IEEE CSR 2026

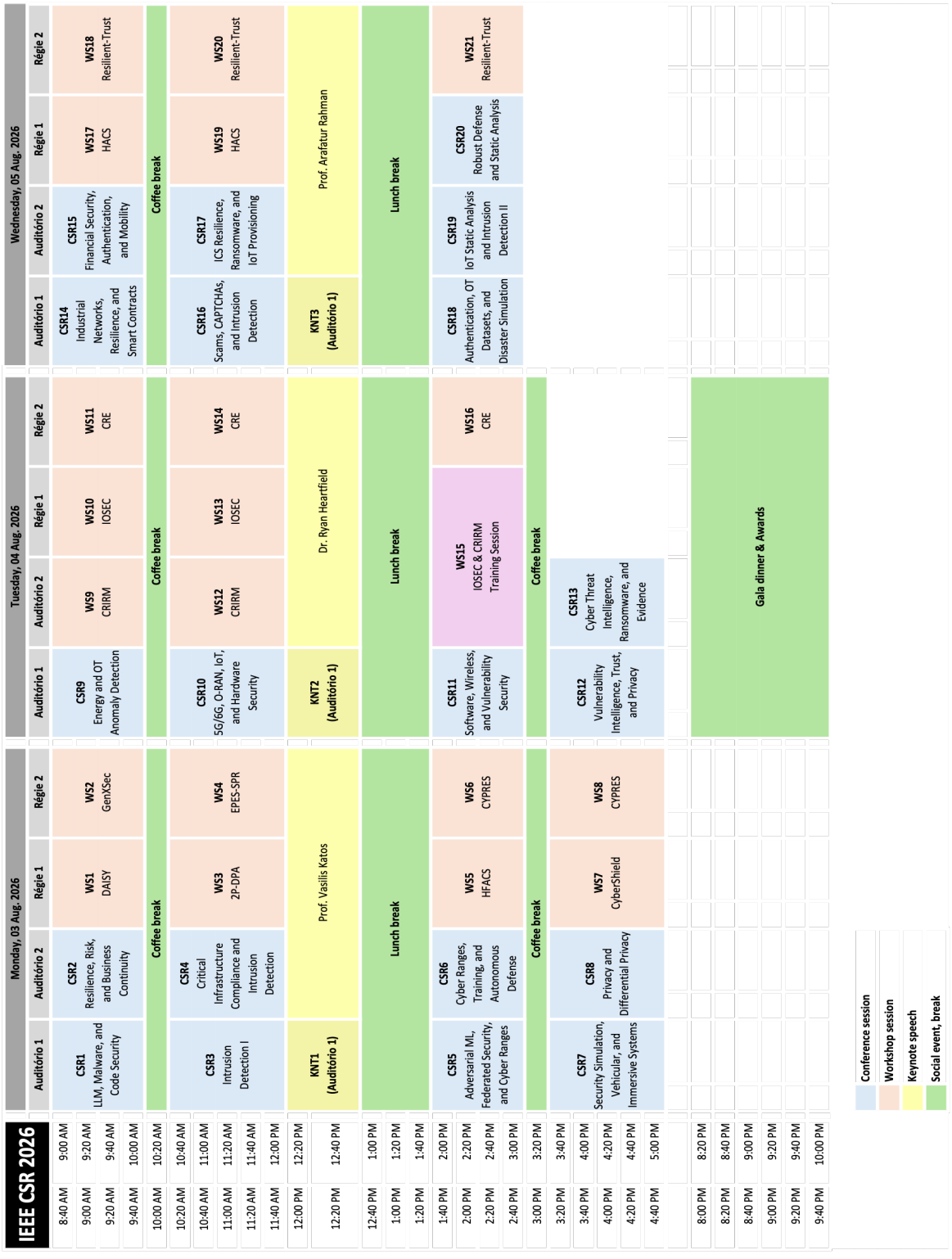
IEEE

IEEE SMC Systems, Man, and Cybernetics Society

LOGOS RI RESEARCH&INNOVATION

Program Handbook

Conference program overview



Monday, 3rd August 2026

08:40–10:00 **Session CSR1: LLM, Malware, and Code Security**

Chair: Alfonso Camblor-Garcia

Room: Auditorio 1

08:40–09:00 Towards Robust LLM-Enabled Fuzzing: Enhancing Test Generation Prompts via Execution Feedback

Marie Louise Uwibambe, Qinghua Li, Yanjun Pan

09:00–09:20 Semantic Preprocessing for LLM-based Malware Analysis

Benjamin Marais, Tony Quertier, Grégoire Barrué

09:20–09:40 COGENT: A Framework for Studying LLM-Guided Adaptive Evasion in Endpoint Security

Ayman Kanso, Hussein Bakri, Ali Chehab, Ali Al-Azwar

09:40–10:00 An Attacker-Oriented Evaluation of OLLVM Obfuscation Resilience Against LLM Deobfuscation

Anton Tkachenko, Gencer Erdogan

08:40–10:00 **Session CSR2: Resilience, Risk, and Business Continuity**

Chair: Almut Herzog

Room: Auditorio 2

08:40–09:00 IT & OT Resilience Challenges and Requirements

Jassim Happa, Konstantinos Mersinas, Endika Gil-Uriarte, Stefano Bianchi, Jorge Bernal Bernabe, Panagiotis Douris, Jose Ramon Almagro Clemente

09:00–09:20 Optimizing Business Continuity: RTO/RPO Selection and ROI-Driven Optimization

Idriss Nguepi Nguefack, Mejri Mohamed

09:20–09:40 Dynamic Risk Assessment by Bayesian Attack Graphs and Process Mining

Francesco Vitale, Simone Guarino, Stefano Perone, Massimiliano Rak, Nicola Mazzocca

09:40–10:00 Resilience Optimization in Complex Systems Using Granular Semantic Neural Networks

Eustathios Triantafellou, Aikaterini Kanta, Rinat Khusainov, Alexander Gegov

08:40–10:00 **Session WS1: DAISY**

Room: Regie 1

08:40–09:00 Beyond IID: Cross-Domain Zero-Day Evaluation of Learning-Based Models for Cyber Threat Detection

Zahra Pooranian, Adil Chaudhry, Rahim Taheri, Fabio Martinelli

09:00–09:20 A Policy-Based Intrusion Detection and Response System for Secure 5G/6G Networks

Mo Adda, Gueltoum Bendiab, Jibrilla A. Tanimu, Prajwal Netkal Sathish , Rinat Khusainov, Stavros Shiaeles

09:20–09:40 Belief-Function-Based Trust Assessment for AI-Aided Tactical Systems: Methodology and Evaluation

Yekta Turk, Engin Zeydan, Luis Blanco, Madhusanka Liyanage

09:40–10:00 Preparing an AI-Augmented SIEM for the EU Cyber Resilience Act: A Practitioner Case Study

Georgios Koutidis, Nikolaos Kekatos, Marina Korgiala Karyda, Alexios Lekidis, and Tom Nianios

08:40–09:40 **Session WS2: GenXSec**

Room: Regie 2

08:40–09:00 LLM-based Proactive Identification of Phishing Domains through Zero-Shot Classification

Simon Baco, Richard Plny, Karel Hynek

09:00–09:20 Uncertainty-Aware Augmentation of Cybersecurity Knowledge through Semantic Entropy

Jacopo Talpini, Vito Cianchini, Matteo Ciniselli, Alice Piemonti, Omran Ayoub

09:20–09:40 Explainable Rule Mining of IPv6 Extension-Header Presence Patterns from Paired-Vantage Captures

Priyanka Sinha, Stylianos Basagiannis, Antonio Bruto da Costa, Nikolaos Kekatos, Alexios Lekidis, Pabitra Mitra, Tom Nianios, Elpiniki Papageorgiou

10:00–10:20 **Coffee break**

10:20–11:40 **Session CSR3: Intrusion Detection I**

Chair: Anton Tkachenko

Room: Auditorio 1

10:20–10:40 Reliable Intrusion Detection via Conformalized Tabular Foundation Models

Thomas Zöller, Alexander Lawall

10:40–11:00 Evaluating Tabular Representation Learning for Network Intrusion Detection

Muhammad Usman Butt, Andreas Hotho, Daniel Schlör

11:00–11:20 LLM-Based Network Intrusion Detection: a Performance Study

Lorena Mehavilla, Maria Rodriguez, Jose Garcia, Ondrej Rysavy, Alvaro Alesanco

11:20–11:40 DARE: A Framework for Drift-Aware Robust Explanations in Unsupervised Intrusion Detection

Beny Nugraha, Thomas Bauschert

10:20–11:40 **Session CSR4: Critical Infrastructure Compliance and Intrusion Detection**

Chair: Benjamin Marais

Room: Auditorio 2

10:20–10:40 A Cybersecurity Conformance Testing Platform For Energy Telecontrol Devices

Elsa Corniani, Mauro Giuseppe Todeschini, Giovanna Dondossola

10:40–11:00 A Standardizable Design for Attack Tree Modeling of Smart Grid Cyber Attacks

Almut Herzog, Simon Rudi, Ömer Sen, Andreas Ulbig

11:00–11:20 From Legacy Documentation to OSCAL: An MCP-Based Agent Pipeline for Threat-Informed Continuous Compliance in Critical Infrastructure

Lea Muth, Marian Margraf

11:20–11:40 Analyzing and Mitigating Poisoning Attacks on Flow-Based Intrusion Detection in Military Networks

Florian Spelter, Johannes Loevenich, Tobias Hürten, Erik Adler, Maxime Schwarzer, Laurin Holz, Roberto Rigolin F. Lopes

10:20–12:00 **Session WS3: 2P-DPA**

Room: Regie 1

10:20–10:40 Visual OSINT-based Integrated Dashboard (VOID): Integrated OSINT-based digital asset platform

Gabriele Peluzzi, Stefano Perone, Simone Guarino, Luca Faramondi, Giovanni Bottazzi, Roberto Setola

10:40–11:00 A Privacy-Preserving Hybrid Machine Learning Pipeline for Regulated Environments: Architecture and Evaluation

Roberto Bagnato, Doriana Medic, Luca Vollero, Anna Sabatini, Tommaso Foglio Bonda, Manuele Innocenti, Marco Aldinucci

11:00–11:20 Performance Analysis and Comparison of Post-Quantum Cryptography Algorithms

Giovanni Maria Cristiano, Salvatore D'Antonio, Jonah Giglio, Alessandro Ortoli

11:20–11:40 When Less is More: Rethinking Differential Privacy Noise in Federated TinyML for IoT

Antonio Guerriero, Francesco Palmieri, Massimo Ficco

11:40–12:00 Quantifying the Privacy Posture of Operator-Side 5G/O-RAN Profiles

Nikolaos Kekatos, Apostolos Valiakos, Alexios Lekidis, Elpiniki Papageorgiou

10:20–12:00 **Session WS4: EPES-SPR**

Room: Regie 2

10:20–10:40 Synthetic Data Augmentation for Imbalanced EV Charging Network Security: An Empirical Study of Generative Models and Feature Transformation

Kosmas Lazaridis, Ioannis Topouzelidis, Ioannis Vagionas, Alexios Lekidis

10:40–11:00 RESILAGENT: A Three-Pillar Architecture for Cyber-Physical Resilience in Electrical Power and Energy Systems

Nikolaos Kekatos, Georgios Koutidis, Konstantinos Antonakopoulos, Stylianos Basagiannis, Sokratis Katsikas, Georgios Kavallieratos, Alexios Lekidis, Tom Nianios, Elpiniki Papageorgiou

11:00–11:20 Federated Detection of KNX Attacks with Network Flow Statistics in Industrial Environments

Christos Dalamagkas, Panagiotis Radoglou-Grammatikis, Antonios Sarigiannidis, Evangelos K. Markakis, Michail-Alexandros Kourtis, Thomas Lagkas, Georgios Th. Papadopoulos, Vasileios Argyriou, Panagiotis Sarigiannidis

11:20–11:40 Real-World Load and Wind Power Forecasting in Greek Island Energy Systems: A Deep Learning Perspective

Dimitrios Christos Asimopoulos, Vasileios Vitsas, Panagiotis Radoglou-Grammatikis, Maria Fotopoulou, Nikolaos Andriopoulos, Georgios Lampsidis-Tompros, Panagiotis Sarigiannidis

11:40–12:00 Securing the Grid Cross Domain Orchestration and Automated Threat Mitigation by ENFORCE

Pedro R. Tomas, Georgios P. Katsikas, Dimitris Manolopoulos, Wissam Mallouli, Dimitrios Klonidis, Luis Cordeiro

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

Chair: Alexios Lekidis

Room: Auditorio 1

12:00–12:40 Threat Landscaping in the AI Gold Rush Era: Capability, Hype, and the Human Layer

Vasilis Katos

12:40–13:40 **Lunch break**

13:40–15:00 **Session CSR5: Adversarial ML, Federated Security, and Cyber Ranges**

Chair: Elsa Corniani

Room: Auditorio 1

13:40–14:00 EAD-FL: Ensemble Anomaly Detection to Mitigate Poisoning Attacks in Federated Learning

Aimen Djemaa, Djamel Djenouri, Phil Legg

14:00–14:20 Deep Reinforcement Learning for Adaptive Trust in Peer-to-Peer Machine Learning

Myria Bouhaddi, Kamel Adi, Feriel Sadoun

14:20–14:40 k-MAn Sampling: Strategic Seed Selection for Label-Efficient Semi-Supervised Threat Detection in Security Operations Centers

Felix Waschke, Alejandro Guerra-Manzanares, Risto Vaarandi

14:40–15:00 ACTING: A Platform for Cyber Ranges Federation

Kyriakos Christou, Maria K. Michael, Stefano Taggi, Matteo Merialdo, Nikolai Stoianov, Vasilis Ieropoulos, Theofanis Eleftheriadis, Philippos Isaia, Eleni Darra, Ilias Koritsas, Antonis Voulgaridis, Giorgos Rizos, Dimitris Kavallieros, Stefanos Vrochidis, Konstantinos Votis, Liliana Medina, Joao Camacho, Tim Gerling, Aimilia Bantouna, Pavel Varbanov

13:40–15:00 **Session CSR6: Cyber Ranges, Training, and Autonomous Defense**

Chair: Konstantinos Mersinas

Room: Auditorio 2

13:40–14:00 Conceptualizing Cybersecurity Training Scenarios with Storytelling Integration: the Case of Seafarers

Agnė Brilingaitė, Evita Roponena, Elizabete Citskovska, Linas Bukauskas, Emīls Laucis, Sandra Lielbārde, Rūta Pirta

14:00–14:20 Cybersecurity Testbench and Dataset for Kubernetes-Based Command-and-Control Systems

Grace Harris, Sandip Roy, Benjamin Drozdenko

14:20–14:40 Autonomous Cyber Operations Gym for Training and Evaluating AI Models for Defence

Tobias Hürten, Johannes Loevenich, Florian Spelter, Erik Adler,

Laurin Holz, Maxime Schwarzer, Thies Moehlenhof, Roberto Rigolin

F. Lopes

14:40–15:00 DeepStage: Learning Autonomous Defense Policies Against Multi-Stage APT Campaigns

Trung Phan Van, Tri Nguyen Gia, Thomas Bauschert

13:40–15:00 **Session WS5: HFACS**

Room: Regie 1

13:40–14:00 Security Ontology to Support Security Event Severity Assessment

Evita Roponena, Inese Poļaka, Jānis Grabis

14:00–14:20 LLM-Augmented SAST Reports for Android: A Pilot Human Study of Vulnerability Triage

Panagiotis Binikos, Ashish Sai

14:20–14:40 The Amplifier Effect: Human-Factor Risks of AI-Suggested Correlation and Auto-Propagation in Multi-Framework GRC Self-Assessments

Nikolaos Kekatos, Michael Ioannou, Marina Korgiala-Karyda, Alexios Lekidis, Tom Nianios

14:40–15:00 Modeling Failure Dynamics in Time-Constrained Authentication Systems: Evidence of a Success Cliff in USSD Workflows

Aklile Seyoum Mamo, Amanuel Abebe Kebede, Anny Christelle Irakoze, Jema David Ndibwile

13:40–15:00 **Session WS6: CYPRES – Part 1: From Climate Risks to Secure Foundations**

Room: Regie 2

13:40–13:45 **Welcome & Opening Remarks**

Room: Regie 2

13:45–14:30 **Session 1: Climate Risk, Prediction & Socio-Technical Resilience**

Room: Regie 2

13:45–14:00 Science-Driven Multi-Hazard Early Warning for Cyber-Physical Infrastructure Resilience: The MedEWSa Framework

Elena Xoplaki, Enrico Scoccimarro, Jürg Luterbacher, Athina Kokonozi

14:00–14:15 A Topology-Aware Recurrent Deep Learning Framework for Multi-Horizon Flood Forecasting

Nikolaos Mitsiou, Dimitrios Kosmanos, Dimitra Kokkinou, George T. Karetsos

14:15–14:30 Technology-Augmented Public-Private-Academic Collaboration for Wildfire Resilience: The SupportCY Ecosystem

Marios Stavrou, Balaji V. Venkatasubramanian, Marilia-Evangelia Gogou, Mathaios Panteli, Efthymios Lekkas

14:30–15:00 **Session 2: Security, Control & Trust Foundations**

Room: Regie 2

14:30–14:45 Securing Two-Party Authentication of SCADA Commands in the Field using PUF-Encrypted Public-Key Signing
Kareem Ahmad, Arman Allahverdi, Vincent John Mooney III, Santiago Grijalva

14:45–15:00 Tamper-Evident Integrity Protection for IEC 61850 Configuration Artifacts Using Detached Signature Sidecars
Rasmus Holberg Seidelin Andersen, Mads Braae Jensen, Sani M. Abdullahi

15:00–15:20 **Coffee break**

15:20–17:00 **Session CSR7: Security Simulation, Vehicular, and Immersive Systems**

Chair: Felix Waschke

Room: Auditorio 1

15:20–15:40 Comparing Cybersecurity Simulators for Attack Defense: Code Review and Benchmarking

Pierre Lledo, Jean-Francois Lalande, Frédéric Majorczyk

15:40–16:00 Evaluating False Alarm and Missing Attacks in CAN IDS

Nirab Hossain, Pablo Moriano

16:00–16:20 Guerilla Number Plates: Spoofed Sensors, Deduced Data Rules

Andrew Peck, Iain Phillips, Yang Lu, Tim Watson

16:20–16:40 ActAuth: Interaction-Triggered, Continuous User Authentication for Controller-Free Virtual Reality

Haoran Li, Omar Achkar, George Zouridakis, Xin Fu, Kyu In Lee

15:20–16:40 **Session CSR8: Privacy and Differential Privacy**

Chair: Kyriakos Christou

Room: Auditorio 2

15:20–15:40 A Zero-Trust Architecture for Private Collective Forecasting

Alfonso Camblor-García, Manuel Fernandez-Veiga

15:40–16:00 Detection and Resolution of Periodic Artifacts in OpenDP's Discrete Laplace Sampler

Cesare Gerolimetto Fabrello, Valeria Rossi, Alberto Trombetta, Massimo Caccia

16:00–16:20 Empirical Analysis of Randomness Quality in Differential Privacy Mechanisms

Cesare Gerolimetto Fabrello, Valeria Rossi, Alberto Trombetta, Massimo Caccia

16:20–16:40 Operationalizing Privacy for Unstructured Medical Text Data: A Platform Approach with Privacy Risk Quantification

WEIJIE NIU, Han Yang, Francisco Enguix, Katharina O. E. M¨uller, Burkhard Stiller

15:20–17:00 **Session WS7: CyberShield**

Room: Regie 1

15:20–15:40 Proactive Adversarial Defense Framework Integrating Lifecycle Robustness in Machine Learning Models for Cybersecurity

Prathmesh Desai, Aditya aa5718@srmist.edu.in, Gokulakrishnan D

15:40–16:00 Multi-Agent System for Automated Red Teaming Workflows: Methodology and Architecture

Ioannis Pastellas, Sophia Karagiorgou, Evangelos Kafantaris

16:00–16:20 ADAPT: Detection of Evolving APTs Across Domains via Continual Few-Shot Meta-Learning

Alifya Kayla Shafa Susanto, Ilham Achmad Fiqrin, Samuel Fricker

16:20–16:40 CYBERFORT: A Compliance-Chain Platform Operationalising the Cyber Resilience Act for SMEs

Nikolaos Kekatos, Georgios Koutidis, Michaela Curca, Angelos Fountoulakis, Marios Ioannou, Michael Ioannou, Elias Iosif, Paul Lacatus, Alexios Lekidis, Avgi Michael, Tom Nianios

16:40–17:00 Energy-Based Counterfactual Explanations for Cybersecurity: Comparative Insights Across Modern Explainable Artificial Intelligence Methods

Spyridon Evangelatos, Eleni Veroni, George Papadopoulos, Sophia Karagiorgou, Ioannis Pastellas, Panagiotis Sarigiannidis

15:20–14:00 Keynote Talk

Room: Regie 2

15:20–14:00 All Disasters Are Equal, but Some Are More Equal Than Others: Rethinking the Empirical Foundations of Community Resilience

Prof. José Palma-Oliveira

16:00–17:00 Session WS8: CYPRES – Part 2: From Intelligent Systems to Infrastructure Resilience

Room: Regie 2

16:00–16:15 Session 3: Intelligent & Autonomous System Resilience

Room: Regie 2

16:00–16:15 Cyber-Resilient Cooperative Context Awareness for Connected and Autonomous Vehicles Using Lightweight Sensing Checks and Multi-Agent Situational Awareness

Amalia Damianou, Grigoris Kalogiannis, Avraam Bardos, Dimitris Tsiktsiris, George Lazaridis, Antonios Lalas, Konstantinos Votis, Dimitrios Tzovaras

16:15–17:00 **Session 4: Resilient Communication & Infrastructure Platforms**
Room: Regie 2

16:15–16:30 Reusing Communication-Oriented RIS Codebooks for Localization in Resilient Programmable Wireless Environments

Maria Anna Pistela, Alexandros I. Papadopoulos, Dimitrios Tyrovolas, Antonios Lalas, Konstantinos Votis, Sotiris Ioannidis, George K. Karagiannidis, Christos Liaskos

16:30–16:45 Towards Emergency Communication During Disaster Wilderness: The SPARROW Paradigm

Konstantinos Roumpeas, Jonathan Hazell, Christina Michailidou, Nikos Papadakis, Pavlos Kosmidis, Eleni Palousi, Christos Laoudias, Alessandro Astolfi

16:45–17:00 A Containerized Living Lab for Modeling and Evaluating 5G Digital Breakdown Scenarios

Athanasios Papadakis, Antonios Lalas, Konstantinos Votis, Dimitrios Tzovaras

Tuesday, 4th August 2026

08:40–10:00 **Session CSR9: Energy and OT Anomaly Detection**

Chair: Hamed Fard

Room: Auditorio 1

08:40–09:00 Grid-Code-Aware Online Anomaly Detection for Grid-Following Converters under Attack

Benedikt Grüger, Helena Sax, Nasiru Umar Bagudu, Philip Jonas Franz, Hendrik Wingbermühle, Tobias Meuser, Björn Scheuermann, Gerd Griepentrog, Florian Steinke

09:00–09:20 ICS-Sense: Anomaly Detection through Physical Media for Industrial Control Systems

Ali Tekeoglu, Ian Hogan

09:20–09:40 Transformer-Based Joint Anomaly Detection and Load Disaggregation for Operational Technology Security

Jorge Rivas, Richard Alves, Preetha Thulasiraman, Giovanna Oriti

09:40–10:00 Impact Analysis of Cyber-Attacks on DC Microgrids

SAQIB ALI, Andrii Chub, Hayretdin Bahsi

08:40–10:00 **Session WS9: CRIRM**

Room: Auditorio 2

08:40–09:00 Cyber Range as a Service over Federated Cyber Range Platforms: Design, Requirements, and Open Challenges

Chhagan lal, Emmanouil Eleftherios Rompogiannakis, Georgios Spathoulas, Evangelos K. Markakis

09:00–09:20 PowerRanger: A Modular Cyber Range Platform for Smart Energy Systems

Vasilis Ieropoulos, Theofanis Eleftheriades, Kyriakos Christou, Philippos Isaia, Maria Michalopoulou, Angelos Marnerides, Christos Laoudias, Maria Michael

09:20–09:40 From Conceptual Scaffold to Prototype: A Standardized Zonal Architecture for Wi-Fi Security Training

Vyron Kampourakis, Efstratios Chatzoglou, Vasileios Gkioulos, Sokratis Katsikas

09:40–10:00 Using LLMs to Elicit Security Requirements for Service-Oriented Cyber Ranges

Michail Takaronis, Athanasia Kollarou, Georgios Kavallieratos, Vasileios Gkoulos, Sokratis Katsikas

08:40–09:40 **Session WS10: IOSEC**

Room: Regie 1

08:40–09:00 An EHDS-Compliant Health Data Pipeline Combining LLM/MCP-Mediated Parameter Derivation with Privacy Enhancing Technologies

George Alexandris, Nikos Kyriakoulis, Spyros Denazis, Dimitris Schizas, Vassiliki Andronikou, Nikos Piliouras

09:00–09:20 Compliant Yet Blind: Multi-Tenant Monitoring Gaps in IEC 62443

WOOWI KIM

09:20–09:40 Metadata-driven CACAO Playbook Recommendation for Incident Response

Evangelos Chanos, Konstantinos Fysarakis, Vasileios Mavroeidis, Mateusz Zych, Ioannis Papaefstathiou

08:40–10:00 **Session WS11: CRE**

Room: Regie 2

08:40–09:00 The CYBER-BRIDGE project: An AI-Powered Platform for Cross-Border Cybersecurity, Compliance and Forensics in the EU
Nikolaos Kekatos, Georgios Koutidis, Charalambos Bratsas, Stefan Bucur, Michaela Curca, Angelos Fountoulakis, Emilios Charalambous, Michael Ioannou, Paul Lacatus, Alexios Lekidis, Avgi Michael, Tom Nianios, Simona Purcaru, Antonios Voulgaridis, Alexandra-Mihaela Chirlejan

09:00–09:20 Hierarchical Security Monitoring for Edge-IoT: A Formal Methods Approach

Nikolaos Kekatos, Marinelio Chintri, Panagiotis Katsaros, Alexios Lekidis, Tom Nianios, Ioannis Seitoglou, Stylianos Basagiannis

09:20–10:00 Ready for Q-day: Post-Quantum Cryptography for Industrial-scale Software Systems

Mr. Volkmar Lotz

10:00–10:20 **Coffee break**

10:20–11:40 **Session CSR10: 5G/6G, O-RAN, IoT, and Hardware Security**

Chair: Ian Hogan

Room: Auditorio 1

10:20–10:40 SKYNET – Secure and resilient intelligent System for 6G Networked Services and Technologies

Nikos Kyriakoulis, Dionysia Varvarigou, Charis Dimopoulos, George Daniil, Nikolaos Filippatos, George Tsiamoulis, Agisilaos Kolliopoulos, Kostas Lampropoulos, Spyros Denazis, Argyro Chatzopoulou, Mays AL-Naday, Ciprian Oprisa

10:40–11:00 Cross-Layer Intrusion Detection in 5G O-RAN: Gains and Limits of Fusing Radio Telemetry with Network Flow Records

Hamed Fard, Ilya Komarov, Gerhard Wunder

11:00–11:20 A 5G-IoT Cyber Range Platform with Integrated Learning Modules

Stylianos Karagiannis, Sarantis Kalafatidis, Giannis Ledakis, Emmanouil Magkos, Christoforos Ntantogian

11:20–11:40 Toward Resilient 5G Networks: Comparative Analysis of Federated and Centralized Learning for RF Jamming Detection

Samhita Kuili, Mohammadreza Amini, Burak Kantarci

10:20–12:00 **Session WS12: CRIRM**

Room: Auditorio 2

10:20–10:40 Agent-Assisted Cyber-Range Authoring: From LLM-Generated Scenarios to Deployment

Notis Mengidis, Nikolaos Kopalidis, Georgios Rizos, Antonios Lalas, Konstantinos Votis

10:40–11:00 Competency- and Proficiency-Based Evaluation of Cyber Range Training: A Proposed Approach

Pilleriin Sara Lillemets

11:00–11:20 DRCRM: A Dynamic Framework for Regulatory and Certification Readiness for Cyber-Resilient Systems

George Alexandris, Vassiliki Andronikou, Nikolaos Piliouras

11:20–11:40 Rethinking Malware Classification: A Systematic Evaluation Grounded in Baseline Performance

Remus Petrache, Camelia Lemnaru, Ciprian Oprișa

11:40–12:00 How much detail it takes to fool an adversary? A testbed to evaluate honeytokens effectiveness

Anthi Petridou, Georgios Spathoulas

10:20–11:00 **Session WS13: IOSEC**

Room: Regie 1

10:20–10:40 Constrained-Action AI Remediation for SIEM/XDR via a NeMo-Guardrails Proxy

Georgios Koutidis, Nikolaos Kekatos, Tom Nianios, Alexios Lekidis

10:40–11:00 Extending Reinforcement Learning-Based Protocol Fuzzing for 5G Core Network Attack Dataset Generation

Nikolaos Vakakis, Antonios Lalas, Konstantinos Votis

10:20–11:40 **Session WS14: CRE**

Room: Regie 2

10:20–11:00 Risks and Mitigations in Generative and Agentic AI

Dr. Mark Maybury

11:00–11:40 Beyond SBOM: SOSBOM as a Knowledge-Graph Foundation for Value Chain Cyber Resilience

Dr. George Sharkov

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

Chair: Nicholas Kolokotronis

Room: Auditorio 1

12:00–12:40 Sustainable Cybersecurity in the Era of Hyperconnected Agentic AI and Cyber-Physical Systems

Ryan Heartfield

12:40–13:40 **Lunch break**

13:40–15:00 **Session CSR11: Software, Wireless, and Vulnerability Security**

Chair: Burak Kantarci

Room: Auditorio 1

13:40–14:00 Implementing Elliptic Curve Cryptography for Wireless Sensor Networks using Recursive Karatsuba-Ofman

Utku Gulen, Selcuk Baktir

14:00–14:20 Security Analysis of Bluetooth Low Energy Medical Device Telemetry

Mia Smith, Thomas C. Draper, Phil Legg

14:20–14:40 How Well Do SAST Tools Work Across Languages? An Empirical Study Using OCPP Implementations

Zachary Wadhams, Emma Sheppard, Dalton Arford, Clemente Izurieta, Ann Marie Reinhold

14:40–15:00 Unifying the Vulnerability Knowledge Space: A Graph-Based Approach

Connor Munson, Brittany Boles, Clemente Izurieta, Ann Marie Reinhold

13:40–15:05 **Session WS15: IOSEC & CRIRM Training Session**

Room: Auditorio 2

13:40–13:45 Welcome

No hardware requirements required for the training.

13:45–14:15 Presentation: Cyber Hygiene

Instructor: Michalis Smyrlis.

14:15–14:20 Q&A

14:20–14:30 Break

14:30–15:00 Presentation: CRA & CSA

Instructor: IOSEC – Kostas Lampropoulos.

15:00–15:05 Q&A

15:05 Closing & distribution of training keys
Up to 15 keys will be distributed on a first-come, first-served basis for dedicated Cyber Hygiene training.

13:40–15:00 **Session WS16: CRE**

Room: Regie 2

13:40–14:20 AI Twinning in Maritime Cyber Resilience

Dr. Gabriel Raicu

14:20–15:00 CRE Panel

Dr. Sharkov, Dr. Maybury, Mr. Lotz, Dr. Raicu, Dr. Paul Nielsen, and paper authors

15:00–15:20 **Coffee break**

15:20–16:40 **Session CSR12: Vulnerability Intelligence, Trust, and Privacy**

Chair: Selcuk Baktir

Room: Auditorio 1

15:20–15:40 Software Vulnerability Fix Prioritization for x/rApps

Loukas Kopanias, Stefanos Vlachos, Nicholas Kolokotronis, Costas Vassilakis

15:40–16:00 Packer Identification using Grayscale Images of Binaries

Rogério de Lemos, Pierre Mondon

16:00–16:20 Stochastic Modeling of Human-Machine Authentication Channels under Partial Information Leakage

Nilesh Chakraborty, Mohammad Zulkernine, Burak Kantarci

16:20–16:40 From 5G to 6G: A Systematic Review and Quantum-Resilient Blockchain-Augmented Federated Learning Framework for Privacy-by-Design in IoT Ecosystems

Norman Nelufule, Crestinah Mudau, Pertunia Senamela, Nokuthaba Siphambili

15:20–16:40 **Session CSR13: Cyber Threat Intelligence, Ransomware, and Evidence**

Chair: Stylianos Karagiannis

Room: Auditorio 2

15:20–15:40 Matching Privacy Mechanisms to Stakeholder Needs in Mobility-as-a-Service

Alyah Alfageh, Theo Tryfonas, Kopo Marvin Ramokapane, Hakan Erdol

15:40–16:00 Adaptive Trust for Coordinating Cyber Threat Intelligence in Coalition Environments

Maxwell Dondo

16:00–16:20 First-Hand Acquisition of Ransomware Data: A Practical Example

Emil Larsson, Meiko Jensen

16:20–16:40 Edge Networks Spidernet Integration for Weighting of IoT Digital Evidence

Soraya Harding, Mo Adda

Wednesday, 5th August 2026

08:40–10:00 **Session CSR14: Industrial Networks, Resilience, and Smart Contracts**

Chair: João Ferreira

Room: Auditorio 1

08:40–09:00 Heterogeneous Graph Fusion for Multi-Modal Industrial Anomaly Detection

Martin Nahalka, Marco Cook, Dimitrios Pezaros

09:00–09:20 HTPG: Hardware Trojan Detection based on Anomalies of Transient Behavior

Quentin Tual, Jean-Christophe Le Lann, Philippe Coussy

09:20–09:40 Implementation of Dynamic Microsegmentation for a Multi-Robot Network

Vishwam Raval, Jaewon Kim, Ravi Pattabhi, Sandip Roy

09:40–10:00 Large Language Models and Smart Contract Security in Autonomous Financial Systems

Halil Efe Aköz, Şerif Bahtiyar

08:40–10:00 **Session CSR15: Financial Security, Authentication, and Mobility**

Chair: Gregory Vsevolozhsky

Room: Auditorio 2

08:40–09:00 Dynamic On Demand Decoy Deployment Using MicroVMs

Mohammad Shariq Farooqui, Amit Kumar Singh, Pushpinder Kaur Chouhan, Zhan Cui

09:00–09:20 Risk-Adaptive Continuous Authentication for Mobile Endpoints Using Identity, Attention, and Observer Cues

Luigi La Spada, Nida Zeeshan, Makhabbat Bakyt, Sabyrzhan Atanov, Khuralay Moldamurat

09:20–09:40 A Flow-Level Risk Assessment Framework for Hybrid Post-Quantum Migration in Healthcare

Farhath Zareen, Arpit Sharma, Deepti Joshi, Jasmin Kaur

09:40–10:00 A Hashing-Assisted Framework for Visual Attack Detection in Connected and Autonomous Vehicles

Amalia Damianou, George Lazaridis , Grigoris Kalogiannis, Antonios Lalas, Konstantinos Votis, Dimitrios Tzovaras

08:40–10:00 **Session WS17: HACS**

Room: Regie 1

08:40–09:00 IHP Open Dataset for Horizontal SCA attacks against kP

Ievgen Kabin, Marcin Aftowicz, Alkistis Aikaterini Sigourou, Peter Langedoerfer, Zoya Dyka

09:00–09:20 Hierarchical Cross-File Detection of G-Code Tampering in Additive Manufacturing Pipelines

Yash Patel, Parag Rughani

09:20–09:40 Lightweight Stream Cipher Design for Post-Quantum Security using Product Registers

Arman Allahverdi, Amishi Mittal, Raghav Raghunath, Vincent Mooney, Santiago Grijalva

09:40–10:00 Active and Passive Attacks against TPM2-based Full Disk Encryption

Sven Freud, Lennart Hein, Dominik Klein

08:40–10:00 **Session WS18: Resilient-Trust**

Room: Regie 2

08:40–09:00 CISE-DualLoss for RF Device Fingerprinting of Model-Identical Radios

Nour Badini, Carlos Fernando Quiroga Ruiz, Fabio Patrone, Mario Marchese

09:00–09:20 Automating Pentesting through AI Agents: an Openclaw-based approach

Hadi Balaghi Eynalou, Giovanni Battista Gaggero, Danilo Greco, Fabio Patrone

09:20–09:40 A Blockchain-Secured Distributed Architecture for AI-Based Drone Detection

Yannis Formery, Jonathan Villain, Léo Mendiboure, Virginie Deniau, Christophe Gransart

09:40–10:00 Deep Learning-Based Jamming Detection in Wi-Fi Networks Using Raw I/Q Signals

Muhammad Saad Sohail, Enrico Sciacca, Enrico Ferrari, Nour Badini, Fabio Patrone, Mario Marchese

10:00–10:20 **Coffee break**

10:20–11:40 **Session CSR16: Scams, CAPTCHAs, and Intrusion Detection**

Chair: Amalia Damianou

Room: Auditorio 1

10:20–10:40 Securing the Lifeline: Enforcing Read and Write Access Control in Vehicular Safety Services

Muhammad Baqer Mollah, George Zouridakis, Kyu In Lee

10:40–11:00 A Distributed K-Nearest Neighbour Based on Decision Tree for Intrusion Detection

Tijana Markovic, Miguel Leon, Aikaterini Kanta

11:00–11:20 Automatic bypassing of image-based puzzle CAPTCHA using edge detection and template matching

Michael Yamsi Tchuindjang, Hamza Attak, Ian Johnson, Phil Legg

11:20–11:40 Uncovering Black-hat SEO based Fake E-commerce Scam Groups from Their Redirectors and Websites

Makoto Shimamura, Shingo Matsugaya, Keisuke Sakai, Kosuke Takeshige, Taiji Watanabe, Masaki Hashimoto

10:20–11:40 **Session CSR17: ICS Resilience, Ransomware, and IoT Provisioning**

Chair: Nikos Fotiou

Room: Auditorio 2

10:20–10:40 Cyber-Physical Resilience in ICS with IEC 62443

Natasha Edeh, Karl Waedt

10:40–11:00 Preservation-First vs. Analysis-First Approaches for Ransomware Mitigation

Junade Ali, Chris Hicks

11:00–11:20 Integrity Boundary Theory and Autonomous Defensive Maneuver Systems

Gregory Vsevolozhsky

11:20–11:40 A Formally Verified Provisioning Protocol for Low-Cost IoT Devices

Sana Gul, Matteo Busi, Riccardo Focardi, Flaminia Luccio, Francesco Palmarini

10:20–11:00 **Session WS19: HACS**

Room: Regie 1

10:20–10:40 A Versatile FPGA Architecture for ASCON Authenticated Encryption and Hashing

Konstantinos Paraskevopoulos, Nikolaos Alachiotis, Nicolas Sklavos

10:40–11:00 Throughput-Optimized and Efficient Hardware Accelerator for Base Extension in Fully Homomorphic Encryption

Selim Kırbıyık, Emre Koçer, Robin Geelen, Tolun Tosun, Florian Hirner, Ingrid Verbauwhede, Erkay Savaş

10:20–12:00 **Session WS20: Resilient-Trust**

Room: Regie 2

10:20–10:40 On-Chip AI-Driven Detection of Hardware Trojan-Based Covert Channels

Emilien Dole, Abdelrahman Emad Abdelazim, Hassan Aboushady, Haralampos-G. Stratigopoulos, Alán Rodrigo Díaz-Rizo

10:40–11:00 Protecting On-Chip Test Instrumentation: Resilient Trust Demonstrator

Joel Åhlund, Markus Törmänen, Erik Larsson

11:00–11:20 SEADIVE: A Secure Maritime Trust Architecture Based on Decentralized Identifiers and Verifiable Credentials

Nicolò Romandini, Alessandro Marchesano, Mario De Biase, Damiano Vallocchia, Lorenzo Lovito, Constantin Minciuna

11:20–11:40 Reliable and Secure PUF Extraction for Advanced SRAM Nodes

Shayesteh Masoumian, Noemie Beringuier-Boher, Sander Steeghs-Turchina, Andries Stam, Asmaa Kassimi, Karthik Keni Yerriswamy, Roel Maes, Said Hamdioui, Mottaqiallah Taouil

11:40–12:00 A Secure IoT SoC Architecture for Lifetime Trust in Ambient Office Devices

Asmaa Kassimi, Sander Steeghs-Turchina, Andries Stam, Noémie Beringuier-Boher, Roel Maes, Jean-Luc Nagel, Andreas Curiger, Sebastian Fernandez, Holger Bock, Boris Danev, Joel Åhlund, Erik Larsson, Markus Törmänen, Said Hamdioui, Mottaqiallah Taouil

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

Chair: Stavros Shiaeles

Room: Auditorio 1

12:00–12:40 From Connectivity to Cyber Resilience: Communication, AI and Cybersecurity for Cyber-Physical Vehicular Health Monitoring Systems

Arafatur Rahman

12:40–13:40 **Lunch break**

13:40–15:00 **Session CSR18: Authentication, OT Datasets, and Disaster Simulation**

Chair: Junade Ali

Room: Auditorio 1

13:40–14:00 Fast and Secure Simultaneous Authentication of Equals for WPA3

João Ferreira, André Zúquete, Hélder Gomes

14:00–14:20 Data4Cyber: Labeled Cyber-Physical Datasets for Distribution-Grid Management Systems Under Representative OT Attacks

Ömer Sen, Lennart Bader, Marawan Emara, Martin Serror, Benedikt Schwalm, Junichi Tsurumi, Tatsumi Oba, Tomohiro Izawa, Yoshihiro Ujiie

14:20–14:40 ZT-TOTP: A Zero-Trust–Aware Extension for Phishing-Resistant Time-Based One-Time Password

Patrick Mutabazi, Festus Edward Ndalama, Taenaka Yuzo, Kadobayashi Youki

14:40–15:00 HEPHAESTUS: A Physics-Informed Wildfire Framework for Real-Time Disaster Simulation

Philippos Isaia, Christophoros Leventis, Panayiotis Georgiou, Marios Stavrou, Balaji Venkatasubramanian, Christos Laoudias, Mathaios Panteli, Christos Panayiotou

13:40–15:00 **Session CSR19: IoT Static Analysis and Intrusion Detection II**

Chair: Luigi La Spada

Room: Auditorio 2

13:40–14:00 NHN as a Connectivity Enabler: a Risk Assessment Overview

Alessandra Galassi, Alessio Carmenini, Fabio Franchi

14:00–14:20 Towards Reliable Detection of Memory Vulnerabilities in IoT Software: An Enhanced Static Analysis Framework.

Salma Salem, Kai Lehniger, Peter Langendörfer, Milad Ghantous, Hassan Soubra

14:20–14:40 Enhancing Anomaly-Based Intrusion Detection Systems with Process Mining

Francesco Vitale, Francesco Grimaldi, Massimiliano Rak, Nicola Mazzocca

14:40–15:00 Zero Trust Architecture for ISO 20022 Cross-Border Payment Networks: Deterministic Sanctions Screening and Micro-Segmentation

Shehnaz Khan

13:40–14:40 **Session CSR20: Robust Defense and Static Analysis**

Chair: Makoto Shimamura

Room: Regie 1

13:40–14:00 Robustness Evaluation of Autonomous Cyber Defense Agents under Adversarial Strategy Variation

Silja Kluge, Laurin Holz, Tobias Hürten, Roberto Rigolin F. Lopes, Johannes Loevenich

14:00–14:20 Improving the Security of Containerized Workloads using Transparency and Traceability Services

Nikos Fotiou, Lefteris Georgiadis, Ignacio Lacalle, George Polyzos, Vasilios Siris

14:20–14:40 Context Guardian: LLM-Assisted Context-Aware Static Analysis for Vulnerability Detection

Edem Schaanning Agbo, Merve Astekin, Phu Nguyen, Arda Goknil

13:40–14:40 **Session WS21: Resilient-Trust**

Room: Regie 2

13:40–14:00 Impact of Compiler Optimizations on Side-Channel Leakage in AES Implementations

Asmaa Kassimi, Jorrit Van Drie, Rik Bieling, Said Hamdioui, Mottaqiallah Taouil

14:00–14:20 Cybersecurity Issues in AI Agents for Personal Devices: an Overview of Current Trends, Attack Surface and Risks

Danilo Greco, Giovanni Gaggero Battista, Md Arafatur Rahman, Nazmul Hussain

14:20–14:40 Machine-Learning Detection of Spoofing Attacks on Short-Range Radar Sensors Across IoT and Cyber-Physical Systems

Mohamad Ibrahim, Md Arafatur Rahman, Rahul Mourya, Muhammad Kamran Naeem, Rashed Al Amin, Roman Obermaisser


IEEE
IEEE
SMC
Technical Commitee
on Homeland Security
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΛΟΠΟΝΝΗΣΟΥ
UNIVERSITY of the PELOPONNESE
UNIVERSITY OF
PORTSMOUTH
TRUST-6G
UNIVERSITY OF THESSALY
FOUNDED 1984
DHLAB
Università Roma Tre
SUMMIT-TEC