Iasi, Romania
Ambrosio Toval, University of Murcia, Spain
Wade Trappe, WINLAB, Rutgers University, United States
Wen-Guey Tzeng, National Chiao Tung University, Taiwan
Ulrich Ultes-Nitsche, University of Fribourg, Switzerland
Dominique Unruh, Saarland University, Germany
Guillaume Urvoy-Keller, Institut Eurecom, France
Sabrina De Capitani di Vimercati, University of Milan, Italy
Yongge Wang, University of North Carolina, United States
Susanne Wetzel, Stevens Institute of Technology, United States
Duminda Wijesekera, George Mason University, United States
Duncan S. Wong, City University of Hong Kong, Hong Kong
S. Felix Wu, University of California, Davis, United States
Chaoping Xing, National University of Singapore, Singapore
Shouhuai Xu, University of Texas at San Antonio, United States
Mariemma Yagüe, University of Malaga, Spain
Alec Yasinsac, SAIT Laboratory, FSU, United States
Sung-Ming Yen, National Central University, Taiwan
Meng Yu, Monmouth University, United States
Moti Yung, RSA Labs and Columbia University, United States
Fangguo Zhang, Sun Yat-sen University, China, China
André Zúquete, University of Aveiro, Portugal

(list not yet complete)