Chapter 1

Introduction

It is often said that "information is power." This is true because information, correctly integrated, analyzed, and synthesized, leads to knowledge and informed decision-making. Today, the vast majority of the world's information resides in, is derived from, and is exchanged among multiple automated systems. Critical decisions are made (to place an order to buy or sell stocks) and critical actions are taken (to administer a transfusion of a certain blood type, or to change runways during a landing) based on information from these systems. For information to become power, the information must be accurate, correct, and timely, and be presented, manipulated, stored, retrieved, and exchanged safely, reliably, and securely. Information assurance (IA) is the enabler of this power.

1.1 Background

The twentieth century began with the industrial revolution and ended with rapid technological innovation that heralded the information revolution of the twenty-first century. The information revolution has brought many advantages to individuals and organizations. Vast quantities of information are available at incredible speeds to a multitude of people worldwide. E-Commerce is a catalyst for rapid business growth, particularly the development of small and home-based businesses.

The information revolution has also brought its share of risks. For example, millions of dollars were spent globally to prepare for and prevent major Y2K-related hazards. As a result of the time and resources applied, these efforts were highly successful. This exercise made modern society realize, in some cases for the first time, our near total dependence on the safe, reliable, and secure operation of interconnected computer technology from multiple industrial sectors; in particular, the eight critical infrastructure systems:

1. Telecommunications systems
2. Banking and financial systems
3. Power generation and distribution systems
4. Oil and gas distribution and storage systems
5. Water processing and supply systems
6. Air, water, and ground transportation systems
7. Emergency notification and response systems
8. Systems supporting critical government services

Preparations for Y2K were limited to transactions based on a single-date event: the transition from December 31, 1999, to January 1, 2000. In contrast, the infrastructure systems mentioned above operate, for the most part, 24 hours a day, 7 days a week, and perform critical transactions continuously. In addition, they interact with every segment of our society: manufacturing, wholesale and retail businesses, the media, hospitals, schools, and postal/package services, not to mention our homes. Consequently, infrastructure systems must operate safely, reliably, and securely at all times to avoid major disruptions to modern society. Ensuring this capability, even in the presence of accidental errors and intentional attacks, is the domain of IA.

1.2 Purpose

This book is a comprehensive yet practical guide to information security and the broader realm of information assurance (IA). This book fills an important gap in the professional literature. It is the first book to:

1. Examine the impact of both accidental and malicious intentional action and inaction on information security and IA
2. Explore the synergy between security, safety, and reliability engineering that is the essence of IA
3. Introduce the concept of IA integrity levels
4. Provide a complete methodology for information security/IA throughout the life of a system

The relationship between information security and IA and why both are needed is explained. Innovative long-term vendor, technology, and application-independent strategies demonstrate how to protect critical systems and data from accidental and intentional action and inaction that could lead to a system failure/compromise. These real-world strategies are applicable to all systems, from small systems supporting a home-based business to those of a multi-national corporation, government agency, or critical infrastructure system. Step-by-step, in-depth solutions take one from defining information security/IA goals through performing vulnerability/threat analyses, implementing and verifying the effectiveness of threat control measures, to conducting accident/incident investigations, whether internal, independent, regulatory, or forensic. A review of historical approaches to information security/IA puts the discussion

in context for today's challenges. Extensive glossaries of information security/IA terms and 80 techniques are an added bonus.

Many information security/IA techniques are borrowed from other engineering disciplines. In some cases, these techniques are used "as is." In others, the techniques or the interpretation of the results obtained from using them have been adapted specifically for information security/IA. In addition, there are several new and hybrid techniques. To help make order out of chaos, this book consolidates and organizes information about the information security/IA techniques, approaches, and current best practices.

IA is a new and dynamic field. Widespread use of the term IA, in particular as it relates to protecting critical infrastructure systems, dates back to the late 1990s. A series of events took place in the United States that helped propel the demand for IA. In 1996, the National Information Infrastructure Protection Act, Title 18 U.S.C. Section 1030, was passed.[178] In October 1997, the President's Commission on Critical Infrastructure Protection issued its final report and recommendations.[176] This led to the issuance of Presidential Decision Directive-63 (PDD-63) on May 22, 1998. PDD-63 established the nation's initial goals, many of which are set for the years 2003 to 2005, for IA and a cooperative framework between industry, academia, and local and national governments. As a result, a lot of people have suddenly inherited responsibility for information security/IA and are learning of its importance for the first time. Consequently, this book provides concrete guidance for those new to the field of information security/IA and those who wish to update the depth and breadth of their skills.

1.3 Scope

This book is limited to a discussion of information security/IA. Information security/IA is a global concern; it is not limited to a single industrial sector, economic segment, or legal jurisdiction. As a result, this book looks at the information security/IA challenges and opportunities from a global perspective.

Electronic privacy rights, intellectual property rights in regard to cryptographic algorithms, and national security concerns about exporting encryption technology are the subject of lively debates. This book acknowledges that these debates are ongoing, but does not participate in them. Instead, the reader is referred to Schneier and Banisar,[408,*] which provides an excellent treatment of these subjects.

The psychological motivation behind computer crime is not within the scope of this book, nor are general-purpose software engineering issues.

1.4 Intended Audience

This book is written for engineers, scientists, managers, regulators, academics, and policy-makers responsible for information security/IA. Readers will

* Schneier, B. and Banisar, D. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, 1997.

find the abundant practical "how-to" information, examples, templates, and discussion problems most useful. This book assumes a basic understanding of software engineering; however, no previous background in information security/IA is expected.

1.5 Organization

This book is organized in eight chapters. This chapter puts the book in context by explaining the rationale and purpose for which the book was written. It defines limitations on the scope of the book's subject matter, identifies the intended audience for whom the book was written, and discusses the organization of the book.

Chapter 2 sets the stage for the remainder of the book by providing an introduction to and overview of the basic concepts related to information security/IA. The use of information security/IA principles in different application and technology domains and its importance to a variety of stakeholders are explored.

Chapter 3 examines the historical precedents and changes in technology that necessitated the development of information security/IA. Specifically, techniques and approaches employed in physical security, communications security (COMSEC), computer security (COMPUSEC), information security (INFOSEC), system safety, and system reliability are reviewed. The benefits, limitations, and weaknesses of these approaches are analyzed relative to today's technology.

Chapters 4 through 8 define the five major components of a comprehensive and effective information security/IA program and the activities involved in each:

1. Defining the boundaries of the system
2. Performing vulnerability and threat analyses
3. Implementing threat control measures
4. Verifying the effectiveness of threat control measures
5. Conducting accident/incident investigations

As will be seen, there is considerably more to information security/IA than firewalls, encryption, and virus protection.

Four informative annexes are also provided. Annex A presents a glossary of acronyms and terms related to information security/IA.

Annex B presents a glossary of 80 information security/IA analysis, design, verification, and accident/incident investigation techniques. A description of each technique is given in the following format:

- **Purpose:** summary of what is achieved by using the technique; why the technique should be used
- **Description:** a summary of the main features of the technique and how to implement it

- **Benefits:** how the technique enhances IA integrity or facilitates assessment; any cost benefits derived from using the technique
- **Limitations:** factors that may limit the use of the technique, affect the interpretation of the results obtained, or impact the cost-effectiveness of the technique
- **References:** sources for more information about the technique

Annex C lists the sources that were consulted during the development of this book and provides pointers to other resources that may be of interest to the reader. Annex C is organized in three parts: standards, publications, and online resources.

Annex D summarizes the components, activities, and tasks of an effective information security/IA program.