Information Security and Cryptography

Paul C. van Oorschot

Computer Security and the Internet

Tools and Jewels

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 300 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 aim to 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, 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.

ISSN 1619-7100

ISBN 978-3-030-33648-6

springer.com

van Oorschot

Computer Security and the Internet

Information Security and Cryptography

Paul C. van Oorschot

Computer Security and the Internet

Tools and Jewels

Springer