IEEE CSR 2021

Cyber Security and Resilience

Athena room (main conference)

Monday 26th of July

08:40–09:00 CET Welcome from the chairs WL
Stavros Shiaeles, Nicholas Kolokotronis, Emanuele Bellini

09:00–10:00 CET Plenary session PL1
Chair: Emanuele Bellini, University of Campania Vanvitelli (IT)

Invited talk: Israel national and organisational cyber resiliency strategy and policy
Isaac Ben Israel

10:00–11:20 CET Technical session CSR1
Chair: Francesco Flammini, Mälardalen University (SE)

10:00–10:20 Anomaly based resilient network intrusion detection using inferential autoencoders
A. Hannan, C. Gruhl, and B. Sick

10:20–10:40 Act proactively: An intrusion prediction approach for cyber security
P. Panagiotidis, C. Angelidis, I. Karalis, G. Spyropoulos, and A. Liapis

10:40–11:00 A stream clustering algorithm for classifying network IDS alerts
R. Vaarandi

11:00–11:20 Statistical metamorphic testing of neural network based intrusion detection systems
F. Rehman and C. Izurieta

11:20–11:40 CET Coffee break

11.40–13:00 CET Technical session CSR2
Chair: Stefano Marrone, University of Campania Vanvitelli (IT)

11.40–12:00 Detecting SQL injection web attacks using ensemble learners and data sampling
R. Zuech, J. Hancock, and T. Khoshgoftaar

12.00–12:20 SK-Tree: A systematic malware detection algorithmon streaming trees via the signature kernel
C. Salvi, T. Lyons, M. Lemercier, T. Cochrane, V. Chhabra, and P. Foster

12.20–12:40 Software vulnerabilities, products and exploits: A statistical relational learning approach
C. Figueiredo, J. G. Lopes, R. Azevedo, G. Zaverucha, D. S. Menasche, and L. Aguiar

12.40–13:00 Rapid ransomware detection through side channel exploitation
M. Taylor, E. Larson, and M. Thornton

13:00–14:00 CET Lunch break

14:00–15:20 CET Technical session CSR3
Chair: Nicholas Kolokotronis, University of the Peloponnese (GR)

14:00–14:20 Reinforcement learning-driven attack on road traffic signal controllers
N. Seifollahpour Arabi, T. Halabi, and M. Zulkernine

14:20–14:40 Resilient boot
S. Ostrikov

14:40–15:00 Cyber resilience for self-monitoring IoT devices
M. Medwed, V. Nikov, J. Renes, T. Schneider, and N. Veshchikov

15:00–15:20 Resilience learning through self adaptation in digital twins of human-cyber-physical systems
E. Bellini, F. Bagnoli, M. Caporuscio, E. Damiani, F. Flammini, I. Linkov, P. Lio, and S. Marrone

15:20–15:40 Coffee break
CET

15:40–17:20 Technical session CSR4
CET Chair: Stavros Shiaeles, University of Portsmouth (UK)

15:40–16:00 Machine learning on knowledge graphs for context-aware security monitoring
J. Soler Garrido, D. Dold, and J. Frank

16:00–16:20 SoK: Investigation of security and functional safety in industrial IoT
E. Tomur, U. Gulen, E. Ustundağ Soykan, M. A. Ersoy, F. Karakoc, L. Karacay, and P. Comak

16:20–16:40 Mc-PUF: memory-based and machine learning resilient strong PUF for device authentication in internet of things
P. Williams, H. Idriss, and M. Bayoumi

16:40–17:00 SoK: Autonomic cybersecurity – Securing future disruptive technologies
C. Rouff, L. Watkins, R. Sterritt, and S. Hariri

17:00–17:20 ERAMO: Effective remote attestation through memory offloading
J. H. Ostergaard, E. Dushku, and N. Dragoni

Tuesday 27th of July

09:00–10:00 Plenary session PL2
CET Chair: Nicholas Kolokotronis, University of the Peloponnese (GR)

Invited talk: Threat modelling for machine-learning systems
Ernesto Damiani

10:00–11:20 Technical session CSR5
CET Chair: Bogdan Ghita, University of Plymouth (UK)

10:00–10:20 ENAD: An ensemble framework for unsupervised network anomaly detection
J. Liao, S. G. Teo, P. P. Kundu, and T. Truong-Huu

10:20–10:40 Using deep packet inspection in cyber traffic analysis
L. Deri and F. Fusco

10:40–11:00 Towards anomaly detection in smart grids by combining complex events processing and SNMP objects
M. L. Itria, E. Schiavone, and N. Nostro

11:00–11:20 Clustering analysis of email malware campaigns
R. Zhang, S. Wang, R. Burton, M. Hoang, J. Hu, and A. Nascimento

11:20–11:40 Coffee break
CET

11.40–13:00 Technical session CSR6
CET Chair: Emanuele Bellini, University of Campania Vanvitelli (IT)

11.40–12:00 Enabling efficient common criteria security evaluation for connected vehicles
A. Stamou, P. Pantazopoulos, S. Haddad, and A. Amditis

12.00–12:20 Analyzing cascading effects of spoofing attacks on ADS-B using a discrete model of air traffic control responses and AGMOD dynamics
M. R. Kamaruzzaman, B. O. Sane, D. Fall, Y. Taenaka, and Y. Kadobayashi

12.20–12:40 Towards HybridgeCAN, a hybrid bridged CAN platform for automotive (security) testing
D. Granata, M. Rak, and G. Salzillo

12.40–13:00 Securing an MQTT-based traffic light perception system for autonomous driving
A.-A. Affia and R. Matulevicius

13:00–14:00 CET **Lunch break**

14:00–15:00 CET **Plenary session PL3**
Chair: Stavros Shiaeles, University of Portsmouth (UK)

Invited talk: Actionable and interpretable AI (AI^2) and resilience
Igor Linkov

15:20–15:40 CET **Coffee break**

15:40–17:20 CET **Technical session CSR7**
Chair: Fudong Li, University of Portsmouth (UK)

15:40–16:00 Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm
S. Shukla, S. Thakur, and J. G. Breslin

16:00–16:20 Enhancing medical data security on public cloud
N. Santos, W. Younis, B. Ghita, and G. Masala

16:20–16:40 Development of a testbed for fully homomorphic encryption solutions
S. Marrone, A. Tortora, E. Bellini, A. Maione, and M. Raimondo

16:40–17:00 On security of key derivation functions in password-based cryptography
G. Kodwani, S. Arora, and P. Atrey

17:20–18:20 CET **Awards session AW**
Chairs: Emanuele Bellini, University of Campania Vanvitelli (IT); Giancalro Fortino, University of Calabria (IT)

Wednesday 28th of July

09:00–10:00 CET **Plenary session PL4**
Chair: Stavros Shiaeles, University of Portsmouth (UK)

Invited talk: Recognising knowledge and skills for cyber security and resilience
Steve Furnell

10:00–11:20 CET **Technical session CSR8**
Chair: Nicholas Kolokotronis, University of the Peloponnese (GR)

10:00–10:20 Real-time, simulation-based identification of cyber-security attacks of industrial plants
A. Patel, T. Schenk, S. Knorn, H. Patzlaff, D. Obradovic, and A. Botero Halblaub

10:20–10:40 Web bot detection evasion using generative adversarial networks
C. Iliou, T. Kostoulas, T. Tsikrika, V. Katos, S. Vrochidis, and I. Kompatsiaris

10:40–11:00 Understanding and mitigating banking trojans: From Zeus to Emotet
K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles

11:00–11:20 Insider threat detection using deep autoencoder and variational autoencoder neural networks
E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis

11:20–11:40 CET Coffee break

11.40–13:00 CET Technical session CSR9
Chair: Costas Vassilakis, University of the Peloponnese (GR)

11.40–12:00 Fast dual-field ECDSA accelerator with increased resistance against horizontal SCA attacks
I. Kabin, D. Klann, Z. Dyka, and P. Langendoerfer

12.00–12:20 On the detection of channel switch announcement attack in 802.11 networks
C. Louca, A. Peratikou, and S. Stavrou

12.20–12:40 Toward automated threat modeling of edge computing systems
C. Mazzocca, A. De Benedictis, R. Montanari, and V. Casola

12.40–13:00 A dynamic reconfiguration-based approach to resilient state estimation
A. Joss, A. Grassbaugh, M. Poshtan, and J. Callenes

13:00–14:00 CET Lunch break

14:00–15:20 CET Technical session CSR10
Chair: Nicholas Kolokotronis, University of the Peloponnese (GR)

14:00–14:20 Systematic and efficient anomaly detection framework using machine learning on public ICS datasets
B. Millot, J. Francq, and F. Sicard

14:20–14:40 Semi-automatic bug generation using test case negation
T. Westland, N. Niu, R. Jha, D. Kapp, and T. Kebede

14:40–15:00 STRIDE-AI: An approach to identifying vulnerabilities of machine learning assets
L. Mauri and E. Damiani

15:00–15:20 Machine learning for threat recognition in critical cyber-physical systems
P. Perrone, F. Flammini, and R. Setola

15:20–15:40 CET Coffee break

15:40–17:20 CET Technical session CSR11
Chair: Emanuele Bellini, University of Campania Vanvitelli (IT)

15:40–16:00 Automated and on-demand cybersecurity certification
S. Karagiannis, M. Manso, E. Magkos, L. L. Ribeiro, and L. Campos

16:00–16:20 Towards a maritime cyber range training environment
G. Potamos, A. Peratikou, and S. Stavrou

16:20–16:40 Cyber-range federation and cyber-security games: A gamification scoring model
J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras

16:40–17:00 Cyber-security training evaluation metrics
N. Koutsouris, C. Vassilakis, and N. Kolokotronis

17:00–17:20 Open source and commercial capture the flag cyber security learning platforms: A case study
M. Swann, J. Rose, G. Bendiab, S. Shiaeles, and F. Li