chess-eu.cs.ut.ee

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

PARTNERS

MUNI Masaryk University

University of Tartu

Brno University of Technology

TalTech

Cybernetica

Red Hat

guardtime

Republic of Estonia Information System Authority

Cyber Security Hub

ASSOCIATED PARTNERS:

NÚKIB

JIC

chess-eu.cs.ut.ee

The Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) brings together leading R&I institutions in both regions to build connected innovation ecosystems to address one of the most important issues confronting Europe today: cyber-security.

Estonia and South Moravia are teaming up to support the EU's safe transition to a digital society. Estonia is among the most advanced digital societies globally, with an outstanding e-government infrastructure. South Moravia is a major Czech ICT powerhouse in industry and education, with a strong focus on cyber-security.

Funded by the European Union

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

CHESS

OBJECTIVES

- Develop a cross-border joint cyber-security research and innovation (R&I) strategy aligned with Czechian and Estonian smart specialisation strategies and Europe's digital society and cyber-security goals
- Apply the strategy in six focus areas of cyber-security:
  - Internet of Secure Things
  - Security Certification
  - Verification of Trustworthy Software
  - Security Preservation in Blockchain Technology
  - Post-Quantum Cryptography
  - Human-Centric Aspects of Cyber-Security
- Initiate at least 12 small-scale R&I projects consolidating academia business linkages, demonstrate validity of ideas, and provide evidence to obtain additional investments
- Develop a training strategy for both regions to increase cross border/ sectoral cooperation and skills around the six priority areas
- Raise visibility, citizen engagement, technology transfer, entrepreneurship training, staff exchange, and mutual learning in cyber-security

CHALLENGE AREAS

INTERNET OF SECURE THINGS

- Privacy and security by design
  - Data minimisation principles
  - Data usage control
- Modern cryptographic schemes
  - Attribute-based credentials
  - Group signatures
- Balance between security, availability, and privacy is essential

SECURITY CERTIFICATION

- Multi-facet approach
  - Organisational structures that produce devices
  - Software that runs on these devices
- Harmonisation schemes
- Standardisation of new and emerging cyber-security technologies

VERIFICATION OF TRUSTWORTHY SOFTWARE

- Preserving reliability of integrated digital systems
- Minimising problems caused by software errors

SECURITY PRESERVATION IN BLOCKCHAIN TECHNOLOGY

- By being decentralised
  - Less vulnerable
  - Improve data privacy and pseudo-anonymity of participants
  - Ensuring legal certainty via smart contracts and digital assets

POST-QUANTUM CRYPTOGRAPHY

- Developing quantum-secure technologies – **Post-Quantum Cryptography** – secure, low-cost and interoperable with existing systems

HUMAN-CENTRIC ASPECTS OF CYBER-SECURITY

- **Regular training** so that they are skilled in working with emerging technologies and responding to new threats
- Guarantee **usability** so that user behaviour will not jeopardize their benefits in terms of security and privacy