▼ Introduction to Cyber Threats, Emerging Risks, and Systemic Concerns Minitrack

Guido Schryen
Institute of Business Information Systems, RWTH Aachen University,
Templergraben 64/V
52062 Aachen
Germany
schryen@winfor.rwth-aachen.de

Jose J. Gonzalez
Faculty of Engineering and Science
Security and Quality in Organizations Research Cell
University of Agder
Service Box 509
NO-4898 Grimstad, Norway
Jose.J.Gonzalez@uia.no

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

The pervasiveness of computer networks in our economic system has increased our vulnerability to systems-based attacks. These attacks are addressed in this minitrack, which covers issues related to anticipating, detecting, mitigating and preventing them. In particular, the minitrack focuses on (1) cyber-threats and information security, which includes assaults on computer systems themselves as well as fraud or other actions taken through the use of computers, (2) emergent risks in operations, which comprise heretofore-underestimated risks from the introduction of technology and technology-based infrastructure, (3) compliance and prevention, (4) information sharing (public regulation or private, confidential information pooling of risks and disclosure might be an interesting option), and (5) modeling and theory building of security topics.

The minitrack consists of six papers with both applied and theoretical approaches. The first of our two sessions examines problems specific to detecting attacks and profiling criminals. *Tang, Ray and Lewis* describe a method and apparatus for security alert analysis that is based on two technologies: (i) event correlation and (ii) a truth maintenance system. *Wynne, Gorton, Almquist, Chatterton and Thurman* describe their experiences in creating a production application for cyber situational awareness based on a middleware platform they have developed. The application exploits the capabilities of several independently developed components and integrates them using SIFT (Scalable Information Fusion and Triage), a service-oriented architecture (SOA) designed for creating domain-independent, enterprise scale analytical applications. The session closes with a paper by *Kwan, Ray and Stephens*, who present an approach for collecting legally valid evidence from cyber crimes, so that appropriate actions can be taken against cyber criminals. This approach is based on honeynets.

The second session contains three papers that examine emergent threats from different theoretical lenses. *Conklin and Dietrich* apply systems science to learn about the interactions of complex systems with their environment and how this knowledge may be applied to designing security architectures. *Siponen and Willison* address software piracy and present a perspective advancing two criminological theories. More specifically, a novel theoretical model is presented, drawing on these theories entitled Techniques of Neutralization and Differential Association Theory. Finally, *Martinez-Moyano, Ackam, Samsa and Burke* present a generic model for information security implementation in organizations. Their model is part of an ongoing research stream related to critical infrastructure protection and insider threat and attack analysis.

The minitrack 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.