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.

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

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

ISSN: 1551-0123
Volume 13, Issue 3

www.jissec.org

EDITORIAL

This Issue reproduces three papers that research both internal and external threats to IT systems, examining intrusions from insiders and external cyber-attacks.

The first paper, entitled "Intrusion Detection System based on Support Vector Machines and the Two-Phase Bat Algorithm", is by Eseoghene Daniel Erigha, Femi Emmanuel Ayo, Oluwatobi Olakunle Dada, and Olusegun Folorunso from Nigeria. It analyses Intrusion Detection System (IDS) and affirms that an IDS can provide better performance if parameter optimization for classifier is embedded in the feature selection process, proposing a hybrid wrapper feature selection approach that combines Binary Bat algorithm with Lévy flights, together with Bat algorithm and Support Vector machines. Experimental results confirm this affirmation.

In the second paper, "A Risk-Based Layered Defence for Managing the Trusted Insider Threat", the authors Leung Chim, Daniel Bilusich, Steven Lord, and Rick Nunes-Vaz, who are from Australia, adapt a successful framework from physical security to support the design of insider threat security layers in a way that supports the evaluation of residual risks. This is a reaction to the fact that a holistic framework for designing and integrating layers of defence is missing, although it is known that the management of insider threats to information security requires the use of multiple layers of countermeasures.

The third paper is entitled "An Overview of Cryptographic Backdoors", and is by Chuck Easttom from the USA. It explains how Cryptographic Backdoors mechanisms can be created within a variety of cryptographic algorithms, including pseudo-random number generators. This has implications for providing perpetrators with a means to break the resulting cipher in significantly less time than would normally be required.

The three papers discuss the risk of intrusion, both from insiders and external threats and provide a useful contribution to professionals and academics alike.

I am sure that you will enjoy reading this Issue.

Gurpreet Dhillon, Editor-in-Chief