Review of the book *"Formal Correctness of Security Protocols"*
by Giampaolo Bella

Springer, 2007
ISBN: 978-3-540-68134-2

Jannik Pewny

1 What the book is about

As the title says, the book is about formal correctness of security protocols. This means that the protocol itself, attackers and other participants as well as the protocol's goals have to be formalized and modeled. Based on this model, it has to be proven that no attacker can violate the protocol's goals. As in general in modern cryptography, the need of such proofs is recognized, but still this topic exceed the basics of protocol creation and analyzation by far.

The model used in this book is called an inductive model, because it does not per se limit the number of concurrent protocol-runs or exchanged messages, to allow the attacker to try to defeat one of the protocol's goals. The interactive theorem prover is used excessively and all proofs are written to be used with it.

The book begins with a short *Introduction* on what formal proofs are for security protocols, why they are important and how the proofs are noted.
The following chapter called *The Analysis of Security Protocols* lists and shortly describes various other mathematical structures, languages and systems, which could be used for formal approaches, but the book's actual content starts in chapter *The Inductive Model*, where the model used is build-up and explained step by step.

Once the model is defined, the chapter *Verifying the Protocol Goals* explains, what it looks like if a certain goal is met (or not met) in the model. The here described conditions basically determine, if a protocol is secure or not.
Goals are already a nice step towards the formality of security for protocols, but a goal also has to be available to a participant - i.e. a participant has to see, whether a certain goal was met for him. This topic is handled in the chapter *The Principle of Goal Availability.*

The following eight chapters - which form the largest part of the book - alternate between the modeling another protocol feature (e.g. the use of timestamps or the use of smartcards) and using the enhanced model to proof (or disproof) another protocol. The protocols mainly handled are the Kerberos Protocols (Version IV and V), the Shoup-Rubin protocol and the Zhou-Gollmann protocol. Other protocols (like TMN, Woo-Lam, Needham-Schroeder) are sometimes used as simple examples or reference, but the above stated protocols are explained and analyzed much more extensively.

After a short conclusion, which lists some interesting trivia about proof-script-sizes, their runtime and the human effort to create them, the book closes with the (incomplete) proof scripts for various proofs, shown over the whole book, and of course the obligatory bibliography.

2 What the book is like

This book is somewhat like the extended version of the author's PhD thesis. Therefore, it is well lectured, grammatically correct and readable. Despite the fact that the matter is pretty complex, the author manages to write clear, non-irritating and significant sentences.

Each chapter begins with a short motivation for the chapter content, which allows the reader to be prepared for what is ahead. At this point, a series of sub-chapters follows, which cover the chapters topic.

The general problem when analyzing protocols, is that one might lose the bird's eye-view, while concentrating on one of the countless details, e.g. the goal availability of key-authentication of participant C to participant A. This book handles it's topic very well, but because of the diversity of the matter, it is not completely possible to always keep the reader on track. The highly categorized chapters (e.g. sub-chapters for single goals) help a lot, but a large part of the book is filled with proof-script-code-snippets or logic expressions and derivations. Even the very good explanations of them can hardly protect from the variety of details.

One also has to mention the detailed references the author gives during each chapter, as one would expect from a book based on a scientific work.

This book is mainly a textbook. Sometimes, the author gives little tables or sums up in text-form, which goals are met for whom in a certain protocol. But nevertheless, it is hard to find the "essence" and result of the proofs. So the book does not make a good reference or a handbook, but a good teaching book, if you can read it without interruption.

3 Recommendation

This book gives you a good introduction proving the formal correctness of security protocols, including approaches and ideas.

This means that I can not recommend it in general for people, who are seeking for basic information on e.g. the design of security protocols. The book does have an introduction into goals and such, but other books, like Protocols for Authentication and Key Establishment by Boyd/Mathuria, cover that level of information much better.
Also, this book does not teach the use of the main-tool, the theorem prover Isabelle, so a reader will most likely not be able to directly apply the techniques of this book.

On the other hand, this book will perfectly fit your needs if you pick it by it's title. This means, if you already know something about protocol design, security goals and reasoning about the security of protocols. If you have already worked with Isabelle, this will be a benefit. All in all, it is a nice book to read, and the ideas, models and proofs will be of great use for anybody, who specifically looks for formal proofs of security protocols.

The reviewer is a student of IT-Security at Ruhr-University of Bochum (Horst Görtz Institute).