Electron Commer Res (2013) 13:237–241
DOI 10.1007/s10660-013-9114-3

IT convergence and security

Stefanos Gritzalis · Justin Z. Zhan · Kitae Jeong

Published online: 9 May 2013

1 Introduction

As we entered the 21st century, the rapid growth of information technology (IT) has changed our lives more conveniently than we have ever speculated. Recently in all fields of the industry, heterogeneous technologies have converged with IT resulting in a new paradigm, information convergence. In the process of information convergence, the latest issues in the structure of data, system, network, and infrastructure have become the most challenging task.

In order to realize IT advantages, it requires the integration of security and data management to be suitable for convergence environments. However, there are still many problems and major challenges waiting for us to solve such as the security risks in convergence application, which could appear when devices interact with different kinds of applications. Therefore, we need to explore a security in convergence environments.

The goal of this issue is to discover a new progressive technology by upgrading the previous technologies and to solve the technical problems that may have occurred in the process of converging technology in various fields. It will reflect the state-of

S. Gritzalis
University of the Aegean, Karlovassi, Samos 83200, Greece
e-mail: sgritz@aegean.gr

J.Z. Zhan
Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411, USA
e-mail: justinzzhan@gmail.com

K. Jeong (✉)
CIST (Center for Information Security Technologies), Korea University, Anam-dong, Seongbuk-gu, Seoul 136-713, Korea
e-mail: kite.jeong@gmail.com

the-art of the computational methods, involving theory, algorithm, numerical simulation, error and uncertainty analysis and/or application of innovative processing techniques in engineering, science, and other disciplines related to IT convergence and security.

The topics of papers submitted in this SI included the following topics:

- Security model for convergence environments
- Security for open convergence system
- Smartphone security Issue
- Embedded security in cars
- Security issues in WSN/RFID
- IPTV security services in the BcN
- Security and privacy for intelligent vehicular systems
- Security for Broadband convergence Network
- Commercial or industrial Issue in convergence environments
- Information security in convergence environments
- Cryptographic technologies for IT convergence and security
- Digital forensics and anti-forensics
- Security applications and services for convergence environments
- Service managements and policies for convergence environments

Each manuscript was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers. After the review process, 10 manuscripts were finally selected for this SI. The titles of selected papers are shown in following.

1. Threat Modeling of a Mobile Device Management System for Secure Smart Work
2. Enhanced security in internet voting protocol using blind signature and dynamic ballots
3. The RBAC Model and Supporting Implementation Technologies in Multi-Domain environment
4. The Effects of Relationship Benefit on relationship Quality and Store Loyalty from Convergence Environments
5. The Security Service Rating Design for IT Convergence Services
6. A Countermeasure against Wormhole Attacks in MANETs using Analytical Hierarchy Process Methodology
7. The Prediction of Network Efficiency in the Smart Grid
8. An Efficient Model of Korean Graphemes Based on a Smartphone Keyboard
9. A Framework for Unified Digital Evidence Management in Security Convergence
10. The Disclosure of an Android Smartphone's Digital Footprint respecting the Instant Messaging utilizing Skype and MSN

2 The papers in this special issue

The first paper, "Threat Modeling of a Mobile Device Management System for Secure Smart Work" by K. Rhee et al., establishes a threat model for an MDM system

by characterizing the system, identifying threat agents, assets, and adverse actions, and defining the threats and their effects. This work will be used to develop security requirements and design a secure system.

The second paper, "Enhanced security in internet voting protocol using blind signature and dynamic ballots" by A. Thi and D. Khanh, allows, in the newly proposed protocol, the adversaries to get more power than in any previous works. They can be coercers or vote buyers outside, and corrupted parties inside our system. The main contribution of this paper is to design an internet voting protocol which is not only satisfies desired security requirements but also unsusceptible to most of sophisticated attacks. The authors employ the blind signature technique and the dynamic ballots instead of complex cryptographic techniques to preserve privacy in electronic voting. Moreover, the authors also aim at the practical system by improving the blind signature scheme and removing physical assumptions which have often been used in the previous works.

The third paper, "The RBAC Model and Implementation Architecture in Multi-Domain Environment" by Z. Yang et al., discusses the domain concept and domain model in order to more adaptively apply the RBAC in multi-domain service oriented environments. Then the authors propose a domain-based RBAC model and give a formal description. Faced to the potential barriers to realize the D-RBAC, the authors also propose the implementation architectures for the individual and composite services respectively, which can efficiently control the service permissions and have a reasonable performance.

The primary concern of CRM is core customers from convergence environments. They show such passionate partnership with the company that they actively put forth their opinion to improve products and service through voluntary pro-company activities and participate in the development of new products through open innovation. Therefore, the top priority of a company should be given to defining its core customers and accurately understanding and managing them, which would contribute to the growth of the company. The fourth paper, "The Effects of Relationship Benefit on Relationship Quality and Store Loyalty from Convergence Environments—NPS Analysis and Moderating Effects—" by J. Jang et al., identifies net promoter score(NPS) of company by adopting index that evaluates the degree of customer loyalty to the company in judging the relationship of company and customer, and later on establishes strategy to increase the number of loyal customers by classifying customers by the score. In addition, as NPS serves as adjustment variable, net promoters are analyzed to contribute to store loyalty significantly.

The fifth paper, "The Security Service Rating Design for IT Convergence Services" by H. Chang, develops a damage compensation index for sustainable security service. In detail, by analyzing damage compensation criteria and cases for general information communication services, a damage compensation index on security services is developed for a goal of VoIP services. It can offer voluntary improvement of service quality for service providers, and simplicity of damage compensation for users. Additionally, it can socially give benefits of increasing the number of companies to apply the security SLA and mitigating legal disputes.

The sixth paper, "A Countermeasure against Wormhole Attacks in MANETs using Analytical Hierarchy Process Methodology" by F. Shi et al., proposes a countermeasure to prevent wormhole attacks in mobile ad hoc networks. The proposed scheme

not only detects wormhole attacks but also locates wormhole nodes. To solve the colluding wormhole attack, the proposed scheme involves a countermeasure named bi-directional wormhole location mechanism.

AMI is core infrastructure of a smart grid and it is expected to be used for many industrial fields. The components of AMI generally include a smart meter, DCU, and MDMS. Since, there are too many devices such as smart meters and DCUs in AMI, it is important to maintain the suitable number of them. In particular, it is necessary to predict the proper number of DCUs for efficient management of AMI. The seventh paper, "The Prediction of Network Efficiency in the Smart Grid" by S. Jung et al., suggests a way to predict the suitable number of DCUs and the proposed method is useful to this heterogeneous AMI.

The eighth paper, "An Efficient Model of Korean Graphemes Based on a Smartphone Keyboard" by Y. Jeong et al., proposes a Korean grapheme model called 'Auto Toggle' by using auto switching between consonants and vowels of Hangul. In addition, Auto Toggle is designed and implemented based on the Android platform. The authors describe the results of a performance evaluation for the number of buttons pushed for each single syllable of Hangul compared with conventional methods. Additionally, Auto Toggle results in a rapid improvement on typing speed with respect to sentence generation. Specifically, the efficiency of Auto Toggle is determined to be high because it solves the problem related to button size that has been considered a source of great inconvenience in smartphone soft keyboards and reduced the number of button pushes.

Digital Forensics is being actively researched and performed in a various area against changing IT environment such as smart phone, cloud service and video surveillance. Moreover, it is necessary to research unified digital evidence management for correlation analysis from diverse sources. Meanwhile, various triage approaches have been developed to cope with the growing amount of digital evidence being encountered in criminal cases, enterprise investigations and military contexts. Despite of debating over whether triage inspection is necessary or not, it will be essential to develop a framework for managing scattered digital evidences. The ninth paper, "A Framework for Unified Digital Evidence Management in Security Convergence" by K. Lim and C. Lee, presents a framework with unified digital evidence management for appropriate security convergence, which is based on triage investigation. Moreover, this paper describes a framework in network video surveillance system to shows how XeBag works as unified evidence container for storing diverse digital evidences, which is a good example of security convergence.

Contemporary IM acts as a convenient tool to communicate with global users in real time because of its competitive rate, high availability, robust reliability, and agile mobility. There are some non-volatile data related to the RAM of the computing device in terms of cyber trails that were unknowingly left on the crime scenes. The tenth paper, "The disclosure of an Android smartphone's digital footprint respecting the Instant Messaging utilizing Skype and MSN" by H. Chu et al., provides a generic paradigm for the above cyber crime investigation.

Acknowledgements We would like to thank all authors for their contributions to this special issue. We would also like to thank all editorial staffs for their valuable supports throughout the preparation and

publication of this special issue. Moreover, we extend our thanks to all external reviewers for their excellent help in reviewing the manuscripts.

Stefanos Gritzalis is the Deputy Head of the Dept. of Information and Communication Systems Engineering, University of the Aegean, Greece and the Director of the Laboratory of Information and Communication Systems Security (Info-Sec-Lab). He holds a BSc in Physics, an MSc in Electronic Automation, and a PhD in Information and Communications Security from the Dept. of Informatics and Telecommunications, University of Athens, Greece. He has been involved in several national and EU funded R&D projects. His published scientific work includes 30 books or book chapters, 100 journals and 130 international refereed conference and workshop papers. The focus of these publications is on Information and Communications Security and Privacy. His most highly cited papers have more than 1,700 citations (h-index = 21). He has acted as Guest Editor in 30 journal special issues, and has been involved in more than 30 international conferences and workshops as General Chair or Program Committee Chair. He has served on more than 300 Program Committees of international conferences and workshops. He is an Editor-in-Chief or Editor or Editorial Board member for 20 journals and a Reviewer for more than 50 journals. He has supervised 10 PhD dissertations. He was an elected Member of the Board (Secretary General, Treasurer) of the Greek Computer Society. His professional experience includes senior consulting and researcher positions in a number of private and public institutions. He is a Member of the Association for Computing Machinery (ACM), the Association for Information Systems (AIS), the Institute of Electrical and Electronics Engineers (IEEE) and the IEEE Communications Society "Communications and Information Security Technical Committee".

Justin Z. Zhan is the director of iLab at Department of Computer Science, North Carolina A&T State University. He has previously been a faculty member at Carnegie Mellon University and National Center for the Protection of Financial Infrastructure in South Dakota State. His research interests include Information Assurance, Social Computing, Biomedical Computing and Health Informatics. He is a steering chair of IEEE International Conference on Social Computing (SocialCom), IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT), and IEEE International Conference on BioMedical Computing (BioMedCom). He is currently an editor-in-chief of International Journal of Privacy, Security and Integrity and International Journal of Social Computing and Cyber-Physical Systems. He has served as a conference general chair, a program chair, a publicity chair, a workshop chair, or a program committee member for 150 international conferences and an editor-in-chief, an editor, an associate editor, a guest editor, an editorial advisory board member, or an editorial board member for 30 journals. In recent years, he has published more than 130 articles in peer-reviewed journals and conferences and delivered above 30 keynote speeches and invited talks. He has been a director of National Center for BioMedical Computing, International Institute of Social Computing and Information Assurance, and Institute of Cyber Engineering and Science.

Kitae Jeong received his PhD degree in Graduate School of Information Security from Korea University, Korea, in 2011. He is now a research professor with Center for Information Security Technologies (CIST) at Korea University. He has served as a program chair for an international conference WTA 2012 and a guest editor for Information—An International Interdisciplinary Journal. His research interests include cryptanalysis and design of block ciphers and stream ciphers.