Lecture Notes in Computer Science 9996

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Quanyan Zhu · Tansu Alpcan
Emmanouil Panaousis · Milind Tambe
William Casey (Eds.)

Decision and Game Theory for Security

7th International Conference, GameSec 2016 New York, NY, USA, November 2–4, 2016 Proceedings

Springer

Editors
Quanyan Zhu
New York University
New York, NY
USA

Tansu Alpcan
The University of Melbourne
Melbourne, VIC
Australia

Emmanouil Panaousis
University of Brighton
Brighton
UK

Milind Tambe
University of Southern California
Los Angeles, CA
USA

William Casey
Carnegie Mellon University
Pittsburgh, NY
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-47412-0 ISBN 978-3-319-47413-7 (eBook)
DOI 10.1007/978-3-319-47413-7

Library of Congress Control Number: 2016953220

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

Communication and information technologies have evolved apace. Recent advances feature greater ubiquity and tighter connectivity for systems exchanging increasingly larger amounts of social, personal, and private information. Indeed, cyberspace, constructed on top of these technologies, has become integral to the lives of people, communities, enterprises, and nation states.

Yet protecting the various assets therein to ensure cybersecurity is a difficult challenge. First, and no differently from physical security, a wide variety of agent utilities abound, including adversarial and antithetical types. Second, being constructed upon heterogeneous, large-scale, and dynamic networks, cyberspace is fairly complex, offering adversaries a large attack surface and ample room for evasive maneuvers, even within carefully designed network and software infrastructure. Nonetheless, security is critical and warrants novel analytic, computational, and practical approaches to thought, planning, policy, and strategic action so we can protect systems and the critical assets they contain, minimize risks and maximize investments, and ultimately provide practical and salable security mechanisms. Collectively our aim is to enhance the trustworthiness of cyber-physical systems.

Recently the analytic and modeling framework of modern game theory has yielded powerful and elegant tools for considering security and the effects of non-cooperative and adversarial types. The problems of security and cybersecurity by necessity must confront the challenging adversarial and worst-case outcomes. To address these, researchers have brought to bear diverse methodologies from control, mechanism design, incentive analysis, economics, and data science to co-evolve advances in game theory, and to develop solid underpinnings of a science of security and cybersecurity.

The GameSec conference brings together academic, industry, and government researchers to identify and discuss the major technical challenges and present recent research results that highlight the connections between and among game theory, control, distributed optimization, and economic incentives within the context of real-world security, trust, and privacy problems. The past meetings of the GameSec conference took place in Berlin, Germany (2010), College Park Maryland, USA (2011), Budapest, Hungary (2012), Fort Worth Texas, USA (2013), Los Angeles, USA (2014), and London, UK (2015). GameSec 2016, the 7th Conference on Decision and Game Theory for Security took place in New York, USA, during November 2–4, 2016. This year we extended the two-day format to a three-day program, allowing GameSec to expand topic areas, include a special track and a poster session.

Since its first edition in 2010, GameSec has attracted novel, high-quality theoretical and practical contributions. This year was no exception. The conference program included 18 full and eight short papers as well as multiple posters that highlighted the research results presented. Reviews were conducted on 40 submitted papers. The selected papers and posters were geographically diverse with many international and transcontinental authorship teams. Whith the geographical diversity underscoring the

global concern for and significance of security problems, the papers this year demonstrated several international efforts formed to address them.

The themes of the conference this year were broad and encompassed work in the areas of network security, security risks and investments, decision-making for privacy, security games, incentives in security, cybersecurity mechanisms, intrusion detection, and information limitations in security. The program also included a special track on "validating models," which aims to close the gap between theory and practice in the domain, chaired by Prof. Milind Tambe. Each area took on critical challenges including the detection/mitigation problems associated with several specific attacks to network systems, optimal and risk-averse management of systems, the increased concern of data integrity, leakage, and privacy, strategic thinking for/against adversarial types, adversarial incentives and robust and novel designs to counter them, and acting/decision making in partially informed adversarial settings.

Collectively the conference presents many novel theoretical frameworks and impacts directly the consideration of security in a wide range of settings including: advanced persistent threat (APT), auditing elections, cloud-enabled internet of controlled things, compliance, crime and cyber-criminal incentives, cyber-physical systems, data exfiltration detection, data leakage, denial of service attacks (DOS), domain name service (DNS), electric infrastructures, green security, Internet of Things (IoT), intrusion detection systems (IDS), patrolling (police and pipeline), privacy technology, routing in parallel link networks, secure passive RFID networks, social networking and deception, strategic security investments, voting systems, and watermarking.

We would like to thank NSF for its continued support for student travel, which made it possible for many domestic and international undergraduate and graduate students to attend the conference. We would also like to thank Springer for its continued support of the GameSec conference and for publishing the proceedings as part of their *Lecture Notes in Computer Science* (LNCS) series. We hope that not only security researchers but also practitioners and policy makers will benefit from this edition.

November 2016

Quanyan Zhu
Tansu Alpcan
Emmanouil Panaousis
Milind Tambe
William Casey

Organization

Steering Board

Tansu Alpcan	The University of Melbourne, Australia
Nick Bambos	Stanford University, USA
John S. Baras	University of Maryland, USA
Tamer Başar	University of Illinois at Urbana-Champaign, USA
Anthony Ephremides	University of Maryland, USA
Jean-Pierre Hubaux	EPFL, Switzerland
Milind Tambe	University of Southern California, USA

Organizers

General Chair

Quanyan Zhu	New York University, USA

TPC Chairs

Tansu Alpcan	University of Melbourne, Australia
Emmanouil Panaousis	University of Brighton, UK

Publication Chair

William Casey	Carnegie Mellon University, USA

Special Track Chair

Milind Tambe	University of Southern California, USA

Local Arrangements and Registration Chair

Raquel Thompson	New York University, USA

Publicity Chairs

Mohammad Hossein Manshaei	Isfahan University of Technology, Iran
Stefan Rass	Universität Klagenfurt, Austria
Charles Kamhoua	US Air Force Research Laboratory, USA

Web Chair

Jeffrey Pawlick	New York University, USA

Technical Program Committee

TPC Chairs

Tansu Alpcan	University of Melbourne, Australia
Emmanouil Panaousis	University of Brighton, UK

TPC Members

Habtamu Abie	Norsk Regnesentral – Norwegian Computing Center, Norway
Saurabh Amin	Massachusetts Institute of Technology, USA
Bo An	Nanyang Technological University, Singapore
Alvaro Cardenas	University of Texas at Dallas, USA
Anil Kumar Chorppath	Technische Universität Dresden, Germany
Sajal Das	Missouri University of Science and Technology, USA
Mark Felegyhazi	Budapest University of Technology and Economics, Hungary
Andrew Fielder	Imperial College London, UK
Cleotilde Gonzalez	Carnegie Mellon University, USA
Jens Grossklags	Penn State University, USA
Yezekael Hayel	LIA/University of Avignon, France
Karl Henrik Johansson	Royal Institute of Technology, Sweden
Murat Kantarcioglu	University of Texas at Dallas, USA
Christopher Kiekintveld	University of Texas at El Paso, USA
Aron Laszka	University of California, Berkeley, USA
Yee Wei Law	University of South Australia, Australia
Pasquale Malacaria	Queen Mary University of London, UK
Mohammad Hossein Manshaei	EPFL, Switzerland
Mehrdad Nojoumian	Florida Atlantic University, USA
Andrew Odlyzko	University of Minnesota, USA
David Pym	University College London, UK
Reza Shokri	Cornell University, USA
Arunesh Sinha	University of Southern California, USA
George Theodorakopoulos	Cardiff University, UK
Pradeep Varakantham	Singapore Management University, Singapore
Athanasios Vasilakos	NTUA, Greece
Yevgeniy Vorobeychik	Vanderbilt University, USA
Nan Zhang	The George Washington University, USA
Jun Zhuang	SUNY Buffalo, USA

Contents