

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>

Massimiliano Albanese · Ross Horne ·
Christian W. Probst (Eds.)

Graphical Models for Security

6th International Workshop, GraMSec 2019
Hoboken, NJ, USA, June 24, 2019
Revised Papers

Editors

Massimiliano Albanese 
George Mason University
Fairfax, VA, USA

Ross Horne 
University of Luxembourg
Esch-sur-Alzette, Luxembourg

Christian W. Probst
Unitec Institute of Technology
Auckland, New Zealand

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-36536-3 ISBN 978-3-030-36537-0 (eBook)
<https://doi.org/10.1007/978-3-030-36537-0>

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

This volume includes all the contributions made to the 6th edition of the International Workshop on Graphical Models for Security (GraMSec 2019). As in the previous four editions, GraMSec 2019 was held as a workshop co-located with the IEEE Computer Security Foundations Symposium (CSF), which was in its 32nd edition (CSF 2019). Both events were hosted at the Stevens Institute of Technology campus located at 1 Castle Point Terrace in Hoboken, New Jersey, USA. GraMSec 2019 was held on June 24, 2019, as a pre-conference workshop.

This edition of GraMSec reflected on the diversity of graphical approaches for analyzing the security of systems. The traditional priority area of GraMSec has been the area of formal methods underpinning graphical models such as attack trees and attack graphs. Attack trees can be used for structured reasoning about the sub-goals of attackers, while attack graphs typically capture the dynamics of an attack surface. As models mature and new applications are explored, GraMSec is taking an increasingly broader view of what constitutes a graphical model in the analysis of systems security. Indeed, taking such a broader view can be regarded as a necessary step in the effort to continually adjust graphical methods to meet the needs of security practitioners and facilitate the transition to practice of research outcomes.

We had the honor to open the workshop with an invited talk by George Cybenko, the Dorothy and Walter Gramm Professor of Engineering at the Dartmouth's Thayer School of Engineering. Prof. Cybenko provided insights into a research direction where control flow graphs, a classical graphical method for program analysis, could be inferred from radio frequency emissions of microprocessors.

Other graphical methods explored in this workshop, beyond attack trees and graphs, included: bow-tie diagrams for modeling causal dependencies surrounding a security risk, and project management enhancements for the EBIOS cyber security methodology. Some papers also considered a graphical subject matter such as social network graphs. However, the mainstay of the research presented remains in the field of attack trees, as is traditional for GraMSec, where papers both extended existing attack tree methodologies and developed compelling case studies.

This year, we received 15 submissions, of which 8 were accepted as regular papers. These proceedings were published after the event, giving authors the opportunity to revise and enhance their manuscripts based on feedback received at the workshop. These proceedings also feature two invited papers from our keynote George Cybenko and from Olga Gadyatskaya and Sjouke Mauw. Papers received an average of 3.5 reviews in a single-blind review process, with each Program Committee member reviewing two papers on average.

We thank the Program Committee members for their timely responses to review requests, and the authors for their sterling contributions. We also extend a special thanks to Barbara Fila and Fabio Persia, who volunteered to chair workshop sessions, thus contributing to the smooth running of the workshop. Finally, we thank Dominic

Duggan, the general chair of CSF 2019, who took the responsibility of coordinating all the logistics for the main conference and co-located workshops. We look forward to future editions of this workshop series.

October 2019

Massimiliano Albanese

Ross Horne

Christian W. Probst

Organization

General Chair

Christian W. Probst	Unitec Institute of Technology, New Zealand
---------------------	---

Program Committee Chairs

Massimiliano Albanese	George Mason University, USA
Ross Horne	University of Luxembourg, Luxembourg

Steering Committee

Sushil Jajodia	George Mason University, USA
Barbara Kordy	INSA Rennes, Irisa, France
Sjouke Mauw	University of Luxembourg, Luxembourg
Christian W. Probst	Unitec, New Zealand
Ketil Stølen	SINTEF Digital and University of Oslo, Norway

Program Committee

Ludovic Apvrille	Télécom ParisTech, France
Zaruhi Aslanyan	Alexandra Institute, Denmark
Stefano Bistarelli	Università di Perugia, Italy
Hasan Cam	U.S. Army Research Laboratory, USA
Nora Cuppens-Boulahia	IMT Atlantique, France
Harley Eades III	Augusta University, USA
Olga Gadyatskaya	SnT, University of Luxembourg, Luxembourg
Guy McCusker	University of Bath, UK
René Rydhof Hansen	Aalborg University, Denmark
Jin B. Hong	The University of Western Australia, Australia
DongSeong Kim	The University of Queensland, Australia
Barbara Kordy	INSA Rennes, Irisa, France
Sjouke Mauw	University of Luxembourg, Luxembourg
Per Håkon Meland	SINTEF ICT, Norway
Guozhu Meng	Chinese Academy of Sciences in Beijing, China
Vivek Nigam	fortiss GmbH, Germany
Andreas Lothe Opdahl	University of Bergen, Norway
Noseong Park	George Mason University, USA
Stéphane Paul	Thales Research and Technology, France
Sophie Pinchinat	INSA Rennes, France
Saša Radomirovic	University of Dundee, UK

Rolando Trujillo Rasúa	Deakin University, Australia
Paul Rowe	The MITRE Corporation, USA
Giedre Sabaliauskaite	Singapore University of Technology and Design, Singapore
Ketil Stølen	SINTEF, Norway
Sridhar Venkatesan	Vencore Labs, USA

Publicity Chair

Ibifubara Iganibo	George Mason University, USA
-------------------	------------------------------

Additional Reviewers

Tim Willemse
Michel Hurfin
Aleksandr Lenin
Francesco Santini
Valérie Viet Triem Tong

Contents

Invited Papers

Graph Models in Tracking Behaviors for Cyber-Security	3
<i>George Cybenko</i>	
Attack-Tree Series: A Case for Dynamic Attack Tree Analysis	7
<i>Olga Gadyatskaya and Sjouke Mauw</i>	

Attack Trees

Attack Trees: A Notion of Missing Attacks	23
<i>Sophie Pinchinat, Barbara Fila, Florence Wacheux, and Yann Thierry-Mieg</i>	
Optimizing System Architecture Cost and Security Countermeasures	50
<i>Sahar Berro, Ludovic Apvrille, and Guillaume Duc</i>	
Security Analysis of IoT Systems Using Attack Trees	68
<i>Delphine Beaulaton, Najah Ben Said, Ioana Cristescu, and Salah Sadou</i>	
Attack–Defense Trees for Abusing Optical Power Meters: A Case Study and the OSEAD Tool Experience Report.	95
<i>Barbara Fila and Wojciech Wideł</i>	

Risk Management and Attack Graphs

Quantifying and Analyzing Information Security Risk from Incident Data . . .	129
<i>Gaute Wangen</i>	
Poster Support for an Obeya-Like Risk Management Approach	155
<i>Stéphane Paul and Paul Varela</i>	
Conceptual Abstraction of Attack Graphs - A Use Case of securiCAD	186
<i>Xinyue Mao, Mathias Ekstedt, Engla Ling, Erik Ringdahl, and Robert Lagerström</i>	
High-Level Automatic Event Detection and User Classification in a Social Network Context.	203
<i>Fabio Persia and Sven Helmer</i>	
Author Index	221