Preface

Information assurance, the body of knowledge, policies, processes, practices, and tools that provide reasonable assurance that one’s information and communications are used only as intended and only by authorized parties, has become a complex discipline. Today, because of Internet interconnectivity, we live in a world where one may reach all. Such interconnectivity and attendant vulnerabilities require that IT managers and end-users have an understanding of the risks and solutions available to better protect their information and operations. This volume was written to address these issues.

When network security is mentioned, the general public is more often aware of security failures than of the technology available for secure communications. Viruses, worms, Trojan horses, denial-of-service attacks, and phishing are well known occurrences. Access controls, authentication, confidentiality, integrity, and non-repudiation, which are measures to safeguard security, are neither well known nor appreciated. However, when these security mechanisms are in place, users can have a degree of confidence that their communications will be sent and received as intended.

The basic principles of secure communications have not changed with technology and communication advances. Today, communications companies are working to provide security services and to implement security mechanisms in email correspondence, virtual private networks, ecommerce, Web services, and wireless products. However, the tremendous increase in the use of technology has made it challenging to keep up with the need for security.

Fortunately, security today is an open research field in which there are thousands of experts looking for weak security implementations. When a weakness is found, for example, in the case of Wi-Fi (Wireless Fidelity Standard—IEEE 802.11a, b, g) in 2004, the crypto community immediately acts and changes are proposed to correct the weakness, which is what happened after this case. By using open standards, it is possible to have security applications reviewed by the world crypto community.

This book started as a collection of lecture notes on cryptography written by the author over many years. It was initially intended as a way to describe the security levels of certain crypto products. This material was later expanded with the addition of other lectures notes written for the Cryptography and Network Security course the author teaches at the University of Dallas in the Graduate School of Management’s MBA and Master of Science in Information Assurance programs.
**Intended Audience**

This book is intended to provide those in the information assurance field with a basic technical reference that provides the language, knowledge, and tools to understand and implement security services, mechanisms, and applications in today’s secure communications networks. This book could also be used as a text in a one-semester information assurance course, especially in Master of Business Administration and Master of Science programs.

Readers with backgrounds in telecommunications and information technology will probably be somewhat familiar with certain parts of the material covered in this book. Other readers, for example, those in the Master of Business Administration in Information Assurance program may find that this book has too much technical information for their future needs. In those situations, professors may decide not to emphasize the technical parts of the material and focus on those principles that are essential to information assurance.

The crypto, security services, and security mechanisms topics presented in this book map the training requirements in CNSS 4011, the National Training Standard for Information Systems Security (INFOSEC) Professionals, and CNSS 4012, the National Information Assurance Training Standard for senior systems managers.

**Standards and Requests for Change**

This book’s approach to information assurance is from the point of view of security services, security mechanisms, and the standards that define their implementation. In this way, it is easier for the reader to associate the standard with a certain security service or security mechanism.

The word “standard” implies a set of guidelines for interoperability. Networks would not be able to operate unless they voluntarily adhered to open protocols and procedures defined by some type of standards. When talking about the Internet and IP networks, the word “standard” is associated with Request For Change (RFC), even though not every RFC is a standard. The need for standards applies not only to interconnecting IP networks, but also to the implementation of security services and mechanisms.

RFCs have been created since the days of the ARPANET, and, later on, for the Internet through the Internet Engineering Task Group (IETG). According to the RFC Index on the IETG.org Web page, RFC 001 was published in April 1969. The first RFC related to security was RFC 644, “On the Problem of Signature Authentication for Network Mail,” written by Bob Thomas, BBN-TENEX, and published in July 1974. The network mail message that Bob Thomas was referring to was the ARPANET. It is interesting to note that e-mail security has been a major concern since the days of the ARPANET; however, there are still very few companies that encipher or authenticate their e-mails.

It is the author’s opinion that when security services and mechanisms are reviewed, their related RFCs should be studied. RFCs as standards define how to implement key exchanges, encryption algorithms, integrity, hash and digital signatures, as well as authentication algorithms. Therefore, in this book, those RFCs that are related to information assurance are explained along with security applications. Understanding security-related RFCs provides excellent knowledge, not only about security mechanisms, but also on secure applications such as email security, VPNs, IPsec, TLS, Web services, and wireless security.
Organization of the Book

This book is organized into three sections. In the first two sections, crypto systems, security mechanisms, and security services are discussed and reviewed. The third section discusses how those crypto services and mechanisms are used in applications such as e-mail security, VPNs, IPsec, TLS, Web services, and wireless security.

The following is a brief description of each chapter:

**Chapter I**, “Classic Cryptography,” provides a historical perspective of cryptography and code breaking, including some of the techniques employed over the centuries to attempt to encode information. Some early crypto machines and the Vernam Cipher, developed by Gilbert Vernam in 1917, are discussed in this chapter.

**Chapter II**, “Information Assurance,” discusses the TCP/IP protocol. When data communications security is discussed in this book, it refers to communications security for the TCP/IP protocol and to the security mechanisms implemented at the different layers of the TCP/IP stack protocol.

**Chapter III**, “Number Theory and Finite Fields,” describes certain basic concepts of number theory such as modular arithmetic and congruence, which are necessary for an understanding of Public-Key crypto systems.

**Chapter IV**, “Confidentiality: Symmetric Encryption,” covers confidentiality using the different types of symmetric encryption stream ciphers and block ciphers. The theory for using shift registers as stream ciphers is also covered in this chapter, as well as DES and Advanced Encryption Standard (AES) block encryption algorithms.

**Chapter V**, “Confidentiality: Asymmetric Encryption (public key),” covers confidentiality using asymmetric encryption (public key). The most used public-key ciphers, including the Pohlig-Hellman algorithm, RSA algorithm, ElGamal algorithm, and Diffie-Hellman are discussed in this chapter.

**Chapter VI**, “Integrity and Authentication,” discusses methods that are used to check if a message was modified using hash functions and ways to verify a sender’s identity by using digital signatures.

**Chapter VII**, “Access Authentication,” describes authentication mechanisms such as (1) IEEE 802.1X access control protocol; (2) extensible authentication protocol (EAP) and EAP methods; (3) traditional passwords; (4) remote authentication dial-in-service (RADIUS); (5) Kerberos authentication service; and (6) X.509 authentication.

**Chapter VIII**, “Elliptic Curve Cryptography,” covers ECC public-key crypto systems, which offer the same level of security as other public-key crypto systems, but with smaller key sizes. This chapter is written for those with some knowledge of cryptography and public-key systems who want a quick understanding of the basic concepts and definitions of elliptic curve cryptography.

**Chapter IX**, “Certificates and Public-Key Architecture,” discusses how the authenticity of a public-key is guaranteed by using certificates signed by a certificate authority. When public-key is used, it is necessary to have a comprehensive system that provides public-key encryption and digital signature services to ensure confidentiality, access control, data integrity, authentication, and non-repudiation. That system, called *public-key infrastructure* or PKI, is also discussed in this chapter.

Chapter XI, “VPNs and IPsec,” covers virtual private networks (VPNs), which emulate a private wide area network (WAN) facility using IP networks, such as the public Internet, or private IP backbones. IPsec, also covered in this chapter, provides security services at the IP network layer such as data origin authentication, access control, confidentiality (encryption), connectionless integrity, rejection of replayed packets (a form of partial sequence integrity), and limited traffic flow confidentiality.

Chapter XII, “TLS, SSL, Secure Electronic Transactions (SET),” describes how transport layer security (TLS) or secure socket layer (SSL) protocols are used to secure an Internet transaction between a secure Web server and a client’s computer that is using a Web browser. Secure electronic transaction (SET), a secure payment process that was proposed by VISA and MasterCard, is also described.

Chapter XIII, “Web Services,” explains Web services and open standards such as extensible markup language (XML), and simple object access protocol (SOAP). The following Web services mechanisms are also discussed in this chapter: (1) XML Encryption, XML signature, and XML key management specification (XKMS); (2) security association markup language (SAML), and Web services security (WS-Security).

Chapter XIV, “Wireless Security,” discusses the three primary categories of wireless networks: wireless local area network (WLAN), wireless metropolitan-area network (WMAN), and wireless personal area network (WPAN), as well as the security services and mechanisms for each of them.