INFORMATICS COLLOQUIUM

Speaker:

Prof. Pavel Laskov, University of Liechtenstein

Can we Trust Artificial Intelligence?

Abstract:
Artificial Intelligence (AI) is omnipresent in the modern society. Its deployment in security-critical domains, e.g., authentication mechanisms of smartphones or computer visions systems of self-driving cars, gave rise to an intense public discourse on trustfulness of AI-driven information systems. The recently announced EU regulation of AI foresees special measures aimed at insuring trust in AI systems when they are deployed in the so-called “high-risk” applications. In this talk, I will address the scientific challenges connected to trust in AI. I will briefly present the key ideas underlying the research in AI security and illustrate them with recent research projects carried out in my group. Subsequently, I will sketch the future legal requirements for high-risk AI systems and discuss the open research questions that need to be addressed in order to meet such requirements.

Bio:
Pavel Laskov is Full Professor at the University of Liechtenstein and head of the Hilti Chair of Data and Application Security. His research is focused on the development of techniques for detection and mitigation of security incidents. The main technical instrument of this research are specialized AI techniques for cybersecurity. Besides the classical problems of intrusion detection, AI techniques are essential for log data analysis, alert correlation, forensic investigation as well as threat intelligence. Due to the growing importance of AI, especially in high-risk applications and critical infrastructures, an important topic of the Chair’s research agenda is investigation of attacks against AI systems and appropriate countermeasures.

Date and time: Tuesday November 2nd, 2021, 2.00 pm
Location: Pérolles 17, room 001, Ch. du Musée 18, Fribourg
Contact person: Prof. Hans-Georg Fill
COVID-19: COVID certificate mandatory
Conference stream available

The colloquium is free and open to the public.