

GUEST EDITORIAL PREFACE

Special Issue on Trust, Security and Privacy in Computing and Communications (Part 1)

Zheng Yan, Xidian University, Xi'an, China and Aalto University, Espoo, Finland

Peter Mueller, IBM Research, Zurich, Switzerland

Xinyi Huang, Fujian Normal University, Fuzhou, China

Xiangjian (Sean) He, University of Technology, Sydney, Australia

Marinella Petrocchi, Istituto di Informatica e Telematica, Pisa, Italy

With the rapid development and increasing complexity of computer systems and communication networks, user requirements for trust, security and privacy are becoming more and more demanding. Therefore, there is a grand challenge that traditional security technologies and measures may not meet user requirements in open, dynamic, heterogeneous, mobile, wireless, and distributed computing environments. As a result, we need to build systems and networks in which various applications allow users to enjoy more comprehensive services while preserving trust, security and privacy at the same time. As useful and innovative technologies, trusted computing and communications are attracting researchers with more and more attention. The title of this special issue for *International Journal of Information Security and Privacy (IJISP)* is therefore coined precisely as “*Special Issue on Trust, Security and Privacy in Computing and Communications*”.

This special issue focuses on innovative methods and techniques for addressing trusted computing and communications, with regard to trust, security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks, and providing a forum to present and discuss emerging ideas and trends in this highly challenging research field. The special issue consists of two parts, for publication in two issues, and 9 advanced results were selected from 23 submissions. The first part of the special issue includes four papers.

The paper “Several Oblivious Transfer Variants in Cut-And-Choose Scenario” proposed several variants of oblivious transfer in a cut-and-choose scenario, providing multiple ways of transferring data in an oblivious manner, with instantiations based on homomorphic encryption.

The paper “Trust of the Same: Rethinking Trust and Reputation Management From a Structural Homophily Perspective” investigated homophily, i.e., love of the same, which is the tendency of individuals to associate and bond with similar others in a social network. The authors discovered its presence and confirmed that structural homophily, i.e., the similar way of connecting other nodes, is fostering trust characteristics and connections among peers in P2P-oriented, next generation of Wireless Sensor Networks. In the paper “Cooperative Transmission against Impersonation Attack Using Inter-Session Interference in Two-Hop Wireless Networks”, the authors presented an eavesdropper model with authentication errors and two eavesdropping ways in two-hop wireless networks. They analyzed the number of eavesdroppers that can be tolerated and draw two conclusions for authentication errors. Ali et al. examined genderwise differences in information security awareness (ISA) among university students in the paper “Observations on Genderwise Differences among University Students in Information Security Awareness”. They found different behaviors, attitudes and actions between male and female students with regard to ISA.

This special issue collects a number of advanced research results, some of which were presented in the 2015 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom2015). We would like to thank all authors for their contributions to it and all the reviewers for their valuable supports. We will be happy if this special issue can extend the big success of IEEE TrustCom2015 and attract more attention in the field of trust, security and privacy.

Zheng Yan

Peter Mueller

Xinyi Huang

Xiangjian (Sean) He

Marinella Petrocchi

Guest Editors

IJISP