

# **2022 IEEE International Conference on Cyber Security and Resilience (CSR 2022)**

**Virtual Conference  
27 – 29 July 2022**



**IEEE Catalog Number: CFP22Y52-POD**  
**ISBN: 978-1-6654-9953-8**

**Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP22Y52-POD
ISBN (Print-On-Demand):	978-1-6654-9953-8
ISBN (Online):	978-1-6654-9952-1

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com



# Table of Contents

Cover page ..... i

Copyright notice ..... ii

Table of contents ..... iii

Message from the chairs ..... x

Conference sponsors ..... xii

Program committees ..... xiii

Authors’ index ..... xxi

## Cyber Security

Flood control: TCP-SYN flood detection for software-defined networks using OpenFlow port statistics ..... 1  
*T. Das, O. Abuhamdan, S. Sengupta, and E. Arslan*

A stable generative adversarial network architecture for network intrusion detection ..... 9  
*R. Soleymanzadeh and R. Kashef*

LSTM-based anomalous behavior detection in multi-agent reinforcement learning ..... 16  
*C. Lischke, T. Liu, J. Mccalmon, M. Rahman, T. Halabi, and S. Alqahtani*

H4rm0ny: A competitive zero-sum two-player Markov game for multi-agent learning on evasive malware generation and detection ..... 22  
*C. Molloy, S. Ding, B. Fung, and P. Charland*

Ensemble of random and isolation forests for graph-based intrusion detection in containers ..... 30  
*A. Iacovazzi and S. Raza*

On usability of hash fingerprinting for endpoint application identification ..... 38  
*J. Heino, A. Gupta, A. Hakkala, and S. Virtanen*



Data volume reduction for deep packet inspection by multi-layer application determination .....	44
<i>M. Vogel, F. Schuster, F. Kopp, and H. Konig</i>	
Host-based cyber attack pattern identification on honeypot logs using association rule learning .....	50
<i>A. Papoutsis, C. Iliou, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris</i>	
Using CyberScore for network traffic monitoring .....	56
<i>L. Deri and A. Cardigliano</i>	
An approach to improve the robustness of machine learning based intrusion detection system models against the Carlini-Wagner attack .....	62
<i>M. Pujari, B. Cherukuri, A. Javaid, and W. Sun</i>	
Semantic-aware vulnerability detection .....	68
<i>Z. Huang and M. White</i>	
OGMA: Visualisation for software container security analysis and automated remediation .....	76
<i>A. Mills, J. White, and P. Legg</i>	
Configuration vulnerability in SNORT for Windows operating systems .....	82
<i>S. Guarino, M. Grassi, R. Setola, L. Faramondi, and C. Alcaraz</i>	
IPASS: A novel open-source intelligence password scoring system .....	90
<i>J. Hubbard, G. Bendiab, and S. Shiaeles</i>	
Auditing a software-defined cross domain solution architecture .....	96
<i>N. Daughety, M. Pendleton, R. Perez, S. Xu, and J. Franco</i>	
ICT in healthcare: The role of IoT and the SECANT solution .....	104
<i>M. Caballero, D. Kavallieros, A. Spyros, A. Tavernarakis, A. Tziouvaras, S. Bonacina, K. Chandrarmouli, M. Coroiu, L. Chen, T. Dounia, I. Giannoulakis, N. Gligoric, E. Kafetzakis, T. Kasig, V. Koumaras, T. Krousarlis, K. Lapidaki, A. Markakis, S. Marin, M. Manulis, S. Menesidou, S. Nifakos, L. Meng, S. Mhiri, M. Nati, K. Ntafloukas, D. Oniga, D. Papamartzivanos, S. Papastergiou, K. Sanchez, C. Sakkas, K. Stelliou, L. Trujillo, T. Tsikrika, E. Venegas, S. Vrochidis, and D. Xydias</i>	
SENTINEL: Approachable, tailor-made cybersecurity and data protection for small enterprises .....	112
<i>T. Trantidou, G. Bravos, P. Valoggia, I. Skourtis, M. Falelakis, K. Poullos, I. Spais, S. Ioannidis, T. Oudin, R. Costa, C. Konialis, D. Holkham, Z. Kasapi, and A. Karantjias</i>	



A blockchain-based trustworthy cloud services digital ecosystem ..... 118  
*E. Bellini, S. Cimato, A. Esposito, and I. Aversa*

CIDS: Collaborative intrusion detection system using blockchain technology ..... 125  
*G. Gurung, G. Bendiab, M. Shiaeles, and S. Shiaeles*

Blockchain-enabled digital forensics for the IoT: Challenges, features, and current frameworks ..... 131  
*S. Brotsis and N. Kolokotronis*

Android device incident response: Viber analysis ..... 138  
*A. Vasilaras, D. Dosis, M. Kotsis, and P. Rizomiliotis*

SeeShells: An optimized solution for utilizing shellbags in a digital forensic investigation ..... 143  
*E. Amoruso, R. Leinecker, and C. Zou*

Evaluating perceptual hashing algorithms in detecting image manipulation over social media platforms ..... 149  
*M. Alkhowaiter, K. Almubarak, and C. Zou*

On the (in)security of memory protection units ..... 157  
*M. Grisafi, M. Ammar, and B. Crispo*

ETHERLED: Sending covert morse signals from air-gapped devices via network card (NIC) leds ..... 163  
*M. Guri*

How to build a SOC on a budget ..... 171  
*R. Vaarandi and S. Mases*

## Cyber Resilience

SoK: Demystifying cyber resilience quantification in cyber-physical systems ..... 178  
*H. Lee, S. Kim, and H. K. Kim*

An approach to address risk management challenges focused on IT governance framework ..... 184  
*H. Alessa, R. Boodai, and A. Alanazi*

CoReTM: An approach enabling cross-functional collaborative threat modeling ..... 189  
*J. Von der Assen, M. Figueredo Franco, and C. Killer*



Enhancing the aggregation of the federated learning for the industrial cyber physical systems ..... 197  
*S. Guendouzi, S. Ouchani, and M. Malki*

Improving resilience in cyber-physical systems based on transfer learning ..... 203  
*M. Saman Azari, F. Flammini, and S. Santini*

## Cyber Physical Systems Security

ML-based anomaly detection system for DER DNP3 communication in smart grid ..... 209  
*M. Abdelkhalek and M. Govindarasu*

Moving target defense routing for SDN-enabled smart grid ..... 215  
*M. Abdelkhalek, B. Hyder, M. Govindarasu, and C. Rieger*

Neural network based temporal point processes for attack detection in industrial control systems ..... 221  
*G. Fortino, C. Greco, A. Guzzo, and M. Ianni*

Control logic obfuscation attack in industrial control systems ..... 227  
*N. Zubair, A. Ayub, H. Yoo, and I. Ahmed*

ML-based anomaly detection for intra-vehicular CAN-bus networks ..... 233  
*S. Purohit and M. Govindarasu*

Powertrace-based fuzzing of CAN connected hardware ..... 239  
*M. Dunne and S. Fischmeister*

A comparative overview of automotive radar spoofing countermeasures ..... 245  
*M. Vu, W. Headley, and K. Heaslip*

BLEND: Efficient and blended IoT data storage and communication with application layer security ..... 253  
*J. Hoglund and S. Raza*

Modelling and assessing the risk of cascading effects with ResilBlockly ..... 261  
*I. Bicchierai, E. Schiavone, and F. Brancati*



## CSR WS Actionable Cyber Threat Intelligence

Towards continuous enrichment of cyber threat intelligence: A study on a honeypot dataset ..... 267  
*A. Spyros, A. Papoutsis, I. Koritsas, N. Mengidis, C. Iliou, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris*

Combining text analysis techniques with unsupervised machine learning methodologies for improved software vulnerability management ..... 273  
*M. Anastasiadis, G. Aivatoglou, G. Spanos, A. Voulgaridis, and K. Votis*

## CSR WS Cyber Resilience and Economics

Policy-based profiles for intrusion response systems ..... 279  
*K. Hughes*

Using potential effects on threat events (PETE) to assess mitigation effectiveness and return on investment (ROI) ..... 287  
*D. Bodeau, R. Graubart, and R. Mcquaid*

Process mining for asymmetric cybersecurity audit ..... 293  
*R. Turner*

## CSR WS Cyber Ranges and Security Training

Leveraging cyber ranges for prototyping, certification and training: The ECHO case ..... 299  
*N. Mengidis, M. Bozhilova, C. Ceresola, C. Colabuono, M. Cooke, G. Depaix, A. Genchev, G. Koykov, W. Mees, M. Merialdo, A. Voulgaridis, T. Tsikrika, K. Votis, and S. Vrochidis*

Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain ..... 305  
*M. Antonopoulos, G. Drainakis, E. Ouzounoglou, G. Papavassiliou, and A. Amditis*



## CSR WS Data Science for Cyber Security

Employing social network analysis to dark web communities .....	311
<i>S. Nikoletos and P. Raftopoulou</i>	
Phishing detection using machine learning algorithm .....	317
<i>J. Tanimu and S. Shiaeles</i>	
Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor .....	323
<i>M. Hirano and R. Kobayashi</i>	
A Bayesian model combination based approach to active malware analysis .....	331
<i>A. Hota and J. Schonwalder</i>	
A comprehensive API call analysis for detecting Windows-based ransomware .....	337
<i>P. Mohan Anand, P. V. Sai Charan, and S. K. Shukla</i>	

## CSR WS Electrical Power and Energy Systems Security, Privacy and Resilience

Protecting IEC 60870-5-104 ICS/SCADA systems with honeypots .....	345
<i>E. Grigoriou, A. Liatifis, P. Radoglou-Grammatikis, T. Lagkas, I. Moscholios, E. Markakis, and P. Sarigiannidis</i>	
Risk analysis of DNP3 attacks .....	351
<i>V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. Markakis, and P. Sarigiannidis</i>	
Privacy preserving human activity recognition using microaggregated generative deep learning .....	357
<i>A. Aleroud, M. Shariah, and R. Malkawi</i>	
Current drainage induced by bias injection attack against Kalman filter of BLDC motor .....	364
<i>Y. Boiko, I. Kiringa, and T. Yeap</i>	

## CSR WS Maritime Cyber Security

A multi-level trust framework for the Internet of underwater things .....	370
<i>A. Almutairi, Y. He, and S. Furnell</i>	





FFDA: A novel four-factor distributed authentication mechanism .....	376
<i>J. Edwards, F. Aparicio-Navarro, L. Maglaras, and C. Douligeris</i>	
A supply chain service cybersecurity certification scheme based on the cybersecurity act .....	382
<i>A. Michota and N. Polemi</i>	
Training the maritime security operations centre teams .....	388
<i>M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo</i>	
Cybersecurity at merchant shipping .....	394
<i>E. D. Charitos, N. A. Kounalakis, and I. Kantzavelou</i>	