Review of the book

Secure Key Establishment:

by Kim-Kwang Raymond Choo

Springer 2009

ISBN-13: 978-0-387-87968-0

Lakshmi Kuppusamy
Queensland University of Technology

01-06-2010

1 Overview

The main goal of this book is to provide a better understanding of various security models in computational complexity approach. Since these security models play a major role both in designing and analysing cryptographic protocols, it is a prerequisite for every beginner (who is interested in doing research in the particular area) to gain deeper knowledge in these models. Though the contents in all chapters of the book are based on the author's publication, readers may understand better while reading it in the book rather than the publication.

The book also explains the importance of security models and the relation between various security models in computational complexity approach. The security models in computer security approach and their links with the security models in computational complexity approach are discussed. In the second chapter of the book, the author not only explained about hard problems on which most of the cryptographic protocols are based on, but also on the current improvements of that hard problems. This book enable the reader to know the history and current state of the definitions/hard problems.

2 About Contents

This book can be roughly classified into three parts:

Chapters 2-4 First of all, various existing security models of Bellare-Rogaway (BR93, BR95, BR2000) and Canetti-krawczyk(CK2001) are described. The way in which the proof for 3PKD protocol in BR95 model is proven invalid may definitely teach the readers on how to analyse the protocol. The repaired version of 3PKD protocol and its elegant new proof are also explained. Then, few attacks are identified in the protocols due to Bellare-Rogaway and Jeonge *et al.* and the ways in which the protocols could be improved were described. The recommendations for adapting various key sharing requirements (proposed by the author) in the Bellare-Rogaway and Canetti-Krawczyk models are also discussed.

Chapters 5-7 The formal study of the models (BR93, BR95, BR2000 and CK2001) to compare their salient features is provided. The proofs for both equivalence and non-equivalence among the models are intuitively explained by figuring out the key differences between the models. Then the extended version of BR93 model and an attack on revised protocol of Boyd which is found after analysing it with the extended version are well presented. The role of session identifiers in various models are defined. The design and analysis of a new provably secure protocol based on Yahalom protocol is introduced. In several protocols, the errors in their security proof that is based on Bellare-Rogaway model were identified and the possibilities for fixing them were also studied. The observation that certain constructions of session keys may contribute to the security of the key establishment protocol paved way for preventing several attacks on the protocol. The recommendations for constructing session keys is also provided.

Chapters 10-11 The approach of using the communication and adversarial models from the computational proof settings in the machine analysis is introduced. The protocols analysed using this new approach helped to capture few unknown flaws in the protocols used for study. This approach is further extended in both the artificial intelligence and planning problem setting and the extended approach also found useful in detecting a new flaw in the protocol taken for case study.

3 Recommendations

This book provides a good comparison of security models and tools to build secure key establishment protocols. The main advantage of this book is that it shows some techniques to analyse and detect any flaws in the protocol design. Every chapter in this book serves as a preamble to the next chapter as this could be a disadvantage for some readers who would like to skip few chapters in between. For me (a beginner in this area), the flow of this book is perfect and it provides more confidence and deeper knowledge in this area as the chapter proceeds. I would recommend this book for the readers who would like to have a fundamental understanding on the models. The comparison of these models itself provides a clear idea to decide which model would be suitable for specific protocol designs.

4 Conclusion

This book explains both the advantages and disadvantages of the security models in the computational complexity approach. Design considerations for both improving existing models and designing and analysing protocols are proposed. This book would be useful for researchers who want to:

- identify a new attack in an existing protocol,
- design a new protocol, and/or
- provide a security proof for an existing or new protocol.

The reviewer is a Ph.D. student at Queensland University of Technology, Australia.