Guest Editorial: Frontiers in Insider Threats and Data Leakage Prevention*

Yoshiaki Hori
Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
hori@inf.kyushu-u.ac.jp

William Claycomb
CERT Program†
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA, USA
claycomb@cert.org

Kangbin Yim
Soonchunhyang University, Dept. of Information Security Engineering
646 Eupnae, Shinchang, Asan, Korea
yim@sch.ac.kr

Organizations continue to be plagued by information leaks caused by insiders with legitimate access to critical or proprietary information. Such unauthorized leaks may result in significant damage to competitiveness, reputation and finances, and organizations should consider proactive approaches to preventing, detecting, and responding to this threat. In this special issue, we have selected eight papers describing recent work on insider threat and data leakage prevention. These include four papers [1][2][3][4] derived from the third International Workshop on Managing Insider Security Threats (MIST 2011)[1] in conjunction with the third IEEE International Conference on Intelligent Networking and Collaborative Systems (IEEE INCoS 2011).

In the first paper, titled "From Insider Threats to Business Processes that are Secure-by-Design" [1], the author suggests that insider threat is a placeholder term indicating the transition from securing IT infrastructures to securing the socio-technical systems. While observing that the concept of an insider is not helpful in today's dynamic heterogeneous organizations, he adopts "business processes that are secure-by-design (sustainable business processes)" as a new paradigm where those processes remain viable even when attacks are launched with insider knowledge. Finally, the author presents two research challenges for the sustainable business processes, modelling socio-technical systems and exploring the foundations of judgement-based risk analysis methods.

The second paper, titled "Combining Baiting and User Search Profiling Techniques for Masquerade Detection" proposes an integrated masquerade detection to combine user behavior profiling with a baiting technique [5]. The proposed approach reduces false positives when compared to user behavior profiling alone. In addition, it is shown that this approach can harden a masquerade attack detector against mimicry attacks.

In the third paper, titled "A Certificateless Ordered Sequential Aggregate Signature Scheme Secure against Super Adversaries" [2], the authors propose an ordered sequential aggregate signature in certificateless setting. Further, they discuss its security against super adversaries who can obtain signature of a target signer but without providing a secret value for a challenger.

The fourth paper titled "Security Analysis of Offline E-cash Systems with Malicious Insider" analyses security of offline anonymous electronic cash systems. This includes recent systems based on the

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

*This special issue is sponsored by National Institute of Information and Communications Technology (NICT), Japan (http://www.nict.go.jp/) and Lab. of Information Systems Security Assurance (LISA) at Soonchunhyang University, Korea (directed by Prof. Kangbin Yim, http://lisa.sch.ac.kr/)

†CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

[1]MIST 2011 was held in Fukuoka, Japan from December 1st to the 2nd, 2011,
`http://isyou.hosting.paran.com/mist11/`

classification of Miyazaki and Sakurai, who systemically analyzed security of offline anonymous electric cash systems by considering insider threats from untrusted authorities [3].

In the fifth paper, titled "A New Trapdoor-indistinguishable Public Key Encryption with Keyword Search" [6], the authors construct an efficient trapdoor-indistinguishable public key encryption with keyword search. They also prove their proposed scheme satisfies PEKS ciphertext indistinguishably and trapdoor indistinguishably without a secure channel between the receiver and the server.

In the sixth paper, titled "A Thief among Us: The Use of Finite-State Machines to Dissect Insider Threat in Cloud Communication" [7], the authors propose a user behavior analysis method by using finite state machine expressions to represent emotional patterns based on trustworthiness attribution theory. They apply their method to virtual betrayal simulation in which virtual teams play a game online.

The seventh paper, titled "A Framework for Detecting Insider Threats using Psychological Triggers" proposes a framework to detect a malicious insider behavior by examining target reaction patterns that are impelled by a psychological trigger[4]. The framework focuses on two malicious users' reactions: deleting evidence and stopping further malicious activities. Also, the author extends the architecture for monitoring servers such as file servers and IMAP email servers as well as clients.

The final paper, titled "Inter-domain Communication Protocol for Real-time File Access Monitor of Virtual Machine" presents an interdomain communication protocol for real-time monitoring of virtual machine and bridging semantic gap [8]. They describe an interdomain communication module between a guest Windows virtual machine and a hypervisor. The communication module enables to monitor the file access of a guest Windows OS in real-time without suspending it.

Finally, with Dr. Ilsun You, the Editor-in-Chief of *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, we would like to extend our special thanks to the authors and reviewers for their countless contribution and dedication to this special issue.

Yoshiaki Hori, William Claycomb, and Kangbin Yim
Guest Editors
March, 2012

References

[1] D. Gollmann, "From Insider Threats to Business Processes that are Secure-by-Design," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 4–12, March 2012.

[2] N. Yanai, R. Tso, M. Mambo, and E. Okamoto, "A Certificateless Ordered Sequential Aggregate Signature Scheme Secure against Super Adverssaries," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 30–54, March 2012.

[3] T. Nishide, S. Miyazaki, and K. Sakurai, "Security Analysis of Offline E-cash Systems with Malicious Insider," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 55–71, March 2012.

[4] T. Sasaki, "A Framework for Detecting Insider Threats using Psychological Triggers," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 99–119, March 2012.

[5] M. B. Salem and S. J. Stolfo, "Combining Baiting and User Search Profiling Techniques for Masquerade Detection," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 13–29, March 2012.

[6] Y. Zhao, X. Chen, H. Ma, Q. Tang, and H. Zhu, "A New Trapdoor-indistinguishable Public Key Encryption with Keyword Search," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 72–81, March 2012.

[7] S. M. Ho and H. Lee, "A Thief among Us: The Use of Finite-State Machines to Dissect Insider Threat in Cloud Communications," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 82–98, March 2012.

[8] R. Ando, K. Takahashi, and K. Suzaki, "Interdomain Communication Protocol for Real-time File Access Monitor of Virtual Machine," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 1/2, pp. 120–l37, March 2012.

Yoshiaki Hori is Associate Professor of Department of Informatics, Kyushu University, Japan since 2004. He was received B.E., M.E., and D.E. of Computer Science from Kyushu Institute of Technology, Iizuka in 1992, 1994, and 2002, respectively . He was also Research Associate with Common Technical Course of Kyushu Institute of Design in 1994. He is interested in computer network and systems. He is a member of IEICE, IPSJ, IEEE, and ACM.

William Claycomb is the Lead Research Scientist for the CERT Enterprise Threat and Vulnerability Management program at Carnegie Mellon University's Software Engineering Institute. His primary research topic is the insider threat; current work includes discovery of insider threat behavioral patterns and corresponding sociotechnical countermeasures. He received a B.S. in Computer Science from the University of New Mexico, and an M.S. and Ph.D. in Computer Science from the New Mexico Institute of Mining and Technology.

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 as he has joined Dept. of Information Security Engineering, Soonchunhyang University since 2003. His research interests include vulnerability analysis, code obfuscation, metamorphic malware, insider threats, access control and secure hardware and systems security.