Preface

In an increasingly digital society that relies heavily on Internet and mobile networks for every aspect of day-to-day life, security is a pressing concern. The sixteen chapters that follow represent the cutting edge of research and scholarship on IT security, as first witnessed in the *International Journal of Information Security and Privacy (IJISP)*. Within these pages, readers will find information on network security, modern encryption protocols, data analysis, and more.

The book begins with “A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment” by Devon Bennett et al., which describes how, in developed economies, electronic communication infrastructures are crucial for daily public, private, and business interactions. Cellular systems are extensively used for business communications, private interaction, and in some cases, public information services, via such uses as mass SMS messaging. The Public Switched Telephone Network (PSTN) is at the core of all communications platforms. It was used primarily for voice communication purposes, but with current technological advances, this platform has been transformed from a voice to voice interface to a web enabled multimedia platform that provides commercial, business, and e-commerce services to the public. In response to the September 11, 2001, terrorist acts in New York City, the UK government introduced a policy of separating and transferring all emergency communication traffic from the PSTN to a digital public safety network based on the TETRA architecture. This chapter extends the utilisation of the TETRA deployment by discussing a secure MANET hybrid solution for use in extreme situations as a short/mid-term EMS organisational communication platform for emergency and rescue operations.

Chapter 2, “A Self-Supervised Approach to Comment Spam Detection Based on Content Analysis” by A. Bhattarai and D. Dasgupta, studies the problems and threats posed by a type of spam in the blogosphere, called blog comment spam. It explores the challenges introduced by comment spam, generalizing the analysis substantially to any other short text type spam. The authors analyze different high-level features of spam and legitimate comments based on the content of blog postings. The authors use these features to cluster data separately for each feature using K-Means clustering algorithm. The authors also use self-supervised learning, which could classify spam and legitimate comments automatically. Compared with existing solutions, this approach demonstrates more flexibility and adaptability to the environment, as it requires minimal human intervention. The preliminary evaluation of the proposed spam detection system shows promising results.

Many peer-to-peer security protocols proposed for wireless communications use one-time shared secrets for authentication purposes. Chapter 3, “A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications” by Ioana Lasc et al., analyses online update mechanisms for one-time shared secrets. A new type of attack against update mechanisms, called desynchronisation attack, is introduced. This type of attack may lead to a permanent denial of service condition. A case
study demonstrates the effectiveness of desynchronisation attacks against a security protocol for mobile satellite communications. A new mutual authentication protocol for satellite communications, incorporating a resynchronisation capability, is proposed to counter the disruptive effects of desynchronisation attacks. The new protocol has an esynchronisation phase that is initiated whenever desynchronisation is suspected. Thus, the possibility of causing permanent denial of service conditions by mounting desynchronisation attacks is eliminated. A security analysis of the proposed protocol establishes its resistance against attacks like replay attacks, dictionary attacks, and desynchronisation attacks.

In the Web dependent world, companies must respect and protect individuals’ information privacy. Companies develop and implement corporate information privacy policies to comply with the domestic and international information privacy laws and regulations. Chapter 4, “Information Privacy: Implementation and Perception of Laws and Corporate Policies by CEOs and Managers” by Garry L. White et al., investigates: (a) the approach used by multinational and domestic companies to develop and implement corporate information privacy policies; and (b) the perception of corporate managers/professionals toward information privacy legislation and secondary use of personally identifiable information (PII) that organizations collect. A survey was conducted to collect data from corporate CEOs, managers, and technical professionals of national and multinational companies. Findings indicate the following: 1) Views regarding the practicality and effectiveness of information privacy legislations are similar for respondents from the national and multinational companies. 2) Respondents are undecided about whether the privacy laws of the United States and foreign countries are equally restrictive. 3) Multinational companies do not favor developing and implementing uniform information privacy policies or different information privacy policies across countries of operations. 4) Respondents strongly agreed that unauthorized secondary use of personal information is unacceptable.

“User Perceptions of Security Technologies,” by Douglas M. Kline et al., explores user perceptions of information systems security through a study of university students. Server authentication, which is often ignored by users, clouded by system administrators, and exploited by hackers, is explored in detail, as it significantly affects usability and requires user knowledge and participation. The study also investigates the respondents’ consistency, gender differences, and assessment of their own knowledge. Although users appear knowledgeable about security technologies, they rely more on peer opinion and reputation of web sites when making security decisions.

Golam Koasar and Xun Yi, in “Secure Two-Party Association Rule Mining Based on One-Pass FP-Tree,” explore Frequent Path tree (FP-tree), a popular method to compute association rules that is faster than Apriori based solutions in some cases. Association rule mining using FP-tree method cannot ensure entire privacy since frequency of the itemsets are required to share among participants at the first stage. Moreover, FP-tree method requires two scans of database transactions which may not be the best solution if the database is very large or the database server does not allow multiple scans. In addition, one-pass FP-tree can accommodate continuous or periodically changing databases without restarting the process as opposed to a regular FP-tree based solution. In this chapter, the authors propose a one-pass FP-tree method to perform association rule mining without compromising any data privacy among two parties. A fully homomorphic encryption system over integer numbers is applied to ensure secure computation among two data sites without disclosing any number belongs to themselves.

In the next chapter, “A Mark-Up Language for the Specification of Information Security Governance Requirements,” Anirban Sengupta and Chandan Mazumdar detail how, as enterprises become dependent on information systems, the need for effective Information Security Governance (ISG) assumes significance. ISG manages risks relating to the confidentiality, integrity and availability of information,
and its supporting processes and systems, in an enterprise. Even a medium-sized enterprise contains a huge collection of information and other assets. Moreover, risks evolve rapidly in today’s connected digital world. Therefore, the proper implementation of ISG requires automation of the various monitoring, analysis, and control processes. This can be best achieved by representing information security requirements of an enterprise in a standard, structured format. This chapter presents such a structured format in the form of Enterprise Security Requirement Markup Language (ESRML) Version 2.0. It is an XML-based language that considers the elements of ISO 27002 best practices.

“On the Security of Self-Certified Public Keys,” by Cheng-Chi Lee et al. explains how many cryptosystems have been developed to solve the problem of information security, and some approaches are based on the self-certified public key proposed by Girault. In Girault’s scheme, the public key is computed cooperatively by both the system authority (SA) and the user. One of the advantages is that the public key is able to implicitly authenticate itself without any additional certificates. Another advantage is that the SA is not able to forge a public key without knowing the user’s secret key. Despite the advantages of Girault’s system, in this chapter, the authors demonstrate that the system still suffers from two main weaknesses. As a result, the authors propose a slight improvement on Girault’s system.

Zero-knowledge authentication protocols are an alternative to authentication protocols based on public key cryptography. Low processing and memory consumption make them especially suitable for implementation in smart card microprocessors, which are severely limited in processing power and memory space. Chapter 9, “Design and Implementation of a Zero-Knowledge Authentication Framework for Java Card” by Ahmed Patel et al., describes a design and implementation of a software library providing smart card application developers with a reliable authentication mechanism based on well-known zero-knowledge authentication schemes. Java Card is used as the target smart card platform implementation based on the evaluation of the Fiat-Shamir (F-S) and Guillou-Quisquater (G-Q) protocols under various performance criteria are presented to show the effectiveness of the implementation and that G-Q is a more efficient protocol.

In the following chapter, “E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems,” Harold Pardue et al. explain that approximately 25% (according to http://verifiedvoting.com/) of voting jurisdictions use direct recording electronic systems to record votes. Accurate tabulation of voter intent is critical to safeguard this fundamental act of democracy: voting. Electronic voting systems are known to be vulnerable to attack. Assessing risk to these systems requires a systematic treatment and cataloging of threats, vulnerabilities, technologies, controls, and operational environments. This chapter presents a threat tree for direct recording electronic (DRE) voting systems. The threat tree is organized as a hierarchy of threat actions, the goal of which is to exploit a system vulnerability in the context of specific technologies, controls, and operational environment. As an abstraction, the threat tree allows the analyst to reason comparatively about threats. A panel of elections officials, security experts, academics, election law attorneys, representatives from governmental agencies, voting equipment vendors, and voting equipment testing labs vetted the DRE threat tree. The authors submit that the DRE threat tree supports both individual and group risk assessment processes and techniques.

S. Srinivasan and S.P. Alampalayam explore the security capabilities of Mobile ad hoc networks (MANETs) in “Intrusion Detection Algorithm for MANET.” MANETs present the opportunity to connect transient nodes to the internet without having central control. This very design supports new nodes to join and leave the network based on their proximity to the MANET. Concurrently, it creates many security challenges for authenticating nodes that are not present in a traditional wired network. Much of the existing work on MANET security has focused on routing and mobility. In this chapter, the authors
present an algorithm that considers the neighboring nodes’ status to determine if a particular node is malicious or not. The authors used NS2 simulation tool to test the algorithm and present the results. The major benefits of this research work are in military applications.

Chapter 12, “An Integrated Security Governance Framework for Effective PCI DSS Implementation” by Mathew Nicho and Hussein Fakhry, analyses relevant IT governance and security frameworks/standards used in IT assurance and security to propose an integrated framework for ensuring effective PCI DSS implementation. Merchants dealing with credit cards have to comply with the Payment Card Industry Data Security Standards (PCI DSS) or face penalties for non-compliance. With more transactions based on credit cards, merchants are finding it costly and increasingly difficult to implement and interpret the PCI standard. One of the top reasons cited for merchants to fail PCI audit, and a leading factor in data theft, is the failure to adequately protect stored cardholder data. Although implementation of the PCI DSS is not a guarantee for perfect protection, effective implementation of the PCI standards can be ensured through the divergence of the PCI standard into wider information security governance to provide a comprehensive overview of information security based not only on security but also security audit and control. The primary contribution of this research is the development of an integrated comprehensive security governance framework for ‘information security’ (rather than data protection) incorporating Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and ISO 27002.

Next, Murthy V. Rallapalli, in “A Privacy Agreement Negotiation Model in B2C E-Commerce Transactions,” presents an alternate approach to effectively address the way privacy agreements are initiated through web services. In this new framework, the consumer and the service provider can mutually negotiate on the privacy terms. It contains a privacy model in which the transaction takes place after a negotiation between the service provider and the web user is completed. In addition, this framework would support various negotiation levels of the agreement lifecycle which is an important aspect of the dynamic environment of a B2C e-commerce scenario. A third party trusted agency and a privacy filter are included to handle privacy information of the web user. The author seeks to raise awareness of the issues surrounding privacy transactions and the potential ongoing impact to both service providers and clients as the use of web services accelerates.

The following chapter, “A Unified Use-Misuse Case Model for Capturing and Analysing Safety and Security Requirements” by O.T. Arogundade et al., proposes an enhanced use-misuse case model that allows both safety and security requirements to be captured during requirements elicitation. The proposed model extends the concept of misuse case by incorporating vulnerable use case and abuse case notations and relations that allows understanding and modeling different attackers and abusers behaviors during early stage of system development life cycle and finishes with a practical consistent combined model for engineering safety and security requirements. The model was successfully applied using health care information system gathered through the university of Kansas HISPC project. The authors were able to capture both security and safety requirements necessary for effective functioning of the system. In order to enhance the integration of the proposed model into risk analysis, the authors give both textual and detailed description of the model. The authors compare the proposed approach with other existing methods that identify and analyze safety and security requirements and discovered that it captures more security and safety threats.

As the nation confronts a growing tide of security breaches, the importance of having quality data breach information systems becomes paramount. Yet too little attention is paid to evaluating these systems. Chapter 15, “Evaluating the Quality and Usefulness of Data Breach Information Systems” by Benjamin
Ngugi, draws on data quality scholarship to develop a yardstick that assesses the quality of data breach notification systems in the U.S. at both the state and national levels from the perspective of key stakeholders, who include law enforcement agencies, consumers, shareholders, investors, researchers, and businesses that sell security products. Findings reveal major shortcomings that reduce the value of data breach information to these stakeholders. The study concludes with detailed recommendations for reform.

Finally, Hassen Sallay writes in “Wild-Inspired Intrusion Detection System Framework for High Speed Networks (φ|π) IDS Framework” that while the rise of the Internet and the high speed networks made information easier to acquire, faster to exchange and more flexible to share, it also made the cybernetic attacks and crimes easier to perform, more accurate to hit the target victim and more flexible to conceal the crime evidences. Although people are in an unsafe digital environment, they often feel safe. Being aware of this fact and this fiction, the authors draw a security framework aiming to build real-time security solutions in the very narrow context of high speed networks. This framework is called (φ|π) since it is inspired by the elephant self-defense behavior which yields π (22 security tasks for 7 security targets).

Hamid R. Nemati
The University of North Carolina at Greensboro, USA