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.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 21, Issue 2

www.jissec.org

EDITORIAL

Arising from the vibrant discussions held at the 24th Annual Security Conference, I keep returning to the definition of Information Systems (IS) security, its functional role and existential concerns for organizations. Although this is not a new concern, the context is evolving rapidly and the Editorial Note in this issue is a call for agile adaptation to new circumstances.

In their paper, 'An Executive Guide to Secure-by-Design AI', Nelson Novaes Neto and Keri Pearlson, from the USA, argue that the integration of the trinity – IT architecture, security frameworks, and AI standards – is essential because IT architecture models do not address AI security. CIOs, CTOs and CSOs need a single, integrated approach for secure by design AI systems. The authors propose an executive framework for building secure AI systems and provide a case study of C6 Bank.

'An Identity and Interaction-based Approach to Network Forensic Analysis' is a paper by Nathan Clarke, Gaseb Alotibi, Dany Joy, Fudong Li, Steven Furnell, Ali Alshumrani and Hussam Mohammed, from the UK, Saudi Arabia and Iraq, which raises concerns about current forensic tools which are falling short of the needs of investigators for dealing with large volumes of encrypted information. A novel approach to N-FATs (Network Forensic Analysis Tools) is presented which may allow the analysis of encrypted network traffic more effectively through the modelling of network traffic that enables better visualisation of interactions.

Nadia Samara and Dionysios Demetis, from Jordan and the UK, use the example of Jordan's attempt to address cybersecurity concerns in the area of e-government in their paper, 'Managing the Cybersecurity of e-Government Programmes: The Case of Jordan'. They examine how information security is managed and approached within e-government programmes and discuss an interpretative case study at the Ministry of ICT in Jordan. By building on the Technical/Formal/Informal (TFI) framework, the study deconstructs information security at these three levels and builds up a customised TFI-informed framework for e-government security.

Please enjoy this second issue of 2025.

Gurpreet Dhillon, Editor-in-Chief