Call for Papers:

3rd Applied Cryptography and Network Security Conference (ACNS) 2005

June 7-10, 2005

Columbia University, New York, NY, USA

http://acns2005.cs.columbia.edu

Original research papers on all technical aspects of cryptology are solicited for submission to ACNS 2005, the 3rd annual conference on Applied Cryptography and Network Security.

Submission Deadline: 26 January 2005
Author Notification: 1 April 2005
Camera-Ready Copy: 15 April 2005

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop that has proceedings. There will be two tracks: an academic track, and a technical/industrial track. Submissions to the academic track should emphasize research advances, while submissions to the technical/industrial track may focus on implementations of known schemes and deployment observations. Submissions to the industrial track may be talk proposals. The PC may move (with author permission) submissions between tracks. Authors should mark their submission as "academic track" or "industrial track." Also, authors should indicate whether submissions should be considered for the best student paper; only papers co-authored and presented by a full-time student are eligible for this award.

Additional information about the submission process and a more complete list of topics is available in the online version of the Call for Papers at: http://acns2005.cs.columbia.edu/cfp.html

Program Committee

Scott Alexander (Telcordia, USA)
Tuomas Aura (Microsoft, UK)
David Brumley (CMU, USA)
Ran Canetti (IBM Research, USA)
Marc Dacier (Eurecom, France)
Ed Dawson (Queensland U. of Tech, Australia)
Glenn Durfee (PARC, USA)
Virgil Gligor (U. of Maryland, USA)
Peter Gutman (U. of Auckland, New Zealand)
Goichiro Hanaoka (U. of Tokyo, Japan)
Amir Herzberg (Bar Ilan U., Israel)
Russ Housley (Vigilsec, USA)
John Ioannidis (Columbia U., USA)
Sotiris Ioannidis (UPenn, USA)
Stas Jarecki (UC Irvine, USA)
Ari Juels (RSA Laboratories, USA)
Angelos Keromytis (Columbia U., USA)
Aggelos Kiayias (UConn, USA)
Tanja Lange (U. Bochum, Germany)
Dong Hoon Lee (Korea U., South Korea)
Fabio Massacci (U. Trento, Italy)
Atsuko Miyaji (JAIST, Japan)
Frederic Muller (DCSSI Crypto Lab, France)
Kaisa Nyberg (Nokia, Finland)
Bart Preneel (K.U. Leuven, Belgium)
Vassilis Prevelakis (Drexel U., USA)
Niels Provos (Google, USA)
Pierangela Samarati (U. of Milan, Italy)
Tomas Sander (HP, USA)
Dan Simon (Microsoft Research, USA)
Tsuyoshi Takagi (T.U. Darmstadt, Germany)
Wen-Guey Tzeng (NCTU, Taiwan)
Dan Wallach (Rice U., USA)
Susanne Wetzel (Stevens, USA)
Moti Yung (Columbia U., USA)
Jianying Zhou (I^2R, Singapore)
Lidong Zhou (Microsoft Research, USA)

Topics:

- cryptographic constructions (payments, fair exchange, auctions, voting)
- security modeling, protocol design with rational malicious adversaries
- efficient protocols, lightweight cryptography
- PKI, key management
- network security policy management
- economic incentives for collaboration, deployment incentives for security technology
- network and distributed systems security (authentication, authorization, integrity, confidentiality, non-repudiation, availability)
- integrating security in Internet protocols (routing, naming, TCP/IP, multicast, network management)
- network perimeter control (firewall, packet filtering, application gateways)
- DoS, DDoS (attacks and countermeasures)
- intrusion avoidance, detection, and response
- web, chat, and e-mail security
- spam detection and prevention
- web application and database security
- security and privacy for emerging technologies (sensor networks, wireless ad hoc networks, p2p systems)