CALL FOR PAPERS

5th International Conference on Applied Cryptography and Network Security (ACNS '07) June 5-8, 2007, Zhuhai, China

http://www.i2r.a-star.edu.sg/icsd/acns2007/

Submissions due: December 14, 2006
Notification by: February 20, 2007

General Chair
Yongfei Han (ONETS, China)

Program Chairs
Jonathan Katz (Univ. of Maryland, USA)
Moti Yung (Columbia University, USA)

Publicity Chair
Jianying Zhou (I^{2}R, Singapore)

Program Committee
Giuseppe Ateniese (Johns Hopkins U., USA)
Michael Backes (Saarland University, Germany)
Feng Bao (I^{2}R, Singapore)
Steven M. Bellovin (Columbia University, USA)
John Black (U. Colorado at Boulder, USA)
Levente Buttyán (Budapest U. of Technology and Economics, Hungary)
Claude Castelluccia (INRIA, France)
Jean-Sébastien Coron (U. Luxembourg)
Nicolas Courtois (Univ. College of London, UK and Gemalto, France)
Kevin Fu (UMass Amherst, USA)
Philippe Golle (PARC, USA)
Michael Goodrich (UC Irvine, USA)
Alejandro Hevia (University of Chile)
Susan Hohenberger (IBM Research, Switzerland)
Nick Hopper (University of Minnesota, USA)
Gene Itkis (Boston University, USA)
Markus Jakobsson (University of Indiana, USA)
Charanjit Jutla (IBM Research, USA)
Kaoru Kurosawa (Ibaraki University, Japan)
Xuejia Lai (Shanghai Jiaotong University, China)
Dong Hoon Lee (CIST, S. Korea)
Phil MacKenzie (Google, USA)
Ilya Mironov (Microsoft Research, USA)
Pascal Paillier (Gemalto, France)
Kenny Paterson (Royal Holloway, U. London, UK)
Raphael Phan (Swinburne U. of Tech., Malaysia)
Benny Pinkas (University of Haifa, Israel)
David Pointcheval (CNRS and ENS, France)
Zulfikar Ramzan (Symantec Inc., USA)
Phil Rogaway (UC Davis, USA and Chiang Mai University, Thailand)
Kazue Sako (NEC, Japan)
Palash Sarkar (Indian Stat. Institute, India)
Vitaly Shmatikov (U. Texas at Austin, USA)
Thomas Shrimpton (Portland State U., USA)
Nigel Smart (University of Bristol, UK)
Ron Steinfeld (Macquarie University, Australia)
Adam Stubblefield (Johns Hopkins Univ., USA)
Mike Szydlo (RSA Labs, USA)
Brent Waters (SRI International, USA)
Avishai Wool (Tel Aviv University, Israel)
Sung-Ming Yen (National Central U., Taiwan)
Jianying Zhou (I^{2}R, Singapore)

Original papers on all aspects of applied cryptography and network security are solicited for submission to ACNS '07. Topics of relevance include but are not limited to:

- Applied cryptography and provably-secure cryptographic protocols
- Design and analysis of efficient cryptographic primitives: public-key and symmetric-key cryptosystems, block ciphers, and hash functions
- Network security protocols
- Techniques for anonymity; trade-offs between anonymity and utility
- Integrating security into the next-generation Internet: DNS security, routing, naming, denial-of-service attacks, TCP/IP, secure multicast
- Economic fraud on the Internet: phishing, pharming, spam, and click fraud
- Email and web security
- Public key infrastructure, key management, certification, and revocation
- Security and privacy for emerging technologies: sensor networks, mobile (ad hoc) networks, peer-to-peer networks, bluetooth, 802.11, RFID
- Trust metrics and robust trust inference in distributed systems
- Security and usability
- Intellectual property protection: metering, watermarking, and digital rights management
- Modeling and protocol design for rational and malicious adversaries
- Automated analysis of protocols

As in previous years, there will be an academic track and an industrial track. Submissions to the academic track should emphasize research contributions, while submissions to the industrial track may focus on implementation and deployment of real-world systems. Submissions for the industrial track must clearly indicate this in the title. Proceedings for the academic track will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Papers accepted to the industrial track will be published in a different venue.

Instructions for authors: Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Submissions should be in English, in PDF format with all fonts embedded, typeset with 11pt font or larger, and using reasonable spacing and margins. They should not exceed 12 letter-sized pages, not counting the bibliography and appendices. Papers should begin with a title, abstract, and an introduction that clearly summarizes the contributions of the paper at a level appropriate for a non-specialist reader. Papers should contain a scholarly exposition of ideas, techniques, and results, including motivation, relevance to practical applications, and a clear comparison with related work. Committee members are not required to read appendices, and papers should be intelligible without them. Submitted papers risk being rejected without consideration of their merits if they do not follow all the above guidelines.

Submissions must not substantially duplicate work that was published elsewhere, or work that any of the authors has submitted in parallel to any other conference or workshop that has proceedings. **Plagiarism** and **double submissions** will be dealt with harshly.

Authors will be asked to indicate whether their submissions should be considered for the best student paper award; any paper co-authored by a full-time student is eligible for this award.

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