

2021 IEEE International Conference on Cyber Security and Resilience (CSR 2021)

**Virtual Conference
26-28 July 2021**



IEEE Catalog Number: CFP21Y52-POD
ISBN: 978-1-6654-0286-6

**Copyright © 2021 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:	CFP21Y52-POD
ISBN (Print-On-Demand):	978-1-6654-0286-6
ISBN (Online):	978-1-6654-0285-9

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	xii
Conference sponsors	xiv
Program committees	xv
Authors' index	xxiii

Cyber Security

Anomaly based resilient network intrusion detection using inferential autoencoders	1
<i>Hannan A., Gruhl C., and Sick B.</i>	
Act proactively: An intrusion prediction approach for cyber security	8
<i>Panagiotidis P., Angelidis C., Karalis I., Spyropoulos G., and Liapis A.</i>	
A stream clustering algorithm for classifying network IDS alerts	14
<i>Vaarandi R.</i>	
Statistical metamorphic testing of neural network based intrusion detection systems	20
<i>Rehman F.U. and Izurieta C.</i>	
Detecting SQL injection web attacks using ensemble learners and data sampling	27
<i>Zuech R., Hancock J., and Khoshgoftaar T.</i>	
SK-Tree: A systematic malware detection algorithm on streaming trees via the signature kernel	35
<i>Cochrane T., Foster P., Chhabra V., Lemercier M., Lyons T., and Salvi C.</i>	
Software vulnerabilities, products and exploits: A statistical relational learning approach	41
<i>Figueiredo C., Lopes J.G., Azevedo R., Zaverucha G., Menasche D.S., and Aguiar L.</i>	

Rapid ransomware detection through side channel exploitation	47
<i>Taylor M., Larson E., and Thornton M.</i>	
Machine learning on knowledge graphs for context-aware security monitoring	55
<i>Garrido J.S., Dold D., and Frank J.</i>	
Mc-PUF: Memory-based and machine learning resilient strong PUF for device authentication in internet of things	61
<i>Williams P., Idriss H., and Bayoumi M.</i>	
SoK: Autonomic cybersecurity - Securing future disruptive technologies	66
<i>Rouff C., Watkins L., Sterritt R., and Hariri S.</i>	
ERAMO: Effective remote attestation through memory offloading	73
<i>Ostergaard J.H., Dushku E., and Dragoni N.</i>	
ENAD: An ensemble framework for unsupervised network anomaly detection	81
<i>Liao J., Teo S.G., Kundu P.P., and Truong-Huu T.</i>	
Using deep packet inspection in cyber traffic analysis	89
<i>Deri L. and Fusco F.</i>	
Clustering analysis of email malware campaigns	95
<i>Zhang R., Wang S., Burton R., Hoang M., Hu J., and Nascimento A.</i>	
Enhancing medical data security on public cloud	103
<i>Santos N., Younis W., Ghita B., and Masala G.</i>	
On security of key derivation functions in password-based cryptography	109
<i>Kodwani G., Arora S., and Atrey P.</i>	
Web bot detection evasion using generative adversarial networks	115
<i>Iliou C., Kostoulas T., Tsikrika T., Katos V., Vrochidis S., and Kompatsiaris I.</i>	
Understanding and mitigating banking trojans: From Zeus to Emotet	121
<i>Grammatikakis K.P., Koufos I., Kolokotronis N., Vassilakis C., and Shiaeles S.</i>	
Insider threat detection using deep autoencoder and variational autoencoder neural networks	129
<i>Pantelidis E., Bendiab G., Shiaeles S., and Kolokotronis N.</i>	
Toward automated threat modeling of edge computing systems	135
<i>Casola V., Benedictis A.D., Mazzocca C., and Montanari R.</i>	

Semi-automatic bug generation using test case negation 141
Westland T., Niu N., Jha R., Kapp D., and Kebede T.

STRIDE-AI: An approach to identifying vulnerabilities of machine learning assets 147
Mauri L. and Damiani E.

Cyber Resilience

Resilient boot 155
Ostrikov S.

Cyber resilience for self-monitoring IoT devices 160
Medwed M., Nikov V., Renes J., Schneider T., and Veshchikov N.

Resilience learning through self adaptation in digital twins of human-cyber-physical systems 168
Bellini E., Bagnoli F., Caporuscio M., Damiani E., Flammini F., Linkov I., Lio P., and Marrone S.

Automated and on-demand cybersecurity certification 174
Karagiannis S., Manso M., Magkos E., Ribeiro L.L., and Campos L.

Towards a maritime cyber range training environment 180
Potamos G., Peratikou A., and Stavrou S.

Cyber-range federation and cyber-security games: A gamification scoring model 186
Diakoumakos J., Chaskos E., Kolokotronis N., and Lepouras G.

Cyber-security training evaluation metrics 192
Koutsouris N., Vassilakis C., and Kolokotronis N.

Open source and commercial capture the flag cyber security learning platforms: A case study 198
Swann M., Rose J., Bendiab G., Shiaeles S., and Li F.

Cyber Physical Systems Security

Development of a testbed for fully homomorphic encryption solutions 206
Marrone S., Tortora A., Bellini E., Maione A., and Raimondo M.

Towards anomaly detection in smart grids by combining complex events processing and SNMP objects	212
<i>Itria M.L., Schiavone E., and Nostro N.</i>	
Reinforcement learning-driven attack on road traffic signal controllers	218
<i>Arabi N.S., Halabi T., and Zulkernine M.</i>	
SoK: Investigation of security and functional safety in industrial IoT	226
<i>Tomur E., Gulen U., Soykan E.U., Ersoy M.A., Karakoc F., Karacay L., and Comak P.</i>	
Enabling efficient common criteria security evaluation for connected vehicles	234
<i>Stamou A., Pantazopoulos P., Haddad S., and Amditis A.</i>	
Analyzing cascading effects of spoofing attacks on ADS-B using a discrete model of air traffic control responses and AGMOD dynamics	241
<i>Kamaruzzaman M.R., Sane B.O., Fall D., Taenaka Y., and Kadobayashi Y.</i>	
Towards HybridgeCAN, a hybrid bridged CAN platform for automotive security testing	249
<i>Granata D., Rak M., and Salzillo G.</i>	
Securing an MQTT-based traffic light perception system for autonomous driving	255
<i>Affia A. and Matulevicius R.</i>	
Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm	261
<i>Shukla S., Thakur S., and Breslin J.G.</i>	
Real-time, simulation-based identification of cyber-security attacks of industrial plants	267
<i>Patel A., Schenk T., Knorn S., Patzlaff H., Obradovic D., and Halblaub A.B.</i>	
Fast dual-field ECDSA accelerator with increased resistance against horizontal SCA attacks	273
<i>Kabin I., Klann D., Dyka Z., and Langendoerfer P.</i>	
On the detection of channel switch announcement attack in 802.11 networks	281
<i>Louca C., Peratikou A., and Stavrou S.</i>	
A dynamic reconfiguration-based approach to resilient state estimation	286
<i>Joss A., Grassbaugh A., Poshtan M., and Callenes J.</i>	
Systematic and efficient anomaly detection framework using machine learning on public ICS datasets	292
<i>Millot B., Francq J., and Sicard F.</i>	

Machine learning for threat recognition in critical cyber-physical systems	298
<i>Perrone P., Flammini F., and Setola R.</i>	

CSR WS Actionable Cyber Threat Intelligence

Mapping cyber threat intelligence to probabilistic attack graphs	304
<i>Gylling A., Ekstedt M., Afzal Z., and Eliasson P.</i>	

A tree-based machine learning methodology to automatically classify software vulnerabilities	312
<i>Aivatoglou G., Anastasiadis M., Spanos G., Voulgaridis A., Votis K., and Tzovaras D.</i>	

Evaluation and enhancement of the actionability of publicly available cyber threat information in digital forensics	318
<i>Dimitriadis A., Lontzetidis E., and Mavridis I.</i>	

A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms	324
<i>Stojkovski B. and Lenzini G.</i>	

CTI blockchain-based sharing using proof-of-quality consensus algorithm	331
<i>Chatziamanetoglou D. and Rantos K.</i>	

Towards intrusion response intel	337
<i>Hughes K., Mclaughlin K., and Sezer S.</i>	

Data sanitisation and redaction for cyber threat intelligence sharing platforms	343
<i>Yucel C., Chalkias I., Mallis D., Cetinkaya D., Henriksen-Bulmer J., and Cooper A.</i>	

Named entity recognition in cyber threat intelligence using transformer-based models	348
<i>Evangelatos P., Iliou C., Mavropoulos T., Apostolou K., Tsikrika T., Vrochidis S., and Kompatsiaris I.</i>	

Towards selecting informative content for cyber threat intelligence	354
<i>Panagiotou P., Iliou C., Apostolou K., Tsikrika T., Vrochidis S., Chatzimisios P., and Kompatsiaris I.</i>	

Trust and quality computation for cyber threat intelligence sharing platforms	360
<i>Mavzer K.B., Konieczna E., Alves H., Yucel C., Chalkias I., Mallis D., Cetinkaya D., and Galindo Sanchez L.A.</i>	

Towards automated matching of cyber threat intelligence reports based on cluster analysis in an Internet-of-vehicles environment	366
<i>Raptis G.E., Katsini C., and Alexakos C.</i>	

CSR WS Cyber Resilience and Economics

Modelling cyber-risk in an economic perspective	372
<i>Bothos I., Vlachos V., Kyriazanos D., Stamatiou I., Thanos K.G., Tzamalīs P., Nikolettseas S., and Thomopoulos S.</i>	
Disposable identities; Enabling trust-by-design to build more sustainable data driven value	378
<i>Isohanni J., Goulden L., Hermsen K.M., Ross M., and Vanbockryck J.</i>	
Influence pathways: Mapping the narratives and psychological effects of Russian COVID-19 disinformation	384
<i>Hoyle A., Powell T., Cadet B., and van de Kuijt J.</i>	

CSR WS Cyber Ranges and Security Training

The current state of the art and future of European cyber range ecosystem	390
<i>Virag C., Cegan J., Lieskovan T., and Merialdo M.</i>	
Frankenstack: Real-time cyberattack detection and feedback system for technical cyber exercises	396
<i>Pihelgas M. and Kont M.</i>	
ECHO federated cyber range: Towards next-generation scalable cyber ranges	403
<i>Oikonomou N., Mengidis N., Spanopoulos-Karalexidis M., Voulgaridis A., Merialdo M., Raisr I., Hanson K., de La Vallee P., Tsikrika T., Vrochidis S., and Votis K.</i>	
The Cyber-MAR project: First results and perspectives on the use of hybrid cyber ranges for port cyber risk assessment	409
<i>Jacq O., Salar P.G., Parasuraman K., Kuusijärvi J., Gkaniatsou A., Latsa E., and Amditis A.</i>	
The SPIDER cyber security investment component (CIC)	415
<i>Tsiodra M., Chronopoulos M., Ghering M., Karapistoli E., Gerosavva N., and Kylilis N.</i>	
The THREAT-ARREST cyber ranges platform	422
<i>Hatzivasilis G., Ioannidis S., Smyrlis M., Spanoudakis G., Frati F., Braghin C., Damiani E., Koshutanski H., Tsakirakis G., Hildebrandt T., Goeke L., Pape S., Blinder O., Vinov</i>	

M., Leftheriotis G., Kunc M., Oikonomou F., Magilo G., Petrarolo V., Chieti A., and Bordianu R.

Cyber security certification programmes 428

Davri E., Darra E., Monogioudis I., Grigoriadis A., Iliou C., Mengidis N., Tsikrika T., Vrochidis S., Peratikou A., Gibson H., Haskovic D., Kavallieros D., Chaskos E., Zhao P., Shiaeles S., Savage N., Akhgar B., Bellekens X., and Amine Ben Farah M.

CSR WS Data Science for Cyber Security

Social media monitoring for IoT cyber-threats 436

Alevizopoulou S., Koloveas P., Tryfonopoulos C., and Raftopoulou P.

Data exfiltration: Methods and detection countermeasures 442

King J., Bendiab G., Savage N., and Shiaeles S.

Detecting adversarial DDoS attacks in software-defined networking using deep learning techniques and adversarial training 448

Nugraha B., Kulkarni N., and Gopikrishnan A.

Unveiling MIMETIC: Interpreting deep learning traffic classifiers via XAI techniques 455

Nascita A., Montieri A., Aceto G., Ciunzo D., Persico V., and Pescape A.

Detecting attacks on IoT devices using featureless 1D-CNN 461

Khan A. and Cotton C.

DAHID: Domain adaptive host-based intrusion detection 467

Ajayi O. and Gangopadhyay A.

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

Enhancing SIEM technology for protecting electrical power and energy sector 473

Sklavidis I., Angelidis C., Babagiannou R., and Liapis A.

A scalable multi-agent system for black start restoration in low voltage microgrids 479

Pasias A., Schoinas A., Drosou A., and Tzovaras D.

TRUSTY: A solution for threat hunting using data analysis in critical infrastructures 485

Radoglou-Grammatikis P., Liatifis A., Grigoriou E., Saoulidis T., Sarigiannidis A., Lagkas T., and Sarigiannidis P.

Increasing resilience of power systems using intentional islanding; a comparison of binary genetic algorithm and deep learning based method 491
Paradell P., Spyridis Y., Colet Subirachs A., Ivanova A., Dominguez-Garcia J.L., Sesis A., and Efstathopoulos G.

Enabling cyber-attack mitigation techniques in a software defined network 497
Pasias A., Kotsiopoulos T., Lazaridis G., Drosou A., Tzovaras D., and Sarigiannidis P.

CSR WS Maritime Cyber Security

Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system 503
Drazovich L., Brew L., and Wetzel S.

The impact of COVID-19 on the security and resilience of the maritime transportation system 510
Brew L., Drazovich L., and Wetzel S.

Impact assessment of anomaly propagation in a naval water distribution cyber-physical system 518
Pelissero N., Merino Laso P., and Puentes J.

A backwards compatible approach to authenticate automatic identification system messages 524
Struck M. and Stoppe J.U.

Quantum cryptography in maritime telecommunications 530
Papathanasaki M., Fountas P., Maglaras L., Douligeris C., and Ferrag M.A.

CSR WS Resilient Artificial Intelligence

Towards resilient artificial intelligence: Survey and research issues 536
Eigner O., Eresheim S., Kieseberg P., Klausner L.D., Pirker M., Priebe T., Tjoa S., Marulli F., and Mercaldo F.

Assessing adversarial training effect on IDSs and GANs 543
Chaitou H., Robert T., Leneutre J., and Pautet L.

Defending against model inversion attack by adversarial examples 551
Wen J., Yiu S., and Hui L.C.



X-BaD: A flexible tool for explanation-based bias detection 557
Pacini M., Nesti F., Biondi A., and Buttazzo G.

Improving classification trustworthiness in random forests 563
Marrone S., Biase M.S.D., Marulli F., and Verde L.