Program

WEDNESDAY, 21 MAY 2025		
Time		
08:00-09:00	Registration	
09:00-09:30	**Conference Opening** ***Tatjana Welzer, General chair IFIP SEC 2025*** ***Mirjana Kljajić Borštnar, Slovenian Society INFORMATIKA*** ***Lili Nemec Zlatolas, Programme committee co-chair IFIP SEC 2025***	
09:30-10:30	**Invited Speaker** **Nastja Cepak, CREAPLUS, Slovenia** **Post-Quantum Cryptography and the Decade of Transition** Hall City A | Chaired by Lili Nemec Zlatolas	
10:30-11:00	Coffee break ☕	
11:00-12:40	**IFIP SEC session 1: Privacy-enhancing technologies** Hall City A | Chaired by Leon Strous	**WISE session 1: Workforce and Curriculum Development** Hall City B
	Advanced strategies for privacy preserving data publishing to improve multi-class classification. *Tibo Laperre, Jenno Verdonck, Kevin De Boeck, Michiel Willocx, and Vincent Naessens.*	WISE Opening Remarks
	COLIBRI: Optimizing Multi-Party Secure Neural Network Inference Time for Transformers. *Daphnee Chabal, Tim Muller, Eloise Zhang, Dolly Sapra, Cees de Laat, and Zoltán Ádám Mann.*	Expanding the Cybersecurity Workforce: Challenges, Current Practices and Future Directions in Attracting and Cultivating Multidisciplinary Talent. *Christos Kallonas; Eliana Stavrou.*
	SAAFL: Secure Aggregation for Label-Aware Federated Learning. *Aftab Akram, Harry N. H. Pham , Melek Önen, Clémentine Gritti.*	INFER: Enhancing Digital Forensics Education through Ready-to-Use Hands-on Labs with Portable Operating Environments. *Tran Ngoc Bao Huynh; Haowen Xu; Brian Almaguer; Jun Dai; Xiaoyan Sun.*
	"We've met some problems": Developers' Issues With Privacy-Preserving Computation Techniques on Stack Overflow. *Patrick Kühtreiber, Sabrina Heimermann, Sebastian Schillinger, and Delphine Reinhardt.*	An Evaluation Process for Tools that Build or Evidence Competency in Cybersecurity: Development and Lessons Learned. *Stephen Miller; Christopher Simpson; Eugene Vasserman; Susanne Wetzel.*
12:40-13:40	Lunch 🍝	
13:40-15:20	**IFIP SEC session 2: Emerging Threats and Countermeasures** Hall City A | Chaired by Edgar Weippl	**WISE session 2: Innovative Approaches to Cybersecurity Awareness** Hall City B
	CoolTest: Improved Randomness Testing Using Boolean Functions. *Jiří Gavenda and Marek Sýs.*	The Cyber Range Lite *Leonardo Martucci; Jonathan Magnusson; Tobias Vehkajärvi; Jonas Karlsson.*
	Uncovering Robot Joint-Level Controller Actions from Encrypted Network Traffic. *Cheng Tang, Diogo Barradas, Urs Hengartner, and Yue Hu.*	A Car Hacking Mini-Unit for High School Cybersecurity Education *Cooper Dean; Brian Almaguer; Timothy Buck; Nichole Kunkle; Christian Nguyen; Preet Patel; Anne Roberts; Marti Shirley; Huirong Fu; Xiaoyan Sun; Jun Dai.*
	Generating and Attacking Passwords with Misspellings by Leveraging Homophones. *Shiva Houshmand, Smita Ghosh, and Jared Maeyama.*	**Invited talk** **Cybersecurity Awareness via Physical Games** ***Steven Furnell***
	Facing the Challenge of Leveraging Untrained Humans in Malware Analysis. *Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Muhammad Ikram, Mohamed Ali Kaafar, Sean Lamont, and Daniel Coscia.*	
15:20-15:50	Coffee break ☕	
15:50-16:10	**WISE Workshop Intro: Advancing Digital Privacy Education: A Global Curriculum Initiative** ***Gurvirender Tejay; Tamara Bonaci; Travis Breaux; Ümit Cali; Ernesto Cuadros-Vargas; Sara Foresti; Andrew McGettrick; Rajendra Raj; Kai Rannenberg; Andrew Seely.*** Hall City A	
16:10-17:50	**IFIP SEC session 3: Industrial and Critical Infrastructure Security** Hall City A | Chaired by Doğan Kesdoğan	**WISE session 3: Gamification in Cybersecurity Education** Hall City B
	Artefact Provenance Graphs for Anomaly Inference in Industrial Control Systems. *Marco M. Cook and Dimitrios Pezaros.*	Loss Aversion and Fixed Reward in Gamified Cyber Security Training. *Nicole Carle; Jacques Ophoff; Lynsay Shepherd.*
	Certified Secure Updates for IoT Devices. *Alberto Tacchella, Emanuele Beozzo, Bruno Crispo, and Marco Roveri.*	Improving Cyber Security Incident Response: A Collaborative Tabletop Game Approach.

		Andreas Seiler; Ulrike Lechner.
	LSAST: Enhancing Cybersecurity through LLM-supported Static Application Security Testing. *Mete Keltek, Rong Hu, Mohammadreza Fani Sani, and Ziyue Li.*	Gamified Defence: Practical Guidelines for Combating Social Engineering Attacks. *Amandla Mpanza; Tapiwa Gundu; Lynn Futcher.*
	FRAMICS: Functional Risk Assessment Methodology for Industrial Control Systems. *Ahmed Elmarkez, Soraya Mesli-Kesraoui, Flavio Oquendo, and Pascal Berruet.*	Lucky the Fish Teaches Children About Phishing. *Given Mnisi; Gunther Drevin; Lynette Drevin.*
18:00-19:00	City tour 🏛️	
19:00-21:00	Welcome Reception at the Oldest Vine House – Wine tasting 🍷	

THURSDAY, 22 MAY 2025			
Time			
08:00-09:00	Registration		
09:00-10:00	**Invited Speaker** **Jaideep Vaidya, Rutgers University, USA – KBA award winner** **AI and Conceptions of Privacy** Hall City A | Chaired by Tatjana Welzer		
10:00-10:30	Coffee Break ☕		
10:30-12:10	**IFIP SEC session 4: Privacy protection** Hall City A | Chaired by Zoltán Ádám Mann		**WISE session 4: Workshop** Hall City B
	Post-Processing in Local Differential Privacy: An Extensive Evaluation and Benchmark Platform. *Alireza Khodaie, Berkay Kemal Balioglu, and M. Emre Gursoy.*		Workshop Advancing Digital Privacy Education: A Global Curriculum Initiative. *Gurvirender Tejay; Tamara Bonaci; Travis Breaux; Ümit Cali; Ernesto Cuadros-Vargas; Sara Foresti; Andrew McGettrick; Rajendra Raj; Kai Rannenberg; Andrew Seely.*
	Rubber Ducky Station: Advancing HID Attacks with Visual Data Exfiltration. *August See, Thimo Großendorf, Jona Laudan, and Mathias Fischer.*		
	PrivTru: A Privacy-by-Design Data Trustee Minimizing Information Leakage. *Lukas Gehring and Florian Tschorsch.*		
	Towards a lightweight and privacy-friendly Architecture for Online Advertising. *Maximilian Wittig and Doğan Kesdoğan.*		
12:10-12:40	Light lunch 🍝		
12:40-13:30	**IFIP SEC session 5: IoT security** Hall City A | Chaired by Vincent Naessens	**IFIP SEC session 6: Risk Management** Hall City C | Chaired by Marko Hölbl	**WISE session 5: Standards / Regulations** Hall City B
	Future-Proof Asynchronous IoT Backups: An Evaluation of Secure IoT Data Recovery Considering Post-Quantum Threats. *Dmytro Shvets, Edona Fasllija, Jakob Heher, and Stefan More.*	Time is money: A temporal model of cybersecurity. *Zoltán Ádám Mann.*	Regulatory Challenges in Cybersecurity – A Critical Analysis of the EU AI Act. *Frederic Tronnier; Sascha Löbner; Marie-Hermance Lacombe; Kai Rannenberg.*
	Checking the Impact of Security Standardization – A Case Study on Bluetooth LE Pairing of Internet-of-Things Devices. *Henrich C. Pöhls and Lukas Steffens.*	Update at Your Own Risk: Analysis and Recommendations for Update-related Vulnerabilities. *Ahmad B. Usman and Mikael Asplund.*	Exposing the Gaps: The State of Supply Chain Coverage in Current Security Standards. *Nico Mexis; Bjarne Lill; Yousef Doleh; Stefan Katzenbeisser.*
14:00-23:00	Half-day excursion to Ptuj and conference dinner at the Dominican Monastery in Ptuj 🏛️		

FRIDAY, 23 MAY 2025			
Time			
08:00-09:00	Registration		
09:00-10:40	**IFIP SEC session 7: Industrial and Critical Infrastructure Security** Hall City A | Chaired by Marcus Belder	**WISE session 6: Curriculum and Research Development** Hall City B	**WNDSS: Opening, Keynote, Session 1** Hall City C | Chaired by Zoltán Ádám Mann

	Data Transformation for IDS: Leveraging Symbolic and Temporal Aspects. *Enzo Zamaï, David Espes, Audrey C. Therrien, and Catherine Dezan.*	A Transdisciplinary Approach to Embedding Cybersecurity Across the Curriculum of an Undergraduate Computing Degree Program in South Africa. *Michael De Jager; Reolyn Heymann; Japie Greeff.*	Opening
	SAFARI: a Scalable Air-gapped Framework for Automated Ransomware Investigation. *Tommaso Compagnucci, Franco Callegati, Saverio Giallorenzo, Andrea Melis, Simone Melloni, and Alessandro Vannini.*	Using Attack Trees for Security Education and Training: Simplifying Threat Analysis. *Aliyu Tanko Ali; Damas Gruska.*	**Keynote** **Security Issues with Networked and Distributed Systems** ***Matt Bishop (University of California Davis, USA)***
	SAVA Deployment for Spoofed Source Attacks. *Wenjie Yang, Yong Tang, and Wenyong Wang.*	Integrating Security Concepts into Introductory Programming Courses. *Alina Torbunova; Ivan Porres.*	WNDSS Session 1: Security of Industrial Control Systems
	Lightweight and Persistent Remote Attestation: Leveraging a Continuous Chain of Trust in Software Integrity Measurements. *Florian Kohnhäuser, Nicolas Coppik, Christian Göttel, and Sören Finster.*	CSEC Foundations Guidelines. *Matt Bishop; Philip Huff; Jun Dai; Melissa Dark.*	A Novel Evidence-Based Threat Enumeration Methodology for ICS. *Can Özkan and Dave Singelée.*
10:40-11:10	Coffee break ☕		
11:10-12:10	**Invited Speaker** **Reinhard Posch, Institute of Applied Information Processing and Communications at Graz University of Technology, Austria** **eIDAS2 – a milestone for security in public services?** Hall City A | Chaired by Kai Rannenberg		**WNDSS Session 2: Binary Protocols and Security of Smart Grids** Hall City C | Chaired by Joaquin Garcia-Alfaro
			Flatdc: Automatic Schema Reverse Engineering of FlatBuffers. *August See, Lilly Sell, Benedikt Ostendorf, and Mathias Fischer.*
			Security Metrics for False Data Injection in Smart Grids. *Moritz Volkmann, Sascha Kaven, and Volker Skwarek.*
12:10-13:10	Lunch 🍝		
13:10-14:50	**IFIP SEC session 8: Data and Application Security** Hall City A | Chaired by Marko Kompara	**WISE session 7: IFIP 11.8 WG AGM and closing session** Hall City B	**WNDSS Session 3: Resilience, Anonymity Networks, and Liveness Detection** Hall City C | Chaired by Alessandro Brighente
	How stealthy is stealthy? Studying the Efficacy of Black-Box Adversarial Attacks in the Real World. *Francesco Panebianco, Mario D'Onghia, Stefano Zanero, and Michele Carminati.*	Annual working group AGM open to all members and WISE participants.	A Quantum Algorithm for Assessing Node Importance in the st-Connectivity Attack. *Iain Burge, Michel Barbeau, and Joaquin Garcia-Alfaro.*
	Certifiably robust malware detectors by design. *Pierre-François Gimenez, Sarath Sivaprasad, and Mario Fritz.*		BERMUDA: A BPSec-Compatible Key Management Scheme for DTNs. *Fiona Fuchs, Felix Walter, and Florian Tschorsch.*
	"You still have to study" – On the Security of LLM generated code. *Andreas Schaad, Stefan Götz, and Dominik Binder.*		Impact Analysis of Sybil Attacks in the Tor Network. *Christoph Sendner, Dominik Schreider, and Alexandra Dmitrienko.*
	Identifying and Analyzing Vulnerabilities and Exploits in On-Premises Kubernetes. *Sunny Chowdhury and Florian Freund.*		Time-Aware Face Anti-Spoofing with Rotation Invariant Local Binary Patterns and Deep Learning. *Moritz Finke and Alexandra Dmitrienko.*
14:50-15:20	**Awards Session** **IFIP SEC 2026** **Conference Closing** ***Marko Hölbl, Organizing committee chair IFIP SEC 2025*** Hall City A		**WNDSS Session 4: IFIP WG11.4 Meeting & Closing Remarks** Hall City C | Chaired by Zoltán Ádám Mann
15:20-15:50	Farewell refreshments and last chats 🥪		