ICISC 2006

Call for Papers

The 9th Annual International Conference on Information Security and Cryptology
Nov. 30 - Dec. 1, 2006, Busan, Korea
http://www.icisc.org/

Submission deadline (extended): July 10. 2006 18:00 KST (GMT + 9 hr)

Original papers pertaining to all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2006, the 9th Annual International Conference on Information Security and Cryptology. ICISC 2006 is sponsored by KIISC (Korean Institute of Information Security and Cryptology) and financially supported by MIC (Ministry of Information and Communication, Korea).

Topics of Interest include, but are not limited to:

- Access Control & Audit
- Authentication and Authorization
- Biometrics
- Block/Stream Ciphers
- Computer Forensics
- Copyright Protection
- Cryptographic Protocols
- Cryptanalysis
- Digital Signatures
- Distributed Systems Security
- Efficient Implementations
- Electronic Commerce
- Elliptic Curve Cryptosystems
- Hash Functions
- Information Hiding
- Internet/Intranet Security
- Intrusion Detection
- Key/Identity Management
- Malicious Codes
- Mobile Communications Security
- Public Key Cryptosystems
- Public Key Infrastructure
- Secret Sharing
- Security Management
- Smart/Java Cards
- Zero Knowledge

Instructions for Authors

Submission should not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any journal or any other conference or workshop that has proceedings. The paper must be anonymous. The length of the submission should not exceed 12 pages excluding the bibliography and clearly marked appendices, using at least 11 point fonts and reasonable margins. Since committee members are not required to read the appendices, the paper should be intelligible without them. All papers must be in PostScript (PS) or Portable Document Format (PDF). It is strongly recommended that submissions be processed using LaTeX2e according to the instruction at http://www.springer.de/comp/lncs/authors.html. Authors of accepted papers must guarantee that their paper will be presented at the conference. Details on the electronic submission process is available on the ICISC 2006 web site, http://www.icisc.org/. Authors should submit their papers electronically through the submission server, https://icisc2006.joongbu.ac.kr/iChair/.

Important Dates

- Submission deadline (extended): July 10. 2006 18:00 KST (GMT + 9 hr)
- Acceptance notification: Aug. 21. 2006
- Final version: Sep. 8. 2006

Conference Proceedings

Proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Instructions about the preparation of a final proceeding version will be sent to the authors of accepted papers.

Organizing Chair

Kyung-Hyune Rhee
Pukyong National University
599-1 Daeyeon 3-Dong Namgu, Busan 608-737, Korea
E-mail: khrhee@pknu.ac.kr

Program Co-Chair

Min Surp Rhee
Dankook University
San #29, Anseo-dong, Cheonan-shi, Chungnam, 330-714, Korea
E-mail: msrhee@dankook.ac.kr

Byoungcheon Lee
Joongbu University
101 Daehak-ro, Chubu-meon, Guemsan-Gun, Chungnam, 312-702, Korea
E-mail: sultan@joongbu.ac.kr

Contact mail : icisc06chair@dankook.ac.kr

Program Committee

Giuseppe Ateniese (The Johns Hopkins University, USA)
Joonsang Baek (Institute for Infocomm Research, Singapore)
Alex Biryukov (Katholieke Universiteit Leuven, Belgium)
John Black (University of Colorado, USA)
Jean-Sebastien Coron (University of Luxembourg, Luxembourg)
Jung Hee Cheon (Seoul National University, Korea)
Kyo-il Chung (ETRI, Korea)
Ed Dawson (Queensland University of Technology, Australia)
Yevgeniy Dodis (New York University, USA)
Serge Fehr (CWI Amsterdam, Netherlands)
Pierre-Alain Fouque (Ecole Normale Superieure, France)
Marc Girault (France Telecom, France)
Philippe Golle (Palo Alto Research Center, USA)
Dieter Gollmann (Hamburg University of Technology, Germany)
Yongfei Han (ONETS, China)
Goichiro Hanaoka(AIST, Japan)
Marc Joye (Gemplus, France)
Jonathan Katz (University of Maryland, USA)
Hiroaki Kikuchi (Tokai University, Japan)
Hwankoo Kim (Hoseo University, Korea)
Kwangjo Kim (Information and Communication University, Korea)
Darko Kirovski (Microsoft Research, USA)
Kaoru Kurosawa (Ibaraki University, Japan)
Taekyoung Kwon (Sejong University, Korea)
Chi Sung Laih (Kun Shan University, Taiwan)
Kwok-Yan Lam (Tsinghua Univ., China)
Kristin Lauter (Microsoft Research, USA)
Dong Hoon Lee (Korea University, Korea)
Pil Joong Lee (POSTECH, Korea)
Sang-Ho Lee (Ewha Womans University, Korea)
Arjen Lenstra (EPFL, Switzerland)
Yingjiu Li (Singapore Management University, Singapore)
Helger Lipmaa (Cybernetica AS & University of Tartu, Estonia)
Javier Lopez (University of Malaga, Spain)
Masahiro Mambo (University of Tsukuba, Japan)
Keith Martin (Royal Holloway, University of London, UK)
Mitsuru Matsui (Mitsubishi Electric Corporation, Japan)
Chris Mitchell (Royal Holloway University of London, UK)
Atsuko Miyaji (JAIST, Japan)
SangJae Moon (Kyungpook National University, Korea)
Yi Mu (University of Wollongong, Australia)
Rei Safavi-Naini (Wollongong University, Australia)
Jesper Buus Nielsen (Aarhus University, Denmark)

DaeHun Nyang (Inha University, Korea)
Rolf Oppliger (eSecuriry Technologies, Switzerland)
Carles Padro (Technical University of Catalonia, Spain)
Raphael Chung-Wei Phan (Swinburne University of Technology, Malaysia)
Kouichi Sakurai (Kyushu University, Japan)
Palash Sarkar (Indian Statistical Institute, India)
Nigel Smart (University of Bristol, UK)
Willy Susilo (University of Wollongong, Australia)
Tsuyoshi Takagi (Future University, Hakodate, Japan)
Serge Vaudenay (EPFL, Switzerland)
Guilin Wang (Institute for Infocomm Research, Singapore)
William Whyte (NTRU Cryptosystems, USA)
Michael Wiener (Cryptographic Clarity, Canada)
Dongho Won (Sungkyunkwan University, Korea)
Sung-Ming Yen (National Central University, Taiwan)
Yongjin Yeom (NSRI. Korea)
Fangguo Zhang (Sun Yat-sen University, China)
Alf Zugenmaier (DoCoMo Euro-Labs, Germany)