CALL FOR PAPERS

4th International Conference on Applied Cryptography and Network Security (ACNS'06)

June 6-9, 2006, Singapore http://acns2006.i2r.a-star.edu.sg/

Submission Due - 15 January 2006 **Author Notification - 12 March 2006** **Camera-ready Copy - 1 April 2006**

General Chair
Feng Bao (I2R, Singapore)

Program Chairs
Jianying Zhou (I2R, Singapore)
Moti Yung (Columbia University, USA)

Publicity Chair
Yongfei Han (ONETS, China)

Program Committee
Carlisle Adams (Univ. of Ottawa, Canada)
Tuomas Aura (Microsoft Research, UK)
Roberto Avanzi (Ruhr Univ., Germany)
Giampaolo Bella (Univ. of Catania, Italy)
Kefei Chen (Shanghai Jiaotong Univ., China)
Ed Dawson (QUT, Australia)
Robert Deng (SMU, Singapore)
Xiaotie Deng (City Univ., Hong Kong)
Yvo Desmedt (UCL, UK)
Marc Girault (France Telecom, France)
Dieter Gollmann (TU Harburg, Germany)
Stefanos Gritzalis (U. of the Aegean, Greece)
Jens Groth (UCLA, USA)
Peter Gutmann (U. Auckland, New Zealand)
Yongfei Han (ONETS, China)
Amir Herzberg (Bar-Ilan Univ., Israel)
John Ioannidis (Columbia Univ., USA)
Jonathan Katz (Univ. of Maryland, USA)
Angelos D. Keromytis (Columbia Univ., USA)
Taekyoung Kwon (Sejong University, Korea)
Wenke Lee (Georgia Institute of Tech., USA)
Ninghui Li (Purdue Univ., USA)
Javier Lopez (Univ. of Malaga, Spain)
Stefan Lucks (Univ. of Mannheim, Germany)
Subhamoy Maitra (ISI, India)
Patrick McDaniel (PSU, USA)
Chris Mitchell (RHUL, UK)
Refik Molva (Eurecom, France)
Sang-Jae Moon (KNU, Korea)
David Naccache (ENS, France)
Rolf Oppliger (eSECURITY, Switzerland)
Elisabeth Oswald (Graz U. of Tech., Austria)
Guenther Pernul (U. Regensburg, Germany)
Raphael Phan (Swinburne UT, Malaysia)
Michael Roe (Microsoft Research, UK)
Rei Safavi-Naini (U. Wollongong, Australia)
Kouichi Sakurai (Kyushu Univ., Japan)
Pierangela Samarati (Univ. of Milan, Italy)
Vitaly Shmatikov (UT Austin, USA)
Masakazu Soshi (JAIST, Japan)
Francois-Xavier Standaert (UCL, Belgium)
Ravi Sundaram (Northeastern Univ., USA)
Tsuyoshi Takagi (Future Univ., Japan)
Pim Tuyls (Philips Research, The Netherlands)
Wen-Guey Tzeng (NCTU, Taiwan)
Guilin Wang (I2R, Singapore)
Xiaofeng Wang (Indiana Univ., USA)
Brent Waters (Stanford Univ., USA)
Shyhtsun Felix Wu (UC Davis, USA)
Yuliang Zheng (UNCC, USA)

Contact: acns06@i2r.a-star.edu.sg

Original papers on all technical aspects of cryptology and network security are solicited for submission to ACNS'06, the 4th annual conference on Applied Cryptography and Network Security. There are two tracks for ACNS: an academic track and an industrial track. The latter has an emphasis on practical applications. Topics of relevance include but are not limited to:

- Applied cryptography, cryptographic constructions
- Cryptographic applications: payments, fair exchange, time-stamping, auction, voting, polling
- Denial of service: attacks and countermeasures
- Email security, spam prevention
- Fundamental services on network and distributed systems: authentication, data integrity, confidentiality, authorization, non-repudiation, and availability
- Implementation, deployment and management of network security policies
- Integrating security in Internet protocols: routing, naming, TCP/IP, multicast, network management
- Integrating security services with system and application security facilities and protocols: message handling, file transport/access, directories, time synchronization, database management, boot services, mobile computing
- Intellectual property protection: protocols, implementations, metering, watermarking, digital rights management
- Intrusion avoidance, detection, and response: systems, experiences and architectures
- Network perimeter controls: firewalls, packet filters, application gateways
- Public key infrastructure, key management, certification, and revocation
- Securing critical infrastructure: routing protocols, and emergency communication
- Security and privacy for emerging technologies: sensor networks, wireless/mobile (and ad hoc) networks, bluetooth, 802.11, and p2p systems
- Security of limited devices: light-weight cryptography, efficient protocols and implementations, and tamper resistance
- Security modeling and protocol design in the context of rational and malicious adversaries
- Security policy construction, management, and systems
- Usable security and deployment incentives for security technology
- Virtual private networks
- Web security and supporting systems security, such as databases, operating systems, etc.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference that has proceedings. The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords, in Portable Document Format with all fonts embedded, at most 15 pages excluding bibliography and appendices. Authors are requested to mark their submissions as "academic track" or "industrial track". Submissions to the academic track may be considered for the industrial track (with author permission). Also, authors are requested to indicate whether submissions are to be considered for the best student paper; only papers co-authored and presented by a full-time student are eligible for this award.

Authors of accepted papers must guarantee that their paper will be presented at the conference.

Proceedings for the academic track will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Proceedings for the industrial track will be published in a separate volume, not the LNCS.