

Recent trends on high-performance computing and security

Jong-Hun Kim · Joong-Kyung Ryu

Published online: 10 May 2013
© Springer Science+Business Media New York 2013

High performance systems and distributed environment usually deployed to improve users' performance and availability. Recent years, High performance systems and distributed environment suffer from security issues and certain vulnerabilities became the sweetest targets to attackers. Some attacks easily and widely transmit other systems, and lead to uncountable financial losses in addition to performance and availability malfunctions. This special issue presents the recent researches in high performance systems and security for better performance and availability as well as for avoiding vulnerabilities, whose topics are certainly the hottest topics in High-Performance Computing and Security [1–3]. We believe that this special issue will have a high citation in the areas of Cluster Computing.

- Cluster Computing and Solutions
- Reconfigurable, Adaptable, and Reflective Approaches
- Digital Convergence Solutions for Ubiquitous Computing
- Multimedia Modeling, Analysis, Design and Management
- Ubiquitous Multimedia for Cluster Computing and Personal Area Networks
- Digital Convergence for Services and Composition
- Software Modeling, Development and Maintenance for Convergence
- Methodologies and Tools for Designing, Implementing, Verifying, and Evaluating Systems

J.-H. Kim (✉) · J.-K. Ryu
Department of Computer Software, Daelim University,
29, Imgok-ro, Dongan-gu, Anyang-si, Gyeonggi-do 431-715,
Republic of Korea
e-mail: ddcome11@daum.net

J.-K. Ryu
e-mail: jkryu@daelim.ac.kr

The first paper, by Kim et al., presents a frequency monitoring system development for wide-area power grid protection. They introduce a system for monitoring regional frequencies in power grid developed as an advanced research project for intelligent wide-area protective relaying in South Korea. They proposed implemented by modeling an actual 345 kV transmission system of South Korea using EMTP-RV and by measuring voltages and currents at five main regions. This monitoring system by incorporating information technology into the power system clustering, They were able to implement a prototype of the frequency monitoring system to assess feasibility of application in actual power grids, and also analyze system's functionality and further requirements.

The second paper, by Lee Park et al., introduces an abnormal event correlation analysis for convergence security monitor. They developed collection interface in each system of study of security policy violation event in physical security area, study of event normalization, and they proposed the method which can classify the information leaker through data mining for human security following the advancements of events. It is collection interface in each system of study of security policy violation event in physical security area, study of event normalization. Also, using normalizing and correlation analysis engine, it makes possible to control the converged security control in real-time.

The third paper, by Kang et al., presents a IP trace back with sparsely-tagged fragment marking scheme under massively multiple attack paths. They proposed a method that optimizes the three parameters at the same time and recovers original IPs quickly and correctly even in the presence of massive multiple attack paths. Also, They technique focuses on PPM, especially with tagging. The proposed algorithm consists of two parts. One is the on/off marking process and the other is the recovery process. The suggested technique

has been rigorously analyzed mathematically and tested extensively through simulation with promising results. The results showed that our method recovers 95 % of the original IPs correctly with no fragment combinations and with zero false positives even in the presence of massive multiple attack paths.

The fourth paper, by Han et al., introduces a DDoS avoidance strategy to provide service availability to those preregistered important users. They proposed strategy, we divide the attack scenario in different time points and provide alternative access channels to already authenticated and other valid users. They separate three different states of the system (green, red, and black) depending of the level of traffic to describe how important users registered previously can receive continuously the critical services even while the attack is being executed. The result of it means that an attack can be executed selectively in several layers of the network, can use different number of bots, and does not have any limitation of where the attack is executed.

This fine collection of papers was achieved by fruitful collaborations. We gratefully acknowledge and express heartfelt thanks to all the authors for their worthy contribution to this special issue. We also would like to thank all the members of the Program Committee and anonymous reviewers for their help in identifying the novel papers and for their careful reading of earlier drafts. Furthermore, we would like to thank Professor Salim Hariri, editor-in-chief of the international research journals Cluster Computing, for his valuable remarks and his undeterred help throughout the publication process of this special issue.

References

1. Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D.: DDoS tolerant networks. In: IEEE International Conference on DARPA Information Survivability Conference and Exposition (DISCEX2003), pp. 73–75 (2003)
2. Wu, Y.C., Tseng, H.R., Yang, W., Jan, R.H.: DDoS detection and traceback with decision tree and grey relational analysis. In: IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE2008), pp. 306–314 (2009)
3. Cabrera, J.B.D., Lewis, L., Qin, X., Gutierrez, C., Lee, W., Mehra, R.K.: Proactive intrusion detection and SNMP based security management. In: Proceedings of IFIP/IEEE Eighth International Symposium on Integrated Net Work Management, pp. 225–254 (2003)



Jong-Hun Kim received B.S. degree from Physics, University of Incheon, Korea, in 2001. He received M.S. and Ph.D. degree in Computer Science & Information Engineering from Inha University, Korea, in 2003 and 2010. From 2010 to 2012, he has been manager of U-Healthcare Department, BIT Computer Co., Ltd. He is currently a professor in the Department of Computer Software, Daelim University, Korea. His research interests include u-healthcare, data mining and artificial intelligence.



Joong-Kyung Ryu received the B.S. degree from Department of Computer Science and Engineering, Korea National Open University, Korea, in 1988 and the M.S. degree from the Department of Information Engineering, Inha University, Korea in 1991. He got Ph.D. degree from the Department of Computer Information Engineering, Inha University, Korea in 2012. From 1983 to 1992, he has been researcher of Department of Computer Center, Daelim Industrial Co., Ltd. He is currently a professor in the Department of Computer Software, Daelim University, Korea. His research interests include computer architecture, u-healthcare, data mining, and HCI.