Guest Editorial: Addressing Insider Threats and Information Leakage[*]

Christian W. Probst[†]
Technical University of Denmark, Denmark
probst@imm.dtu.dk

Ilsun You
Korean Bible University, Republic of Korea
isyou@bible.ac.kr

Dongwan Shin
New Mexico Tech, USA
doshin@nmt.edu

Kouichi Sakurai
Kyushu University, Japan
sakurai@csce.kyushu-u.ac.jp

Insider threats are one of the problems of organizational security that are most difficult to handle. It is often unclear whether or not an actor is an insider, or what we actually mean by "insider". It also is often impossible to determine whether an insider action is permissible, or whether it constitutes an insider attack. From a technical standpoint, the biggest concern is the discrimination between legal insider actions representing a threat, and legal insider actions representing normal work. This is where many of the standard techniques fail, since they require a clear separation between insiders and outsiders, between "good" employees and attackers. A successful defense against insider threats must therefore not only consider technical approaches, it must also integrate sociological and socio-technical approaches to help identifying insider threats.

This special issue collects a series of papers that discuss different aspects of insider threats and information leakage, one of the main concerns with insider attacks. The focus of the selected articles is on technical approaches to prevent or detect insider attacks, and on techniques for modeling and subsequently identifying insiders.

In the first article [1], "Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques", a broad introduction into the topic of this special issue is given, including a definition of the terms "insider" and "insider threat", as well as technical, socio-technical, and sociological approaches.

The second article [2], "A Preliminary Model of Insider Theft of Intellectual Property", develops two models of insider theft of intellectual property, the Entitled Independent and the Ambitious Leader, and discusses their aspects, especially to identify indicators for early warning. The two models were developed using empirical data from cases involving actual insider compromise.

The next article [3], "Model for a Common Notion of Privacy Leakage on Public Database", discusses how to identify data leakage from public databases. When considering insider threats this is an important technique to use, since it provides a lower bound for the damage an insider can cause; thus shortcomings in data protection can be identified and hopefully be fixed.

One of the technical approaches discussed above, that often are used against insider attacks, is collaborative intrusion detection systems, which use the insights from different location in the network to get better insights into attacks than individual systems. These systems are essential for auditing activity and must therefore be hardened against insider attacks. In [4], "Collaborative Intrusion Detection Networks and Insider Attacks", these collaborative systems are surveyed and their robustness against insider attacks is analyzed.

While technical approaches are essential for detecting insider threats, they often lack support for adding human behavior to their detection mechanisms. The next article [5], "Representing Humans in System Security Models: An Actor-Network Approach", proposes a system model that includes human

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

[*] This special issue is supported by SAKURAI Laboratory at Kyushu University, Japan (http://itslab.csce.kyushu-u.ac.jp/).

[†] He is the leading guest editor for this special issue.

actions, inspired by the sociological actor-network theory, treating humans and non-humans symmetrically. Based on this model, the article discusses algorithms for finding attacks.

However, also models including human actions require techniques for identifying where actors are located, and [6], "Improved Estimation of Trilateration Distances for Indoor Wireless Intrusion Detection", presents a technique that allows more precise location of wireless devices inside of buildings, thus supporting, *e.g.*, location-based access control.

The last paper [7], "Improving Stepping Stone Detection Algorithms using Anomaly Detection Techniques", discusses another technique for improving detection of attackers, by hardening anomaly detection algorithms against evasion.

The articles collected in this special issue discuss important aspects of detecting insider attacks. This requires models that allow to include human actions, and that allow to specify what kind of behavior is of interest. It also requires to be able to audit and detect actions of attackers on the IT infrastructure, currently certainly the main resource used in performing insider attacks. The question of identifying the motivation of inside attackers goes clearly beyond the scope of this special issue, but is equally important and challenging.

Christian W. Probst, Ilsun You, Dongwan Shin and Kouichi Sakurai
Guest Editors
March, 2011

References

[1] J. Hunker and C. W. Probst, "Insiders and insider threats—an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4–27, 2011.

[2] A. P. Moore, D. M. Cappelli, T. C. Carony, E. Shaw, D. Spooner, and R. F. Trzeciak, "A preliminary model of insider theft of intellectual property," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 28–49, 2011.

[3] S. Kiyomoto and K. M. Martin, "Model for a common notion of privacy leakage on public database," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 50–62, 2011.

[4] C. Fung, "Collaborative intrusion detection networks and insider attacks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 63–74, 2011.

[5] W. Pieters, "Representing humans in system security models: An actor-network approach," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 75–92, 2011.

[6] P. Nobles, S. Ali, and H. Chivers, "Improved estimation of trilateration distances for indoor wireless intrusion detection," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 93–102, 2011.

[7] G. D. Crescenzo, A. Ghosh, A. Kampasi, R. Talpade, and Y. Zhang, "Detecting anomalies in active insider stepping stone attacks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 103–120, 2011.

Christian W Probst is an Associate Professor in the department for Informatics and Mathematical Modelling at the Technical University of Denmark, where he works in the section for Language-Based Technologies. The motivation behind Christian's research is to realize systems with guaranteed properties. An important aspect of his work are questions related to safety and security properties, most notably insider threats. He is the creator of ExASyM, the extendable, analysable system model, which supports the identification of insider threats in organisations.

Ilsun You received his M.S. and Ph.D. degrees in Computer Science from Dankook University, Seoul, South Korea in 1997 and 2002, respectively. From 1997 to 2004, he worked for the THINmultimedia Inc., Internet Security Co., Ltd. and Hanjo Engineering Co., Ltd. as a Research Engineer. Since March 2005, he has been an Assistant Professor in the School of Information Science at the Korean Bible University, South Korea. Prof. You has served or is currently serving on the organizing or program committees of international conferences and workshops such as IMIS, CISIS, MobiWorld, MIST and so forth. He is EiC of Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). He is in the editorial board for International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), Journal of Computer Systems, Networks, and Communications (IJSH) and Journal of Korean Society for Internet Information (KSII). His main research interests include Internet security, authentication, access control, MIPv6 and ubiquitous computing.

Dongwan Shin is currently an Associate Professor of the Computer Science and Engineering Department and founding director of the Secure Computing Laboratory at New Mexico Tech. His primary research interest lies in the areas of system and information security, especially in the following areas: access control, digital identity and privacy management, pervasive computing security, and cloud computing. Since he joined New Mexico Tech in 2005, his research has been supported by National Science Foundation, Department of Defense, Sandia Labs, Los Alamos Lab, and Intel. Dongwan received his MS in Computer Science and PhD in Information Technology from the University of North Carolina at Charlotte in 1999 and 2004, respectively.

Kouichi Sakurai received B.E., M.E., and D.E. degrees from Kyushu University, Fukuoka, Japan in 1986, 1988, and 1993, respectively. From 1986 to 1993, he was a Researcher of Mitsubishi Electronics Co., Ltd. From 1994 to 2001, he was an Associate Professor in the Department of Computer Science and Communication Engineering, Kyushu University. From 2002, he has been a Professor in the Department of Computer Science and Communication Engineering, Kyushu University. From 2004, he has been also the general manager of information security laboratory of Institute of Systems, Information Technologies (ISIT).