MIST 2016: 8th International Workshop on Managing Insider Security Threats

Ilsun You
Department of Information Security Engineering
Soonchunhyang University
22 Soonchunhyangro, Asan-si, Chungnam-do, 336-745
Republic of Korea
ilsunu@gmail.com

Elisa Bertino
Department of Computer Science, Purdue University
305 N. University Street
West Lafayette, IN 47907
bertino@purdue.edu

ABSTRACT
This paper introduces the 8th International Workshop on Managing Insider Security Threats (MIST 2016). MIST 2016 takes place in conjunction with the 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016). Its main goal is to provide a forum for sharing recent challenges and advanced technologies in managing insider security threats.

CCS Concepts
• **Security and privacy**

Keywords
Insider threats; Data leakage prevention; Cyber security and defense

1. INTRODUCTION
Insider threats can be defined as threats by authorized users [1]. Such users typically have access to systems, data, and other sensitive resources within their organizations. Insider attacks can result in critical damages such as theft of confidential data and business secrets, sabotage, fraud, and so forth, which are more severe than the ones by outsiders. Therefore, they are regarded as a significant security risk for organizations [2]. Despite recent extensive research, managing insider threats and attacks still stays one of the most difficult challenges in the areas of security [3, 4].

The MIST workshop has been annually held since 2009 in order to bring together researchers from industry and academia in order to exchange new ideas and approaches in the area of insider threats. We believe that this workshop has remarkably triggered further related research and technology improvements.

The main topics of MIST 2015 include but not limited to:

- Theoretical foundations and algorithms for addressing insider threats
- Insider threat assessment and modeling
- Security and cryptography technologies to prevent, detect and predict insider threats
- Cryptographic protocols against insider threats
- Validating the trustworthiness of staff
- Post-insider threat incident analysis
- Data breach modeling and mitigation techniques
- Registration, authentication and identification
- Certification and authorization
- Database security
- Device control system
- Digital forensic system
- Fraud detection
- Network access control system
- Intrusion detection
- Keyboard information security
- Information security governance
- Information security management systems
- Risk assessment and management
- Log collection and analysis
- Trust management
- IT compliance (audit)
- Continuous auditing
- Corporate ethics, accountability and integrity

2. HISTORY
The MIST workshop has the following history:

- **1st MIST** (in conjunction with IFIPTM 2009)
  June 16, 2009, Purdue University, West Lafayette, USA
- **2nd MIST** (in conjunction with IFIPTM 2010)
  June 15, 2010, Morioka, Iwate, Japan
- **3rd MIST** (in conjunction with InCos 2011)
  December 1-2, 2011, Fukuoka Institute of Technology, Fukuoka, Japan
- **4th MIST**
  November 8-9, 2012, Kyushu University, Fukuoka, Japan
- **5th MIST**
  October 24-25, 2013, Pukyong National University, Busan, Rep. of Korea

CCS'16, October 24-28, 2016, Vienna, Austria
ACM 978-1-4503-4139-4/16/10.
http://dx.doi.org/10.1145/2976749.2990482

- **6th MIST**
  November 21-22, 2014, Konkuk University, Seoul, Rep. of Korea
- **7th MIST**
  October 16, 2015, The Denver Marriot City Center, Denver, Colorado, USA (with ACM CCS 2015)

3. PROGRAM COMMITTEE

We are grateful to the members of the MIST 2016 program committee:

- Ioannis Agrafiotis (Oxford University, UK)
- Joonsang Baek (Khalifa Univ. of Sci., Tech. and Research, UAE)
- Matt Bishop (UC Davis, USA)
- Will Casey (Carnegie Mellon University, USA)
- William R. Claycomb (Carnegie Mellon University, USA)
- Steven Furnell (University of Plymouth, UK)
- Florian Kammuelle (Middlesex University, UK)
- Andrew Stephen MCGough (Durham University, UK)
- Kazuhiro Minami (Institute of Statistical Mathematics, Japan)
- Jose A. Morales (Carnegie Mellon University, USA)
- Jason Nurse (Oxford University, UK)
- Günther Pernul (University of Regensburg, Germany)
- Christian W. Probst (Technical University of Denmark, Denmark)
- Andrew Stephen MCGough (Durham University, UK)
- Malek Ben Salem (Accenture, USA)
- Willy Susilo (University of Wollongong, Australia)
- Hassan Takabi (University of North Texas, USA)
- Shambhu Upadhyaya (SUNY Buffalo, USA)
- Danfeng (Daphne) Yao (Virginia Tech, USA)
- Meng Yu (The University of Texas at San Antonio, USA)
- Quanyan Zhu (NYU Tandon School of Engineering, USA)

In addition, our thanks go to the following reviewers:

- Gaurang Gavai (PARC, USA)
- Yassir Hashem (University of North Texas, USA)
- Gökhan Kul (The State University of New York at Buffalo, USA)
- Alessio Merlo (University of Genova, Italy)

4. WORKSHOP ORGANIZERS

Ilsun You (general co-chair) received his M.S. and Ph.D. degrees in Computer Science from Dankook University, Seoul, Korea in 1997 and 2002, respectively. Also, he obtained his second Ph.D. degree from Kyushu University, Japan in 2012. Now, he is working as an associate professor at Soonchunhyang University, Republic of Korea. Dr. You has published more than 120 papers and 30 special issues in his main areas including internet security, formal security analysis, and insider threats. He is now serving as EiC of Journal of Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). He is a Fellow of the IET and a Senior member of the IEEE.

Elisa Bertino (general co-chair) is professor of computer science at Purdue University, and serves as Director of the Purdue Cyber Space Security Lab (Cyber2SLab). She is also an adjunct professor of Computer Science & Info Tech at RMIT. Prior to joining Purdue in 2004, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory (now Almaden) in San Jose, at the Microelectronics and Computer Technology Corporation, at Rutgers University, at Telcordia Technologies. Her recent research focuses on data security and privacy, digital identity management, policy systems, and security for drones and embedded systems. She is a Fellow of ACM and of IEEE. She received the IEEE Computer Society 2002 Technical Achievement Award, the IEEE Computer Society 2005 Kanai Award and the 2014 ACM SIGSAC outstanding contributions award. She is currently serving as EiC of IEEE Transactions on Dependable and Secure Computing.

5. ACKNOWLEDGMENTS

We would like to extend our sincere thanks to all authors who submitted papers as well as the program committee members for their timely and nice review work.

6. REFERENCES

[1] G. Gavai, K. Sricharan, D. Gunning, J. Hanley, M. Singhal, and R. Rolleston, 2015. 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*. 6, 4 (December 2015), 47-63.

[2] G. Kul and S. Upadhyaya , Towards a Cyber Ontology for Insider Threats in the Financial Sector 2015, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.* 6, 4 (December 2015), 64-85.

[3] Huth , C. L., Chadwick , D. W., Claycomb , W. R., and You, I., 2o13. Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers*. 15, 1 (Mar. 2013), 1-4.

[4] C. W. Probst, I. You, D. Shin, and K. Sakurai , 2011, Guest Editorial: Addressing Insider Threats and Information Leakage, 2, 1 (March 2011), 1-3