
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.

Editor-in-Chief
Gurpreet Dhillon
The University of North Carolina,
Greensboro, USA

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

Publishing Manager
Mark Crathorne
ISEG, Universidade de Lisboa, Portugal

ISSN: 1551-0123
Volume 16, Issue 2

www.jissec.org

EDITORIAL

The three papers of this Issue all focus on the key area of cyber security. They share the latest developments regarding digital identity, describing how blockchain can be used to create an independent self-sovereign digital identity, and show how a theoretical predator prey/obligate mutualism model can be used in systems security. In addition, the mitigation of cyber risk in cross-border financial systems is discussed.

The first paper, entitled “Cyber Securing Cross-border Financial Services: The Need for a Financial Cybersecurity Action Task Force”, is written by, Keman Huang and Stuart Madnick from the USA. It develops a taxonomy to understand the effect of trade policies for cyber-securing cross-border financial services. The analysis reveals that a Financial Cybersecurity Action Task Force involving both the public and private sectors is needed to create and promote cyber norms to balance innovation and systematic cyber risk in cross-border financial systems to face the new cyber threats.

In the second paper, “Security Dependent Parameters in a Predator Prey/Obligate Mutualism Infosec Model”, the author Norman Pendegraft, from the USA, presents a theoretical predator prey/obligate mutualism model of information security which is extended to allow for some of the parameters to be non-constant and dependent on security. A numerical example demonstrates the evolution of the critical point as security increases and the impact of security changes in the 3D case is illustrated with a graphical estimation of the basins of attraction of the critical points.

The third paper is entitled “Online Privacy - Self-Sovereign Identity”, and is by Kristine Sunda, also from the USA. This paper explores the role of self-sovereign identity in online privacy. It shows how the latest generation of identity management introduces self-sovereign identity, using blockchain to create an independent digital identity, strengthening the traditional password protection and biometric/dual-factor authentication. It demonstrates how self-sovereign identity uses decentralized identifiers (DIDs) to enable verifiable, decentralized digital identity and ties users to identities and certified credentials using blockchain.

I hope that you enjoy reading this Issue.

Gurpreet Dhillon, Editor-in-Chief