MIST 2017: 9th 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 9th International Workshop on Managing Insider Security Threats (MIST 2017), which takes place in conjunction with the 24th ACM Conference on Computer and Communications Security (ACM CCS 2017). Its objective is to present recent challenges and advanced technologies in managing insider security threats by publishing high-quality work that will be a trigger for further research related to this subject.

CCS Concepts

• **Security and privacy**

Keywords

Insider threats; Data leakage prevention; Cyber security and defense

1. INTRODUCTION

Insider threats refer to the jeopardise to operations caused by sanctioned users having adequate access to the system, data, or any other sensitive information of their organizations [1]. These threats are astronomically hazardous as these can result in access to confidential data, disclosing business information, defamation, embezzlement, etc [2, 3]. Such threats are more perplexed and difficult to identify than the ones caused by outsiders [4]. There have been a plethora of research in this direction, but still, this is one of the most arduous challenges in the areas of security.

The MIST workshop has been annually held since 2009 to assemble researchers from industry and academia to exchange incipient conceptions and approaches in the area of insider threats with practical paramountcy. We believe that this workshop has remarkably triggered further cognate research and technology amelioration.

The main topics of MIST 2017 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 '17, October 30-November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3148525

- **6thMIST**
  November 21-22, 2014, Konkuk University, Seoul, Rep. of Korea
- **7thMIST** (in conjunction with ACM CCS 2015)
  October 16, 2015, The Denver Marriot City Center, Denver, Colorado, USA
- **8thMIST** (in conjunction with ACM CCS 2016)
  October 28, 2016, Hofburg Palace, Vienna, Austria

3. PROGRAM COMMITTEE

We are grateful to the members of the MIST 2017 program committee:

- Ioannis Agrafiotis (Oxford University, UK)
- Joonsang Baek (Khalifa University of Science, Technology and Research, UAE)
- William Casey (Software Engineering Institute - Carnegie Mellon University, USA)
- William R. Claycomb (Carnegie Mellon University, USA)
- Ing-Ray Chen (Virginia Tech, USA)
- Raymond Choo (The University of Texas at San Antonio, USA)
- Steven Furnell (University of Plymouth, UK)
- Florian Kammuelle (Middlesex University, UK)
- Fang-YieLeu (Tunghai University, Taiwan)
- Jason Nurse (Oxford University, UK)
- W. Michael Petullo (United States Military Academy, West Point, USA)
- Christian W. Probst (Technical University of Denmark, Denmark)
- Kyung-Hyune Rhee (Pukyong National University, South Korea)
- Malek Ben Salem (Accenture, USA)
- Fei Song (Beijing Jiaotong University, China)
- Hassan Takabi (University of North Texas, USA)
- Danfeng (Daphne) Yao (Virginia Tech, USA)
- Jeong Hyun Yi (Soongsil University, South Korea)
- Meng Yu (The University of Texas at San Antonio, USA)
- Quanyan Zhu (New York University, USA)

In addition, our thanks go to the following reviewer:

- Gökhan Kul (The State University of New York at Buffalo, USA)
- Vishal Sharma (Soonchunhyang University, South Korea)

4. WORKSHOP PROGRAM

MIST 2017 is held on October 30, 2017 as one day. It is composed of presentations for the 7 full and 5 short accepted papers. In addition, we invite one keynote, where Dr. Kim-Kwang Raymond Choo from The University of Texas at San Antonio talks about "Research Challenges and Opportunities in Big Digital Forensic Data".

5. 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.

6. 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.

7. REFERENCES

[1] I. Agrafiotis, A. Erola, M. Goldsmith, and S. Creese, 2017, Formalising policies for insider-threat detection: A tripwire grammar. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 8, 1, (March 2017), 26-43.

[2] F. Kammüller, M. Kerber, and C. W. Probst, 2017, Insider Threats and Auctions: Formalization, Mechanized Proof, and Code Generation. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 8, 1, (March 2017), 44-78.

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

[4] C. W. Probst, I. You, D. Shin, and K. Sakurai, 2011, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Guest Editorial: Addressing Insider Threats and Information Leakage, 2, 1 (March 2011), 1-3.