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 11, Issue 1

www.jissec.org

EDITORIAL

This first issue for 2015 publishes three papers, all of which are related to the increasingly-relevant topic of cybersecurity. The task of matching system assets and services with their respective security policies is increasingly complex and information security features must be updated on a regular basis. Network intrusion detection schemes are an important priority for Information Systems Security Managers. The frequency and scale of worm attacks on the Internet is ever increasing and worms in a p2p network are capable of spreading much faster than the Internet, due to the rich host connectivity and constant data exchange

The first paper, entitled "Towards structured implementation of network security policies", by Jordan Shropshire from the University of South Alabama, USA and Art Gowan from James Madison University, USA describes the need to change functional aspects of computer systems, as these have dynamic needs, and also the fact that information security features must be updated on a regular basis. The research develops a structured process for updating security controls, whilst minimizing human errors at the same time.

The second paper, entitled "Network payload anomaly detection using layered statistical dispersion", by Sun-il Kim1 and William Edmonds from the University of Alabama in Huntsville, USA and also Nnamdi Nwanze of the iDEA Hub, Nigeria, presents a network intrusion detection scheme based on detecting anomalies. The paper presents performance studies of both the training and detection stages for implementing such a system, and is innovative in that the authors' solution tolerates the use of training traffic that may not be completely free of anomalies or attacks. Future research in this area includes investigating a strategy to build a mesh of detection schemes in an attempt to simultaneously filter incoming data.

The third paper, entitled "Secure peer-to-peer (p2p) patch dissemination in a race against topological worms" by Narasimha Shashidhar from the Sam Houston State University, Huntsville and Lei Chen, from Georgia Southern University, Statesboro, USA, describe strategies to curb the spread of worms in p2p networks and offers countermeasures against this emerging cyber threat. In particular, the authors study the problem of disseminating security patches over a p2p network, while simultaneously containing the spread of topological worms in the network.

Happy reading!

Gurpreet Dhillon, Editor-in-Chief