



A Special Section of Intelligent Automation and Soft Computing

APPLICATIONS AND SECURITY IN WEB AND PERSVASIVE ENVIRONMENTS

BY

CHING-HSIEN HSU

*Department of Computer Science and Information Engineering
Chung Hua University
Taiwan*

Web and Pervasive Environments (WPE) are emerging rapidly as an exciting new paradigm including technologies of ubiquitous computing, wireless communication and ambient intelligence to provide computing and communication services any time and anywhere. It usually refers to the creation and deployment of computing technology in such a way that it becomes an invisible part of the fabric of everyday life and commerce. As pervasive computing presents a new trend of information and communication technologies for connecting cyber and physical domains, in such era, computers in the traditional sense gradually fade from view. Namely, information and communication mediated by computers is available anywhere and anytime through devices that are embedded in our environment, completely inter-connected, intuitive, effortlessly portable and constantly available.

Although pervasive computing presents exciting enabling opportunities, the benefits will only be reaped if security aspects can be appropriately addressed. As a result, to realize the advantages of intelligent services in web and pervasive environments, it requires the security issue of its services and applications to be suitable for WPE. Therefore, the security of pervasive computing is an important challenge for commerce, the public sector, academia and the individuals. For example, threats exploiting infirmities of user interfaces, operating systems, networks, and wireless communications give rise to new concerns about loss of confidentiality, integrity, privacy, and availability. How can these risks be avoided to an acceptable level? This special issue is intended to foster the dissemination of state-of-the-art research in the area of secure WPE including security models, security systems, application services, and novel applications associated with its utilization as that security and privacy is the indefeasible right of individuals to control the ways in which personal information is obtained, processed, distributed, shared, and used by any other entity.

This special issue includes an extended version of the selected paper originally presented at the International Workshop on Application and Security Services in Web and Pervasive Environments, held at HuangShan, China; an invited paper contributed by G. Kambourakis, S. Grizalis and J. H. Park; and four regular papers selected from 26 external submissions,

comprising a 15% acceptance rate. The papers selected for this issue not only contribute valuable insights and results but also have particular relevance to the security and pervasive computing community. All of them present high quality results for tackling problems arising from the ever-growing web and pervasive services.

This special issue includes six papers from researchers in Korea, Greece, China and USA, who have demonstrated the effectiveness and efficiency of a variety of security issues and applications in different areas of web and pervasive computing.

G. Kambourakis, S. Gritzalis and J. H. Park in their paper entitled "Device Authentication in Wireless and Pervasive Environments" survey all major potential solutions and trends to the device authentication issue and examine its pros and cons. Each scheme is further analyzed and compared with the others based on some indicative qualitative criteria giving a comprehensive view about its applicability and robustness in terms of security. Some comments including implementation problems and research challenges have been provided, probing its applicability for both infrastructure and ad-hoc deployments. User's privacy issues as a side-effect of device authentication were investigated as well.

The paper by Y. Jin, L. Wang, Y. Kim and X. Yang entitled "Coverage and Connectivity Problems under Border Effects in Wireless Sensor Networks" studies the coverage and connectivity issues with the consideration of border effects in wireless sensor network. In a circle-shaped region, the coverage of entire network could be estimated by using probability theorem. To guarantee the collected data to be arrived at the sink node, the lower bound of network connectivity is also derived. The findings in this study are useful in predicting the coverage of a sensor network, estimating the necessary number of nodes to achieve a specific network coverage ratio, determining the necessary number of nodes to achieve a specific network connectivity probability, and calculating the necessary number of nodes to guarantee full/partial coverage and connectivity requirements simultaneously.

The paper by C. Lee, H. J. Kim, J.H. Park and T. H. Kim entitled: "A Pervasive Secret Sharing Scheme for Embedded Visual Communication System" deals with the secret sharing for secure visual communications. The secret sharing scheme allows a group of participants at different locations to share a secret (i.e., an image) among them by splitting it into pieces ("shares" or "shadows"). The proposed scheme can be used as an image encryption technique. Achievements and result of study is valuable in developing applications in pervasive systems as it is easy to implement with power-conserving and secure communication.

Baodian Wei, Fangguo Zhang and Xiaofeng Chen in their paper entitled "Efficient Online/Offline Signcryption Scheme" propose an efficient provably secure online/offline signcryption scheme and its online/offline version from pairings. Based on the assumption of $k + 1$ square roots, the scheme is proven, without random oracles, to be secure against existential forgery under an adaptive chosen message attack. A comparison has been made with existing schemes from the viewpoint of computational cost and the size of ciphertexts; the proposed scheme appears to be one of the most efficient signcryption schemes. This implementation is ideally suitable for the electronic wallets and smart cards.

The paper by J. Choi, D. Moon and S. Lee entitled "A New Primitive for Stream Ciphers Applicable to Pervasive Environments" addresses the problem of confidentiality and integrity of stream ciphers for pervasive applications. The authors propose a new primitive for stream ciphers called PC-AddRotR (Pervasive Computing - Adder Right Rotation), which is implemented by light-weight hardware with simple arithmetic operations. As a result, it is easily implemented in both hardware and software. Essentially, the proposed primitive is suitable for applications of cryptographic technologies in pervasive environments whose devices have limited processing power, storage, and battery capacity.

The paper by E. J. Yoon and K. Y. Yoo entitled “A New Fingerprint Biometric Remote User Authentication Scheme using Chaotic Hash Function on Mobile Devices” deals with the problem of remote user authentication, which is a mechanism to authenticate remote users over insecure communication networks. The authors demonstrate that chaotic hash-based fingerprint biometric remote user authentication scheme (by Khan et al.) is vulnerable to a privileged insider’s attack and impersonation attacks by using lost or stolen mobile devices. In order to isolate such problems, the authors present an improved remote user authentication scheme for mobile devices.

All of the above papers address either security issues in pervasive computing systems or propose novel application models in the various WPE fields. They also trigger further related research and technology improvements in application and security services of WPE. Honorably, this special issue serves as a landmark source for education, information, and reference to professors, researchers and graduate students interested in updating their knowledge about or active in security and novel application models for web and pervasive computing systems.

The guest editor would like to express sincere gratitude to Dr. Mo Jamshidi (AutoSoft EIC), for giving me the opportunity to prepare this special issue. In addition, I am deeply indebted to numerous reviewers for their professional effort, insight and hard work put into commenting on the selected articles which reflect the essence of this special issue. Last but not least, I am grateful to all authors for their contributions and for undertaking two-cycle revision of their manuscripts, without which this special section could not have been produced.

Prof. Ching-Hsien Hsu

Chung Hua University, Taiwan

E-mail address: chh@chu.edu.tw URL: www.chu.edu.tw/~chh

Guest Editorial Board

Amit K Awasthi, Hindustan College of Science and Technology, India

Cunsheng Ding, HKUST, Hong Kong, China

Xin Guan, Heilongjiang University, China

Xinyi Huang, University of Wollongong, Australia

Min-Shiang Hwang, National Chung Hsing University, Taiwan

Tom Karygiannis, NIST, USA

Byoungcheon Lee, Joongbu University, Korea

Javier Lopez, University of Malaga, Spain

Hyun-A Park, CIST/Korea University, Korea

Timothy K. Shih, National Taipei University of Education, Taiwan

Sundaram Suresh, INRIA, France

Willy Susilo, University of Wollongong, Australia

Tatsuya Suto, University of Nevada, USA

Vassilis Tsagaris, University of Patras, Greece

Jianjun Wang, Fudan University, China

Shiuh-Jeng Wang, Central Police University, Taiwan

Chao-Tung Yang, Tunghai University, Taiwan

Sang-Soo Yeo, BTWorks Inc., Korea

Justin Zhan, Carnegie Mellon University, USA

Lixin Zhang, IBM Austin Research Laboratory, USA