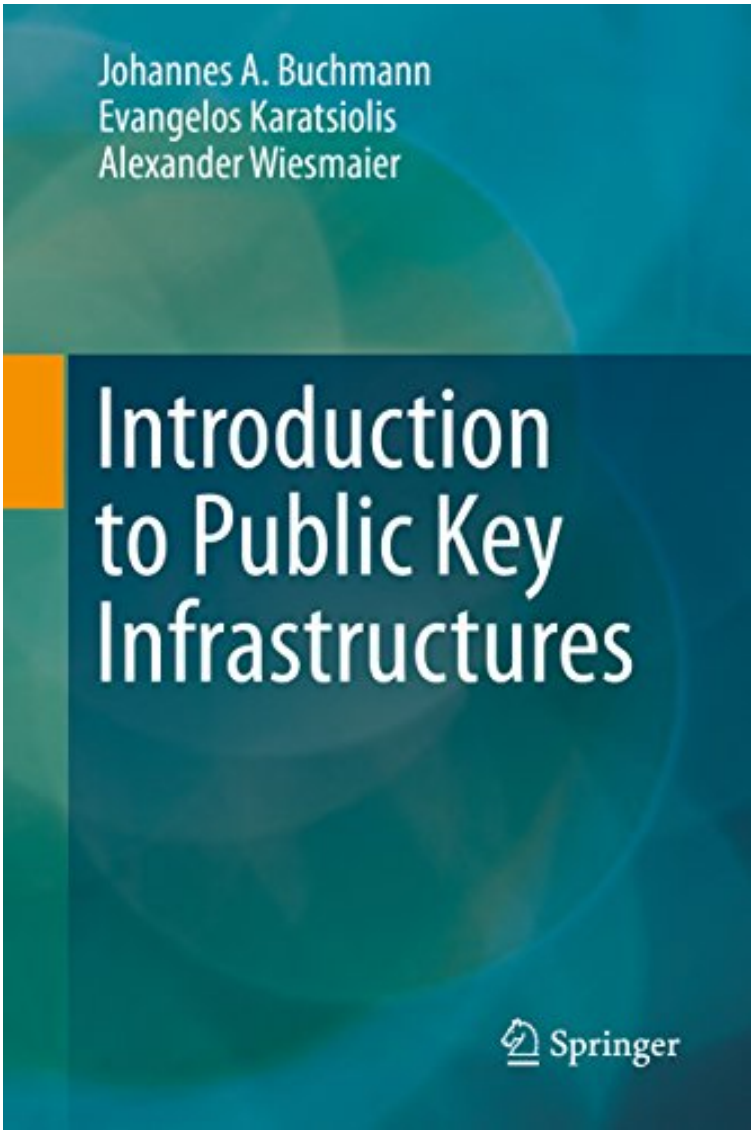
Introduction to Public Key Infrastructures

Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier
*ePub | *DOC | audiobook | ebooks | Download PDF*



#872520 in eBooks 2013-11-19 2013-11-19File Name: B00HWUYFC0 | File size: 23.Mb

Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier : Introduction to Public Key Infrastructures before purchasing it in order to gage whether or not it would be worth my time, and all praised Introduction to Public Key Infrastructures:

1 of 5 people found the following review helpful. it's perfect as anBy Emilio Navarrete Linerosit's perfect as an introduction2 of 7 people found the following review helpful. Buy it and learn it.By Charles M. KentAs a collage professor, I had to obtain a certification in all the subjects I taught, plus a master's degree. PKI was a major arear in the Security+ exam and 70-80% of my computer forensics degree involved PKI. Once learned, network security becomes the mainstay of any network security manager. Unfortunately, most run of the mill network administrators have no

clue as to what this subject covers.

The introduction of public key cryptography (PKC) was a critical advance in IT security. In contrast to symmetric key cryptography, it enables confidential communication between entities in open networks, in particular the Internet, without prior contact. Beyond this PKC also enables protection techniques that have no analogue in traditional cryptography, most importantly digital signatures which for example support Internet security by authenticating software downloads and updates. Although PKC does not require the confidential exchange of secret keys, proper management of the private and public keys used in PKC is still of vital importance: the private keys must remain private, and the public keys must be verifiably authentic. So understanding so-called public key infrastructures (PKIs) that manage key pairs is at least as important as studying the ingenious mathematical ideas underlying PKC. In this book the authors explain the most important concepts underlying PKIs and discuss relevant standards, implementations, and applications. The book is structured into chapters on the motivation for PKI, certificates, trust models, private keys, revocation, validity models, certification service providers, certificate policies, certification paths, and practical aspects of PKI.This is a suitable textbook for advanced undergraduate and graduate courses in computer science, mathematics, engineering, and related disciplines, complementing introductory courses on cryptography. The authors assume only basic computer science prerequisites, and they include exercises in all chapters and solutions in an appendix. They also include detailed pointers to relevant standards and implementation guidelines, so the book is also appropriate for self-study and reference by industrial and academic researchers and practitioners.

From the reviews:ldquo;The layout and chapter exercises make the book suitable for use as a course textbook. hellip; The authors explain the complex workings of public-key cryptography and the infrastructure necessary to support it. The chapters are well illustrated with diagrams and figures. It is not necessary to understand how PKI works to securely use the Internet, but if you do want to understand the minutia of PKI then this book will help.rdquo; (David B. Henderson, Computing s, March, 2014)From the Back CoverThe introduction of public key cryptography (PKC) was a critical advance in IT security. In contrast to symmetric key cryptography, it enables confidential communication between entities in open networks, in particular the Internet, without prior contact. Beyond this PKC also enables protection techniques that have no analogue in traditional cryptography, most importantly digital signatures which for example support Internet security by authenticating software downloads and updates. Although PKC does not require the confidential exchange of secret keys, proper management of the private and public keys used in PKC is still of vital importance: the private keys must remain private, and the public keys must be verifiably authentic. So understanding so-called public key infrastructures (PKIs) that manage key pairs is at least as important as studying the ingenious mathematical ideas underlying PKC.nbsp;In this book the authors explain the most important concepts underlying PKIs and discuss relevant standards, implementations, and applications. The book is structured into chapters on the motivation for PKI, certificates, trust models, private keys, revocation, validity models, certification service providers, certificate policies, certification paths, and practical aspects of PKI.This is a suitable textbook for advanced undergraduate and graduate courses in computer science, mathematics, engineering, and related disciplines, complementing introductory courses on cryptography. The authors assume only basic computer science prerequisites, and they include exercises in all chapters and solutions in an appendix. They also include detailed pointers to relevant standards and implementation guidelines, so the book is also appropriate for self-study and reference by industrial and academic researchers and practitioners.About the AuthorJohannes A. Buchmann received a PhD in Mathematics in 1982. He is a Professor of Computer Science and Mathematics at TU Darmstadt specializing in cryptography and IT security. In 1993 he received the Leibniz Award of the German Science Foundation, the most prestigious science award in Germany. He is a member of the German National Academy of Sciences Leopoldina and the German Academy of Science and Engineering. He is also the author of the Springer Undergraduate Text in Mathematics "Introduction to Cryptography".Evangelos Karatsiolis received a PhD in computer science in 2007. He works as a software engineer at FlexSecure GmbH in Darmstadt, designing and implementing PKI projects. He has lectured on PKI and has served on several program committees in the field of IT security.Alexander Wiesmaier obtained a PhD in computer science in 2008. He works as a Lead Architect and a Senior Researcher at AGT International in Darmstadt. He specializes in critical infrastructure protection and national cyberspace defense. He is a consulting expert for the European Network and Information Security Agency, advising the agency on electronic identities and applied cryptography. He has lectured on IT security and has served on various program committees in the field of IT security.