

Preface

This volume contains the papers presented at BalkanCryptSec 2014, the first international conference on cryptography and information security in the Balkans, held October 15–16, 2015, in Istanbul, Turkey.

As a result of the Call for Papers, 36 submissions were received from 21 countries. Each submission was reviewed by at least three, and on average 3.8, Program Committee members. After the conference a second round of reviews was held for the revised papers. The committee decided to select 15 papers for the proceedings. The proceedings also include an overview paper authored by one of the invited speakers.

The Program Committee consisted of 51 members representing 22 countries. These members were carefully selected to represent academia and industry, as well as to include world-class experts in various research fields of interest to BalkanCryptSec. The Program Committee was supported by 20 external reviewers.

Additionally, the workshop included four excellent invited talks. Katerina Mitroko-tsa from Chalmers University of Technology discussed her vision of authentication, in a talk entitled “Authentication in Constrained Settings.” Aggelos Kiayias from University of Connecticut, described his research in a talk entitled “Cryptocurrencies: Bitcoin and Beyond.” Benedikt Gierlichs from KU Leuven and iMinds discussed his vision of secure embedded systems in a talk entitled “Embedded Security.” Mariye Umay Akkaya from the Turkish Standards Institution discussed her vision of common criteria in a talk entitled “Crypto Module Standardization (ISO/IEC 1970 and 24759) and Common Criteria.”

We wish to thank everyone who made the conference possible. First and foremost the authors who submitted their papers, the presenters of the accepted papers, and the invited speakers. The hard task of reading, commenting, debating, and finally selecting the papers for the conference fell on the Program Committee members. The Program Committee also used external reviewers, whose names are listed on the following pages, to extend the expertise and ease the burden. We want to express our deepest gratitude to them as well.

We would like to thank the Turkish Standards Institution (TSE) for sponsoring our workshop and specially Mariye Umay Akkaya for her assistance in acquiring this sponsorship.

We would also like to thank the very hard working local Organizing Committee, consisting of nine wonderful research and teaching assistants of the Department of Electronics and Communication Engineering at the Istanbul Technical University: Mehmet Akif Ozkan, Ramazan Yeniceri, Emre Goncu, Ahmet Cagri Bagbaba, Buse Ustaoglu, Busra Tas, Emrah Abtioglu, and Latif Akcay.

Special thanks to the EasyChair team that provided a friendly environment for handling the submissions and creating these proceedings.

The dream of having a cryptography and security conference in the Balkans belongs to Svetla Nikova and Tsonka Baicheva. We deeply thank them for their dream and for their hard work to make it come true. We hope this newborn conference will have a long life.

April 2015

Berna Ors
Bart Preneel

Cryptography and Information Security in the Balkans
First International Conference, BalkanCryptSec 2014,
Istanbul, Turkey, October 16-17, 2014, Revised
Selected Papers
Ors, B.; Preneel, B. (Eds.)
2015, X, 251 p. 43 illus., Softcover
ISBN: 978-3-319-21355-2