Section for Cybersecurity Engineering

DTU Compute

Section Summary

Cybersecurity engineering focuses on the methods, processes and tools for the design, development and analysis of secure computing systems that are accessible through a network, typically the Internet, which is often known as cyberspace.

We are particularly interested in these fields;

Cybersecurity in Pervasive Computing
Contacts: Nicola Dragoni, Emmanouil Vasilomanolakis, Gaurav Choudhary, Lejla Islami

Cryptography: Symmetric, Quantum and Post-Quantum
Contacts: Christian Majenz, Tyge Tiessen, Carsten Baum, Luisa Siniscalchi

Cybersecurity in Pervasive Computing

Our research focuses on the design, development, and testing of cybersecurity services for networked computing systems. This includes models, policies, and mechanisms to support secure collaboration in open dynamic systems, such as sensor networks, mobile systems, the Internet of Things (IoT) and Cyber-Physical Systems (CPS). We are especially active in the field of "proactive security", in particular defensive cyber-deception techniques meant to attract and catch malicious actors by means of deceptive tactics.

Our research also covers intrusion detection, biometric authentication, trust management, malware detection, blockchain, cloud security, IoT/CPS/edge security, botnet monitoring, alert data correlation and machine/deep learning, to mention a few.

Cryptography

We investigate complex cryptographic algorithms and protocols, from digital signatures up to versatile tools such as multiparty computation. Here, we strive to shed light on the fundamental properties of such algorithms and protocols, and work on more efficient concrete constructions.

We develop and analyse symmetric-key cryptographic algorithms with a particular focus on developing novel cryptanalytic techniques. We also develop symmetric cryptographic algorithms with low multiplicative complexity for usage in zero-knowledge proofs, fully-homomorphic encryption and secure multi-party computation.

We analyse the security of cryptographic algorithms, from hash functions and block ciphers to public-key encryption and digital signatures, against quantum attacks. Our work leads to security proofs that reduce the cryptographic attack surface of these algorithms.

ML-based malware detection in Drones/Robots

Contact: Gaurav Choudhary

Description: In this project, you can explore ML-based malware detection in drones/robots, which means using machine learning (supervised, anomaly detection, or deep learning) to identify malicious activity from system logs, network traffic, or binaries. The challenge is balancing detection accuracy, resource constraints, and real-time performance.

Lightweight Misbehavior Detection Management of Embedded IoT Devices

Contact: Gaurav Choudhary

Description: The proposed thesis, "Lightweight Misbehavior Detection Management of Embedded IoT Devices," focuses on developing an efficient security framework for resource-constrained IoT systems. Since traditional intrusion detection systems are too heavy for embedded devices, the project aims to design a lightweight solution that monitors device behavior (e.g., network traffic, resource usage, sensor activity) to detect anomalies or malicious activity in real-time with minimal overhead. Using techniques like rule-based detection, TinyML models, and federated learning, the framework will enable both local responses (blocking traffic, resetting processes) and centralized management via dashboards. The outcome will be a prototype that demonstrates how IoT devices can be secured effectively against threats while preserving performance, energy, and memory resources.

Cyber Security Monitoring Framework for SMEs/IoT devices/CPS

Contact: Gaurav Choudhary

Description: Develop monitoring solutions focused on critical business processes. By integrating threat data, IT data, and business data, organizations can equip themselves with context-rich alerts to help prioritize incident handling and streamline incident investigation.

Designing User-Friendly Privacy Controls for Mobile Applications

Contact: Lejla Islami

Description: The objective of this project is to improve the usability of privacy settings in mobile applications. The project involves evaluating current privacy interfaces, identifying usability issues, and designing a prototype that simplifies user control over personal data sharing. Through user testing and analysis, the project aims to balance strong privacy protection with intuitive, accessible design – enhancing users' ability to make informed privacy decisions.

Designing a Privacy Dashboard for Smart Home Devices

Contact: Lejla Islami

Description: Smart home devices often lack transparency in data collection. This thesis involves designing a centralized, user-friendly dashboard that gives users clear insights and control over the data collected by their IoT devices.

Building Secret Sharing with the Chinese Remainder Theorem

Contact: Luisa Siniscalchi

Description: The project focuses on exploring Chinese Remainder Theorem (CRT)-based secret sharing (SS) and its applications in modern cryptography. Secret sharing is a fundamental technique for distributing sensitive information among multiple parties in a secure way, and CRT-based methods offer unique advantages in terms of efficiency and structure.

In particular, the project investigates the performance of weighted encryption schemes when implemented with CRT-based secret sharing. The study combines both theoretical analysis and practical implementation, allowing students to evaluate efficiency, security properties, and potential applications of these schemes.

Through this work, students will gain hands-on experience with cryptographic protocol design, performance evaluation, and the practical challenges of implementing advanced mathematical techniques.

How to implement secure voting.

Contact: Luisa Siniscalchi

Description: This project is focused on understanding and implementing how to realize secure voting between three users and what are the security requirements of the realized solution.

Study of threshold signature schemes

Contact: Luisa Siniscalchi

Description: This project is focused on understanding threshold signature schemes. At a high level, in threshold signature schemes, a new signature can only be generated cooperatively among a set of multiple users, but no user alone is able to generate a new signature. The project studies threshold signature schemes and their applications.

Sum Check and Range proofs in Cryptography

Contact: Carsten Baum

Description: In cryptography, we often use Interactive or Zero-Knowledge proofs to convince a verifier that a prover has done something honestly. A very popular technique used in this is the so-called Sumcheck protocol. It allows to build highly efficient (zero-knowledge) proof systems where the verifier performs less work than the prover!

In this project, you will learn about the Sumcheck protocol and a recent application of it to so-called range proofs. The project requires a solid mathematics background and familiarity in working with finite fields.

Estimating block cipher security with SAT-solvers

Contact: Tyge Tiessen

Description The difficulty of breaking block ciphers is expected to grow exponentially with the size of the key. In this project the goal is to give an estimate of the time that it would take a SAT-solver to break a block cipher by extrapolating from the time it takes to break reduced-key size variants.