JISSec 1(2) 2005

The Information Institute

Journal of Information System Security

www.jissec.org

Editorial

Meeting the Information System Security Challenge

The first issue of Journal of Information System Security (JISSec) had established the nature and scope of the papers that would be acceptable to the JISSec audience. Clearly there is a need to address enterprise security issues from both the technical as well as the social and organizational perspectives. Technical solutions to security cannot be sustained without an adequate understanding of the social world. At the same time advances in technical solutions are critical for addressing the information assurance needs. The interplay between the technical and the social is illustrated in the three papers in this issue of JISSec.

The first paper, *Methodology to Assess the Impact of Investments in Security Tools and Products,* is by Sriraman Ramachandran and Greg White. The authors argue that it is hard to measure the intangible benefits from security tools and products. The lack of metrics that take into account the intangible benefits forbid a comprehensive assessment of value of investment security tools and products. Using research undertaken in the information technology payoff literature, the authors develop a methodology for assessing both the tangible and intangible aspects of security investments.

The second paper, *SoapSy - Unifying Security Data from Various Heterogeneous Distributed Systems into a Single Database Architecture,* is authored by Nikolaos Avourdiadis, Andrew Blyth and Paula Thomas. This is a largely technical paper, which introduces SoapSy as a means to secure access mechanism for heterogeneous distributed sources. The authors also present a database architecture that can be used with SoapSy for unifying data from heterogeneous distributed systems. A description of how the architecture can evolve and how additional heterogeneous sensors can be used is also presented.

The third paper is a computer hack case study written by Sharon Perez. The case is an "eye opener" for all involved as to how quickly, easily and stealthily the systems could be taken over. The tools utilized were all readily

available on the internet. The fact that the password policy was inadequate was already known, though the ramifications of such a decision were not fully explored. The case brings together issues related to development challenges in identifying, procuring and implementing security tools and products and the challenges associated with calculating the cost of breaches and perhaps the benefits of implementing security tools.

Gurpreet Dhillon
James Backhouse
Vijay Masurkar