

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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

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

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Contents

Design of Load Forecast Systems Resilient Against Cyber-Attacks	1
<i>Carlos Barreto and Xenofon Koutsoukos</i>	
Identifying Stealthy Attackers in a Game Theoretic Framework Using Deception	21
<i>Anjon Basak, Charles Kamhoua, Sridhar Venkatesan, Marcus Gutierrez, Ahmed H. Anwar, and Christopher Kiekintveld</i>	
Choosing Protection: User Investments in Security Measures for Cyber Risk Management	33
<i>Yoav Ben Yaakov, Xinrun Wang, Joachim Meyer, and Bo An</i>	
When Is a Semi-honest Secure Multiparty Computation Valuable?	45
<i>Radhika Bhargava and Chris Clifton</i>	
You only Lie Twice: A Multi-round Cyber Deception Game of Questionable Veracity	65
<i>Mark Bilinski, Kimberly Ferguson-Walter, Sunny Fugate, Ryan Gabrys, Justin Mauger, and Brian Souza</i>	
Honeypot Type Selection Games for Smart Grid Networks	85
<i>Nadia Boumkheld, Sakshyam Panda, Stefan Rass, and Emmanouil Panaousis</i>	
Discussion of Fairness and Implementability in Stackelberg Security Games.	97
<i>Victor Bucarey and Martine Labbé</i>	
Toward a Theory of Vulnerability Disclosure Policy: A Hacker's Game	118
<i>Taylor J. Canann</i>	
Investing in Prevention or Paying for Recovery - Attitudes to Cyber Risk . . .	135
<i>Anna Cartwright, Edward Cartwright, and Lian Xue</i>	
Realistic versus Rational Secret Sharing.	152
<i>Yvo Desmedt and Arkadii Slinko</i>	
Solving Cyber Alert Allocation Markov Games with Deep Reinforcement Learning.	164
<i>Noah Dunstatter, Alireza Tahsini, Mina Guirguis, and Jelena Tešić</i>	

Power Law Public Goods Game for Personal Information Sharing in News Commentaries	184
<i>Christopher Griffin, Sarah Rajtmajer, Prasanna Umar, and Anna Squicciarini</i>	
Adaptive Honeypot Engagement Through Reinforcement Learning of Semi-Markov Decision Processes	196
<i>Linan Huang and Quanyan Zhu</i>	
Deceptive Reinforcement Learning Under Adversarial Manipulations on Cost Signals.	217
<i>Yunhan Huang and Quanyan Zhu</i>	
DeepFP for Finding Nash Equilibrium in Continuous Action Spaces	238
<i>Nitin Kamra, Umang Gupta, Kai Wang, Fei Fang, Yan Liu, and Milind Tambe</i>	
Effective Premium Discrimination for Designing Cyber Insurance Policies with Rare Losses.	259
<i>Mohammad Mahdi Khalili, Xueru Zhang, and Mingyan Liu</i>	
Analyzing Defense Strategies Against Mobile Information Leakages: A Game-Theoretic Approach	276
<i>Kavita Kumari, Murtuza Jadliwala, Anindya Maiti, and Mohammad Hossein Manshaei</i>	
Dynamic Cheap Talk for Robust Adversarial Learning.	297
<i>Zuxing Li and György Dán</i>	
Time-Dependent Strategies in Games of Timing	310
<i>Jonathan Merlevede, Benjamin Johnson, Jens Grossklags, and Tom Holvoet</i>	
Tackling Sequential Attacks in Security Games.	331
<i>Thanh H. Nguyen, Amulya Yadav, Branislav Bosansky, and Yu Liang</i>	
A Framework for Joint Attack Detection and Control Under False Data Injection.	352
<i>Luyao Niu and Andrew Clark</i>	
QFlip: An Adaptive Reinforcement Learning Strategy for the FlipIt Security Game	364
<i>Lisa Oakley and Alina Oprea</i>	
Linear Temporal Logic Satisfaction in Adversarial Environments Using Secure Control Barrier Certificates	385
<i>Bhaskar Ramasubramanian, Luyao Niu, Andrew Clark, Linda Bushnell, and Radha Poovendran</i>	

Cut-The-Rope: A Game of Stealthy Intrusion	404
<i>Stefan Rass, Sandra König, and Emmanouil Panaousis</i>	
Stochastic Dynamic Information Flow Tracking Game with Reinforcement Learning	417
<i>Dinuka Sahabandu, Shana Moothedath, Joey Allen, Linda Bushnell, Wenke Lee, and Radha Poovendran</i>	
Adversarial Attacks on Continuous Authentication Security: A Dynamic Game Approach	439
<i>Serkan Sarıtaş, Ezzeldin Shereen, Henrik Sandberg, and György Dán</i>	
On the Optimality of Linear Signaling to Deceive Kalman Filters over Finite/Infinite Horizons	459
<i>Muhammed O. Sayin and Tamer Başar</i>	
MTDeep: Boosting the Security of Deep Neural Nets Against Adversarial Attacks with Moving Target Defense	479
<i>Sailik Sengupta, Tathagata Chakraborti, and Subbarao Kambhampati</i>	
General Sum Markov Games for Strategic Detection of Advanced Persistent Threats Using Moving Target Defense in Cloud Networks.	492
<i>Sailik Sengupta, Ankur Chowdhary, Dijiang Huang, and Subbarao Kambhampati</i>	
Operations over Linear Secret Sharing Schemes	513
<i>Arkadii Slinko</i>	
Cyber Camouflage Games for Strategic Deception	525
<i>Omkar Thakoor, Milind Tambe, Phebe Vayanos, Haifeng Xu, Christopher Kiekintveld, and Fei Fang</i>	
When Players Affect Target Values: Modeling and Solving Dynamic Partially Observable Security Games	542
<i>Xinrun Wang, Milind Tambe, Branislav Bošanský, and Bo An</i>	
Perfectly Secure Message Transmission Against Independent Rational Adversaries	563
<i>Kenji Yasunaga and Takeshi Koshihara</i>	
Author Index	583