Preface

Today's network has quickly grown to be a critical resource for a variety of services as network sophistication has become increasingly complex than ever. User dependency and acceptance led to many new software packets and embedded applications have become the most extensively used tool for delivery of data services all over the WWW. As large data is being used in more important services, implementation and design of these applications is getting more and more complex. These activities has also induced many mischievous activities that try to take advantage of easy access to the Internet and associated user-centric solutions. User-centric solutions can target a wide range of applications, ranging from individual devices communicating with other connected devices, through to data-sharing in cloud computing and open grids on very powerful computing systems. The key factor in making user-centric solutions successful is ensuring peace of users' mind. To achieve this, the security, privacy and trust of the user-centric ecosystem must be ensured. This issue primarily concerns with security issues in the Internet and considers cryptographic approaches that try to take advantage of the frameworks for everyday personal computing devices, including smartphones, smart cards and sensors.

Internet security has become an independent branch of computer security dealing with the Internet, and often involves applications or operating systems on a whole besides browser security. The sole objective is to establish rules that can be used against potential attacks (Gralla, 2007). As the Internet offers an insecure channel for swapping information, leading to a great risk of invasion or scam (Rhee, 2003). Recent introduction of IoT (Internet of Things) has further enhanced its usefulness as well added new ways of attacking distributed storage system in the cloud. The main objective of the book is to provide relevant theoretical frameworks and latest empirical research findings in the area. It has been targeted for professionals who want to improve their understanding of the basic principles, underlying challenges and potential applications of computer and cyber security. The book is helpful in identifying interesting and exciting areas where these techniques can be applied for future research. In addition, it is an excellent reference book in teaching a course on computer and cyber security. The material is expected to prepare students in terms of understanding the motivation of the attackers, exercising schemes for enhanced protection, and how to deal with and mitigate the situation in an efficient and effective way.

In each communication session between two entities, Internet Protocol Security (IPsec) protocol suite (Thayer, Doraswamy, & Glenn, 1998) is used for authentication and encryption of each IP (Internet Protocol) packet. IPsec supports network-level peer authentication, data origin authentication, data integrity, data encryption, and replay protection. IPsec uses the following protocols to perform various functions such as Authentication Headers (AH), Encapsulating Security Payloads (ESP), and Security Associations (SA). AH guarantees connectionless reliability and data origin confirmation of IP packets and protects against replay attacks by discarding old packets. ESP provides origin authenticity, integrity

and confidentiality protection of packets. SA serves as the basis for building security functions into IP by bundling algorithms and parameters used for encryption and authentication of a particular flow. IPsec can be incorporated both in a host-to-host passage mode, as well as in a network tunneling mode. In transport mode, the IP header is neither modified nor encrypted and only the payload of the IP packet is usually encrypted. In tunnel mode used to create virtual private networks, the entire IP packet is encrypted and encapsulated into a new IP packet. Security-attack is any type of unfriendly exercise employed by individuals that targets Internet or IoT (https://en.wikipedia.org/wiki/Cyber-attack) by various means of nasty acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system and can be labeled as either a Cyber campaign, cyber-warfare or cyber-terrorism. Cyber-attacks can range from installing spyware on a PC and have become increasingly sophisticated and dangerous (Karnouskos, 2011).

A number of different techniques can be utilized in cyber-attacks and are broken down into Syntactic and Semantic attacks. Syntactic attacks contain malicious software including viruses, worms, and Trojan horses and can be handled in a straight forward manner. Semantic attack involves variation and propagation of improper information. Once a cyber-attack is initiated, certain targets (Linden, 2007) such as control systems, energy resource, finance, telecommunications, transportation, and water facilities are crippled by the opponent. Various susceptibilities are possible to compromise an individual's delicate data and excellent steps have been summarized as follows (https://msdn.microsoft.com/en-us/library/cc750215.aspx):

- Monitor networks boundaries for attacks.
- Ensure that routers are not converting layer 3 broadcasts into layer 2 broadcasts.
- Restrict routers to allow only the use of ports that are necessary for the site to function.
- Disable unnecessary or optional services.
- Enable TCP/IP filtering and restrict access to only necessary ports.
- Unbind Network Basic Input/Output System over TCP/IP where it is not needed.
- Configure static IP addresses and parameters for public adapters.
- Configure registry settings for maximum protection.
- Follow the steps for configuring Windows NT and Internet Information Services.

In spite these excellent suggestions, intruder always find their way to create problems for a generic user. This book contains chapters dealing with different aspects of cyber-security. These include fundamentals, overviews, and trends in Cyber Security, IoT and both wired and wireless systems, Security and privacy in ad hoc networks, Security and privacy in wireless sensor networks Cyber risk and vulnerability assessment, Business & Management, Medicine & Healthcare Public Administration. Security & Forensics Social Science, Visual analytics for cyber security, Security and privacy in social applications and networks, Critical infrastructure protection, Security and privacy in industrial systems, Security and privacy in pervasive/ubiquitous computing, Intrusion detection and prevention, Botnet detection and mitigation, Security and privacy using DNA sequence, Biometric security and privacy, Security and privacy in cloud computing, Human factors in security and privacy, Cybercrime and warfare, Security and privacy in cloud computing, Network security and management, Cyber threats, Security in IoT, and social media Security.

In Chapter 1, authors present the issues of security and privacy of a network in great detail by discussing countermeasures for different kinds of attacks. They separately discuss privacy and its importance also known as network anonymity that is usually achieved by employing redundancy at the cost of some associated overheads. They start off with the introduction of the basic idea in data security, then discuss available standards for different types of networks and powerful tools like Encryption. From there, they build up to known types of attacks and a brief study of major data breaches of recent times. They also discuss various experimental measures and proposed solutions. They end the chapter with their projections on data security and the summarize what to expect in future.

In Chapter 2, authors study the privacy-preserving data publishing problem on a mobile social network. Along a propagation path, a series of tables will be locally created at each participant, and the tables' privacy-levels should be gradually enhanced. However, the tradeoff between these tables' overall utility and their individual privacy requirements are not trivial: any inappropriate sanitization operation under a lower privacy requirement may cause dramatic utility loss on the subsequent tables. For solving the problem, the authors propose an approximation algorithm by previewing the future privacy requirements. Extensive results show that this approach successfully increases the overall data utility, and meet the strengthening privacy requirements.

In Chapter 3, authors present a survey which analyzes and compares the most important efforts carried out in an application-based detection area and extended to cover the mitigation approaches for the Botnet-based DDoS flooding attacks. It accomplishes four tasks: first, an extensive illustration on Internet Security; second, an extensive comparison between representative detection mechanisms; third, the comparison between the mitigation mechanisms against Botnet-based DDoS flooding and fourth, the description of the most important problems and highlights in the area. They concluded that the area has achieved great advances so far, but there are still many open problems.

Chapter 4 focuses on the cyber risk issue. The authors aim to describe the global state of the art and point out the potential negative consequences of this type of systemic risk. Cyber risk increasingly affects both public and private institutions. Some of the risks that entities face are the following: computer security breaches, cyber theft, cyber terrorism, cyber espionage. Developed nations but also emerging markets suffer from cyber risk. It is therefore important to examine the different security regulation implemented across different markets. Moreover, cyber risk is a concern for all economic sectors. In particular, it is a crucial issue in banking sector because of the negative effects of cyber attacks, among others, the financial losses and the reputational risk. However, the awareness is increasing and cyber insurance is growing.

Chapter 5 illustrates the general characteristics of ad hoc networks and computing models that make obligatory to design secure protocols in such environments. Further, authors present a generic classification of various threats and attacks. In the end, they describe the security in MANETs, VANETs and cloud computing. The chapter concludes with a description of tools that are popularly used to analyze and access the performance of various security protocols.

In Chapter 6, authors propose a hybrid neural tree model to enhance the performance of the AQM steganalyser. Practically, false negative errors are more expensive than the false positive errors, since they cause a greater loss to organizations. The proposed neural model is operating with the cost ratio of false negative errors to false positive errors of the steganalyser as the activation function. Empirical results show that the evolutionary neural tree model designed based on the asymmetric costs of false negative and false positive errors proves to be more effective and provides higher accuracy than the basic AQM steganalyser.

Chapter 7 presents an introduction of Petri nets, its applications and security challenges. Petri nets are a graphical and mathematical modeling tool available to many systems. Once a system is modeled as a Petri net, the behavior of the system can be simulated by using tokens on the Petri net. Petri nets' abundant techniques can be used to solve many problems associated with the modeled system. Moreover, this chapter gives formal definitions, properties and analysis methods of Petri nets, and gives several examples to illustrate some basic concepts and successful application areas of Petri nets. Furthermore, this chapter presents Petri nets based challenges to security such as Intrusion Detection System, security policy design and analysis, and cryptography tool.

In Chapter 8, authors describe a method for detecting periodic communications by analyzing network flows for security monitoring. In particular they use a clustering technique to identify periodic communications between hosts. They performed various experiments with both simulated and real world data to evaluate the efficacy of method.

In Chapter 9, authors present a thorough survey on the secure and privacy preserving keyword search over large scale cloud data. They investigate existing research arts category by category, where the category is classified according to the search functionality. In each category, they first elaborate on the key idea of existing research works, then they conclude some open and interesting problems.

In Chapter 10, authors discuss the detailed incidences of XSS attacks in the recent period on the platforms of OSN. A high level of taxonomy of XSS worms is illustrated in this article for the precise interpretation of its exploitation in multiple applications of OSN like Facebook, Twitter, LinkedIn, etc. They have also discussed the key contributions of current defensive solutions of XSS attacks on the existing frameworks of OSN. Based on this study, authors identified the current performance issues in these existing solutions and recommend future research guidelines.

In Chapter 11, authors discuss the basic concepts of digital watermarking techniques, performances parameters and its potential applications in various fields. In addition, they also discuss various spatial and transform domain techniques and compare the performance of some reported wavelet based watermarking techniques. Finally, the latest applications of watermarking techniques have been discussed.This chapter will be more important for researchers to implement effective watermarking method.

In Chapter 12, authors discuss various security issues and countermeasures of online transaction in E-commerce. Moreover, E-commerce security must ensure the major security features of cryptography: privacy, authentication, access control, confidentiality and protect data from un-authorized access. In addition, authors cover all aspects regarding e-commerce from its introduction to its security, countermeasures and an example of doing secure payment from any website.

In Chapter 13, authors introduces techniques wherein secure communication between humans and their surrounding devices can be facilitated by applying human physiological information as the identifying factor. Different biometric techniques are investigated, and the rationale behind their applicability is argued. Additionally, the benefits and possible use-cases for each technique are presented, and the associated open research problems are brought to light.

In Chapter 14, author discusses provable security for public key cryptosystems and explains how to prove that the cryptosystem is secure. There are two general approaches for structuring the security proof. One is reductionist approach and other is game-based approach. In these approaches the security proofs provides the polynomial time algorithm to reduce a well known problem (such as discrete logarithm, RSA) to an attack against a proposed cryptosystem. With this approach the security of public key cryptosystem can be prove formally under the various models viz. random oracle model, generic group

model and standard model. Furthermore, authors explain these approaches along with the security proofs of well known public key cryptosystems under the appropriate model.

In Chapter 15, authors discuss that CPS has bridged the gap between physical world to the cyber world. It is envisioned that wireless sensor networks (WSN) plays an important role in the actuality of CPS. Due to wireless communication in WSN, it is more vulnerable to security threats. Key establishment is an approach, which is responsible for establishing a session between two communicating parties and therefore, a lightweight key establishment scheme is essential. In addition, authors present state of the art review of these solutions by discussing key establishment in WSN. Also, a discussion has been carried out to capture few challenges in implementing them in real and future research directions in this area are explored to transport the field to an improved level.

In Chapter 16, authors propose a security threat classification model which allows to study the threats class impact instead of a threat impact as a threat varies over time. Moreover, this chapter deals with the threats classification problem and its motivation. It addresses different criteria of information system security risks classification and gives a review of most threats classification models. In addition, in this paper, authors present recent surveys on security breaches costs.

In Chapter 17, authors discuss recent developments in cloud computing, various security issues and challenges associated with Cloud computing environment, various existing solutions provided for dealing with these security threats and provide a comparative analysis of these approaches. This provide better understanding of the various security problems associated with the cloud, current solution space, and future research scope to deal with such attacks in better way.

Chapter 18 addresses the issues caused by hanging pages in Web computing. This Chapter has four important objectives. First, authors compare and review the different types of link structure based ranking algorithms in ranking Web pages. PageRank is used as the base algorithm throughout this Chapter. Second, authors present study on hanging pages, explore the effects of hanging pages in Web security and compare the existing methods to handle hanging pages. Third, authors present the study on Link spam and explore the effect of hanging pages in link spam contribution and lastly, they discuss their study on Search Engine Optimization (SEO) / Web Site Optimization (WSO) and explore the effect of hanging pages in Search Engine Optimization (SEO).

In Chapter 19, authors present a review of various face recognition techniques in video for biometric security and discuss the emerging trends of the research in this area. The primary focus of the authors is to summarize some well-known methods of face recognition in video sequences for application in biometric security and enumerate the emerging trends.

Chapter 20 summarizes various security models and techniques that are being discovered, studied and utilized extensively in order to ensure computer security. It also discusses numerous security principles and presents the models that ensure these security principles. Security models (such as access control models, information flow models, protection ring, etc.) form the basis of various higher level and complex models. Therefore, learning such security models is very much essential for ensuring the security of the computer and cyber world.

In Chapter 21, authors present a DNA Sequence based cryptographic solution for secure image transmission. The concept of using DNA Cryptography has been identified as a possible technology that brings forward a new hope for unbreakable algorithms as traditional cryptographic systems are now vulnerable to certain attacks. Therefore, this chapter outlines a hybrid encryption scheme based on DNA sequences.

B. B. Gupta
National Institute of Technology Kurukshetra, India

Dharma P. Agrawal
University of Cincinnati, USA

Shingo Yamaguchi
Yamaguchi University, Japan

REFERENCES

Gralla, P. (2007). *How the internet works*. Indianapolis, IN: Que Pub.

Karnouskos, S. (2011). *Stuxnet worm impact on industrial cyber-physical system security*. Paper presented at the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia. doi:10.1109/IECON.2011.6120048

Linden, E. (2007). *Focus on terrorism*. New York: Nova Science Publishers, Inc.

Rhee, M. Y. (2003). *Internet security: Cryptographic principles, algorithms and protocols*. Chichester, UK: Wiley.

Thayer, R., Doraswamy, N., & Glenn R. (1998). *IP security document roadmap*. IETF- RFC 2411.