Editorial

Most of all, it is my great pleasure to share with you the news that our journal belongs to Q2 class as well as has 1.73 cites per doc according to Scopus. Indeed, it is a meaningful achievement, which makes us proud.

This third issue of 2014 collects six papers, most of which are extended from the selected papers presented at the 2014 Asian Conference on Availability, Reliability and Security (AsiaARES 2014)[1].

- The first article "Efficient variant of Rainbow using sparse secret keys" [1] focuses on improving Rainbow, which is a Multivariate Public Key Cryptosystems (MPKC) digital signature scheme. The authors combine two variants of Rainbow, which reduce the secret key size and accelerate the signature generation by using sparse secret keys. As a result, the combined scheme achives smaller key size as well as more efficient signature generation than those of the two variants.

- In the second article "Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing" [2], the authors present a security assessment technique for computer networks, which is based on the attack graphs as well as can be applied for contemporary Security Information and Event Management (SIEM) systems. For the proposed technique, the security metrics are defined by differentiating available input data, and used to decide current security situation including development of attacks, attacks sources and targets, attackers' characteristics. A case study is given to show how the suggested technique is applied.

- The next article "A Model-Driven Approach to Noninterference" [3] introduces a model-driven approach, which supports to develop with secure information flow the systems composed of mobile apps and web services based on intuitive modeling guidelines. Especially, the authors describe the automatic generation of the formal model and highlight several advantages which the proposed model-driven approach can bring for the practical application of information flow control.

- In the fourth article "Genie in a Model? Why Model Driven Security will not secure your Web Application" [4], the authors comprehensively evaluate current Model Driven Security (MDS) approaches based on a web application scenario regarding the most common web security attacks. Moreover, they discuss the strengths and limitations of the MDS approaches as well as the practicability of MDS for modern web application security in general.

- The next article "Evaluating data utility of privacy-preserving pseudonymized location datasets" [5] studies tradeoffs between user privacy and data utility in a pseudonymized datasets. For this goal, the authors conduct various experiments with a real location dataset including mobility traces of taxi cabs in San Francisco, USA. According to the experimental results, it is feasible to satisfy realistic privacy requirements as well as provide sufficient data utility.

- The final paper "Secure and Scalable Multimedia Sharing between Smart Homes" [6] evaluates the architecture for multimedia sharing in smart home environments, which was previously introduced by the authors. Especially, it deeply analyzes scalability, security and fault tolerance aspects of their architecture, and then shows that the architecture can allow each user to easily gain access to various types of resources at home while roaming to other users' home networks once authenticating his or her terminal with a node in the home or visited environment.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 5, number: 3, pp. 1-2

[1] AsiaARES 2014 was held in Bali, Indonesia, on April 14th - 17th, 2014. `http://http://asiaares.org/`

Finally, my special thanks are extended to authors as well as reviewers for their contribution, which makes this issue a reality.

Dr. Ilsun YOU, FIET[2]
Editor-in-Chief
September 2014

References

[1] T. Yasuda, T. Takagi, and K. Sakurai, "Efficient variant of rainbow using sparse secret keys," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 3–13, September 2014.

[2] I. Kotenko and E. Doynikova, "Evaluation of computer network security based on attack graphs and security event processing," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 14–29, September 2014.

[3] K. Stenzel, K. Katkalov, M. Borek, and W. Reif, "A model-driven approach to noninterference," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 30–43, September 2014.

[4] C. Hochreiner, P. Frühwirt, Z. Ma, P. Kieseberg, S. Schrittwieser, and E. Weippl, "Genie in a model? why model driven security will not secure your web application," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 44–62, September 2014.

[5] T. Tanjo, K. Minami, K. Mano, and H. Maruyama, "Evaluating data utility of privacy-preserving pseudonymized location datasets," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 63–78, September 2014.

[6] R. U. Islam, M. Schmidt, H.-J. Kolbe, and K. Andersson, "Secure and scalable multimedia sharing between smart homes," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 3, pp. 79–93, September 2014.

[2]Associate Professor, Dept. of Computer Software, Korean Bible University, Seoul, Republic of Korea, Email: isyou@bible.ac.kr