

Lecture Notes in Networks and Systems

Volume 310

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA,
School of Electrical and Computer Engineering—FEEC, University of Campinas—
UNICAMP, São Paulo, Brazil

Okyay Kaynak, Department of Electrical and Electronic Engineering,
Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University
of Illinois at Chicago, Chicago, USA; Institute of Automation, Chinese Academy
of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering,
University of Alberta, Alberta, Canada; Systems Research Institute,
Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering,
KIOS Research Center for Intelligent Systems and Networks, University of Cyprus,
Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong,
Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.


All books published in the series are submitted for consideration in Web of Science.


More information about this series at <http://www.springer.com/series/15179>


Kim-Kwang Raymond Choo ·
Tommy Morris · Gilbert Peterson ·
Eric Imsand
Editors


National Cyber Summit (NCS) Research Track 2021

Editors

Kim-Kwang Raymond Choo 
Department of Information Systems
and Cyber Security
The University of Texas at San Antonio
San Antonio, TX, USA

Tommy Morris 
Department of Electrical
and Computer Engineering
University of Alabama in Huntsville
Huntsville, AL, USA

Gilbert Peterson 
Department of Electrical
and Computer Engineering
Air Force Institute of Technology
Wright-Patterson Air Force Base, OH, USA

Eric Imsand 
Information Technology and Systems
Center (ITSC)
University of Alabama in Huntsville
Huntsville, AL, USA

ISSN 2367-3370

ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-3-030-84613-8

ISBN 978-3-030-84614-5 (eBook)

<https://doi.org/10.1007/978-3-030-84614-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed 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

While governments around the world have focused on strengthening their cybersecurity posture in recent years, cybersecurity remains a topic of ongoing importance. For example, in the “Executive Order on Improving the Nation’s Cybersecurity (May 12, 2021)”¹, it was reported that:

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

As we have noted in the past years, there is a continuing need to keep a watchful brief on the cyber threat landscape, and this is the intention of this conference proceedings.

This conference proceedings contains a total of 13 papers consisting of both regular and invited papers from the 2021 National Cyber Summit Research Track. The 2021 National Cyber Summit was originally planned to be held in Huntsville, Alabama, from June 8 to 10, 2021. However, due to the COVID-19 pandemic, all tracks of the 2021 National Cyber Summit were delayed until September of 2021. The 2021 National Cyber Summit Research Track was held in-person from September 28 to 30. Authors from each selected paper presented their work and took questions from the audience.

¹<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

The papers were selected from submissions from universities, national laboratories, and the private sector from across the USA. All of the papers went through an extensive review process by internationally recognized experts in cyber-security.

The Research Track at the 2021 National Cyber Summit has been made possible by the joint effort of a large number of individuals and organizations worldwide. There is a long list of people who volunteered their time and energy to put together the conference and deserved special thanks. First and foremost, we would like to offer our gratitude to the entire Organizing Committee for guiding the entire process of the conference. We are also deeply grateful to all the Program Committee members for their time and efforts in reading, commenting, debating, and finally selecting the papers. We also thank all the external reviewers for assisting the Program Committee in their particular areas of expertise as well as all the authors, participants, and session chairs for their valuable contributions.

Tommy Morris
Kim-Kwang Raymond Choo
Gilbert Peterson
Eric Imsand

Organization

Organizing Committee

General Chairs

Tommy Morris	The University of Alabama in Huntsville, USA
Kim-Kwang Raymond Choo	The University of Texas at San Antonio, USA

Program Committee Chairs

Gilbert L. Peterson	Air Force Institute of Technology, USA
Eric Imsand	The University of Alabama in Huntsville, USA

Program Committee and External Reviewers

Program Committee Members

Cong Pu	Marshall University, USA
Jun Dai	California State University, USA
Ezhil Kalaimannan	University of West Florid, USA
David Dampier	Marshall University, USA
Robin Verma	University of Texas at San Antonio, USA
Jianyi Zhang	Beijing Electronic Science and Technology Institute, China
Patrick Jungwirth	US Army Research Laboratory, USA
Junggab Son	Kennesaw State University, USA
Reza M. Parizi	Kennesaw State University, USA
Jaewoo Lee	University of Georgia, USA
Vahid Heydari	Rowan University, USA
Yifei Wang	Alipay, USA
Wei Zhang	University of Louisville, USA

David Coe	University of Alabama in Huntsville, USA
Junghee Lee	Korea University, South Korea
Huijun Wu	Arizona State University, USA
Ravi Rao	Fairleigh Dickinson University, USA
Rongxing Lu	University of New Brunswick, Canada

External Reviewers

Einaam Alim
Raphael Barata
Pinyao Guo
Hussam Al Hamadi
David Hayes
Erdal Kose
Yaoqing Liu
Zach Tackett
Chunxu Tang
Benjamin Turnbull
Xiaolu Zhang
Shaohua Wang

Contents

Cyber Security Education	
An Integrated System for Connecting Cybersecurity Competency, Student Activities and Career Building	3
Li-Chiou Chen, Andreea Cotoranu, Praviin Mandhare, and Darren Hayes	
Simulating Industrial Control Systems Using Node-RED and Unreal Engine 4	13
Steven Day, William “Kohler” Smallwood, and Joshua Kuhn	
Student Educational Learning Experience Through Cooperative Research	22
Melissa Hannis, Idongesit Mkpong-Ruffin, and Drew Hamilton	
Digital Forensics Education: Challenges and Future Opportunities	28
Megan Stigall and Kim-Kwang Raymond Choo	
Designing a Cybersecurity Curriculum Library: Best Practices from Digital Library Research	47
Blair Taylor, Sidd Kaza, and Melissa Dark	
Design of a Virtual Cybersecurity Escape Room	60
Tania Williams and Omar El-Gayar	
Cyber Security Technology	
A Novel Method for the Automatic Generation of JOP Chain Exploits	77
Bramwell Brizendine and Austin Babcock	
Increasing Log Availability in Unmanned Vehicle Systems	93
Nickolas Carter, Peter Pommer, Duane T. Davis, and Cynthia E. Irvine	

Testing Detection of K-Ary Code Obfuscated by Metamorphic and Polymorphic Techniques 110
George T. Harter and Neil C. Rowe

Enhancing Secure Coding Assistant System with Design by Contract and Programming Logic. 124
Wenhui Liang, Cui Zhang, and Jun Dai

Social Engineering Attacks in Healthcare Systems: A Survey 141
Christopher Nguyen, Walt Williams, Brandon Didlake, Donte Mitchell, James McGinnis, and Dipankar Dasgupta

Identifying Anomalous Industrial-Control-System Network Flow Activity Using Cloud Honeypots. 151
Neil C. Rowe, Thuy D. Nguyen, Jeffery T. Dougherty, Matthew C. Bieker, and Darry Pilkington

Risks of Electric Vehicle Supply Equipment Integration Within Building Energy Management System Environments: A Look at Remote Attack Surface and Implications 163
Roland Varriale, Ryan Crawford, and Michael Jaynes

Author Index. 175