IWSEC 2017 The 12th International Workshop on Security

August 30 (Wed) - September 1 (Fri), 2017
International Conference Center Hiroshima, Hiroshima, Japan
Web: http://www.iwsec.org/2017/
Mail: iwsec2017-inquiry@klab.is.sci.toho-u.ac.jp

Co-organized by CSEC of IPSJ, Japan and ISEC of IEICE, Japan

Call for Papers

Original papers on the research and development of various security topics, as well as case studies and implementation experiences, are solicited for submission to IWSEC 2017. Topics of interest for IWSEC 2017 include all theory and practice of cryptography, information security, and network security, as in previous IWSEC workshops. In particular, we encourage the following topics this year:

- Big Data Analysis for Security
- Critical Infrastructure Security
- Cryptanalysis
- Cryptographic Protocols
- Cybersecurity Economics
- Digital Forensics
- Enriched Cryptography
- Financial Security
- Formal Methods
- Information Law and Ethics
- IoT security

- Machine Learning for Security
- Malware Countermeasures
- Measurements for Cybersecurity
- Multiparty Computation
- Post Quantum Cryptography
- Privacy Preserving
- Rational Cryptography
- Real World Cryptography
- Security Management
- Visualization for Security

Important Dates

**Submission of papers ** extended ** **	March 14, 2017 (23:59 JST)
Notification of decision	May 10, 2017
Final version due	May 30, 2017

Proceedings

The proceedings is planned to be published by Springer-Verlag in the Lecture Notes in Computer Science series. The proceedings of IWSEC 2006 to IWSEC 2016 appeared as LNCS 4266, 4752, 5312, 5824, 6434, 7038, 7631, 8231, 8639, 9241 and 9836 respectively.
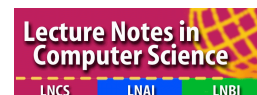
Instructions for Authors

Submitted papers must be original, unpublished, and not submitted to other conferences or journals for consideration for publication. Papers must be written in English and be fully anonymous with no author names, affiliations, acknowledgements, or obvious references. They should be at most 16 pages long in total (including bibliography and appendices), in the standard LNCS format (except for author names and affiliations). They should be submitted electronically in PDF format. A detailed description of the electronic submission procedure will be available at the workshop website. Submissions not meeting the submission guidelines risk rejection without consideration of their merits. A part of papers may be accepted as short papers. At least one author of each accepted paper is required to register with the workshop until final version due, and is also required to present the paper in the conference. If no author registers or presents the paper, the paper will be rejected regardless of the reasons. Note that, if your paper is accepted, the title and the author list in your submission cannot be changed when preparing the final version without the approval of the program co-chairs.

Best Paper Awards

Prizes will be awarded to the authors of the best paper(s) and the best student paper(s).

Poster Session

IWSEC 2017 plans to have a poster session. Posters can present on-going study, idea or project that is not mature yet, but interesting work in progress. The details and submission deadline will be announced on the web page. Prizes will be awarded to the authors of the best poster presentation(s).

Social Events

Social events are planned in the conference. Their details will be announced on the web page.

Keynote Talks

We will have keynote talks from the following world-leading researchers.

Dr. Khaled El Emam (University of Ottawa, Canada)
Title: To be announced

Dr. Khaled El Emam is a Professor at the University of Ottawa, Faculty of Medicine, and a Senior Investigator at the Children's Hospital of Eastern Ontario Research Institute. From 2005 to 2015 he held the Canada Research Chair in Electronic Health Information at the University of Ottawa. His main area of research is developing techniques for health data anonymization and secure disease surveillance for public health purposes. He is also the founder and president of Privacy Analytics Inc., which develops solutions for the de-identification of health information. In 2016 Privacy Analytics was acquired by IMS Health Inc (now QuintilesIMS).
Previously Khaled was a Senior Research Officer at the National Research Council of Canada, and prior to that he was head of the Quantitative Methods Group at the Fraunhofer Institute in Kaiserslautern, Germany. In 2003 and 2004, he was ranked as the top systems and software engineering scholar worldwide by the Journal of Systems and Software based on his research on measurement and quality evaluation and improvement, and ranked second in 2002 and 2005. He holds a Ph.D. from the Department of Electrical and Electronics, King's College, at the University of London (UK).

Dr. Kazue Sako (NEC, Japan)
Title: To be announced

Dr. Kazue Sako received her B.S. degree and PhD from Kyoto University. Her research interest is in cryptographic protocols that enhance privacy and fairness, e.g. electronic voting protcols, group signature schemes, digital lottery systems and blockchain architecture. In order to promote the use of anonymous authentication, she edited ISO/IEC 29191 and ISO/IEC 20008-2. She served as Program co-Chair/ Chair for ASIACRYPT 2012, 2013 and RSA conference 2016 Cryptographer's Track. She is a strong advocate of Personal Data EcoSystem, which empowers individuals with their own data. She is Senior Principal Engineer at NEC. She is also a member of the Science Council of Japan.

Committees

General co-chairs: Kazuto Ogawa (Japan Broadcasting Corporation, Japan)
Masayuki Terada (NTT DOCOMO, Japan)

Program co-chairs: Satoshi Obana (HOSEI University, Japan)
Koji Chida (NTT, Japan)

Poster chair: Takumi Yamamoto (Mitsubishi Electric Corporation, Japan)

Program Committees

Mohamed Abid (University of Gabes, Tunisia)
Mitsuaki Akiyama (NTT, Japan)
Elena Andreeva (KU Leuven, Belgium)
Reza Azarderakhsh (Florida Atlantic University, USA)
Josep Balasch (KU Leuven, Belgium)
Gregory Blanc (Telecom SudParis, France)
Olivier Blazy (Universite de Limoges, France)
Aymen Boudguiga (Institute for Technological Research SystemX, France)
Kai-Chi Chang (National Center for Cyber Security Technology, Taiwan)
Yue Chen (Florida State University, USA)
Celine Chevalier (Universite Pantheon-Assas, France)
Koji Chida (NTT, Japan) ** chair **
Sabrina De Capitani di Vimercati (DI - Universita degli Studi di Milano, Italy)
Herve Debar (Telecom SudParis, France)
Itai Dinur (Ben-Gurion University, Israel)
Josep Domingo-Ferrer (Universitat Rovira i Virgili, Spain)
Oriol Farras (Universitat Rovira i Virgili, Spain)
Atsushi Fujioka (Kanagawa University, Japan)
Dawu Gu (Shanghai Jiao Tong University, China)
Roberto Guanciale (KTH Royal Institute of Technology, Sweden)
Atsuo Inomata (Tokyo Denki University, Japan)
Akira Kanaoka (Toho University, Japan)
Florian Hahn (SAP, Germany)
Hiroaki Kikuchi (Meiji University, Japan)
Hyung Chan Kim (The Affiliated Institute of ETRI, Korea)
Yuichi Komano (Toshiba Corporation, Japan)
Noboru Kunihiro (The University of Tokyo, Japan)
Maryline Laurent (Telecom SudParis, France)
Heejo Lee (Korea University, South Korea)
Hyung Tae Lee (Nanyang Technological University, Singapore)
Zhou Li (RSA Labs., USA)
Frederic Majorczyk (DGA-MI/CentraleSupelec, France)
Florian Mendel (Graz University of Technology, Austria)

Bart Mennink (Radboud University, The Netherlands)
Kirill Morozov (Tokyo Institute of Technology, Japan)
Koichi Mouri (Ritsumeikan University, Japan)
Ivica Nikolic (Nanyang Technological University, Singapore)
Ryo Nojima
   (National Institute of Information and Communications Technology, Japan)
Satoshi Obana (HOSEI University, Japan) ** chair **
Alexis Olivereau (CEA LIST, France)
Kaan Onarlioglu (Northeastern University, USA)
Thomas Peyrin (Nanyang Technological University, Singapore)
Yusuke Sakai
   (National Institute of Advanced Industrial Science and Technology, Japan)
Yu Sasaki (NTT, Japan)
Dominique Schroder
   (Friedrich-Alexander Universität Erlangen-Nürnberg, Germany)
Yannick Seurin
   (Agence Nationale de la Securite des Systemes d'Information, France)
Yuji Suga (Internet Initiative Japan Inc., Japan)
Willy Susilo (University of Wollongong, Australia)
Mio Suzuki
   (National Institute of Information and Communications Technology, Japan)
Katsuyuki Takashima (Mitsubishi Electric Corporation, Japan)
Mehdi Tibouchi (NTT, Japan)
Giorgos Vasiliadis (Qatar Computing Research Institute, HBKU, Greece)
Cong Wang (City University of Hong Kong, Hong Kong)
Sven Wohlgemut (Hitachi, Ltd., Japan)
Pa Pa Yin Minn (Yokohama National University, Japan)
Chung-Huang Yang (National Kaohsiung Normal University, Taiwan)
Kan Yasuda (NTT, Japan)
Maki Yoshida
   (National Institute of Information and Communications Technology, Japan)
Rui Zhang (Chinese Academy of Sciences, China)