Tentative- NordSec 2026 — Conference Programme

11–12 November 2026 · [Preben hornung stuen building 1422 132, Aarhus University, Aarhus]

Day 0 – Tuesday, 10 November 2026

Venue:

Time	Activity	Venue
18:00 – 20:00	Get together for people who arrive on Monday	To be announced

Day 1 — Wednesday, 11 November 2026

Venue:

Preben Hornung Stuen, building 1422 - 132
Richard Mortensen Stuen, building 1422 - 122

<table>
<tr><td>08:00–
09:00</td><td colspan="2">Registration</td></tr>
<tr><td>09:00–
09:30</td><td colspan="2">Conference opening</td></tr>
<tr><td>09:30–
10:30</td><td colspan="2">Keynote talk
Markus Miettinen (Faculty of Information Technology, University of Jyväskylä, Finland):
Topic: Whodunit in the age of AI? A Tale of Beautiful Models, Rogue Agents, Poison and the Mystery of the Trigger – How AI is shaping the field of cybersecurity research
Session chair: [To be announced]
Room: [To be announced]</td></tr>
<tr><td>10:30–
11:00</td><td colspan="2">Coffee break</td></tr>
<tr><td rowspan="2">11:00–
12:30</td><td>Session 1: Cryptography and Secure Computation
Session chair: [To be announced]
Room: [To be announced]</td><td>Session 2: Threat Intelligence, Adversarial Behavior, and Cybercrime
Session chair: [To be announced]
Room: [To be announced]</td></tr>
<tr><td>Thi Van Thao Doan, Olivier Pereira and Thomas Peters: MAYAsk: Swiss-Knife Extensions to the MAYA Logarithmic Shuffle Argument

Esra Yeniaras: QML-PipeGuard: Detecting Channel-Substitution Attacks on Quantum Machine Learning Pipelines in Untrusted Clouds</td><td>Nuriel Taha, Ubaid Ur Rehman and Jürgen Schönwälder: Label-Efficient DNS Tunneling Detection over DoH: An Empirical Study of Contrastive Self-Supervised Pretraining and Tree Ensembles

Stamatia Papageorgiou, Luca D'Este, Carlos E. Budde, Nicola Dragoni and Andrea Burattin: An Approach to Capture Attack Descriptions via a Controlled Natural Language</td></tr>
</table>

	Markku-Juhni Saarinen: HOVER: Higher-Order Vanishing Endomorphism Recovery	**Ilaria Giacometti, Radu Candea, Alberto Mongardini and Emmanouil Vasilomanolakis**: Realistic IP Camera Deception with Multi-Vendor Honeypots
12:30–13:30	Lunch	
13:30–15:00	**Session 3: AI, Agentic AI, and Human-Centered Security** **Session chair:** [To be announced] **Room:** [To be announced]	**Session 4: Software, Systems, and Web Security** **Session chair:** [To be announced] **Room:** [To be announced]
	Viggo Tellefsen Wivestad, Per Håkon Meland, Tron Vedul Tronstad, Femke B. Gelderblom and Marte Høiby: Does Dialect Diversity Protect Against Deepfake Vishing? Evidence from a Norwegian Listening Experiment **Jan-Niclas Hilgert, Michael Külper, Martin Lambertz and Jan Gruber**: When AI Takes Action: MCP Forensics from Evidence to Attribution	**William Bundgaard, Jacopo Mauro, Morten Jakobsen and Oliver Nordestgaard**: PipTemp: CI/CD Security Challenges in Constrained Environments **Ebraam Mesak, Shaoqi Jiang, Mohammad Mannan and Amr Youssef**: QLscanner: Finding GraphQL Vulnerabilities in the Wild **Nour Al-Satari, Mohammad Mannan and Amr Youssef**: Watching the Watchers: Privacy and Security Failures in Employee Monitoring Software
15:00–15:30	Coffee break	
15:30–17:00	**Session 5: IoT, Mobile, and Hardware Security** **Session chair:** [To be announced] **Room:** [To be announced]	**Session 6: Formal Methods, Verification, and Analysis** **Session chair:** [To be announced] **Room:** [To be announced]
	Simon Autechaud, Fabrizia Marrucco, Mosabbah Mushir Ahmed and Alieeldin Mady: Characterizing Electromagnetic Fault Injection Effects on Edge Neural Network Accelerators: An Empirical Case Study of the Google Coral Edge TPU **Tatjana Wingarz, Jeetesh Gupta, Lars Schumacher and Mathias Fischer**: SHIoT'26: A Specialized IoT Intrusion Detection Dataset for Smart Home Environments **Maciej Klimek, Adrian Listkiewicz, Szymon Szott and Mathy Vanhoef:** Revisiting Wi-Fi Management Frame	**Matteo Busi, Riccardo Focardi, Sana Gul and Flaminia Luccio**: Secure Key Management Policies in Tamarin **Azimjon Akhmadjonov, Ubaid Ur Rehman and Jürgen Schönwälder**: Stability-Aware Additive Refinement for Seccomp Profile Synthesis **Niels Pfau, Patrick Kochberger and Philipp Haindl**: Snapshot-Based Fuzzing for Complex Enterprise Applications: An Empirical Evaluation of Performance and Practicality

	Attacks: Extended Device Evaluation of SSID Confusion and SA-Query Vulnerabilities	
18:30	Conference dinner — restaurant Det Glade Vanvid	

Day 2 — Thursday, 12 November 2026

Venue:

Preben Hornung Stuen, building 1422 - 132
Richard Mortensen Stuen, building 1422 - 122

<table>
<tr><td>09:00–
09:30</td><td colspan="2">Registration</td></tr>
<tr><td>09:30–
10:30</td><td colspan="2">Keynote talk
Anders Møller (Computer Science, Aarhus University and Coana):
Topic: Program Analysis for Software Supply Chain Security
Session chair: [To be announced]
Room: [To be announced]</td></tr>
<tr><td>10:30–
11:00</td><td colspan="2">Coffee break</td></tr>
<tr><td rowspan="2">11:00–
12:30</td><td>Session 7: Privacy, Trust, and Data Protection
Session chair: [To be announced]
Room: [To be announced]</td><td>Session 8: Security Engineering, Governance, and Compliance
Session chair: [To be announced]
Room: [To be announced]</td></tr>
<tr><td>Judit Borcsiczky, Lukas Moog and Boel Nelson: Investigating Data Flows from Android Games

Bautista Marelli and Alejandro Russo: Schema-Driven Generation of Reconstructable Datasets from Aggregate Releases

Florian Foerster, Philipp Schubaur, Fabian Bley, Shih-Wei Li and Dominik Merli: Trust vs. Robustness: Denial-of-Service Impact on TLS Partitioning Strategies using TrustZone for Arm Cortex-A</td><td>Matiss Veigurs: Towards Community-Based Solutions for NIS2 Compliance: The Case of Latvian Essential and Important Entities

Alina Torbunova, Juuso Rytilahti, Erkki Kaila and Ivan Porres: Integrating Security into Introductory Programming with MISCPRO: A Quasi-Experimental Case Study

Toni Matthes and Zoltan Mann: PACE: Predictive Assessment of Common Vulnerabilities and Exposures for Capacity-Constrained Prioritization</td></tr>
<tr><td>12:30–
13:30</td><td colspan="2">Lunch</td></tr>
<tr><td rowspan="2">13:30–
15:00</td><td>Session 9: Security, Society, and Critical Infrastructures]
Session chair: [To be announced]
Room: [To be announced]</td><td></td></tr>
<tr><td>Marius Cotiga, Lene Tolstrup Sørensen and Edlira Dushku: SOK: Interoperability Gaps of Civilian and Military OT Cyber Resilience Frameworks

Elias Nechwatal, Dominik Brunke, Nicolai Kröger, Wolfgang Kellerer, Michael</td><td></td></tr>
</table>

	Meier, Michael Rademacher and Hartmut Koenig: RRC Ping-Pong: Pre-Authentication Denial-of-Service Loops in 4G and 5G **Roland Plaka, Mikael Asplund and Simin Nadjm-Tehrani**: Moving Target Defense in SDN-enabled EV Charging Networks	
15:00 - 15:30	Coffee break	
15:30–17:00	Panel Discussion From Lessons Learned to What's Next: Rethinking Cyber Security for a Changing World Best paper award Conference Closing	