Guest Editorial: Information Leakage Prevention in Emerging Technologies (MIST 2012 Volume 2)

Kangbin Yim*
Soonchunhyang University
Shinchang, Asan, Republic of Korea
yim@sch.ac.kr

Yoshiaki Hori
Dept. of Informatics
Kyushu University, Fukuoka, Japan
hori@inf.kyushu-u.ac.jp

The ICT (Information and Communication Technologies) infrastructure has been tremendously changed during the last couple of decades and the result made a big change in the computing environment. Due to this drastic advance, now we are enjoying a convenient living environment that we couldn't have ever experienced before. In addition to this situation, the prospective emerging technologies such as the cloud computing and the mobile computing are newly approached and trying to realize a new life infrastructure combined with so-called a whole-cyber complex that is becoming fully connected and proportional to our real world. These results of this evolutionary transformation are part of essential components of the world with the augmented three dimensional common user interface to a single unified cyber-physical space.

Even though the convenience the ICT environment gives, some accompanied adverse activities have been arisen continuously. In particular, the information leakage is a severe one of these problems. Due to the features of the digitalized data, which are pseudo-invisible and pseudo-conceptual, they tend to be more easily exposed to others than the physical resources in the traditional environment. Moreover, the situation is becoming worse because these data are extended to include such sensitive information as personal privacy and enterprise secrets. Additionally, adversaries can easily deceive legitimators though the legitimators have difficulties to detect the adversaries during a leakage happens. For example, the user passwords are stealthily duplicated through eavesdropping the keyboard inputs. Even secure USB memories are completely copied through several trials of reversing. To make the problem worse, the networked environment may also provide potential covert holes for the leakage.

As the information leakage has been one of the most concerned problems in the existing ICT environment, this will still look much more serious in the new cyber-physical environment because its complex combinations of vulnerabilities may become the foundation for potential leaks. Even though many researches have been trying to evade the problem, preventing the information leakage is still more than a degree of challenge, of which technologies span from theories to practices including cryptography, access control, management, assessment and etc. As mentioned, the two representative entities in the new environment will be the cloud and the mobile, which are the server and the client in the new service space. In public cloud services, many independent people or companies may delegate processing and storing most of their own information to unauthorized remote agents and access it through the mobile clients. Unauthorized leak of critical information in this case can cause a significant damage to the agent's reputation and to the customers' property as well.

For this special issue, we qualified the presentations in MIST2012[1](The 4th International Workshop on Managing Insider Security Threats held on November 8-9, 2012 at Kyushu University in Japan) and the thirteen best papers were carefully selected through several rounds of strict three reviews. During

Journal of Internet Services and Information Security (JISIS), volume: 2, number: 3/4, pp. 1-2

*Corresponding author: LISA Laboratory, Soonchunhyang University, 9418 Engineering Building, 646 Eupnae, Shinchang, Asan, 336-745 Republic of Korea, Tel: +82-(0)41-530-1741, Web: http://lisa.sch.ac.kr

[1]http://isyou.info/conf/mist12/

the selection, we also considered the papers to cover different aspects of the information leakage and its prevention. We believe that these papers will contribute to the practical development and the theoretical extension in this field. We would like first to give thanks to all authors for their submitted papers and the efforts found in revising the manuscripts based on the feedbacks from reviewers. We also would like to appreciate the efforts of the reviewers for their detailed comments and advises. At last, we would like to extend our special thanks to Dr. Ilsun You, the Editor-in-Chief of *Journal of Internet Services and Information Security*, for the invitation to the work on this special issue.

Kangbin Yim and Yoshiaki Hori
Guest Editors
November 2012

Kangbin Yim received his B.S., M.S., and Ph.D. from Ajou University, Suwon, Korea in 1992, 1994 and 2001, respectively. He is currently an associate professor in the Department of Information Security Engineering, Soonchunhyang University. He has served as an executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as a committee chair of the international conferences and workshops and the guest editor of the journals such as JIT, MIS and JoWUA. His research interests include vulnerability assessment, code obfuscation, malware analysis, leakage prevention, secure platform architecture and mobile security. Related to these topics, he has worked on more than forty research projects and published more than ninety research papers.

Yoshiaki Hori received B.E., M.E, and D.E. degrees on Computer Engineering from Kyushu Institute of Technology, Iizuka, Japan in 1992, 1994, and 2002 respectively. From 1994 to 2003, he was a Research Associate at the Common Technical Courses, Kyushu Institute of Design. From 2003 to 2004, he was Research Associate at the Department of Art and Information Design, Kyushu University. From 2004, he was an Associate Professor at the Department of Computer Science and Communication Engineering, Kyushu University. Since 2009, he has been an Associate Professor of the Department of Informatics, Kyushu University. His research interests include network security, network architecture, and performance evaluation of network protocols on various networks. He is a member of IEEE, ACM, and IPSJ.