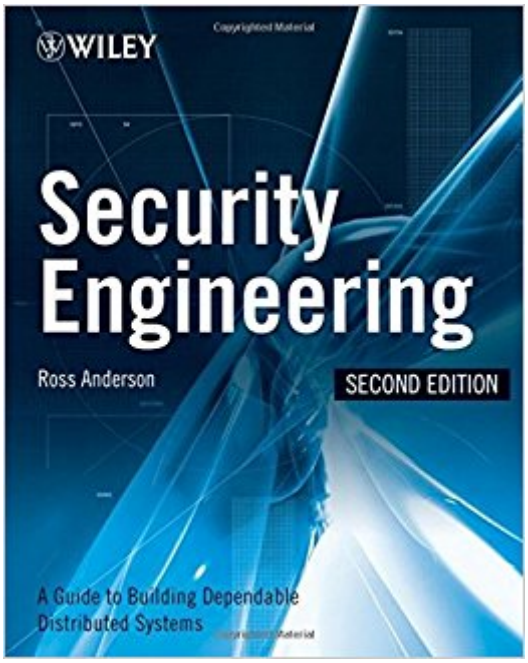
Security Engineering: A Guide To Building Dependable Distributed Systems



Synopsis

The world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here?s straight talk on critical topics such as technical engineering basics, types of attack, specialized protection mechanisms, security psychology, policy, and more.

Book Information

Hardcover: 1080 pages

Publisher: Wiley; 2 edition (April 14, 2008)

Language: English

ISBN-10: 0470068523

ISBN-13: 978-0470068526

Product Dimensions: 7.7 x 2.4 x 9.3 inches

Shipping Weight: 3.9 pounds (View shipping rates and policies)

Average Customer Review: 4.1 out of 5 stars 63 customer reviews

Best Sellers Rank: #80,534 in Books (See Top 100 in Books) #23 inÃ Â Books > Computers & Technology > Certification > CompTIA #24 inÃ Â Books > Textbooks > Computer Science > Algorithms #48 inÃ Â Books > Computers & Technology > Computer Science > Systems Analysis & Design

Customer Reviews

"At over a thousand pages, this is a comprehensive volume." Engineering & Technology Saturday 7 June 2008

"Security engineering is different from any other kind of programming. . . . if you’re even thinking of doing any security engineering, you need to read this book." Ã¢â ¬â • Bruce Schneier "This is the best book on computer security. Buy it, but more importantly, read it and apply it in your work." Ã¢â ¬â • Gary McGraw This book created the discipline of security engineering The world has changed radically since the first edition was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy Ã¢â ¬â • and as they specialize, they get better. New applications, from search to social

networks to electronic voting machines, provide new targets. And terrorism has changed the world. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here’s straight talk about Technical engineering basics Ã¢â ¬â • cryptography, protocols, access controls, and distributed systems Types of attack Ã¢â ¬â • phishing, Web exploits, card fraud, hardware hacks, and electronic warfare Specialized protection mechanisms Ã¢â ¬â • what biometrics, seals, smartcards, alarms, and DRM do, and how they fail Security economics Ã¢â ¬â • why companies build insecure systems, why it’s tough to manage security projects, and how to cope Security psychology Ã¢â ¬â • the privacy dilemma, what makes security too hard to use, and why deception will keep increasing Policy Ã¢â ¬â • why governments waste money on security, why societies are vulnerable to terrorism, and what to do about it

IÃƒÂ¢Ã â ¬Ã â„¢m currently endeavoring on a journey to attain the CISSP-ISSAP (architecture level) security certification.While studying for the CISSP exam I was forced to familiarize myself in many areas of security I had previously skirted ÃƒÂ¢Ã â ¬Ã â œ thus it was grueling work. Few of the CISSP level exam questions require in-depth knowledge; overall the CISSP requires an eye-in-the-sky view of the entire security field, and how different concepts fit together. At the level of the CISSP there are many good resources and it only took me two weeks of study to prep for a passing score.Studying for the CISSP-ISSAP has been more challenging. Not only is the training availability extremely limited, there are few good study resources for the exam. I understand the ISSAP concentration requires detailed knowledge of the inner workings of many technical systems (and not just those normally administered by security professionals). To pass this exam you not only need to retain that knowledge, but know how it all works in minute detail.A long foreword, but the point being stumbling across this book has been a lucky break. Ross dives into security engineering at the street level and comes up for air only to relate real world cases of security failure and how they can be avoided. Not only does he get down to the detail level required on much of the CISSP-ISSAP curriculum, his book is heavily weighted in the technical control fields that are core to the ISSAP exam.If youÃƒÂ¢Ã â ¬Ã â„¢re tasked with engineering security controls in any information system or joining me in studying for the ISSAP concentration I highly recommend this read.This book was published in 2010 making it currently 7 years old. This means there are some glaring exemptions from his review of historical security failures and a bit of weakness in mobile, social and cloud. It should be noted that. Despite being 10 years out of date many of his observations seem eerily prescient given what has occurred during the intervening interval and

although lacking in examples pertaining to Social Mobile Analytics and Cloud ÃƒÂ¢Ã â ¬Ã â œ he accurately predicted the systemic issues encountered in these areas proving good fundamental coverage still useful in 2017.Trailing note. This is 1080 pages - if you’re expecting a casual read look elsewhere, while Ross does an excellent job of keeping this digestible be prepared for some focused attention on every passage.Ross A++

A very lengthy and dense book. It is a good reference book, but a horrible choice to have budding professionals read to learn the basics. But there seems to be no dearth of information in here.

a little old but many of the concepts are still relevant and it is incredibly eye opening. I learned much more about current and historical security problems from this book than I did from books less than a year old.

Those of us in the computer security business have been mining Ross Anderson’s web site for years, since he’s done some really unique and important work in the field. Finally he’s pulled it into an incredible book, one that’s essential for anyone interested in information security.Two elements combine make this book unique: first, the book manages to cover all of the major topics in the field, and second, the book covers the whole range of attacks that systems can face: technical, procedural and physical. Historically, writers on information security have focused on computers and disembodied "users," downplaying the crucial issues of physical security, perimeters, operating procedures, and the limits of human behavior. This book tries to integrate such concerns into information security thinking, instead of treating them as "special concerns that computer geeks don’t really care about."Best of all, the book is a great read. Ross has a fine way of drawing out the irony we encounter in user behavior, enterprise behavior, and even in the actions of presumed authorities in industry and government. At one point he discusses a government endorsed security evaluation process "which, as mentioned, is sufficient to keep out all attackers but the competent ones."Ross unabashedly explains several aspects of information security that most writers ignore entirely, like security printing, seals, tamper resistance, and associated procedures. In my own books, reviewers have chided me for including such "irrelevant" topics, even though they play an essential part in making a real system work. As Ross ably points out, most successful attacks these days are pretty mundane and don’t involve cryptanalysis or sophisticated protocol hacking. ATM fraud, for example, often relies on pre-computer technology like binoculars to pick up a victim’s PIN. This book should open a lot of peoples’ eyes.

It goes very deep into the heart of security with many technical examples and real world security issues that companies have faced in the past as well as how they were resolved.

Certainly a top 5 in its space. Especially notable for its broad coverage and excellent references to other more detailed material. This is a very worthwhile update from the first edition (which is freely available from the author's web site as a PDF).

Required for my MS but still a very good/informative read. However. like most books similar to this it can get a bit dry.

I have just started a course in Security Engineering with the recommended Security Engineering Textbook which I am reviewing. I found the text simple to understand, full of examples that illustrate concepts and I think I enjoy using it.

Biochemical Engineering/Biotechnology) (v. 1) Building the Empire State Building: An Interactive Engineering Adventure (You Choose: Engineering Marvels) ISO/IEC 27001:2013, Second Edition: Information technology - Security techniques - Information security management systems - Requirements Security Risk Management: Building an Information Security Risk Management Program from the Ground Up Hacking: Basic Security, Penetration Testing and How to Hack (hacking, how to hack, penetration testing, basic security, arduino, python, engineering Book 1) Crowdsourcing: Uber, Airbnb, Kickstarter, & the Distributed Economy Innovation and Disruption at the GridÃ¢â ¬â„¢s Edge: How distributed energy resources are disrupting the utility business model