Preface

Over the past decades, information security has emerged from being a specialist topic studied primarily by military cryptographers to being a general subject area relevant for every professional who wishes to better understand, develop, or use modern information and communication systems. Most courses on information security emphasize theory and basic concepts: cryptography, algorithms, protocols, models and selected applications. This is essential in providing the reader with a basic understanding of the subject. But information security is ultimately about getting your hands dirty and putting these ideas to work. That is where this book comes in.

Our goal in writing this book is to provide a hands-on experimental counterpart to the more theoretically-oriented textbooks available. We approach information security from the perspective of a laboratory where students carry out experiments, much like they do in other courses such as physics or chemistry. Our aim is to help students better understand the theory they have learned by putting it directly to use and seeing first-hand the practical consequences and the subtleties involved. Just like with other lab courses, this book is not intended to be a replacement for a theory course and associated textbooks; it is complementary and has the aim of building on and extending the students' knowledge.

This book arose out of a lab course held at ETH Zurich, starting in 2003 and still held today. The course's goal is exactly that stated above: to provide a counterpart to the more theoretical courses offered in information security at ETH Zurich. Students taking this course receive this book together with software containing three networked virtual machines, running in a virtual environment. The book confronts the reader with problems related to different topics in information security, and the software allows them to carry out experiments and apply the concepts they have previously learned.

The main focus of this book is on the security of networks, operating systems, and web applications. Each of these topics is vast and could be the subject of its own book. We restrict our attention to central security questions in each of these areas, for example, well-established topics like authentication and access control, logging, typical web application vulnerabilities, and certificates. This fits well with

our intention of having the laboratory complement a more theoretically-oriented course in information security.

This book goes hand-in-hand with software. The software is distributed on the Internet and can be downloaded from www.appliedinfsec.ch. By using virtualization, the course software is completely self-contained. The software runs on most operating systems — including Windows, Linux, Macintosh and OpenSolaris — supporting VirtualBox, which is a freely available virtualization environment for x86 and AMD64/Intel64 platforms.

How to use this book

This book can be used in either of two ways. First, it can be used for self-study. When we teach this course at ETH Zurich, the students work independently through all of the chapters, answering the given questions. Those students who have taken a first course in information security and have experience working with some Unix derivative can complete most of the exercises on their own. To make the book suitable for self-study, we have included answers to the questions in an appendix.

Second, the book can be used as part of a laboratory course at a university or within industry. For the course we hold at ETH Zurich, we supplement the laboratory exercises with a project. During the project, the students work in groups of up to four students. Their task is to develop a complete system in accordance with a given specification. The system must be delivered as a set of virtual machines running under VirtualBox. Towards the end of the course the virtual machines are distributed among the groups of students, and each system is reviewed by a different group. The overall grade awarded for the course is based on the grade given for the project and the grade achieved in a final examination.

In either usage, the chapters are best read in the order presented. Chapter 1 provides background on the basic security principles that are used throughout the book. Chapter 2 introduces the VirtualBox environment, which is needed for the exercises. Afterwards, come two mostly independent parts: Chaps. 3–5 are on network and operating system security, and Chaps. 6–7 are on web application security and certificates. There is some overlap, however, as applications use network services and run on operating systems; hence we recommend covering both parts in the order presented.

The book's final chapter is on risk analysis. This chapter is independent of the other chapters and is of a different flavor. It describes a general procedure for analyzing the security of entire systems, i.e., analyzing the whole rather than just the individual parts. For self-study, this section can be omitted. However, it is essential for those readers carrying out the project and it is an important topic in its own right.

The book has four appendices. Appendices A–B give a detailed example of a possible project, which we have successfully used at ETH Zurich. Appendix C provides a brief overview of Linux and various utility programs that are useful for the exercises and the project. The material in this appendix is elementary, but our expe-

rience is that it is helpful for readers with limited prior experience using Linux-like systems. Appendix D provides answers to all questions posed in this book.

Notation and terminology

We use various conventions in the book. To start with, as is often the case in security texts, we tell stories with the characters Alice, Bob, and Mallet. We use these names for different purposes and use distinct fonts to indicate the intended purpose. Alice and Bob play the roles of honest agents, whereas Mallet is a malicious agent who tries to break into systems or compromise their security in some way. Each of these agents is assigned its own virtual machine with the same name as the agent. The host **`alice`** runs a desktop operating system with a graphical user interface, whereas the host **`bob`** is configured as a typical server providing only command-line access. Agent Mallet's machine, the host **`mallet`**, runs a desktop operating system providing tools to break into other systems. Finally, the agents' names are also used as usernames for certain applications. For example, *`bob`* denotes Bob's login name on the host **`bob`**.

We often present system input and output. To denote this, we use typewriter font for `commands`, `command-line inputs`, `outputs`, and `file names`.

The software in this book is based on Linux. All of the ideas we illustrate apply to other Unix-like systems like BSD, Solaris, Mac OS, etc. Moreover most of the commands we give will work on these other systems, perhaps with minor variations. In general we use the term Linux to refer to any Unix-like system.

We include both problems and exercises in this book. The distinction is as follows. Problems are interleaved with the text and allow readers to check their knowledge as they go. Brief solutions are given to all problems in Appendix D. We use a special environment to highlight problems

Problem 0.1 This is a problem with a solution provided in Appendix D.

Most chapters also end with additional exercises in the form of questions. When used as part of a course, these exercises allow a tutor to check the students' knowledge, as homework or in an exam. Hence answers are not provided.

Finally, we use boxes to highlight important text. To indicate actions that the reader is expected to perform, we prefix the action with the ▷ symbol and frame it in a box.

▷ This is an action the reader is expected to perform.

We also use boxes to frame principles, clarify settings, and the like.

Thou shalt not kill, steal, or leave application input unvalidated.

For brevity we abbreviate console output where it is obvious or unimportant. For example, we omit the current working directory and write `alice@alice:$` instead of `alice@alice:/var/log$`.

History and acknowledgements

The Information Security Laboratory at ETH Zurich was established by David Basin and Michael Näf in 2003. They designed a series of experiments in information security built on top of a virtualized environment, wrote a script based on the experiments, and used it for a lab course that they held starting in the 2003/4 winter semester. With its distinctly hands-on approach, the course has continued to be popular with advanced students. When Michael Näf left the department in 2007 to found the company Doodle, Patrick Schaller took over the lab and gave the course together with David Basin and tutorial assistants.

Apart from minor amendments, the teaching material for the course, consisting of a script and associated software, remained basically unchanged between 2004 and 2009. This high degree of stability testifies to the quality of the initial course but also to the difficulty inherent in changing the virtual machines supplied to the students. In 2010, however, we decided that the time was ripe for a major revision of the script and the software delivered with it. We kept the initial structure of the script but revised, updated, or changed a considerable part of the content. In addition we replaced the software (virtual machines) with up-to-date versions. The result is the basis for this book.

Numerous people assisted in producing the material for this course, much of which made its way into this book, in one form or another. The main contributors to the first version are David Basin, David Gubler, Manuel Hilty, Tilman Koschnik, Michael Näf, Rico Pajarola, Patrick Schaller, Paul Sevinç, and Florian Schütz. Michael Näf, in particular, was the main driver behind course material development in the early years. The first, major revision was undertaken mainly by David Basin, Luka Malisa, Pascal Sachs, Patrick Schaller, and Michael Schläpfer. We thank all of our collaborators for their tremendous assistance in making this book possible. We also thank Barbara Geiser who produced all the pictures used in this text and Jeffrey Barnes for his help in copy editing.

Zurich, Switzerland
August 2011

David Basin
Patrick Schaller
Michael Schläpfer

http://www.springer.com/978-3-642-24473-5

Applied Information Security
A Hands-on Approach
Basin, D.; Schaller, P.; Schläpfer, M.
2011, XIV, 202 p., Hardcover
ISBN: 978-3-642-24473-5