The proliferation of Internet services and applications is bringing systems and Web services security issues to the fore. There is a consensus that a key, contributing factor leading to cyberthreats is the lack of integrated and cohesive strategies that extend beyond the network level, to protect the applications and devices at system level as well. Many techniques, algorithms, protocols, and tools have been developed in the different aspects of cybersecurity, namely, authentication, access control, availability, integrity, privacy, confidentiality, and nonrepudiation as they apply to both networks and systems.

The IT industry has been talking about Web services for many years. The benefits of having a loosely coupled, language-neutral, platform-independent way of linking applications within organizations, across enterprises, and across the Internet, are becoming more evident as Web services are used in pilot programs and in wide-scale production. Moving forward, customers, industry analysts, and the press identify a key area that needs to be addressed as Web services become more mainstream: security.

The purpose of this book is to bring together the technologies and researchers who share interest in the area of e-business and Web services security. The main aim is to promote research and relevant activities in security-related subjects. It also aims at increasing the synergy between academic and industry professionals working in this area. This book can also be used as the textbook for graduate courses in the area of Web services security. This book is comprised of 20 chapters that cover various aspects of Web services security and e-business. The scope of the chapters is summarized hereunder.

The first chapter gives a practical overview of the brief implementation details of the IEEE802.11 wireless LAN and the security vulnerabilities involved in such networks. Specifically, it discusses the implementation of EAP authentication using RADIUS server with WEP encryption options. The chapter also touches on the ageing WEP and the cracking process, along with the current TKIP and CCMP mechanisms. War driving and other security attacks on wireless networks are also briefly covered. The chapter
concludes with practical security recommendations that can keep intruders at bay. The authors hope that any reader would thus be well informed on the security vulnerabilities and the precautions that are associated with 802.11 wireless networks.

The increasingly important role of security for wireless Web services environments has opened an array of challenging problems centered on new methods and tools to improve existing data encryption and authentication techniques. Real-time recurrent neural networks offer an attractive approach to tackling such problems because of the high encryption capability provided by the structural hidden layers of such networks. In the second chapter, a novel neural network-based symmetric cipher is proposed. This cipher releases the constraint on the length of the secret key to provide the data integrity and authentication services that can be used for securing wireless Web services communication. The proposed symmetric cipher design is robust in resisting different cryptanalysis attacks. Simulation results are presented to validate its effectiveness.

In the third chapter, the business implications, as well as security and privacy issues of the widespread deployment of radio frequency identification (RFID) systems, were discussed. At first, the components that make up an RFID system to facilitate better understanding of the implications of each were discussed, and then the commercial applications of the RFID were reviewed. Further, the security and privacy issues for RFID systems, and what mechanisms have been proposed to safeguard these, were discussed. The topics discussed in this chapter highlight the benefits of using RFIDs for user convenience in ubiquitous and pervasive commercial services and e-businesses, while maintaining the integrity of such systems against malicious attacks on the users' security and privacy. This is vital for a business establishment to coexist with peers, and remain competitively attractive to customers.

Over the years, computer systems have evolved from centralized monolithic computing devices supporting static applications, into client-server environments that allow complex forms of distributed computing. Throughout this evolution, limited forms of code mobility have existed. The explosion in the use of the World Wide Web, coupled with the rapid evolution of the platform-independent programming languages, has promoted the use of mobile code and, at the same time, raised some important security issues. The fourth chapter introduces mobile code technology, and discusses the related security issues.

Multicast communication demands scalable security solutions for group communication infrastructure. Secure multicast is one such solution that achieves the efficiency of multicast data delivery. Key generation plays an important role in enforcing secure and efficient key distribution. The fifth chapter addresses the issues focused on the area of key generation on key management cryptographic algorithms that support security requirements in multicast group communications. These issues are of importance to application developers wishing to implement security services for their multicast applications. The three main classes: centralized, decentralized, and distributed architec-
tasures, are investigated and analyzed here, and insight is given to their features and goals. The area of group key generation is then surveyed, and proposed solutions are classified according to the efficiency of the cryptographic algorithms and multicast security requirements. The open problems in this area are also outlined.

Agent technologies have grown rapidly in recent years as Internet usage has increased tremendously. Despite its numerous practical benefits and promises to provide an efficient way of mitigating complex distributed problems, mobile agent technology is still lacking effective security measures, which severely restricts their scope of applicability. The sixth chapter analyzes and synthesizes the different security threats and attacks that can possibly be imposed to the mobile agent systems. The security solutions to resolve the problems and the research challenges in this field are presented.

The seventh chapter introduces the intrusion detection system (IDS). It started with a brief explanation of history of IDS, proceeded with generic components of IDS. Besides highlighting current advances in IDS, the chapter describes recent challenges to the system. The authors hope that this chapter will shed a light for readers who are unfamiliar with this domain.

ZKP-based authentication protocols provide a smart way to prove an identity of a node without giving away any information about the secret of that identity. There are many advantages, as well as disadvantages, to using this protocol over other authentication schemes, as well as challenges to overcome in order to make it practical for general use. The eighth chapter examines the viability of ZKPs for use in authentication protocols in networks. It is concluded that nodes in a network can achieve a desired level of security by trading off key size, interactivity, and other parameters of the authentication protocol. This chapter also provides data analysis, which can be useful in determining expected authentication times based on device capabilities. Pseudocode is provided for implementing a graph-based ZKP on small or limited processing devices.

Web services enable the communication of application to application in a heterogeneous network and computing environment. The powerful functionality of Web services has given benefits to enterprise companies, such as rapid integrating between heterogeneous e-business systems, easy implementation of e-business systems, and reusability of e-business services. While providing the flexibility for e-business, Web services tend to be vulnerable to a number of attacks. Core components of Web services such as simple object access protocol (SOAP), Web services description language (WSDL), and universal description, discovery, and integration (UDDI) can be exploited by malicious attacks due to lack of proper security protections. These attacks will increase the risk of an e-business that employs Web services. The ninth chapter aims to provide a state-of-the-art view of Web services attacks and countermeasures. This chapter also examines various vulnerabilities in Web services, followed by the analysis of respective attacking methods. Further, this chapter also discusses preventive countermeasures against such attacks to protect Web services deployments in e-business, and finally address future trends in this research area.

The 10th chapter presents a new simple scheme for verifiable encryption of elliptic curve digital signature algorithm (ECDSA). The protocol presented is an adjudicated protocol, that is, the trusted third party (TTP) takes part in the protocol only when there is a dispute. This scheme can be used to build efficient fair exchanges and certified e-mail protocols. In this chapter, the authors also present the implementation issues. The
chapter presents a new algorithm for multiplying two $2n$ bits palindromic polynomials modulo $x^n - 1$ for prime $p = 2^n + 1$ for the concept defined in Blake and Roth (1998) and it is compared with the Sunar-Koc parallel multiplier given in Sunar and Koc (2001). Finally, the chapter concludes that the proposed multiplication algorithm requires $(2n^2 - n + 1)$ XOR gates, which is approximately 34% extra, as compared to $1.5(n^2 - n)$ XOR gates required by the Sunar-Koc parallel multiplier, and 50% less than the speculated result $4n^2$ XOR gates given by Sunar and Koc (2001). Moreover, the proposed multiplication algorithm requires $(2n^2 - n)$ AND gates, as compared to $n^2$ AND gates which is doubled that of the Sunar-Koc method.

Firstly, the fact that business intelligence (BI) applications are growing in importance, and secondly, the growing and more-sophisticated attacks launched by hackers, the concern of how to protect the knowledge capital or databases that come along with BI or, in another words, BI security, has thus arisen. In the eleventh chapter, the BI environment, with its security features, is explored, followed by a discussion on intrusion detection (ID) and intrusion prevention (IP) techniques. It is understood, through a Web-service case study, that it is feasible to have ID and IP as counter measures to the security threats; thus, further enhancing the security of the BI environment or architecture.

In the 12th chapter, the concept of “trust transfer” using chain signatures will be presented. Informally, transferring trust involves creating a trust (or liability) relationship between two entities, such that both parties are liable in the event of a dispute. If such a relationship involves more than two users, we say they are connected in a chained trust relationship. The members of a chained trust relationship are simultaneously bound to an agreement with the property that additional members can be added to the chain, but once added, members cannot be removed thereafter. This allows members to be incrementally and noninteractively added to the chain. We coin the term “chained signatures” to denote signatures created in this incremental way. An important application of chained signatures is in e-commerce transactions involving many users. We present a practical construction of such a scheme that is secure under the Diffie-Hellman assumption in bilinear groups.

The recent increase in the malicious usage of the network has made it necessary that an IDS should encapsulate the entire network rather than at a system. This was the inspiration for the birth of a distributed intrusion detection system (DIDS). Different configurations of DIDSs have been actively used, and are also rapidly evolving due to the changes in the types of threats. The thirteenth chapter gives an overview and the structure of DIDS. The various agents that are involved in DIDS, and the benefits are given in brief. In the end, directions for future research work are discussed.

In the 14th chapter, we discuss how security protocols can be attacked by exploiting the underlying block cipher modes of operation. This chapter presents a comprehensive treatment of the properties and weaknesses of standard modes of operation. Further, this chapter shows why all modes of operation should not be used with public-key ciphers in public-key security protocols. This includes the cipher block chaining (CBC) mode, when there is no integrity protection of the initialisation vector (IV). In particular, it was shown that it is possible in such instances to replace a block at the beginning, middle, or end of a CBC-encrypted message. This chapter demonstrates that the security of single-block encryptions can be reduced to the security of the electronic codebook.
(ECB) mode, and show that in the absence of integrity, one could exploit this to aid in known- and chosen-\textit{IV} attacks. Finally, this chapter also presents chosen-\textit{IV} slide attacks on counter (CTR) and output feedback (OFB) modes of operation. Results show that protocol implementers should carefully select modes of operation, be aware of the pitfalls in each of these modes, and incorporate countermeasures in their protocols to overcome them. It is also important to realize that modes of operation only provide confidentiality, and that when used in the context of security protocols, these modes should be combined with authentication and integrity protection techniques.

The 15\textsuperscript{th} chapter addresses the need of cryptographic algorithm to prepare unbreakable cipher. Though the performance of symmetric key algorithms is far better than asymmetric key algorithms, it still suffers with key distribution problem. It is highly evident that there is always a demand for an algorithm to transfer the secret key in a secure manner between the participants. This chapter argues that by providing the randomness to the secret key, it would be increasingly difficult to hack the secret key. This chapter proposes an algorithm effectively utilizes the random nature of stock prices, in conjunction with plain text, to generate random cipher. This algorithm can be used to exchange the secret key in a secure manner between the participants.

In the 16\textsuperscript{th} chapter, a watermarking scheme that utilizes error correction codes for added robustness is proposed. A literature survey covering various aspects of the watermarking scheme, such as the arithmetic redundant residue number system and concepts related to digital watermarking, is given. The requirements of a robust watermarking scheme are also described. In addition, descriptions and experimental results of the proposed watermarking scheme are provided to demonstrate the functionality of the scheme. The authors hope that with the completion of this chapter, the reader will have a better understanding of ideas related to digital watermarking, as well as the arithmetic redundant number system.

A security framework for secure message delivery and off-line message viewing of the electronic bills is presented in the seventeenth chapter. This framework is implementable towards smart applications such as electronic bill presentment and payment systems. Chapter XVIII, introduces the concept of access control and its objectives in fulfilling security requirements for the computing world. The main arrears in access control, namely DAC, MAC, and RBAC, will be covered; thus, giving enough background knowledge to the reader on existing policies and framework. Hence, the reader will be able to comprehend the concept of task delegation with regard to access control policies, and how delegated tasks or roles can affect existing risk levels in an organization. Measuring risk has a two-fold benefit: one is that it enables security officials to be prepared with more accurate security measures with higher granularity and secondly, this will certainly be useful for security plans for mitigating potential risks.

Internet protocol version 6 (IPv6) is the next generation Internet protocol proposed by the Internet Engineering Task Force (IETF) to supplant the current Internet protocol version 4 (IPv4). Lack of security below the application layer in IPv4 is one of the reasons why there is a need for a new IP. IPv6 has built-in support for the Internet protocol security protocol (IPSec). The nineteenth chapter reports work done to evaluate implications of compulsory use of IPSec on dual stack IPv4/IPv6 environment.

Finally, in the last chapter provides a conceptual modeling approach for Web services (WS) security risk assessment, which is based on the identification and analysis of
stakeholder intentions. There are no similar approaches for modeling Web services security risk assessment in the existing pieces of literature. The approach is, thus, novel in this domain. The approach is helpful for performing means-end analysis; thereby, uncovering the structural origin of security risks in Web services, and how the root causes of such risks can be controlled from the early stages of the projects. The approach addresses “why” the process is the way it is, by exploring the strategic dependencies between the actors of a security system, and analyzing the motivations, intents, and rationales behind the different entities and activities in constituting the system.

This book aims to help toward technical strategy and a roadmap whereby the industry/academia can produce and implement a standards-based architecture that is comprehensive, yet flexible enough to meet the Web services security needs of real businesses.

References

Blake & Roth. (1998)
Sunar & Koc. (2001)