	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
8:30 - 9:00	Welcome and introduction	Welcome and introduction	Welcome and introduction	Welcome and introduction	Welcome and introduction
9:00 - 10:30	Lea Schönherr - Can We Trust Generative AI? Understanding and Mitigating Security Threats in Today’s Machine Learning Systems	Maximilian Golla - Password Pain and Passkey Promise: The Future of User Authentication	Alvaro Cardenas - Security and privacy of cyber-physical systems, including autonomous vehicles, drones, and SCADA systems controlling the power grid and other critical infrastructures	V.S. Subrahmanian - Leveraging Robust Generative AI for Advanced Mobile Threat Detection, IP protection and phishing detection	Ilias Tsingenopoulos - Adaptive Attacks and Defenses for Robust and Secure AI systems
10:30 - 11:00	coffee break	coffee break + group picture	coffee break	coffee break	coffee break
11:00 - 12:30	Lea Schönherr - Can We Trust Generative AI? Understanding and Mitigating Security Threats in Today’s Machine Learning Systems	Maximilian Golla - Password Pain and Passkey Promise: The Future of User Authentication	Alvaro Cardenas - Security and privacy of cyber-physical systems, including autonomous vehicles, drones, and SCADA systems controlling the power grid and other critical infrastructures	V.S. Subrahmanian - Leveraging Robust Generative AI for Advanced Mobile Threat Detection, IP protection and phishing detection	Ilias Tsingenopoulos - Adaptive Attacks and Defenses for Robust and Secure AI systems
12:30 - 14:00	lunch	lunch	lunch	lunch	lunch
14:00 - 15:30	Team Building	Laboratory activity	Laboratory activity	Laboratory activity	Project presentation
15:30 - 16:00	coffee break	coffee break	coffee break	coffee break	Coffee break
15:30 - 18:30	Tutorial	Mentoring session	Free time	Laboratory activity	Closure and free time
			Social dinner - Location TBD		

The lectures will be at the Faculty of Engineering and Architecture, Room "Alfa" https://maps.app.goo.gl/Mdh1V63y9mnqYLo59

🟩	lecture
🟪	laboratory
🟦	extra