Editorial

This issue of Journal of Information System Security has three very interesting papers. In the first paper John D'Arcy, Towson University, USA and Anat Hovav, Korea University, South Korea, discuss aspects of fit between security countermeasures and misuse behavior. In there paper, "Towards a Best Fit Between Organizational Security Countermeasures and Information Systems Misuse Behaviors", the authors examine how certain countermeasures are more or less effective depending on the type of IS misuse behavior. The authors assess the deterrent effectiveness of security policies, security education, training, and awareness programs, and computer monitoring on a range of IS misuse behaviors that vary in severity. The main contribution of the paper is in differentiating between control measures for particular misuse behaviors. For instance the authors found computer monitoring to be effective in deterring severe forms of IS misuse. Security policies and other related awareness programs were found to be useful in maintaining a generally good secure environment.

The second paper, "A Framework to Facilitate Forensic Investigation of Falsely Advertised BGP Routes" is by Indrajit Ray, Eunjong Kim and Daniel Massey, Colorado State University, USA. The authors identify a significant issue with the Internet's global routing protocol, which lacks basic authentication and monitoring functionalities. As a result, it is possible to maliciously deny service or misdirected traffic. The authors argue that an ability to identify false paths through efficient validation, proper recording and forensic analysis of routing data, will help in the prosecution of the miscreant and will act as a strong deterrent. In this respect path verification schemes introduced by the authors help in keeping track of malicious attempts.

The third paper, "Do anti-spam measures effectively cover the e-mail communication network? A formal approach" is by Guido Schryen, Aachen University, Germany. The author presents a model for Internet e-mail infrastructure that can offer a better service. Based on automata theory, the paper proposes a basis for a directed graph and a deterministic finite automation for spam delivery. This paper presents some rather innovative ideas, which may help in curbing spam.

**Gurpreet Dhillon
Editor-in-Chief**