Review of the book

"Introduction to Public Key Infrastructures"

by Johannes A. Buchmann, Evangelos Karatsiolis, and Alexander Wiesmaier

Springer 2013

ISBN: 978-3-642-40656-0

S. V. Nagaraj

2015-07-30

1 Summary of the review

The introduction of public key cryptography (PKC) ushered in substantial progress in the field of information security. It enables sharing of confidential information between entities in open networks such as the Internet without the need for previous involvement. It offers mechanisms such as digital signatures that have no analogue in traditional cryptography. In PKC, proper management of the private and public keys is quite indispensable. For example, the private keys must stay private, and the public keys must be verifiably bona fide. In this book, the authors explain the key concepts behind public key infrastructures. They also look at applications, implementations, and relevant standards. The book has ten chapters and an appendix. It includes chapters on public key infrastructures, certificates, trust models, private keys, revocation, validity models, certification service providers, certificate policies, certification paths, and practical aspects of public key infrastructure (PKI). The book is available in hardcover as well as e-book formats. Individual chapters of the e-book may also be purchased online.

2 Summary of the book

The book offers an introduction to public key infrastructures. It has ten chapters and an appendix.

Chapter 1 (The purpose of PKI) introduces concepts such as confidentiality, integrity, entity authentication, data authenticity, and non-repudiation. It also brings in concepts related to cryptography such as secret key encryption, public key encryption, the Rivest Shamir Adleman (RSA) public key cryptosystem and other public key cryptosystems, digital signatures, and the need for PKI.

Chapter 2 (Certificates) introduces the concept of certificates. X.509 certificates and their extensions are described briefly. Other types of certificates such as attribute certificates, card verifiable certificates, Pretty Good Privacy (PGP) certificates, Wireless Access Protocol (WAP) certificates, Simple Public Key Infrastructure (SPKI) certificates, and traceable anonymous certificates are introduced.

Chapter 3 (Trust models) ushers in the concept of trust. Direct trust, Web of trust, hierarchical trust, and ways of combining trust hierarchies are described.

Chapter 4 (Private keys) explains the need for keeping private keys secret. The private key life cycle and personal security environments including those based on software as well as hardware are mentioned.

Chapter 5 (Revocation) explains concepts related to the process of invalidating certificates prior to their expiration. This process is known as revocation. Certificate revocation lists, certificate extensions

related to revocation, the Online Certificate Status Protocol (OCSP), and other revocation mechanisms are explored.

Chapter 6 (Validity models) discusses various validity models for digital signatures. Three important models include the shell model, the chain model, and the modified shell model.

Chapter 7 (Certification service provider) describes the entity that is responsible for certificate life cycle management. This entity is known as the certification service provider. The certificate life cycle, the registration authority, the certification authority, and communication within certificate service providers are looked at in this chapter.

Chapter 8 (Certificate policies) explains the rules followed by the certification service providers. These rules are known as certificate policies. This chapter describes the structure of certificate policies, relevant certificate extensions, and extended validation certificates.

Chapter 9 (Certification paths: retrieval and validation) explains the concept of certification paths. The Lightweight Directory Access Protocol (LDAP), other ways of retrieving certificates, mechanisms for building certification paths and validating such certification paths are elucidated in this chapter. The Server-based Certificate Validation Protocol (SCVP) and relevant certificate extensions are briefly mentioned.

Chapter 10 (PKI in practice) presents applications that utilize the concepts of public key cryptography and PKIs. The Internet, email, code signing, Virtual Private Networks, legally binding electronic signatures, and e-government are studied in this chapter.

There is an appendix on the basic path validation algorithm.

3 What is the book like (style)?

This book is a well written introductory book on public key infrastructures. The authors are experienced information security professionals. Johannes Buchmann is well-known for his work in the field of cryptography. This textbook developed as a result of a course on PKI that was offered by the authors at the Technical University of Darmstadt, Germany. Consequently, the book is well-suited for introductory courses on public key cryptography and public key infrastructure. Every chapter of the book includes exercises to test the understanding of the reader. Solutions to the exercises are also provided at the end of the book. The book will be suitable for self-study by students who are interested in PKI. It will be useful for professionals working or planning to work on PKI projects. The pre-requisites for this book are basic computer science. The book includes numerous pointers to the literature for further study.

4 Would you recommend this book?

This book is very good primer on public key infrastructures. I strongly recommend this book as well as its ebook version for students, researchers, and practitioners.

The reviewer is a Professor of Computer Science and Engg. at VIT University, Chennai campus, India