International School on Foundations of Security Analysis and Design

The LNCS series entitled *Foundations of Security Analysis and Design* (FOSAD) began on 2001 with the aim of proposing a collection of tutorial papers accompanying lectures given at the FOSAD summer school. This year we present the 7th volume in the series, which is dedicated to FOSAD 2012 and 2013. FOSAD has been one of the foremost educational events established to disseminate knowledge in the area of security for computer systems and networks. Over the years, both the summer school and the book series have represented a reference point for graduate students and young researchers from academia or industry, interested in approaching the field, investigating open problems, and following priority lines of research. The topics covered in this book include model-based security, automatic verification of secure applications, information flow analysis, cryptographic voting systems, encryption in the cloud, and privacy preservation.

The opening paper by Fabrice Bouquet, Fabien Peureux, and Fabrice Ambert presents a survey of model-based approaches for security testing, by discussing existing techniques, the state of the art, and deployment. A specific model-based tool-supported technique is presented in the contribution by Jan Jürjens et al., who describe a dynamic approach to security engineering using UMLsec.

Automatic verification through formal methods is the main topic of the paper by Bruno Blanchet, who introduces the specific case of ProVerif, an automatic protocol verifier that relies on the symbolic model of cryptography, a process algebraic specification language, and resolution- based proof techniques. Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Sergio Maffeis present a tutorial of the Defensive JavaScript language, which is a typed subset of JavaScript with specific security guarantees. In particular, they show how to use it to program secure applications and analyze them automatically through ProVerif. Willem De Groef, Dominique Devriese, Mathy Vanhoef, and Frank Piessens discuss information flow control mechanisms for the security analysis and control of Web scripts. To this aim, they formalize both a static type-system and a dynamic enforcement mechanism. The paper by Gilles Barthe et al. introduces a machine-checked framework, called EasyCrypt, supporting the construction and automated verification of cryptographic systems in the computational model.

David Bernhard and Bogdan Warinschi propose a survey of the main ideas and techniques used in cryptographic voting systems. As a real-world example, they describe the security properties of the Helios voting system. In their paper, Samarati et al. address the issue of protecting sensitive information from uncontrolled access in the cloud. In order to preserve confidentiality and integrity in this setting, they discuss the benefits of data encryption and data fragmentation.

Finally, Ruben Rios, Javier Lopez, and Jorge Cuellar describe location privacy issues in wireless sensor networks, by categorizing solutions and open problems.

We would like to thank all the institutions that have promoted and founded FOSAD in the last few years. We are particularly grateful to the IFIP Working Groups 1.7 on Theoretical Foundations of Security Analysis and Design and 11.14 on Secure Engineering (NESSoS), the ERCIM Working Group in Security and Trust Management (STM), and the EPSRC CryptoForma network.

To conclude, we also wish to thank all the staff of the University Residential Centre of Bertinoro for the organizational and administrative support.

June 2014

Alessandro Aldini
Javier Lopez
Fabio Martinelli

Table of Contents

Foundations of Security Analysis and Design