Now updated—your expert guide to twenty-first century information security

Information security is a rapidly evolving field. As businesses and consumers become increasingly dependent on complex multinational information systems, it is more imperative than ever to protect the confidentiality and integrity of data. Featuring a wide array of new information on the most current security issues, this fully updated and revised edition of Information Security: Principles and Practice provides the skills and knowledge readers need to tackle any information security challenge.

Taking a practical approach to information security by focusing on real-world examples, this book is organized around four major themes:

- **Cryptography**: classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers, information hiding, and cryptanalysis

- **Access control**: authentication and authorization, password-based security, ACLs and capabilities, multilevel security and compartments, covert channels and inference control, security models such as BLP and Biba's model, firewalls, and intrusion detection systems

- **Protocols**: simple authentication protocols, session keys, perfect forward secrecy, timestamps, SSH, SSL, IPSec, Kerberos, WEP, and GSM
• **Software**: flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering, digital rights management, secure software development, and operating systems security

This Second Edition features new discussions of relevant security topics such as the SSH and WEP protocols, practical RSA timing attacks, botnets, and security certification. New background material has been added, including a section on the Enigma cipher and coverage of the classic "orange book" view of security. Also featured are a greatly expanded and upgraded set of homework problems and many new figures, tables, and graphs to illustrate and clarify complex topics and problems. A comprehensive solutions manual is available to assist in course development.

Minimizing theory while providing clear, accessible content, Information Security remains the premier text for students and instructors in information technology, computer science, and engineering, as well as for professionals working in these fields.

---

**ABOUT THE AUTHOR**

**MARK STAMP, P HD**, is Professor of Computer Science at San José State University, where he teaches undergraduate and graduate-level information security courses. In addition to his experience gained in private industry and academia, Dr. Stamp has seven years' experience working as a cryptanalyst at the U.S. National Security Agency. He has written dozens of academic papers and two books on the topic of information security.

---

**NEW TO EDITION**

2nd edition features:

• A greatly expanded set of homework problems

• An appendix which covers necessary background information, like networking basics

• A solutions manual and a comprehensive set of classroom-tested PowerPoint slides to assist instructors and students

• Many completely new figures, tables, and graphs to illustrate and clarify complex topics and problems
FEATURES

2nd edition features:

• A greatly expanded set of homework problems

• An appendix which covers necessary background information, like networking basics

• A solutions manual and a comprehensive set of classroom-tested PowerPoint slides to assist instructors and students

• Many completely new figures, tables, and graphs to illustrate and clarify complex topics and problems

For additional product details, please visit https://www.wiley.com/en-us