Guest Editorial: Insider Threat Solutions - Moving from Concept to Reality

Jason R.C. Nurse[1] and Elisa Bertino[2]
[1]*Department of Computer Science, University of Oxford, UK*
jason.nurse@cs.ox.ac.uk
[2]*Department of Computer Science, Purdue University, USA*
bertino@purdue.edu

As society has embraced technology and systems to promote services, trade and ubiquitous communication, it has also inadvertently exposed itself to a plethora of security risks. One of the most significant of these risks is that of insider threat, where privileged insiders (be they employees or trusted third-parties) within an enterprise, intentionally or inadvertently cause harm their organisations [1]. While the topic of insider threat has been examined and researched for decades [2, 3], the problem still persists, and some would even argue that it is becoming worse [4]. Could this be the result of a disconnect between approaches and solutions being researched and those that are (or can be) actually implemented?

In this special issue titled, "Insider Threat Solutions: Moving from Concept to Reality", we focus on novel systems to tackle insider threat which also provide a clear path for how they can be deployed in organisations. Our aim is to help bridge the gap between research concepts and the reality that businesses face day-to-day as they seek to prevent, detect and respond to insider attacks. This special issue includes four papers that outline novel and practical approaches to addressing the insider threat challenge. They focus on various solution perspectives, from multi-policy access control systems to formal approaches for network security policy validation. These best papers are selected from articles submitted to, and presented in, the 8th International Workshop on Managing Insider Security Threats (MIST) [3] which was held in Conjunction with ACM SIGSAC Conference on Computer and Communications Security 2016 at the Hofburg Palace, Vienna, Austria, on October 24-28, 2016.

The first article, "Linear Time Algorithms to Restrict Insider Access using Multi-Policy Access Control Systems" [5], discusses an implementation of the Next Generation Access Control (NGAC) standard from the American National Standards Institute (ANSI). The main contributions of their research are: (a) being the first ever study to demonstrate the scalability of the NGAC multi-policy access control system; (b) the creation of a novel visualization approach to enable review of user object access on NGAC systems; and (c) the definition of linear time algorithms for performing access control decisions and review of user access rights.

In the second article, "Formalising Policies for Insider-threat Detection: A Tripwire Grammar" [6], the authors describe their recent research into how they intend to enhance anomaly detection systems by capturing actions of concern. They view concerning actions as something that they can design and implement *tripwires* within a system to detect. The aim, therefore, being to orchestrate these tripwires in conjunction with an anomaly detection system to better detect insider attacks. Overall, their work seeks to provide a single framework for unambiguously capturing tripwires, alongside a library of existing ones in use. Therefore, tripwires may be used to map experiences regardless of the heterogeneity of the security tools and practices deployed.

The third article, "Insider Threats and Auctions: Formalization, Mechanized Proof, and Code Generation" [7], applies machine assisted formal methods to explore insider threats for auctions. The contributions of the paper are: (a) a formalization of the cocaine protocol using Isabelle's inductive approach including the formalization and proof of the absence of the sweetheart deal and the impossibility of excluding collusion of insiders; (b) the extension of the inductive approach to auctions by expressing arbitrary numbers of rounds, broadcast messages, an anonymity layer, and by merging with the Isabelle insider framework; (c) a practical solution by defining a constructive test predicate that implements the protocol, applying the code generation mechanism of Isabelle to generate Scala code from that, and proving correctness of the test predicate with respect to the specification within Isabelle.

The final article, "A formal approach for network security policy validation" [8], proposes a novel approach for validating network policy enforcement, by checking the network status and configuration, and detection of the possible causes in case of misconfiguration or software attacks. The authors' contribution exploits formal methods to model and validate the packet processing and forwarding behaviour of security controls, and to validate the trustworthiness of the controls by using remote attestation. Finally, they propose a prototype implementation of their approach to validate different scenarios.

We would like to express our sincere appreciation of the contributions made by all the authors and our deep gratitude to all reviewers who have carefully analysed the assigned papers and contributed to improve their quality. Our special thanks go to Prof. Ilsun You, Editor in Chief of the JoWUA for his invaluable support throughout this special issue preparation.

Jason R.C. Nurse and Elisa Bertino
Guest Editors
March 2017

References

[1] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *Proc. of the 2014 IEEE Security and Privacy Workshops (SPW'14), San Jose, California, USA*. IEEE, May 2014, pp. 214–228.

[2] L. F. Fischer, "Characterizing information systems insider offenders," in *Proc. of the the 45th Annual Conference of the International Military Testing Association, Pensacola, Florida, USA*. IMTA, November 2003, pp. 289–296.

[3] I. You and E. Bertino, "MIST 2016: 8th International Workshop on Managing Insider Security Threats," in *Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16), Vienna, Austria*. ACM, October 2016, pp. 1890–1891.

[4] Ericka Chickowski, "8 Surprising Statistics About Insider Threats," August 2016, http://www.darkreading.com/vulnerabilities---threats/8-surprising-statistics-about-insider-threats/d/d-id/1326653 [Online; Accessed on March 1, 2017].

[5] P. Mell, J. Shook, R. Harang, and S. Gavrila, "Linear Time Algorithms to Restrict Insider Access using Multi-Policy Access Control Systems," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 8, no. 1, pp. 4–25, March 2017.

[6] I. Agrafiotis, A. Erola, M. Goldsmith, and S. Creese, "Formalising policies for insider-threat detection: A tripwire grammar," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 8, no. 1, pp. 26–43, March 2017.

[7] F. Kammüller, M. Kerber, and C. W. Probst, "Insider Threats and Auctions: Formalization, Mechanized Proof, and Code Generation," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 8, no. 1, pp. 44–78, March 2017.

[8] F. Valenza, T. Su, S. Spinoso, A. Lioy, R. Sisto, and M. Vallini, "A formal approach for network security policy validation," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 8, no. 1, pp. 79–100, March 2017.

Author Biography

Jason R.C. Nurse is Senior Researcher (Oxford Research Fellow) in the Department of Computer Science at the University of Oxford. He received his B.Sc. in Computer Science and Accounting (UWI, Barbados – 2001), M.Sc. in Internet Computing (Hull, UK – 2006), and Ph.D. degree in Computer Science specialising in Web Services Security and e-Business (Warwick, UK – 2010). He has worked within industry and academia throughout his career. This has included various IT roles within industry, and academic posts such as Research Fellow at Warwick University, and more recently, Fellow at Oxford. Jason has published several articles at both journal and conference levels and also sits on the various cybersecurity programme committees. His research interests include insider threat, corporate information security, cybersecurity capacity maturity models, the risks to identity security and privacy in cyberspace, information trust, human factors of security, and services security. In 2014, Nurse was selected as a Rising Star in research as a part of the UK's EPSRC RISE awards campaign.

Elisa Bertino 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