DEVELOPMENTS in information systems technologies over the past fifty years have resulted in computerizing many applications in various business areas. Data has become a critical resource in many organizations and therefore efficient access to data, sharing the data, extracting information from the data, and making use of the information have become urgent needs. As a result, there have been several efforts on integrating the various data sources scattered across several sites. Furthermore, the advent of the World Wide Web and, more recently, of Web 2.0 technologies, has enabled users to store, manage and share vast quantities of structured and unstructured data scattered around the world. Due to the explosion of the data, some of which may be sensitive or private, securing the data from unauthorized access or modification has become a critical need. Therefore, as newer data management technologies emerge, efforts for securing these technologies, as well as the applications that are hosted on them, have also increased a great deal. This has resulted in the emergence of a new field called Data and Applications Security and Privacy (DASPY) with special conferences devoted to this field.

The early developments in DASPY in the 1970’s focused mainly on enforcing discretionary security policies for relational database systems. In the 1980’s attention shifted towards designing and developing multilevel secure database management systems for relational as well as object-oriented database systems. With the advent of the World Wide Web in the 1990’s, much of the developments during that decade focused on securing emerging data management systems such as data warehouses and multimedia data systems, as well as applications such as e-commerce and workflow. The focus was not only on securing data, but also on securing information and knowledge. Various access control models as well as trust models emerged during this period. A comprehensive overview of the early developments has been given in [1]. A special issue devoted to these early developments, especially on multilevel secure database systems, was published in 1996 [2].

During the past decade, with the explosion of web technologies such as social networks and semantic web, as well as analysis technologies such as data mining and machine learning, ensuring the privacy of individual has become a critical need. For example, one could infer highly sensitive and private information from the various websites and social networks, or one could also extract such information by applying today’s available sophisticated data mining tools. Much of the focus during this period included designing privacy-preserving data mining algorithms, securing social networks, and developing privacy-aware access control models and DBMSs. Semantic web technologies have been utilized to represent and reason about the various confidentiality, privacy and trust policies. Some of the developments, especially in access control models, have been reported in [3]. A special issue on the emerging privacy-preserving data mining algorithms was published in 2007 [4].

Due to some of the major breakthroughs over the past five years in securing various types of data and application systems as well as ensuring the privacy of individuals, we decided to publish this special issue. It consists of four papers that reflect some of these recent developments. The first paper titled “Privacy Preserving Enforcement of Spatially Aware RBAC,” by M.S. Kirkpatrick, G. Ghinita and E. Bertino, focuses on protecting the location of mobile users and subsequently ensuring the privacy of these individuals. The authors state that some of the current geospatial security models do not protect the location of the individuals due to the fact that the service providers are not trusted. They then describe cryptographic protocols that address this limitation. The second paper titled “Query Profile Obfuscation by Means of Optimal Query Exchange between Users,” by D. Rebollo-Monedero, J. Forné, and J. Domingo-Ferrer, focuses on protecting the profiles of mobile users. The authors state that it is possible to identify the users from their query profiles. They then propose a method where multiple users may collaborate and decide the types of queries to pose to minimize the disclosure of their identities. The third paper titled “Constraint-Aware Role Mining via Extended Boolean Matrix Decomposition,” by H. Lu, J. Vaidya, V. Atluri, and Y. Hong, describes novel techniques for role mining. The authors state that current approaches including Boolean Matrix Composition do not take into consideration aspects such as separation of duty. They describe techniques for enhancing Boolean Matrix Composition to take such constraints into consideration. The fourth paper titled “Access Control with Privacy Enhancements a Unified Approach,” by S. Barker and V. Genovese,
describes a framework based on logic that can unify the specification of both access control and privacy policies. This enables a unified approach to represent and reason about security and privacy policies. We hope that this special issue will spawn new ideas, concepts and solutions for next generation DASPY systems.

We would like to dedicate this special issue to the late Dr. Steve Barker, the coauthor of the fourth paper, who passed away in January 2012. Steve has been a major contributor of DASPY for the past fifteen years and will be sadly missed by the DASPY community.

Elena Ferrari
Bhavani Thuraisingham
Guest Editors

REFERENCES


Elena Ferrari is a full professor of computer science at the University of Insurbria, Italy and scientific director of the K&SM Research Center. Her research activities are related to various aspects of data management, including access control, privacy and trust, secure social networks, secure cloud computing and emergency management, secure semantic web, multimedia databases. On these topics she has published more than 170 scientific publications in international journals and conference proceedings. In 2009, she received the IEEE Computer Society’s prestigious Technical Achievement Award for outstanding and innovative contributions to secure data management. In 2011, she was named ACM Distinguished Scientist. Dr. Ferrari gave several invited lectures and tutorials in Italian and foreign universities as well as on international conferences and workshops. She has served as program chair of the 4th ACM Symposium on Access Control Models and Technologies (SACMAT ’04), software demonstration chair of the 9th International Conference on Extending Database Technology (EDBT ’04), cochair of the third IFIP WG 11.11 International Conference on Trust Management, 2009, the first and second ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD, 2008/2009, and the first COMPASAC ’02 Workshop on Web Security and Semantic Web. She has also served as program committee member of leading international conferences on data management. Professor Ferrari is on the editorial board of the IEEE Transactions on Knowledge and Data Engineering, the IEEE Transactions on Dependable and Secure Computing, the Transactions on Data Privacy, and the International Journal of Information Technology (IJIT). She is a distinguished member of ACM and senior member of IEEE. Elena Ferrari received her MS degree in computer science from the University of Milano (Italy) in 1992 and a PhD in computer science from the same university in 1998. From 1998 until January 2001, she has been an assistant professor in the Department of Computer Science of the University of Milano (Italy).