Editorial

Risk Analysis for Security Applications

Securing critical infrastructure and computer networks is one of the most important challenges of our modern, interconnected society. In real-world security domains it is necessary to predict, mitigate, and react to intentional threats from adversarial agents, often under significant uncertainty.

Decisions must be made quickly, by processing large amounts of information, and taking into account the goals and capabilities of the adversary.

We believe that meeting these challenges will require the development and integration of new methods in multi-agent systems, risk analysis, computational game theory, machine learning, and other related fields. Developing and applying the tools needed to analyze and manage complex security problems will be a high-impact area for decades to come.

Several recent examples of deployed security applications point to progress and potential in this area.

For example, a deployed software system called ARMOR applies game-theoretic reasoning to help police officers at the Los Angeles International Airport make critical decisions about how to schedule both vehicle checkpoints and canine patrols.

This system has been in active use at the airport since 2007, and has received numerous accolades from the police, the popular press, and the research community.

We believe that the success of this application is just the beginning, and that new research will allow exciting new applications to be built and deployed.

For example, there are potential applications in robotic patrolling, automated security cameras, border security screening policies, and intrusion detection tools for computer networks.

Despite recent progress, there is a need for more research to address fundamental challenges in real-world security domains to provide comprehensive risk analysis and management tools.

First, most real domains are extremely large with complex, interacting decisions.

New algorithms that exploit domain structure are needed to apply sophisticated reasoning such as decision-theoretic or game-theoretic analysis to these domains.

These difficulties are further magnified by the need to model and reason about uncertainty in the domain, and to account for the fact that human decision-makers may behave in ways that are not easily captured in mathematical models of perfect rationality.

In many domains, even building a reliable, validated model of the domain is a significant challenge, whether by elicitation of the model from domain experts or through the use of simulation tools or empirical evidence.

Finally, the problem of evaluating deployed security systems poses numerous challenges, including the lack of controlled studies and limited access to data.

We are pleased to bring out this special issue of the Informatica journal which comprises of four papers that were presented at the inaugural workshop on Quantitative Risk Analysis for Security Applications (QRASA). These papers touch on many of the themes outlined above, and each paper makes a significant contribution to this exciting, emerging area of research.

We hope that the reader will be inspired by these papers to explore and participate in this dynamic and growing field of study.

The first paper titled "A Framework for Evaluating Deployed Security Systems: Is There a Chink in your ARMOR?" by Matthew E. Taylor, Christopher Kiekintveld, Craig Western and Milind Tambe, addresses the challenges of evaluating deployed security systems, using the ARMOR system as a case study to raise many of the issues involved in evaluating security systems in general. In addition to discussing these issues, the paper lays out a framework for guiding the evaluation process, giving insights into the different types of analyses that are possible and the kinds of evaluations that could further improve knowledge of a given systems' utility.

The second paper titled "Application of Microsimulation to the Modeling of Epidemics and Terrorist Attacks" by Ian Piper, Daniel Keep, Tony Green and Ivy Zhang describes a simulation tool for agent-based simulation. The authors describe the benefits of this tool and evaluate the tool on a case study, modeling the spread of an infectious disease in a community, based on real historical incident. In addition to the relevance of this study for biological attacks, the authors describe some other possible uses for this tool in modeling terrorist attack scenarios.

The third paper titled "Strategic Modeling of Information Sharing Among Data Privacy Attackers" by Quang Duong, Kristen LeFevre and Michael P. Wellman propose a framework for modeling multiple attackers with heterogeneous background knowledge, supporting analysis of their strategic incentives for sharing information prior to attack. The framework posits a decentralized mechanism by which agents decide whether and how much information to share, and defines a normal-form game representing their strategic choice setting. This paper represents one of the first applications of game theory to study possible attacks against databases.

The fourth paper titled "Planning to Discover and Counteract Attacks" by Tatiana Kichkaylo, Tatyana Ryutov, Michael D. Orosz and Robert Neches develops a set of tools that can provide decision support for recognizing plans in an adversarial setting. The approach is demonstrated in a network security setting, showing how an attacker's plan can be decomposed into separate actions and how recognizing the overall intent of the plan requires complex analysis of these independent plan fragments. The tool described in this paper assists security experts with analyzing various possible attack scenarios.

The special editors would like to thank Professor Matjaz Gams (Managing editor of Informatica) for providing the opportunity to edit this special issue on Risk Analysis for Security Applications. Finally, we would like to thank the authors of the papers for their individual contributions and all of the referees for their helpful comments. Their efforts helped to ensure the high quality of the material presented here.

Christopher Kiekintveld
University of Southern California
Los Angeles, CA 90089
kiekintv@usc.edu

Janusz Marecki
Mathematical Sciences Department
IBM T.J. Watson Research Center
marecki@us.ibm.com

Praveen Paruchuri
Carnegie Mellon University
Pittsburgh, PA 15232
paruchur@gmail.com

Katia Sycara
Carnegie Mellon University
Pittsburgh, PA 15232
katia@cs.cmu.edu