Editorial

Welcome to the inaugural issue of *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*. This peer-reviewed quarterly journal mainly focuses on publishing original and high-quality contributions including regular papers, short papers, tutorials, book reviews and surveys. Also, *JoWUA* aims at being an international forum for researchers, professionals, and industrial practitioners on all topics related to wireless mobile network, ubiquitous computing and their applications.

This inaugural issue serves as the proceedings of *the 2nd International Workshop on Managing Insider Security Threats (MIST 2010)* held in Morioka, Japan in June 15th, 2010. *MIST 2010* had received high quality submissions from all over the world. After a rigorous peer-review process where each submission is reviewed by at least three referees, seven papers were finally accepted for presentation.

The first paper, "Detecting Masqueraders: A Comparison of One-Class Bag-of-Words User Behavior Modeling Techniques" by Malek Ben Salem and Salvatore J. Stolfo, evaluates the operational characteristics of two one-class user behavior profiling techniques used for masquerade attack detection: one-class Support Vector Machines (ocSVMs) and a Hellinger-distance based user behavior profiling technique. The authors have compared both accuracy results and computational efficiency of the two bags of word-based modeling methods. They show that ocSVMs are more effective for masquerade detection.

The next paper entitled "Reducing the Risk of Insider Misuse by Revising Identity Management and User Account Data" by Ludwig Fuchs and Günther Pernul, proposes the methodology contROLE for structured Identity Management, which includes a systematic cleansing of account data. The authors show that cleansing of identity and account data can acheive a considerable increase of data quality. Also, the methodology is evaluated through a case study with account data of a real company.

In the third paper, "Using Budget-Based Access Control to Manage Operational Risks Caused by Insiders", Debin Liu *et al.* present a Budget-Based Access Control Model to mitigate the insider threat. Through the experimental study, it is shown that the proposed model has a positive impact on rational users' risk attitudes, and reduces the organizational risk caused by the access exceptions.

The next paper, "Safe Authentication Protocol for Secure USB Memories" by Kyungroul Lee *et al.*, analyzes the existing authentication protocols for the secure USB memories and demonstrates their vulnerabilities leading to privacy exposures. In addition, the authors classify these vulnerabilities into nine categories, based on which the protocols are then compared.

The fifth paper entitled "Specifying and Enforcing a Fine-Grained Information Flow Policy: Model and Experiments" by Valérie Viet Triem Tong *et al.*, introduces a model for specifying and enforcing a fine-grained information flow policy. In order to demonstrate the utility of the proposed model, the authors develop a prototype that is used to highlight two different cases where an information flow policy can easily express and enforce restrictions that are not well supported by traditional access control systems.

The next paper entitled "Towards Side-Effects-free Database Penetration Testing" by Que Nguyet Tran Thi and Tran Khanh Dang, proposes an extended and specific methodology for side-effect-free

penetration testing in detection of database security flaws. Based on the proposed methodology, the authors design the architecture for automated testing tool and implement its prototype in Oracle Database Server 10g/11g. The prototype demonstrates the applicability and effectiveness of the proposed methodoligy.

The last paper, "Reliable Social Trust Management with Mitigating Sparsity Problem" by Mucheol Kim *et al.*, introduces a reliable social trust model that is made through combinations of actual relations and virtual ones. Its motivation is to address the sparsity problem of relations between nodes, which is one of the major problems in trust management for social networks. With the experimental results, the authors show that the proposed approach using virtual relations is a better solution for the sparcity problem.

I would like to extend special thanks to all authors as well as reviewers for their enthusiasm and dedication, which brought this inaugural issue to fruition. Also, I thank *DIGIKITE*, which is a Korean IT solution company (`http://www.digikite.com`), for sponsoring this issue. Finally, I hope that the readers find the techniques given in the issue useful and a source of valuable new insights that will benefit their future research.

Editor-in-Chief
Ilsun You