Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Radha Poovendran Walid Saad (Eds.)

Decision and Game Theory for Security

5th International Conference, GameSec 2014
Los Angeles, CA, USA, November 6-7, 2014
Proceedings

Volume Editors

Radha Poovendran
University of Washington
Electrical Engineering Department, Network Security Lab
Box 352500, Seattle, WA 98195-2055, USA
E-mail: rp3@uw.edu

Walid Saad
Virginia Tech, Department of Electrical and Computer Engineering
Whittemore Hall 302, 1185 Perry Street, Blacksburg, VA 24061, USA
E-mail: walids@vt.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-12600-5 e-ISBN 978-3-319-12601-2
DOI 10.1007/978-3-319-12601-2
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014951399

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Recent advances in networking, communications, computation, software, and hardware technologies have revolutionized the information technology landscape. Indeed, this cyberspace has become an integral part of every person's daily life and the way we conduct business. Protecting the sensitive content of every nation's cyberspace infrastructure has thus become critical to ensure economic growth, prosperity, and advancement. However, the heterogeneous, dynamic, and large-scale nature of modern-day networked and information technology infrastructure warrants novel analytical and practical approaches for securing its assets and maintaining its trustworthiness.

Owing to its powerful analytical and modeling frameworks, game theory has recently emerged as a key tool for building resilient, secure, and dependable networked systems. Coupled with synergistic techniques such as dynamic control, mechanism design, and economics, game theory, along with incentives and mechanisms design, is expected to provide one of the pillars of the "science of security." The proceedings of the GameSec 2014 conference contain original contributions presenting theoretical and practical contributions that will build the knowledge base in the science of security, in general, and game-theoretic security, in particular.

The topics cover multiple facets of cybersecurity that include: rationality of adversary, game-theoretic cryptographic techniques, vulnerability discovery and assessment, multi-goal security analysis, secure computation, economic-oriented security, and surveillance for security. These aspects are covered in a multitude of domains that include networked systems, wireless communications, border patrol security, and control systems. The GameSec conference aims to provide a forum for engineers, game and control theorists, and computer scientists from research and industry to contribute and develop the foundation of the next generation of security science. We are pleased to bring these proceedings to your hands. Enjoy!

September 2014

Walid Saad
Radha Poovendran

Organization

Steering Board

Tansu Alpcan	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

Organizers

General Chair

Radha Poovendran	University of Washington, USA
------------------	-------------------------------

TPC Chair

Walid Saad	Virginia Tech, USA
------------	--------------------

Publicity Chair

Quanyan Zhu	NYU, USA
-------------	----------

Publication Chair

Rahul Jain	USC, USA
------------	----------

Local Arrangements Chair

Terry Benzel	USC, USA
--------------	----------

Web Chair

Hao Shi	USC, USA
---------	----------

Finance Chair

Albert Jiang	USC, USA
--------------	----------

Technical Program Committee

TPC Chair

Walid Saad	Virginia Tech, USA
------------	--------------------

TPC Members

Ali Khanafer	UIUC
Jia Liu	OSU
Veronica Belmega	ETIS / ENSEA
Samir Perlaza	Inria, France
Andrey Garnaev	St. Petersburg State University, Russia
Xiang-Yang Li	Illinois Institute of Technology, USA
Tansu Alpcan	University of Melbourne, Australia
Jens Grossklags	Penn State University, USA
Nan Zhang	GWU
Alvaro Cardenas	University of Texas, Dallas, USA
John S. Baras	University of Maryland, USA
Stefan Schmid	TU Berlin, Germany
Radu State	University of Luxembourg
John Chuang	UC Berkeley, USA
Bud Mishra	NYU, USA
Murat Kantarcioglu	University of Texas, Dallas, USA
M. Hossein Manshaei	University of Isfahan, Iran
Sankardas Roy	KSU
Mehrdad Nojournian	Southern Illinois University, USA
Amitav Mukherjee	Hitachi
Andrew Odlyzko	University of Minnesota, USA
John Musacchio	UC - Santa Cruz, USA
Yingying Chen	Stevens Institute of Technology, USA
Ross Anderson	Cambridge University, UK
Manos Panaousis	Queen Mary, University of London, UK
Pradeep Varakantham	Singapore Management University
Yevgeniy Vorobeychik	Vanderbilt University, USA
Christopher Kiekintveld	University of Texas at El Paso, USA
Rong Yang	XEROX PARC

Table of Contents

Full Papers

Defending Against Opportunistic Criminals: New Game-Theoretic Frameworks and Algorithms	3
<i>Chao Zhang, Albert Xin Jiang, Martin B. Short, P. Jeffrey Brantingham, and Milind Tambe</i>	
Addressing Scalability and Robustness in Security Games with Multiple Boundedly Rational Adversaries	23
<i>Matthew Brown, William B. Haskell, and Milind Tambe</i>	
Empirical Game-Theoretic Analysis of an Adaptive Cyber-Defense Scenario (Preliminary Report)	43
<i>Michael P. Wellman and Achintya Prakash</i>	
Strategic Discovery and Sharing of Vulnerabilities in Competitive Environments	59
<i>M.H.R. Khouzani, Viet Pham, and Carlos Cid</i>	
Optimal Contracts for Outsourced Computation	79
<i>Viet Pham, M.H.R. Khouzani, and Carlos Cid</i>	
A Supervisory Control Approach to Dynamic Cyber-Security	99
<i>Mohammad Rasouli, Erik Miehl, and Demosthenis Teneketzis</i>	
Numerical Computation of Multi-goal Security Strategies	118
<i>Stefan Rass and Benjamin Rainer</i>	
Realizable Rational Multiparty Cryptographic Protocols	134
<i>John Ross Wallrabenstein and Chris Clifton</i>	
Limiting Adversarial Budget in Quantitative Security Assessment	155
<i>Aleksandr Lenin and Ahto Buldas</i>	
FlipThem: Modeling Targeted Attacks with FlipIt for Multiple Resources	175
<i>Aron Laszka, Gabor Horvath, Mark Felegyhazi, and Levente Buttyán</i>	
Secure Message Delivery Games for Device-to-Device Communications	195
<i>Emmanouil Panaousis, Tansu Alpcan, Hossein Fereidooni, and Mauro Conti</i>	

A Three-Stage Colonel Blotto Game: When to Provide More Information to an Adversary	216
<i>Abhishek Gupta, Tamer Başar, and Galina A. Schwartz</i>	
Toward Optimal Network Topology Design for Fast and Secure Distributed Computation	234
<i>Ji Liu and Tamer Başar</i>	
An Economic Model and Simulation Results of App Adoption Decisions on Networks with Interdependent Privacy Consequences	246
<i>Yu Pu and Jens Grossklags</i>	
Cybersecurity Games and Investments: A Decision Support Approach	266
<i>Emmanouil Panaousis, Andrew Fielder, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi</i>	
Data Integrity and Availability Verification Game in Untrusted Cloud Storage	287
<i>Brahim Djebaili, Christophe Kiennert, Jean Leneutre, and Lin Chen</i>	

Short Papers

Empirical Comparisons of Descriptive Multi-objective Adversary Models in Stackelberg Security Games	309
<i>Jinshu Cui and Richard S. John</i>	
A Dynamic Bayesian Security Game Framework for Strategic Defense Mechanism Design	319
<i>Sadeqh Farhang, Mohammad Hossein Manshaei, Milad Nasr Esfahani, and Quanyan Zhu</i>	
Can Less Be More? A Game-Theoretic Analysis of Filtering vs. Investment	329
<i>Armin Sarabi, Parinaz Naghizadeh, and Mingyan Liu</i>	
Online Learning Methods for Border Patrol Resource Allocation	340
<i>Richard Klíma, Christopher Kiekintveld, and Viliam Lisý</i>	
A Distributed Optimization Algorithm for Attack-Resilient Wide-Area Monitoring of Power Systems: Theoretical and Experimental Methods	350
<i>Jianhua Zhang, Prateek Jaipuria, Aranya Chakraborty, and Alefiya Hussain</i>	
Testing for Hardware Trojans: A Game-Theoretic Approach	360
<i>Charles A. Kamhoua, Manuel Rodriguez, and Kevin A. Kwiat</i>	

Surveillance for Security as a Pursuit-Evasion Game	370
<i>Sourabh Bhattacharya, Tamer Başar, and Maurizio Falcone</i>	
Author Index	381