Preface

This is the instructor's manual to complement *Security in Computing, Fifth Edition* (copyright 2015). This fifth edition is a significant modification from previous editions, with major changes in many places.

This instructor's manual is organized in the order of the chapters of the book. Each chapter contains three parts:

- An introduction to the chapter
- A detailed outline of the chapter
- Solutions to selected exercises

The introduction to the chapter gives student objectives and suggestions for teaching the chapter. The detailed chapter outline can be transformed into projector slides or distributed to the students for their note-taking during a lecture.

We have not included answers to many of the more open-ended questions, which require creativity on the part of the student whose answers can vary considerably. In cases where an answer is given for a more open-ended question, the answer is, obviously, only a suggestion, and other possibilities should also be accepted.

We would be pleased to hear of additions, extensions, and new uses for this book that make it more useful in a course or more accessible to students. We also welcome suggestions for this solutions manual. It is not appropriate to put it on the web, because some students would be tempted to use its answers instead of working on the exercises themselves.

Although we are very pleased with the careful production job that was done on this book, a few errors always remain. We would like to correct these as soon as I can. Please send comments, suggestions, or corrections on either the main text or this solutions manual to us at ⟨chuck@pfleeger.com, shari@pfleeger.com, jonathan@qmulos.com⟩. Thank you.

Version: 20-Mar-15

1: Introduction

This chapter has three major purposes: (1) introduce students to the field of computer security and motivate study, (2) introduce concepts and terms, and (3) introduce frameworks for thinking about security problems. The students will probably be familiar with the concepts in general (such as threat, vulnerability, and control) from practical experience. In this chapter, students should develop a more formal understanding of these concepts, although some concepts will be refined and elaborated upon in later chapters. For example, authentication is discussed in Chapter 2, and network attacks are discussed in Chapter 6. It is often sensible to move quickly through this chapter and get to the later chapters that contain more substance. Similarly, exam questions for this chapter may be rather simple, so it may be more appropriate to defer an exam until after covering chapters containing material that better lends itself to exam questions.

Several of the exercises in this chapter require the student to demonstrate understanding of concepts by answering security questions with examples from everyday experience. There is no single "right" answer to these questions.

Many instructors follow the chapters out of order or skip sections in order to get to later material. The students are often particularly interested in Chapter 6, "Networks," and so they like to study that material relatively early in the course.

Outline

I. What Is Computer Security?
   a. Protection of Assets
      i. Hardware
      ii. Software
      iii. Data
   b. Vulnerability
   c. Threat
   d. Attack
   e. Control/Countermeasure

II. Threats
   a. C-I-A Triad
      i. Confidentiality, Integrity, and Availability
      ii. Also: Authentication, Nonrepudiation
   b. Confidentiality
      i. Unauthorized Person (Subject) Accesses Data (Object)
   c. Integrity
      i. Threat to Precision, Accuracy, or Consistency

d. Availability
e. Types of Threats
    i. Human vs. Nonhuman
    ii. Malicious vs. Nonmalicious
    iii. Random vs. Directed
f. Advanced Persistent Threat (APT)
    i. Organized, Directed, Malicious, Sophisticated
g. Types of Attackers
    i. Individuals
    ii. Organized, Worldwide Groups
    iii. Organized Crime
    iv. Terrorists

III. Harm
a. Risk Management
    i. Impact
    ii. Likelihood
b. Method
c. Opportunity
d. Motive

IV. Vulnerabilities
a. Weakness in Design, Implementation, Procedures, etc.

V. Controls
a. Prevent, Deter, Deflect, Mitigate, Detect, or Recover
b. Types of Control
    i. Physical
    ii. Procedural/Administrative
    iii. Technical
c. “Defense in Depth” or “Overlapping Controls”

Exercises

1. Distinguish between vulnerability, threat, and control.