CHESS: 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

Abstract

Given the European Union's aim to fully digitise by 2030, cybersecurity is one of the Europeans' strategic goals. It requires comprehensive approaches at local, national, and European levels, emphasising both current vulnerabilities and future threats through research and innovation. This paper presents the CHESS project, the goal of which is to conduct a thorough needs analysis of the two regions (Estonia and South Moravia) and develop a joint cross-border research and innovation strategy for cybersecurity. The project targets such challenge areas as the Internet of secure things (IoST), security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography and human-centric aspects of security. The project contributes to strategy development on the EU level, joins policy discussions, engages with policymakers, and provides cybersecurity training for IT professionals, students, and educators.

Keywords

cybersecurity, research & innovation, secure system engineering, Internet of things, blockchain, certification

1. Introduction

Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) [1] is a European project implemented under the scheme of the European Framework Programme for Research and Innovation, Horizon Europe. The project is funded by the European Research Executive Agency (REA). Within four years of the project (Jan 2023 – Dec 2026), CHESS aims to strengthen partnerships between innovation regions and create better links between academia, business, and government. The project brings together the expert teams in the area of cybersecurity from the South Moravian region, Czechia, and Estonia to work together on different small-scale Research and Innovation (R&I) projects to create new collaborations between regions and sectors and prepare long-term cybersecurity R&I strategy.

The project targets such open challenge areas as the Internet of secure things (IoST), security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography and human-centric aspects of security. The project contributes to

RPE@CAiSE'24: Research Projects Exhibition at the International Conference on Advanced Information Systems Engineering, June 3–7, 2024, Limassol, Cyprus

*Corresponding author.
bakhtina@ut.ee (M. Bakhtina); vemolova@rect.muni.cz (Z. Vémolová); matyas@fi.muni.cz (V. Matyáš)
0000-0002-9421-8566 (M. Bakhtina)

[1] https://chess-eu.cs.ut.ee/

strategy development on the EU level, join policy discussions and engages with policymakers, and provides cybersecurity training for IT professionals, students, and educators.

2. Objectives and Background

The **aim of the project** is to conduct a thorough needs analysis of the two regions (Estonia and South Moravia in Czechia) and develop a joint cross-border research and innovation strategy for cybersecurity [1]. There are a number of intermediate objectives to be achieved:

- Connecting fundamental research with economic and societal exploitation.
- A cross-border joint Cybersecurity R&I strategy aligned with Czech and Estonian smart specialisation strategies in ICT.
- Action and investment plans for implementation of the strategy in each of its six focus areas of cybersecurity.
- A training strategy for both regions to increase cross-border and sectoral cooperation and increase needed skills around the six priority areas.
- Raising citizen engagement, technology transfer, staff exchange, mutual learning.

Known as the "Czech Silicon Valley" the South Moravian (SM) region has the largest concentration of software development companies, SMEs and start-ups that are producing and developing advanced ICT solutions and technologies in the Czech Republic. The region is renowned for its extensive know-how in cybersecurity, demonstrated by the presence of two important development centres of global leaders in endpoint security (Avast and ESET Software). The concentration of experts, public research base, and presence of important state institutions (incl. the headquarters of the National Cyber and Information Security Agency and National Centre of Competence of Cybersecurity) provide the conditions for the founding and growth of tech start-ups.

Due to the small size of Estonia, the region is unique as it has a close interconnection of national government activities, as reflected in the consortium composition. In 2021 Estonia was ranked first in Europe in e-government indicators by DESI [2]. This includes 5^{th} in open data, 2^{nd} in digital public services for citizens and businesses, 1^{st} in pre-filled forms and 4^{th} in e-government users, with 90% of Internet users having used e-government services in the previous year. Another important driver of ICT/Cybersecurity R&I is human capital. DESI 2021 indicated Estonia was 5^{th} in Europe in human capital – 3^{rd} in Advanced skills development, and 8^{th} in Internet user skills.

The project relies upon quadruple helix model [2, 3] of innovation. Aiming to create a cybersecurity hub that addresses the EU's strategic goals [4] and solves state-of-the-art cybersecurity issues in the selected region, we built links between academia, industry, government, and society. First, such collaboration enables, incorporating societal concerns and values into the innovation process, which can help ensure that research outcomes are relevant and responsive to real-world needs. Second, the approach enables the technological knowledge exchange and bridges universities' research with the industry with access to the running information systems

[2] https://digital-strategy.ec.europa.eu/en/policies/desi

and stakeholders. Finally, the government's involvement enables research-based cybersecurity policy development and its delivery on the national level.

Having expertise in cybersecurity as well as having access to the ecosystems of ICT advanced regions, the project partners are working on building the knowledge base for the selected establishing security-related challenges. The project consortium involves universities, large and small companies, governmental information security agencies and some other regional players (see Table 1).

Table 1
Project partners.

Partner type	Estonia	South Moravia
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 (NUKIB)
Other	Estonian Information Security Association	CyberSecurity Hub, South Moravian Innovation Centre

3. Setup and Research Scope

The research activities within the project are conducted as small-scale research projects within the selected six Challenge Areas (CAs). The CA are defined in a way that (i) a particular strength of one region either allows knowledge transfer that will significantly improve the quality of R&I partner region or where (ii) both regions deliver excellent R&I, which justifies the assumption that their connection may result in synergies for developing the cybersecurity strategy. CAs work largely independently of each other and have a high degree of autonomy. At the beginning of the project, each CA defined several priorities and started two to three small-scale research projects. Every year, the teams evaluate their research and are free to shift their research focus. Along with the research priorities, each CA has a defined plan for disseminating the research results and training for delivering the knowledge to ICT professionals and society.

Figure 1 depicts the targeted CAs. Two of the "grounding" CAs are focused on post-quantum cryptography and the research and development of formal methods for system verification. Three other CAs are focused on analysing the security of information systems (based on blockchain or the Internet of Things) and their security certification. The final CA concerns the human aspects of cybersecurity. Below in the paper, we focus on the three CAs that are the most relevant to information systems engineering.

The CA **"Internet of Secure Things (IoST)"** aims to design, validate and deploy IoST systems in various sectors, such as transportation. The designed transportation information systems (e.g., smart parking) should demonstrate how advanced technologies allow for improved security.

Within CA **"Security Preservation in Blockchain"**, the research aims to (i) illustrate the

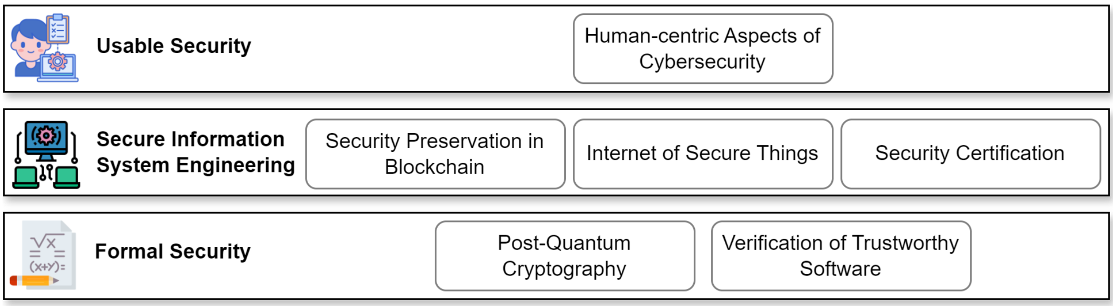
Usable Security
Human-centric Aspects of Cybersecurity
Secure Information System Engineering
Security Preservation in Blockchain
Internet of Secure Things
Security Certification
Formal Security
Post-Quantum Cryptography
Verification of Trustworthy Software

Figure 1: Targeted Challenge Areas.

state-of-the-art use of blockchain in the vehicular communication environment; (ii) develop building blocks for hardware wallets with multiparty computation (MPC); and (iii) demonstrate that blockchain can be used to manage traffic signals for emergency vehicles.

For **"Security Certification"**, we will (i) develop lightweight and automated (re)certification processes to ensure scalability; (ii) develop methods of cybersecurity certification and deployment that ensure all layers and threats are correctly weighted. Additionally, we will develop security certification labels for devices, software and organisations that provide a simple and unambiguous depiction of the level(s) of the security being certified.

4. Current Status and Intermediate Results

4.1. Formal Security Methods

The research on formal security methods resulted in the following publications [5, 6, 7, 8] on software verification and testing. We have organized several events to bring actors from different sectors together. For example, researchers and practitioners in formal methods from academia and industry shared practical experience with methods and tools for software analysis, verification and testing during the *Industrial Day 2023* organized in Brno, Czechia. Meanwhile, the feasibility of post-quantum cryptography usage in the systems has been investigated in [9, 10, 11].

4.2. Usable Security

As a part of the human-centric aspects of cybersecurity, Masaryk University prepared multiple cybersecurity training events for students and educators using their open-source interactive learning environment (KYPO Cyber Range Platform [3] and Cyber Sandbox Creator [4]). As a result, the analysis of the cybersecurity training system [12] usability has been presented in [13].

As a part of the research that focuses on improving the usability of penetration testing reports, we organised two workshops in Estonia with two main objectives. First, we showed what is hiding behind the penetration testing reports. Second, we aimed to find the pain points

[3] https://crp.kypo.muni.cz/

[4] https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator

of penetration testing reports and get the feedback on how to improve the quality of such reports. The workshops were tailored to cater to a diverse audience, ranging from technical professionals such as developers, validators, and administrators, to cybersecurity managers and decision-makers.

4.3. Secure Information System Engineering

At the time of writing the paper, there are a few results of interest to the information system engineering community. Within the CA of "Internet of Secure Things", Daubner et al. [14] developed a forensic readiness qualitative factor reference model that supports the requirements elicitation for forensic-ready software systems. In [15], the authors conducted a case study of integrating forensic readiness capabilities into SensitiveCloud, an information system for storing and processing sensitive data. Additionally, within CA, we conducted an empirical study on information security and privacy management in intelligent transportation systems in Estonia and South Moravia [16]. For disseminating the results and bringing the external practitioner to the discussion on building secure intelligent infrastructure systems, the *International Workshop on Security and Privacy in Intelligent Infrastructures* [5] in conjunction with the *18th International Conference on Availability, Reliability and Security* (ARES 2023) has been organised. During the next year of the project, we will continue the analysis of security-aware and privacy-preserving smart parking and ride-sharing solutions (as examples of intelligent transportation systems). After, we will start the investigation of security and privacy automated systems and technologies, focusing on manufacturing systems, similar to the study in [16].

Within the CA "Security Certification", two tools have been researched and developed, which aim to support the certification of organisations and their information systems:

- **MASS** [6]: The European NIS2 directive [17] aims to enhance the security of the digital society by mandating that various sectors adopt security measures. To assess progress, systematic evaluation of security levels is crucial. F4SLE (the framework for security level evaluation) [18], along with its updating method MUSE and presentation engine MASS [19], provides institutions with immediate feedback on their security status, enables benchmarking, and centralises aggregated data for comprehensive evaluation.
- **`sec-cert`** [7]: Security certification frameworks like Common Criteria and FIPS 140 form a large landscape of thousands of certificates, security targets, and protection profiles. Using data mining and natural language processing, we developed insights into the certification ecosystem dynamics and proactive analysis of the impact of past and possible future vulnerabilities. The expertise available within the CHESS project enabled us to improve the usefulness of analyses and features available to end-users and better assess the impact of certification rigour level on subsequent frequency and seriousness of the product vulnerabilities [20].

During the next year, the certification tools will be validated further. Additionally, the CA "Security Certification" will start research on the common criteria protection profile for secure

[5] https://2023.ares-conference.eu/workshops-eu-symposium/sp2i-2023/

[6] https://mass.cloud.ut.ee/massui/

[7] https://seccerts.org/

computing applications.

To address the challenge of security preservation in blockchain, a series of workshops is developed to educate industry representatives and students. Within each event, the attendants learn what blockchain is and when information systems engineers should consider a decentralised application as a part of the information system [21]. One of the recently started small-scale projects explores secure information transmission in intelligent vehicles. Additionally, the usage of blockchain-based identity management for securing cross-organisational data exchange between standalone information systems has been explored in [22]. Within the upcoming year, the CA will also start research on the privacy of blockchain transactions and methods like zero-knowledge proof for more compact and secure blockchain-based systems.

5. Future activities

The future activities within the CHESS project include the research within the challenge areas mentioned above, along with applying the research results to the development of cross-border joint cybersecurity R&I strategy. Based on the identified opportunities and needs obtained from the research results in small-scale projects, the project will outline actions to be taken. The actions will involve: (i) formulating an action plan for each research area; (ii) training and knowledge sharing; (iii) inter-sectoral and inter-regional knowledge transfer; (iv) development of the investment plan with the goal of innovation ecosystem support through creating CHESS-enabled cybersecurity start-ups or spin-offs; and (v) outreach activities.

To support the highlighted activities, the project partners will organise brokerage events. The goals of such events are: (i) to get feedback on ongoing and future CHESS research directions from the viewpoints of different sectors (industry, academia, government and civil society), (ii) to gather people and organisations to form international project consortia, and (iii) to enlarge the CHESS network of collaborators. The first brokerage event will take place on 31 July – 1 August.2024 in the Czech Republic, during ARES conference [8] to attract its participants. The second brokerage event will take place in Tallinn, Estonia in autumn.

For increasing teaching capacity within the regions, CHESS partners will participate in training on how to conduct cybersecurity training for students and professionals using the MUNI open-source interactive learning environment (KYPO Cyber Range Platform and Cyber Sandbox Creator). Pilot courses will be held for students (high school and university) and end-users (IT professionals) across both CHESS regions.

6. CHESS and Information Systems Engineering Research

Among six CAs targeted in the CHESS project, four of them are of primary interest to the information systems engineering (ISE) community. Thus, research activities within CAs for the Internet of Secure Things (IoST), Security Preservation in Blockchain, and Security Certification altogether aim to improve the quality of developed information systems of the selected type. While ISE research focuses on eliciting and assuring the functional and non-functional

[8] https://www.ares-conference.eu/

requirements of the built systems, the research within the mentioned CHESS areas aims to show how the non-functional requirements can support, enforce or prevent the expected information system operations. Thus, within CHESS we investigate intersection of security and privacy requirements with other typed of requirements, and analyse the trade-offs, dependencies, constraints, and integrations involved in meeting these requirements in the information systems. Additionally, the research in the area of Human-Centric Aspects of Cyber-Security analyses how to train users in selected aspects of cybersecurity and also how to make security features usable within the information systems.

As a result, we believe that collaboration between the ISE community and CHESS can, first, supply the project with new open research questions originating from information systems engineering and, second, provide the ISE community with the developed open-source solutions for securing the systems.

Finally, as a part of the developed strategy, our research produces best practices and guidelines for secure system design and development. Thus, information system engineers can benefit from these insights by incorporating them into their design processes, leading to more resilient and secure information systems.

As the new small-scale projects are reviewed each year and the next review takes place in December 2024, the project partners are open to proposals on research topics originating from ISE community needs. Also, having some intermediate results, the project participants are open to requests of the ISE community to demonstrate the developed solutions and show how to apply them to the running information systems.

Acknowledgments

This paper is supported by the European Union under Grant Agreement No. 101087529.
The paper authors are grateful to all the CHESS project participants for their contribution.

References

[1] Cyber-security Excellence Hub in Estonia and South Moravia. Project description, 2022. https://doi.org/10.3030/101087529.

[2] E. G. Carayannis, D. F. Campbell, 'Mode 3'and'Quadruple Helix': toward a 21st century fractal innovation ecosystem, International journal of technology management 46 (2009) 201–234.

[3] E. G. Carayannis, D. F. J. Campbell, Mode 3 Knowledge Production in Quadruple Helix Innovation Systems, Springer New York, 2012, pp. 1–63. doi:10.1007/978-1-4614-2062-0_1.

[4] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, 2020.

[5] V. Malík, F. Nečas, P. Schrammel, T. Vojnar, 2ls: Arrays and loop unwinding, in: S. Sankaranarayanan, N. Sharygina (Eds.), Tools and Algorithms for the Construction and Analysis of Systems, Springer Nature Switzerland, Cham, 2023, pp. 529–534.

[6] T. Schwarzová, J. Strejcek, J. Major, Reducing acceptance marks in emerson-lei automata

by QBF solving, in: SAT, volume 271 of *LIPIcs*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, pp. 23:1–23:20. doi:10.4230/LIPICS.SAT.2023.23.

[7] D. Klaska, A. Kucera, M. Kurecka, V. Musil, P. Novotný, V. Rehák, Synthesizing resilient strategies for infinite-horizon objectives in multi-agent systems, in: IJCAI, ijcai.org, 2023, pp. 171–179.

[8] D. Klaška, A. Kučera, V. Kůr, V. Musil, V. Řehák, Optimizing local satisfaction of long-run average objectives in markov decision processes, 2023. arXiv:2312.12325.

[9] P. Muzikant, J. Willemson, Deploying post-quantum algorithms in existing applications and embedded devices, in: Ubiquitous Security, Springer Nature Singapore, 2024, pp. 147–162. doi:10.1007/978-981-97-1274-8_10.

[10] P. Dobias., S. Ricci., P. Dzurenda., L. Malina., N. Snetkov., Lattice-based threshold signature implementation for constrained devices, in: SECRYPT, INSTICC, SciTePress, 2023, pp. 724–730. doi:10.5220/0012112700003555.

[11] P. Dobias, L. Malina, P. Ilgner, P. Dzurenda, On efficiency and usability of group signatures on smartphone and single-board platforms, in: ARES, ACM, 2023, pp. 127:1–127:9.

[12] Masaryk University, KYPO cyber range platform, n.d. https://docs.crp.kypo.muni.cz/.

[13] V. Švábenský, J. Vykopal, P. Čeleda, J. Dovjak, Automated feedback for participants of hands-on cybersecurity training, Education and Information Technologies (2023).

[14] L. Daubner, R. Matulevičius, B. Buhnova, A model of qualitative factors in forensic-ready software systems, in: Research Challenges in Information Science: Information Science and the Connected World, Springer Nature Switzerland, Cham, 2023, pp. 308–324.

[15] L. Daubner, R. Matulevicius, B. Buhnova, M. Antol, M. Ruzicka, T. Pitner, A case study on the impact of forensic-ready information systems on the security posture, in: CAiSE, volume 13901 of *Lecture Notes in Computer Science*, Springer, 2023, pp. 522–538.

[16] M. Bakhtina, R. Matulevičius, L. Malina, Information security and privacy management in intelligent transportation systems, Complex Systems Informatics and Modeling Quarterly (2024) 100–131. doi:10.7250/csimq.2024-38.04.

[17] European Parlament, Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive), 2022.

[18] M. Seeba, T. Oja, M. P. Murumaa, V. Stupka, Security level evaluation with F4SLE, in: ARES, ACM, 2023. doi:10.1145/3600160.3605045.

[19] M. P. Murumaa, Designing a Security Sensitive Self-assessment Framework, Master's thesis, University of Tartu, 2023. URL: https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=77886.

[20] A. Janovsky, J. Jancar, P. Svenda, Łukasz Chmielewski, J. Michalik, V. Matyas, sec-certs: Examining the security certification practice for better vulnerability mitigation, 2023. arXiv:2311.17603.

[21] M. Iqbal, Blockchain and decentralized application development, 2023. https://chess-eu.cs.ut.ee/2023/06/22/blockchain-workshop.

[22] M. Bakhtina, K. L. Leung, R. Matulevičius, A. Awad, P. Švenda, A decentralised public key infrastructure for X-Road, in: ARES, ACM, 2023, pp. 128:1–128:8. doi:10.1145/3600160.3605092.