

Editorial

I would like to warmly welcome readers to the volume 5, number 4 of *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. In addition, I am very delight to see that the volume 5 is now well ended.

This issue is composed of six regular articles, which provide useful and meaningful research results related to the fields of the wireless mobile networks, ubiquitous computing, and dependable applications.

- The first article “Empowering Personal Health Records with Cloud Computing: How to encrypt with forthcoming fine-grained policies efficiently” [1] aims at allowing patients to control the access to their Personal Health Record (PHR) efficiently and easily though the emerging cloud technology. For this goal, the authors propose the notion of Online/Offline Ciphertext-Policy Attribute-Based Proxy Re-Encryption scheme (OOC-AB-PRE) and a set of security requirements while defining two security models, which cover both outsider and insider attacks. Moreover, a concrete OO-CP-AB-PRE construction is built, and proven to be secure under the well known complexity assumptions and follow the defined security models.
- In the second article “Anomaly Detection in Computer Networks: A State-of-the-Art Review” [2], the authors survey the state-of-the-art studies on the problem of anomaly detection in computer networks. They don’t only describe the anomaly detection problem and the different categorizations of its solutions, but also introduce some recent state-of-the-art solutions on the network level and current trends in handling malware-induced anomalies in smartphone networks. Furthermore, the presented solutions are evaluated while their shortcomings are highlighted.
- In the next article “eCK Secure Single Round ID-based Authenticated Key Exchange Protocols with Master Perfect Forward Secrecy (Extended Version)” [3], the authors extend and complete their preliminary version presented at the 2014 Network and System Security (NSS’14), Xi’an, China, October 15-17, 2014 [4]. Note that the preliminary version proposed the first ID-based extended Canetti-Krawczyk (eCK) secure single round Authenticated Key Exchange (AKE) protocols with *Perfect Forward Secrecy* (PFS) and *Master Perfect Forward Secrecy* (MPFS) in the random oracle model. This article provides formal proofs to show that all these protocols are secure under the *Gap Bilinear Diffie-Hellman* (GBDH) problem.
- The fourth article “Design of Virtual Local Area Network Scheme Based on Genetic Optimization and Visual Analysis” [5] presents an approach to genetic optimization of Virtual Local Area Network (VLAN) scheme using the developed software — VLAN scheme design tool. The authors provide a formal statement of the problem of VLAN scheme optimization as well as show that the problem considered is related to one of the forms of Boolean Matrix Factorization. Through the VLAN scheme design tool, it is possible to solve the problem by genetic optimization, form a visual representation of the progress of solving the problem, and provide an estimation of the genetic algorithm. According to the experimental results, the proposed genetic algorithm achieves high effectiveness.
- In the next article “Mobile App Security Analysis with the MAVeriC Static Analysis Module” [6], the authors present the Static Analysis Module (SAM), a toolkit which integrates and orchestrates the reverse engineering, permission checking, code review, malware analysis, and application verification modules to support automatic assessment of Android applications. Especially, the SAM

serves as the core component of the Mobile Application Verification Cluster (MAVeriC) platform, which is a framework for the systematic security analysis of third-party mobile apps. The SAM's features are demonstrated by analyzing real Android applications.

- The final paper “Flow Mobility Management in PMIPv6-based DMM (Distributed Mobility Management) Networks” [7] proposes a flow mobility-enabled scheme employing PMIPv6-based distributed mobility management architecture. In this scheme a centralized control function manages device location and flow information while a distributed mobile function routers forward data packets. The numerical analysis shows that the proposed scheme achieves better packet delivery cost compared to the centralized ones.

Finally, I would like to specially thank both authors and reviewers for their countless contribution.

Dr. Ilsun YOU, FIET¹
Editor-in-Chief
December 2014

References

- [1] C. Gritti, W. Susilo, T. Plantard, K. Liang, and D. S. Wong, “Empowering personal health records with cloud computing: How to encrypt with forthcoming fine-grained policies efficiently,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 3–28, December 2014.
- [2] S. A.-H. Baddar, A. Merlo, and M. Migliardi, “Anomaly detection in computer networks: A state-of-the-art review,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 29–64, December 2014.
- [3] T. Pandit, R. Barua, and S. Tripathy, “eck secure single round id-based authenticated key exchange protocols with master perfect forward secrecy (extended version),” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 65–85, December 2014.
- [4] T. Pandit and R. Barua, “eck secure single round id-based authenticated key exchange protocols with master perfect forward secrecy,” in *Proc. of the 8th International Conference on Network and System Security (NSS'14), Xi'an, China, LNCS*, vol. 8792. Springer International, October 2014, pp. 435–447.
- [5] I. Saenko and I. Kotenko, “Design of virtual local area network scheme based on genetic optimization and visual analysis,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 86–102, December 2014.
- [6] A. Armando, G. Bocci, G. Chiarelli, G. Costa, G. D. Maglie, R. Mammoliti, and A. Merlo, “Mobile app security analysis with the maveric static analysis module,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 103–119, December 2014.
- [7] K. Sun and Y. Kim, “Flow mobility management in pmipv6-based dmm (distributed mobility management) networks,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 5, no. 4, pp. 120–127, December 2014.

¹Associate Professor, Dept. of Computer Software, Korean Bible University, Seoul, Republic of Korea, Email: isyou@bible.ac.kr