Preface

About ten years ago, Sjouke Mauw and Erik de Vink established the computer security research group at the Eindhoven University of Technology. Given their background in formal methods, they focused on the formal modeling of security protocols and their properties. The underlying assumption was that reasoning in a relatively simple model, based on well-understood notions from the area of operational semantics, would help to understand the complexities inherent to security protocols. Soon after starting this research, Cas Cremers joined the group and took up the challenge to further develop these ideas for his PhD thesis.

Over the years, we have used the resulting model not only for theoretical research, but also for teaching the fundaments of security protocols to master students. During this time we developed the Scyther tool. The efficient tool support enabled us to quickly prove or disprove hypotheses, and enabled us to apply our approach to practical protocols.

The purpose of this book is threefold. First, it aims to present our approach in such a way that it can be used as an introduction to conducting theoretical research on security protocols. Second, it is designed to serve as a basis for teaching courses on protocol verification. Third, by providing the theoretical foundations underlying our approach, it can aid in practical protocol analysis. We hope that after reading this book, the reader has gained an understanding of the inner workings and possibilities of formal protocol analysis.

This book would have not been possible without the support of many people. First and foremost we express our great appreciation to Erik de Vink. He contributed to the conception and development of many of our technical results and we have greatly benefited from our stimulating discussions.

We are grateful to Jos Baeten and David Basin, who provided us with the opportunity to work on this research topic and the subsequent book for several years. We also express our gratitude to our editor, Ronan Nugent, who patiently provided us with support throughout the writing of this book.

The theory developed in this book and its presentation have undergone many changes over the years. We are grateful to the following people for helping to shape our ideas into their current form: David Basin, Ton van Deursen, Hugo Jonker, Bar-

bara Kordy, Simon Meier, Matthijs Melissen, Marko Horvat, Saša Radomirović, Benedikt Schmidt, and Christoph Sprenger.

Finally, our families provided moral support throughout the writing of this book. Without them, this book would not have seen the light of day.

Zürich, Cas Cremers
Luxembourg Sjouke Mauw

http://www.springer.com/978-3-540-78635-1

Operational Semantics and Verification of Security Protocols

Cremers, C.; Mauw, S.

2012, XIV, 174 p., Hardcover
ISBN: 978-3-540-78635-1