

Preface

The Third International Conference on Research in Security Standardization was held at the National Institute for Standards and Technology (NIST), in Gaithersburg, MD, USA, during December 5–6, 2016. This event was the third in what is now an established series of conferences focusing on the theory, technology, and applications of security standards.

SSR 2016 built on the successful SSR 2014 and SSR 2015 conferences, held near London, UK, in December 2014 and in Tokyo, Japan, during December 2015. The proceedings of the 2014 and 2015 conferences were published in volumes 8893 and 9497 of the *Lecture Notes in Computer Science*.

The conference program consisted of two invited talks, 12 contributed papers, and a panel session. We would like to express our special thanks to the distinguished keynote speakers, John Kelsey (NIST, USA) and William Whyte (Security Innovation, USA), who gave very enjoyable and enlightening talks. Special thanks are also due to Salvatore Francomacaro (NIST, USA) who organized the panel session on “Can Security Standards Be Ahead of the Game?,” and to the panel members, who included: Ligu Chen, Eric Hibbard, Russ Housley, and David McGrew.

Out of 18 submissions with authors from nine countries, 12 papers were selected, presented at the conference, and included in these proceedings. The accepted papers cover a range of topics in the field of security standardization research, including hash-based signatures, algorithm agility, secure protocols, access control, secure APIs, payment security, and key distribution.

The success of this event depended critically on the help and hard work of many people, whose help we gratefully acknowledge. First, we heartily thank the Program Committee and the additional reviewers, listed on the following pages, for their careful and thorough reviews. Each paper was reviewed by at least three people, and on average by almost four. A significant time was spent discussing the papers. Thanks must also go to an (anonymous) hard-working shepherd for guidance and helpful advice on improving one of the papers. We also thank the general chair for her excellent organization of the conference, as well as Sara Kerman from NIST for her expert and dedicated assistance in ensuring the success of the conference.

We must also sincerely thank the authors of all submitted papers. We further thank all the authors of papers in this volume for revising their papers in accordance with the various referee suggestions and for returning the source files in good time. The revised versions were not checked by the Program Committee, and so authors bear final responsibility for their contents.

Thanks are due to the staff at Springer for their help with producing the proceedings. We must further thank the developers and maintainers of the EasyChair software, which greatly helped simplify the submission and review processes, as well as the production of these proceedings.

Security Standardisation Research
Third International Conference, SSR 2016,
Gaithersburg, MD, USA, December 5–6, 2016,
Proceedings
Chen, L.; McGrew, D.; Mitchell, C. (Eds.)
2016, IX, 275 p. 64 illus., Softcover
ISBN: 978-3-319-49099-1