Guest Editorial: Special Issue on Advances in Insider Threat Detection

Ioannis Agrafiotis[1] and Gökhan Kul[2]
[1]Cybersecurity Analytics Group, Department of Computer Science, University of Oxford,
Wolfson Building, Parks Road, Oxford, OX1 3QD, UK
[2]University of Massachusetts Dartmouth, Dartmouth, MA 02747 United States

The Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) has been a hub of international research, providing opportunities to a range of stakeholders, from researchers and professionals to industrial practitioners, to discuss and push the boundaries of knowledge on a variety of security-related IT topics. Special issues of JoWUA provide an excellent platform to communicate state-of-the-art research on highly debatable topics. Over the last ten years, the topic of insider threat has attracted significant interest in the research community, therefore this special issue is dedicated to theoretical and practical works that provide novel solutions to insider threat detection and contribute to the mitigation of insider threats.

Insider threats have increased in size and impact over the last few years, featuring amongst the most highly significant risks for organisations, governments and institutions. Yet, the majority of the organisations are ill-equipped to detect insider attacks and mitigate the harms of malicious behaviour from their employees. The authorised access to critical systems that insiders hold for their daily legitimate tasks, alongside the intricate knowledge of the security practices of organisations that they possess, render the detection and mitigation of such attacks a daunting task. Research on the insider threat problem is two-fold; theoretical understanding of the motivations and behavioural aspects of insider threats and designing of detection systems which usually utilise machine learning algorithms and rely mainly on network data. Embedding information from theoretical models, regarding the behavioural aspects of insiders, to detection systems, can enhance their accuracy. Such information, however, is difficult to capture and challenging to use for training machine learning architectures.

In this special issue, accepted papers endeavoured to address the problem of incorporating behavioural aspects to machine learning architectures. The authors of *"Use of Expert Judgements to Inform Bayesian Models of Insider Threat Risk"* suggest that the lack of sociotechnical data on indicators related to insider threats can be surpassed by consulting experts who can expand knowledge bases to be used in reasoning tasks. The work in *"A Bayesian approach to insider threat detection"* demonstrates that Bayesian models are accurate predictors of insider threat behaviour. Behavioural and psychological profile of an employee is often disregarded in the literature. The authors explain how behavioural aspects of insiders can be rendered into features and be incorporated in specially crafted Bayesian networks.

The second strand of papers focused on enhancing the security controls which organisation implement to advance their security posture. Authors of *"Impact Analysis of Training Data Characteristics for Phishing Email Classification"* focus on improving the machine learning model by tailoring the training data for systems that detect phishing emails, a mechanism often used to initiate insider attacks. They provide insightful information on how to set up the balance in training sets between phishing and legitimate emails for systems utilising machine learning techniques, both for structural and text mining approaches.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications(JoWUA), 12(2):1-2, June 2021
DOI:*10.22667/JOWUA.2021.06.30.001*

Finally, authors of *"Securing Opportunistic Networks: An Encounter-based Trust-driven Barter Mechanism"*, propose a protocol that utilises cryptographic techniques to enhance resilience against collusion network attacks. Such attacks may be exploited by insiders, especially in cases of sabotage.

We would like to extend our gratitude to all the authors that submitted their novel work to this special issue and have extended the boundary of knowledge on insider threat detection. We are thankful to the reviewers for their valuable input, which helped to enhance the final version of the published papers. Last, but not least, we would like to thank Prof. Ilsun You, Editor in Chief of JoWUA, for providing the opportunity to discuss the topic of insider threat in JoWUA and for his invaluable support in preparing this special issue.

Ioannis Agrafiotis & Gökhan Kul
Guest Editors
June 2021

Author Biography

Ioannis Agrafiotis is an Officer in Capacity Building at the European Union Agency for Cybersecurity (ENISA) working in the area of securing AI and responsible for organising Capture-the-Flag challenges. Ioannis has an affiliation with the University of Oxford, where he acts as a Senior Researcher in cybersecurity with the Department of Computer Science and as a James Martin Fellow at the Global Cyber Security Capacity Centre. In his academic role, he has participated in various projects conducting research in capacity building, risk analysis and resilience in the cyber domain, cyber insurance, and anomaly detection for internal and external threats. Ioannis completed his doctoral studies in Engineering at the University of Warwick (2012, EPSRC-funded). He also holds an MSc in Analysis, Design and Management of Information Systems from the London School of Economics and Political Science (2008) and a BSc in Applied Informatics from the University of Macedonia in Greece (2006).

Gökhan Kul is an assistant professor at the Department of Computer and Information Science and the associate director of the Cybersecurity Center of the University of Massachusetts Dartmouth. He received his B.S. and M.S. degrees in Computer Engineering from TOBB University of Economics and Technology in 2010 and Middle East Technical University in 2012 in Turkey, respectively. He received his Ph.D. degree in 2018 at the University at Buffalo, SUNY. His research interests include cybersecurity, database systems, data engineering and security, and software engineering. He is a member of IEEE and ACM.