Review of the book

*"Security in Computing Systems"*

by Joachim Biskup

Springer, 2009

ISBN: 978-3-540-78441-8

S. V. Nagaraj
Hadhramout University

2010-03-15

# 1 What the book is about

The book is a monograph on "Security in Computing Systems". It looks at challenges, approaches, and solutions. It is organized into four parts: challenges and basic approaches; fundamentals of information flow and inference control; security mechanisms; and implementations. These parts require cross-referencing for better understanding.

Part One, on "Challenges and Basic Approaches" consists of three chapters.

Chapter 1 (Introduction) offers an introduction to security in computing systems. It discusses the need for security, the fundamental aspects of security, the notions of security, the design cycle for secure computing systems, and the life cycle of such systems.

Chapter 2 (Fundamental Challenges) describes the fundamental challenges in ensuring security in computing systems. Topics such as information flow from senders to receivers, security interests, and tradeoffs are looked at. Security interests include aspects such as availability, integrity, authenticity, nonrepudiation, confidentiality, anonymity, and accountability.

Chapter 3 (Computing Systems and their Basic Vulnerabilities) focuses on computing systems and their basic vulnerabilities. The architecture of such systems and the complexity of computations are studied in this chapter.

Part Two, on "Fundamentals of Information Flow and Inference Control" consists of two chapters.

Chapter 4 (Messages, Inferences, Information and Knowledge) discusses aspects concerning messages, inferences, information and knowledge. Mathematical models and basics of inference control are introduced by this chapter.

Chapter 5 (Preventive Inference Control) looks at inference control for sequential programs, parallel programs, and inference control for various types of systems.

Part Three, on "Security Mechanisms" consists of eleven chapters.

Chapter 6 (Key Ideas and Examples) looks at notions such as redundancy, isolation, and indistinguishability.

Chapter 7 (Combined Techniques) discusses concepts such as identification, proof of authenticity, permissions and prohibitions.

Chapter 8 (Techniques of Control and Monitoring: Essentials) is on the essentials of the techniques of control and monitoring. Topics such as proof of authenticity, access decisions, and monitoring are described.

Chapter 9 (Conceptual Access Rights) studies conceptual models of discretionary approaches, semantics for access decisions, policy algebras, granting and revoking, analysis of control states, privileges and information flow, and conceptual models for mandatory approaches.

Chapter 10 (Elements of a Security Architecture) deals with establishing trust in computing systems, layered design, certificates and credentials, and firewalls.

Chapter 11 (Monitoring and Intrusion Detection) discusses monitoring and intrusion detection. Signature-based and anomaly-based approaches are focused in this chapter.

Chapter 12 (Techniques of Cryptography: Essentials) discusses the essentials of the techniques of cryptography. The basic building blocks of cryptography, probability-theoretic security and complexity-theoretic security are looked at in this chapter.

Chapter 13 (Encryption) attempts a survey and classification. Different types of ciphers such as Vernam ciphers, stream ciphers, and block ciphers (such as those based on RSA, ElGamal, elliptic curves, DES, and IDEA) are described. There is also an introduction to a theory of encryption.

Chapter 14 (Authentication) attempts a survey and classification concerning authentication. Different types of digital signatures are described. There is also an introduction to a theory of authentication.

Chapter 15 (Anonymization) is on anonymity. This chapter looks at blind signatures and unlinkable obligations, superimposed sending, and MIX networks.

Chapter 16 (Some Further Cryptographic Protocols) looks at some cryptographic protocols. Covert commitments, secret sharing, zero-knowledge proofs, and multiparty computations are described.

Part Four, on "Implementations" consists of just one chapter (Chapter 17 Design of Selected Systems) that studies the design of selected systems. The UNIX operating system, the ORACLE/SQL database management system, CORBA middleware, Kerberos, Simple Public Key Infrastructure (SPKI/SDSI), Pretty Good Privacy (PGP) among others are looked at from the security design perspective.

The book has an appendix that covers briefly the following: E-R diagrams, first-order logic, random variables and entropy, number theory, and finite algebras. The book includes a list of references and an index.

## 2 What is the book like (style)?

The author covers a wide range of topics related to security in computing systems. This is a very vast and encyclopedic subject. It is doubtful whether any single book can cover all the topics related to it. There are numerous books available in the market on specialized topics related to securing computing systems. However, many books overlook recent developments or focus only on some topics. This book attempts to cover many facets of present day efforts at securing computing systems. However, even a book of this size needs to be supplemented with other books for better understanding. The author has provided numerous links to the literature in order to facilitate this. A book of this size cannot be understood completely by non-specialists. There are many topics in the book that are actually in the realm of experts. It has to be mentioned that there are numerous textbooks devoted solely to topics

that are just scraped by this book. Examples include firewalls, intrusion detection, cryptography, encryption, authentication, anonymity, and cryptographic protocols among others. It should be remarked that the discussion on intrusion detection in this book is meagre and unsatisfactory. The last part of the monograph has an interesting discussion concerning the security design of selected systems. This is to be welcomed and praised. By looking at the design of selected systems a designer may gain useful insight into the shortcomings of such systems. This could lead to better designs. Only in this part of the book are some real-world systems looked at whereas in other chapters the approach seems to be completely theoretical, dry, prosaic, and stand-alone. The inclusion of some material on hacking and cryptanalysis in the book would have been beneficial.

It should be mentioned that the book is to too voluminous and advanced for non-specialists. Perhaps the author could have attempted a more concise text. Cutting down on empty verbiage and avoiding repetition of some topics or merging common ideas may have resulted in a shorter and more readable monograph.

## 3 Would you recommend this book?

The book tries to focus on the essentials of secure computing and aims to provide a collection of the most promising security mechanisms. To a large extent the book achieves this objective and this is one reason why I recommend this book. The author mentions that the intended audience includes those who are familiar with computer science and engineering and are able to go beyond what is presented in the book besides delving into specialized textbooks. This essentially means that one must have a strong background in various aspects of securing computer systems. I feel this book is best suited only for those specializing in securing computing systems. The author claims that the book presents the fundamentals and leaves more practical details for specific situations to either the experience of the reader or to other texts. This once again calls for discerning expertise from the readers. I feel that students, researchers, designers, and others may also gain useful insight from the security mechanisms discussed in this monograph.

*The reviewer is Head of the Dept. of Computer Science, Faculty of Science, Hadhramout University, Mukalla, Yemen*