

2025 IEEE International Conference on Cyber Security and Resilience (CSR 2025)

**Chania, Crete, Greece
4-6 August 2025**

Pages 1-569



**IEEE Catalog Number: CFP25Y52-POD
ISBN: 979-8-3315-3592-6**

**Copyright © 2025 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:	CFP25Y52-POD
ISBN (Print-On-Demand):	979-8-3315-3592-6
ISBN (Online):	979-8-3315-3591-9

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

Table of contents iii

Message from the chairs xx

Conference sponsors xxii

Program committees xxiii

Authors’ index xxxviii

Cyber security

SafetilBERT: An efficient and explained LLM for IoMT attacks classification 1
M. Niang, H. Nakouri, and F. Jaafar

Reimagining the usermode process space by utilizing hardware-enforced sub-process isolation..... 9
M. Nelson and M. Mirakhorli

Evasion of deep learning malware detection via adversarial selective obfuscation 17
C. Greco, M. Ianni, A. Guzzo, and G. Fortino

DP-Tabula: Differentially private synthetic tabular data generation with large language models..... 23
W. Niu, Z. Zhang, A. Huertas, C. Feng, J. Von Der Assen, N. Nezhadsistani, and B. Stiller

A machine learning approach to automate greybox testing..... 29
A. Hijazi, D. Mezher, E. Zeidan, and C. Bassil



Offloading key switching on GPUs: A path towards seamless acceleration of FHE.....	36
O. Papadakis, M. Papadimitriou, A. Stratikopoulos, M. Xekalaki, J. Fumero, and C. Kotselidis	
Towards DoS attack detection for IoT systems: A cross-layer oriented approach based on machine learning techniques.....	42
D. Tasiopoulos, A. Xenakis, A. Lekidis, D. Kosmanos, C. Chaikalis, and V. Vlachos	
Audio-deepfake: Generation methods, legitimate applications and the potential for misuse	50
G. Bendiab, K. Zelti, M. Bader El Den, and S. Shiaeles	
Enhancing deep learning based IDS adversarial robustness with causal inference.....	57
M. François, P. E. Arduin, and M. Merad	
Defending against beta poisoning attacks in machine learning models	63
N. Gulciftci and M. E. Gursoy	
Reducing human-induced label bias in SMS spam with context-enhanced clustering (CEC).....	71
G. Shu Fuhnwi, A. M. Reinhold, and C. Izurieta	
A novel GNN-based approach for detection of prompt injection attacks	77
G. Jadhav, A. K. Singh, Z. Khanam, and R. Hercock	
Enhancing cyber threat intelligence sharing through data spaces in critical infrastructures.....	83
M. Akbari Gurabi, Ö. Sen, N. Rahimidanesh, A. Ulbig, and S. Decker	
Explainable ransomware detection through static analysis and machine learning.....	91
G. Ciaramella, F. Martinelli, A. Santone, and F. Mercaldo	
Space cyber risk management: Desired properties.....	99
E. Ear, B. Bailey, and S. Xu	
Machine-learning anomaly detection for early identification of DDOS in smart home IoT devices	105
R. Lamptey, M. Saedi, and V. Stankovic	
LDP3: An extensible and multi-threaded toolkit for local differential privacy protocols and post-processing methods.....	111
B. K. Balioglu, A. Khodaie, and M. E. Gursoy	
Efficient and privacy-preserving authentication using verifiable credentials	119
A. Badirova, S. D. Varnosfaderani, and R. Yahyapour	



Evasive ransomware attacks using low-level behavioral adversarial examples.....	125
M. Hirano and R. Kobayashi	
Integrating cyber threat intelligence into threat modeling for autonomous ships using PASTA and MISP.....	133
M. Erbas, J. Vanharanta, J. Paavola, L. Tsiopoulos, and R. Vaarandi	
Budget-conscious differentially private aggregation of power data timeseries.....	140
F. Kserawi and G. Ghinita	
Technological framework for secure and resilient food supply chain.....	146
M. Fischer, R. Tönjes, R. Bohara, M. Ross, A. Hegde, C. Wressnegger, and M. Brunner	
Classification of software vulnerability artifacts using public Internet data	153
L. Ambrus De Lima, E. Rabello Ussler, M. A. Santos Bicudo, D. Sadoc Menasché, A. Kocheturov, and G. Srivastava	
PCIe monitoring for secure code execution in heterogeneous system architectures.....	159
I. Georgakas, E. Papadogiannaki, K. Georgopoulos, and S. Ioannidis	
Abstract attack intention inference using low-rank gated arithmetic interactive attention	166
W. Yang, M. Wang, and D. Wojtczak	
A reinforcement learning approach to multi-parametric input mutation for fuzzing	174
M. L. Uwibambe, A. Tyagi, and Q. Li	
The notional risk scores approach to space cyber risk management.....	180
E. Ear, B. Bailey, and S. Xu	
Optimized security measure selection: Leveraging MILP solvers to balance risk and cost	186
P. Saha Fobougong, M. Mejri, and K. Adi	
Large scale cyber security log classification using semi-supervised clustering.....	194
P. Cai, M. Lazarescu, S. T. Soh, and R. Ryan	
Security vulnerabilities in AI-generated JavaScript: A comparative study of large language models	200
D. Aydın and Ş. Bahtiyar	
Contrastive self-supervised network intrusion detection using augmented negative pairs	206
J. Wilkie, H. Hindy, C. Tachtatzis, and R. Atkinson	
Design and implementation of a tool to improve error reporting for eBPF code.....	214
R. Rizza, R. Sisto, and F. Valenza	



FE4MQTT - Using functional encryption to improve the privacy in publish-subscribe communication schemes.....220
M. Fischer and R. Tönjes

Metamorphic relation prediction for security vulnerability testing of online banking applications.....226
K. Rahman, A. M. Reinhold, and C. Izurieta

A collusion-resistant DECO-based attestation protocol for practical applications234
U. Şen, M. Osmanoğlu, and A. A. Selçuk

An efficient methodology for real-time risk and impact assessment in 5G networks.....240
D. Varvarigou, K. Lampropoulos, O. Koufopavlou, S. Denazis, and P. Kitsos

Adaptive weighted ensemble learning for intrusion detection in industrial IoT and edge computing248
S. Ruiz Villafranca, L. M. Garcia Sáez, J. Roldán Gómez, J. Carrillo Mondéjar, J. M. Castelo Gómez, and J. L. Martínez

CONSENTIS - An innovative framework for identity and consent management for EU digital and data strategies.....254
N. Kyriakoulis, C. Dimopoulos, G. Daniil, K. Lampropoulos, V. Prevelakis, P. Karantzias, A. B. Popescu, A. Fuentes Exposito, N. Nikolaou, S. Papastergiou, G. Alexandris, M. Tasouli, G. Karavias, E. Kosta, and O. Mihaila

MiniLib: A flow analysis-based approach for attack surface reduction through software debloating260
L. Kopanias, P. Sotiropoulos, N. Kolokotronis, and C. Vassilakis

RuleXploit: A framework for generating suricata rules from exploits using generative AI267
A. Papoutsis, A. Dimitriadis, I. Koritsas, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris

C2-based malware detection through network analysis using machine learning275
M. Martijan, V. Krinickij, and L. Bukauskas

A Bayesian–Markov framework for proactive and dynamic cyber risk assessment driven by EPSS281
P. Cheimonidis and K. Rantos

From one network to another: Transfer learning for IoT malware detection287
K. Bosinaki, D. Natsos, G. Siachamis, and A. L. Symeonidis



Post-quantum security evaluation of aeronautical communications	295
K. Spalas and N. Kolokotronis	
Trusted identity authentication for digital scholarship participants based on verifiable credential.....	302
X. Wu, Z. Wu, and H. Li	
HyperDtct: Hypervisor-based ransomware detection using system calls.....	308
J. Von Der Assen, A. Huertas Celdran, J. M. Lüthi, J. M. Jorquera Valero, F. Enguix, G. Bovet, and B. Stiller	
Using topic modeling and LLMs to recommend CAPEC attack patterns: A comparative study.....	314
U. Moore, X. Yuan, and H. Moradi	
A multi-level user identity authentication scheme based on environmental detection	320
N. Zeeshan, L. L. Spada, and M. Bakyt	
A comprehensive 5G dataset for control and data plane security and resource management.....	326
B. Nugraha, M. Hajizadeh, T. Niehoff, A. Venkatesh Jnanashree, T. V. Phan, D. Triantafyllopoulou, O. Krause, M. Mieth, K. Moessner, and T. Bauschert	
CTI-GEN: A framework for generating STIX 2.1 compliant CTI using generative AI	334
A. Papoutsis, A. Dimitriadis, D. Kavallieros, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, and G. Meditskos	
Practical confidential data cleaning using trusted execution environments	342
A. Basu, M. Yoshino, and M. Toba	
Scalable and adaptive security framework for the IoT-edge-cloud continuum.....	350
S. Cuñat Negueroles, I. Makropodis, L. Cabanillas Rodriguez, C. Xenakis, I. Chouchoulis, C. Palau, and I. Lacalle	
PASTA threat modeling for cyber resilience and COLREG compliance in autonomous ship systems	358
M. Erbas, G. Visky, O. Maennel, L. Tsiopoulos, and R. Vaarandi	
ResViT: A hybrid model for robust deepfake video detection.....	366
A. Aria, S. L. Mirtaheri, S. A. Asghari, R. Shahbazian, and A. Pugliese	
eIDPS: A comprehensive comparative analysis of packet-level and flow-level intrusion detection and prevention.....	372
S. Kostopoulos, D. Papatsaroucha, I. Kefaloukos, and E. K. Markakis	



Cyber resilience

An AI-powered pipeline for enabling self-healing in software systems 379
G. Siachamis, G. Papadopoulos, and A. Symeonidis

Designing AI systems with correction mechanisms towards attack-resilient architectures 387
E. Kafali, C. N. Spartalis, T. Semertzidis, C. Z. Patrikakis, and P. Daras

Accounting for the impact of real-world data and costs in autonomous cyber defence..... 393
A. Neal, A. Acuto, P. Green, C. Lear, N. Hare, and S. Maskell

A lightweight firmware resilience engine for real-time operating systems..... 401
U. Budak, F. De Santis, O. Yasar, M. Safieh, and G. Sigl

Adapt-LFA: Adaptive gradient-guided label flipping attack against federated learning-based intrusion detection in IoT 407
H. Rezaei, R. Taheri, I. Jordanov, and S. Shiaeles

A structured process for scenario-based gamification of cyber threat intelligence for space system security..... 413
M. Kriesten, M. Thinyane, and D. Ormrod

ReLATE: Resilient learner selection for multivariate time-series classification against adversarial attacks..... 419
C. I. Kocal, O. Gungor, A. Tartz, T. Rosing, and B. Aksanli

Mapping of maritime ecosystem components in the cybersecurity landscape..... 425
E. Roponena, S. Lielbārde, E. Citskovska, A. Brilingaitė, L. Bukauskas, and R. Pirta

A novel MQTT-ZT secure broker: Zero trust architecture for IoT security..... 433
M. James, T. Newe, D. O'Shea, and G. D. O'Mahony

Cybersecurity mesh architecture for electric vehicle charging infrastructure 440
R. Bohara, M. Ross, and O. Joglekar

Optimizing network services with quantum dynamic programming and Grover’s search 447
E. Zeydan, J. Manges Bafalluy, Y. Turk, A. Aydeger, and M. Liyanage

Informed defense: How attacker profiles transform vulnerability assessments 453
M. Z. Naseer, V. Fodor, and M. Ekstedt

Sunburst vapor - A cybersecurity prompted case study of national-scale organizational transformation..... 461
E. Moore, S. Fulton, T. Amador, R. Mancuso, I. Martinez, and D. Likarish



Machine learning model complexity as a mitigation strategy against industrial espionage through membership inference attacks469
R. Dautov, H. Song, C. Schaefer, S. Kim, and V. Pietsch

Composite product cybersecurity certification using explainable AI based dynamic risk assessment.....476
N. Basheer, S. Islam, S. Papastergiou, and E. Maria Kalogeraki

An approach for a supporting multi-LLM system for automated certification based on the German IT-Grundschutz.....482
L. Muth and M. Margraf

A preliminary ontology for 5G network resilience: Hybrid threats, risk reduction, compliance.....490
R. A. Paskauskas

Using legends into AI-based business decision making: Embedding ethics, cybersecurity and resilience498
G. Sargsyan and E. Damiani

Cyber resilience strategies throughout the system development lifecycle504
G. Deffenbaugh and S. Kameneni

A proposal for an ontology to enhance IT architecture resilience.....510
B. Mbaye, M. Mejri, and P. Saha Fobougong

FAIR: Facilitating artificial intelligence resilience in manufacturing industrial Internet518
Y. Zeng, I. Lourentzou, X. Deng, and R. Jin

Development of an SDN-based space system simulation framework for intrusion detection.....524
U. Uhongora, M. Thinyane, and Y. W. Law

Cyber physical systems security

Anomaly identification in power systems using dynamic state estimation and deep learning530
F. Alsaeed, E. Abukhousa, S. S. F. Syed Afroz, A. Qwbaiban, and A. S. Meliopoulos

Driving resilience: Assessing security incidents' criticality in autonomous vehicles537
Y. Qendah and S. Katzenbeisser



A lightweight IDS framework using FPGA-based hardware fingerprinting on Zynq SoC	544
A. W. Mohammed, A. Ali, H. Arif, F. R. P. Mohammed, and H. Malik	
DFA: Dynamic frame alteration for video manipulation attack in IoT environments	550
B. C. Nchelem, A. K. Singh, and H. Mouratidis	
Fault tolerance vs. attack detection in industrial control systems: A deep learning approach.....	556
H. Mehrpouyan	
Security risk analysis of logistical support solutions for MaaS and DLT-based mitigations	562
G. Kisa Isik, A. Eker, T. Tryfonas, and G. Oikonomou	
CAN-MAID: An intrusion detection protocol for CAN bus	570
K. Marquis and J. Chandy	
Application and evaluation of a substation threat modeling language for automatic attack graph generation	578
E. Rencelj Ling and M. Ekstedt	
TPKey: Using TPMS signals for secure and usable intra-vehicle device authentication.....	586
O. Achkar, L. Nissen, S. Raza, R. Shirsat, N. Klingensmith, G. Zouridakis, and K. I. Lee	
Not-so-secret authentication: The SyncBleed attacks and defenses for zero-involvement authentication systems	592
I. Ahlgren, R. Shirsat, O. Achkar, G. K. Thiruvathukal, K. I. Lee, and N. Klingensmith	
Ontology-driven threat modeling analysis of CPSs.....	600
M. Kordi and N. Maunero	
Vulnerability assessment combining CVSS temporal metrics and Bayesian networks	606
S. Perone, S. Guarino, L. Faramondi, and R. Setola	
Securing DRL-based traffic signal control against experience replay manipulation attacks	612
M. Bouhaddi	
ThreatSpider: CTI-driven semi-automated threat modelling for cybersecurity certification	619
A. Amro and G. Kavallieratos	
Cybersecurity-oriented digital twins: A double-edged sword or a game changer?.....	626
S. Abdullahi and S. Lazarova Molnar	



Towards safety and security testing of cyberphysical power systems by shape validation	632
A. Geiger, I. Hacker, Ö. Sen, and A. Ulbig	
Evaluating smart home privacy: The relationship between encrypted sensor data and occupancy prediction through machine learning	638
S. Mohanty, D. Papadopoulos, and C. Schindelbauer	
Strategic interactions in multi-sensor networks against false data injection	646
V. Bonagura, C. Foglietta, S. Panzieri, F. Pascucci, and L. Badia	
Lessons learned from a cybersecurity risk assessment of OpenADR in smart grid planning	652
G. Erdogan, A. Omerovic, E. Solvang, A. Killingberg, A. Kvinnesland, and I. Abrahamsen	
Post-quantum cryptography for maritime systems	660
D. Berger, A. Lye, A. Maidl, J. Stoppe, and A. Windhorst	
Indepth analysis of a side-channel message recovery attack against FrodoKEM	666
P. A. Berthet	
Knowledge systematization for security orchestration in CPS and IoT systems	672
P. Nguyen, H. Song, R. Dautov, N. Ferry, A. Rego, E. Rios, E. Iturbe, V. Valdes, A. R. Cavalli, and W. Maloulli	
Wicked problem, parsimonious solution: Securing electric vehicle charging station software	679
E. Sheppard, Z. Wadhams, D. Arford, C. Izurieta, and A. M. Reinhold	
NetPacketformer: Real-time, context-aware network intrusion detection with transformers	687
A. Domi, C. Zonios, G. Tatsis, A. Drosou, and D. Tzovaras	
Data manipulation attack mitigation in power systems using physics-informed neural networks	693
S. Falas, M. Asprou, C. Konstantinou, and M. K. Michael	
The invisible threat: Simulating and analyzing the coordinated sensor manipulation attack (CSMA) on UAVs	699
S. Sadeghpour and P. Madani	



CSR Workshop on Privacy-Preserving Data Processing and Analysis (2P-DPA)

A real-time data capture probe for anomaly detection in industrial cyber-physical systems 707
R. F. Salazar Buttiglione, A. Gallo, S. Perone, E. Del Prete, and R. Setola

Implementation and experimental evaluation of defense techniques against adversarial attacks 713
G. M. Cristiano, S. D'Antonio, J. Giglio, and G. Mazzeo

Security challenges and solutions in containerized environments: A comprehensive review 720
R. Bagnato, L. Notarianni, A. Sabatini, and L. Vollero

Towards a privacy-preserving health data sharing: Architecture and critical implementation factors 725
A. Petruolo, A. Iannaccone, and S. D'Antonio

A game-theoretic multi-patroller approach for critical infrastructure monitoring 731
G. P. Rimoli, V. U. Castrillo, D. Pascarella, and M. Ficco

CSR Workshop on Cyber Resilience and Economics (CRE)

Addressing the economics of critical national infrastructure (CNI) security 737
S. A. Shaikh

Cybersecurity for sustainability: A path for strategic resilience 745
J. Saveljeva, I. Uvarova, L. Peiseniece, T. Volkova, J. Novicka, G. Polis, S. Kristapsone, and A. Vembris

CSR Workshop on Cyber Range, Insurance, and Risk Management (CRIRM)

LLM-powered intent-based categorization of phishing emails 753
E. Eilertsen, V. Mavroeidis, and G. Grov



CYBERUNITY: A federated architecture for next-generation cybersecurity training 759
C. Lal, A. V. Grammatopoulos, M. Takaronis, M. M. Yamin, G. Spathoulas, and C. Xenakis

ERMIS: A cybersecurity market assurance and insurance-as-a-service 765
A. Paragioudakis, M. Smyrlis, and G. Spanoudakis

Modelling attack and defense scenarios on federated cyber ranges 771
M. M. Yamin and B. Katt

From concept to deployment: An AI assistant for generating and configuring cyber range scenarios 777
G. S. Rizos, N. Kopalidis, N. Mengidis, A. Lalas, and K. Votis

The challenges of cyber-insurance: The case of Greece 783
E. Vergis, E. Aliberti, and S. Asteriou

Cyber insurance in emerging European markets: A case study of Greece and Cyprus 789
D. Smyrli, V. Kakariaris, and M. Smyrlis

CSR Workshop on Cyber-Vehi-Care for Automotive Cybersecurity (CVC)

Integration of forensic analysis and event data recorders in automotive regulation: A proposed approach 795
F. B. Soomro, R. Caviglia, G. B. Gaggero, M. Djihadi, and M. Marchese

Detection of C-V2X spoofing attacks using physical layer features and graph neural networks 801
D. Greco, M. S. Sohail, and M. Marchese

Cybersecurity for connected vehicle networks: Leveraging sampled network traffic beyond the CAN protocol 807
A. Yehezkel and E. Elyashiv

VPTaaS: An AI-driven cybersecurity framework for connected vehicles — Concept, validation, and feasibility study 812
S. W. Tan, M. A. Rahman, N. Refat, and P. Pillai



CyberVehiCare: A testbed for cybersecurity of vehicle to everything (V2X) automotive systems.....818
M. A. Rahman, T. Sze Wei, M. S. Sohail, G. B. Gaggero, F. Patrone, M. Marchese, and P. Pillai

CSR Workshop on Cybersecurity Innovation and Resilience (CYBERSHIELD)

A PUF-based root-of-trust for resource-constrained IoT devices824
E. N. Sassalou, S. Vasileiadis, S. A. Kazazis, G. Protogerou, N. Varvitsiotis, D. S. Karras, A. Giannetsos, and S. Tsintzos

CYRUS – A personalised, customised, work-based training framework for enhanced cyber-security skills across industrial sectors.....832
E. Frumento, K. Lange, and A. Golfetti

CoEvolution: A comprehensive trustworthy framework for connected machine learning and secure interconnected AI solutions838
A. Makris, A. Fournaris, A. Aghaie, I. Arakas, A. M. Anaxagorou, I. Arapakis, D. Bacciu, B. Biggio, G. Bouloukakis, S. Bouras, A. Bröring, A. Carta, M. Caselli, O. Giannakopoulou, N. Gkatzios, A. Gkillas, E. Haleplidis, S. Ioannidis, E. M. Kalogeraki, P. Karantzias, E. Kritharakis, A. Lalos, D. Lenk, S. Markopoulou, E. Metai, A. Miaoudakis, H. Mouratidis, J. Najar, T. Panagiotakopoulos, B. Peischl, M. Pintor, N. Piperigkos, V. Prevelakis, C. Segura, G. Spanoudakis, O. Tsirakis, O. Veledar, and K. Tserpes

C-Shield: A holistic solution for secure end-to-end Kubernetes multi-cluster management and online threat mitigation using LLMs846
S. Kalafatidis, G. Kitsos, and N. Papageorgopoulos

Hypervisor-based double extortion ransomware detection method using Kitsune network features.....854
M. Hirano and R. Kobayashi

On learning with confidentiality through encrypted AI pipelines861
T. Anastasiou, S. Iatropoulou, and S. Karagiorgou

Trust or bust: Reinforcing trust-aware path establishment with implicit attestation capabilities867
N. Fotos, S. Vasileiadis, and T. Giannetsos



Feature-enhanced deep learning models for cyber-physical system security..... 875
J. Vaughn, Y. Acquaah, and K. Roy

CSR Workshop on Cyber-Physical Resilience and Security Against Digital Breakdowns (CYPRES)

MOMENT: A multi-objective mitigation engine using NSGA-II techniques for cyber
threat response 881
K. Milousi, N. Vakakis, A. Mystakidis, M. S. Mazi, A. Voulgaridis, C. Tjortjis, K.
Votis, and D. Tzovaras

Deciphering standards for cybersecurity in Industry 4.0: Advisory AI for cybersecure
IIoT 887
A. Batziakas, I. Schoinas, A. Lalas, A. Drosou, N. Chatzidiamantis, and D. Tzovaras

Quantifying cascading impacts of natural hazards on power-communication
interdependent networks 893
B. V. Venkatasubramanain, C. Laoudias, and M. Panteli

Towards a new taxonomy of infrastructures: Implications for resilience 899
J. Palma Oliveira, D. Antunes, B. Rosa, D. Garcia Sanchez, A. Sarroeira, and A.
Cardoni

Beyond technical skills: Human, emotional, and resilience demands in CSIRT operations..... 905
D. Antunes, A. Salgado, V. Figueiredo, N. Oliveira, J. Ferreira, J. G. Santos, and J.
Palma Oliveira

Smart cities under threat: A systematic review and conceptual risk model 911
E. Roponena, R. Matisons, E. Citskovska, P. G. Rinkevičs, R. Pirta, and G. Priedols

Advancing B5G security: An AI-augmented intrusion detection system using a real-time
attack generator..... 917
G. Lazaridis, A. Damianou, A. Lalas, P. Chatzimisios, K. Votis, and D. Tzovaras



CSR Workshop on Electrical Power and Energy Systems Security, Privacy and Resilience (EPES-SPR)

Evaluating 5G-enabled EV charging infrastructure's resilience through stealthy cyber-attacks 923
D. Psaltis, K. Ntouros, A. Lekidis, S. Brotsis, and N. Kolokotronis

Detection of masquerade attacks on protection of digital substations using real-time measurements 929
M. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael

Neural cryptanalysis of lightweight block ciphers using residual MLPs 936
C. Eleftheriadis, G. Andronikidis, A. Lytos, E. Fountoukidis, P. A. Karypidis, T. Lagkas, V. Argyriou, I. Nanos, and P. Sarigiannidis

Fortified control-plane encapsulation with session-key derivation for secure IP mesh routing..... 944
G. Amponis, P. Radoglou Grammatikis, T. Lagkas, V. Argyriou, A. Sarigiannidis, N. Kazakli, T. Boufikos, and P. Sarigiannidis

Surrogate-guided adversarial attacks: Enabling white-box methods in black-box scenarios 950
D. C. Asimopoulos, P. Radoglou Grammatikis, P. Fouliras, K. Panitsidis, G. Efstathopoulos, T. Lagkas, V. Argyriou, I. Kotsiuba, and P. Sarigiannidis

CSR Workshop on Generative AI Applications to Security of Cyber-Physical Assets (GAIA-SEC)

LLM-based generation of formal specification for run-time security monitoring of ICS..... 957
G. Raptis, M. T. Khan, C. Koulamas, and D. Serpanos

Efficient classification of partially faked audio using deep learning 963
A. Alali, G. Theodorakopoulos, and A. Emad

Data generation and cybersecurity: A major opportunity or the next nightmare? 969
F. Marulli, L. Campanile, G. Ragucci, S. Carbone, and M. Bifulco

Explainable malware detection by means of federated machine learning..... 975
G. Ciaramella, F. Martinelli, A. Santone, and F. Mercaldo



An explainable method for access control policies classification 983
L. Petrillo, F. Martinelli, A. Santone, and F. Mercaldo

CSR Workshop on Hardware Cybersecurity Systems (HACS)

Atomic patterns: Field operation distinguishability on cryptographic ASICs..... 990
A. A. Sigourou, Z. Dyka, P. Langendoerfer, and I. Kabin

Acceleration of McEliece cryptosystem with instruction set extension for RISC-V 996
S. Kennedy and B. Halak

Miti-CAT: Mitigating power side-channel vulnerabilities in FPGA-based CNN accelerators through distributed convolution computation..... 1002
J. He and M. Zwolinski

SpectreShield: Design and analysis of Spectre countermeasures on RISC-V using gem5 1008
M. Khan, M. Mushtaq, R. Pacalet, and L. Apvrille

A hardware-efficient AEAD stream cipher based on a hybrid nonlinear feedback register structure 1016
A. Allahverdi and V. Mooney

Protection of the digital circuitry of a single-slope ADC against side-channel attacks 1024
K. Ahmad, E. Öztürk, C. Körpe, H. Yang, J. Yang, K. Tihaiya, R. Tran, G. Dündar, V. Mooney, and K. Ozanoglu

CSR Workshop on Information and Operational Technology Security (IOSEC)

Attacking the DLMS/COSEM advanced metering infrastructure..... 1031
I. Papadopoulos, D. Merkouris, C. Dalamagkas, N. Nikoloudakis, and A. Arvanitis

ATHENA: A federated architecture for cross-border cybersecurity operations and situational awareness 1037
A. Peratikou, E. Charalambous, P. Smyrli, and S. Stavrou

A hybrid transformer–LLM pipeline for function name recovery in stripped binaries..... 1043
R. Petrache and C. Lemnar



Privacy-preserving classification of partially encrypted feature vectors using multi-key homomorphic encryption..... 1049
D. E. Petrean and R. Potolea

DISTIL: Digital identities for the evaluation of job skills..... 1057
D. Kasimatis, P. Papadopoulos, W. J. Buchanan, C. Chrysoulas, S. Sayeed, A. Mylonas, and N. Pitropakis

SecAwarenessTruss: A federated cyber range solution for critical infrastructures..... 1063
M. Smyrlis, E. Floros, N. Nikoloudakis, E. Stavrou, D. Merkouris, A. Arvanitis, G. Spanoudakis, S. E. Papadakis, G. Potamos, and S. Stavrou

Fraud detection in Web content using machine learning and natural language processing 1069
A. Dance, A. Fraticiu, and C. Oprisa

CSR Workshop on Securing the Management of 6G Networks (SECMAN-6G)

DLT-EVA: Hardening O-RAN auditing and digital evidence preservation through blockchain..... 1075
K. Ntouros, E. Poulitsis, S. Brotsis, K. P. Grammatikakis, and N. Kolokotronis

Zero-trust and reinforcement learning for secure federated intelligence in 6G edge networks..... 1082
G. Bendiab, M. Guerar, H. Haiouni, and L. Verderame

AI-enhanced hybrid CFAR for 6G integrated sensing and communication (ISAC)..... 1088
K. Belhi, S. Chabbi, and M. Guerar

Evaluating forensic log readiness in simulated 6G networks..... 1094
S. Rizvi, B. A. S. Al Rimy, N. Anjum, and A. Kanta

Federated learning for securing medical imaging against deepfakes in 6G smart hospitals 1100
E. Perales, R. Verdy Ricard, M. A. Labiod, G. Bendiab, and Y. Chenoune



CSR Workshop on Security, Privacy and Resilience of Critical Assets in Critical Infrastructure (SPARC)

Vulnerability analysis of Web 3.0 based decentralised oracle networks.....	1106
D. Zhukovsky and M. T. Khan	
CyberHeraclius: Cyber defence evaluation methodology	1113
G. Hatzivasilis and S. Ioannidis	
Cyber physical systems security risks based on OPC-UA set-up vulnerability in manufacturing industries	1119
S. Abdullahi, M. Götz, and S. Lazarova Molnar	
Securing firmware updates using transparency and traceability services	1127
N. Fotiou, L. Georgiadis, G. Polyzos, and V. Siris	