CDIS Cybercampus Spring Conference 2025

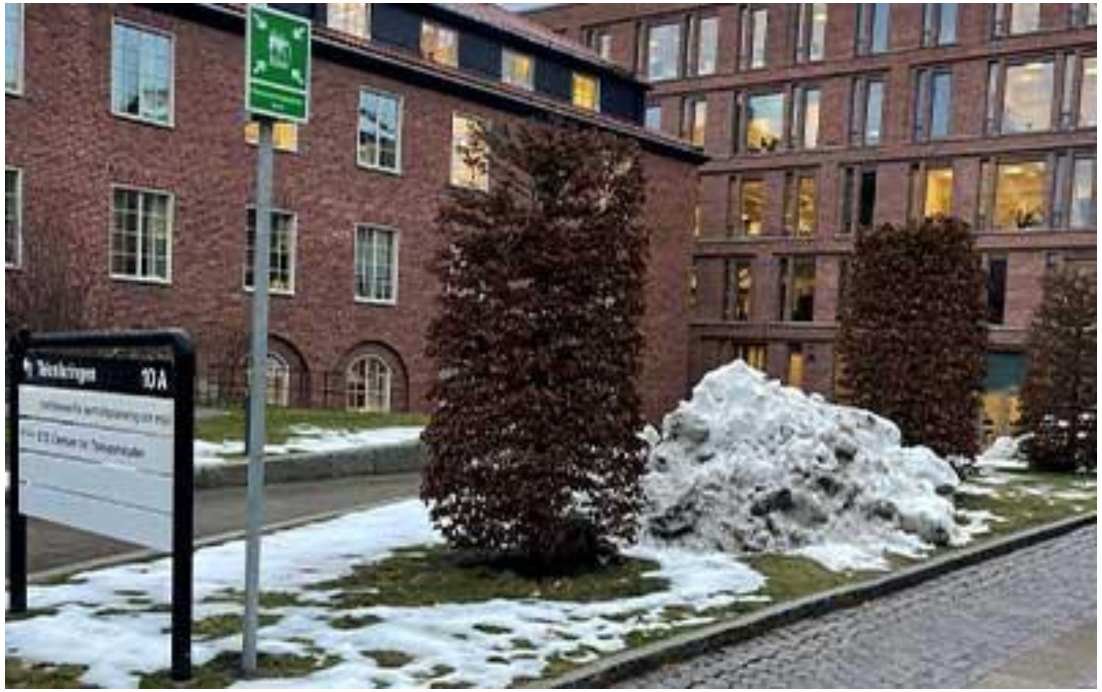
Welcome to CDIS Spring Conference 2025

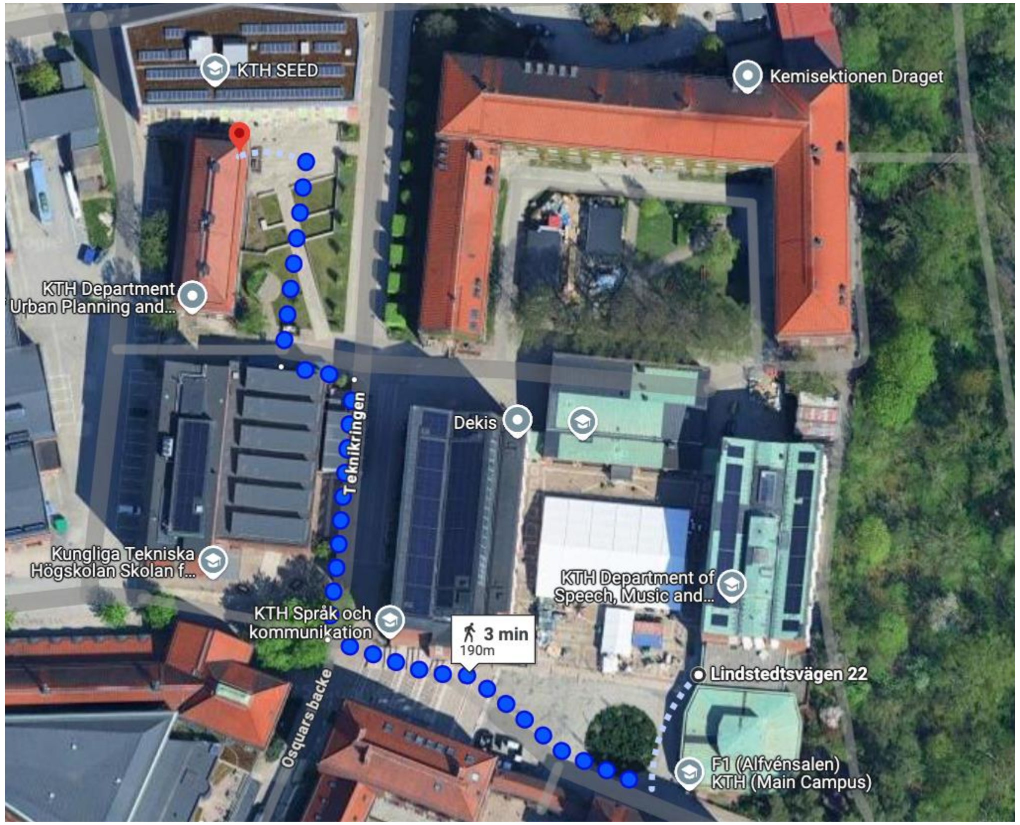
Musard Balliu, KTH

Safety First

Emergency exits: 2 on the front and 2 on the back

Gathering point in case of evacuation: Teknikringen 10 A/B




KTH SEED
Kemisektionen Draget
KTH Department Urban Planning and...
Dekis
Teknikringen
Kungliga Tekniska Högskolan Skolan f...
KTH Språk och kommunikation
3 min
190m
KTH Department of Speech, Music and...
Lindstedtsvägen 22
Osquars backe
F1 (Alfvénsalen) KTH (Main Campus)

CDIS Cybercampus Spring Conference 2025

Program:

09:00 Welcome and Introduction (Musard Balliu, KTH; Pontus Johnson, KTH; David Olgart, Cybercampus)
09:30 Keynote: Malware research: History, milestones, and open problems (Davide Balzarotti, Eurecom)
10:30 Break
11:00 Real-world cryptography: Construct, analyze, code, document, and deploy. Repeat. (Douglas Wikström KTH)

11:30 TRUVALT: A framework for secure and confidential upgradable functions in Trusted Execution Environments (Marcus Birgersson, CDIS)
11:50 Modeling and Simulating with Adversary-driven System Architecture Dynamics (Viktor Engström, CDIS)

12:10 Lunch; CDIS posters and demos

13:30 On the quantum threat to cryptography, its mitigation, and our quantum cryptanalysis research (Martin Ekerå, Swedish Armed Forces)
14:00 Protection against quantum computers through lattice problems (Joel Gärtner, CDIS)
14:20 Adaptable Partitioning with a Real-Time Separation Kernel (Henrik Karlsson, CDIS)

14:40 Break
15:00 Keynote: War in the Smartphone Age (Matthew Ford, FHS)

15:45 Panel: Reflections on navigating dual-use research and innovation during the transition from research to resilience (Moderator: Göran Olofsson, Cybercampus Sweden), with an introduction by Henrik Friman (Strategic Solutions). Panelists: Davide Balzarotti, Matthew Ford, Henrik Friman

16:30 Closing
16:40 Reception

CDIS Cybercampus Spring Conference 2025

Poster and Demo Program: 12:10 – 13:30

- Jakob Nyberg: Automated Decision Learning for Systems with Relational Data
- Leonhard Grosse, Sara Saeidian, Mikael Skoglund, Tobias J. Oechtering: Privacy Mechanism Design Based on Empirical Distributions
- Marco Campione, Mateus Marinheiro, Tsvetelin Tsonev, Aws Jaber: Simulating Advanced Cyber Threats for Enhanced Cybersecurity – With Demo
- Henrik Karlsson, Roberto Guanciale: Capability-based Partitioning Kernel
- Kiarash Kazari, Aris Kanellopoulos, György Dán: Quickest Detection of Adversarial Attacks Against Correlated Equilibria
- Mauricio Byrd Victorica, György Dán, Henrik Sandberg: Saliuit: Ensemble Salience Guided Recovery of Adversarial Patches against CNNs
- Sandor Berglund: First Person Attacker Simulation in MAL
- Muhammad Zeshan Naseer, Viktoria Fodor, Mathias Ekstedt: Informed Defense: How Attacker Profiles Transform Vulnerability Assessments
- Martin Brisfors: Attacking and Securing the Clock Randomization and Duplication Side-Channel Attack Countermeasure
- Andrei Buhaiu: SAC3S/Tyr Attack Simulation Demonstration – With Demo
- Cyber soldiers: Information about the cyber soldier conscription program at the Swedish Armed Forces