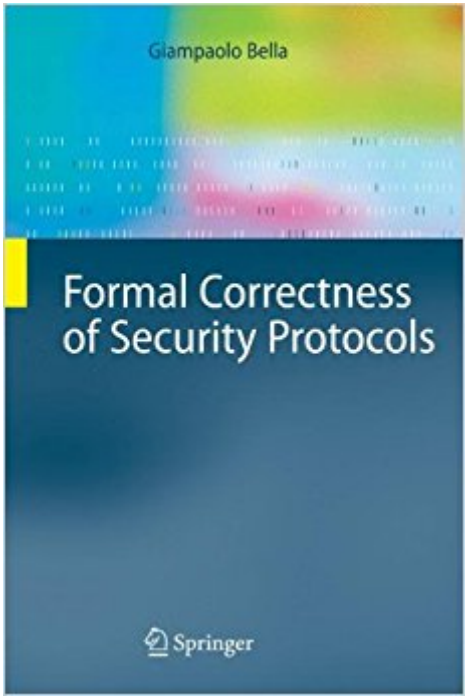
Formal Correctness Of Security Protocols (Information Security And Cryptography)



Synopsis

The author investigates proofs of correctness of realistic security protocols in a formal, intuitive setting. The protocols examined include Kerberos versions, smartcard protocols, non-repudiation protocols, and certified email protocols. The method of analysis turns out to be both powerful and flexible. This research advances significant extensions to the method of analysis, while the findings on the protocols analysed are novel and illuminating.

Book Information

Series: Information Security and Cryptography

Hardcover: 274 pages

Publisher: Springer; 2007 edition (April 4, 2007)

Language: English

ISBN-10: 3540681345

ISBN-13: 978-3540681342

Product Dimensions: 6.1 x 0.7 x 9.2 inches

Shipping Weight: 1.3 pounds (View shipping rates and policies)

Average Customer Review: Be the first to review this item

Best Sellers Rank: #1,544,851 in Books (See Top 100 in Books) #254 inÂ Books > Computers & Technology > Computer Science > AI & Machine Learning > Machine Theory #288 inÂ Books > Computers & Technology > Hardware & DIY > Internet & Networking #341 inÂ Books > Computers & Technology > Certification > CompTIA

Customer Reviews

From the reviews: "This book is about the Inductive Method technique for proving the correctness of security protocols. It is very well suited for the reader who wants to know the state of the art of proving protocol security using the Inductive Method and the interactive theorem prover Isabelle. â | The book could be used as a textbook on the advanced topics in protocol security. It is highly recommended to the newcomer in the field who wants technical information, and to the researcher in the area â | ." (Yongge Wang, Mathematical Reviews, Issue 2008 f) "In summary, my opinion is that this is a great book in the field of computer security, for the practitioner and theoretician alike, since it provides an ideal mixture of theoretical results and applications of them in real protocol analysis scenarios. The book combines, in an ideal way, the features of a rigorous book and a â œcookbookâ •. ... In conclusion, I would strongly recommend this book to people involved in formally proving properties about security protocols as well as students making their first steps in

studying such protocols." (Yannis C. Stamatiou, Univ. of Ioannina, Greece, ACM SIGACT News Book Review 41(1) 2010) â œThe book addresses the software development theorists interested in both modelling and automatic verification of security protocols. â | The present text â | includes a valuable contribution devoted to apply the inductive method for verifying properties of real-world communication protocols. â | The interested computer scientist â | find here valuable hints for future important developments in specifying and verifying secure network communication protocols.â • (Tudor BÄƒlÄƒnescu, Zentralblatt MATH, Vol. 1176, 2010)

Computer network security is critical to fraud prevention and accountability. Network participants are required to observe predefined steps called security protocols, whose proof of correctness is evidence that each protocol step preserves some desired properties. The author investigates proofs of correctness of realistic security protocols in a formal, intuitive setting. The protocols examined include Kerberos versions, smartcard protocols, non-repudiation protocols, and certified email protocols. The method of analysis, the Inductive Method in the theorem prover Isabelle, turns out to be both powerful and flexible. This research advances significant extensions to the method of analysis, while the findings on the protocols analysed are novel and illuminating. This book will benefit researchers and graduate students in the fields of formal methods, information security, inductive methods, and networking.

techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005) ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Cryptography and Network Security: Principles and Practice (7th Edition) Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Looking for Information: A Survey of Research on Information Seeking, Needs, and Behavior: 4th Edition (Studies in Information) Looking for Information: A Survey of Research on Information Seeking, Needs, and Behavior (Studies in Information) Security Risk Management: Building an Information Security Risk Management Program from the Ground Up Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security)