Funded by
the European Union

CHESS

CAiSE'24

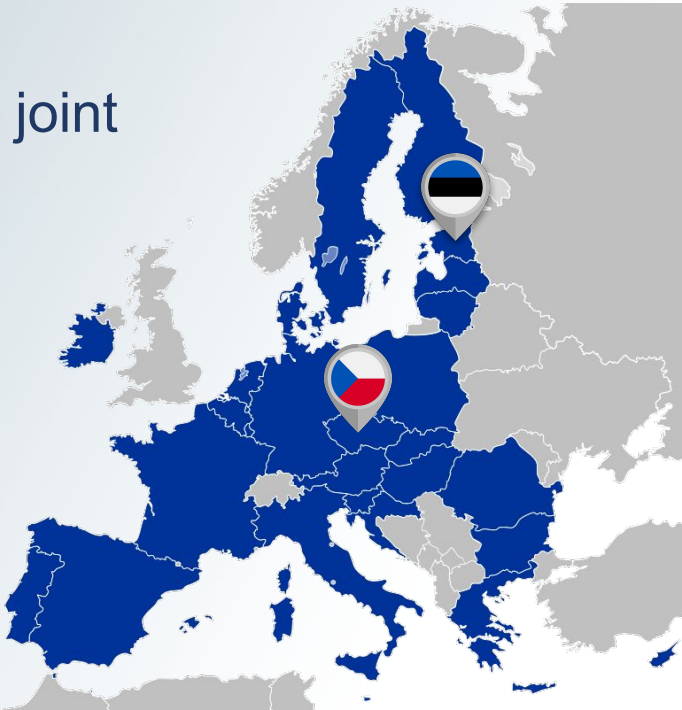
Cyber-security Excellence Hub in Estonia and South Moravia

Mariia Bakhtina[1], Zuzana Vémolová[2] and Vashek Matyáš[2]

[1] University of Tartu, Tartu, Estonia
[2] Masaryk University, Brno, Czechia

Goals

- collaboration between academia, business, and government
- conduct a needs analysis and develop a joint cross-border research and innovation strategy for cybersecurity



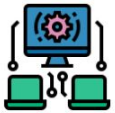
Partners

Partner type	Estonia 	South Moravia (Czechia) 
Academia	University of Tartu (UT) Tallinn University of Technology (TalTech)	Masaryk University (MUNI) Brno University of Technology (BUT)
Industry	Cybernetica AS Guardtime	Red Hat
Government	Estonian Information System Authority (RIA)	National Cyber and Information Security Agency

Research Challenge Areas

Usable Security

- Human-centric Aspects of Cybersecurity



Secure Information System Engineering

- Security Preservation in Blockchain
- Internet of Secure Things
- Security Certification

Formal Security

- Post-Quantum Cryptography
- Verification of Trustworthy Software

Security Preservation in Blockchain

- Automated trust through self-sovereign identity in the data exchange systems
- Blockchain-related operation protected by cryptographic hardware
- Emergency Information transmission using blockchain in Intelligent Vehicular Communication
- Privacy of blockchain transaction

Automated trust through self-sovereign identity in the data exchange systems

- A Decentralized Public Key Infrastructure for Trust Management in X-Road (2023)

Demo

- The Power of Many: Securing Organisational Identity Through Distributed Key Management
  - Session 12 – Session Trust, Security and Risk
  - Room: MEGARON B
  - 14:00

CAiSE'24

Internet of Secure Things (IoST)

- Empirical research on security and privacy management in intelligent transportation systems
- Privacy-preserving smart parking solutions
- Secure and privacy-preserving access to sharing vehicles in smart cities
- Security risk management in automated systems for manufacturing
- Security and privacy in teleoperated systems

Information Security and Privacy Management in Intelligent Transportation Systems (ITSs)

paper

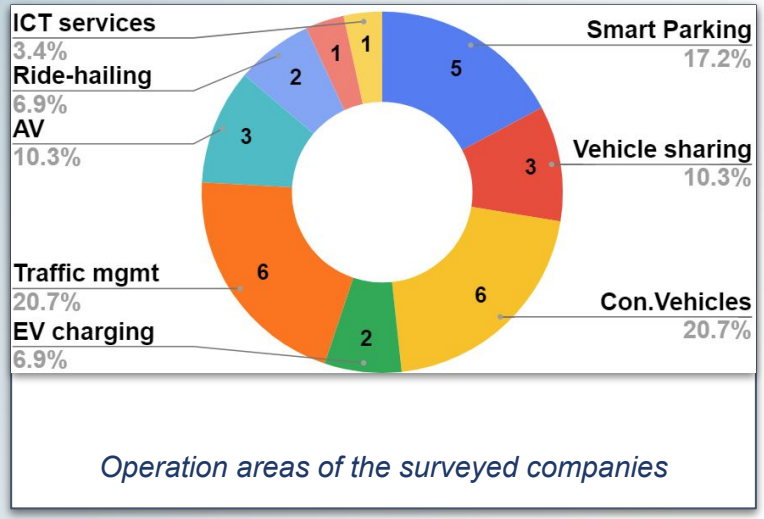
Dimension	Category	Attribute
P. People	PA. Actors	Actors, stakeholders, entities
		Goals, tasks, motives
	PR. Relationships	Relationships and dependencies between actors
O. Organisation	OS. Strategy	Purpose for the system usage, org. design & strategy
		Challenges to address
	OC. Formal Constraints	Legislation, regulation, standard
	OI. Information Involved	Type of information used
		How the information is manipulated
		Security criteria
		Privacy objectives
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices
	CE. Training & Education	Training & education
	CT. Technology	Architectural measures
		Use case-oriented technological measures
		Cryptographic building blocks
		Others technological measures
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle
	PrU. Usage of the System	Use cases of the system as a part of the business processes

- Literature review of measures
  - 24 papers
- Survey of organisations
  - 15 organisations

Information Security and Privacy Management in Intelligent Transportation Systems (ITSs)

paper

Aspects which the surveyed organisations highlighted as challenges



Operation areas of the surveyed companies

Information Security and Privacy Management in Intelligent Transportation Systems (ITSs)

paper

Dimension	Category	Attribute	Attribute instances										
P. People	PA (Actors)	PA	Time-stamping authority	Defence	Parking/Toll Officer	Trusted Authority	Passenger	Parking Service Provider	System provider	Employee	City Government	Driver	
O. Organi-sation	OS (Strategy)	OS System purpose	Safety of urban traffic	Reduced cost for goods delivery	More livable cities	Improved parking facilities	Public transport control	Decreased the traffic congestion	Improved city services	On-demand mobility			
		OS Challenges	Hetero- geneous network	Resource constrained devices	High system quality expectations	Privacy vs efficiency	User data privacy and security	Data minimisation	Expected level of security	Lack of industry regulations	Interoperability		
	OC (Formal Constraints)	OC regulations	EU 2019/2144	EU 2018/858	ITS Directive	UN R155	GDPR						
		OC standards	NIST SP	Other standards from ISO/IEC 27000-series	E-ITS	ETSI standards series	Cyber Security Act in Czechia	ISO 27001					
	OI (Information types)	OI	Information about roadside units	Other information	Information about passenger	Information about transactions	Aggregated information	Information about driver	Information about vehicle				
C. Sec. & Privacy Counter-measures	CP (Practicies & Policies)	CP	Normal best practices	Penetration testing	Threat modelling	Security Development Lifecycle	Risk management	Security framework	Security strategy				
	CE (Training & Education)	CE Trainings Employees	Reading news about security isues	Cyber hygiene trainings	Trainings for raising awareness about security threats	Data protection trainings							
		CE Sources For Survey	Documentation	Colleagues	Knowledge of the organisation	Knowledge of the system							
	CT (Technology)	CT Crypto	Homomorphic encryption	Zero- Knowledge Proof	Oblivious pseudorandom function (OPRF)	Blind signature	Oblivious transfer protocol	Trusted execution environment (TEE)	Private set intersection (PSI)	Hash-based message authent. codes	Elliptic curve cryptography	Diffie-Hellman group key exchange	RSA digital signature
		CT Secure Communication	Custom asymmetric encryption	IPSec protocol	Other secured communication protocol	Customer end-to-end encryption	VPN solution	TLS protocol					
		CT Architectural Measures	Blockchain- based system	Multi-party computation (MPC)	Storage of anotated data	Secret-sharing	Anonymous authentication	Storage of personal data on the data subject device	Securing data in transit				

Cell colour mapping: 0 | 3 | 6 | 14 (by number of supporting responses)

Text colour mapping: **measure1 (black)** - state-of-the-art measure; measure2 (grey) - other

Distribution of the measures usage by the surveyed organisations

Result:

Recommendations for organisations developing ITSs

Security Certification

- Testing the method for evaluating organisations' information security level
- Enriching certification report analysis with other open-source intelligence
- Common Criteria Protection Profile for secure computing applications as PETs

Why is it relevant for CAiSE?

From you:

- New open research questions from CAiSE community

From us:

- open-source solutions for securing the systems
- best practices and guidelines for secure system design

Let’s keep in touch!

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Mariia Bakhtina bakhtina@ut.ee

Follow CHESS in LinkedIn

CHESS LinkedIn

Read the project paper: https://ceur-ws.org/Vol-3692/paper2.pdf