Book Review by N. Asokan (UWaterloo and Aalto U, Helsinki)
*Computer Security and the Internet – Tools and Jewels* (first edition, Springer 2020)

**★★★★★ A modern textbook for computer security**
Reviewed in Canada on December 12, 2020

I was sent an instructor's copy for this book earlier this year. Even before that, I had started looking through the chapters made available through the author's webpage. There have been a couple of standard computer security textbooks that are widely used in undergrad computer security courses around the world. None has been entirely satisfactory (some include material that is outright incorrect). So it was refreshing to see a textbook written by a well-known academic known for his contributions to information security. The book does not disappoint!

In 11 chapters, it covers most of the material that one would expect in a first university-level textbook on computer security. Right from the beginning, it becomes clear that the book is a modern treatment of the subject. For example, chapter 1 identifies four fundamental goals of security, including "authorization" to the traditional list of confidentiality, integrity, and availability. Similarly, chapter 1 also identifies a set of design principles for computer security (which are referred back to frequently in subsequent chapters). This list is an extended and updated version of Saltzer and Schroeder's classic 45-year old list of principles for the "protection of information in computer systems".

Two aspects about this book sets it apart from all previous "traditional" computer security textbooks:

First, the careful, deliberate effort at systematization and exposition. The author presents a clear but concise typesetting convention at the beginning (using different font styles and colours) so that the nature of terms are visually salient (e.g., technical terms vs. names of systems vs. security principles, etc.). The rest of the textbook painstakingly adheres to this convention. This is of immense pedagogical value.

Second, topics are presented not only by explaining them but also setting them in the context of a bigger picture and providing ample notes and pointers for further reading on state-of-the-art research for the interested reader. This is not typical in other textbooks written by career academics or professional textbook authors. Dr. van Oorschot is not only a leading computer security academic (hence well-versed in current research) but also has a wealth of experience in industry (hence the effort to explain concepts in real-world context, rather than as dry academic topics). For example, in the chapter on Software Security (Chapter 6, which I used in my computer security course this year), the basic software security topics are covered first (integer-based vulnerabilities, buffer overflows, race conditions etc.), followed by explaining essential background context (e.g., what are the challenges for the attacker in crafting effective shellcode) and pointers to further reading which covers almost till the frontier of state-of-the-art research (e.g., return-oriented programming and data-oriented attacks are not yet covered but pretty much everything leading up to them are).

Overall, this textbook is significantly better than the traditional computer security textbooks. Instructors teaching traditionally structured first courses in computer security will therefore be better off using this book instead. The only major gap in this book (from the perspective of the course I teach: computer security and privacy) is that privacy is not adequately covered. I hope a chapter on privacy, including technical as well as regulatory aspects (which have been emerging in many jurisdictions) will be added in the next edition.

This review is available via the link: https://twitter.com/nasokan/status/1341414957573939203
which then points to: https://www.amazon.ca/Computer-Security-Internet-Tools-Jewels/dp/3030336484