

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>

George Hatzivasilis · Sotiris Ioannidis (Eds.)

Model-driven Simulation and Training Environments for Cybersecurity

Second International Workshop, MSTEC 2020
Guildford, UK, September 14–18, 2020
Revised Selected Papers

Editors

George Hatzivasilis 
Foundation for Research
and Technology - Hellas
Heraklion, Greece

Sotiris Ioannidis
Technical University of Crete
Chania, Greece

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-62432-3 ISBN 978-3-030-62433-0 (eBook)
<https://doi.org/10.1007/978-3-030-62433-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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 contains the papers presented at the Second Workshop on Model-driven Simulation and Training Environments for Cybersecurity (MSTEC 2020), held virtually on September 17, 2020, under the ESORICS 2020 conference.

The MSTEC 2020 workshop addressed recent advances in the field of cyber modeling and simulation. It aimed to provide a forum of practitioners and researchers to discuss cyber modeling and simulation (M&S) as well as its application to the development of cyber-security training scenarios and courses of action (COAs). Specifically, it focused on the verification and validation (V&V) process, which provides the operational community with confidence in knowing that cyber models represent the real world, and discusses how defense training may benefit from cyber models. It also investigates advances in emulators, simulators, and their potential combination. The papers presented at MSTEC 2020 took a holistic approach to the overall system assurance process, presenting advances in the simulation of people, policies, processes, and technologies currently available in the field. The workshop aimed to connect the multiple threads that currently compose M&S into a coherent view of what is usable in order to train experts and non-computer-savvy users towards an assured operation of critical systems.

There were 20 submissions. Each submission was reviewed by at least three Program Committee members. The committee decided to accept 10 papers.

The main sponsorship was provided by the European Union Horizon's 2020 research and innovation program THREAT-ARREST (www.threat-arrest.eu) under the grant agreements No. 786890.

We would like to thank the committee members and the reviewers for their voluntary effort as well as all the authors of the submitted papers for their contributions.

September 2020

George Hatzivasilis
Sotiris Ioannidis

Organization

Program Committee Chair

Sotiris Ioannidis Technical University of Crete, Greece

General Chairs

Ernesto Damiani University of Milan, Italy
Vassilis Prevelakis Technical University of Braunschweig, Germany
George Spanoudakis Sphynx Technology Solutions AG, Switzerland
Michael Vinov IBM, Israel

Technical Committee

George Hatzivasilis FORTH, Greece
Fulvio Frati University of Milan, Italy
Marinos Tsantekidis Technical University of Braunschweig, Germany
Kostantinos Fysarakis Sphynx Technology Solutions AG, Switzerland
Ludger Goeke Social-Engineering Academy, Germany
Hristo Koshutanski ATOS, Spain
George Leftheriotis TUV Hellas, Greece
George Tsakirakis ITML, Greece

Additional Reviewers

Othonas Soultatos Iason Somarakis
Eftychia Lakka Manos Michalodimitrakis
Georg Leftheriotis Manos Chatzimpyros
Torsten Hildebrandt Dirk Wortmann
Stelvio Cimato Chiara Braghin
George Bravos Vina Rompoti
Robert Bordianu Menelaos Ioannidis
Oleg Blinder Maria Crociani
Fotis Oikonomou Takis Varelas
Giovanni Gorgoni Libor Manda

Contents

Cyber Security Training Modelling

| | |
|---------------------------------------------------------------------------------------------------------------------------|---|
| Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems | 3 |
| <i>Marcus Knüpfer, Tore Bierwirth, Lars Stiemert, Matthias Schopp, Sebastian Seeber, Daniela Pöhn, and Peter Hillmann</i> | |

| | |
|------------------------------------------------------------------------------------------------------------|----|
| Cyber Range Training Programme Specification Through Cyber Threat and Training Preparation Models. | 22 |
| <i>Michail Smyrlis, Konstantinos Fysarakis, George Spanoudakis, and George Hatzivasilis</i> | |

Serious Games

| | |
|-------------------------------------------------------------------------------------------------------|----|
| A Pond Full of Phishing Games - Analysis of Learning Games for Anti-Phishing Education | 41 |
| <i>Rene Roepke, Klemens Koehler, Vincent Drury, Ulrik Schroeder, Martin R. Wolf, and Ulrike Meyer</i> | |

| | |
|--------------------------------------------------------------------------------|----|
| Conceptualization of a CyberSecurity Awareness Quiz. | 61 |
| <i>Sebastian Pape, Ludger Goeke, Alejandro Quintanar, and Kristian Beckers</i> | |

Emulation and Simulation Studies

| | |
|-------------------------------------------------------------------------------------------------------------|----|
| Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges | 79 |
| <i>Chiara Braghin, Stelvio Cimato, Ernesto Damiani, Fulvio Frati, Elvinia Riccobene, and Sadegh Astaneh</i> | |

| | |
|--------------------------------------------------------------------------------|----|
| Automatically Protecting Network Communities by Malware Epidemiology | 92 |
| <i>Xiao-Si Wang, Jessica Welding, and Tek Kan Chung</i> | |

Attacks

| | |
|-------------------------------------------------------------------|-----|
| Chasing Botnets: A Real Security Incident Investigation | 111 |
| <i>George Hatzivasilis and Martin Kunc</i> | |

| | |
|-------------------------------------------------------------------|-----|
| Software System Exploration Using Library Call Analysis | 125 |
| <i>Marinos Tsantekidis and Vassilis Prevelakis</i> | |

Security Policies

A Pattern–Driven Adaptation in IoT Orchestrations to Guarantee SPDI Properties. 143
Papoutsakis Manos, Fysarakis Konstantinos, Michalodimitrakis Emmanouil, Lakka Eftychia, Petroulakis Nikolaos, Spanoudakis George, and Ioannidis Sotiris

Password Management: How Secure Is Your Login Process? 157
George Hatzivasilis

Author Index 179