Editorial

Elena Ferrari*

Department of Computer Science and Communication
University of Insubria
Via Mazzini, 5, 21100 Varese, Italy
Fax: +39 0332–218909
E-mail: elena.ferrari@uninsubria.it
*Corresponding author

Bhavani Thuraisingham

Department of Computer Science
University of Texas at Dallas
800 W. Campbell Road, MS EC31
Richardson, Texas 75080, USA
Fax: +1 972–883–2399
E-mail: bhavani.thuraisingham@utdallas.edu

Abstract: This editorial outlines the scope and contents of the Special Issue on Data and Application Security, Volume 2, Number 4, of the *International Journal of Information and Computer Security (IJICS).*

Keywords: security; privacy; access control; identification.

Reference to this paper should be made as follows: Ferrari, E. and Thuraisingham, B. (2008) 'Editorial', *Int. J. Information and Computer Security*, Vol. 2, No. 4, pp.325–327.

Biographical notes: Dr. Elena Ferrari is a Professor of Computer Science at the University of Insubria, Italy, where she heads the Database and Web Security Group. She received her MS degree in Computer Science from the University of Milano, Italy in 1992. In 1998, she received a PhD in Computer Science from the same university. Her main research activities are web security, access control and privacy. On these topics she has published more than a hundred scientific publications in international journals and conference proceedings. Dr. Ferrari is on the Editorial Board of the *VLDB Journal*, the *Transactions on Data Privacy*, and the *International Journal of Information Technology (IJIT).* She is a member of the ACM and senior member of IEEE.

Dr. Bhavani Thuraisingham joined The University of Texas at Dallas (UTD) in October 2004 as a Professor of Computer Science and Director of the Cyber Security Research Center in the Erik Jonsson School of Engineering and Computer Science. She is an elected Fellow of three professional organisations: the Institute for Electrical and Electronics Engineers (IEEE), the American Association for the Advancement of Science (AAAS) and the British Computer Society (BCS). She received the IEEE Computer Society's prestigious 1997 Technical Achievement Award for "outstanding and innovative contributions to secure data management". Her work in information security and information management has resulted in over 80 journal articles, eight books, over 200 refereed conference papers and three US patents.

1 Introduction

The number of computerised databases has been increasing rapidly over the past three decades. Data has become a critical resource in many organisations, and therefore, efficient access to data, sharing the data, extracting information from the data, and making use of the information has become an urgent need. The advent of the internet has made the access to data and information much easier. Users can now access large quantities of information in a short space of time. As the demand for data and information management increases, there is also a critical need for maintaining the security of the databases, applications and information systems. Data and information have to be protected from unauthorised accesses as well as from malicious corruption. Therefore, we need effective and efficient mechanisms for securing access to data and applications able to fulfill the demand of new applications and scenarios.

The five papers included in this special issue cover some of the most important aspects of data and application security and can be a valuable reference point for this challenging area. The papers in this special issue were selected from a total of 17 received papers. The selected papers were carefully reviewed by at least three reviewers before being accepted for publication.

The focus of the first paper 'Supporting dynamic administration of RBAC in web-based collaborative applications during run-time', by Mavridis *et al.*, is on dynamic administration of access control at run-time. The paper describes an authorisation architecture, based on the Dynamically Administering Role Based Access Control (DARBAC) model, which supports active security through temporal activation of assigned roles for a particular objective, extended decentralisation of administrative care depending on rules, constraint-based privacy protection, dynamic separation of duties based on collaborative goals, and synchronisation of permission availability for users with different responsibilities. The application of the implemented access control system in a typical workflow subsystem is also demonstrated.

The second and third papers deal with privacy protection. Privacy-preserving data mining is today a very active research field, whose main purpose is the development of methods and tools capable of analyzing massive datasets of personal information to the purpose of extracting models of social and commercial interest, while preserving, at the same time, an high degree of privacy and anonymity of the individuals to whom data under analysis are referred. In the paper 'Privacy-preserving data mining in the malicious model', Kantarcioglu and Kardes make an analysis of trade-offs between performance and security in privacy-preserving distributed data mining algorithms, under both the malicious and semi-honest models. Singh *et al.* in their paper 'Privacy analysis and enhancements for data sharing in *nix systems' analyse the data sharing mechanisms of *nix systems and point out the need for better privacy support. To cope with the identified privacy requirements they propose an administrative auditing tool which can alert administrators and users when their private data is at risk, and a View Based Access Control (VBAC) mechanism which provides stronger privacy support wrt existing solutions.

The paper 'Prompt damage identification for system survivability', by Zuo, addresses the problem of prompt damage assessment and containment in mission critical systems. While no security mechanisms can guarantee absolute security, attack resilience and survivability are necessary to support reliable functions of mission critical systems. The paper presents a model designed to control damage, isolate malice, and avoid fault epidemic, by, at the same time, keeping low the computational overhead.

Finally, the last paper of this special issue ‘Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection’, by Nikam and Agarwal deals with fingerprint based biometrics systems, which are today widely used due to increasing demand on security, privacy and anti-terrorism. Unfortunately, such systems may be subject to serious security threats. To make such systems more robust, the paper proposes a new liveness detection method, based on multiresolution analysis of time series fingerprint ridge lines, to safeguard fingerprint scanners from fake fingerprint attacks.

Acknowledgement

The guest editors of the Special Issue on Data and Application Security, Vol. 2, No. 4, of the *International Journal of Information and Computer Security (IJICS)*, would like to thank the editor in chief of IJICS, Prof. Dr. Eldon Y. Li, and all the authors that submitted to this special issue. To the authors with their papers selected to be published in this issue after international refereeing, we would like to show appreciation for their enthusiasm, commitment, and their endless cooperation.

Special thanks go to all the reviewers for their thorough comments that helped in enhancing the quality of the papers.