

ISC 2018



General Chair

Steve Schneider, United Kingdom

Program Chairs

Liquan Chen, United Kingdom
Mark Manulis, United Kingdom
email: isc2018-0@easychair.org

Program Committee

Jean-Philippe Aumasson, Switzerland
Paulo Barreto, USA
Marina Blanton, USA
Ioana Boureanu, United Kingdom
Colin Boyd, Norway
Liquan Chen, United Kingdom
Sherman S. M. Chow, Hong Kong
Mauro Conti, Italy
James H. Davenport, United Kingdom
Lucas Davi, Germany
Alexandra Dmitrienko, Germany
Josep Domingo-Ferrer, Catalonia
François Dupressoir, United Kingdom
Thomas Espitau, France
Nils Fleischhacker, USA
Danilo Gligoroski, Norway
Tibor Jager, Germany
Stefan Katzenbeisser, Germany
Franziskus Kiefer, Germany
Xuejia Lai, China
Shujun Li, United Kingdom
Joseph Liu, Australia
Javier Lopez, Spain
Masahiro Mambo, Japan
Mark Manulis, United Kingdom
Catherine Meadows, USA
Florian Mendel, Germany
Chris Mitchell, United Kingdom
Atsuko Miyaji, Japan
Maire O'Neill, United Kingdom
Yanbin Pan, China
Andreas Peter, Netherlands
Duong Hieu Phan, France
Bertram Poettering, United Kingdom
Jeyavijayan Rajendran, USA
Peter Y. A. Ryan, Luxembourg
Mark Ryan, United Kingdom
Peter Scholl, Denmark
Jörg Schwenk, Germany
Luisa Siniscalchi, Italy
Willy Susilo, Australia
Melanie Volkamer, Sweden
Ding Wang, China
Lei Wang, China
Qian Wang, China
Jianying Zhou, Singapore

The 21th Information Security Conference will be organised by the Surrey Centre for Cyber Security (SCCS) and held at the University of Surrey in London (Guildford), UK. The proceedings of ISC 2018 will be published by Springer.



The conference seeks submissions presenting novel research on all technical aspects of applied cryptography, cyber security (incl. network and computer security) and privacy. This includes submissions from academia/industry on traditional and emerging topics and new paradigms in these areas, with a clear connection to real-world problems, systems or applications. Submissions may focus on the modelling, design, analysis (incl. security proofs and attacks), development (e.g. implementations), deployment (e.g. system integration), and maintenance (e.g. performance measurements, usability studies) of algorithms, protocols, standards, implementations, technologies, devices, or systems standing in relation with applied cryptography, cyber security and privacy, while advancing or bringing new insights to the state of the art. Some topics of interest include but not limited to:

Access control	Email and web security	Privacy/anonymity, PETs
Applied cryptography	Future Internet security	Pervasive security
Automated security analysis	Identity management	Security in e-commerce
Biometric security/privacy	IP protection	Security in P2P systems
Complex systems security	Internet fraud, cybercrime	Security in grid systems
Critical infrastructures	Internet-of-Things security	Cloud security/privacy
Cryptographic primitives	Intrusion detection	Security/privacy metrics
Cryptographic protocols	Key management	Trust management
Data protection	Malware	Ubiquitous security/privacy
Database/system security	Mobile/wireless/5G security	Human factors in security
Digital rights management	Network security protocols	Usability in security/privacy

Submission	16 Apr 2018
Notification	18 June 2018
Final version	02 July 2018



Instructions for authors Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other venue with formally published proceedings. Information about submissions may be shared with program chairs of other conferences for that purpose. Each submission must begin with a title, author names and affiliations, short abstract, and a list of keywords. The introduction should summarise the contributions of the paper at a level appropriate for a non-specialist reader. All submissions must follow the original LNCS format (see <http://www.springeronline.com/lncs>) with a page limit of 18 pages (incl. references) for the main part (reviewers are not required to read beyond this limit) and 30 pages in total. Authors of accepted papers must guarantee that their paper will be presented at the conference and must make a full version of their paper available online. Any paper co-authored by at least one full-time student who will present the paper at the conference is eligible for the best student paper award. Papers should be submitted electronically via <https://easychair.org/conferences/?conf=isc20180>