CALL FOR PAPERS

7th International Conference on
Applied Cryptography and Network Security (ACNS '09)
June 2-5, 2009, Paris-Rocquencourt, France

http://acns09.di.ens.fr

ACNS '09 is organized by INRIA, CNRS and ENS, in France, in cooperation with the International Association for Cryptologic Research.

Submissions due: January 12, 2009
Notification by: March 8, 2009

General Chairs
Pierre-Alain Fouque (ENS, France)
Damien Vergnaud (ENS, France)

Program Chairs
Michel Abdalla (ENS, France)
David Pointcheval (ENS, France)

Program Committee
Gildas Avoine (UCL, Belgium)
Feng Bao (I2R, Singapore)
Christophe Bidan (Supélec, France)
Alex Biryukov (Univ. of Luxembourg)
Xavier Boyen (Voltage, USA)
Dario Catalano (Univ. di Catania, Italy)
Liqun Chen (HP, UK)
Jean-Sébastien Coron (Univ. of Luxembourg)
Jacques Demerjian (CS, France)
Aline Gouget (Gemalto, France)
Louis Granboulan (EADS, France)
Peter Gutmann (Univ. of Auckland, New-Zealand)
Nick Howgrave-Graham (NTRU Cryptosystems, USA)
Stanislaw Jarecki (UC at Irvine, USA)
Marc Joye (Thomson R&D, France)
Jaeyeon Jung (Intel, USA)
Seny Kamara (Microsoft Research, USA)
Jonathan Katz (Univ. of Maryland, USA)
Aggelos Kiayias (Univ. of Connecticut, USA)
Xuejia Lai (SJTU, China)
Javier Lopez (Univ. de Malaga, Spain)
Olivier Orcière (Thales, France)
Kenny Paterson (Royal Holloway, UK)
Giuseppe Persiano (Univ. di Salerno, Italy)
Josef Pieprzyk (Univ. of Macquarie, Australia)
Matt Robshaw (Orange Labs, France)
Kazue Sako (NEC, Japan)
Palash Sarkar (Indian Statistical Institute, India)
Berry Schoenmakers (TUE, The Netherlands)
Hovav Shacham (UC at San Diego, USA)
Jessica Staddon (PARC, USA)
Michael Szydlo (Akamai, USA)
Serge Vaudenay (EPFL, Switzerland)
Avishai Wool (Tel Aviv University, Israel)
Duncan Wong (City University of Hong Kong)
Jianying Zhou (I2R, Singapore)

Original papers on all aspects of applied cryptography and network security are solicited for submission to ACNS '09. 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.

Instructions for authors: Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any journal or other conference or workshop that has proceedings.
Submissions will take place entirely via a web system, available from https://acns09.di.ens.fr/iChair/.
All submissions will be blind reviewed. The paper must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. It should begin with a title, a short abstract, and a list of keywords.

The final proceedings version will be a paper of at most 18 pages in the llncs style, which corresponds to around 7000 words of text. The document submitted (excluding appendices) should correspond to what the authors expect to be published if their paper is accepted without modification. We therefore strongly recommend that authors check whether their paper (without appendices) will fit within the above llncs space constraints. Committee members are not required to review more than that, so the paper should be intelligible and self-contained within this length. Submissions not meeting these guidelines risk rejection without consideration of their merits.

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.

The proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference.
Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers. Authors of accepted papers must guarantee that their paper will be presented at the conference.