Telecommun Syst (2013) 52:1341–1342
DOI 10.1007/s11235-011-9646-6

Advances in security and multimodality for pervasive computing environments

TS Special Issue

Jong Hyuk Park · Ching-Hsien Hsu · Naveen Chilamkurti · Mieso Denko

Published online: 5 November 2011

Pervasive computing or ubiquitous computing calls for the deployment of a wide variety of smart devices throughout our working and living spaces. These devices are intended to react to their environment and coordinate with each other and with other network services. This results in a giant, ad-hoc distributed system, with tens of thousands of people, devices, and services coming and going. Due to the uncertainty and mobility of pervasive computing environments, trust modelling has been regarded as an important problem. Context-awareness, mobility and integration are the properties every pervasive computing environment embodies. Pervasive computing environments (PE) present specific peculiarities with respect to aspects like security and multimodality. While enlarging and easing the ways to access to the environment, security threats arise and the environment must be properly equipped in order to protect itself from malicious attacks and/or from wrong action performed by inexpert users.

J.H. Park (✉)
Seoul National University of Science & Technology, Seoul, Korea
e-mail: jonghyuk09@gmail.com

C.-H. Hsu
Chung Hua University, Hsinchu, Taiwan
e-mail: robertchh@gmail.com

C.-H. Hsu
e-mail: robertchh@gmail.com

N. Chilamkurti
La Trobe University, Melbourne, Australia
e-mail: N.Chilamkurti@latrobe.edu.au

M. Denko
University of Guelph, Guelph, Canada
e-mail: denko@cis.uoguelph.ca

Research areas of relevance to this special issue as listed, but not only limited to:

- Context-Awareness in multimodal applications
- Middleware services for multimodal and pervasive applications
- Trust models and frameworks for PE
- Multimodal mobile and ubiquitous services
- Intelligent Context-Aware System Architecture in PE
- Security model for pervasive computing
- Advanced multimodal interfaces
- Human oriented interfaces
- Virtual reality and ubiquitous computing
- Security standards for next pervasive computing
- Key management and authentication in pervasive computing
- Security in Human Centred Environments
- Intelligent multimedia security services in pervasive computing.

We received thirteen manuscripts. Each manuscript was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers. After the review process, six manuscripts were finally selected for this Special Issue.

The first paper in this special issue is on Mobility A Context-Aware Study for Sentence Ordering, by Gongfu Peng, Yanxiang He, Naixue Xiong, Soocheol Lee, Seungmin Rho. This work proposes a context-aware method for sentence ordering in multi-document summarization task, which combines support vector machine (SVM) and Grey Model (GM). Multi-Documents summarization task focus on how to extract main information of document set, this paper proves the coherence of summary based on the context of document set. Firstly, the method trains the SVM with sentences of each source document and predict sentences sequence of summary as primary dataset. Secondly,

using Grey Model to process the primary dataset, according to the analysis this work achieves the final sequence of summary sentences. Experiments on 100 summaries shown this method provide a much higher precision than probabilistic model in sentence ordering task.

The second paper in this special issue is on HiTrust: Building Cross-organizational Trust Relationship based on a Hybrid Negotiation Tree, by Jianxin Li, Bo Li, Lu Liu, Dazhi Sun, Xudong Liu. They propose a hybrid negotiation tree based modeling approach, named HiTrust, to build cross-organizational trust relationship. The HiTrust is used to characterize the gradual interactions state during the trust establishment between the principals from different security organizations. Compared with the original disclosure tree model, the hybrid tree model in HiTrust can embed both policies and credential sets in a tree node, and is able to describe fine-grained security policy with attributes or negotiation context information. This property endows the HiTrust with the capability of describing complex trust establishment requirements, and makes it more efficient to search desired tree node. Furthermore, to enhance the usability and efficiency of negotiation service, they propose a session state maintenance mechanism based on a policy stack and an asynchronous trust chain propagation mechanism. They have also implemented the HiTrust prototype system, and experimentally verified that the HiTrust is effective and scalable.

The third paper in this special issue is on Efficient Three-Party Key Exchange Protocols with Round Efficiency, by Taek-Young Youn, Eun Sook Kang, Changhoon Lee. The paper reviews some insecurity of Lu and Cao's protocol and analyzes two improved protocols proposed by Guo et al. and Chung and Ku. The paper also shows that the protocols are still insecure. They are vulnerable to an adversary who performs an off-line password guessing attack. The paper provides a countermeasure by performing detailed analysis on the security flaws in two improved protocols, and presents a secure three-party password-authenticated key exchange protocol which requires three rounds.

The fourth paper in this special issue is on A Scalable and Robust Hierarchical Key Establishment for Mission-Critical Applications over Sensor Networks, by Jangseong Kim, Kwangjo Kim. They propose a scalable and robust hierarchical key establishment which enhances resilience against node capture, traffic analysis attack and acknowledgment spoofing attack. The proposed scheme provides periodic key updates without communication costs for key transport. They also verify that the proposed scheme requires less storage, computation and communication cost compared with the previous scheme in the open literature.

The fifth paper in this special issue is on The Study on a Convergence Security Service for Manufacturing Industries, by Jonggu Kang, Jaepil Lee, Chungtae Hwang, Hangbae Chang. This work develops a convergence security service that can provide a comprehensive security service for manufacturing industries with different business process. This service can have the following effects: 1. Able to provide an extensible and flexible platform through induction of SaaS (Software as a Service) structure using SOA (Service-oriented architecture) and Semantic technology. 2. Semantic technology facilitates the connection between systems by standardizing security policies, that is, it provides a smooth convergence security service.

The last paper in this special issue is on A Security Model for IPTV with One-Time Password and Conditional Access System for Smart Mobile Platform, by Manhyun Chung, Younghoon Lee, Taeshik Shon, Jongsub Moon. In the paper, the authors propose an effective method to improve the security system for smart mobile platforms. In this method, both the content server and IPTV use an OPT in order to apply a security code to the contents. In addition, the model performs CAS to manage user rights and keys. Such a method for smart mobile platforms will decrease the load between the server and the client network and secure the transfer of user certification, content security, and stream data.

Finally, we would like to thank all authors for their contributions to this special issue. We also extend our thanks to the following external reviewers for their excellent job in reviewing the manuscripts: Fei Li, Jangsung Kim, Yuanyuan Zeng, Bart Lano, Jaeik Cho, Jianhua Yang, Nam Su Chang, Tae Hyun Kim, Kyusuk Han, HongJoo Lee, Taehee Jo, Hyo Hyun Choi, Jonghyuk Lee, Sudip Misra, Jongsung Kim, Naixue Xiong, Changhoon Lee, Yangsun Lee, Isaac Woungang, Sang-Soo Yeo, Deok Gyu Lee, Taeshik Shon, Hangbae Chang, Seungmin Rho, and Jong Hyuk Park.