The 2009 ICAPS conference is sponsored by

University of Macedonia, Greece

Institute of Cognitive Sciences and Technologies, National Research Council (ISTC-CNR), Italy

Information and Communication Technology Department, National Research Council (ICT-CNR), Italy

Planning and Scheduling Team, ISTC-CNR, Italy

National Science Foundation (NSF), USA

Artificial Intelligence Journal, Elsevier

International Joint Conference on Artificial Intelligence (IJCAI)

European Coordinating Committee for Artificial Intelligence (ECCAI), Europe

Willow Garage, USA

David E. Smith, USA

NICTA, Australia

European Science Foundation, COST Action, Europe

Marathon Data Systems, Greece

Hellenic Artificial Intelligence Society (EETN), Greece

Prefecture of Thessaloniki, Greece

Hellenic Ministry of Culture, Greece

Klidarithmos Publishing, Greece

Held in cooperation with the Association for the Advancement of Artificial Intelligence

ICAPS 2009

Proceedings of the First Workshop on Intelligent Security (SecArt '09)

Edited by
Mark Boddy and Stefan Edelkamp

Cover painting courtesy Yannis Stavrou.

Contents

Papers

Preface

This is the first in what we hope will build into a series of workshops exploring issues at the intersection of Computer Security and Artificial Intelligence. This is a fertile area for research, and has been attracting an increasing amount of interest in both communities. In addition to this workshop (organized primarily from the AI side), AISEC-2009, "The 2nd Workshop on Security and Artificial Intelligence" will be held this November in Chicago. As with AISEC-2008, this workshop is held in conjunction with the ACM Conference on Computer and Communications Security (CCS) and so is organized primarily from the Computer Security community.

This is a large and growing area, both for research and for applications. Our increasingly networked world continues to provide new opportunities for security breaches to have severe consequences at the personal level (identity theft, and resulting financial losses), for businesses (theft of intellectual property, or business plans, or costly responses to the theft of customer data), and for governments. Computing and the internet have become crucial parts of the infrastructure of almost every significant commercial or governmental enterprise. Turning off the computers or disconnecting from the network has become tantamount to turning off the power.

The use of techniques drawn from AI is increasingly relevant as the scale of the problem increases, in terms of the size and complexity of the networks being protected, in terms of the variety of applications and services provided using that infrastructure, and with the sophistication of the attacks being made. Filtering the faint signals of intrusion from a flood of data related to normal operations can be viewed as data-mining. Learning methods can be applied to generate classifiers for this process, or to detect the presence of new means of attack. As one of the papers in this workshop discusses, planning methods can be used to generate compact representations of possible attacks, which can then be used to deploy counter-measures. Plan or intent recognition are important areas of research as well, and are the focus of several workshop papers. The detection of anomalous operations or network traffic can be viewed as a component of many security functions, including both intrusion detection and plan recognition. One of the papers in this workshop discusses improved means of anomaly detection, using the ubiquitous and increasingly powerful graphics processors in our computers. Due to the distributed nature of computer networks, they are susceptible to attack that comes from multiple directions, which can be mounted by an individual in a single location. Thus, the issue of information fusion (combining indications drawn from separate data-streams) is an important tool, as well.

With this workshop, we hope to encourage dialogue and collaboration, both between the AI and Security communities, and among researchers on both sides, working on similar problems. Further, we hope that this will foster a continuing interaction, rather than a single (or even an occasional) gathering together.

— Mark Boddy and Stefan Edelkamp
Workshop co-Chairs

Organizing Committee

Mark Boddy, Adventium Labs , USA
Stefan Edelkamp , University of Bremen , Germany

Programme Committee

Armin Biere, Johannes Kepler University, Austria
Carsten Bormann, Universität Bremen, Germany
Alessandro Cimatti, IRS, Italy
Joerg Hoffmann, SAP Research, Germany
S. K. Gosh, Indian Institute of Technology, India
Patrik Haslum, Australian National University, Australia
Alessio Lomuscio, Imperial College London, UK
Howie Shrobe ,MIT, USA
Karsten Sohr, Universität Bremen, Germany
Thomas Wagner, Universität Bremen, Germany
Luca Vigano, Università di Verona, Italy
Yacine Zemali , ONERA/ DCSD, France