Information Assurance and Security

J.UCS Special Issue

Ajith Abraham
(Chung-Ang University, Seoul, Korea, ajith.abraham@ieee.org)

Johnson Thomas
(Oklahoma State University, Tulsa, USA, jpt@cs.okstate.edu)

Sugata Sanyal
(Tata Institute of Fundamental Research, India, sanyal@tifr.res.in)

Lakhmi Jain
(University of South Australia, Australia, lakhmi.jain@unisa.edu.au)

The global economic infrastructure is becoming increasingly dependent upon information technology, with computer and communication technology being essential and vital components of Government facilities, power plant systems, medical infrastructures, financial centres and military installations to name a few. Finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. The First International Symposium on Information Assurance and Security (IAS'04) which was organized in conjunction with the 2004 IEEE International Conference on Information Technology Coding and Computing (ITCC'04) attracted information security experts representing various problem domains. This special issue comprising of 11 papers present some of the cutting edge research results on security issues such as authentication and authorization, data and system protection and integrity, steganography, security models, risk analysis, cryptography, secure e-commerce protocols, agent and mobile code security, wireless networks security, database security to computer forensics, information quality assurance, internet security and intrusion detection. Papers were selected on the basis of fundamental ideas/concepts rather than the thoroughness of techniques deployed. The papers are organized as follows.

Wireless local area networks are increasingly popular as they are easy to deploy at low cost. Unfortunately, they are easily vulnerable to attacks since their signals can be detected by eavesdroppers at great distances. Wireless Intrusion Detection Systems (WIDS) provides a security framework by combining intrusion detection with physical location detection using directional antennas. Adelstein *et al*. in the first paper illustrate the performance of WIDS using inexpensive hardware.

Digital forensics involves collection and analysis of digital data within an investigative process and the key challenge here is the collection of data in the least intrusive manner. In the second paper, Sitaraman and Venkatesan present a checkpoint methodology for a disk that has a Unix-like file system. The task is to record a checkpoint of a disk drive mounted as a file system on a host machine

without disrupting the disk's normal operations. The proposed algorithm can be used to checkpoint disks formatted for other file systems such as NTFS etc.

Security in mobile ad hoc networks is a difficult problem as these networks are infrastructureless, have arbitrary movement and possess scarce resources and limited power. Existing ad hoc routing protocols are either unicast or multicast. Khor *et al*. propose a sliding window protocol which is a simple extension to the Dynamic Source Routing Protocol (DSR) to cater for group communications where all nodes addresses are unicast addresses and there is no single multicast address. It is found that that the sliding window protocol improves both communications and security performance.

Multimedia data hiding techniques have developed a strong basis for the steganography area with a growing number of applications like digital rights management, hiding executables for access control, annotation etc. In the fourth paper, Nedeljko and Seppänen present a novel high bit rate LSB audio watermarking method that reduces embedding distortion of the host audio. Using the proposed algorithm watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition. Listening tests also showed that the watermarked audio has a better perceptual quality than the standard LSB method.

Most cryptography systems are based on the modular exponentiation to perform the non-linear scrambling operation of data. It is performed using successive modular multiplications, which are time consuming for large multiplicands. Nedjah and Mourelle proposes a genetic algorithm approach to yield the minimum sequence of powers, generally called an addition chain, that needs to be computed to finally obtain the modular exponentiation result. The authors also present a co-design methodology to engineer a cryptographic device that accelerates the encryption/decryption throughput without requiring considerable hardware area.

There are several applications that rely on encryption services provided by cryptographic protocols to ensure confidentiality, integrity, and authentication during secure transactions over the network. Joglekar and Tate in the sixth paper present an anomaly based intrusion detection system '*ProtoMon*' for detecting malicious use of cryptographic and application level protocols. Some of the unique characteristics of '*ProtoMon*' are the ability to monitor cryptographic protocols and application level protocols in encrypted sessions, a very light weight monitoring process and the ability to react to protocol misuse by modifying protocol response directly.

Security of network communications is arguably the most important issue in the world today given the vast amount of valuable information that is passed around in various networks. Vasudevan *et al*. present a novel encryption-less algorithm to enhance security in transmission of data in networks. The algorithm is based on the simple idea of a '*jigsaw*' puzzle to break the data into multiple parts where these parts form the pieces of a puzzle. These parts are packaged into packets and sent to the receiver. The algorithm is designed to provide information-theoretic security by the use of a one-time pad like scheme so that no intermediate or untended node can obtain the entire data. An authentication code is also used to ensure authenticity of every packet and a parallelizable design has been adopted for the implementation.

Protecting digital content from illegal copying and distributing is one of the key issues worrying owners and distributors in the digital world. In the eighth paper, Veerubhotla *et al*. present two new construction techniques for q-ary gossip codes

from t-designs and traceability schemes. The proposed gossip codes achieve the shortest code length specified in terms of code parameters and can withstand erasures in digital fingerprinting applications. Some discussions related to the construction of concatenated codes and realization of erasure model through concatenated codes is also provided in the paper.

In networks which share huge amounts of confidential and shared data, policies are the means by which security rules are defined and enforced. The ability to evaluate policies is becoming more and more relevant, especially when referred to the cooperation of services belonging to un-trusted domains. Casola *et al*. presents a reference model for security level evaluation based on fuzzy techniques to characterize a policy. The reference evaluation model represents different security levels and different policies are evaluated and compared. The framework is validated using a case study.

Electronic goods delivery over the Internet is a business process where a commodity or service is exchanged for its electronic payment or an acknowledgement of its receipt from a customer. In the tenth paper, Nenadić *et al*. propose an efficient security protocol for certified e-goods delivery with several important features.

Information quality assurance under the existence of uncertainty can be investigated in the context of soft security, where an agent maintains trustworthiness evaluations of its information sources to assist in the evaluation of incoming information quality from those sources. Since dependency inherently exists in a system where agents do not have self-sufficient sensing or data collection capabilities, finding an appropriate set of information sources is important for assuring the quality of information and for increasing the agent's goal achievement. In the last paper, Park and Barber propose an approach for selecting information sources as partners. Authors used trustworthiness, information cost and goal coverage as the metrics for information valuation while adopting a lazy exploration of information sources combination space.

The editors wish to thank Professor Hermann Maurer (Managing Editor) and Ms. Dana Kaiser (Assistant Editor) of The Journal of Universal Computer Science (J.UCS) for all the help and providing the opportunity to edit this special issue on Information Assurance and Security (IAS). We would also like to thank all our referees who have critically evaluated the papers within the short stipulated time. Finally we hope the reader will share our joy and find this special issue very useful and informative.

December 15, 2004

Ajith Abraham, *Seoul, S. Korea*
Johnson Thomas, *Tulsa, USA*
Sugata Sanyal, *Mumbai, India*
Lakhmi Jain, *Adelaide, Australia*