

Technical program

Session A Join URL: <https://aalto.zoom.us/j/66423022236>

Meeting ID: 664 2302 2236

9:00 – 10:20 Session 1A

Runtime Implementations for Memory Safety in C

Nikola Nemeš

Memory vulnerability types, attacks, and mitigation methods

Alazar Alemayehu Abebaw

Micro-architectural Side-channel Attacks and Defenses

Ayoub Chouak

Recent Developments in Messaging Layer Security

Hamna Zahid

10:20 – 10:30 Short break

10:30 – 12:10 Session 2A

Adversarial machine learning attacks

Aleksandar Nedakovic

Software package management with SAT and other combinatorial search methods

Sofia Bogdanova

Web-based mobile augmented reality

Michal Czuper

Authorization with OAuth: security considerations, best practices and recent developments

Zara Wajid Butt

Games for elderly people

Emma Engblom

12:10 – 13:10 Lunch break

13:10 – 14:30 Session 3A

Protecting Memory Safety with ARM's Memory Tagging Extension and Pointer Authentication

Brent Carey

Security for Dynamic Host Configuration Protocol (DHCP)

Svitlana Chaplinska

Causal reasoning in Reinforcement Learning

Anupam Dahal

Machine Learning-based Traffic Flow Prediction

Nafis Kamal

14:30 – 14:40 Short break

14:40 – 16:00- Session 4A

A review of Deep Learning Methods in Traffic Flow Prediction

Tahsinur Rahman

Authentication and Authorization for Constrained Environments: A Survey

Adhirath Kabra

Adversarial machine learning attacks

Joseph Attieh

Web-based mobile Augmented Reality

Tomasz Czajewski