IEEE CSR 2025

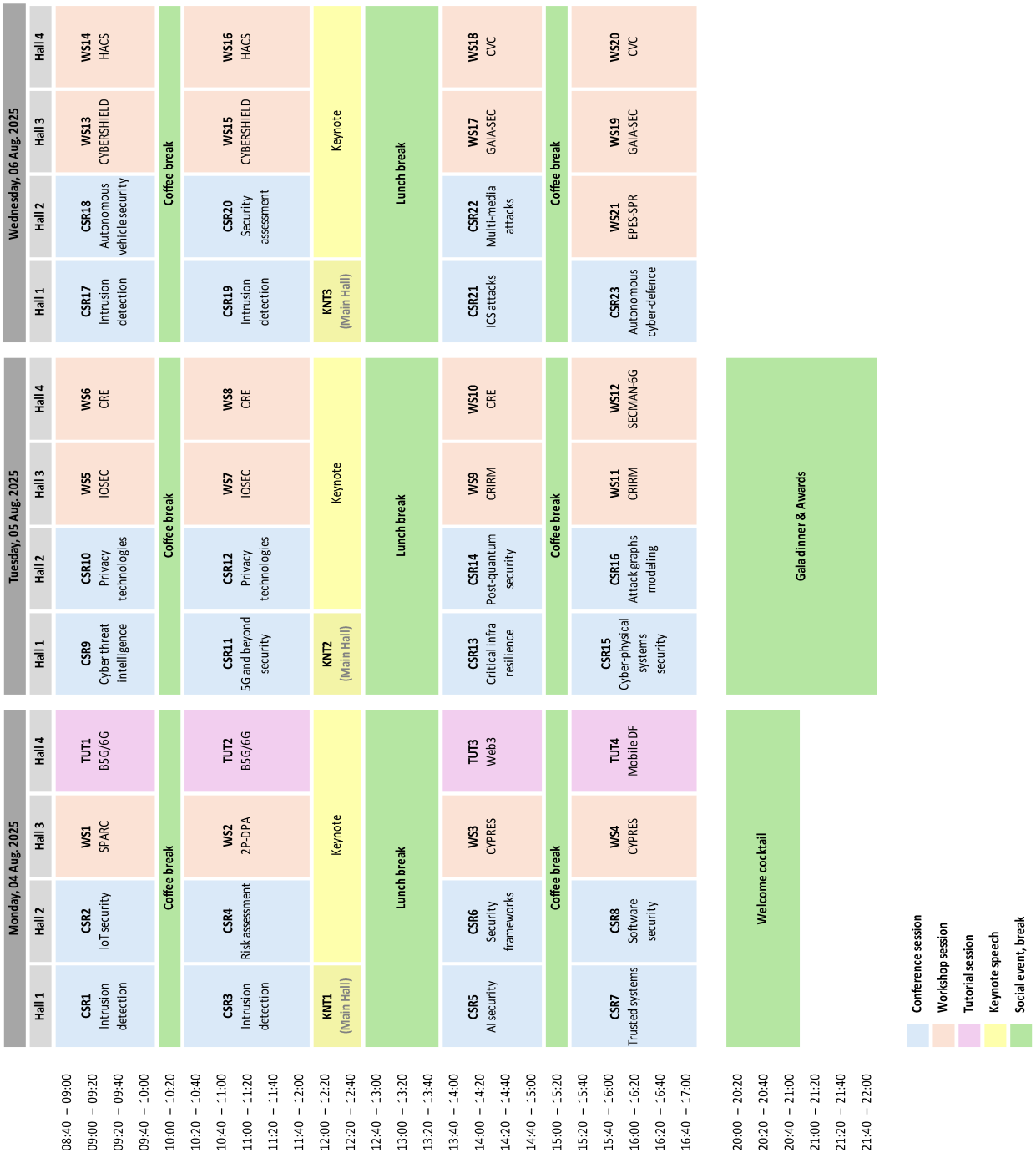
IEEE

IEEE SMC Systems, Man, and Cybernetics Society

LOGOS RI RESEARCH&INNOVATION

Program Handbook

Conference program overview



Monday, 04 Aug. 2025

08:40–10:00 **Session CSR1: Intrusion detection**

Chair: Alexios Lekidis, University of Thessaly (GR)

Room: Hall 1

08:40–09:00 Towards DoS attack detection for IoT systems: A cross-layer oriented approach based on machine learning techniques

D. Tasiopoulos, A. Xenakis, A. Lekidis, D. Kosmanos, C. Chaikalis, and V. Vlachos

09:00–09:20 Machine-learning anomaly detection for early identification of DDOS in smart home IoT devices

R. Lamptey, M. Saedi, and V. Stankovic

09:20–09:40 Adapt-LFA: Adaptive gradient-guided label flipping attack against federated learning-based intrusion detection in IoT

H. Rezaei, R. Taheri, I. Jordanov, and S. Shiaeles

09:40–10:00 Adaptive weighted ensemble learning for intrusion detection in industrial IoT and edge computing

S. Ruiz Villafranca, L. M. Garcia Sáez, J. Roldán Gómez, J. Carrillo Mondéjar, J. M. Castelo Gómez, and J. L. Martínez

08:40–10:00 **Session CSR2: IoT security**

Chair: Wanrong Yang, University of Liverpool (UK)

Room: Hall 2

08:40–09:00 Abstract attack intention inference using low-rank gated arithmetic interactive attention

W. Yang, M. Wang, and D. Wojtczak

09:00–09:20 A novel MQTT-ZT secure broker: Zero trust architecture for IoT security

M. James, T. Newe, D. O'Shea, and G. D. O'Mahony

09:20–09:40 Not-so-secret authentication: The SyncBleed attacks and defenses for zero-involvement authentication systems

I. Ahlgren, R. Shirsat, O. Achkar, G. K. Thiruvathukal, K. I. Lee, and N. Klingensmith

09:40–10:00 Fault tolerance vs. attack detection in industrial control systems: A deep learning approach

H. Mehrpouyan

08:40–10:00 Session WS1: SPARC workshop

Chair: George Hatzivasilis, Technical University of Crete (GR)

Room: Hall 3

08:40–08:40 Welcome by the chairs

N. Saxena, G. Hatzivasilis, and C. Hankin

08:40–09:00 Vulnerability analysis of Web 3.0 based decentralised oracle networks

D. Zhukovsky and M. T. Khan

09:00–09:20 CyberHeraclius: Cyber defence evaluation methodology

G. Hatzivasilis and S. Ioannidis

09:20–09:40 Cyber physical systems security risks based on OPC-UA set-up vulnerability in manufacturing industries

S. Abdullahi, M. Götz, and S. Lazarova Molnar

09:40–10:00 Securing firmware updates using transparency and traceability services

N. Fotiou, L. Georgiadis, G. Polyzos, and V. Siris

08:40–10:00 Session TUT1: IEEE CSR tutorials

Room: Hall 4

08:40–10:00 Applying data engineering and blockchain for B5G/6G networks: A step-by-step approach

M. Liyanage and E. Zeydan

10:00–10:20 Coffee break

10:20–12:00 **Session CSR3: Intrusion detection**

Chair: Angelos Papoutsis, Centre for Research and Technology Hellas (GR)

Room: Hall 1

10:20–10:40 Enhancing deep learning based IDS adversarial robustness with causal inference

M. François, P. E. Arduin, and M. Merad

10:40–11:00 Contrastive self-supervised network intrusion detection using augmented negative pairs

J. Wilkie, H. Hindy, C. Tachtatzis, and R. Atkinson

11:00–11:20 eIDPS: A comprehensive comparative analysis of packet-level and flow-level intrusion detection and prevention

S. Kostopoulos, D. Papatsaroucha, I. Kefaloukos, and E. K. Markakis

11:20–11:40 RuleXploit: A framework for generating suricata rules from exploits using generative AI

A. Papoutsis, A. Dimitriadis, I. Koritsas, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris

11:40–12:00 CAN-MAID: An intrusion detection protocol for CAN bus

K. Marquis and J. Chandy

10:20–12:00 **Session CSR4: Risk assessment**

Chair: Pierre Saha Fobougong, Laval University (CA)

Room: Hall 2

10:20–10:40 Optimized security measure selection: Leveraging MILP solvers to balance risk and cost

P. Saha Fobougong, M. Mejri, and K. Adi

10:40–11:00 A Bayesian–Markov framework for proactive and dynamic cyber risk assessment driven by EPSS

P. Cheimonidis and K. Rantos

11:00–11:20 Composite product cybersecurity certification using explainable AI based dynamic risk assessment

N. Basheer, S. Islam, S. Papastergiou, and E. Maria Kalogeraki

11:20–11:40 Lessons learned from a cybersecurity risk assessment of OpenADR in smart grid planning

G. Erdogan, A. Omerovic, E. Solvang, A. Killingberg, A. Kvinnesland, and I. Abrahamsen

11:40–12:00 Security risk analysis of logistical support solutions for MaaS and DLT-based mitigations

G. Kisa Isik, A. Eker, T. Tryfonas, and G. Oikonomou

10:20–12:00 Session WS2: 2P-DPA workshop

Chair: Salvatore D' Antonio, Trustup srl/University of Naples Parthenope (IT)

Room: Hall 3

10:20–10:20 Welcome by the chairs

S. D' Antonio

10:20–10:40 A real-time data capture probe for anomaly detection in industrial cyber-physical systems

R. F. Salazar Buttiglione, A. Gallo, S. Perone, E. Del Prete, and R. Setola

10:40–11:00 Implementation and experimental evaluation of defense techniques against adversarial attacks

G. M. Cristiano, S. D'Antonio, J. Giglio, and G. Mazzeo

11:00–11:20 Security challenges and solutions in containerized environments: A comprehensive review

R. Bagnato, L. Notarianni, A. Sabatini, and L. Vollero

11:20–11:40 Towards a privacy-preserving health data sharing: Architecture and critical implementation factors

A. Petruolo, A. Iannaccone, and S. D'Antonio

11:40–12:00 A game-theoretic multi-patroller approach for critical infrastructure monitoring

G. P. Rimoli, V. U. Castrillo, D. Pascarella, and M. Ficco

10:20–12:00 **Session TUT2: IEEE CSR tutorials**

Room: Hall 4

10:20–12:00 Applying data engineering and blockchain for B5G/6G networks: A step-by-step approach

M. Liyanage and E. Zeydan

12:00–12:40 **Session KNT1: IEEE CSR keynote speakers**

Chair: Stavros Shiaeles, University of Portsmouth (UK)

Room: Main Hall

12:00–12:40 Unifying security: How trusted execution environments secure AI on the edge and the battle against side-channel attacks

K. Markantonakis

12:40–13:40 **Lunch break**

Location: Elia restaurant

13:40–15:00 **Session CSR5: AI security**

Chair: Baris Aksanli, San Diego State University (US)

Room: Hall 1

13:40–14:00 Designing AI systems with correction mechanisms towards attack-resilient architectures

E. Kafali, C. N. Spartalis, T. Semertzidis, C. Z. Patrikakis, and P. Daras

14:00–14:20 Defending against beta poisoning attacks in machine learning models

N. Gulciftci and M. E. Gursoy

14:20–14:40 ReLATE: Resilient learner selection for multivariate time-series classification against adversarial attacks

C. I. Kocal, O. Gungor, A. Tartz, T. Rosing, and B. Aksanli

14:40–15:00 FAIR: Facilitating artificial intelligence resilience in manufacturing industrial Internet

Y. Zeng, I. Lourentzou, X. Deng, and R. Jin

13:40–15:00 Session CSR6: Security frameworks

Chair: Hafiz Malik, University of Michigan – Dearborn (US)

Room: Hall 2

13:40–14:00 Scalable and adaptive security framework for the IoT-edge-cloud continuum

S. Cuñat Negueroles, I. Makropodis, L. Cabanillas Rodriguez, C. Xenakis, I. Chouchoulis, C. Palau, and I. Lacalle

14:00–14:20 Development of an SDN-based space system simulation framework for intrusion detection

U. Uhongora, M. Thinyane, and Y. W. Law

14:20–14:40 A lightweight IDS framework using FPGA-based hardware fingerprinting on Zynq SoC

A. W. Mohammed, A. Ali, H. Arif, F. R. P. Mohammed, and H. Malik

14:40–15:00 Technological framework for secure and resilient food supply chain

M. Fischer, R. Tönjes, R. Bohara, M. Ross, A. Hegde, C. Wressnegger, and M. Brunner

13:40–15:00 Session WS3: CYPRES workshop

Chair: Mathaios Panteli, University of Cyprus (CY)

Room: Hall 3

13:40–13:40 Welcome by the chairs

M. Panteli, U. Stecchi, and A. Lalas

13:40–14:00 A multi-objective optimization framework for cyber threat mitigation using NSGA-II

K. Milousi, N. Vakakis, A. Mystakidis, M. S. Mazi, A. Voulgaridis, C. Tjortjis, K. Votis, and D. Tzovaras

14:00–14:20 Deciphering standards for cybersecurity in Industry 4.0: Advisory AI for cybersecure IIoT

A. Batziakas, I. Schoinas, A. Lalas, A. Drosou, N. Chatzidiamantis, and D. Tzovaras

14:20–14:40 Smart cities under threat: A systematic review and conceptual risk model
E. Roponena, R. Matisons, E. Citskovska, P. G. Rinkevičs, R. Pirta, and Ģ. Priedols

14:40–15:00 Advancing B5G security: An AI-augmented intrusion detection system using a real-time attack generator
G. Lazaridis, A. Damianou, A. Lalas, P. Chatzimisios, K. Votis, and D. Tzovaras

13:40–15:00 Session TUT3: IEEE CSR tutorials
Room: Hall 4

13:40–15:00 Web3: Securing advanced communication networks, the Internet and digital platforms
A. Vizzarri

15:00–15:20 Coffee break

15:20–17:00 Session CSR7: Trusted systems
Chair: Utku Budak, Technical University of Munich (DE)
Room: Hall 1

15:20–15:40 Practical confidential data cleaning using trusted execution environments
A. Basu, M. Yoshino, and M. Toba

15:40–16:00 A collusion-resistant DECO-based attestation protocol for practical applications
U. Şen, M. Osmanoğlu, and A. A. Selçuk

16:00–16:20 PCIe monitoring for secure code execution in heterogeneous system architectures
I. Georgakas, E. Papadogiannaki, K. Georgopoulos, and S. Ioannidis

16:20–16:40 A lightweight firmware resilience engine for real-time operating systems
U. Budak, F. De Santis, O. Yasar, M. Safieh, and G. Sigl

16:40–17:00 Reimagining the usermode process space by utilizing hardware-enforced sub-process isolation
M. Nelson and M. Mirakhorli

15:20–17:00 **Session CSR8: Software security**

Chair: Georgios Siachamis, Aristotle University of Thessaloniki (GR)

Room: Hall 2

15:20–15:40 An AI-powered pipeline for enabling self-healing in software systems

G. Siachamis, G. Papadopoulos, and A. Symeonidis

15:40–16:00 Security vulnerabilities in AI-generated JavaScript: A comparative study of large language models

D. Aydın and Ş. Bahtiyar

16:00–16:20 Cyber resilience strategies throughout the system development lifecycle

G. Deffenbaugh and S. Kameneni

16:20–16:40 A reinforcement learning approach to multi-parametric input mutation for fuzzing

M. L. Uwibambe, A. Tyagi, and Q. Li

16:40–17:00 Metamorphic relation prediction for security vulnerability testing of online banking applications

K. Rahman, A. M. Reinhold, and C. Izurieta

15:20–17:00 **Session WS4: CYPRES workshop**

Chair: Mathaios Panteli, University of Cyprus (CY)

Room: Hall 3

15:20–16:00 [Invited talk] AI for natural hazard resilience: Standards, early warning systems, and risk reduction in a changing climate

E. Xoplaki

16:00–16:20 Quantifying cascading impacts of natural hazards on power-communication interdependent networks

B. V. Venkatasubramanain, C. Laoudias, and M. Panteli

16:20–16:40 Towards a new taxonomy of infrastructures: Implications for resilience

J. Palma Oliveira, D. Antunes, B. Rosa, D. Garcia Sanchez, A. Sarroeira, and A. Cardoni

16:40–17:00 Beyond technical skills: Human, emotional, and resilience demands in CSIRT operations

D. Antunes, A. Salgado, V. Figueiredo, N. Oliveira, J. Ferreira, J. G. Santos, and J. Palma Oliveira

15:20–17:00 Session TUT4: IEEE CSR tutorials

Room: Hall 4

15:20–17:00 Mobile forensics fundamentals

S. Harding

20:00–21:00 Welcome cocktail

Location: Tholos Bar

Tuesday, 05 Aug. 2025

08:40–10:00 **Session CSR9: Cyber threat intelligence**

Chair: Mehdi Akbari Gurabi, Fraunhofer FIT / RWTH Aachen University (DE)

Room: Hall 1

08:40–09:00 Enhancing cyber threat intelligence sharing through data spaces in critical infrastructures

M. Akbari Gurabi, Ö. Sen, N. Rahimidanesh, A. Ulbig, and S. Decker

09:00–09:20 CTI-GEN: A framework for generating STIX 2.1 compliant CTI using generative AI

A. Papoutsis, A. Dimitriadis, D. Kavallieros, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, and G. Meditskos

09:20–09:40 ThreatSpider: CTI-driven semi-automated threat modelling for cybersecurity certification

A. Amro and G. Kavallieratos

09:40–10:00 A structured process for scenario-based gamification of cyber threat intelligence for space system security

M. Kriesten, M. Thinyane, and D. Ormrod

08:40–10:00 **Session CSR10: Privacy technologies**

Chair: Weijie Niu, University of Zurich UZH (CH)

Room: Hall 2

08:40–09:00 DP-Tabula: Differentially private synthetic tabular data generation with large language models

W. Niu, Z. Zhang, A. Huertas, C. Feng, J. Von Der Assen, N. Nezhadsistani, and B. Stiller

09:00–09:20 LDP3: An extensible and multi-threaded toolkit for local differential privacy protocols and post-processing methods

B. K. Balioglu, A. Khodaie, and M. E. Gursoy

09:20–09:40 Budget-conscious differentially private aggregation of power data timeseries

F. Kserawi and G. Ghinita

09:40–10:00 Evaluating smart home privacy: The relationship between encrypted sensor data and occupancy prediction through machine learning

S. Mohanty, D. Papadopoulos, and C. Schindelhauer

08:40–10:00 Session WS5: IOSEC workshop

Chair: Kostas Lampropoulos, University of Patras (GR)

Room: Hall 3

08:40–08:40 Welcome by the chairs

K. Lampropoulos and C. Oprisa

08:40–09:20 [Invited talk] Cybersecurity engineering in the age of AI

C. Oprisa

09:20–09:40 Attacking the DLMS/COSEM advanced metering infrastructure

I. Papadopoulos, D. Merkouris, C. Dalamagkas, N. Nikoloudakis, and A. Arvanitis

09:40–10:00 SecAwarenessTruss: A federated cyber range solution for critical infrastructures

M. Smyrlis, E. Floros, N. Nikoloudakis, E. Stavrou, D. Merkouris, A. Arvanitis, G. Spanoudakis, S. E. Papadakis, G. Potamos, and S. Stavrou

08:40–10:00 Session WS6: CRE workshop

Chair: Nicholas J. Multari, Indiana University (US)

Room: Hall 4

08:40–08:40 Welcome by the chairs

N. J. Multari and R. McQuaid

08:40–09:00 Cybersecurity for sustainability: A path for strategic resilience

J. Saveljeva, I. Uvarova, L. Peiseniece, T. Volkova, J. Novicka, G. Polis, S. Kristapsone, and A. Vembris

09:00–09:20 Strategic allocation of defence resources against multi-step cyberattacks using evolutionary game theory

J. Zhang and W. Wang

09:20–10:00 [Invited talk] Unveiling the invisible: Knowledge graph-driven discovery of hidden cascade risks in critical infrastructure supply chains

G. Sharkov

10:00–10:20 Coffee break

10:20–12:00 Session CSR11: 5G and beyond security

Chair: Dionysia Varvarigou, University of Patras (GR)

Room: Hall 1

10:20–10:40 An efficient methodology for real-time risk and impact assessment in 5G networks

D. Varvarigou, K. Lampropoulos, O. Koufopavlou, S. Denazis, and P. Kitsos

10:40–11:00 A comprehensive 5G dataset for control and data plane security and resource management

B. Nugraha, M. Hajizadeh, T. Niehoff, A. Venkatesh Jnanashree, T. V. Phan, D. Triantafyllopoulou, O. Krause, M. Mieth, K. Moessner, and T. Bauschert

11:00–11:20 A preliminary ontology for 5G network resilience: Hybrid threats, risk reduction, compliance

R. A. Paskauskas

11:20–11:40 MiniLib: A flow analysis-based approach for attack surface reduction through software debloating

L. Kopanias, P. Sotiropoulos, N. Kolokotronis, and C. Vassilakis

11:40–12:00 NetPacketformer: Real-time, context-aware network intrusion detection with transformers

A. Domi, C. Zonios, G. Tatsis, A. Drosou, and D. Tzovaras

10:20–12:00 **Session CSR12: Privacy technologies**

Chair: Aytaj Badirova, University of Göttingen (DE)

Room: Hall 2

10:20–10:40 Efficient and privacy-preserving authentication using verifiable credentials

A. Badirova, S. D. Varnosfaderani, and R. Yahyapour

10:40–11:00 CONSENTIS – An innovative framework for identity and consent management for EU digital and data strategies

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

11:00–11:20 Trusted identity authentication for digital scholarship participants based on verifiable credential

X. Wu, Z. Wu, and H. Li

11:20–11:40 FE4MQTT – Using functional encryption to improve the privacy in publish-subscribe communication schemes

M. Fischer and R. Tönjes

11:40–12:00 Offloading key switching on GPUs: A path towards seamless acceleration of FHE

O. Papadakis, M. Papadimitriou, A. Stratikopoulos, M. Xekalaki, J. Fumero, and C. Kotselidis

10:20–12:00 **Session WS7: IOSEC workshop**

Chair: Kostas Lampropoulos, University of Patras (GR)

Room: Hall 3

10:20–10:40 ATHENA: A federated architecture for cross-border cybersecurity operations and situational awareness

A. Peratikou, E. Charalambous, P. Smyrli, and S. Stavrou

10:40–11:00 Privacy-preserving classification of partially encrypted feature vectors using multi-key homomorphic encryption

D. E. Petrean and R. Potolea

11:00–11:20 A hybrid transformer–LLM pipeline for function name recovery in stripped binaries

R. Petrache and C. Lemnaru

11:20–11:40 Fraud detection in Web content using machine learning and natural language processing

A. Dance, A. Fraticiu, and C. Oprisa

11:40–12:00 DISTIL: Digital identities for the evaluation of job skills

D. Kasimatis, P. Papadopoulos, W. J. Buchanan, C. Chrysoulas, S. Sayeed, A. Mylonas, and N. Pitropakis

10:20–12:00 Session WS8: CRE workshop

Chair: Rosalie McQuaid, MITRE Corporation (US)

Room: Hall 4

10:20–10:40 Addressing the economics of critical national infrastructure (CNI) security

S. A. Shaikh

10:40–11:20 [Invited talk] Learning to adapt: The role of AI in shaping maritime cybersecurity

G. Raicu

11:20–12:00 [Invited talk] Towards crypto agility in complex software systems

V. Lotz

12:00–12:40 Session KNT2: IEEE CSR keynote speakers

Chair: Emanuele Bellini, University of Roma Tre (IT)

Room: Main Hall

12:00–12:40 Digital twins for trustworthy autonomy

F. Flammini

12:40–13:40 Lunch break

Location: Elia restaurant

13:40–15:00 **Session CSR13: Critical infra resilience**

Chair: Elizabete Citskovska, Riga Technical University (LV)

Room: Hall 1

13:40–14:00 Mapping of maritime ecosystem components in the cybersecurity landscape
E. Roponena, S. Lielbārde, E. Citskovska, A. Brilingaitė, L. Bukauskas, and R. Pirta

14:00–14:20 Space cyber risk management: Desired properties
E. Ear, B. Bailey, and S. Xu

14:20–14:40 The notional risk scores approach to space cyber risk management
E. Ear, B. Bailey, and S. Xu

14:40–15:00 A proposal for an ontology to enhance IT architecture resilience
B. Mbaye, M. Mejri, and P. Saha Fobougong

13:40–15:00 **Session CSR14: Post-quantum security**

Chair: Daniel Berger, German Aerospace Center (DE)

Room: Hall 2

13:40–14:00 Post-quantum cryptography for maritime systems
D. Berger, A. Lye, A. Maidl, J. Stoppe, and A. Windhorst

14:00–14:20 Post-quantum security evaluation of aeronautical communications
K. Spalas and N. Kolokotronis

14:20–14:40 Indepth analysis of a side-channel message recovery attack against FrodoKEM
P. A. Berthet

14:40–15:00 Optimizing network services with quantum dynamic programming and Grover's search
E. Zeydan, J. Mangues Bafalluy, Y. Turk, A. Aydeger, and M. Liyanage

13:40–15:00 **Session WS9: CRIRM workshop**

Chair: Michalis Smyrlis, Sphynx (GR)

Room: Hall 3

13:40–13:40 Welcome by the chairs

M. Smyrlis and G. Spathoulas

13:40–14:00 CYBERUNITY: A federated architecture for next-generation cybersecurity training

C. Lal, A. V. Grammatopoulos, M. Takaronis, M. M. Yamin, G. Spathoulas, and C. Xenakis

14:00–14:20 Modelling attack and defense scenarios on federated cyber ranges

M. M. Yamin and B. Katt

14:20–14:40 From concept to deployment: An AI assistant for generating and configuring cyber range scenarios

G. S. Rizos, N. Kopalidis, N. Mengidis, A. Lalas, and K. Votis

14:40–15:00 LLM-powered intent-based categorization of phishing emails

E. Eilertsen, V. Mavroeidis, and G. Grov

13:40–15:00 **Session WS10: CRE workshop**

Chair: Nicholas J. Multari, Indiana University (US)

Room: Hall 4

13:40–14:20 [Invited talk] Mitigating biased, brittle and baroque generative AI

M. T. Maybury

14:20–15:00 [Panel discussion] AI/ML and it's ramifications on cyber security and resilience

G. Sharkov, M. T. Maybury, V. Lotz, G. Raicu, and CRE authors

Panel moderator: Rosalie McQuaid

15:00–15:20 **Coffee break**

15:20–17:00 **Session CSR15: Cyber-physical systems security**

Chair: Marzieh Kordi, IMT School for Advanced Studies Lucca (IT)

Room: Hall 1

15:20–15:40 Ontology-driven threat modeling analysis of CPSs

M. Kordi and N. Maunero

15:40–16:00 Towards safety and security testing of cyberphysical power systems by shape validation

A. Geiger, I. Hacker, Ö. Sen, and A. Ulbig

16:00–16:20 Strategic interactions in multi-sensor networks against false data injection

V. Bonagura, C. Foglietta, S. Panzieri, F. Pascucci, and L. Badia

16:20–16:40 Knowledge systematization for security orchestration in CPS and IoT systems

P. Nguyen, H. Song, R. Dautov, N. Ferry, A. Rego, E. Rios, E. Iturbe, V. Valdes, A. R. Cavalli, and W. Maloulli

16:40–17:00 Cybersecurity-oriented digital twins: A double-edged sword or a game changer?

S. Abdullahi and S. Lazarova Molnar

15:20–17:00 **Session CSR16: Attack graphs modeling**

Chair: Muhammad Zeshan Naseer, KTH Royal Institute of Technology (SE)

Room: Hall 2

15:20–15:40 Informed defense: How attacker profiles transform vulnerability assessments

M. Z. Naseer, V. Fodor, and M. Ekstedt

15:40–16:00 Application and evaluation of a substation threat modeling language for automatic attack graph generation

E. Rencelj Ling and M. Ekstedt

16:00–16:20 Vulnerability assessment combining CVSS temporal metrics and Bayesian networks

S. Perone, S. Guarino, L. Faramondi, and R. Setola

16:20–16:40 Integrating cyber threat intelligence into threat modeling for autonomous ships using PASTA and MISP

M. Erbas, J. Vanharanta, J. Paavola, L. Tsiopoulos, and R. Vaarandi

16:40–17:00 PASTA threat modeling for cyber resilience and COLREG compliance in autonomous ship systems

M. Erbas, G. Visky, O. Maennel, L. Tsiopoulos, and R. Vaarandi

15:20–17:00 Session WS11: CRIRM workshop

Chair: Michalis Smyrlis, Sphynx (GR)

Room: Hall 3

15:20–16:00 [Invited talk] From cyber ranges to cyber-physical ranges

S. Katsikas

16:00–16:20 ERMIS: A cybersecurity market assurance and insurance-as-a-service

A. Paragioudakis, M. Smyrlis, and G. Spanoudakis

16:20–16:40 The challenges of cyber-insurance: The case of Greece

E. Vergis, E. Aliberti, and S. Asteriou

16:40–17:00 Cyber insurance in emerging European markets: A case study of Greece and Cyprus

D. Smyrli, V. Kakariaris, and M. Smyrlis

15:20–17:00 Session WS12: SECMAN-6G workshop

Chair: Gueltoum Bendiab, University of Freres Mentouri – Constantine 1 (DZ)

Room: Hall 4

15:20–15:20 Welcome by the chairs

G. Bendiab, B. Brik, and B. A. S. Al-rimy

15:20–15:40 Zero-trust and reinforcement learning for secure federated intelligence in 6G edge networks

G. Bendiab, M. Guerar, H. Haiouni, and L. Verderame

15:40–16:00 Evaluating forensic log readiness in simulated 6G networks

S. Rizvi, B. A. S. Al Rimy, N. Anjum, and A. Kanta

16:00–16:20 DLT-EVA: Hardening O-RAN auditing and digital evidence preservation through blockchain

K. Ntouros, E. Poulitsis, S. Brotsis, K. P. Grammatikakis, and N. Kolokotronis

16:20–16:40 AI-enhanced hybrid CFAR for 6G integrated sensing and communication (ISAC)

K. Belhi, S. Chabbi, and G. Meriem

16:40–17:00 Federated learning for securing medical imaging against deepfakes in 6G smart hospitals

R. Verdy Ricard, E. Perales, M. A. Labiod, G. Bendiab, and Y. Chenoune

20:00–22:00 Gala dinner & Awards

Location: Thalassa restaurant or Athina hall

Wednesday, 06 Aug. 2025

08:40–10:00 **Session CSR17: Intrusion detection**

Chair: Zeba Khanam, BT Security Research (UK)

Room: Hall 1

08:40–09:00 A novel GNN-based approach for detection of prompt injection attacks

G. Jadhav, A. K. Singh, Z. Khanam, and R. Hercock

09:00–09:20 SafetilBERT: An efficient and explained LLM for IoMT attacks classification

M. Niang, H. Nakouri, and F. Jaafar

09:20–09:40 Design and implementation of a tool to improve error reporting for eBPF code

R. Rizza, R. Sisto, and F. Valenza

09:40–10:00 HyperDtct: Hypervisor-based ransomware detection using system calls

J. Von Der Assen, A. Huertas Celdran, J. M. Lüthi, J. M. Jorquera Valero, F. Enguix, G. Bovet, and B. Stiller

08:40–10:00 **Session CSR18: Autonomous vehicle security**

Chair: Yaman Qendah, University of Passau (DE)

Room: Hall 2

08:40–09:00 Driving resilience: Assessing security incidents' criticality in autonomous vehicles

Y. Qendah and S. Katzenbeisser

09:00–09:20 Cybersecurity mesh architecture for electric vehicle charging infrastructure

R. Bohara, M. Ross, and O. Joglekar

09:20–09:40 Wicked problem, parsimonious solution: Securing electric vehicle charging station software

E. Sheppard, Z. Wadhams, D. Arford, C. Izurieta, and A. M. Reinhold

09:40–10:00 TPKey: Using TPMS signals for secure and usable intra-vehicle device authentication

O. Achkar, L. Nissen, S. Raza, R. Shirsat, N. Klingensmith, G. Zouridakis, and K. I. Lee

08:40–10:00 Session WS13: CYBERSHIELD workshop

Chair: Sophia Karagiorgou, UBITECH Ltd (GR)

Room: Hall 3

08:40–09:00 Welcome by the chairs

S. Karagiorgou, G. Ledakis, and D. Ariu

09:00–09:20 CoEvolution: A comprehensive trustworthy framework for connected machine learning and secure interconnected AI solutions

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

09:20–09:40 On learning with confidentiality through encrypted AI pipelines

T. Anastasiou, S. Iatropoulou, and S. Karagiorgou

09:40–10:00 Feature-enhanced deep learning models for cyber-physical system security

J. Vaughn, K. Roy, and Y. Acquaah

08:40–10:00 Session WS14: HACS workshop

Chair: Peter Langendoerfer, IHP GmbH Leibniz Institute for High Performance Microelectronics & BTU Cottbus-Senftenberg (DE)

Room: Hall 4

08:40–09:00 Welcome by the chairs

P. Langendoerfer, C. Bobda, and N. Sklavos

09:00–09:20 Atomic patterns: Field operation distinguishability on cryptographic ASICs

A. A. Sigourou, Z. Dyka, P. Langendoerfer, and I. Kabin

09:20–09:40 Protection of the digital circuitry of a single-slope ADC against side-channel attacks

K. Ahmad, E. Öztürk, C. Körpe, H. Yang, J. Yang, K. Tihaiya, R. Tran, G. Dündar, V. Mooney, and K. Ozanoglu

09:40–10:00 Miti-CAT: Mitigating power side-channel vulnerabilities in FPGA-based CNN accelerators through distributed convolution computation

J. He and M. Zwolinski

10:00–10:20 Coffee break

10:20–12:00 Session CSR19: Intrusion detection

Chair: Giovanni Ciaramella, Institute for Informatics and Telematics, National Research Council of Italy (IT)

Room: Hall 1

10:20–10:40 Explainable ransomware detection through static analysis and machine learning

G. Ciaramella, F. Martinelli, A. Santone, and F. Mercaldo

10:40–11:00 Evasive ransomware attacks using low-level behavioral adversarial examples

M. Hirano and R. Kobayashi

11:00–11:20 Evasion of deep learning malware detection via adversarial selective obfuscation

C. Greco, M. Ianni, A. Guzzo, and G. Fortino

11:20–11:40 From one network to another: Transfer learning for IoT malware detection

K. Bosinaki, D. Natsos, G. Siachamis, and A. L. Symeonidis

11:40–12:00 C2-based malware detection trough network analysis using machine learning

M. Martijan, V. Krinickij, and L. Bukauskas

10:20–12:00 Session CSR20: Security assessment

Chair: Lea Muth, Freie Universität Berlin (DE)

Room: Hall 2

10:20–10:40 A machine learning approach to automate greybox testing

A. Hijazi, D. Mezher, E. Zeidan, and C. Bassil

10:40–11:00 Large scale cyber security log classification using semi-supervised clustering

P. Cai, M. Lazarescu, S. T. Soh, and R. Ryan

11:00–11:20 An approach for a supporting multi-LLM system for automated certification based on the German IT-Grundschutz

L. Muth and M. Margraf

11:20–11:40 Classification of software vulnerability artifacts using public Internet data

L. Ambrus De Lima, E. Rabello Ussler, M. A. Santos Bicudo, D. Sadoc Menasché, A. Kocheturov, and G. Srivastava

11:40–12:00 Using topic modeling and LLMs to recommend CAPEC attack patterns: A comparative study

U. Moore, X. Yuan, and H. Moradi

10:20–12:00 Session WS15: CYBERSHIELD workshop

Chair: Sophia Karagiorgou, UBITECH Ltd (GR)

Room: Hall 3

10:20–10:40 A PUF-based root-of-trust for resource-constrained IoT devices

E. N. Sassalou, S. Vasileiadis, S. A. Kazazis, G. Protogerou, N. Varvitsiotis, D. S. Karras, A. Giannetsos, and S. Tsintzos

10:40–11:00 Trust or bust: Reinforcing trust-aware path establishment with implicit attestation capabilities

N. Fotos, S. Vasileiadis, and T. Giannetsos

11:00–11:20 CYRUS – A personalised, customised, work-based training framework for enhanced cyber-security skills across industrial sectors

E. Frumento, K. Lange, and A. Golfetti

11:20–11:40 C-Shield: A holistic solution for secure end-to-end Kubernetes multi-cluster management and online threat mitigation using LLMs

S. Kalafatidis, G. Kitsos, and N. Papageorgopoulos

11:40–12:00 Hypervisor-based double extortion ransomware detection method using Kitsune network features

M. Hirano and R. Kobayashi

10:20–12:00 **Session WS16: HACS workshop**

Chair: Peter Langendoerfer, IHP GmbH Leibniz Institute for High Performance Microelectronics & BTU Cottbus-Senftenberg (DE)

Room: Hall 4

10:20–10:40 A hardware-efficient AEAD stream cipher based on a hybrid nonlinear feedback register structure

A. Allahverdi and V. Mooney

10:40–11:00 SpectreShield: Design and analysis of Spectre countermeasures on RISC-V using gem5

M. Khan, M. Mushtaq, R. Pacalet, and L. Apvrille

11:00–11:20 Acceleration of McEliece cryptosystem with instruction set extension for RISC-V

S. Kennedy and B. Halak

12:00–12:40 **Session KNT3: IEEE CSR keynote speakers**

Chair: Nicholas Kolokotronis, University of the Peloponnese (GR)

Room: Main Hall

12:00–12:40 Adversarial bypasses on detection engines, from code to binaries

C. Patsakis

12:40–13:40 **Lunch break**

Location: Elia restaurant

13:40–15:00 **Session CSR21: ICS attacks**

Chair: Myria Bouhaddi, Université du Québec en Outaouais (CA)

Room: Hall 1

13:40–14:00 Securing DRL-based traffic signal control against experience replay manipulation attacks

M. Bouhaddi

14:00–14:20 Data manipulation attack mitigation in power systems using physics-informed neural networks

S. Falas, M. Asprou, C. Konstantinou, and M. K. Michael

14:20–14:40 Anomaly identification in power systems using dynamic state estimation and deep learning

F. Alsaeed, E. Abukhousa, S. S. F. Syed Afroz, A. Qwbaiban, and A. S. Meliopoulos

14:40–15:00 The invisible threat: Simulating and analyzing the coordinated sensor manipulation attack (CSMA) on UAVs

S. Sadeghpour and P. Madani

13:40–15:00 Session CSR22: Multi-media attacks

Chair: Seyedeh Leili Mirtaheri, University of Calabria (IT)

Room: Hall 2

13:40–14:00 ResViT: A hybrid model for robust deepfake video detection

A. Aria, S. L. Mirtaheri, S. A. Asghari, R. Shahbazian, and A. Pugliese

14:00–14:20 Audio-deepfake: Generation methods, legitimate applications and the potential for misuse

G. Bendiab, K. Zeltni, and M. Bader El Den

14:20–14:40 DFA: Dynamic frame alteration for video manipulation attack in IoT environments

B. C. Nchelem, A. K. Singh, and H. Mouratidis

13:40–15:00 Session WS17: GAIA-SEC workshop

Chair: Fiammetta Marulli, Università della Campania “Luigi Vanvitelli” (IT)

Room: Hall 3

13:40–14:00 Welcome by the chairs

F. Marulli, F. Mercaldo, and A. De Benedictis

14:00–14:20 LLM-based generation of formal specification for run-time security monitoring of ICS

G. Raptis, M. T. Khan, C. Koulamas, and D. Serpanos

14:20–14:40 Explainable malware detection by means of federated machine learning

G. Ciaramella, F. Martinelli, A. Santone, and F. Mercaldo

14:40–15:00 An explainable method for access control policies classification

L. Petrillo, F. Martinelli, A. Santone, and F. Mercaldo

13:40–15:00 Session WS18: CVC workshop

Chair: Giovanni Gaggero, University of Genova (IT)

Room: Hall 4

13:40–14:00 Welcome by the chairs

M. A. Rahman, G. Gaggero, and K.-K. R. Choo

14:00–14:20 VPTaaS: An AI-driven cybersecurity framework for connected vehicles — Concept, validation, and feasibility study

S. W. Tan, M. A. Rahman, N. Refat, and P. Pillai

14:20–14:40 Cyber threat intelligence for smart vehicles

G. Asenov and E. Apeh

14:40–15:00 CyberVehiCare: A testbed for cybersecurity of vehicle to everything (V2X) automotive systems

M. A. Rahman, T. Sze Wei, M. S. Sohail, G. B. Gaggero, F. Patrone, M. Marchese, and P. Pillai

15:00–15:20 Coffee break

15:20–17:00 Session CSR23: Autonomous cyber-defence

Chair: Clemente Izurieta, Montana State University (US)

Room: Hall 1

15:20–15:40 Accounting for the impact of real-world data and costs in autonomous cyber defence

A. Neal, A. Acuto, P. Green, C. Lear, N. Hare, and S. Maskell

15:40–16:00 Reducing human-induced label bias in SMS spam with context-enhanced clustering (CEC)

G. Shu Fuhnwi, A. M. Reinhold, and C. Izurieta

16:00–16:20 A multi-level user identity authentication scheme based on environmental detection

N. Zeeshan, L. L. Spada, and M. Bakyt

16:20–16:40 Machine learning model complexity as a mitigation strategy against industrial espionage through membership inference attacks

R. Dautov, H. Song, C. Schaefer, S. Kim, and V. Pietsch

16:40–17:00 Sunburst vapor – A cybersecurity prompted case study of national-scale organizational transformation

E. Moore, S. Fulton, T. Amador, R. Mancuso, I. Martinez, and D. Likarish

15:20–17:00 Session WS19: GAIA-SEC workshop

Chair: Fiammetta Marulli, Università della Campania "Luigi Vanvitelli" (IT)

Room: Hall 3

15:20–15:40 Efficient classification of partially faked audio using deep learning

A. Alali, G. Theodorakopoulos, and A. Emad

15:40–16:00 Data generation and cybersecurity: A major opportunity or the next nightmare?

F. Marulli, L. Campanile, M. Bifulco, S. Carbone, and G. Ragucci

16:00–16:20 Exploratory analysis of key factors for a sustainable green transition and EU regulatory compliance in companies

F. Marulli, A. Balzanella, R. Verde, R. Mattera, and G. Borrata

15:20–17:00 Session WS20: CVC workshop

Chair: Giovanni Gaggero, University of Genova (IT)

Room: Hall 4

15:20–15:40 Cybersecurity for connected vehicle networks: Leveraging sampled network traffic beyond the CAN protocol

A. Yehezkel and E. Elyashiv

15:40–16:00 Detection of C-V2X spoofing attacks using physical layer features and graph neural networks

D. Greco and M. S. Sohail

16:00–16:20 Integration of forensic analysis and event data recorders in automotive regulation: A proposed approach

F. B. Soomro, R. Caviglia, G. B. Gaggero, and M. Marchese

15:20–17:00 Session WS21: EPES-SPR workshop

Chair: Panagiotis Radoglou-Grammatikis, University of Western Macedonia (GR)

Room: Hall 2

15:20–15:20 Welcome by the chairs

P. Sarigiannidis, P. Radoglou-Grammatikis, and D. Pliatsios

15:20–15:40 Detection of masquerade attacks on protection of digital substations using real-time measurements

M. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael

15:40–16:00 Evaluating 5G-enabled EV charging infrastructure's resilience through stealthy cyber-attacks

D. Psaltis, K. Ntouros, A. Lekidis, S. Brotsis, and N. Kolokotronis

16:00–16:20 Surrogate-guided adversarial attacks: Enabling white-box methods in black-box scenarios

D. C. Asimopoulos, P. Radoglou Grammatikis, P. Fouliras, K. Panitsidis, G. Efstathopoulos, T. Lagkas, V. Argyriou, I. Kotsiuba, and P. Sarigiannidis

16:20–16:40 Fortified control-plane encapsulation with session-key derivation for secure IP mesh routing

G. Amponis, P. Radoglou Grammatikis, T. Lagkas, V. Argyriou, A. Sarigiannidis, N. Kazakli, T. Boufikos, and P. Sarigiannidis

16:40–17:00 Neural cryptanalysis of lightweight block ciphers using residual MLPs

C. Eleftheriadis, G. Andronikidis, A. Lytos, E. Fountoukidis, P. A. Karypidis, T. Lagkas, V. Argyriou, I. Nanos, and P. Sarigiannidis

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΛΟΠΟΝΝΗΣΟΥ
UNIVERSITY of the PELOPONNESE

UNIVERSITY OF
PORTSMOUTH

MITRE