Preface

With the rapid progression of computer technology, computer attacks become more and more sophisticated. Once these attacks successfully explore the vulnerabilities of an information system, the confidential information in the system would become accessible to those who are not authorized to access to the information. Hence, this book will be targeting on providing a source of knowledge regarding information assurance and security.

This book details current trends and advances in information assurance and security, as well as explores emerging applications. This book is divided into four sections: attacks and vulnerabilities, security technologies, risk assessment and management, and strategic planning of information security. Together, it provides the readers with a broad view of information confidentiality, protection, and management. Each section contains several chapters that are contributed by well-known researchers or recognized practitioners from different countries. At the end of each chapter, it includes a summary and bibliography for further reading.

The objective of this book is not only to introduce various network and information security technologies but also to provide solutions to meet practitioner’s requirements in information assurance. Due to the rapid development in specialized areas of information assurance and security, this book will cover a broad range of topics on information assurance and security as well as provide in depth investigation of up-to-date technologies. In summary, this book will be very useful to the readers because:

• It will build up a strong, fundamental understanding of information assurance and resulting algorithms.
• It will offer balanced coverage of information security methods and their applications.
• It will address emerging methods and applications in information assurance and security.
• It will provide a strong foundation for launching new applications.
• It will include a wealth of illustrative examples and instructive results.

This book provides the readers with a unique opportunity to build a strong, fundamental understanding of theory and methods and thus to find solutions for many of today’s most interesting and challenging problems regarding information assurance and security. Though this book is not focused on any information security certificate exam or personal information protection, it is designed for those scientific and technical people who want to pursue their career in the field of information assurance and security. In the mean time, we would like this book become the most utilizable one for those professionals who use it as a reference to find specific information as well as for novices who use it as a study guide to learn various information assurance and security subjects.
With the help of numerous examples, illustrations and tables summarizing the results of quantitative analysis studies, this book will serve all different kinds of reading levels. The target readers include:

- The graduate students will benefit from the broad range of topics covered by the book and therefore build a solid foundation for future investigation.
- The researchers can use it as an up-to-date reference since it offers a broad survey of the relevant literature.
- The scientists, research and development engineers, and technical managers and executives will find it useful in the design and the implementation of information security systems.

This book is organized into four sections: attacks and vulnerabilities, security technologies, risk assessment and management, and strategic planning of information security.

Section 1 provides readers with an overview of attacks and vulnerabilities, which includes two chapters. Computer attacks could be categorized based on the courses of action used to exploit vulnerabilities or on the result of attacks. In Chapter 1, the author categorizes the attacks, according to attackers’ motivations, into ten categories. In each category, the author uses recent incidents to illustrate the motives of people who attack company IT systems.

An increasing number of people are using wireless technologies in their life, with a corresponding increase in the number of people who use malicious tools to abuse unprotected wireless networks, thus posing a serious threat to both individuals and organizations. Security becomes a highly important part of the wireless network. Chapter 2 starts with the history of wireless technology. Wireless security threats in wireless local area network and wireless personal area network are also discussed in this chapter and it ends with the presence of countermeasures of wireless attacks.

Section 2 presents the most up-to-date information assurance and security technologies available. In Chapter 3, the authors review anomaly detection and misuse detection approaches in detecting worms spreading through the Internet. The authors also produce discussions regarding the analysis, development and deployment of statistical anomaly detection techniques for e-mail traffic.

Mobile phone forensics is a quite new research topic in the field of digital forensics. Chapter 4 starts with an introduction of GSM and CDMA cellular wireless technologies, followed by investigates forensics issues such as guidelines, procedures, tools, and threats. Current researches and trends on mobile phone forensics are also discussed.

Authentication is very important in protecting computer systems. In the beginning of Chapter 5, the authors explore the ideas about trust models in electronic transactions. The authors then research electronic transactions security using continuous authentication processes in trust in electronic communications systems, brief revision about conventional authentication models, continuous authentication concepts, and biometrics.

Cryptography is the science that use key to encrypt a message into ciphertext and decrypt the ciphertext back into plaintext. Identity-Based cryptography (IBC) uses a public key for encryption, which the key represents the identification of a user. IBC is the topic of Chapter 6. IBC attacks, its security vulnerabilities and solutions to those vulnerabilities are also covered.

As indicated in Chapter 7, biometrics gradually plays an important part on information technology in individual’s identity and access control. With the use of more and more reliable user authentication techniques, the security of information systems are therefore enhanced. In this chapter, the authors begin with the introduction of the background of audio-visual systems. Then the authors propose an audio-visual...
system using face and voice modality biometrics technology and therefore the system could handle large volume of people recognition over internet protocol.

Chapter 8 is focused on Firewall. Firewalls protect personal computers and infrastructure networks from malicious threats away. Based upon a set of rules, firewalls examines traffic passing through and only allow legitimate messages to pass. In this chapter, the author introduces different types of firewalls, security policies on firewalls, firewall architecture, and firewall implementation considerations.

In Section 3, the attention is directed to the Risk Assessment and Management. Risk Assessment and Real Time Vulnerability Identification in IT Environments are discussed in Chapter 9. Security risk assessment is a process to ensure that the security controls for a system are fully commensurate with its risks. Implementing such assessment will prevent unauthorized access to saved and confidential information. For all businesses using a wireless network, security should be a priority. The authors not only examine risks, attacks, threats and vulnerabilities in a business but also explore the main risk assessment techniques and frameworks. They even present a pro-active framework for identifying vulnerabilities and assessing risk and demonstrate their model using a client/server approach.

In Chapter 10, the author describes the challenges of managing privacy impact assessment of personally identifiable information followed by a discussion on privacy impact assessment of new and in-service projects. A model showing how to conduct privacy impact assessment on both new and in-service projects is also presented.

A lack of security and privacy requirements could lead to insecure software. Security and privacy requirements engineering focuses on identifying software security and privacy risks in early stages of a software development lifecycle. Chapter 11 demonstrates a model that integrates the security risk assessment techniques with privacy risk assessment techniques. To make sure that both the existing security and the privacy risk assessment techniques follow the same methodology and require the same expertise, a classification scheme of risk assessment methods is applied. Also, the authors use pseudo-software development projects to evaluate the feasibility of their proposed model.

The last section, Section 4, we provide strategies of security policy design and threat mitigation and response to risks. The information data of an organization must be available when needed and well protected from unauthorized inside and outside intruders. How to manage and protect the information data must be carefully planned. Regulatory and policy compliance in the field of information security and legislation’s impact on regulatory compliance are explored in Chapter 12. Not only did the authors provide guidelines for the development of policies for responding to identity theft, but also they present policy compliance for achieving the policy’s goals and auditing to determine whether policy compliance has actually been achieved.

Te-Shun Chou
East Carolina University, USA