Preface

The field of cyber security has assumed utmost importance in today's information age. Cyber security encompasses both information and network security. Information security covers the understanding of security requirements, classification of threats, attacks, and information protection systems and methodologies. Encryption is a key enabling technology for data and information security. Network security, on the other hand, includes both security protocols as well as systems, which create a security perimeter around networks for intrusion detection and avoidance. Network security protocols combine encryption and several related mechanisms, like hashing and digital signatures, along with procedures for key and session management, which allow for parties to establish secure communication links over otherwise insecure communication networks and exchange private information such as personal and financial data.

As part of proactive information security, Security Information Management (SIM) systems are set up by those tasked with managing information security in their respective organizations. These systems consolidate and analyze the information system usage logs in near real-time for alerting and in off-line mode for demonstrating system security and compliance to standards and regulations. At this time real-time audio, video, and instant messaging systems are used ubiquitously over integrated and converged public communication networks. Their security requirements include protection against eavesdropping and end to end authentication. To this end security protocols such as Secure Real Time Protocol (SRTP) for streaming media security have been developed by the Internet Engineering Task Force (IETF).

Cyber security of industrial manufacturing and utility industries, such as power, water, and gas, has assumed national defense status. Most industries, including power generation and manufacturing, use PLC's (programmable logic controllers) that are connected to computers for remote control. SCADA and industrial systems security includes protection of SCADA control units or industrial equipment in production, power generation & distribution, fabrication, refining, public and private infrastructure institutions, and large communication systems. The area of industrial and infrastructure security is very important and various governments have mandated the compliance by all institutions and services to many security regulations.

This book aims to provide a comprehensive reference in cyber security covering all important topics including encryption, authentication, integrity, security infrastructure, and protocols. It covers areas that pertain to digital information encryption techniques, secure networking protocols, security management systems, and industrial and SCADA security standards. We believe that it would not only serve as a reference for existing technologies, it would also become a reference for innovation in this field. It would serve a broad audience including researchers and practitioners in cyber and industrial security, e-commerce and web security experts, academicians, students, and working professionals in utilities, manufacturing, municipal services, government, defense, and networking companies.

Wireless technologies are bringing significant changes to data networking and telecommunication services, making integrated networks a reality. By removing the wires, personal networks, local area networks, mobile radio networks and cellular systems, offer an entirely distributed mobile computing and communications environment. Due to their unique features such as shared medium, limited resources, and dynamic topology, wireless ad hoc networks are vulnerable to a variety of potential attacks. However, the common security measures employed for wired networks are not enough to protect the nodes of the networks against complex attacks. Therefore, a new line of defense, called intrusion detection, has been added. In the first chapter the main wireless technologies are introduced along with their characteristics. Then, a description of the attacks that can be mounted on these networks is given. A separate section reviews and compares the most recent intrusion detection techniques for wireless ad hoc networks. Finally, based on the current state of the art, the conclusions and major challenges are discussed.

Handheld devices like smartphones must include rigorous and convenient handheld data protection in case the devices are lost or stolen. The second chapter proposes a set of novel approaches to protecting handheld data by using mobile usage pattern matching, which compares the current handheld usage pattern to the stored usage patterns. If they are drastically different, a security action such as requiring a password entry is activated. Various algorithms of pattern matching may be used. Two of them discussed in the chapter are (i) approximate usage string matching and (ii) usage finite automata. The first method uses approximate string matching to check device usage and the second method converts the usage tree into a deterministic finite automaton (DFA). Experimental results show this method is effective and convenient for handheld data protection, but the accuracy may need to be improved.

An important part of ISO/IEC 27002 cyber security standard is the conservation of confidentiality that falls under its computer facility protection part which insures that the computer and its stored information can only be accessed by the authorized users. Securing mobile devices and mobile data to ensure the confidentiality, integrity, and availability of both data and security applications requires special consideration to be paid to the typical mobile environment in which a mobile computing device would be utilized. Protecting mobile devices includes multiple security technologies such as the right identification of its particular user, data encryption, physical locking devices, monitoring and tracking software, and alarms. Chapter 3 reviews security-specific hardware and software applied to mobile computing and presents its advantages and drawbacks. Then it considers the concept of usability constraints in context of mobile computing security and introduces the seamless security method for identity proof of a particular user or device.

Social media is transforming the way we find, create, and share information during the course of our personal life and work. The rapid growth of social media and the ubiquitous sharing and access of information through various digital channels has created new vulnerabilities and cyber threats. Chapter 4 provides an overview of the security and privacy implications of social networks and communities. It examines and raises awareness about cyber security threats from social media, to describe the state of technology to mitigate security risks introduced by social networks, to shed light on standards for identity and information sharing or lack thereof, and to present new research and development. The chapter will serve as a reference to students, researchers, practitioners, and consultants in the area of social media, cyber security, and Information and Communication Technologies (ICT).

The Internet, originally designed in a spirit of trust, uses protocols and frameworks that are not inherently secure. This basic weakness is greatly compounded by the interconnected nature of the Internet, which, together with the revolution in the software industry, has provided a medium for large-scale exploitation, for example, in the form of botnets. Despite considerable recent efforts, Internet-based

attacks, particularly via botnets, are still ubiquitous and have caused great damage on both national and international levels. Chapter 5 provides a brief overview of the botnet phenomena and its pernicious aspects. Current governmental and corporate efforts to mitigate the threat are also described, together with the bottlenecks limiting their effectiveness in various countries. The chapter concludes with a description of lines of investigation that could counter the botnet phenomenon.

Due to the rapidly evolving nature of network attacks, a considerable paradigm shift has taken place with focus now on Network-based Anomaly Detection Systems (NADSs) that can detect zero-day attacks. At this time, it is important to evaluate existing anomaly detectors to determine and learn from their strengths and weaknesses. Chapter 6 aims to evaluate the performance of eight prominent network-based anomaly detectors under malicious portscan attacks. These NADSs are evaluated on three criteria: accuracy (ROC curves), scalability (with respect to varying normal and attack traffic rates, and deployment points), and detection delay. Based on experiments, promising guidelines are identified to improve the accuracy and scalability of existing and future anomaly detectors. It is shown that the proposed guidelines provide considerable and consistent accuracy improvements for all evaluated NADSs.

Quantum cryptography holds the promise of unbreakable encryption systems and is based in using photons. In chapter 7 the author presents a method to estimate parameters of the decoy state protocol based on one decoy state protocol for both BB84 and SARG04. This method can give different lower bound of the fraction of single-photon counts, the fraction of two-photon counts, the upper bound QBER of single-photon pulses, the upper bound QBER of two-photon pulses, and the lower bound of key generation rate for both BB84 and SARG04. The effects of statistical fluctuations on some parameters of our QKD system have been presented. We have also performed the optimization on the choice of intensities and percentages of signal state and decoy states which give out the maximum distance and the optimization of the key generation rate. The numerical simulation has shown that the fiber based QKD and free space QKD systems using the proposed method for BB84 are able to achieve both a higher secret key rate and greater secure distance than that of SARG04. Also, it is shown that bidirectional ground to satellite and inter-satellite communications are possible with this protocol. The experiment of decoy state QKD has been demonstrated using ID-3000 commercial QKD system based on a standard 'Plug & Play' set-up. One decoy state QKD has been implemented for both BB84 and SARG04 over different transmission distance of standard telecom fiber.

Designing and implementing security protocols are known to be error-prone tasks. Recent research progress in the field of formal methods applied to security protocols has enabled the use of these techniques in practice. The authors' objective in chapter 8 is to give a circumstantial account of the state-of-the-art reached in this field, showing how formal methods can help in improving quality of security protocols. Since automation is a key factor for the acceptability of these techniques in the engineering practice, the chapter focuses on automated techniques and illustrates in particular how high-level protocol models in the Dolev-Yao style can be automatically analyzed and how it is possible to automatically enforce formal correspondence between an abstract high-level model and an implementation.

Not long ago, it was thought that only software applications and general purpose digital systems i.e. computers were prone to various types of attacks against their security. The underlying hardware, hardware implementations of these software applications, embedded systems, and hardware devices were considered to be secure and out of reach of these attacks. However, during previous few years, it has been demonstrated that novel attacks against the hardware and embedded systems can also be mounted. Not only viruses, but worms and Trojan horses have been developed for them, and they have also been demonstrated to be effective. Whereas a lot of research has already been done in the area of security

of general purpose computers and software applications, hardware and embedded systems security is a relatively new and emerging area of research. Chapter 9 provides details of various types of existing attacks against hardware devices and embedded systems, analyzes existing design methodologies for their vulnerability to new types of attacks, and along the way describes solutions and countermeasures against them for the design and development of secure systems.

A Supervisory Control and Data Acquisition (SCADA) system is composed of number of remote terminal units (RTUs) for collecting field data. These RTUs send the data back to a master station, via a communication network. The master station displays the acquired data and allows the operator to perform remote control tasks. An RTU is a microprocessor based standalone data acquisition control unit. As the RTUs work in harsh environment, the processor inside the RTU is susceptible to random faults. If the processor fails, the equipment or process being monitored by it will become inaccessible. Chapter 10 proposes a fault tolerant scheme to untangle the RTU's failure issue. According to the scheme, every RTU will have at least two processing elements. In case of either processor's failure, the surviving processor will take over the tasks of the failed processor to perform its tasks. With this approach, an RTU remain functional despite the failure of the processor inside the RTU. Reliability and availability modeling of the proposed fault tolerant scheme have been presented. Moreover, cyber security for SCADA system and recommendations for the mitigation of these issues have been discussed.

The world's critical infrastructure includes entities such as the water, waste water, electrical utilities, and the oil and gas industry. In many cases, these rely on pipelines that are controlled by supervisory control and data acquisition (SCADA) systems. SCADA systems have evolved to highly networked, common platform systems. This evolutionary process creates expanding and changing cyber security risks. The need to address this risk profile is mandated from the highest government level. Chapter 11 discusses the various processes, standards, and industry based best practices that are directed towards minimizing these risks.

C4ISR stands for Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance. C4ISR systems are primarily used by organizations in the defense sector. However, they are also increasingly being used by civil sector organizations such as railways, airports, and oil and gas exploration departments. The C4ISR system is a system of systems and it can also be termed as network of networks and works on similar principles as the Internet. Hence it is vulnerable to similar attacks called cyber attacks and warrants appropriate security measures to save it from these attacks or to recover if the attack succeeds. All of the measures put in place to achieve this are called cyber security of C4ISR systems. Chapter 12 gives an overview of C4ISR systems focusing on the perspective of cyber security warranting information assurance.

A rapidly changing face of Internet threat landscape has posed remarkable challenges for security professionals to thwart their IT infrastructure by applying advanced defensive techniques, policies, and procedures. Today, nearly 80% of total applications are web-based and externally accessible depending on the organization policies. In many cases, number of security issues discovered not only depends on the system configuration but also the application space. Rationalizing security functions into the application is a common practice but assessing their level of resiliency requires structured and systematic approach to test the application against all possible threats before and after deployment. The application security assessment process and tools presented in Chapter 13 are mainly focused and mapped with industry standards and compliance including PCI-DSS, ISO27001, GLBA, FISMA, SOX, and HIPAA, in order to assist the regulatory requirements. Additionally, to retain a defensive architecture, web application firewalls have been discussed and a map between well-established application security standards (WASC, SANS, OWASP) is prepared to represent a broad view of threat classification.

With a wide variety of current topics in Cyber Security treated in this handbook we hope it proves to be a suitable reference to the topics which are covered in various chapters. We hope you have as much pleasure and intellectual fulfillment in reading these chapters as we have had in editing and managing their evolution from original single page chapter proposals to final camera ready drafts that constitute the handbook that you hold.

Junaid Ahmed Zubairi
State University of New York at Fredonia, USA

Athar Mahboob
National University of Sciences & Technology, Pakistan