Guest Editors' Introduction: Special Section on Learning, Games and Security

Christos Dimitrakakis, *Senior Member*, *IEEE*,
Tom Karygiannis, *Senior Member*, *IEEE*, and Aikaterini Mitrokotsa, *Senior Member*, *IEEE*

SECURITY applications are a point where machine learning and game theory naturally meet. This is true especially in contexts where some learning from data occurs, whose source may be adversarial, or where decision making involves interactions between multiple agents.

Part of this special issue deals with principled approaches to security problems, which employ learning or game theory. This involves problems in adversarial learning, learning in distributed settings, privacy issues of learning, or games with partial information. This issue is quite timely, for three reasons. Firstly, there has been a significant amount of recent work on learning approaches for game-theory. At the same time, game theory has been employed in a number of learning contexts, especially in adversarial learning and multiagent reinforcement learning. Finally, privacy issues related to data mining are also of high importance, due to the collection of data by numerous organisations. The strong interconnections between machine learning, cryptography and game theory, become apparent in the papers contained in this issue.

Half of the papers in this special issue deal with privacy preservation. The first paper, "Incentive Compatible Privacy-Preserving Distributed Classification," by Robert Nix and Murat Kantarcioglu, focuses on the problem of distributed data mining, where agents are required to be truthful, but where verification would violate privacy. In order to tackle this problem they employ game theoretic mechanism design to encourage agents to be truthful. The second paper, "Large Margin Gaussian Mixture Models with Differential Privacy," by Manas A. Pathak and Bhiksha Raj, deals with the problem of privacy-preserving classification, using a Gaussian mixture model. They show, both experimentally and theoretically, that their solution leads to good privacy guarantees with a very small performance loss relative to a classifier that has does not preserve privacy. Finally, "On Privacy of Encrypted Speech Communications," by Ye Zhu, Yuanchao Lu, and Anil Vikram, shows that a seemingly innocuous feature of Internet speech communication, silence suppression, can lead to privacy leakage through the revelation of speech patterns.

The remaining papers deal with security issues, and in particular with detection and responses to intrusion. The paper by Adam Barth, Benjamin I.P. Rubinstein, Mukund Sundararajan, John C. Mitchell, Dawn Song, and Peter L. Bartlett, "A Learning-Based Approach to Reactive Security," presents a generalised model of a security system which learns from experience to optimally allocate resources for counteracting future attacks. Assuming that the attacker's payoffs are unknown, but previous attacks are revealed, they prove that their algorithm performs nearly as well as the best fixed proactive strategy. The paper by Jun-Won Ho, Matthew Wright, and Sajal K. Das, "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," deals with the problem of detecting compromised nodes in wireless sensor networks. Using the classic technique of sequential hypothesis testing, they are able to efficiently identify and remove suspect nodes in an online setting. Theoretically, they show that their strategy effectively bounds the attacker's gain in their setting. Finally, "DoubleGuard: Detecting Intrusions in Multitier Web Applications," by Meixing Le, Angelos Stavrou, and Brent ByungHoon Kang, describes an intrusion detection system in a web application. They experimentally show that, with a small performance overhead, they are able to very effectively detect intrusions, while achieving very small false positive rates.

Overall, we believe that this issue has achieved its primary purpose of collecting state-of-the-art research at the intersection of learning, games and security. The papers contained in this issue not only represent important theoretical advances, which offer opportunities for further research, but also describe interesting and effective applications in real domains.

Christos Dimitrakakis
Tom Karygiannis
Katerina Mitrokotsa
Guest Editors

- *C. Dimitrakakis is with LIA, EPFL, Station 14, CH-1015, Lausanne. E-mail: christos.dimitrakakis@epfl.ch.*
- *T. Karygiannis is with the National Institute of Standards and Technology, Gaithersburg, MD 20899. E-mail: karygiannis@nist.gov.*
- *A. Mitrokotsa is with LASEC, EPFL, Station 14, CH-1015, Lausanne. E-mail: katerina.mitrokotsa@epfl.ch.*

For information on obtaining reprints of this paper, please send e-mail to: tdsc@computer.org.

Christos Dimitrakakis is a senior researcher (Marie Curie Fellow) at the artificial intelligence laboratory at EPFL, Switzerland. His research interests are reinforcement learning, decision theory, applied statistics, stochastic optimisation, multiagent systems and telecommunications. He was a postdoctoral researcher at the University of Leoben, Austria, the University of Amsterdam the Netherlands and FIAS, at Goethe-University Frankfurt, in Germany. He holds a Bachelor degree from the University of Manchester and a Masters degree from the University of Essex. After a stint at Atmel corporation he obtained his PhD from EPFL in 2006, while working at the IDIAP Research Institute in the small, but charming, town of Martigny. He is a senior member of the IEEE.

Tom Karygiannis is a senior researcher at the National Institute of Standards and Technology. His responsibilities include developing standards, metrics, tests, and validation tools to promote, measure, and validate security systems, particularly for new and emerging technologies. As a senior researcher at NIST, Tom has conducted research in secure electronic commerce, wireless security, network intrusion detection, mobile device security, RFID security, and ad hoc network security. Tom has served on expert panels organized by DHS, DNI, DARPA, NSF, the Department of Commerce Office of Technology Policy, the White House Office of Science and Technology Policy (OSTP), the Department of Transportation, the Defense Information Systems Agency, and the National Security Council's Critical Infrastructure Protection Office. Tom holds a PhD in Computer Science from the George Washington University and a Master and Bachelor of Science degree in Electrical Engineering from Bucknell University. He is a senior member of the IEEE.

Aikaterini Mitrokotsa is a senior researcher (Marie Curie fellow) at the LASEC group in EPFL. Formerly, she held positions as a postdoctoral researcher in TU Delft and as a visitor assistant professor in the Department of Computer Science at the Free University (Vrije Universiteit) in Amsterdam. In 2007, she received a PhD in Computer Science from the University of Piraeus in Greece. She has been active both in European and National research projects while she has been awarded the Rubicon Research Grant by the Netherlands Organization for Scientific Research (NWO) and a Marie Curie Intra European Fellowship. Her main research interests lie in the area of network security, intrusion detection systems, privacy-preservation, denial of service attacks and machine learning and decision making applications to RFID, fixed, wireless ad hoc and sensor networks security, as well as distance bounding protocols. She is a senior member of the IEEE.