Editorial

Nasir Memon

Department of Computer Science,
Polytechnic University,
Brooklyn, NY 11201, USA
E-mail: memon@poly.edu

Rajni Goel

Department of Information Systems and Decision Sciences,
Howard University,
Washington DC, 20059, USA
E-mail: rgoel@howard.edu

Biographical notes: Nasir Memon is a Professor in the Computer Science Department at Polytechnic University, New York. He is the Director of the Information Systems and Internet Security (ISIS) lab at Polytechnic. His research interests include data compression, computer and network security, digital forensics, and multimedia data security.

Rajni Goel received her PhD in Information Technology from George Mason University in 2003. Her thesis topic focused on Information Security. She is currently an Assistant Professor in the Department of Information Systems and Decision Sciences at Howard University, Washington DC. Her current research interests include information assurance, digital forensics and enterprise security.

1 Introduction

Computer networks are an integral component of a nation's critical infrastructure. Accurate attribution of attacks and reconstructing attack actions is crucial to mitigating threats to this infrastructure. Digital forensics is the scientific study of the processes involved in acquiring, preserving, examining, analysing and presenting all forms of electronic evidence, and network forensics is a subfield of digital forensics where evidence is captured from the networks. The IFIP Working Group 11.9 on Digital Forensics is an active international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in the emerging field of digital forensics.

This special issue on Network Forensics presents a selection of four updated and enhanced edited papers presented at the Second Annual IFIP WG 11.9 International Conference on Digital Forensics, held in National Centre for Forensic Science, Orlando, Florida, USA on January 29–February 1, 2006. The authors investigate the major technical challenges facing network forensics analysis and provide requirements and mechanisms that enhance the network forensics arena, while addressing a range of themes.

Indrajit Ray and Nayot Poolsappasit, in their paper titled 'Using mobile ad hoc networks to acquire digital evidence from remote autonomous agents', present a framework for an autonomous digital evidence acquisition system when uploading evidence to a remote central server using a mobile ad hoc network. In Forensic Analysis of SCADA Systems and Networks, T. Kilpatrick, J. González, R. Chandia, M. Papa and S. Shenoi describe an architecture that supports the 'Forensic analysis of SCADA systems and networks'. This architecture is implemented in a prototype networked environment for the popular Modbus TCP protocol and the mechanisms monitor process behaviour and record process trends. A third paper, 'On the (un)reliability of eavesdropping', Eric Cronin, Micah Sherr, and Matt Blaze analyse the theme of interception and analysis of internet traffic from the eavesdropper's point of view, and investigate the reliability of current generation eavesdropping tools. Finally, J.S. Okolica, G.L. Peterson and R.F. Mills, in 'Using PLSI-U to detect insider threats by datamining e-mail', discuss an approach to assist investigators in identifying potential insider threats by extending the PLSI Hoffman (1999) clustering algorithm to include individuals and discerning employees interests from their daily emails. The depth of each topic and the analysis needed demonstrates the richness and vitality of the network forensics discipline.