CALL FOR PAPERS

8th International Conference on Applied Cryptography and Network Security (ACNS '10)
June 22-25, 2010, Beijing, China

www.tcgchina.org/acns2010/

Submissions due Feb. 5, 2010 (FIRM)
Notification by Mar. 31, 2010
Camera-ready due Apr. 20, 2010

Original papers on all aspects of applied cryptography and network security are solicited for submission to ACNS '10. 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 and digital rights management
- Modeling and protocol design for rational and malicious adversaries
- Automated analysis of protocols

Papers suggesting novel paradigms, original directions, or non-traditional perspectives are especially welcome.

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. Please indicate in the title for submissions to the industrial track. The academic track will have proceedings published in Springer's LNCS and will be available at the conference. The industrial track will only have presentations without formal proceedings.

Instructions for authors: 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. 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.

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.

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