

## Editorial

### Intelligent manufacturing system and security and assurance

Jong Hyuk Park · Deqing Zou · Tai-hoon Kim ·  
Javier Lopez · Hangbae Chang

Published online: 27 March 2009  
© Springer Science+Business Media, LLC 2009

Today, information security and assurance is emerging as an important research issue in the manufacturing environments due to the rapid advances in IT. The special issue would concentrate on the research of intelligent manufacturing system and its security and assurance (IMSA). The goal of this special issue is to bring together the researchers from academia and industry as well as practitioners to share ideas, problems, and solutions related to the multifaceted aspects of IMSA. Moreover, we expect that the special issue will be a trigger for further related researches and foster technology improvements in this vital subject.

We are pleased to mention that responses to the call for papers have been very well received from 2008 International Conference on Information Security and Assurance (ISA-08) and after several rounds of paper review by the guest editors,

we have included five papers with high qualities to form this special issue.

Accordingly, a number of papers included in this special issue focus on ubiquitous e-business, security of networked manufacturing, distributed denial of service, sensor network security, and detection.

More specifically, Y. Shin presents a telebiometric system mechanism model and biometric network protocol for the security of networked manufacturing. Shin analyzed the vulnerabilities of the biometric system used for access control and the authentication of access to confidential information in the networked manufacturing system.

S. Oh also presents a new role-based access control in ubiquitous e-business environment. And in this study, he proposes the new access components such as space, space hierarchy, and context constrains. The Ubi-RBAC covers the context awareness and mobility of subject.

Cheng introduces quality assurance evidence collection model for msn forensics. The emphasis of this paper is on the development of an effective evidence collection control mechanism and Cheng proposes an evidence collection control model used in network forensics, called QAEC (Quality Assurance Evidence Collection) which adjusts the amount of data from evidence flow.

Sardana presents deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate Dos attacks in ISP domain: honeypot based approach. The results of this paper show that the proposed approach is comparable to previously reported approaches with an advantage of variable rate attack detection with minimum false positives and negatives.

Levi proposes simple, extensible, and flexible random key pre-distribution schemes for wireless sensor networking using reusable key pools. In detail, he presents random key pre-distribution schemes for wireless sensor networks

---

J. H. Park (✉)  
Department of Computer Science and Engineering,  
Kyungnam University, Masan, South Korea  
e-mail: parkjonghyuk1@hotmail.com

D. Zou  
School of Computer Science and Technology, Huazhong  
University of Science and Technology, Wuhan, China  
e-mail: Deqingzou@mail.hust.edu.cn

T.-h. Kim  
Hannam University, Daejeon, Korea  
e-mail: taihoonn@empal.com

J. Lopez  
Computer Science Department, University of Malaga,  
Malaga, Spain  
e-mail: jlm@lcc.uma.es

H. Chang  
Daejin University, Pocheon, Korea  
e-mail: hbchang@daejin.ac.kr

that provide varying ranges of security. And examined performance of schemes and compared them with well known random key pre-distribution schemes.

Eventually, we would like to extend our sincere appreciation to all the authors for their priceless dedication and also to the referees for their support and hard work for reviewing the papers in a timely manner despite of busyness. We firmly

believe that the accepted papers would be a meaningful contribution to researchers, students, and practitioners studying this field of intelligent manufacturing system and security and assurance. Our special thanks go to the editorial board for this SI and Professor Andrew Kusiak, who is the Editor-in-Chief of Journal of Intelligent Manufacturing for his support throughout the whole publication processes.