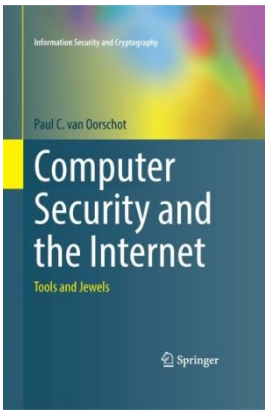
Computer Security and the Internet

Tools and Jewels



Paul C. van Oorschot [Carleton University]

Publ. 03/2020, 390 pp., ISBN 978-3-030-33648-6

Information Security & Cryptography Book Series

Foreword by Peter G. Neumann

Table of Contents

Overview

This book provides a concise yet comprehensive overview of computer and Internet security, suitable for a one-term introductory course for junior/senior undergrad or first-year graduate students. It is also suitable for self-study by anyone seeking a solid footing in security – including software developers and computing professionals, technical managers and government staff. An overriding focus is on brevity, without sacrificing breadth of core topics or technical detail within them. The aim is to enable a broad understanding in roughly 350 pages. Further prioritization is supported by designating as optional selected content within this. Fundamental academic concepts are reinforced by specifics and examples, and related to applied problems and real-world incidents.

The first chapter provides a gentle overview and 20 design principles for security. The ten chapters that follow provide a framework for understanding computer and Internet security. They regularly refer back to the principles, with supporting examples. These principles are the conceptual counterparts of security-related error patterns that have been recurring in software and system designs for over 50 years.

The book is “elementary” in that it assumes no background in security, but unlike “soft” high-level texts it does not avoid low-level details, instead it selectively dives into fine points for exemplary topics to concretely illustrate concepts and principles. The book is rigorous in the sense of being technically sound, but avoids both mathematical proofs and lengthy source-code examples that typically make books inaccessible to general audiences. Knowledge of elementary operating system and networking concepts is helpful, but review sections summarize the essential background. For graduate students, inline exercises and supplemental references provided in per-chapter endnotes provide a bridge to further topics and a springboard to the research literature; for those in industry and government, pointers are provided to helpful surveys and relevant standards, e.g., documents from the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology.

Comments

“Extremely clear and well-organized. The best introduction to the field.”

[Cormac Herley, Microsoft Research]

Comments (contd.)

"The book makes considerable headway into underlying realities that otherwise tend to make things difficult to understand, to design, and to implement correctly. Also, much of what is described here is well chosen, because it has survived the test of time … Understanding everything in this book is an essential precursor to achieving meaningfully trustworthy systems … Paul's realistic approach and structural organization in this book are likely to provide a very useful early step – particularly for students and emerging practitioners, but also for computer users interested in a better understanding of what attaining security might entail."

[Peter G. Neumann, SRI International]

"This is THE textbook we've been waiting for when redesigning our introductory computer security course! Well-balanced emphasis on the right issues, getting to the bone where necessary. Paul's book filled in the gap we identified quite some time ago."

[Vashek Matyáš, Masaryk University]

"This book's combination of grounding and theory addresses an important gap, and will serve new students well!"

[Adam Shostack, author of "Threat Modeling: Designing for Security"]

"Paul's book does an amazing job of distilling the chaotic panoply of the security world into a remarkably coherent, principled, and (crucially) accessible form. It's a wonderful gift to the security field, especially those tasked with teaching security to up-and-coming developers, engineers, and researchers. I'm excited to already be using it in my class."

[Bryan Parno, Carnegie Mellon University]

"The only book I could previously recommend as a textbook for introductory security classes was published in 2002 and outdated in multiple ways. I have been looking for a new textbook for years, but I could not find a book that covered the topics I was going to cover. [This] book, not long, yet remarkably comprehensive, put an end to my search."

[Kemal Bıçakcı, TOBB University of Economics and Technology]

"I have been teaching Computer Security for 25 years, and I have finally found the perfect text for my computer security course! Paul Van Oorschot has once again written a game changing book. His previous work, the Handbook of Applied Cryptography in 1997 was my go-to reference for anything crypto related. In this book he has done for applied network security what he previously accomplished for cryptography. This is an accessible, must have book that can serve as a textbook for an introductory college course, or as the perfect read for anyone wanting to master Internet security."

[Avi Rubin, Johns Hopkins University]

"This book is a fantastic introduction to computer and Internet security concepts. Not only is it accessible to those new to the field, but it also manages to present a thorough treatment of the subject matter complete with rich real-world examples and helpful exercises. As a security practitioner, I consider this book not only suitable as a trusted reference in an academic setting but also for those actually working in the computer security field. In fact, this text has quickly become an essential (and well used) part of my team's reference material."

[David Whyte, Cyber Resilience Coordination Centre, Bank for International Settlements]

"This book is perfect for my foundational security course. Its relatively short length (which makes it appropriate for a one semester course) is misleading – the book is rich with material, presented in a manner such that every word counts. It is sufficiently comprehensive to be used as a reference, yet clear enough to be used as a teaching text. Protocols, practices, and concepts are not just presented, but also motivated, often with historical background. I will be using it, and my students will have a much more comprehensive understanding of security because of it."

[Douglas Szajda, University of Richmond, Virginia]