INFORMATION SECURITY

INFORMATION SECURITY

Principles and Practice

Second Edition

Mark Stamp
San Jose State University
San Jose, CA

WILEY

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Stamp, Mark.
Information security: principles and practice / Mark Stamp. — 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-62639-9 (hardback)
1. Computer security. I. Title.
QA76.9.A25S69 2011
005.8—dc22 2010045221

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

To Miles, Austin, and Melody, with love.

Contents

Preface

Please sir or madam won't you read my book?
It took me years to write, won't you take a look?
— Lennon and McCartney

I hate black boxes. One of my goals in writing this book was to illuminate some of those black boxes that are so popular in information security books today. On the other hand, I don't want to bore you to death with trivial details (if that's what you want, go read some RFCs). As a result, I often ignore details that I deem irrelevant to the topic at hand. You can judge whether I've struck the proper balance between these two competing goals.

I've strived to keep the presentation moving along so as to cover a broad selection of topics. My goal is to cover each item in just enough detail so that you can appreciate the basic security issue at hand, while not getting bogged down in details. I've also attempted to regularly emphasize and reiterate the main points so that crucial information doesn't slip by below the radar screen.

Another goal of mine was to present the topic in a reasonably lively and interesting way. If any computing subject should be exciting and fun, it's information security. Security is happening now and it's in the news—it's clearly alive and kicking.

I've also tried to inject a little humor into the material. They say that humor is derived from pain, so judging by the quality of my jokes, I'd say that I've led a charmed life. In any case, most of the really bad jokes are in footnotes so they shouldn't be too distracting.

Some security textbooks offer a large dollop of dry useless theory. Reading one of those books is about as exciting as reading a calculus textbook. Other books offer a seemingly random collection of apparently unrelated facts, giving the impression that security is not really a coherent subject at all. Then there are books that present the topic as a collection of high-level managerial platitudes. Finally, some texts focus on the human factors in security. While all of these approaches have their place, I believe that, first and foremost, a

security engineer must have a solid understanding of the inherent strengths and weaknesses of the underlying technology.

Information security is a huge topic, and unlike more established fields, it's not clear what material should be included in a book like this, or how best to organize it. I've chosen to organize this book around the following four major themes:

- Cryptography
- Access Control
- Protocols
- Software

In my usage, these themes are fairly elastic. For example, under the heading of access control I've included the traditional topics of authentication and authorization, along with such nontraditional topics as firewalls and CAPTCHAs. The software theme is particularly flexible, and includes such diverse topics as secure software development, malware, software reverse engineering, and operating systems.

Although this book is focused on practical issues, I've tried to cover enough of the fundamental principles so that you will be prepared for further study in the field. In addition, I've strived to minimize the background requirements as much as possible. In particular, the mathematical formalism has been kept to a bare minimum (the Appendix contains a review of all necessary math topics). Despite this self-imposed limitation, I believe this book contains more substantive cryptography than most security books out there. The required computer science background is also minimal—an introductory computer organization course (or comparable experience) is more than sufficient. Some programming experience is assumed and a rudimentary knowledge of assembly language would be helpful in a couple of sections, but it's not mandatory. Networking basics arise in a few sections. The Appendix contains a brief overview of networking that provides more than sufficient background material.

If you are an information technology professional who's trying to learn more about security, I would suggest that you read the entire book. However, if you want to avoid the material that's most likely to slow you down and is not critical to the overall flow of the book, you can safely skip Section 4.5, all of Chapter 6 (although Section 6.6 is highly recommended), and Section 8.4.

If you are teaching a security class, you need to realize that this book has more material than can be covered in a one-semester course. The schedule that I generally follow in my undergraduate security class appears in Table 1. This schedule allows ample time to cover a few of the optional topics.

If the syllabus in Table 1 is too busy, you could cut Section 8.9 of Chapter 8 and some of the topics in Chapters 12 and 13. Of course, many other variations on the syllabus are possible.

Chapter	Hours	Comments
1. Introduction	1	All
2. Classic Cryptography	3	All
3. Symmetric Key Crypto	4	Omit Section 3.3.5
4. Public Key Crypto	4	Omit Section 4.5
5. Hash Functions++	3	Omit 5.6
		Omit attack details in 5.7
		Omit Section 5.9.1
6. Advanced Cryptanalysis	0	Omit entire chapter
7. Authentication	4	All
8. Authorization	2	Omit 8.4.1 and 8.4.2
		Omit 8.10
9. Authentication Protocols	4	Omit 9.4
10. Real-World Protocols	4	Omit either WEP or GSM
11. Software Flaws and Malware	4	All
12. Insecurity in Software	4	Omit 12.3
13. OS and Security	3	All, time permitting
Total	40	

Table 1: Suggested Syllabus

Security is not a spectator sport—doing a large number of homework problems is essential to learning the material in this book. Many topics are fleshed out in the problems and additional topics are often introduced. The bottom line is that the more problems you solve, the more you'll learn.

A security course based on this book is an ideal venue for individual or group projects. Chapter 6 is a good source for crypto projects, while the annotated bibliography provides a starting point to search for additional project topics. In addition, many homework problems lend themselves well to class discussions or in-class assignments (see, for example, Problem 19 in Chapter 10 or Problem 33 in Chapter 11).

The textbook website is at

`http://www.cs.sjsu.edu/~stamp/infosec/`

where you'll find PowerPoint slides, all of the files mentioned in the homework problems, errata, and so on. If I were teaching this class for the first time, I would particularly appreciate the PowerPoint slides, which have been thoroughly "battle tested" and improved over several iterations. In addition, a solutions manual is available to instructors (sorry, students) from the publisher.

It is also worth noting how the Appendices fit in. Appendix A-1, Network Security Basics, is relevant to Sections 8.9 and 8.10 of Chapter 8 and also for

all of Part III. Even if students have a solid foundation in networking, it's probably worthwhile to review this material, since networking terminology is not always consistent and the focus here is on security.

The Math Essentials of Appendix A-2 are assumed in various places throughout the text. Elementary modular arithmetic (Appendix A-2.2) arises in a few sections of Chapter 3 and Chapter 5, while some of the relatively advanced concepts are required in Chapter 4 and Section 9.5 of Chapter 9. I've found that the vast majority of my students need to brush up on modular arithmetic basics. It only takes about 20 to 30 minutes of class time to cover the material on modular arithmetic and that will be time well spent prior to diving into public key cryptography. Trust me.

Permutations, which are briefly discussed in Appendix A-2.3, are most prominent in Chapter 3, while elementary discrete probability (Appendix A-2.4) appears in several places. The elementary linear algebra in Appendix A-2.5 is only required in Section 6.5.

Just as any large and complex piece of software must have bugs, this book inevitably has errors. I would like to hear about any errors—large or small—that you find. I will maintain a reasonably up-to-date errata on the textbook website. Also, don't hesitate to provide any suggestions you might have for future editions of this book.

What's New for the Second Edition?

Cats right themselves; books don't.
— John Aycock

One major change for this second edition is that the number and quality of the homework problems have both greatly increased. In addition to the new-and-improved homework problems, new topics have been added, some new background material has been included, virtually all of the existing material has been updated and clarified, and all known errors have been corrected. Examples of new topics include a practical RSA timing attack, a discussion of botnets, and coverage of security certification. Examples of added background material include a section on the Enigma cipher and coverage of the classic "orange book" view of security.

Information security is a rapidly evolving field and there have been some significant changes since the first edition of this book was published in 2005. Nevertheless, the basic structure of the book remains intact. I believe the organization and list of topics has held up well over the past five years. Consequently, the changes to the content for this second edition are more evolutionary than revolutionary.

Mark Stamp
San Jose State University

About The Author

I've got nearly 20 years of experience in information security, including extensive work in industry and government. My work experience includes more than seven years at the National Security Agency followed by two years at a Silicon Valley startup company. While I can't say too much about my work at NSA, I can tell you that my job title was Cryptologic Mathematician. In industry I helped design and develop a digital rights management security product. This real-world work was sandwiched between academic jobs. While in academia, my research interests have included a wide variety of security topics.

When I returned to academia in 2002, it seemed to me that none of the available security textbooks had much connection with the real world. I felt that I could write an information security book that would fill this gap, while also containing information that would be useful to working IT professionals. Based on the feedback I've received, the first edition was apparently a success.

I believe that this second edition will prove even more valuable in its dual role as a textbook and as a resource for working professionals, but then I'm biased. I can say that many of my former students who are now at leading Silicon Valley technology companies tell me that the information they learned in my courses has been useful to them. And I certainly wish that a book like this had been available when I worked in industry, since my colleagues and I would have benefitted from it.

I do have a life outside of information security.[1] My family includes my wife, Melody, and two wonderful sons, Austin (whose initials are AES), and Miles (whose initials are not DES, thanks to Melody). We enjoy the outdoors, with regular local trips involving such activities as bicycling, hiking, camping, and fishing. I also spend way too much time working on my fixer-upper house in the Santa Cruz mountains.

[1] Well, sort of...

Acknowledgments

My work in information security began when I was in graduate school. I want to thank my thesis advisor, Clyde F. Martin, for introducing me to this fascinating subject.

In my seven years at NSA, I learned more about security than I could have learned in a lifetime anywhere else. From my time in industry, I want to thank Joe Pasqua and Paul Clarke for giving me the chance to work on a fascinating and challenging project.

The following San Jose State University students helped greatly with the first edition: Fiona Wong, Martina Simova, Deepali Holankar, Xufen Gao, Subha Rajagopalan, Neerja Bhatnager, Amit Mathur, Ali Hushyar, Smita Thaker, Puneet Mishra, Jianning Yang, Konstantin Skachkov, Jian Dai, Thomas Nikl, Ikai Lan, Thu Nguyen, Samuel Reed, Yue Wang, David Stillion, Edward Yin, and Randy Fort.

Richard Low, a colleague here at SJSU, provided helpful feedback on an early version of the manuscript. David Blockus (God rest his soul) deserves special mention for providing detailed comments on each chapter at a particularly critical juncture in the writing of the first edition.

For this second edition, many of my SJSU masters students "volunteered" to serve as proofreaders. The following students all contributed their time and energy to correct errors in the manuscript: Naidele Manjunath, Mausami Mungale, Deepti Kundu, Jianrui (Louis) Zhang, Abhishek Shah, Sushant Priyadarshi, Mahim Patel, Lin Huang, Eilbroun Benjamin, Neha Samant, Rashmi Muralidhar, Kenny Zhang, Jyotsna Krishnaswamy, Ronak Shah, Gauri Gokhale, Arnold Suvatne, Ashish Sharma, Ankit Patel, Annie Hii, Namrata Buddhadev, Sujandharan Venkatachalam, and Sathya Anandan. In addition, Piyush Upadhyay found several errors in the first edition.

Many other people made helpful comments and suggestions. Here, I would like to specifically thank Bob Harris (Penn State University) for the visual crypto example and exercise, and a very special thanks goes to John Trono (Saint Michael's College) for his many detailed comments and questions.

Undoubtedly, errors remain. Of course, all remaining flaws are my responsibility alone.