Book Review by Edgar Weippl (University of Vienna), August 2021
Computer Security and the Internet: Tools and Jewels (Springer, 2020-2022)
author: Paul C. van Oorschot (Carleton University, Canada)

What sets this book apart from other books is that it covers not only the fundamentals but also timely and relatively new concepts that have become important in the last years. Moreover, there are no outdated parts as some other "established" textbooks have. Pointing out what seems obvious, is, however, relevant for adopting this book as a textbook for courses. In many other textbooks there are outdated parts where I had to tell students to interpret these parts as "history lessons" and not as contemporary information. There are still textbooks that describe DES or MD5 as secure or talk about air gaps as being an almost 100% barrier for malware.

A second thing I like about the book is that Chapter 1 starts with security goals and requirements and continues with risk analysis. Only then it covers security mechanisms or building blocks such as cryptography (Chapter 2) or user authentication (Chapter 3). Authors of so many other books seem so eager to explain technical fundamentals that the initial chapters often cover those topics before actually explaining that the logical first step is always a risk assessment – covered in this book on page 6.

In an increasingly networked world, authentication protocols and key establishment (Chapter 4) are extremely relevant as almost all systems – such as on a modern car – are themselves a networked system and proper authentication of communication parties is a prerequisite for access control (Chapter 5).

In Chapter 6 (Software Security) the author not only explains the usual buffer overflows and missing input validation but provides a good starting point on the idea of return-oriented-programming and explains return-to-libc exploits in a quite detailed way – at least for an introductory book. Having understood the basics of systems security, the reader can now understand better how modern malware (Chapter 7) works.

The final chapters (8-11) in the book's first edition cover network security (PKI, web security, IDS/IPS and firewalls). The second edition of the book slightly updates the first eleven chapters, and two new chapters were added: security in wireless networking (Chapter 12) and Blockchain (Chapter 13). Chapter 13 builds on the basics covered in the previous chapters and gives comparatively many details on how, for instance, Bitcoin works. This last chapter nicely shows how basic security building blocks are used in modern systems and gives readers some of the necessary knowledge to understand the many new papers published in the domain of security/privacy in distributed ledger technologies.

The book is provided as hardcover and as DRM-free PDF directly from Springer. As DRM makes access to the book for the honest buyer more difficult, I strongly support publishing (and purchasing) DRM-free versions. The author also offers a free download of a PDF version on a website.

I can recommend using this book for teaching introductory and intermediate classes in computer security. In particular, the freely and legally available version makes it a good choice for students.