Editorial

This issue is composed of four papers, which provide innovative research results related to the fields of insider threats and mobile software security. Especially, the first three papers are the fully extended versions, whose preliminary one was originally presented at the 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST'15)[1].

- In the first article "Ben-ware: Identifying Anomalous Human Behavior in Heterogeneous Systems Using Beneficial Intelligent Software" [1], the authors introduce the concept of "Ben-ware", which is a beneficial software system that makes use of low-level data collection from employees' computers to detect anomalous behavior of an employee. In order to minimize the risk of false positives, this work attempts to utilize human factors, artificial intelligence, and risk analysis through an interdisciplinary collaboration involving computer scientists, a criminologist and behavioral analysis experts. It is demonstrated that Ben-ware enables to detect potentially malicious acts as well as has low impact on the resources of the organization.

- In the second article "Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data" [2], the authors aim to detect insider threats by analyzing enterprise social and online activity data of employees. For such an aim, two approaches are studied: the unsupervised and supervised approaches. Especially, these approaches are tested with a real world data set with artificially injected insider threat events. The test results show that the proposed approaches are effective in identifying insider threat events.

- In the next article "Towards a Cyber Ontology for Insider Threats in the Financial Sector" [3], the authors aim at classifying insider attack suspicions by using an ontology they develop, which focus on insider attacks in the banking domain targeting database systems. This paper's contributions are as follows: (i) supporting the security experts in the investigation process (ii) developing a framework of a cyber ontology for insider threats in the financial sector with focus on relational database management systems (iii) integrating this ontology with commonly used ontologies (iv) using ontologies as a supporting mechanism to verify the outcome of other anomaly detection systems.

- The final paper "Effects of Code Obfuscation on Android App Similarity Analysis" [4] analyzes empirically the effects of code obfuscation on Android app similarity analysis. The authors make the empirical measurements on five different Android apps with DashO obfuscator. According to the experimental results, similarity measures at bytecode level are more effective than those at source code level to analyze software similarity.

Last but not the least, I would like to express my special thanks to authors and reviewers for their countless contribution.

Dr. Ilsun YOU, FIET[2]
Editor-in-Chief
December 2015

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 4, pp. 1-2

[1] MIST'15 was held as one of ACM CCS 2015 workshops. For details, refer to `http://isyou.info/conf/mist15/`

[2] Associate Professor, Dept. of Information Security Engineering, Soonchunhyang University, Asan-si, Republic of Korea, Email: isyou@sch.ac.kr

References

[1] A. S. McGough, B. Arief, C. Gamble, D. Wall, J. Brennan, J. Fitzgerald, A. van Moorsel, S. Alwis, G. Theodoropoulos, and E. Ruck-Keene, "Ben-ware: Identifying anomalous human behaviour in heterogeneous systems using beneficial intelligent software," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 4, pp. 3–46, December 2015.

[2] G. Gavai, K. Sricharan, D. Gunning, J. Hanley, M. Singhal, and R. Rolleston, "Supervised and unsupervised methods to detect insider threat from enterprise social and online activity data," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 4, pp. 47–63, December 2015.

[3] G. Kul and S. Upadhyaya, "Towards a cyber ontology for insider threats in the financial sector," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 4, pp. 64–85, December 2015.

[4] J. Park, H. Kim, Y. Jeong, S. je Cho, S. Han, and M. Park, "Effects of code obfuscation on android app similarity analysis," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 4, pp. 86–98, December 2015.