Guest Editorial
Part 1: Special Issue on Secure Knowledge Management

KNOWLEDGE management is the methodology for systematically gathering, organizing, and disseminating information. It essentially consists of processes and tools to effectively capture and share data as well as use the knowledge of individuals within an organization. Knowledge-management systems (KMSs) promote sharing information among employees and should contain security features to prevent any unauthorized access. Security is becoming a major issue revolving around KMS. Security methods may include authentication or passwords, cryptography programs, intrusion-detection systems, or access-control systems. Issues include insider threat (protecting from malicious insiders), infrastructure protection (securing against subversion attacks) and establishing correct policies and refinement and enforcement. Furthermore, KMS content is much more sensitive than a raw data stored in databases and issues of privacy also become important.

Since the attacks on September 2001, many organizations, especially the U.S. government, have increased their concern about KMS. With the advent of intranets and web access, it is even more crucial to protect a corporate knowledge as numerous individuals now have access to the assets of a corporation. Therefore, we need effective mechanisms for securing data, information, and knowledge, as well as the applications. The purpose of this special issue is to serve researchers, designers, and implementers of secure knowledge management, with emphasis on security, privacy and content management. It is anticipated that this special issue will help in raising the awareness of academics and practitioners in this critical area and develop important questions that need to be tackled by the research community.

The theme of this special issue coincides with the First National Science Foundation/Air Force Research Laboratory (NSF/AFRL) sponsored Workshop on Secure Knowledge Management held at Buffalo, NY, 2004, but the topics and submissions were not restricted to the proceedings of this workshop. The workshop received 55 submissions of which a total of 25 were chosen for presentation. Subsequently, we received a total of 17 submissions, several of which (but not all) had been vetted at the workshop. We finally selected six regular papers and two Transactions Briefs. Every submission was sent to at least three referees. We received a total of 55 reviews back and papers needing a major revision were sent out for a second round of review. A paper with results of a Delphi survey done mostly on the attendees of the SKM workshop is included as Part II of the editorial of this special issue.

Although, we would have liked to have a good mix of current, successful efforts, and innovative ideas on secure knowledge management—both conceptual and experimental, the space limitation in the special issue and the type of submissions we received may have precluded some key topics of secure knowledge management. Yet, we believe that the special issue encompasses major topics of secure knowledge management. The selected papers are classified into four groups: 1) security policies and access control; 2) trust management; 3) business perspectives on secure knowledge management; and 4) privacy preserving data sharing and dissemination. Many of these are areas of considerable growth in the years to come and we hope that this special issue will set the pace for the design and implementation of secure KMSs.

The first three papers belong to the "security policies and access control" and "trust management" themes. The paper "Secure Knowledge Management" by E. Bertino, L. Khan, R. Sandhu, and B. Thuraisingham provides an overview of secure knowledge management including such components as security strategies, metrics, processes, technologies, and techniques. The paper also focuses on three important aspects of secure knowledge management: confidentiality, trust, and privacy management. The authors discuss the three aspects of secure knowledge management in detail by investigating prominent access-control techniques, such as role-based access control (RBAC) and usage control (UCON), and by exploring trust management and privacy control. The second paper "Security Policies for Sharing Knowledge in Virtual Communities" by G. Boella and L. van der Torre puts forward a model of policies for distributed secure knowledge management. Adopting a normative multiagent systems approach, the model attempts to strike a balance between local autonomy and global policy for a multiinstitutional set of agents in a virtual community. The paper provides insight that can help address two important issues in distributed KMSs: how to maintain local access control to an individual participant's knowledge while conforming global security rules and how to specify duties and permissions of local authorities in the rules of policies for a virtual community of multiinstitutional agents. The third paper "Trust Management and Theory Revision" by J. Ma presents a methodology for revising theories of trust for the multiagent systems. The main contributions of the paper are a methodology for modeling the dynamics of trust for agent-based systems, and techniques to obtain evolving theories for agent-based systems in dynamic environments. The new theory developed in this

Digital Object Identifier 10.1109/TSMCA.2006.871643

paper will play an important role in expressing and reasoning about agent beliefs and security properties of systems in a changing environment.

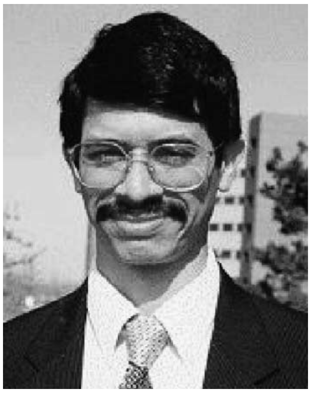
The next three papers give a "business perspective of secure knowledge management." In "Secure Electronic Markets for Private Information," R. Garfinkel, R. Gopal, D. Rice, and M. Nunez develop a foundational framework for an electronic market for private information. The authors propose a secure e-Market mechanism, in which the key information is protected by a concentric union of n line segments in n-space, using a simulation analysis to provide critical insights. In "Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Perspective," R. Singh and A. F. Salam attempt to integrate three areas of research—Semantic Web Technologies, Information Assurance, and eBusiness Process, and develop a framework for secure interorganizational business processes. They use ontologies to analyze and characterize e-business processes, apply description logics to representation knowledge, and propose to integrate a role-based knowledge access schema for eBusiness security with an ontology-based representation of business processes. H. Arora, B. K. Mishra, and T. S. Raghu analyze different incarnations of autonomic computing systems (ACSs) and compare their applicability in different security scenarios in "Autonomic Computing Approach to Secure Knowledge Management: A Game Theoretic Analysis." The focus of the paper is self-healing and self-protection aspects of ACS. The authors show that moving to a partial autonomic system with self-healing mechanisms can provide a stable environment for securing enterprise knowledge assets and can reduce hacking.

The last two papers are in the Transactions Brief category, describing new ideas on the "privacy preserving data sharing and dissemination" theme. In "Trust-Based Privacy Preservation for Peer-to-Peer Data Sharing" by Y. Lu, W. Wang, D. Xu, and B. Bhargava, the authors adopt the trust relation between a peer and its collaborators called buddies. The buddy works as a proxy to send requests and acquire data, thus providing a shield under which the identity of the requester and the accessed data cannot be linked. The authors then present a privacy measuring method, and discuss dynamic assessment and enhancement to supplier's privacy. L. Lilien, and B. Bhargava propose an interesting architecture for the privacy preserving data dissemination in "An Architecture for Privacy-preserving Data Dissemination," which is the last paper of this special issue. The authors suggest a self-destructive atomic bundle of private data and privacy preference metadata as a solution to a privacy control in a network of asymmetric trust relationships. The concepts of an atomic apoptosis and adaptive evaporation presented in the paper offer a novel approach to controlling the access to a disseminated private data, especially when transitive trust relationships prevent the owner of the private data from controlling subsequent data-sharing of the primary guardian of the private data.

Finally, we would like to express our thanks to the authors of all submitted papers and the referees for their outstanding review in a timely manner. This special issue would not have been possible without the support of Dr. Brown, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS (TSMC) Editor-in-Chief who stood behind our effort on this special issue on secure knowledge management. We would also like to thank JinKyu Lee and Insu Park who have done an excellent job of bookkeeping and coordinating the reviews and A. T. Scheman-Moje of IEEE TSMC for her help throughout this project.

H. RAGHAV RAO, *Guest Editor*
Department of Management Science and Systems
State University of New York at Buffalo
Amherst, NY 14260
e-mail: mgmtrao@buffalo.edu

SHAMBHU J. UPADHYAYA, *Guest Editor*
Department of Computer Science and Engineering
State University of New York at Buffalo
Amherst, NY 14260
e-mail: shambhu@cse.buffalo.edu



H. Raghav Rao received the Ph.D. degree from the Krannert Graduate School of Management, Purdue University, IN, in 1987.

He is a Professor of management science and systems at the State University of New York at Buffalo. His interests are in the areas of management information systems, decision support systems, and expert systems and information assurance. He has chaired sessions at international conferences and presented numerous papers. He has authored or coauthored more than 100 technical papers, of which more than 70 are published in archival journals. He has received funding for his research from the National Science Foundation (NSF), the Department of Defense and the Canadian Embassy, and has received the University's prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. He is a co-editor of a special issue of *The Annals of Operations Research*, the *Communications of ACM*, and associate editor of *Decision Support Systems, Information Systems Research* and IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, and co-editor-in-Chief of *Information Systems Frontiers.* He is co-editor of a forthcoming book on *Managing Information Assurance in Financial Services* to be published by Idea Group. He would like to dedicate this issue to the memory of his mother and likes to thank his family for their support in this endeavor.

Dr. Rao received Best Paper and Best Paper Runner Up Awards at AMCIS and ICIS.

Shambhu J. Upadhyaya (S'84–M'86–SM'01) received the Ph.D. degree from the University of Newcastle, Newcastle, Australia, in 1987.

He is an Associate Professor of Computer Science and Engineering and Director of the Center of Excellence in Information Systems Assurance Research and Education at the State University of New York at Buffalo, Amherst, NY. Prior to July 1998, he was a Faculty Member at the Electrical and Computer Engineering department. His research interests are information assurance, computer security, fault diagnosis, fault tolerant computing, and very large scale integration (VLSI) testing. He has authored or coauthored more than 150 articles in refereed journals and conferences in these areas. His current projects involve intrusion detection, insider threat modeling, security in wireless networks, SoC test scheduling, analog circuit diagnosis, and RF testing. His research has been supported by the NSF, Rome Laboratory, the U.S. Air Force Office of Scientific Research, Defense Advanced Research Projects Agency (DARPA), and National Security Agency. In May 1999, International Business Machines (IBM) Corporation sponsored a new Electronic Test and Design Automation Lab to support his teaching and research on VLSI testing. He has been awarded an IBM Faculty Partner Fellowship for year 2000–2001 in recognition of his research accomplishments in the area of testing and fault tolerance. He was also a National Research Council (NRC) faculty fellow, in 2001 and 2002. In 2005, he received Cisco equipment donation to build a computer security lab. He has held Visiting Research Faculty positions at the Center for Reliable and High-Performance Computing, University of Illinois, Urbana–Champaign, Intel Corporation, Folsom, CA, AFRL, Rome, NY, and the Naval Research Laboratory, Washington, DC. He was the Program Co-Chair of the Fifth IEEE/Association for Computing Machinery (ACM) Great Lakes Symposium on VLSI, 1995. He has served on various Conference Committees including the IEEE Simulation Conference, Fault Tolerant Computing Symposium, IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, and IEEE Symposium on Reliable Distributed Systems. He was the Publicity Chair of 1998 IEEE International Computer Performance and Dependability Symposium, and served as the USA Program Chair of IEEE Symposium on Reliable Distributed Systems at Nuernberg, Germany, in 2000. He was a guest co-editor of a book entitled: *Mobile Computing: Implementing Pervasive Information and Communication Technologies* (Kluwer Academic, 2002). He was a guest co-editor of a special issue on *Reliable Distributed Systems* in IEEE TRANSACTIONS ON COMPUTERS, February 2003. He was on the Program Committee of the *Third IEEE International Information Assurance Workshop*, Washington, DC, March 2005, the Sixth Annual IEEE Information Assurance Workshop, West Point, NY, June 2005, and the Dependable Computing and Communications Symposium of IEEE International Conference on Dependable Systems and Networks (DSN)-2005, among others. He is an Associate Editor of IEEE TRANSACTIONS ON COMPUTERS.

Dr. Upadhyaya is a member of the editorial board of the *International Journal on Reliability, Quality, and Safety Engineering* published by the World Scientific Publishers and is a member of IEEE Computer Society since 1984.