Internet Vulnerabilities and Cyber-Threats

Eliot Rich  
Department of Information Technology Management  
School of Business  
University at Albany  
1400 Washington Avenue  
Albany, NY 12222  
e.rich@albany.edu

Jose J. Gonzalez  
Faculty of Engineering and Science  
Security and Quality in Organizations Research Cell  
Agder University College  
Groosvn. 36  
NO-4876 Grimstad, Norway  
Jose.J.Gonzalez@hia.no

The “Internet Vulnerabilities and Cyber Threats” mini-track addresses issues related to detecting, mitigating and preventing the threat of computer based attacks. The pervasiveness of computer networks in our economic system has increased our vulnerability. In response, organizations have increased the attention paid to computer-based threats to their information, systems, and processes. In addition, there has been a marked increase in government attention to information security as a critical component of our national and international infrastructures, as well as its integral role for financial reporting and regulation. These constituencies are combining technical, managerial, forensics, regulation, law enforcement, and social engineering to combat a difficult and growing problem.

The mini-track consists of two sessions. Session 1 looks at how organizations detect and react to compromising events. Guido Schryen (RWTH Aachen University, Germany) charts the possible modes of spamming by using a graph model of the Internet’s email infrastructure and discusses the effectiveness of anti-spam procedures in terms of their coverage. Slobodan Petrović (Gjøvik University College, Norway), Gonzalo Álvarez, Agustín Orfila, (both with the Institute of Applied Physics, C.S.I.C., Madrid, Spain), and Javier Carbó (Carlos III University of Madrid, Spain) provide a paper on a cluster-labeling strategy to characterize abnormal behavior in an IDS dealing with a DoS scenario. Finally, Neil C. Rowe (Cebrowski Institute, U.S. Naval Postgraduate School) evaluates several methods to assess the effectiveness of honeypots (attack-data collecting sites disguised as ordinary internet hosts).

Session 2 is about issues surrounding the interface of security and operations. Kent Marett (Washington State University, United States), David Biros (Oklahoma State University, United States) and Brent Langhals (United States Air Force) present a study of the effectiveness of various arousal procedures to enhance vigilance and error detection. David W. Johnson and Harold Koch (Utah Valley State College, United States) provide empirical evidence about a disturbing fact: home-based small business owners are highly aware of security threats but this awareness does not translate into action and willingness to pay for protection. Eliot Rich (University at Albany, United States) and Jose J. Gonzalez (Agder University College, Norway) close the session with a preliminary study of security risks and their impact on safety in an offshore gas and oil company that is moving from traditional offshore operation to e-operations conducted from an onshore center.

The mini-track is our attempt to bring together an international group of scholars looking at many different facets of the continuing problems of Internet vulnerabilities. The chairs want to express our appreciation to our colleagues who submitted papers, provided insightful reviews, and facilitated our work in this fascinating field. We hope you enjoy the sessions.