Journal of Computers

Special Issue on Trusted Computing and Communications

FOREWORD

Trusted Computing Environments are able to provide secure and efficient network communication capabilities in a wide variety of applications where traditional security techniques are not possible to meet the demand for various security threats. There are numerous scenarios a Trusted Computing Environment can be used to provide secure interactions such as two-party communications over insecure networks, identity-based RSA multisignature with verifiable for mobile communications, proxy signature for dynamic delegation in grid environments, hash-based communication scheme with privacy and mutual authentication in RFID applications, and threshold cryptography for distributed trust in cluster-based communications.

The objective of this special issue is to present research and achievement in latest aspects of trusted computing and communications by bring together their fruitful results concerning the relevant issues. This special issue selects 7 high quality papers, covers various research topics in trusted computing and communications. In the first paper, Prof. Ya-Fen Chang, Po-Chun Chen and Tse-Hsiang Chen proposed a verifiable identity-based RSA multisignature scheme for mobile communications. Users can easily verify the generated digital signature by the signer's identities and PKG's public key and no extra certificate is needed to authenticate signers. In the second paper, Prof. Chi-Tung Chen, Ming-Tsun Lin and Iuon-Chang Lin propose a dynamic delegation scheme for grids using proxy signature. The scheme can satisfy the requirements of nonrepudiation and known signer in grids. In the third paper, Prof. Chun-Ta Li demonstrated an efficient and secure communication scheme for trusted computing environments. The scheme ensures the security and enhances the performance of the two-party communications by using one-time signature and hash-chain techniques. In the fourth paper, Prof. Chao-Chen Yang present a robust authentication method applied both cyclic redundancy check and hash function to detect stego-images while retaining high capacity of embedding information. In the fifth paper, Prof. G.S.R. Emil Selvan, S. Sivagurunathan and P. Subathra proposed a cluster based approach for mobile ad hoc network security by using a threshold security mechanism with a mobility based clustering algorithm. In the sixth paper, Prof. Vasudevan and Sukumar propoed a multi server architecture that uses LKH and dynamic split and merge for group key management to improve the packet delivery ratio. In the last paper, Prof. Min-Shiang Hwang, Chia-Hui Wei, and Cheng-Yee Lee survey recent technical researches on the problems of privacy and security for various applications in RFID. We wish this special issue serve as good reference for beginner in this active research field.

On behalf of the editorial committee, We would like to thank all the authors and reviewers for their contributions to this special issue. We are also appreciative to the editorial committee members for their great contributions. Thank you very much for your interest on this special issue.

Min-Shiang Hwang, Guest Editor
Professor
Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road
Taichung City 407
Taiwan, Republic of China
Email: mshwang@nchu.edu.tw

Chun-Ta Li, Guest Editor
Assistant Professor
Department of Information Management
Tainan University of Technology
529 Jhong Jhen Road
Tainan County 710
Taiwan, Republic of China
Email: th0040@mail.tut.edu.tw