The 8th International Conference on
CRYPTOLOGY AND NETWORK SECURITY (CANS 2009)

12 - 14 December 2009
Kanazawa, Ishikawa, Japan

Web Page: http://www.rcis.aist.go.jp/cans2009/   Contact: cans2009-info@m.aist.go.jp

- Call for Papers -

Overview

The main goal of this conference is to promote research on all aspects of network security, as well as to build a bridge between research on cryptography and on network security. We therefore welcome scientific and academic papers with this focus. Previous CANS have been held in Taipei (2001), San Francisco (2002), Miami (2003), Xiamen (2005), Suzhou (2006), Singapore (2007), and Hong Kong (2008).

Topics

Areas of interest for CANS 2009 include, but are not limited to:

- Ad Hoc and Sensor Network Security
- Access Control for Networks
- Anonymity and Pseudonymity
- Authentication Services
- Block and Stream Cipher Design
- Cryptographic Protocols and Schemes
- Denial of Service Protection
- Digital Rights Management
- Fast Cryptographic Algorithms
- Hash Functions
- Identity and Trust Management
- Information Hiding and Watermarking
- Internet and Router Security
- Intrusion Detection and Prevention
- Mobile and Wireless Network Security
- Multicast Security
- Phishing and Online Fraud Prevention
- Peer-to-Peer Network Security
- PKI
- Security Modeling and Architectures
- Secure Protocols (SSH, SSL, ...) and Applications
- Spam Protection
- Spyware Analysis and Detection
- Virtual Private Networks

Instructions for Authors

Papers on cryptology and network security are welcome. Papers that make a substantial link between these areas will be given priority. Authors of such papers are encouraged to elaborate on the relevant connection in a subsection of the introduction. High-quality papers on pure cryptology or pure network security may also be accepted.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel for consideration of any other conference or workshop with proceedings. Submissions should have at most 12 pages excluding the bibliography and appendices, and at most 20 pages in total, using at least 11-point fonts and with reasonable margins. The total length of the final versions for Springer's LNCS will be at most 20 pages. Committee members are not required to read appendices; the paper should be intelligible without them. All submissions should be anonymous. Authors of accepted papers must guarantee that at least one of the authors will attend the conference and present their paper.

Submitted papers should follow the formatting instructions of the Springer LNCS Style. Please check the Information for LNCS Authors page at Springer at http://www.springer.com/lncs for style and formatting guidelines. Submissions not meeting the submission guidelines risk rejection without consideration of their merits.

Proceedings

The conference proceedings will be published in the Lecture Notes in Computer Science series by Springer Verlag (http://www.springer.com/lncs), and be available at the conference.

Important Dates

Submission Deadline (extended): 17 June 2009 (12:00:00 JST)
Acceptance Notification: 14 August 2009 (JST)
Camera-ready Copy Due: 4 September 2009
Conference: 12 - 14 December 2009

Invited Speakers

Title: Building Secure Networked Systems with Code Attestation   Speaker: Adrian Perrig (CMU, US)
Title: TBA.   Speaker: Adam Smith   (Penn State Univ, US)

Best Paper Award

The Program Committee will consider giving a Best Paper Award to the submission with highest merits. (Details to be announced.)

Stipend

A limited number of stipends are available to those unable to obtain funding to attend the conference, and to students whose papers are accepted and who will present the paper themselves. Requests for stipends should be addressed to the general chair by August 31st.

Program Committee and Organizers

Jointly Organized By:
National Institute of Advanced Industrial Science and Technology (AIST), Japan
Japan Advanced Institute of Science and Technology (JAIST), Japan

Supported By:
Special Interest Group on Computer Security (CSEC), IPSJ, Japan
Technical Group on Information Security (ISEC), IEICE, Japan
Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan
Society of Information Theory and its Applications (SITA), Japan

Sponsored By:
National Institute of Information and Communications Technology (NICT), Japan
Institute of Regional Information Systems (IRIS), Japan
ComWorth Co., LTD, Japan
Hitachi, Ltd., Japan
Hokuriku Telecommunication Network Co.,Inc., Japan

CANS Steering Committee:

Yvo Desmedt	University College London, UK	Yi Mu	University of Wollongong, Australia
Matt Franklin	UC Davis, US	David Pointcheval	CNRS and ENS, France
Lucas Hui	The University of Hong Kong, China	Huaxiong Wang	NTU, Singapore

General Chair:
Akira Otsuka   AIST, Japan

Program Co-Chairs:

Juan A. Garay	AT&T Labs - Research, US	Atsuko Miyaji	JAIST, Japan

Program Committee:

Jean-Luc Beuchat	Tsukuba Univ, Japan	Subhamoy Maitra	Indian Statistical Institute, India
Alexandra Boldyreva	Georgia Tech, US	Mark Manulis	TU Darmstadt, Germany
Colin Boyd	Queensland Univ of Technology, Australia	David Nowak	AIST, Japan
		Wakaha Ogata	Tokyo Institute of Technology, Japan
Emmanuel Bresson	DCSSI Crypto Lab, France	C. Pandu Rangan	IIT Madras, India
Mike Burmester	FSU, US	Kenny Paterson	Royal Holloway, University of London, UK
Koji Chida	NTT Labs, Japan	Rene Peralta	NIST, US
Ee-Chien Chang	National University of Singapore, Singapore	Josef Pieprzyk	Macquarie University, Australia
		German Saez	UPC, Spain
Rosario Gennaro	IBM Watson, US	Taizo Shirai	Sony, Japan
Trevor Jim	AT&T Labs - Research, US	Adam Smith	Penn State Univ, US
Charanjit Jutla	IBM Watson, US	Jessica Staddon	PARC, US
Seny Kamara	Microsoft Research, US	Douglas Stinson	University of Waterloo, Canada
Aggelos Kiayias	UConn, US	Willy Susilo	University of Wollongong, Australia
Vladimir Kolesnikov	Bell Labs, US	Tsuyoshi Takagi	Future University - Hakodate, Japan
Tanja Lange	Technical University Eindhoven, Netherlands	Gene Tsudik	UC Irvine, US
		Ivan Visconti	University of Salerno, Italy
Dong Hoon Lee	Korea Univ, Korea	Xiaoyun Wang	Shandong University, China
Pil Joong Lee	Pohang University of Science and Technology, Korea	Duncan S Wong	City University of Hong Kong, China
		Sung-Ming Yen	National Central University, Taiwan
Benoit Libert	UCL, Belgium	Hong-Sheng Zhou	UConn, US
Helger Lipmaa	Cybernetica AS, Estonia	Jianying Zhou	I2R, Singapore

Organizing Committee:

Tomoyuki Asano	Sony, Japan	Yutaka Oiwa	AIST, Japan
Isao Echizen	NII, Japan	Takeshi Okamoto	Tsukuba University of Technology, Japan
Shoichi Hirose	University of Fukui, Japan	Kazumasa Omote	JAIST, Japan
Atsuo Inomata	NAIST, Japan	Kensuke Shibata	NTT Labs, Japan
Daisuke Inoue	NICT, Japan	Yuji Suga	IIJ, Japan
Shinichiro Matsuo	NICT, Japan	Toshihiro Tabata	Okayama University, Japan
Tatsuyuki Matsushita	Toshiba, Japan	Katsuyuki Takashima	Mitsubishi Electric, Japan
Natsume Matsuzaki	Panasonic, Japan	Keisuke Takemori	KDDI R&D Labs., Japan
Kunihiko Miyazaki	Hitachi, Japan	Shoko Yonezawa	AIST, Japan
Takao Ogura	Fujitsu Laboratories, Japan		