Introduction

The main objective of this edited volume is to provide a broad coverage of technical as well as socio-economic perspectives of utilizing Information and Communication Technologies to provide practical solutions in Cyber Security, Cyber Crime and Cyber Forensics for a multitude of industrial applications. Recent developments in this domain have attracted researcher and practitioner interests from technological, organizational and policy-making perspectives. Technological advances address challenges in information sharing, surveillance and analysis. However, organizational advances are much needed in fostering collaborative arrangements between federal, state and local agencies as well as the private sector. Initiatives to strengthen security clearly benefit from well-designed policies that address developments in science & technology and collaborations between entities. Much of the literature in this area is fragmented and often narrowly focused within specific domains. This edited volume strives to address a wide range of perspectives in cyber security, cyber crime and cyber forensics. We have assembled insights from a representative sample of academicians and practitioners and addressed this topic from a variety of perspectives ranging from technologies, economics and social studies, organizational and group behavior, and policy-making.

Many of the chapters in this book are based on research and position papers presented at the Indo-US conference & workshop on cyber-security, cyber-crime and cyber-forensics held at Amrita Vishwa Vidyapeetham, Kochi, India in August 2009. This conference and workshop received over 100 papers on a wide-range of topics related to cyber security, cyber crime and cyber forensics. A select set of authors from the conference was asked to submit extended versions of their work for publication consideration in this Book. In addition to the peer-reviews conducted as part of the Indo-US conference, each chapter went through a peer-review process from the editors when it was submitted for the book chapter.

The chapters in the book are divided into three main sections – Cyber Crime: Policies and Implications, Cyber Security: Technology Review, and Cyber Security: Methods and Algorithms. The chapters addressing policies and implications are intended to address broad range of issues in the area. The chapters in this section discuss the significant challenges that governments and societies face when information access and usage becomes ubiquitous. The ubiquity raises legal challenges for business entities that engage with each other, and raises unique challenges for law enforcement and policy makers in designing new rules and policies and enforcing them. The chapters in the section, Cyber security: Technology Review, analyze the potential of emerging technologies for providing information assurance in the cyber world. The discussion here provides a good sample of various types of application contexts and
solutions. The section on Cyber Security: Methods and Algorithms dives deep into review and analysis of techniques and approaches that secure information at its fundamental level. Overall, the selection of chapters demonstrates the kind of multi-disciplinary research effort needed to address the wide range of challenges facing us today in the Information Age.

**INTENDED AUDIENCE & USE**

The intended audience for this book includes:

- Graduate and advanced undergraduate level students in Information Sciences, Information Systems, Computer Science, Systems Engineering, Social Studies, and Public Policy.
- Researchers engaged in cyber security related research from a wide range of perspectives including but not limited to informatics, decision sciences, organizational behavior and social studies, and public administration.

This book is intended for use as both a textbook and a comprehensive research handbook. The contributors to this edited volume are renowned experts in their respective fields. Most of the chapters contained in this book provide an updated comprehensive survey of the related field and also specific findings from cutting-edging innovative research.

**CHAPTER SUMMARIES**

**Cyber-Crime: Policies and Implications**

The first chapter in this Section by Chakraborthy, Rengamani, Kamaraguru and Rao The Unique Identification Number Project: Issues and Analysis discusses the unique ID project initiated in India recently. While similar types of citizen identification approaches have operated in other countries for a number of years (e.g., USA, UK, etc.), the population of India and geography present interesting and unique challenges in making this project a success. The authors present a comprehensive review of the technological, administrative and legal challenges. The enormous scale of this project prompts the authors to call for a unit specifically tasked with fighting cyber crime incidents.

The second Chapter in this section by Axelrod and Haldar Combined Impact of Outsourcing and Hard Times on BPO Risk and Security examines security risks of business process outsourcing. The authors argue that cyber risks in outsourced processes escalate when the general economic conditions worsen. Risk mitigation strategies related to provider viability, quality of service, loss of control, and other significant issues are discussed in detail in this Chapter.

The third chapter by Maheshwari, Hyman and Agrawal A Comparison of Cyber-crime Definitions in India and the United States tackle the inconsistent and often incompatible definitions of cyber crime in India and the United States. The impact of inconsistencies can be significant due to the increasing business relationships and information exchange between India and the United States. The authors draw a
distinction in the approach of United States, which treats cybercrimes by extending traditional criminal
codes, and India, which has passed a separate set of laws dedicated to addressing electronic commerce,
communication and information technology.

The fourth chapter in this section by Shankar, Agrawal and Rao *Emergency Response to Mumbai
Terror Attacks: An Activity Theory Analysis* presents a unique approach analyzing the use of Information
and Communication Technologies in a large-scale terrorist attack incident. Using activity theory based
analysis of the response by various law enforcement agencies, the authors examine the coordination
dimension requirements of emergency response that includes the concurrency and interdependence
dimensions.

The final chapter in this section by Chaudhury and Kang *Pirates of the Copyright and Cyberspace:
Issues Involved* explore the legal aspects of copyright violations in an inter-connected world. Protecting
intellectual property, especially digital works, is a vexing issue for governments across the world. A
big challenge is the myriad of legal frameworks and enforcement approaches. The authors suggest an
international dispute resolution system to handle copyright issues across national boundaries.

**Cyber Security: Technology Review**

The first chapter in this section by Ramachandran, Mundada, Bhattacharjee, Murthy and Sharma *Class-
sifying Host Anomalies: Using Ontology in Information Security Monitoring* argue for automating
information filtering in security environments to reduce the burden on security analysts. The authors
examine the feasibility of using an Ontology based approach to information filtering. An ontology based
approach allows explicit representation of domain knowledge and cause-effect relationship modeling.

The chapter by Talukder *Securing Next Generation Internet Services* defines next generation internet
services as “computer communication, telecommunication, or consumer entertainment services that
are user-agent agnostic, device agnostic, network agnostic, and location agnostic over Internet.” The
chapter argues that security must be defined at each of the seven levels of the Open Systems Interface
(OSI) model. The author presents a framework for defining security for next generation internet services.

Giuliani and Murty *An Examination of Identity Management Models in an Internet Setting* examine
the criteria for identity management systems and present arguments for better identity management
models for use on the Internet. A key aspect of the model is to move from a centralized system of identity
management to a federated model in which identity providers also play a role in transactions.

Continuing the theme of security in services oriented environments, Harini, Shyamala and Padmanab-
han *Securing Cloud Environment* present a review of challenges faced by adopters of cloud computing
technologies. A secure architecture framework is utilized to present the overarching security related
issues in this environment.

While the first four chapters discuss security issues in enterprise environments, Kaur, Gaur, Suresh
and Laxmi *DoS Attacks in MANETs: Detection and Countermeasures* focus specifically on mobile ad
hoc networks (MANETs). Ad hoc networks, by their very nature are vulnerable to denial of service
(DoS) attacks. The authors present an overview of DoS attacks and countermeasures using the protocol
stack as the underlying framework.

The Chapter by Virendra, Duan and Upadhyaya *Detecting Cheating Aggregators and Report Dropping
Attacks in Wireless Sensor Networks* tackle the issues of misaggregating and dropping attacks in wireless
sensor networks. The authors develop cryptographic techniques to address the security issues. A unique
contribution of this chapter is that unlike conventional reliability and security schemes, the security model is tunable to obtain a desired tradeoff between control overhead and the accuracy of detection.

Investigating cyber security related events require that systems store and process massive amounts of data. However, storing high volume data in heavy traffic environments is difficult, if not infeasible. To address this problem, Kumar, Prasad and Pilli Extended Time Machine Design using Reconfigurable Computing for Efficient Recording and Retrieval of Gigabit Network Traffic present the design and implementation of a system that efficiently records gigabit network traffic. The system features both dedicated hardware and application programming interface.

The final chapter in this section by Vinod, Laxmi and Gaur Metamorphic Malware Analysis and Detection Methods presents a survey of different malware identification techniques. A key distinguishing feature of metamorphic malware is that they mutate and generates new variants of the code that are structurally different from the original. The authors present a survey of metamorphic malware detection techniques and present directions for future research.

Cyber Security: Methods and Algorithms

The first Chapter by Narendra Kumar, Harshit Shah and Shyamasundar Towards Checking Tampering of Software surveyed issues, strategies and techniques that have been used to check tampering of software. It also discusses how semantic malware detection approach can be effectively applied to arrive at notions of birthmark.

The second Chapter in this section by Srinivasan, Lakshmy and Sethumadhavan Complexity Measures of Cryptographically Secure Boolean Functions discusses various complexity measures of cryptographically secure Boolean functions and the major tradeoffs between them, which will help to get an insight into study of such functions and to design stream ciphers.

The third Chapter by Narayanankutty and Achuthan Einstein-Podolsky-Rosen Paradox and Certain Aspects of Quantum Cryptology with Some Applications presents some factors preventing wider adoption of Quantum Cryptology outside high security areas. They include equipment costs, lack of demonstrated threat to existing key exchange protocols etc.

The fourth Chapter by Sindhu, Sajan Kumar and Sethumadhavan Error Linear Complexity Measures of Binary Multisequences presents two algorithms for finding the joint linear complexity of periodic binary m-fold multisequences and an algorithm for finding error multisequence which are extensions to the case of single sequence

The final Chapter by Amritha and Giresh Kumar A Survey on Digital Image Steganographic Methods provides a state of the art review of different existing embedding methods of steganography drawn from the literature and gives a survey on the usual struggle of steganographic methods with achieving a high embedding rate and good imperceptibility.

CONCLUDING REMARKS

Cyber security and cyber crime are at the center of research and practitioner interests in an increasingly inter-connected world. Information and communication technologies are embedded into the daily life of citizens and therefore the risks inherent in their use understood and acted upon by all stakeholders.
The main objective of this book is bringing attention to the multi-disciplinary approach needed to engage all stakeholders in a collaborative fashion. The contributing authors in this book have taken the initial steps to define and explore the underlying issues related to cyber security and cyber crime. We hope that this book continues to engage practitioners and researchers on this important topic.

*Raghu Santanam*  
*Arizona State University, USA*

*M. Sethumadhavan*  
*Amrita Vishwa Vidyapeetham, India*

*Mohit Virendra*  
*State University of New York at Buffalo, USA*