JISSec
Journal of Information System Security

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 13, Issue 1

www.jissec.org

EDITORIAL

This Issue reproduces three papers that were presented at the 2016 Security Conferences of Lisbon and Las Vegas. The underlying theme is insider threat detection, which is receiving increasing attention from academia and practitioners.

The first paper, entitled "Ethical Issues of User Behavioral Analysis through Machine Learning", is by Georg Thomas from Charles Sturt University, Australia, and, Patrick Duessel and Michael Meier from the University of Bonn, Germany. It examines the asset-centric and content-based methodologies of insider threat detection, and focuses especially on user-centric content-based behavioural anomaly detection that utilizes four distinct ethical dimensions.

The second paper, "Towards a Robust Fingerprint Authentication System Protocol", by Kishor Krishnan Nair, and Johannes van der Merwe from the Council for Scientific and Information Research (CSIR), South Africa, and Albert Helberg, from North-West University (NWU), Potchefstroom Campus, also in South Africa, describes biometric authentication systems. More specifically it examines Fingerprint Authentication Systems (FASs), analysing their susceptibility to the inherent security vulnerabilities associated with biometric modalities in general, and conceptualises an FAS protocol that can address the major FAS protocol security vulnerabilities.

The third paper is entitled "Evaluation of Vulnerabilities in Computer Systems Users", and is by Isabel Candal-Vicente and Segundo Castro-Gonzáles from Universidad del Este, Puerto Rico, and also Janely García-Cortés from Xapiens International, Puerto Rico. It recounts the findings of a study that categorises levels of user knowledge with regards to the risk of internet connectivity, categorises protection strategies that are used to control the risk of information security, and also analyses the relationships between the different levels of knowledge regarding connection risk versus protection strategies for computer security.

All three papers discuss how computers and systems are becoming more efficient in addressing the risks of data theft and internet connectivity vulnerability through user authentication, and they present highly up-to-date and innovative developments.

I am sure that you will enjoy reading this Issue.

Gurpreet Dhillon, Editor-in-Chief