Review of the book

"Operational Semantics and Verification of Security Protocols"

by Cas Cremers, Sjouke Mauw

Springer Science & Business Media, 2012

ISBN: 9783540786368

Sashank Dara
Cisco Systems Inc

24/12/2014

1 Summary of the review

This book serves as a great resource for any one who wants to do research in Security analysis of protocols. It is written in text book style by authors who have excellent command over the subject. It could be used as self study too as it is self contained and self sufficient. Overall the book does superb justice to the subject in every aspect. This is definitely not a casual read and it is for serious researchers on the subject.

2 Summary of the book

As the authors have mentioned in the preface, the book provides a very good basis for formal theoretical modeling of security protocols, verification and analysis of protocol analysis.

2.1 Chapter 1

The first chapter provides a historical context of the subject. It also briefly and neatly introduces the concept of protocol analysis and how it is different from developing and analyzing cryptographic algorithms itself.

2.2 Chapter 2

This chapter introduces the necessary notation, syntax used in rest of the book.

2.3 Chapter 3

This is an important chapter for the entire book. This introduces all the necessary background needed for understanding what *Operational Semantics* is all about. The notation is tough read for those who are not trained academicians. But the nature of the subject being dealt requires such rigorous definitions and formalism. The concepts like *Security Protocol Specification* , *Protocol Execution* and *Operational Semantics* are established neatly with appropriate examples.

2.4 Chapter 4

This chapter describes the security properties that are expected from the protocols being analyzed. Security Properties are modeled as *Claim Events*. All the security properties like *Secrecy, Authentication, Message Agreement* are well laid and explained with detailed granularity and examples. The chapter concludes with working example of *breaking* and *fixing NS* protocol along with proofs which gives readers a taste of what it is like ensuring security properties in the protocols and proving their *Claims*.

2.5 Chapter 5

This chapter describes algorithms needed for analysis of security protocols. Importantly provides a framework for verifying the security properties by introducing concepts called *Patterns*. The algorithms presented here tries to identify these patterns in the traces of the protocols in order to determine whether a security property being claimed is valid or not. This also introduces the tool *Scyther* and its features.

2.6 Chapter 6

Multi protocol attacks are the surprise package of this book. Usually many of the papers that propose security protocols prove their claims in isolation. But this book emphasizes that protocols proven to be secure in isolation may be prone to attacks due to other protocols in the system, this is an excellent aspect considered from a practical view point. This chapter further describes what these multi protocol attacks are and gives experimental evidence and results of finding such attacks.

2.7 Chapter 7

This protocol generalizes the *NSL* protocol for multi-party authentication. Such generalization is very important and needed especially for proving security claims in multi-party computation protocols. The recent advances in Secure multi-party computation needs such techniques.

2.8 Chapter 8

There are many tools, techniques and methods for proving security of the protocols. It may be quite confusing for readers on what their strengths and short comings are for each of them unless they read this chapter. This chapter nicely summarizes the historical background and further reading.

3 What is the book like (style)?

It is a text book style written for both teachers who teach this subject or as self-study book for students who want to gain expertise in this area. The nature of the book needs rigorous formalism and syntax so practitioners may be find it tough read if they are not trained enough for such formalism.

4 Would you recommend this book?

Yes. I would strongly recommend this book. This is one stop book if you are pursing research in Security analysis of protocols. Even for serious practitioners who are designing protocols and need formal methods to prove their properties this book is a must read.