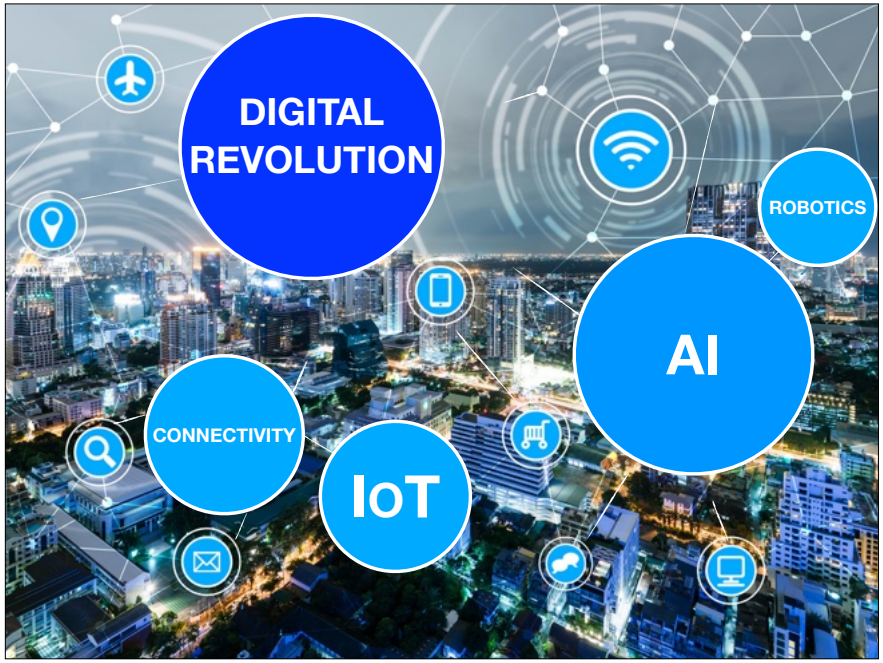
Nicola Dragoni
Professor in Secure Pervasive Computing, PhD
DTU Compute, Technical University of Denmark (DTU)

Deputy Director at DTU Compute
Head of Section Cybersecurity Engineering
Head of DTU Center for Digital Security

Cybersecurity @ DTU

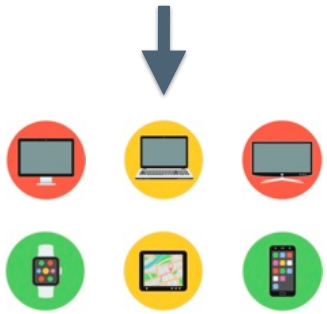


Digital Revolution: Documents Take a Digital Form

1

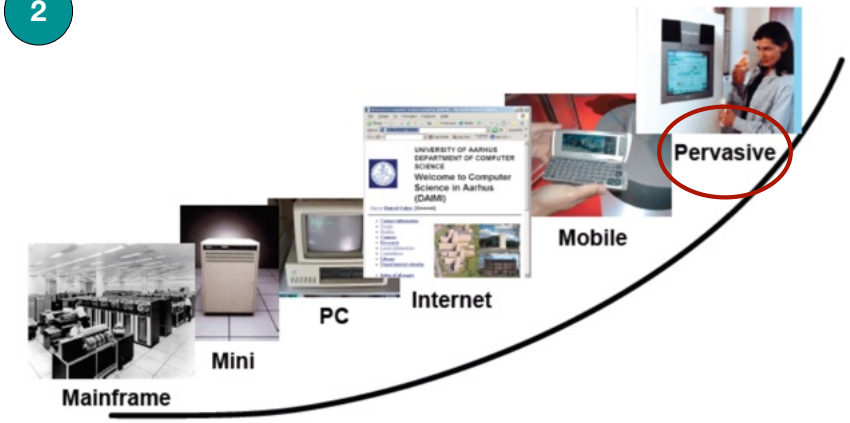
Digital Revolution: Processes Take a Digital Form

1



Pervasive Computing

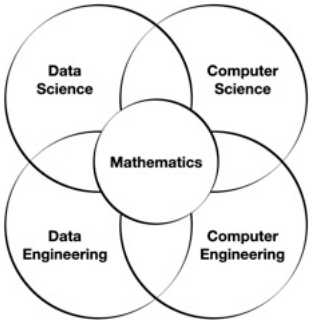
2

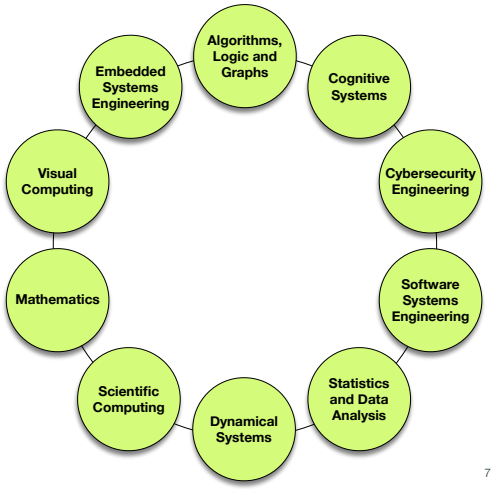


COMPUTING + CONNECTIVITY
EMBEDDED EVERYWHERE!

DTU Compute Research Structure

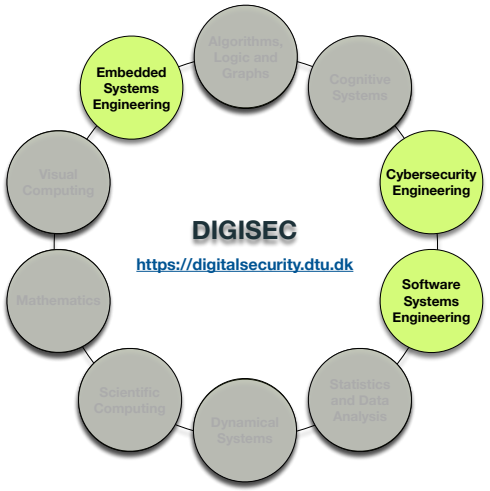
DTU Compute is an engineering research department with a long established tradition of advancing **mathematics**, **data science** and **computer science and engineering** together by exploring synergies between them.





7

DTU Center for Digital Security (DIGISEC)



8

Key Research Areas

Cybersecurity for Pervasive Computing

Nicola Dragoni
- IoT and CPS security
- Human-centred cybersecurity

Christian D. Jensen
- Computational trust and trust management (incl. zero trust architectures)

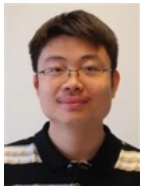
Emmanouil Vasilomanolakis
- Novel detection theory (e.g., cyber-deception and collaborative threat detection algorithms)
- Human aspects of cybersecurity (incl. cyber-psychology and sociological factors)

Weizhi Meng
- Intrusion detection
- Blockchain technologies

Nicola Dragoni
Professor, Head of Section

Christian D. Jensen
Associate Professor

Emmanouil Vasilomanolakis
Associate Professor



Weizhi Meng
Associate Professor

Cryptography: Symmetric, Quantum, Post-Quantum

Christian Majenz
- Provable security for post-quantum cryptography
- Mathematical techniques in quantum information and quantum computing

Carsten Baum
- Privacy-enhancing technologies (incl. multiparty computation, zero knowledge protocols, blockchain)
- Post-quantum cryptography

Tyge Tiessen
- Construction and security analysis of the fundamental building blocks of symmetric cryptography (mostly block ciphers)

Luisa Siniscalchi
- Secure multi-party computation (emphasis on primitives which are secure against MITM attacks)
- Blockchain technologies and zero-knowledge proofs

Christian Majenz
Associate Professor

Carsten Baum
Associate Professor

Tyge Tiessen
Assistant Professor

Luisa Siniscalchi
Assistant Professor

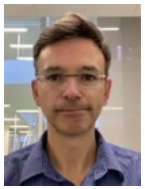
Formal Methods for Security and Privacy

Alberto Lluch Lafuente
- Security risk/threat modelling & assessment with graphical models

Sebastian Mödersheim
- Security protocols verification
- Automated verification of privacy properties
- Verification of post-compromise security guarantees and recovery mechanisms

Christoph Matheja
- Robust programming in rust with automated verification tools

Christian Kalhauge
- Automated library testing with fuzzing



Alberto Lluch Lafuente
Professor, Head of Section

Sebastian Mödersheim
Associate Professor

Christoph Matheja
Assistant Professor

Christian Gram Kalhauge
Assistant Professor

Safety

Paul Pop
- Methods and tools for the safety assurance of Cyber-Physical Systems-of-Systems
- Analysis and configuration of safe and secure Time-Sensitive networking (TSN)
- Dependable Edge Computing for safe and secure real-time applications

Xenofon Fafoutis
- Trustworthy embedded AI
- Dependable and maintainable IoT infrastructures

Sven Karlsson
- Large-scale data analysis and computing infrastructures: privacy and security

Michael Reichhardt Hansen
- Formal methods for real-time and safety-critical systems

Paul Pop
Professor, Head of Section

Xenofon Fafoutis
Associate Professor

Sven Karlsson
Associate Professor

Michael R. Hansen
Associate Professor

Technologies and Uses Cases

Projects

- We are active in a number of **national and international projects**
- Majority of our research is carried out within **collaborative research projects**
- Projects funded by different agencies (HORIZON, ECSEL, Erasmus+, …)

SbD SECURITY BY DESIGN

TRANSACT

ASTRID

ASSURE

SecDNS

ENGINE

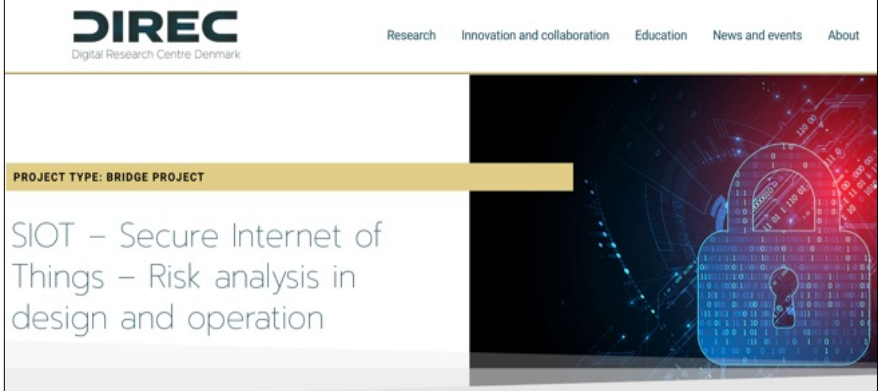
fora

Cyber Security for Europe –

DataVaults

Latest Highlights: Secure Internet of Things

- Research: DTU, AU, AAU, CBS, Alexandra Institute
- Industry: Micro Technic, SecuriOT, Beumer Group, Grundfos, Develco, Terma, Seluxit
- February 1st, 2022 - January 31st, 2025
- Total Budget DKK 25.10M DKK, 4M to DTU



Latest Highlights: Digital Ghost Ships

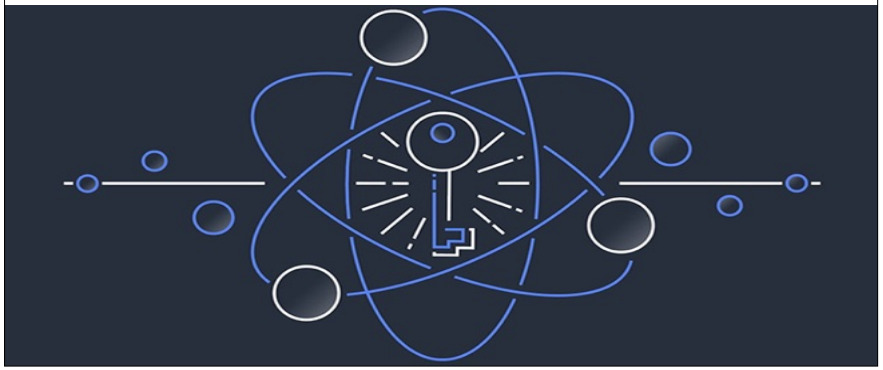
- **Unveiling the Threat of Misconfigured and Obsolete Systems**
- **Goal**: **to identify Digital Ghost Ships (DGS), which is the first step into making them secure, and also to examine how human psychology plays a role in creating DGS**
- Collaboration between **DTU**, **Cambridge University** and the **University of Colorado**
- DFF grant of 2.9M DKK
- September 1st, 2022 - December 31st, 2025

Latest Highlights: Quantum-Safe Internet

- **The training network provides research and training opportunities to a new generation of PhD students, who, in the long-run, shall address the Grand Challenge of providing "Quantum-Safe Internet", i.e. a communication infrastructure that is secure against not only classical attacks but also those enabled by quantum technologies**
- MSCA Doctoral Training Network, 276k € (DTU's share)
- October 1st, 2022 - September 30th, 2026

Latest Highlights: QUID-PRO

- **Quantum-Safe Information Distribution for Cryptographic Protocols**
- Cryptography protects private information at rest or in transit through computer algorithms
  These algorithms use so-called **private keys to achieve protection**
- **Goal: to investigate how to safeguard cryptographic keys against hacking attacks, for cryptography that is secure against quantum computers**
- The research outcomes will make modern and future cryptography more secure
- Villum Young Investigator, 6M DKK



Latest Highlights: IM-3PQC

- **Idealized Models for Provably-Secure Practical Post-Quantum Cryptography**
- **Goal: to develop mathematical methods for analyzing cryptographic algorithms in a quantum computing setting**
- These methods will be used for **writing mathematical proofs** for the fact that certain important **cryptographic algorithms**, like, for example, digital signatures and so-called hash functions, are secure despite being under quantum computing attack
- Preparing IT security for the quantum computing age
- DFF Sapere Aude, 5.6M DKK

Education

We educate new generations of engineers, scientists and professionals in the foundations, principles and state-of-the-art methods and technologies to address the secure development, deployment and operation of (networked) computing systems

Research-based MSc with cybersecurity tracks
- Safe and Secure by Design
- Computer Security
  - Specialist Programme in Cybersecurity

Joint International Education Programmes
- Erasmus Mundus MSc SECCLO
- European Training Networks

Continuing Education
- Master of Cyber Security
- Single courses

Continuing Education

Continuing Education

Do you want to strengthen your professional competencies and the competitiveness of your company in the digital society of the future?
DTU Compute's continuing education courses are based on the latest research in computer science and give you the opportunity to integrate your expertise in the course, update you with the latest technology and dress for the tasks of the future.

We offer both short courses, tailor-made courses and competence development courses, workshops, a flexible master's in cyber security, as well as free courses for small and medium-sized companies in utilizing new technology. Read more here on the page or contact us to find out more.

Kontakt

Line Katrine Harder Clemmensen
Associate Professor
DTU Compute
+45 45 25 37 64
lkhc@dtu.dk

https://www.compute.dtu.dk/english/continuing-education

Latest Highlights: Cyber4Boards

Cybersecurity Course for Board Members, Directors, and Executives

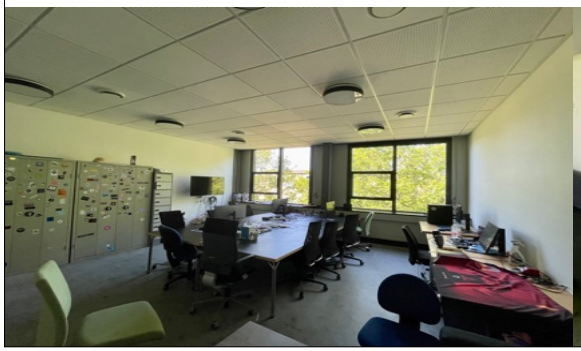
- To ensure the long-term success and resilience of an organization, it is **crucial to focus on cybersecurity in the board room**
  - This requires board members, directors, and executives to possess **a comprehensive understanding of cybersecurity and cyber-risk management**
- **Effective cybersecurity requires the active involvement of key decision-makers** to oversee the company's risks effectively, to assess emerging threats and the organisation's response to them
  - However, **key decision-makers often lack sufficient knowledge and competences** to be able to address cyber risks appropriately and thus to take well-informed decisions

The purpose of the course is to increase awareness of cyber risks and to strengthen cyber security competences in Boards and Executive Managements

Attending the course empowers key decision-makers with the knowledge, skills, and mindset necessary to navigate the complex cyber landscape, make informed decisions, and safeguard their organizations against evolving cyber threats

DTU HackerLab

- Laboratory facility located in building 322 at DTU Compute, Kgs Lyngby
- Offers an assortment of **equipment dedicated to penetration testing** in the form of **hacker tools** and a **space for peers to exchange ideas** about cybersecurity
- Provide a **selection of commercial technology, networks and cases** that aspiring ethical hackers and security experts can try experimenting with
- The **daily operator** is available for assistance in any experiments that works towards improving the cybersecurity in an increasingly technologically advanced world



Nicola Dragoni
Professor in Secure Pervasive Computing, PhD
DTU Compute, Technical University of Denmark (DTU)

Deputy Director at DTU Compute
Head of Section Cybersecurity Engineering
Head of DTU Center for Digital Security

Thank you!

ndra@dtu.dk