IT convergence security

Hangbae Chang · Jongsung Kim · Jonghyuk Park

Received: 14 February 2013 / Accepted: 15 February 2013 / Published online: 27 February 2013
© Springer Science+Business Media New York 2013

Abstract A recent emerging issue in information technology is the convergence of different kinds of applications. Convergence brings a user-centric environment to provide computing and communication services. In order to realize IT advantages, it requires the integration of security and data management to be suitable for pervasive computing environments. Security convergence refers to the convergence of two historically distinct security functions—physical security and information security—within enterprises; both are integral parts of any coherent risk management program. In this special issue, we have discussed current IT-Converged security issues, security policy and new security services which will lead to successful transfer smart space which is a new paradigm of future.

Keywords Safety and security · Security model and practice · Security convergence · Human factor security

Introduction

The traditional and detailed security management process has been generally divided into three areas including physical, managerial, and technical area. Although such system is under the same governance structure, the object and subject of management are different. Therefore the guarantee of

inter-connectedness amongst management areas is difficult to be realized. Namely, despite each of well-constructed security management system, once the vulnerability of certain area take place, it is not easy to prevent or cope with security breaches/accidents (Anderson 2007; Rahman and Donahue 2010). Hence to take preventive measures against security breaches/accidents, it is necessary to manage three areas (physical, managerial, and technical) in the perspective of integrated management and security management under this point of view is considered as “IT Convergence Security” (Alliance for Enterprise Security Risk Management 2006; Hwangkwon 2011).

Papers in this issue

The goal of this special issue is to provide an opportunity for scientists, engineers, researchers, and practitioners to discuss and exchange their novel ideas, research results, work in progress and experiences on all aspects of IT convergence security.

- (1) The paper “Construction of a Secure Two-Factor User Authentication System using Fingerprint Information and Password” by Woong Go, Kwangwoo Lee and Jin Kwak presented a secure two-factor user authentication system using fingerprint information and password to solve the existing two-factor problem. The proposed scheme is secure against reuse of a fingerprint. It does not need an extra device, so efficiency and accessibility are improved.
- (2) The paper “Content-based Control of HTTPs Mail for Implementation of IT-Convergence Security Environment” by Young Ran Hong and Dongsoo Kim presented a method that controls HTTPs web mail contents by

H. Chang (✉)
Department of Business Administration, Sangmyung University,
Seoul, Korea
e-mail: hbchang@smu.ac.kr

J. Kim
Department of Mathematics, Kookmin University, Seoul, Korea

J. Park
Department of Computer Engineering, Seoul National University
of Science and Technology, Seoul, Korea

- using a proxy server and distributing the SSL (Secure Socket Layer) certificate to user's PC. Using the protocol derived in the present study, HTTPs web mail contents can be controlled as an effect of content-awareness. Network DLP is effected by monitoring, blocking and logging suspicious mail contents using HTTPs.
- (3) The paper "A Secret Sharing Scheme for EBTC using Steganography" by Cheonshik Kim, Dongyoo Shin, Dongil Shin, Raylin Tso and Chin-Nung Yang presented a new method based on Block Truncation Coding (BTC) and the half toning technique for secret sharing of lossy compressed images. Experimental results show that proposed scheme provides secret sharing with proper authentication and acceptable computational complexity.
 - (4) The paper "Fast Password Recovery Attack: Application to APOP" by Fanbao Liu, Yi Liu, Tao Xie, Dengguo Feng and Yumeng Feng presented a fast password recovery attack to application APOP in local that can recover a password with 11 characters in <1 min, recover a password with 31 characters extremely fast, about 6 min, and for 43 characters in practical time. These attacks truly simulate the practical password recovery attacks launched by malware in real life, and further confirm that the security of APOP is totally broken.
 - (5) The paper "Analyzing and comparing the AES architectures for their power consumption" by Ahmet Dogan, S. Berna Ors and Gokay Saldamli presented a new architecture improving the composite field and BMN methods, and show their effectiveness by providing area, time and power dissipation figures. As a result, we see that our improved s-box architectures yields the smallest, fastest and least power consuming circuit for the serial, the outer round pipeline and inner-outer round pipeline implementation of the AES.
 - (6) The paper "Unbalanced states violates RFID privacy" by Imran Erguler, Emin Anarim and Gokay Saldamli presented any RFID authentication protocol involving unbalanced states are traceable to a stateful-adversary and to examine the privacy of some existing protocols and showed that they fail to fulfill untraceability property.
 - (7) The paper "Towards an Accurate Evaluation of Quality of Cloud Service in Service-oriented Cloud Computing" by Shangguang Wang, Zhipiao Liu, Qibo Sun, Hua Zou and Fangchun Yang presented an accurate evaluation approach of QoCS in service-oriented cloud computing. The simulation results demonstrate that proposed approach can perform an accurate evaluation of QoCS in service-oriented cloud computing.
 - (8) The paper "A Practical Implementation of Fuzzy Fingerprint Vault for Smart Cards" by Daesung Moon, Yongwha Chung, Changho Seo, Sung-Young Kim and Jeong-Nyeo Kim implemented the fuzzy fingerprint vault for the smart card environment. Especially, we implemented a complete system carefully and fingerprints having a few minutiae could also be applied accurately by using an adaptive degree of the polynomial. Based on the experimental results using FVC2002 DB1 Set A, we confirm that only the authorized user can access the secret stored in a smart card by providing the valid fingerprint.
 - (9) The paper "A Image Contrast Enhancement for Intelligent Surveillance Systems Using Multi-local Histogram Transformation" by Hwan-Joo Kwak and Gwi-Tae Park presented the multi-local histogram transformation as a contrast enhancement method suitable for surveillance systems. In contrast to conventional histogram enhancement methods, this method includes a consideration of the visual deterioration caused by excessive histogram modification. By using this advantage of the multi-local histogram transformation, surveillance systems can improve image quality and increase the surveillance's ability to identify conditions in remote areas.
 - (10) The paper "The industrial security management model for SMBs in smart work" by Yanghoon Kim and Hangbae Chang presented to design industrial security management model for organizations' industrial technology leakage prevention which is differentiated from those of large enterprises based on current status of small and medium-sized organizations' industrial technology leakage.
 - (11) The paper "Forensic Analysis of Satellite Automotive Navigation Systems: A Case Study in Korea" by Kyung-Soo Lim, Changhoon Lee, Jong Hyuk Park and Sang-Jin Lee presented that valuable features of the user information files stored on Mappy in SD card were analyzed. The analysis confirmed that the navigation software internally stores user information such as data on frequently visited locations and routes.
 - (12) The paper "Study on two privacy-oriented protocols for information communication systems" by Taek-Young Youn and Jongsung Kim presented two protocols and show their insecurities. Authors showed the insecurity of the Hsu-Chuang scheme by describing a known session key attack, in which an adversary can recover the private key of a user or disguise a user. And authors also showed that a malicious service provider can easily recover the private key of a user by executing a number of legitimate runs of the scheme. Moreover, authors provide a simple countermeasure which can enhance the

security of the Hsu-Chuang scheme. Secondly, authors reviewed the Harn-Ren scheme and showed that the scheme has a potential incompleteness and two security weaknesses.

- (13) The paper “Ubiquitous-City Integrated Authentication System (UCIAS)” by Jae-Soo Jang and Hyung-Min Lim presented a U-City Integrated Authentication System (UCIAS), which is a unified authentication model installed in a U-City using the Ubiquitous Role-based Access Control (U-RBAC) protocol—the modified version of the original RBAC protocol.
- (14) The paper “Information Security Strategies: Towards an Organizational Multi-Strategy Perspective” by Atif Ahmad, Sean B. Maynard and Sangseo Park presented a research agenda that calls for research on enterprise-wide multiple strategy deployment with a focus on how to combine, balance and optimize strategies.

References

- Anderson, K. (2007). Convergence: A holistic approach to risk management. *Network Security*, 7, 2007.
- Alliance for Enterprise Security Risk Management. (2006). Convergent security risks in physical security systems and IT infrastructures. *ISACA Information Security Management Conference, 2006*.
- Hwangkwon, A. (2011). A study on the development of convergence security with the changes in security environments. *Journal of Information and Security*, 11(5), 31–40.
- Rahman, S. M., & Donahue, S. E. (2010). Convergence of corporate and information security. *International Journal of Computer Science and Information Security*, 7(1), 63–68.