

ACNS 2016 | Call for Papers

14th International Conference on Applied Cryptography and Network Security



19-22 June 2016 in London (Guildford), United Kingdom

<http://acns2016.sccs.surrey.ac.uk>

General Chair

Steve Schneider, United Kingdom

Program Chairs

Mark Manulis, United Kingdom

Ahmad-Reza Sadeghi, Germany

Program Committee

Giuseppe Ateniese, Italy

Elias Athanasopoulos, Greece

Man Ho Au, Hong Kong

Liqun Chen, United Kingdom

Sherman Chow, Hong Kong

Mauro Conti, Italy

Lucas Davi, Germany

Alexandra Dmitrienko, Germany

Michael Franz, USA

Sebastian Gajek, Germany

Jens Groth, United Kingdom

Goichiro Hanaoka, Japan

Feng Hao, United Kingdom

Michael Huth, United Kingdom

Tibor Jager, Germany

Aniket Kate, USA

Stefan Katzenbeisser, Germany

Negar Kiyavash, USA

Vladimir Kolesnikov, USA

Wenke Lee, USA

Mark Manulis, United Kingdom

Ivan Martinovic, United Kingdom

Azalia Mirhoseini, USA

Atsuko Miyaji, Japan

Payman Mohassel, USA

Jörn Müller-Quade, Germany

David Naccache, France

Michael Naehrig, USA

Hamed Okhravi, USA

Claudio Orlandi, Denmark

Panos Papadimitratos, Sweden

Thomas Peyrin, Singapore

Bertram Poettering, Germany

Bart Preneel, Belgium

Christian Rechberger, Denmark

Peter Y. Ryan, Luxembourg

Rei Safavi-Naini, Canada

Thomas Schneider, Germany

Ozgur Sinanoglu, UAE

Douglas Stebila, Australia

Thorsten Strufe, Germany

Gang Tan, USA

Vanessa Teague, Australia

Mehdi Tibouchi, Japan

Ivan Visconti, Italy

Wenyuan Xu, USA

Moti Yung, USA

Jianyong Zhou, Singapore

The 14th International Conference on Applied Cryptography and Network Security 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 ACNS 2016 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/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	10 Feb 2016
Notification	27 Mar 2016
Final version	02 Apr 2016



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=acns2016>