*Journal of Universal Computer Science, vol. 15, no. 5 (2009), 967-969
submitted: 24/2/09, accepted: 28/2/09, appeared: 1/3/09 © J.UCS*

Data Security and Privacy Protection in Pervasive Computing Environments

J.UCS Special Issue

Byoung-Soo Koh
(DigiCAPS Co., Ltd, Seoul, Korea
secure2000@gmail.com)

Mieso Denko
(University of Guelph, Guelph, Canada
denko@cis.uoguelph.ca)

Stefanos Gritzalis
(University of the Aegean, Mytilene, Greece
sgritz@aegean.gr)

Ching-Hsien Hsu
(Chung Hua University, Hsinchu, Taiwan
robertchh@gmail.com)

The integration of advanced wireless technology and Internet tends to increase connections of computing devices. Because Pervasive Computing environments make people get accustomed to computing, they naturally forget the fact that they are using computers. Furthermore, smart devices around offer them services such as user location information, user situation, and user data maintenance/management. In order to achieve these purposes, various aspects should be integrated from hardware and networks to operating systems, middleware, user interfaces, and applications.

However, in Pervasive Computing, data security and privacy concerns, such as personal information outflows, has not been considered in depth. Therefore, in Pervasive Computing, data security management and diverse security technologies should be considered. This special issue solicits state-of-the-art approaches and solutions in the area of data security and privacy protection in modern Pervasive Computing environments.

We received twenty-three manuscripts. After the pre-review process, twenty-two manuscripts were selected for the first review. Nine manuscripts (one invited) were finally selected for this Special Issue after the first, second, and third review processes. Each manuscript selected from the pre-review was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers.

The invited paper in this special issue is on Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents, by Pablo Najera, Francisco Moyano, and Javier Lopez. This work presents the concept and security requirements of general-use e-documents, analyze the most comprehensive security solution and its suitability for general-purpose e-documentation. This work finally proposes alternatives for the weakest and less suitable protocol from ePassports.

The first paper in this special issue is on Agent Platform for Wireless Sensor Network with Support for Cryptographic Protocols, by Peter Pecho, Frantisek Zboril jr., Martin Drahansky, and Petr Hanacek. This work outlines the possible usage of cryptographic protocols for securing of a wireless sensor network and present how to make applications for the MICAz devices which uses agent based principles together with some cryptographic protocols.

The second paper in this special issue is on Security Analysis of the Full-Round CHESS-64 Cipher Suitable for Pervasive Computing Environments, by Changhoon Lee, Jongsung Kim, Seokhie Hong, and Yang-Sun Lee. They show CHESS-64 doesn't have a high security level, more precisely, they present two related-key differential attacks on CHESS-64, which are the first known cryptanalytic results on CHESS-64 so far.

The third paper in this special issue is on Protecting Mobile TV Multimedia Content in DVB/GPRS Heterogeneous Wireless Networks, by Shiguo Lian and Yan Zhang. They study the architecture, protocol, user identification and digital right management (DRM) for protecting mobile TV multimedia content. The result indicates that the DVB/GPRS heterogeneous networks integration is able to make full use of the two networks advantages with respect to bandwidth, data rate and implementation complexity.

The fourth paper in this special issue is on *Light-Weight* Key Exchange with Different Passwords in the Standard Model, by Jeong Ok Kwon, Ik Rae Jeong, and Dong Hoon Lee. They propose a light-weight password-based authenticated key exchange protocol with different passwords. It requires only 2 rounds and 4 modular exponentiations per user. The protocol provides forward secrecy, known-key secrecy, key secrecy against the curious server, and security against undetectable online dictionary attacks without random oracles.

The fifth paper in this special issue is on USF-PAS: Study on Core Security Technologies for Ubiquitous Security Framework, by Jong Hyuk Park. He proposes privacy and access control scheme by surveillance which is one of core security technologies for ubiquitous hybrid intelligent security framework. In this scheme, the device information and the signature information can be added to the image data obtained by the image capturing device to maintain security of the image data and use the image data as digital proof when a specific event is generated.

The sixth paper in this special issue is on Vascular Pattern Analysis towards Pervasive Palm Vein Authentication, by Debnath Bhattacharyya, Poulami Das, Tai-hoon Kim, and Samir Kumar Bandyopadhyay. They propose an Image Analysis technique for Vascular Pattern of Hand Palm, which in turn leads towards Palm Vein Authentication of an individual. The proposed three algorithms are proved to improve the recognition performance with different training samples.

The seventh paper in this special issue is on Cooperation Enforcement in a Highly Dynamic Mobile Ad Hoc Network, by Yao H. Ho, Ai Hua Ho, Kien A. Hua, and Fei Xie. This work investigates techniques to enforce collaboration among mobile devices by identify and punish misbehaving users in supporting the virtual router functionality.

Simulation results based on various system configurations are given. They indicate that the proposed technique is effective.

The last paper in this special issue is on A Neural Network Based Vehicle Classification System for Pervasive Smart Road Security, by Naixue Xiong, Jing He, Jong Hyuk, ParkDonald Cooley, and Yingshu Li. The goal of this work is to normalize the image of a vehicle so that regardless of its lane or position in a lane, the features will be approximately the same. They use a single camera system mounted on a pole to look down on the traffic scene, and detecting and classifying vehicles in multiple lanes are for any direction of traffic flow.

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: Antoine Bagula, A. Tsakountakis, Agustinus Borgy Waluyo, Bhabani Sinha, Bidyut Gupta, Binod Vaidya, C. Kolias, C. Lambrinoudakis, Charalampos Patrikakis, Chuan Lin, Damien Sauveron, Debnath Bhattacharyya, Deok Gyu Lee, Deqing Zou, Dieter Hutter, Dimitris Geneiatakis, Domenico Rosaci, Dongchan An, DongHoon Lee, Dong Seong Kim, Martin Drahansky, E. Konstantinou, E. Rekleitis, G. Karopoulos, Han-Chieh Chao, Henry Y.T. Ngan, Ik Rae Jeong, Jaechul Sung, Jeong Ok Kwon, Jiqiang Lu, Josef Skvarek, Jung-Shian Li, Massimo Esposito, P. Rizomiliotis, Shiguo Lian, T. Balopoulos, Xuefeng Liang, Yan Zhang, Yang Liu and Antoine Bagula.

Byoung-Soo Koh
Mieso Denko
Stefanos Gritzalis
Ching-Hsien Hsu
February, 2009