Preface

Justin Zhan

Department of Computer Science,
North Carolina A&T State University,
1601 East Market Street, Greensboro, NC, 27410, USA
E-mail: zzhan@ncat.edu

Biographical notes: Justin Zhan is the Director of iLab within the Department of Computer Science at NCAT. His research interests include social network science, social computing, information assurance, data mining, and simulation tool development. He has founded the IEEE International Conference on Social Computing (SocialCom), one of the premier conferences focusing on the social network and computing field. He is the Steering Committee Chair of the IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT). In recent years, he has published 130 articles in peer-reviewed journals and conference proceedings and delivered 30 keynote speeches and invited talks.

Information privacy and security is becoming more and more important in our lives. The security and privacy technologies, applications and online services have implications for us all, but is particularly pertinent for people who use technologies to uncover fraud, corruption and development malpractice. The information privacy and security technologies will continue to influence the future roadmap in science and engineering.

The *International Journal of Information Privacy, Security and Integrity (IJIPSI)* now released by Inderscience aims at being a high impact peer-reviewed international journal featuring innovative scientific articles covering all aspects of information privacy, security, and integrity. *IJIPSI* will bring together the researches from academia and industries as well as practitioners to share ideas and visions on multifaceted aspects of information privacy, security, and integrity, and to disseminate the innovative research and development of all aspects of information privacy, security and integrity, including their models, services, and novel applications associated with their utilisation. *IJIPSI* topics include, but are not limited to: privacy and security foundations, privacy enhancing technologies, privacy-preserving computing, privacy policies and laws, economics of information privacy, security and integrity, network and communication security, secure systems, secure computing, database privacy and security, risk analysis, modelling and management, trustworthy computing, management and evaluation, theoretical foundation of information integrity, information integrity structure and design, legal, procedural, regulatory, and ethical aspects of information integrity, impacts of lack of information integrity, trustworthy dimension of information integrity, interactions and integration of information privacy, security and integrity.

We are honoured to feature seven articles from world scientists for this inaugural volume of *IJIPSI*. The first issue starts with five invited articles. The article entitled 'Enhanced privacy ID from bilinear pairing for hardware authentication and attestation' introduces a cryptographic scheme (EPID) that enables the remote authentication and assentation of a hardware device while preserving the privacy of the device. EPID has a device which can be revoked so that the revocation manager finds the corrupted private

key. This article discusses a new security notion of EPID with formal definitions of anonymity and unforgeability and provides a construction of an EPID scheme from bilinear pairing. The EPID scheme is efficient and provably secure in the random oracle model under the strong Diffie-Hellman assumption and the decisional Diffie-Hellman assumption.

The second article, entitled 'Analysing security and privacy issues of using e-mail address as identity', discusses and analyses security and privacy problems resulting from using e-mail address as identity via well-designed user behaviour survey and by investigating websites' design schemes. The produced results illustrate that using e-mail address as identity poses high security and privacy risks. This is mainly because of the multiple usages of e-mail addresses and users' improper online habits.

The article entitled 'Ontology-based access control for social network systems' proposes an assess control model based on semantic web technologies that takes into account the above mentioned complex relations. The proposed model enables expressing much more fine-grained access control policies on a social network knowledge base than the few existing models. The authors demonstrate the applicability of our approach by implementing a proof-of-concept prototype of the proposed access control framework and evaluating its performance.

The next article, entitled 'A general model for trust management', discusses a trust management model that resides on the decision-maker's device and provides a highly flexible solution where individual users may leverage peer stereotyping to personalise privacy policies in a scalable way. The trust model can handle trust chains of trust formation, trust dissemination, and trust evolution.

The last article, entitled 'Integrating privacy requirements considerations into a security requirements engineering method and tool', examines a method for identifying privacy requirements within the context of a security requirements engineering method, describes the security quality requirements engineering (SQUARE) methodology, discusses the definition of privacy and the associated privacy concerns as well as a novel modification to the SQUARE method and tool to incorporate privacy considerations.

These five articles have high quality and relevance that we expect for developing *IJIPSI*. Finally, we would like to thank all authors, reviewers, and members of the editorial board of *IJIPSI*.