**Atlantis Ambient and Pervasive Intelligence**

Volume 6

Series Editor: **Ismail Khalil**

# Atlantis Ambient and Pervasive Intelligence

Series Editor:

Ismail Khalil, Linz, Austria

(ISSN: 1875-7669)

**Aims and scope of the series**

The book series 'Atlantis Ambient and Pervasive Intelligence' publishes high quality titles in the fields of Pervasive Computing, Mixed Reality, Wearable Computing, Location-Aware Computing, Ambient Interfaces, Tangible Interfaces, Smart Environments, Intelligent Interfaces, Software Agents and other related fields. We welcome submission of book proposals from researchers worldwide who aim at sharing their results in this important research area.

For more information on this series and our other book series, please visit our website at:

*www.atlantis-press.com/publications/books*

ATLANTIS PRESS

AMSTERDAM – PARIS – BEIJING

# Trustworthy Ubiquitous Computing

**Ismail Khalil (Ed.)**

Institute of Telecooperation, Johannes Kepler University Linz,
Altenberger Strasse 69, A-4040 Linz, Austria

**Teddy Mantoro (Ed.)**

Advanced Informatics School, University of Technology Malaysia,
UTM International Campus, Jalan Semarak, 54100 Kuala Lumpur, Malaysia

ATLANTIS
PRESS

AMSTERDAM – PARIS – BEIJING

**Atlantis Press**

8, square des Bouleaux
75019 Paris, France

For information on all Atlantis Press publications, visit our website at: *www.atlantis-press.com*

**Atlantis Ambient and Pervasive Intelligence**

Volume 1: Agent-Based Ubiquitous Computing - Eleni Mangina, Javier Carbo, José M. Molina
Volume 2: Web-Based Information Technologies and Distributed Systems - Alban Gabillon, Quan Z. Sheng, Wathiq Mansoor
Volume 3: Multicore Systems On-Chip: Practical Software/Hardware Design - Abderazek Ben Abdallah
Volume 4: Activity Recognition in Pervasive Intelligent Environments - L. Chen, C.D. Nugent, J. Biswas, J. Hoey
Volume 5: Computer Vision and Action Recognition - Atiqur Rahman Ahad

ISBNs
Print: 978-94-91216-70-1
E-Book: 978-94-91216-71-8
ISSN: 1875-7669

# Editorial: Trustworthy Ubiquitous Computing

Ismail Khalil

Institute of Telecooperation, Johannes Kepler University Linz, Austria

Teddy Mantoro

Advanced Informatics School, University of Technology Malaysia, Malaysia

Ubiquitous Computing (UbiComp) is a vision of rich and seamless interaction with the surrounding computing environment. In spite of the many applications and projects in the area of ubiquitous and pervasive computing the success is still far away. One of the main reasons is the lack of acceptance of and confidence in this technology. Although researchers and industry are working in all of these areas, a forum to elaborate on security, reliability and privacy issues, that resolve in trustworthy interfaces and computing environments for people interacting within these ubiquitous environments is important. The user experience factor of trust thus becomes a crucial issue for the success of UbiComp applications.

The goal of this book is to provide a state the art on trustworthy ubiquitous computing to address recent research results and to present and discuss the ideas, theories, technologies, systems, tools, applications and experiences on all theoretical and practical issues in developing a trustworthy interfaces which are more secure and richer.

The book compiles a series of interesting and timely papers in the areas of 1) trust and context in UbiComp environments, 2) methods and concepts to enhance and ensure reliability in UbiComp environments 3) distributed attacks detection and secure access protocol in MANET, WSN and UbiComp environments and 4) access control and mobile payment in Trustworthy UbiComp environment.

### Part 1: Trust and context in UbiComp environments

This part introduces the concepts of trust and trust in ubiquitous environments and consists of three chapters: Chapter 1 presents automatic trust management of self-adaptive multi-display environments which is an important issue in Trustworthy Ubiquitous Computing due to the fact that during the use of multi-display systems, it can impair user trust and thus user acceptance. Chapter 2 introduces malicious pixels using QR codes as attack vector. This is a proof-of-concept phishing attack on QR codes, which is based on the idea of changing the encoded data of a QR code by turning white modules into black ones. This chapter proposes an algorithm for finding similar QR codes for the attack and showed its feasibility with an example.

Chapter 3 presents a virtual performance stage as a space for children to create and perform stories. This study discusses the development of the Wayang Authoring tool, which aims to assist young people in creating and performing stories, developing an appreciation for cultural artifacts, and enhancing intercultural empathy while building a young story teller community within a virtual world. Wayang Authoring is designed as a type of social software for children to compose the story individually or collaboratively and be more on creative production. By using Wayang Authoring children can express their creativity by producing visual stories and sharing them. Wayang Authoring serves all three kinds of a participatory including affiliation, expression and collaboration. The tagging system in the authoring tool support children to have experiences in story structure. The children can learn to structure and re-structure a story's sequence by using the Wayang Authoring digital tool. The aesthetic coupled with the interactive functions support children to explore virtual and narrative worlds. This virtual creative production tool provides a space for young people to change their role from a simple user to a (co-)creator.

### Part 2: Methods and concepts to enhance and ensure reliability in UbiComp environments

In this second part, the study on network forensics for detection and mitigation of botnet malicious code via Darknet is presented in Chapter 4. The main types of malwares – worms and botnet detection using Darknet is covered. This chapter shows how Darknet as a network forensic technique perform passive detection of malware infected computers.

Chapter 5 introduces the trusted log management system, which can be used to handle the accounting scandals. As the log system cannot guarantee the transfer of trusted logs across a vulnerable transfer path, it is unacceptable for use in digital forensics. The solution of this problem is by defining an efficient log file format by introducing a new CSV and using YAML Ain't Markup Language and making a transversal search among log files.

Chapter 6 introduces a framework for the reasoning of collaborative human behaviour in security-critical work practices. The framework is based on cognitive-based human activities study and information security, in which it consists of a model and a process. Under the security context, the model defines the properties and characteristics of collaborative communication behavior of human users, while the process defines three main steps of observation, simulation and reason and construction of practical security workflows. This security framework evaluates and captures potential security "failure" and "conflict" and envisages the framework to be used for effective handling of security incidents such as information leakage. The resulting simulation and workflow can then be used to minimize potential security incidents, devise better, easy to follow security policies, technical mechanisms that may be automated, and better collaborative processes.

### Part 3: Distributed attacks detection and secure access protocol in MANET, WSN and UbiComp environments

Chapter 7 introduces mitigation of wormhole attack in wireless sensor networks, which looks at the WSN in regard to security issues and challenges. This study proposed a network discovery approach to mitigate its effect in the domain of hierarchal or cluster based wireless sensor networks which use hierarchal routing protocols.

Chapter 8 presents the protocol for secure access in mobile ad-hoc network (MANET) for emergency services using group based access control model. As MANET is operated based on wireless environment, it is vulnerable to threats and intruders due to the fact that information flow can be intercepted and tampered. To solve this problem, a protocol for secure access in emergency services is constructed and implemented in Group Based Access Control (GBAC) model. The goal of this security solution for MANETs is to provide security services such as authentication, confidentiality, integrity, trust and also authorization or access privileges to mobile users. The GBAC model in this chapter presents a protocol for secure access to information between MG and members in the same group, which is known as Intra-access protocol. The protocol is constructed using various cryptographic methods such as encryption, decryption, digital signature and hash functions. The protocol employs three processes for secure access which are member registration, tag creation, and the access control protocol. This study presents analyses using cryptographic and direct proofing method are applied to the protocol, to ensure that the protocol for secure access meeting the security properties such as trust, authentication, authorization, confidentiality, integrity and non-repudiation.

Chapter 9 presents the distributed attacks detection using a lightweight graph-based pattern recognition scheme in mobile ad hoc networks, as the unique characteristics of MANETs can also be their limitations. The shared wireless medium, distributed and self-configuring network architecture and highly dynamic nodes have made them highly susceptible to many attacks. This chapter proposes a distributed hierarchical graph neuron (DHGN) to be incorporated into a cooperative intrusion detection system (IDS) using lightweight, low-computation, distributed intrusion detection scheme in mobile ad-hoc networks (MANETs). To identify possible attacks, the collaborative IDS that incorporate pattern discovery approach are presented.

### Part 4: Access Control and Mobile Payment in Trustworthy UbiComp environment

Chapter 10 presents security framework for mobile banking, as banking sector is always looking for new services' delivery platforms to improve customer confidence and satisfaction. To achieve this, the banking service delivery platform must provide end-to-end security to safeguard the information exchange between the bank and the customer. Unfortunately, many banks adopt generic user authentication systems that was developed for the desktop environment or other complex authentication systems with a number of user intrusive activities. Therefore, the usability and adoption of the mobile banking technology has been extremely slow. This chapter proposes a protocol to solve this problem which use a minimum number of communication messages in registration, authentication and authorization processes by generation algorithm which is implemented using HASH functions and Triple DES encryption algorithm. The authentication and authorization uses non-intrusive methods and hence user inputs are not required for the process. The proposed model improves the efficiency and the usability of the mobile banking services by using an extra 4-digit user PIN to prevent SIM cloning and mobile user impersonation attacks. This followed by the discussion on anonymous, secure and fair micropayment system to access location-based services in Chapter 11.

Chapter 12 presents privacy preserving with a purpose-based privacy data graph. As privacy is critical before the implementation process privacy must be considered first to avoid expensive errors in the deployed system. This chapter 1) expresses access policy by graph, which describes the data access policy, and illustrates the direct-linkages and indirect-linkages between data elements, 2) supports Role Based Access Control to allow administrator role to assign necessary role-level data access permissions. This simplifies the specification and management on individual users, especially in the case of large number of users and finally 3) provides role-level and personal-level access control to specific usage of privacy data.

Trustworthy Ubiquitous Computing has been studied in a number of disciplinary areas such as pervasive/ubiquitous computing, ambient intelligence, intelligent environments, mobile computing and ambient assisted living, research results have been disseminated in a number of conferences and journals. However, there is a lack of sources that can give a complete, systematic view on the state of the art work on trustworthy ubiquitous computing. This book intends to provide professional practitioners – researchers, technology and system developers as well as application users, in various research communities with a one-stop hand-on reference book for trustworthy ubiquitous computing in theoretical and practical issues, which cover the full spectrum of research issues, novel approaches, algorithms, robust technologies and exemplar applications.

Happy reading.

Ismail Khalil and Teddy Mantoro

Editors

**Ismail Khalil** (`http://www.iiwas.org/ismail/`) is a senior researcher and lecturer at the institute of telecooperation, Johanes Kepler University Linz, Austria, since October 2002. He is the president of the international organization of Information Integration and Web-based Applications & Services (@WAS). He holds a PhD in computer engineering and received his habilitation degree in applied computer science on his work on agents' interaction in ubiquitous environments in May 2008. He currently teaches, consults, and conducts research in Mobile Multimedia, Cloud Computing, Agent Technologies, and the Semantic Web and is also interested in the broader business, social, and policy implications associated with the emerging information technologies. Before joining Johannes Kepler University of Linz, he was a research fellow at the Intelligent Systems Group at Utrecht University, Netherlands from 2001-2002 and the project manager of AgenCom project at the Software Competence Center Hagenberg - Austria from 2000-2001. Dr. Khalil has authored around 100 scientific publications, books, and book chapters. He is the editor of the Handbook of Research on Mobile Multimedia series, the book Mobile Multimedia:

Communication Engineering Perspective, the book Multimedia Transcoding in Mobile and Wireless Networks, the book Innovations in Mobile Multimedia Communications and Applications: New Technologies and the book Advancing the Next-Generation of Mobile Computing: Emerging Technologies. He serves as the Editor-in-Chief of the International Journal on Web Information Systems (IJWIS), International Journal on Pervasive Computing and Communication (IJPCC) both published by Emerald Group publishing, UK, Journal of Mobile Multimedia (JMM) published by Rinton Press, USA, International Journal of Mobile Computing and Multimedia Communication (IJMCMC) published by IGI Global, USA, Advances in Next Generation Mobile Multimedia book series published by IGI Global, USA, and Atlantis Ambient and Pervasive Intelligence book series published by Atlantis. He is on the editorial board of several international journals. His work has been published and presented at various conferences and workshops.

**Teddy Mantoro** is an associate professor at School of Advanced Informatics, University of Technology Malaysia (UTM), Kuala Lumpur, Malaysia. He holds a PhD, an MSc and a BSc, all in Computer Science. He was awarded a PhD from Research School of Computer Science, the Australian National University (ANU), Canberra, Australia. His research interest is in Ubiquitous Computing, Pervasive Computing, Context Aware Computing and Intelligent Environment. He has authored several research papers, a book on Intelligent Environment, several book chapters and has four patents pending to his credits in the area of pervasive/ubiquitous computing.

# Contents