Editorial

Craig Valli and Christopher Bolan

School of Computer and Information Science,
Edith Cowan University,
2 Bradford Street, Mount Lawley, WA 6050, Australia
Fax: +61 8 6304 5144   E-mail: c.valli@ecu.edu.au
E-mail: c.bolan@ecu.edu.au

Biographical notes: Craig Valli is a Senior Lecturer in Computer and Network Security at Edith Cowan University and leader of the SCISSEC Research Cluster. His areas of active research include honeypots, digital forensics, network security and compute clustering. He consults to industry on computer and network security issues. He is co-editor of the *Journal of Information Warfare*, Chair of *Australian Digital Forensics Conference*, and Co-Chair of the *Australian Information Security Management Conference*.

Christopher Bolan lectures in Computer Security in the School of Computer and Information Science at Edith Cowan University. He is currently completing a PhD in Computer Science in the area of RFID Security. His research interests lie mainly in RFID, however previous projects have included medical and privacy related subjects.

This special issue of IJICS was created using selected papers from both the *3rd Australian Information Security Management and the 3rd Australian Computer, Network and Information Forensics Conferences*. These conferences were hosted by the School of Computer and Information Science, SCISSEC Security Research Group at Edith Cowan University in Perth, Western Australia over the 29–30 of September 2005.

The conferences were very successful, garnering international paper submissions and delegates. Overall, 33 papers were accepted for the conferences from a field of 46 submissions. From the accepted papers the conference organising committee selected the six best papers for this issue of the journal. The selected papers were subjected to a further round of blind peer reviews before acceptance.

The first paper from Hutchinson examines an approach to developing an Information Security course based on information rather than solely on the security aspects of information technology to create a more human centric approach. Next, Pye and Warren discuss the dynamic nature of threats and vulnerabilities within the e-business environment that may impede online functionality, compromise organisational or customer information, contravene security implementations and thereby undermine online customer confidence. The third paper, from Bolan investigates some low-cost proposals for securing RFID tags from potential misuse through authentication and encryption. The fourth paper from Jansen et al. describes two novel types of smart card with unconventional form factors, designed to take advantage of common interfaces built into many current handheld devices.

Next, Williams discusses the lack of threat realisation in medical based environments and provides a process for how security may be improved by those who are responsible for it. In the final paper Valli explores issues surrounding the deployment and design of honeypot technologies as an internal countermeasure to insider malfeasance.

In closing, we would like to thank the Editor in chief of IJICS, Professor Eldon Y. Li, all the authors that submitted to this special issue, and the members of the organising committee of both conferences.