NordSec 2026 — Conference Programme

11–12 November 2026 · Richard Mortensen Stuen and Preben Hornung Stuen, building 1422, Aarhus University, Aarhus
AU Conference Center, Fredrik Nielsens Vej 2-4, 8000 Aarhus C · Google Maps

Day 0 – Tuesday, 10 November 2026

Venue:

Time	Activity	Venue
From 18:00	Get together for people who arrive on Tuesday	Banken Foodhall, Kannikegade 4, 8000 Aarhus C (map)

Day 1 — Wednesday, 11 November 2026

Venue:

Richard Mortensen Stuen, building 1422 - 122 (keynotes, opening, closing and Sessions 1, 3, 5, 7, 9)
Preben Hornung Stuen, building 1422 - 132 (Sessions 2, 4, 6, 8)

<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
Room: Richard Mortensen Stuen (1422 - 122)</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: Abhishek Vaish
Room: Richard Mortensen Stuen (1422 - 122)</td></tr>
<tr><td>10:30–11:00</td><td colspan="2">Coffee break</td></tr>
<tr><td>11:00–12:30</td><td>Session 1: Cryptography and Secure Computation
Session chair: Anders Andersen
Room: Richard Mortensen Stuen (1422 - 122)
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
Markku-Juhani Saarinen: HOVER: Higher-Order Vanishing Endomorphism Recovery</td><td>Session 2: Threat Intelligence, Adversarial Behavior, and Cybercrime
Session chair: Boel Nelson
Room: Preben Hornung Stuen (1422 - 132)
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
Ilaria Giacometti, Radu Candea, Alberto Mongardini and Emmanouil Vasilomanolakis: Realistic IP Camera Deception with Multi-Vendor Honeypots</td></tr>
</table>

12:30–13:30	Lunch	
13:30–15:00	**Session 3: AI, Agentic AI, and Human-Centered Security** **Session chair:** Raimundas Matulevičius **Room:** Richard Mortensen Stuen (1422 - 122) **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	**Session 4: Software, Systems, and Web Security** **Session chair:** Aslan Askarov **Room:** Preben Hornung Stuen (1422 - 132) **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:** Christian Damsgaard Jensen **Room:** Richard Mortensen Stuen (1422 - 122) **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 Attacks: Extended Device Evaluation of SSID Confusion and SA-Query Vulnerabilities	**Session 6: Formal Methods, Verification, and Analysis** **Session chair:** René Rydhof Hansen **Room:** Preben Hornung Stuen (1422 - 132) **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 in Network Daemons **Niels Pfau, Patrick Kochberger and Philipp Haindl:** Snapshot-Based Fuzzing for Complex Enterprise Applications: An Empirical Evaluation of Performance and Practicality
18:30	Conference dinner — restaurant Det Glade Vanvid, Pakkerivej 2, 8000 Aarhus C (map)	

Day 2 — Thursday, 12 November 2026

Venue:

Richard Mortensen Stuen, building 1422 - 122 (keynotes, opening, closing and Sessions 1, 3, 5, 7, 9)
Preben Hornung Stuen, building 1422 - 132 (Sessions 2, 4, 6, 8)

09:00–09:30	Registration	
09:30–10:30	**Keynote talk** Anders Møller (Computer Science, Aarhus University and Coana): **Topic: Program Analysis for Software Supply Chain Security** **Session chair:** Aslan Askarov **Room:** Richard Mortensen Stuen (1422 - 122)	
10:30–11:00	Coffee break	
11:00–12:30	**Session 7: Privacy, Trust, and Data Protection** **Session chair:** Jacopo Mauro **Room:** Richard Mortensen Stuen (1422 - 122) **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	**Session 8: Security Engineering, Governance, and Compliance** **Session chair:** Abhishek Vaish **Room:** Preben Hornung Stuen (1422 - 132) **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
12:30–13:30	Lunch	
13:30–15:00	**Session 9: Security, Society, and Critical Infrastructures** **Session chair:** Christian Damsgaard Jensen **Room:** Richard Mortensen Stuen (1422 - 122) **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 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– 16:45	**Panel Discussion** **From Lessons Learned to What's Next: Rethinking Cyber Security for a Changing World** **Moderator:** Dieter Gollmann **Room:** Richard Mortensen Stuen (1422 - 122) **Panellists:** Markku-Juhani Saarinen, Nicola Dragoni and Boel Nelson *15:30 Opening remarks · 15:40 Panellists' statements · 15:55 Discussion and audience Q&A*
16:45– 16:55	**Announcement of NordSec 2027** Christian Damsgaard Jensen
16:55– 17:00	**Conference closing** Christian Damsgaard Jensen

Venue map

