

# **Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators**

Vlasti Broucek, Paul Turner

*School of Information Systems, University of Tasmania, GPO Box 252-87 Hobart, Tasmania, Australia, E-mail: Vlasti.Broucek@utas.edu.au, Paul.Turner@utas.edu.au*

## **Extended Abstract**

The traditional divide between technical and legal areas of expertise is increasingly problematic in the age of malware, hactivism and cyber-warfare. Technical advances in the ability of systems to detect intrusions, denial of services attacks and also to enhance network monitoring and maintenance are well documented and subject to constant research and development. These advances provide systems administrators with tools to treat the symptoms of such illegal and/or inappropriate behaviours. However, these technical responses do little to treat the causes of these or future problematic behaviours. Significantly, these technical solutions are not currently designed to collect forensic data making evidence acquisition difficult. Additionally systems administrators are often unfamiliar with the processes for evidence collection, collation and presentation suitable for the legal sphere. At the same time, legal regimes globally are struggling to address the challenges posed by illegal and inappropriate behaviours conducted in cyberspace. These challenges include both conceptual problems of definition and practical problems of legal jurisdiction (Broucek & Turner, 2002). Legal professionals are suffering from a limited understanding of technical advances and continue to lack confidence in the ability of technical specialists to produce evidence that will be admissible in a court of law. As recent judgements will be shown to illustrate there is a critical need to bridge this divide.

In this context, this paper presents a discussion of the development of forensic computing as an academic discipline (Broucek & Turner, 2001a, 2001b) and highlights the importance of creating forensic awareness amongst the network/system administrators, computer security community and legal professionals.

The paper is divided into two parts. Part one discusses the significance of the relationship between computer security and forensic computing and how this has affected the approaches of systems administrators to cyber-attacks. This part defines the relationship between the two areas, explores their commonalities and identifies the key fundamental differences between them. Part two explores the issues surrounding evidence acquisition and the suitability of Intrusion Detection Systems (IDS) for the requirements of legal admissibility. This part reveals strong disagreement amongst technical and legal experts over the suitability of IDS as a tool for collecting, collating and presenting forensic evidence. For some authors IDS are unsuitable as a forensic tool (Sommer, 1998), for others they suggest some suitability (Stephenson, 2000) while yet authors leave the question unaddressed (Yuill, Wu, Gong, & Huang, 1999). The paper concludes by identifying key principles for systems administrators to follow in considering data gathering for legal proceedings and raises several key questions for future forensic research.

## References

- Broucek, V., & Turner, P. (2001a, 11 July 2001). *Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline*. Paper presented at the 5th Australian Security Research Symposium, Perth, Australia.
- Broucek, V., & Turner, P. (2001b). Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare. *Journal of Information Warfare*, 1(2), 95-108.
- Broucek, V., & Turner, P. (2002, 8-11 June 2002). *Risks and Solutions to problems arising from illegal or Inappropriate On-line Behaviours: Two Core Debates within Forensic Computing*. Paper presented at the EICAR2002, Berlin, Germany.
- Sommer, P. (1998, 14-16 September 1998). *Intrusion Detection Systems as Evidence*. Paper presented at the Recent Advances in Intrusion Detection - RAID'98, Louvain-la-Neuve, Belgium.
- Stephenson, P. (2000, 2-4 October 2000). *The Application of Intrusion Detection Systems in a Forensic Environment*. Paper presented at the Recent Advances in Intrusion Detection - RAID 2000, Toulouse, France.
- Yuill, J., Wu, S. F., Gong, F., & Huang, M.-Y. (1999, 7-9 September 1999). *Intrusion Detection for an On-Going Attack*. Paper presented at the Recent Advances in Intrusion Detection - RAID'99, Purdue, IN, USA.

## About Authors

### **Vlasti Broucek, Researcher**

Vlasti has been working in computer industry since 1985 in various research and hands-on positions. Currently, he is a researcher at the School of Information Systems, University of Tasmania and a network administrator at the School of Psychology, University of Tasmania, Australia. His current research interest is in Forensic Computing. He has an extensive knowledge in system administration of various systems (Novell Netware, Unix flavours), computer security, mathematics and Expert Systems. He has MSc degree from the Czech Technical University in Prague and currently is pursuing PhD at the University of Tasmania.

Contact: School of Information Systems, GPO Box 252-87, Hobart TAS 7001, Australia;  
Phone: +61-3-62262346; Fax: +61-3-62262883; E-mail: [Vlasti.Broucek@utas.edu.au](mailto:Vlasti.Broucek@utas.edu.au)

### **Dr. Paul Turner, Senior Research fellow**

Prior to joining the School of Information Systems, Paul was a research fellow at CRID (Computer, Telecommunications and Law Research Institute) in Belgium where he worked on a variety of European Commission contracts in the field of electronic commerce, telecommunications and intellectual property rights. Paul has also worked as an independent information and telecommunications consultant in a number of countries in Europe and was for three years editor of the London-based monthly publication Telecommunications Regulation Review. Paul's strong research focus in the field of electronic commerce continues both in his work as senior research fellow at the University of Tasmania and in his concurrent position as research manager for the Tasmanian Electronic Commerce Centre (TECC). In Paul's work for the TECC he is responsible for coordinating research at basic, applied and strategic levels across a range of industry sectors with a focus on small to medium sized enterprises electronic business practices.

Contact: School of Information Systems, GPO Box 252-87, Hobart TAS 7001, Australia;  
Phone: +61-3-62262930; Fax: +61-3-62262913; E-mail: [Paul.Turner@utas.edu.au](mailto:Paul.Turner@utas.edu.au)