Lecture Notes in Computer Science 11836

More information about this series at http://www.springer.com/series/7410

Tansu Alpcan · Yevgeniy Vorobeychik ·
John S. Baras · György Dán (Eds.)

Decision and Game Theory for Security

10th International Conference, GameSec 2019
Stockholm, Sweden, October 30 – November 1, 2019
Proceedings

Springer

Editors
Tansu Alpcan
University of Melbourne
Melbourne, VIC, Australia

John S. Baras
University of Maryland, College Park
College Park, MD, USA

Yevgeniy Vorobeychik
Washington University in St. Louis
St. Louis, MO, USA

György Dán
KTH Royal Institute of Technology
Stockholm, Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-32429-2 ISBN 978-3-030-32430-8 (eBook)
https://doi.org/10.1007/978-3-030-32430-8

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

It is difficult today to imagine the modern world without connectivity, information, and computing. We are now entering a new era in which typically isolated residential, commercial, and industrial devices form Cyber-Physical Systems (CPS) or Internet of Things (IoT). An important aspect of this modern connected world is complex interactions and decisions between humans, devices, and networks. Game theory, which studies multi-agent or person decision making provides a solid mathematical foundation for models investigating decisions in these emerging connected, distributed, and complex systems.

Ubiquitous connectivity creates enormous value, but also comes at a cost: connected devices and people are also more vulnerable, as malicious parties are now able to gain access to them in ways that would have been impractical only a decade ago. Consequently, information security and privacy has gained paramount importance. Traditional approaches to security and privacy view this largely as a system engineering problem, focusing on specific applications and systems. The GameSec conference, in contrast, aims to study it from a more holistic perspective, using the tools borrowed from decision theory (including optimization and control theories) and game theory, as well as, more recently, from AI and machine learning.

This volume contains the papers presented at GameSec 2019, the 10th Conference on Decision and Game Theory for Security held during October 30–November 1, 2019, in Stockholm, Sweden. The GameSec conference series was inaugurated in 2010 in Berlin, Germany. GameSec 2019 was the 10th instantiation, and in this span, it has become widely recognized as an important venue for interdisciplinary security research. The previous conferences were held in College Park (Maryland, USA, 2011), Budapest (Hungary, 2012), Fort Worth (Texas, USA, 2013), Los Angeles (USA, 2014), London (UK, 2015), New York (USA, 2016), Vienna (Austria, 2017), and Seattle (Washington, USA, 2018).

As in past years, the 2019 edition of GameSec featured a number of high-quality novel contributions. The conference program included 21 full paper presentations, as well as 11 short papers. The program contained papers on traditional GameSec topics such as game-theoretic models of various security problems, as well as an increasing number of papers at the intersection of AI, machine learning, and security, particularly in reinforcement learning, some of which were presented at the Adversarial AI special track. There is, in addition, a clear increase in the interest in this GameSec program of modeling and studying deception through a game-theoretic lens.

Several organizations supported GameSec 2019. We thank, in particular, KTH Digitalisation Research Platform, Association for Computing Machinery (ACM), Springer, Ericsson, SAAB, and F-Secure.

We hope that the readers will find this volume a useful resource for their security and game theory research.

October 2019

Tansu Alpcan
Yevgeniy Vorobeychik
John S. Baras
György Dán

Organization

Program Committee

Habtamu Abie	Norwegian Computing Centre, Norway
Tansu Alpcan	The University of Melbourne, Australia
Saurabh Amin	Massachusetts Institute of Technology, USA
Bo An	Nanyang Technological University, Singapore
Konstantin Avrachenkov	Inria, France
Svetlana Boudko	NR, Norway
Alvaro Cardenas	The University of Texas at Dallas, USA
Andrew Clark	Worcester Polytechnic Institute, USA
Jens Grossklags	Technical University of Munich, Germany
Yezekael Hayel	LIA, University of Avignon, France
Hideaki Ishii	Tokyo Institute of Technology, Japan
Eduard Jorswieck	TU Dresden, Germany
Charles Kamhoua	US Army Research Laboratory, USA
Murat Kantarcioglu	The University of Texas at Dallas, USA
Arman Mhr Khouzani	Queen Mary University of London, UK
Christopher Kiekintveld	University of Texas at El Paso, USA
Sandra König	Austrian Institute of Technology, Austria
Aron Laszka	University of Houston, USA
Yee Wei Law	University of South Australia, Australia
Bo Li	University of Illinois at Urbana-Champaign, USA
Daniel Lowd	University of Oregon, USA
Mohammad Hossein Manshaei	Florida International University (FIU), USA
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
Shana Moothedath	University of Washington, USA
Mehrdad Nojoumian	Florida Atlantic University, USA
Andrew Odlyzko	University of Minnesota, USA
Miroslav Pajic	Duke University, USA
Emmanouil Panaousis	University of Surrey, UK
Sakshyam Panda	Nokia, Finland
Radha Poovendran	University of Washington, USA
David Pym	University College London, UK
Bhaskar Ramasubramanian	University of Washington, USA
Stefan Rass	System Security Group, Universität Klagenfurt, Germany
Henrik Sandberg	KTH Royal Institute of Technology, Sweden
Stefan Schauer	AIT Austrian Institute of Technology GmbH, Austria
Arunesh Sinha	University of Michigan, USA

George Theodorakopoulos	Cardiff University, UK
Long Tran-Thanh	University of Southampton, UK
Yevgeniy Vorobeychik	Washington University in St. Louis, USA
Haifeng Xu	University of Southern California, USA
Quanyan Zhu	New York University, USA
Jun Zhuang	SUNY Buffalo, USA

Additional Reviewers

Basak, Anjon
Collinson, Matthew
Elfar, Mahmoud
Gan, Jiarui
Gutierrez, Marcus
Li, Zuxing
Liang, Bei
Milosevic, Jezdimir
Misra, Shruti
Nekouei, Ehsan
Ortiz, Anthony
Sagong, Sang Uk
Sahabandu, Dinuka
Saritaş, Serkan
Thakoor, Omkar
Tsaloli, Georgia
Veliz, Oscar
Wang, Yu
Williams, Julian
Xiao, Baicen
Zhang, Jing

Contents