# Preface

Few topics in the *information technology* (IT) field today generate as much interest as security. Interestingly, the IT world has been struggling with security issues for over 30 years, yet many security problems remain unsolved, unaddressed, and serious. As those responsible for securing systems and networks address security issues by a combination of hardware, software, procedures, policy, and the law, intruders and insiders circumvent protection mechanisms, discover new and unpublished vulnerabilities, or find lapses in an organization's policy and procedure in their efforts to damage systems, destroy data, or simply for mischief purposes. The attacker clearly has an advantage in this struggle between those who protect and those who penetrate. While the protector must close all vulnerabilities, the attacker need only find one to exploit.

Security in enterprise computing systems is also not simply a matter of technology and cannot be addressed satisfactorily with hardware and software alone. It is also a matter of managing people, establishing and enforcing strong (and correct) policies, implementing procedures that strengthen security, and periodically checking the effectiveness of the security architecture and making necessary changes. The provision of security in any enterprise must also be tailored to that particular organization. While the principles of computing security and common wisdom in the IT field are important, the actual application of such principles depends largely on a number of factors that often vary from enterprise to enterprise (e.g., confidentiality needs for data, customers, access requirements, volatility of data value, and others). Those individuals responsible for enterprise security must balance the need for security against the need for access to their system (by customers and employees), must be concerned with the cost of the security measures compared to the overall strength of the security architecture being constructed, and must also be cognizant of how well the security perimeter is performing. These are difficult tasks indeed. Success in these tasks requires vigilant attention to many factors, and the successful security manager must constantly re-educate him- or herself and his or her staff.

This book was edited by a management information systems professor and a computer science professor — both of whom believe that a cross-disciplinary approach to the security problem is important and that architected solutions are possible in any enterprise to provide "sufficient" or "adequate" security. The original thought in developing this book was to provide a collection of chapters useful to corporate security staff, government security administrators, and students of security who wish to examine a particular topic in some detail. We sometimes referred to the book as "good airplane reading" because one can read one or two chapters easily on a typical flight. We also considered this book as useful in the classroom. During a typical 16-week semester, students can spend each week discussing a different chapter of interest. Therefore, the reader can feel free to pick and choose chapters to read in any order — depending simply on the reader's interest. Each chapter stands alone, but they have been grouped into five distinct topic areas: security policy and management; security implications for business; security engineering; security technologies; and authentication issues. The mix of authors is interesting, too. We have purposely chosen authors to contribute who represent industry (practicing security engineers) as well as academia, and authors who present an international perspective (e.g., Australia, Finland, Singapore, China). There is a mix of practice and research embedded in the chapters, with the stronger emphasis on practice. As such, the reader may on occasion find conflicts in advice or conclusion between chapters. Given that the practice of security today is not exact, this is a natural result of independent views and writings.

We begin the book with four chapters addressing *security policy and management*. This topic was placed first since one must understand the policies to be enforced and management practices before a security solution can be considered. In Chapter I, Fink, Huegle, and Dortschy address the "role" of IT governance in e-business applications and propose a model framework for such governance activity. Past initiatives to provide IT governance frameworks are included here as well. Warkentin and Johnston build on this theme in Chapter II and discuss the problem of governance and the framework for ensuring that an organization's security policies are implemented over time. They also include a healthy discussion on whether such governance should be centralized or decentralized. Chapter III by Griffy-Brown and Chun presents a real-world case study of implementation of a strong security policy in the automotive industry and the lessons learned in dealing with security policy conflicts with business practices and needs. Finally, in Chapter IV, Sharman, Krishna, Rao, and Upadhyaya discuss procedures necessary to address malicious code. Virus, spyware, and scam spoofs are on the rise today, so no security architecture would be complete without addressing this area.

The second major division is *security implications for business*. Here we placed six chapters that examine specific nuances of small- and medium-sized businesses, e-commerce, and the law. Mishra and Dhillon address the impact of the Sarbanes-Oxley (SOX) Act on IT governance and internal controls in Chapter V. SOX has been highly controversial since its adoption and few large businesses have not been impacted by this legislation. Du, Jiao, and Jiao then provide an international perspective in Chapter VI on the development of a security blueprint for e-business applications, and they include a case study as an example of an implementation. Chapter VII, written by Masood, Sedigh-Ali, and Ghafoor, then discusses the principles of security management for an e-enterprise. These authors include a set of security metrics that the reader will find useful. In Chapter VIII, Weippl and Klemen provide another international view of a set of principles for implementation of IT security in small- and medium-sized enterprises or SME, which are often distinctly different than those that govern security design in large enterprises. Chapter IX continues to examine security implications in e-commerce applications. Here Furnell reiterates some of the same principles previously suggested by other authors, but applies them to the e-commerce practice. Finally, this section concludes with Chapter X addressing a topic made critical by the terrorist attacks of September 2001 — namely, survivability. Here Snow, Straub, Baskerville, and Stucke discuss the need for dispersal of people, technology, and physical assets.

In the third major section, focused on *security engineering*, we chose to include five important chapters. As might be expected, the authors in this section have significant industrial experience and several are practicing security engineers. Chapter XI was authored by Henning, a security engineer with Harris Corporation of Melbourne, Florida. Here she presents some basic tenets of security analysis that can be applied by any systems engineer to ensure early integration of security constraints into the system definition and development process. Ms. Henning's experience over many years of practice adds to the credibility of this work. Chapter XII addresses the issue of product selection and how one evaluates the strength of a product given current government procedures and laboratory analysis. Vaughn discusses this topic and provides some historical background that the reader will find interesting. In Chapter XIII, Murphy provides insights into the development of a robust *demilitarized zone* (DMZ) as an *information protection network* (IPN). Dr. Murphy's many years of experience at EDS and now as the president and founder of Dexisive Inc. are apparent to the reader as he discusses various approaches to implementing a DMZ. Chapter XIV proposes a unification of the process models of software engineering and security engineering in order to improve the steps of the software life cycle that would better address the underlying objectives of both engineering processes. This chapter, by Zulkernine and Ahamed, is based on an academic's view and is a good addition to the practical bent of the surrounding chapters. Last, Chapter XV by Graham and Steinbart addresses wireless security — an area of growing concern today as more enterprises move toward wireless infrastructures.

All security engineers and managers involved in the provision of security for IT systems must, at some point, consider specific *security technologies*, the topic of our fourth major division. We include five chapters here, each of which we found extremely interesting and informative reading. Chapter XVI by Dampier and Siraj provides an overview of what intrusion detection systems are and some guidelines on what to look for in such technologies. In Chapter XVII, Dodge and Ragsdale provide a most excellent treatment of honeypots, an evolving technology useful in many ways. Honeypots (and honeynets) are placed on one's network and designed to be attacked while being closely monitored. Such devices are helpful to determine who is attacking your system, whether or not you have an internal threat, and as a sensor inside a protected network to monitor the effectiveness of the security perimeter, among other uses described in this chapter. Warkentin, Schmidt, and Bekkering provide a description of the steganography problem in Chapter XVIII, where sensitive information may be secretly embedded in apparently innocuous messages or images, and discuss how steganalysis is used to find incidences of this problem. Chapter XIX, by Villarroel, Fernández-Medina, Trujillo, and Piattini, takes a more academic bent and provides ideas on how one might architect a secure data warehouse. Here we have ideas from researchers in Spain and Chile presented. The last chapter in this section, Chapter XX, provides an overview of investigative techniques used to find evidence of wrongdoing on a system. Here Dampier and Bogen present the intricacies of digital forensics and how one might intelligently respond to incidents requiring a digital forensic application.

The area of authentication issues makes up the last major division of the book. Authentication is an important factor in securing IT systems in that policy decisions made by a computer must be based on the identity of the user. We provide three distinct views here — one academic, one international, and one industrial and government combined. In Chapter XXI, Taylor and Eder provide an exploratory, descriptive, and evaluative discussion of security features in the widely used Windows and Linux operating systems. This is followed in Chapter XXII by a contribution from Finland, where Pulkkis, Grahn, and Karlsson provide an excellent taxonomy of authentication methods in networks. As an academic contribution, they also provide some research efforts in which they are involved. Last, we have a chapter on the important topic of identity management. In Chapter XXIII, Hollis (U.S. Army) and Hollis (EDS) provide the reader with an excellent discussion of what comprises identity management, what technologies are useful in building this capability, and how one makes a return on investment argument for such a capability.

We hope that you find this book useful, and we would enjoy hearing from its readers.

# Acknowledgments

The authors would like to acknowledge the efforts of the many contributors to the work contained within this book. Without their willingness to participate in this endeavor, there would be no book. Their hard work in developing the manuscripts, revising them as necessarily, and editing them for final form constitutes the heart of this project. We also wish to thank all the reviewers who volunteered to provide invaluable input by identifying manuscripts worthy of inclusion in the book and who also supplied important guidance into the improvement of each chapter during revisions.

The authors also wish to thank Jordan Shropshire, whose hard work and diligence in assisting us with the administrative processing of submissions, revisions, author information, and communications were important contributions to the success of this project. We also wish to acknowledge the support of Idea Group Inc., especially Kristin Roth, whose facilitation of the activities at each stage of the process and prompt response to our many questions helped make the process a smooth one.

*Merrill Warkentin, Mississippi State University, USA*
*Rayford Vaughn, Mississippi State University, USA*

* * * * *

I wish to thank my wife, Kim Davis, whose suggestions and general support provide me with the opportunity to pursue my professional goals. Kim has collaborated with me on security-related investigations and has frequently provided interesting professional perspectives on my various projects. But most importantly, her constant personal support provides the foundation for all my endeavors.

I also wish to thank Harold and Rosena Warkentin, who as parents and as teachers provided me with the motivation and desire to pursue my dreams, to work hard, and to always ask “why?”

Finally, I would like to thank the Center for Computer Security Risk (CCSR) at Mississippi State University (Ray Vaughn, Director) for its continuing support for my IA research and for that of my doctoral students.

*Merrill Warkentin*

* * * * *

I would also like to acknowledge my wife, Dianne Vaughn, for being supportive of me while I spent so much time at the office and at home working on this and other projects that seem to occupy much of my life. I would also like to acknowledge the Computer Science and Engineering Department at Mississippi State University for providing support and encouragement during the production of this book.

*Rayford Vaughn*