Cybersecurity has emerged as one of the foremost priorities on the global research and development agenda today. The urgent need for new and innovative cybersecurity technologies capable of effectively addressing this pressing danger cannot be overstated. Software security is paramount to maintaining the integrity of modern software applications.

Given the broad spectrum of real-world applications, different security challenges are evaluated based on the specific use case. In this presentation, we will dissect a variety of security issues that have arisen in diverse applications, examining both the associated challenges and effective strategies in software security.

We will delve into the technique of fuzzing, an efficient and effective automated process vital for software testing. Additionally, we will explore strategies for detecting security vulnerabilities in software. We will also scrutinize security considerations in binary code applications, including those in IoT devices and Windows low-level components. By viewing AI models as software, we will further address the significant security problems present within deep learning models.

Machine learning has seen significant advancements in recent years and has proven to be highly effective in a wide array of applications, including intrusion detection systems (IDS). However, while working in adversarial environments, machine learning-based systems are known to be vulnerable to a range of attacks. In this talk, we will discuss techniques aimed at strengthening machine learning-based IDS.

On the one hand, we explore techniques for enhancing the performance and robustness of IDS in adversarial environments, where we propose a contrastive learning-based approach that builds highly differentiating IDS. On the other hand, we develop efficient security mechanisms to thwart common attacks, including an adversarial example (AE) detector that filters out suspicious inputs at the model testing time, and a robust model evaluation method that leverages latent space representations to build resiliency in model aggregation against model poisoning attacks in federated learning. This talk will report our research results along this line of research.
- A Revocable Outsourced Data Accessing Control Scheme with Black-Box Traceability.
- LocKey: Location-based Key Extraction from the WiFi Environment in the User's Vicinity.

12:00 Luncheon
Blockchain - M1 (Room M1)
- BAHS: Blockchain-Aided Hash-Based Signature Scheme
- Lever: Making Intensive Validation Practical on Blockchain

14:00
Applied Cryptography - S2 (Room S9)
- Isogeny-based Multi-Signature Scheme
- Security Analysis of WAGE against Division Property based Cube Attack
- When MPC in the Head meets VC.

15:00 Afternoon Coffee Break
Web and Network Security - M1
- Quantum Key Distribution as a Service and Its Injection into TLS
- XFedGraph-Hunter: An Interpretable Federated Learning Framework for Hunting Advanced Persistent Threat in Provenance Graph
- XSS attack detection by attention mechanism based on script tags in URLs.

Blockchain - S1
- SIOCEN: Secure Integrity Verification of Outsourced Data in Cloud Storage using Blockchain.

16:30 Closing Ceremony.

Brede Værk Garden
Get up close to 250 years of industrial architecture with factory buildings, workers' homes and master's homes, and get an impression of the small community. The river Mølleåen is dammed and the course of the water can be flowed beneath the buildings.

Brede Høker
The charming restaurant itself is located in Brede Værk's old building, dating back to 1893. A historic location for Danish industry, over the centuries the buildings have produced grain, gunpowder, copper and textiles. And now, exquisite cuisine.

Brede Værk Garden
Get up close to 250 years of industrial architecture with factory buildings, workers' homes and master's homes, and get an impression of the small community. The river Mølleåen is dammed and the course of the water can be flowed beneath the buildings.

Brede Høker
The charming restaurant itself is located in Brede Værk's old building, dating back to 1893. A historic location for Danish industry, over the centuries the buildings have produced grain, gunpowder, copper and textiles. And now, exquisite cuisine.