Section for Cybersecurity Engineering at DTU Compute

Credit: ChatGPT/Dragoni

The success of digitalization fundamentally depends on the security of the data and computing systems that underpin our daily lives. Cybersecurity plays a central role in ensuring that these data and systems remain secure, resilient, and trustworthy.

We focus on and advance the methods, processes, and tools used to design, develop, and analyze secure computing systems.

We serve as a key partner for cybersecurity and cryptography research in Denmark and worldwide.

Cybersecurity engineering is concerned with the methods, processes, and technologies required to design, build, and analyze secure computing systems that are accessible through a network, typically the Internet (often known as *cyberspace*).

Our **mission** is to strengthen, advance and integrate foundational and applied research in cybersecurity and cryptography in order to anticipate and respond to evolving scientific, technological, and societal challenges.

The mission is realized through a strong synergy between **cutting-edge research** and **research-driven education**.

Through our educational activities, we prepare future engineers, scientists, and IT professionals with the theoretical foundations, practical methodologies, and state-of-the-art technologies needed to securely develop, deploy, and operate complex networked computing systems.

Research Areas

Cybersecurity: Our work addresses the design, development, and validation of cybersecurity services for networked computing systems. This includes models, mechanisms, protocols and policies to enable secure and trustworthy collaboration in open and dynamic systems, such as Cyber-Physical Systems (CPS).

Cryptography: We study the security of existing cryptographic algorithms and investigate ways to build future-proof cryptography secure against quantum computers. We also focus on Privacy-Enhancing Technologies such as Zero-Knowledge proofs and Secure Multiparty Computation and their applications.

Contact
Nicola Dragoni
Professor,
Deputy Director,
Head of Section.
DTU Compute
ndra@dtu.dk

www.compute.dtu.dk/sections/cybsec

January 2026

DTU

Technical University of Denmark

Cybersecurity: Securing the Cyber and the Cyber-Physical World

The transformative evolution of computing – from centralized mainframes to personal devices (phones, wearables, smart home devices, …) and industrial systems (i.e., critical infrastructures) interconnected through the Internet – has fundamentally transformed cybersecurity, shifting it from closed, isolated environments to an open cyberspace in which any connected device may be accessed, and potentially compromised, from anywhere in the world.

*Security has become a **public safety issue**!*

Networked computing systems are evolving into increasingly **socio-technical systems**. Their effective defence against cyber-attacks requires a **holistic approach** that considers human and technical factors, from organisational security awareness and behaviour to the design, implementation, and enforcement of security policies and protective mechanisms.

Our research addresses the design, development, and evaluation of cybersecurity services for networked computing systems. We advance models, protocols, policies, and mechanisms that enable secure and trustworthy collaboration in open and dynamic environments, such as sensor networks, the Internet of Things (IoT) and Cyber-Physical Systems (CPS).

We are active in the area of **proactive security**, with a strong focus on the emerging field of **defensive cyber deception**, which employs deceptive techniques to detect and mislead malicious actors.

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

Cryptography: Future-Proofing Algorithms and Privacy-Enhancing Technologies

Cryptography is the science of providing and analysing the fundamental algorithms needed for secure communication. Cryptography plays a key role in safeguarding security and privacy for today's more and more digitalized and interconnected society.

Advances in cryptanalysis and the development of quantum computers are threatening the security of our currently deployed cryptography. Meanwhile, newly developed cryptographic protocols can achieve privacy-related objectives far exceeding what is currently deployed. This leads to an increased need for the development of new cryptographic algorithms and techniques for cryptanalysis and security proofs.

Our cryptography group focuses on three **core areas**:

1. We investigate and build 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.

2. 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.

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

Education: Cybersecurity Specialization!

As society becomes increasingly dependent on computer systems, from controlling critical infrastructure to providing public services over the Web, the importance of protecting against cyber threats from criminals, industrial espionage and cyber terrorism has grown dramatically.

Our **Cybersecurity specialization in the MSc in Computer Science and Engineering** equips students with the essential knowledge and skills to address the secure design, development, deployment, and operation of interconnected computer systems across open, dynamic, and heterogeneous networks.

The specialization involves various key cybersecurity topics, including advanced courses on ethical hacking, risk management, incident response, usable security and privacy, and cryptography (including post-quantum cryptography).