2023 IEEE International Conference on Cyber Security and Resilience (CSR 2023)

Venice, Italy
31 July – 2 August 2023

IEEE Catalog Number: CFP23Y52-POD
ISBN: 979-8-3503-1171-6

Copyright © 2023 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:	CFP23Y52-POD
ISBN (Print-On-Demand):	979-8-3503-1171-6
ISBN (Online):	979-8-3503-1170-9

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
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings.com

Table of Contents

Cover page i

Table of contents iii

Message from the chairs xiii

Conference sponsors xv

Program committees xvii

Authors' index xxv

Cyber Security

Comparative analysis of pattern mining algorithms for event logs 1
O. Gasimov, R. Vaarandi, and M. Pihelgas

To TTP or not to TTP?: Exploiting TTPs to improve ML-based malware detection 8
Y. Sharma, E. Giunchiglia, S. Birnbach, and I. Martinovic

stealthML: Data-driven malware for stealthy data exfiltration 16
K. Chung, P. Cao, Z. Kalbarczyk, and R. Iyer

Explaining binary obfuscation 22
C. Greco, M. Ianni, A. Guzzo, and G. Fortino

New version, new answer: Investigating cybersecurity static-analysis tool findings 28
A. M. Reinhold, T. Weber, C. Lemak, D. Reimanis, C. Izurieta

Qerberos: A protocol for secure distribution of QRNG keys 36
D. Soler, C. Dafonte, M. Fernandez-Veiga, A. Fernandez, F. Novoa, and R. Diaz-Redondo

Efficiency of malware detection based on DNS packet analysis over real network traffic 42
L. Principi, M. Baldi, A. Cucchiarelli, and L. Spalazzi

A cost-efficient threat intelligence platform powered by crowdsourced OSINT 48
A. Daou, F. Li, and S. Shiaeles

A driver detection method by means of explainable deep learning 54
F. Martinelli, F. Mercaldo, and A. Santone

Optimizing AI for mobile malware detection by self-built-dataset GAN oversampling and LGBM 60
O. Dayan, L. Wolf, F. Wang, and Y. Harel

Cream skimming the underground: Identifying relevant information points from online forums 66
F. Moreno-Vera, M. Nogueira, C. Figueiredo, D. Menasché, M. Bicudo, A. Woiwood, E. Lovat, A. Kocheturov, and L. Pfleger de Aguiar

Anomaly-based intrusion detection in IIoT networks using transformer models 72
J. Casajus-Setien, C. Bielza, and P. Larrañaga

Key update for the IoT security standard OSCORE 78
R. Hoglund, M. Tiloca, S. Bouget, and S. Raza

A multi-class intrusion detection system based on continual learning 86
C. Oikonomou, I. Iliopoulos, D. Ioannidis, and D. Tzovaras

Blockchain-based trustworthy O2O interaction in the next 6G ecosystem 92
E. Bellini, E. Damiani, and S. Marrone

A recipe for cost-effective secure IoT: The Safe Place project case study 99
F. Palmarini, L. Veronese, M. Busi, R. Focardi, and F. Luccio

VulDetect: A novel technique for detecting software vulnerabilities using language models 105
O. Marwan and S. Shiaeles

Understanding human factors of cybersecurity: Drivers of insider threats 111
M. Green and P. Dozier

DDoS attack detection in a real urban IoT environment using federated deep learning 117
K. Ahmadi and R. Javidan

Moving target defense strategy selection against malware in resource-constrained devices 123
J. von der Assen, A. Huertas Celdran, N. Huber, G. Bovet, G. Martinez Perez, and B. Stiller

HSchain: Anonymous permissioned blockchain with enhanced auditability 130
J. Hou, L. Xu, L. Zhu, P. Jiang, and S. Song

Real-time APT detection technologies: A literature review 136
S. Mönch and H. Roth

Hunting IoT cyberattacks with AI-powered intrusion detection 142
S. Grigoriadou, P. Radoglou-Grammatikis, I. Makris, T. Lagkas, V. Argyriou, A. Lytos, E. Fountoukidis, and P. Sarigiannidis

BTV2P: Blockchain-based trust model for secure vehicles and pedestrians networks 148
M. Chelghoum, G. Bendiab, M. Benmohammed, S. Shiaeles, and E. Bellini

Efficient early anomaly detection of network security attacks using deep learning 154
T. Ahmad and D. Truscan

An explainable artificial intelligence approach for a trustworthy spam detection 160
A. Ibrahim, M. Mejri, and F. Jaafar

Assessing cybersecurity hygiene and cyber threats awareness in the campus – A case study of higher education institutions in Portugal and Poland 168
L. Oliveira, A. Chmielewski, P. Rutecka, K. Cicha, M. Rizun, N. Torres, and P. Pinto

Multi-party computation for privacy and security in machine learning: A practical review 174
A. Bellini, E. Bellini, M. Bertini, D. Almhaithawi, and S. Cuomo

Federated learning-based credit card fraud detection: Performance analysis with sampling methods and deep learning algorithms 180
N. F. Aurna, M. Hossain, Y. Taenaka, and Y. Kadobayashi

Early detection of reconnaissance attacks on IoT devices by analyzing performance and traffic characteristics 187
P. Keshavamurthy and S. Kulkarni

Cyber incident scenarios in the maritime industry: Risk assessment and mitigation strategies 194
M. Ben Farah, O. Al-Kadri, Y. Ahmed, R. Abozariba, and X. Bellekens

A taxonomic survey of model extraction attacks 200
D. Genç, M. Özuysal, and E. Tomur

Phishing and smishing detection using machine learning 206
H. El Karhani, R. Al Jamal, Y. Bou Samra, I. Elhajj, and A. Kayssi

Evaluation of applying LDA to redacted documents in security and safety analysis 212
K. Umezawa, S. Wohlgemuth, K. Hasegawa, and K. Takaragi

Denial of service attack detection via differential analysis of generalized entropy progressions 219
O. Subasi, J. Manzano, and K. Barker

Ransomware detection based on network behavior using machine learning and hidden Markov model with Gaussian emission 227
A. Srivastava, N. Kumar, A. Handa, and S. K. Shukla

A taxonomy for tsunami security scanner plugins 234
G. Lima, V. Gonçalves, and P. Pinto

ML and network traces to M.A.R.S. 240
W. Cruz, L. Michel, B. Drozdenko, and S. Roodbeen

Deepfake detection with deep learning: Convolutional neural networks versus transformers 246
V. Thing

A survey of attacks and defenses for deep neural networks 254
D. Machooka, X. Yuan, and A. Esterline

Mitigating membership inference attacks in machine learning as a service 262
M. Bouhaddi and K. Adi

Attacking a packet analyzer: Caronte case study 269
D. Granata, M. Rak, and F. Grimaldi

Exposed: Critical vulnerabilities in USSD banking authentication protocols 275
Z. Lamoyero and O. Fajana

Cyber Resilience

SoK: Static configuration analysis in infrastructure as code scripts 281
P. R. R. Konala, V. Kumar, and D. Bainbridge

Detecting internal reconnaissance behavior through classification of command collections 289
L. Vandenberghe, H. M. Koduvely, and M. Pospelova

Understanding resilience: Looking at frameworks & standards – A systematic study from cyber perspective 295
N. Laxman, D. Krohmer, M. Damm, R. Schwarz, and P. O. Antonino

Merging model-based and data-driven approaches for resilient systems digital twins design 301
L. Campanile, M. S. De Biase, R. De Fazio, M. Di Giovanni, F. Marulli, and L. Verde

A semi-automatic approach for enhancing the quality of automatically generated inventories 307
S. Bonomi, M. Cuoci, and S. Lenti

Cyber threat hunting using unsupervised federated learning and adversary emulation 315
S. Sheikhi and P. Kostakos

Automated patch management: An empirical evaluation study 321
V. Ahmadi Mehri, P. Arlos, and E. Casalicchio

Towards automated cyber range design: Characterizing and matching demands to supplies 329
E. Ear, J. Remy, and S. Xu

Nudge to promote employees' information security compliance behavior: A field study 335
M. Inaba and T. Terada

Cyber Physical Systems Security

Formal verification of a V2X privacy preserving scheme using Proverif 341
S. Bussa, F. Valenza, and R. Sisto

A game of age of incorrect information against an adversary injecting false data 347
L. Badia, V. Bonagura, S. Panzieri, and F. Pascucci

Proactive measures for cyber-physical systems cybersecurity 353
K. Taha

Enhancing cyber-resilience in self-healing cyber-physical systems with implicit guarantees 359
R. Loh and V. Thing

Detecting subspace malicious vectors attack against smart grid using sequence-alignment method 367
K. Alotaibi, R. Rob, D. Nour, and D. Zamzami

Small satellite system modeling for vulnerability analysis 373
K. Murbach, T. Morris, F. Wiersig, and J. Golden

SPAT: A testbed for automotive cybersecurity training 381
R. Caviglia, G. B. Gaggero, M. Marchese, N. Vincis, A. Aceti, and O. Morando

Enhancing industrial cyber-physical systems security with smart probing approach 387
V. Bonagura, C. Foglietta, S. Panzieri, and F. Pascucci

Control-implications-based side-channel monitoring for embedded systems 394
S. Roy and B. Drozdenko

Identification of vulnerable IoT enabled transportation infrastructure into a cyber-physical transportation network 400
K. Ntafloukas, L. Pasquale, B. M. Pastor, and D. McCrum

Default credentials vulnerability: The case study of exposed IP cams 406
S. Perone, L. Faramondi, and R. Setola

Evaluating machine learning approaches for cyber and physical anomalies in SCADA systems 412
S. Guarino, L. Faramondi, R. Setola, and F. Flammini

Evaluating a process-aware IDS for smart grids on distributed hardware 418
V. Menzel, K. O. Großhanten, and A. Remke

A feature-aware semi-supervised learning approach for automotive ethernet 426
K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, and Y. Kadobayashi

Trojan triggers for poisoning unmanned aerial vehicles navigation: A deep learning approach 432
M. Mynuddin, S. U. Khan, and M. N. Mahmoud

Trustworthiness-related risks in autonomous cyber-physical production systems – A survey 440
M. Zahid, F. Flammini, and A. Bucaioni

IoT forensics: Analysis of Ajax systems' mobile app for the end user 446
E. Dragonas and C. Lambrinoudakis

IoT forensics: Investigating the mobile app of Dahua technology 452
E. Dragonas, C. Lambrinoudakis, and M. Kotsis

CSR WS Cyber Resilience and Economics

Cyber resilience, societal situational awareness for SME 458
R. van Kranenburg and R. Bohara

Continuous security assurance of modern supply-chain ecosystems with application in autonomous driving 464
G. Hatzivasilis, S. Ioannidis, G. Kalogiannis, M. Chatzimpyrros, G. Spanoudakis, G. Jiménez Prieto, A. Rojas Morgan, M. Juaniz Lopez, B. Cataldo, and J. F. Ruiz

Verified value chains, innovation and competition 470
A. Weber, S. Guilley, R. Rathfelder, M. Stoettinger, T. Grawunder, C. Lueth, M. Malenko, S. Reith, A. Puccetti, J.-P. Seifert, N. Herfurth, G. Heiser, and H. Sankowski

CSR WS Data Science for Cyber Security

Improving the detection of unknown DDoS attacks through continual learning 477
B. Nugraha, K. Yadav, P. Patil, and T. Bauschert

RoG: A pipeline for automated sensitive data identification and anonymisation 484
S. Nikoletos, S. Vlachos, E. Zaragkas, C. Vassilakis, C. Tryfonopoulos, and P. Raftopoulou

Reviewing BPMN as a modeling notation for CACAO security playbooks 490
M. Zych, V. Mavroeidis, K. Fysarakis, and M. Athanatos

Minimizing software-rooted risk through library implementation selection 496
P. Sotiropoulos, C.-M. Mathas, C. Vassilakis, and N. Kolokotronis

Learning when to say goodbye: What should be the shelf life of an indicator of compromise? 503
B. Tostes, L. Ventura, E. Lovat, M. Martins, and D. Menasché

CSR WS Dependability and Resilience in Digital Cultural Heritage Ecosystems

An open sharing method for digital heritage assets based on self-sovereign identity technology 511
J. Zhu and Z. Wu

Metadata and semantic annotation of digital heritage assets: A case study 516
A. Amato, S. Venticinque, G. Renda, S. Mataluna, and D. Branco

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

Modelling and analysing security threats targeting protective relay operations in digital substations 523
M. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael

Threat intelligence using digital twin honeypots in cybersecurity 530
M. Nintsiou, E. Grigoriou, P.-A. Karypidis, T. Saoulidis, E. Fountoukidis, and P. Sarigiannidis

PHOENI2X – A European cyber resilience framework with artificial-intelligence-assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange 538
K. Fysarakis, A. Lekidis, V. Mavroeidis, K. Lampropoulos, G. Lyberopoulos, I. Garcia-Milà Vidal, J. C. Terés i Casals, E. Rodriguez Luna, A. A. Moreno Sancho, A. Mavrelos, M. Tsantekidis, S. Pape, A. Chatzopoulou, C. Nanou, G. Drivas, V. Photiou, G. Spanoudakis, and O. Koufopavlou

Towards a hybrid blockchain-based energy trading market for microgrids 546
P. Savvidis, N. Vakakis, A. Voulgaridis, E. Bellini, D. Ioannidis, K. Votis, and D. Tzovaras

CSR WS Hardware Cybersecurity Systems

Area-delay efficient security scheme for smart hospital systems 552
K. Tsantikidou, D. Boufeas, and N. Sklavos

A PUF based on the non-linearity of memristors 558
C. Aitchison

Breaking AES-128: Machine learning-based SCA under different scenarios and devices 564
S. Tehranipoor, N. Karimian, and J. Edmonds

A new fast and side-channel resistant AES hardware architecture 572
M. Macchetti, H. Pelletier, and C. Groux

Randomized addressing countermeasures are inefficient against address-bit SCA 580
I. Kabin, Z. Dyka, and P. Langendoerfer

Counteracting modeling attacks using hardware-based dynamic physical unclonable function 586
J. Dofe and S. Rajput

Algorithm for simplifying the SHA-256 operations tree 592
A. Levina and A. Plotnikov

CSR WS Privacy-Preserving Data Processing and Analysis

A practical and scalable privacy-preserving framework 598
S. D'Antonio, N. Avgerinos, I. Kamara, C. Kotselidis, I. Lazarou, T. Mannarino, G. Meditskos, K. Papachristopoulou, A. Papoutsis, and P. Roccetti

Introducing the TRUMPET project: Trustworthy multi-site privacy enhancing technologies 604
A. Pedrouzo-Ulloa, J. Ramon, F. Pérez-González, S. Lilova, P. Duflot, Z. Chihani, N. Gentili, P. Ulivi, M. A. Hoque, T. Mukammel, Z. Pritzker, A. Lemesle, J. Loureiro-Acuña, X. Martínez, and G. Jiménez-Balsa

Practical multi-key homomorphic encryption for more flexible and efficient secure federated average aggregation 612
A. Pedrouzo-Ulloa, A. Boudguiga, O. Chakraborty, R. Sirdey, O. Stan, and M. Zuber

Comparison of machine learning models applied on anonymized data with different techniques 618
J. Sainz-Pardo Diaz and A. Lopez Garcia

Privacy-preserving federated learning system for fatigue detection 624
M. Mohammadi, R. Allocca, D. Eklund, R. Shrestha, and S. Sinaei

FedGA-Meta: Federated learning framework using genetic algorithms and meta-learning for aggregation in industrial cyber-physical systems 630
B. S. Guendouzi, S. Ouchani, H. Al Assaad, and M. El Zaher Jradi

How to secure the IoT-based surveillance systems in an ELEGANT way 636
A. Pawlicka, D. Puchalski, M. Pawlicki, R. Kozik, and M. Choraś

The alliance of HE and TEE to enhance their performance and security 641
S. D'Antonio, G. Lazarou, G. Mazzeo, O. Stan, M. Zuber, and I. Tsavdaridis

Detection of radio frequency interference in satellite ground segments 648
F. Uccello, L. Coppolino, S. D'Antonio, A. Lyratzis, C. Bakalis, S. Touloumtzi, and I. Papoutsis

Comparison of machine learning algorithms trained under differential privacy for intrusion detection systems 654
I. Siachos, K. Kaltakis, K. Papachristopoulou, I. Giannoulakis, and E. Kafetzakis