JISSec 5(3) 2009

Journal of Information System Security

www.jissec.org

Editorial

Many of you would have noticed a revamped JISSec website and the related systems. The editorial team has been busy trying to streamline the processes involved in publishing quality information security research. Support from the community and their understanding has been overwhelming, particularly as we have transitioned into a new submission system. In the first four years of the journals publication, we were only able to produce three issues per year. This was largely because we did not want to compromise on the quality of the research published in JISSec. In 2009 however we will be publishing four issues. As is evident from the research papers in this issue, they are all cutting edge and aspire to define the information security field.

Personally two information security issues have always troubled me. First, majority of information security problems occur because someone in the organization subverts the controls to gain access. Second, information security cannot be implemented if we do not have a good understanding of the business processes and the related vulnerabilities. In spite of decades of research in the socio-organizational aspects of information security, we have as yet to come up with a well-defined body of knowledge in this area. While we hope that behavioral compliance will help in bringing uniformity to the organizations, it necessarily does not help in curtailing un-ethical behaviors. As the ancient adage goes – *it only takes one rotten apple to spoil the others*. Education and training could help. However, the content of such education and training programs matters more than just having a training program. And perhaps we need to understand the intricacies of the business processes first in order to fine tune and education and a training agenda. Whatever be the mix of issues that are to be addressed, it is prudent nevertheless to be proactive in developing a sound understanding.

The three papers in this issue address an aspect of information security, which is important and further research in the respective areas will be defining at best. The first paper in this issue is “The effect of security education training and awareness programs and awareness programs and individual characteristics on end user tool usage”, which has been co-authored

by Robert E Crossler of University of Texas Pan American, USA and France Bélanger of Virginia Polytechnic Institute and State University, USA. The research presented in this paper is very timely and focuses upon issues of employee behavior. Extant research has noted that employee behavior has an important bearing on prevention of security breaches. The authors investigate the effect of some individual characteristics and a security education, training, and awareness program on security tool usage by individuals. Using an experimental design the authors report that an employee's level of computer self-efficacy and gender, significantly impact his or her use of security tools. Hence the authors argue that users need to be educated in the use of security tools in order to improve usage and therefore the overall security of an enterprise.

The second paper in this issue is "Consideration of risks and internal controls in business process modeling", which has been co-authored by Rosalyn Mansour and Uday S Murthy of University of South Florida, USA. The authors argue that lack of internal business process controls result in susceptibility of systems, processes and data to material errors, irregularities and fraud. In the paper, the authors propose a methodology for identifying risks and internal controls in business processes. In illustrating the methodology the authors model the revenue cycle business process. They identify risks, corresponding objectives and the necessary internal control procedures. The research presented in the paper could form a useful basis for defining an internal control ontology.

The third paper in this issue is "Threat modeling the enterprise", which has been co-authored by Jeffrey A Ingalsbe of Ford Motor Company, USA, Dan Shoemaker of University of Detroit Mercy, USA, Nancy R Mead of Carnegie Mellon University, USA and Antonio Drommi of University of Detroit Mercy, USA.

The authors argue that since current modeling methodologies are biased towards systems currently being developed, organizations with a large number of legacy systems are left with few options. The authors describe a means to represent an IT portfolio from a security perspective. UML deployment diagrams are used, which forms the basis for defining a process.

I hope you enjoy this issue. Keep a look out for further enhancements to the journal.

Gurpreet Dhillon,
Editor-in-Chief