IFIP SEC/WISE Schedule

Tuesday 9th June 2026

Due to the on-going global situations, unfortunately, some delegates are unable to attend in-person.

= Pre-recorded presentation **= Live remote presentation (Teams)** **Name (bold/underline) = presenting author** **Name (bold) = attending author**

Time (AWST)	Grand River Ballroom West	Mt Newman	Pilbara
08:30-09:00	**Registration (foyer)** Arrival tea/coffee		
09:00-09:20	**Opening Ceremony** **Welcome to Country** *Noongar Elder, Mr Barry Winmar* **Welcome to IFIP SEC/WISE 2026** *General Chair: Helge Janicke* *TC11 Chair: Paul Haskell-Dowland*		
09:20-10:20	**Keynote** *Session Chair: Helge Janicke* Converging Disruptions, Compounding Risks: How Research becomes a Critical Capability for Organisations, Industry and Societal Resilience ***Dr Gayan Benedict, MIT CISR Industry Research Fellow, Partner PwC***		
10:20-11:00	**Break (foyer)**		
11:00-12:00	**Session 1: Data and Applications Security** *Session Chair: Ahmed Ibrahim* Cross-Network Transfer Learning for Cryptocurrency Fraud Detection ***Denizhan Dalgıç*** *and Şerif Bahtiyar* Clovery: Identifying Affected Versions in C/C++ Public Security Vulnerability Reports ***Duyeong Kim****, Jimin Kang, Yeonhee Kim, Seunghoon Woo and Heejo Lee*	**Session 2: AI for Cyber Security** *Session Chair: Marcus Belder* MLLM-IGDD: Instance-Guided Deepfake Detection via Multimodal Large Lan-guage Models ***Yanfei Tong****, Yiran He, Yun Cao, Yuqi Pang, Meineng Zhu, Xiahui Kuang and Zhendong Wu* MCTS-VUL: Self-Training Large Language Models via Monte Carlo Tree Search for Vulnerability Detection ***Jujie Wang****, Kangfeng Zheng, Bin Wu, Chunhua Wu, Yulin Yao, Jiaqi Gao and Minjiao Yang*	**Session 3: Experiential Learning in Cybersecurity** *Session Chair: Jacques Ophoff* WISE Opening *Conference Chair: Jacques Ophoff* *WG11.8 Chair: Erik Moore* Provoking Interest in Cybersecurity Using Physical Games ***Steven Furnell****, James Todd, Lucija Smid, Simon Castle-Green, and Xavier Carpent*
12:00-13:00	**Lunch (foyer)**		
13:00-14:30	**Session 4: Privacy, Identification, Authentication and Access Control** *Session Chair: Kai Rannenberg* Homogeneous Control of Security Functions via Cross-Domain Delegation *Nicola Poidomani,* ***Daniele Canavese****, Daniele Bringhenti, Fulvio Valenza and Matteo Repetto* PatMine: Advancing Cloud Security through Graph-based Context-Aware Access Pattern Mining *Vakkalagadda Satya Sai Prakash,* ***Srinivas Reddy Gopu*** *and Rajidi Satish Reddy* Privacy-Preserving Clinical Data De-Identification and Evaluation Framework Using Synthetic Data *Ebenezer Addo-Maclean,* ***Hatem Ahriz*** *and Shadi Hajar*	**Session 5: Cryptography** *Session Chair: Iqbal Sarker* Pepper: High-bandwidth and Scalable Anonymous Broadcast with Cryptographic Privacy *Chenghao Li and* ***Xianghang Mi*** Shape Before You Build: Secure Cryptographic Code Generation via Prompt Optimization *Zihan Ni,* ***Jialiang Dong****, Runtao He, Nan Sun, Willy Susilo, Surya Nepal and Siqi Ma* An Acceleration Framework for Privacy-Preserving Neural Network Inference Using Fully Homomorphic Encryption ***Fanqi Kong****, Ziming Zhao, Yongheng Li, Jing Wen, Shaoling Liang and Baohua Huang*	**Session 6: Experiential Learning in Cybersecurity** *Session Chair: Michael de Jager* A Simulation-Based Approach for the Training of TaHiTI Practitioners *Tebogo Mokoena and* ***Rudi Serfontein*** Investigating in a Post-Truth World: Multi-NPC Simulations for Digital Forensics Education ***Jarred Orfão*** *and Wai Sze Leung* A Design Science Approach to Modular Scenario Modeling for Cyber Security Exercises *Sandra Tomeschek,* ***Christoph Jungbauer****, and Christian Luidold*
14:30-15:00	**Break (foyer)**		
15:00-16:30	**Session 7: Network and Systems Security** *Session Chair: Tatjana Welzer* Reinforcement Learning-based Optimal Firewall Placement and Configuration (RL_OFPC) ***Zahra Torabi****, David Eyers and Veronica Liesaputra* AMPhitryon: Efficient Small Data Compression for Low-Bandwidth Covert Channels ***Steffen Wendzel****, Sebastian Zillien and* ***Sebastian Zander*** BRIDG-Q: Barren-Plateau-Resilient Initialisation with Data-Aware LLM-Generated Quantum Circuits ***Ngoc Nhi Nguyen****, Thai T Vu, John Le, Hoa Khanh Dam, Dung Hoang Duong and Dinh Thai Hoang*		**Session 8: Experiential Learning in Cybersecurity** *Session Chair: Danilo Gentile* Learning Through National Cybersecurity Competitions: An Evaluation of Honours Students' Experiences in the SANReN Cybersecurity Challenge ***Michael de Jager*** *and Lynette Drevin* Bridging the Curricula Gap: Integrating Indicators of Compromise into Cybersecurity Education *Daniel Braund and* ***Jacques Ophoff***

16:30-18:30

Welcome Reception (foyer)

with First Nations Cultural Artefact Presentation

ifip SEC 2026 PERTH AUSTRALIA

Wednesday 10th June 2026

ifip WISE 2026 PERTH AUSTRALIA

Time (AWST)	Grand River Ballroom West	Mt Newman	Pilbara
08:30-09:00	**Registration (foyer)** Arrival tea/coffee		
09:00-10:00	**Session 9: Data and Applications Security** *Session Chair: Edgar Weippl* Parser Instrumentation for Semantic-Aware Applicative Intrusion Detection ***Grégor Quetel**, Pierre-François Gimenez, Thomas Robert and Laurent Pautet* ▶ A Categorical Data Watermarking Scheme via Multi-Attribute Joint Distribution Preservation ***Hongxia Ma**, Jing Yu, Shuguang Yuan, **Jianing Wang** and Chi Chen*		**Session 10: Human Factors, Security Behavior and Cybersecurity Awareness** *Session Chair: Susanne Wetzel* Maybe Alice and Bob are the same? Cybersecurity Awareness Preferences Among Swedish Men and Women *Joakim Kävrestad, Erik Bergström, Nathan Clarke, and **Steven Furnell*** Unveiling Behavioral Phishing: a Study on Attack Strategies and User Decision-Making ***Danilo Gentile**, Gennaro Esposito Mocerino, Claudio Velotti, Luigi Gallo, Alessio Botta, and Giorgio Ventre*
10:00-10:30	**Break (foyer)**		
10:30-12:30	**Session 11: AI for Cyber Security** *Session Chair: Iqbal Sarker* Feature-Selective Representation Misdirection for Machine Unlearning ***Taozhao Chen**, Linghan Huang, Kim-Kwang Raymond Choo and Huaming Chen* Parameter-Efficient LLMs for Flow-Based Intrusion Detection ***Mamdouh Muhammad**, Anton Wunsch and Loui Al Sardy* Threat Model-Driven Test Framework for Security and Privacy of Agentic LLM Applications *Mario Raciti, Giampaolo Bella and **Dimitri Van Landuyt*** APART: Access Policy-AwaRe LLM Fine-Tuning ***Nouha Oualha***	**Session 12: Data and Applications Security** *Session Chair: Ahmed Ibrahim* ▶ VulnArrow: Data-Driven Vulnerability Root-Cause Analysis with Differential Sample Generation ***Hongwei Li**, Wenmeng Zhang and Yongjun Wang* ▶ The Hidden Risk of Auto-Generated OpenAPI Specifications: An Analysis of WordPress Plugins and Lightweight Specification Correction ***Ohiremen Grace Oluwabunmi** and **Beom Heyn Kim*** ▶ BFA-Shield: A Resilient Collaborative Defense Framework for DNNs Against Bit-Flip Attacks ***Jianing Wang**, Xue Tian, **Hongxia Ma**, Jing Yu and Chi Chen* Hop-Decayed Influence: New Vulnerabilities of Structural Auxiliary Indexing in GraphRAG Pipelines with LLM ***Jisung Park**, John Le and Heath Cooper*	**Session 13: Curriculum Design and Pedagogical Frameworks for Cybersecurity Education** *Session Chair: Erik Moore* A Framework and Checklist for Secure and Reflective Review of AI-Generated Code *Peter Idem, Johan van Niekerk, and **Petrus MJ Delport*** Improving Workforce Readiness Through Research Education *Agnes Chan and **Susanne Wetzel*** CyberEducation 5.0: Transforming Cybersecurity Education into CyberSecPro *Narges Arastouei, Cristina Alcaraz, Abdelkader Magdy Shaaban, Ruben Rios, and **Kai Rannenberg*** ▶ A Governable GenAI Tutoring Framework for Cybersecurity Education ***Madhav Mukherjee**, John Le, and Yang-Wai Chow*
12:30-13:30	**Lunch (foyer)**		
13:30-15:00	**Session 14: Privacy, Identification, Authentication and Access Control** *Session Chair: Leon Strous* Revealing Power Imbalances in Data Privacy: A Privacy Privilege Model ***May Alhajri**, Carsten Rudolph and Gillian Oliver* Adaptive Attribute Inference Attack: Exploiting Privacy Risks Under Adversarial Perturbations *Xinyu Liu, Yanrong Lu, Aohan Sun, Wencheng Yang, Yan Li and **Michael Johnstone*** Convolutional Auto-Encoder-Based Finger Vein Spoof Generation and Detection ***Kashif Shaheed** and Umair Ul Hassan*	**Session 15: Network and Systems Security** *Session Chair: Helge Janicke* ▶ Resource-Bounded Early Identification of Encrypted Video Traffic at Line Rate ***Chong Chen**, Lizhi Peng, Liang Jiao and Rui Li* ▶ AlertSAGE: Semantic-Aware Alert Graph Embedding for Cybersecurity Incident Discovery ***Shuang Jiang**, Zhicheng Liu, Yijing Wang, Zhihao Zhang, Han Wang and Yueyue Hu* ▶ AutoSecGPU: Lightweight GPU-TEE Made Practical with Automatic Evidence Generation ***Fengyuan Yu**, Chenlin Huang, Renyu Yang, Hua Cheng, Yan Ding, Yuncong Ma, Keming Wang and Zhihang Zhang*	**Session 16: Workforce Readiness and Professional Development in Cybersecurity** *Session Chair: Rudi Serfontein* A Design-Oriented Onboarding Framework for Tier 1 SOC Analysts *Tom Perez, **Petrus Marthinus Jacobus Delport**, and Johan van Niekerk* Cybersecurity Job Skills Evolution in South Africa: Replication and Longitudinal Analysis ***Suné von Solms***
15:00-15:30	**Break (foyer)**		

15:30-17:00

Tour of Perth Mint (a four-minute walk from the hotel)

19:00-22:00

Conference Dinner (Grand River Ballroom East)

Thursday 11th June 2026

Time (AWST)	Grand River Ballroom West	Mt Newman	Pilbara
08:30-09:00	**Registration (foyer)** Arrival tea/coffee		
09:00-10:00	**WISE Keynote / KBA Award** *Session Chair: Jacques Ophoff* Information Security Research: A 35-year journey ***Professor Rossouw von Solms*** Presentation of KBA Award		
10:00-10:30	**Break (foyer)**		
10:30-12:00	**Session 17: AI for Cyber Security** *Session Chair: Marcus Belder* Is This Mission Possible? A Study on Developer Challenges in Using Generative AI for Secure Software Development in Industry *Sathwik Amburi,* ***Tiago Gasiba****, Tobias Fertig,* ***Ulrike Lechner*** *and* ***Maria Pinto-Albuquerque*** Unsupervised Graph Learning for Insider Threat Detection ***Simon Bertrand****, Pascal Germain and Nadia Tawbi* ONE-MS-1 : A Micro-Services Based Network Traffic Dataset **Pedro Tomás**, Jorge Proença, Tomás Dias, *Luis Rosa, Luís Cordeiro, Tarik Taleb and Tiago Cruz*	**Session 18: Cyber-Physical Systems Security** *Session Chair: Ahmad Mohsin* Robustness Analysis of Translation Tampering in Multi-Sensor Object Detection ***Mahdieh Safarzadehvahed*** *and Mohammad Zulkernine* Systematic Integration of Digital Twins and Constrained LLMs for Interpretable Cyber-Physical Anomaly Detection ***Konstantinos E Kampourakis****, Vasileios Gkioulos and Sokratis Katsikas* Cross-Modal Geometric Regularization for Multivariate Cybersecurity Anomaly Detection ***Sourav Rai****, Christophe Rodrigues, Thomas Czernichow, Damien Lescos and Nga Nguyen*	IFIP 11.8 WG AGM
12:00-13:00	**Lunch (foyer)**		
13:00-14:00	**Session 19: Cyber-Physical Systems Security** *Session Chair: Edgar Weippl* HASAC: Energy Adaptive Secure Firmware Updates for Critical IoT Systems ***Sayon Duttagupta*** ICSSPulse: A Modular LLM-Assisted Platform for Industrial Control System Penetration Testing ***Michail Takaronis****,* ***Athanasia Kollarou****, Vyron Kampourakis, Vasileios Gkioulos and Sokratis Katsikas*	**Session 20: Data and Applications Security** *Session Chair: Rossouw von Solms* Developing Security Metrics for Automated Compliance Checking ***Immanuel Kunz****, Nico Haas, Angelika Schneider and Christian Banse* Evaluation Framework for Multi-Channel Spoofing Detection Through Redesign of the ReMASC Corpus ***Takuo Yamaguchi****,* ***Sayaka Shiota*** *and Naohiro Tawara*	IFIP 11.8 WG AGM and WISE closing session
14:00-14:30	**Closing Ceremony** SEC Closing Ceremony Presentation of Awards COSE Best Paper Award Yves Deswarte Award (Best Student Paper) SEC27 Launch	*Setup for Corporates Compromised™ Workshop*	

14:30-16:30

Goodbye sundowner (foyer)

Delegates are invited to participate in the Corporates Compromised™ workshop running in the Mt Newman room with drinks available in the foyer.

Corporates Compromised™ Workshop (Mt Newman)

Helge Janicke, Ahmad Mohsin, Ahmed Ibrahim

About Corporates Compromised™

Corporates Compromised™ is a cyber security awareness training tool designed to equip staff with the knowledge and understanding of current cyber security risks facing organisations. Originally developed by the Cyber Security Cooperative Research Centre it is now maintained and developed by Janicke Consulting. The simulation walks through a realistic cyber security incident affecting a fictitious organisation, providing valuable insights and skills. You experience the process in real time, while learning core aspects of an effective cyber security strategy.

https://corporatescompromised.com.au/