

---

**Editorial**

---

This issue of the Journal of Information System Security presents three very interesting papers.

The first paper, "A Model for Predicting Hacker Behavior" is by Nicole Lang Beebe and Jan Guynes Clark of The University of Texas at San Antonio, USA. Observing that little research has been conducted in order to develop a predictive model to classify individuals as potential or actual hackers, the authors empirically developed a discriminant model to categorize an individual's likelihood of engaging in unauthorized access to information systems. The study explores the influence of factors such as demographics, ethical ideologies and professional status on attitudes and beliefs regarding the ethicality of hacking. Subsequently, the influence of such attitudes and beliefs on the willingness to engage in illegal hacking behavior is discussed. One of the main findings of the study was the emergence of personal moral philosophy as a significant predictor of an individual's attitude toward the ethicality of hacking.

In the second paper, "Security Metaphors Shaping the Emerging Practice of Secure Information Systems Development", Theodore Tryfonas of University of Glamorgan, Wales, revisits the roots of the emergent professional practice of developing secure information systems. The author argues that contemporary practice is shaped by an engineering perspective that has major implications in producing less secure systems. In order to tackle this issue, the author defends the assumption of a holistic perspective. According to this view, the actions of information security practitioners have to be defined by considering not only a security engineering standpoint, but also social, organizational and political concerns. In the paper, this argument is explored by applying the concept of metaphors to the organizational discourse on security.

The third paper, "Challenges in Managing Information Security in Academic Institutions: Case of MDI in India", is co-authored by Varadharajan Sridhar and D. K. Ahuja of Management Development Institute, India. Implementing and maintaining information security infrastructures are major activities in the field of information systems security. The researchers note that the cost of those activities can be very high, especially for small and medium size organizations as well as for non-profit organizations such as educational

institutions. With this idea in mind, the authors conducted a case study to analyze the issues in managing information security in the context of an educational institution. The paper shows the challenges and difficulties in managing information security in an open access academic community and describes the decisions and outputs reached during the stages of the security system development life cycle.

**Gurpreet Dhillon, PhD**  
**Editor-in-Chief**