JISSec
Journal of Information Systems Security

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's 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.

Editor-in-Chief
Gurpreet Dhillon
University of North Texas, USA

Managing Editor
Filipe de Sá-Soares
University of Minho, Portugal

Publishing Manager
Mark Crathorne
ISEG, Universidade de Lisboa, Portugal

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 20, Issue 2

www.jissec.org

EDITORIAL

This Issue commences with an Editorial Note that explores how scientific research goes beyond mere replication and includes a broader concept known as robustness. It highlights the significance of replication research within the field of cybersecurity, especially as the Journal of Information Systems Security actively encourages the publication of replication studies, which it considers to be important. The three selected research papers concentrate on the human aspect of cyber-security, both from the angle of overcoming laissez-faire and biased attitudes by security professionals, as well as the need for intelligent mechanisms to identify fraudsters.

The first paper, entitled 'Trust me, I am Accountable: Factors Influencing the Perception of Benefits of Blockchain Technology', is by Mohamed Abdelhamid, Ruchi Isaac and Katja Crusius, all from the USA. Although blockchain holds great potential for a variety of industries and despite great advancements in its security, awareness of blockchain technology remains limited, hindering its widespread adoption. This paper provides insights from various studies that address the risks related to blockchain in cybersecurity, develops a seven-layer structure to combat those risks, and proposes an invoice financing platform that establishes data confidentiality.

In the second paper, 'The Rationality of Automation Bias in Security Operation Centers', the authors, Jack Tilbury and Stephen Flowerday, from the USA, discuss the challenge of the volume of alerts that need to be assessed by Security Operation Centers (SOCs) and the tendency for human operators to become over-reliant on automated systems, despite the presence of contradictory information. In their study, they develop four critical success factors (CSFs) for the adoption of automation within SOCs, in an attempt to mitigate automation bias and help SOC analysts to be more cognitively aware and respect contradictory information that can flag up cyber-attacks.

The third paper is entitled 'Detecting Collusive Seller Shill Bidding using Social Network Analysis', and is by Nazia Majadi and Jarrod Trevathan, from Bangladesh and Australia, respectively. The authors study the detection of collusive shill bidding that amounts to fraud. They propose a real-time algorithm utilising social network metrics to identify fraudulent seller accounts involved with multiple seller collusive shill bidding practices. They prove that their algorithm is capable of identifying potential shill bidding parties in real-time and can thus combat fraud.

I trust that you will find this Issue informative and interesting reading.

Gurpreet Dhillon, Editor-in-Chief