D3.1 Mid-term evaluation report of CHESS R&I activities

Project Name	Cyber-security Excellence Hub in Estonia and South Moravia
Project acronym	CHESS
Grant agreement no.	101087529
Call	HORIZON-WIDERA-2022-ACCESS-04
Type of action	HORIZON-CSA
Project starting date	1 January 2023
Project duration	48 months
Deliverable Number	D3.1
Deliverable name	Mid-term evaluation report of CHESS R&I activities
Lead Beneficiary	CYBER
Type	R – Document, report
Dissemination Level	PU – Public
Work Package No	WP3
Date	20 December 2024
Version	1

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.

Editor

- Liina Kamm (CYBER)

Contributors

- Raimundas Matulevičius (UTARTU)
- Lukáš Malina (BUT)
- Václav Matyáš (MUNI)
- Liina Kamm (CYBER)
- Antonín Kučera (MUNI)
- Pawel Sobocinski (TalTech)
- Mubashar Iqbal (UTARTU)
- Petr Švenda (MUNI)
- Jan Willemson (CYBER)
- Jan Hajný (BUT)
- Pavel Čeleda (MUNI)
- Martin Ukrop (Red Hat)
- Alo Lilles (Guardtime)
- Hendrik Pillmann (RIA)

Reviewers

- Zuzana Vémolová (MUNI)
- Václav Matyáš (MUNI)

CHESS Consortium

Participant organisation name	Short name	Country
Masaryk University	MUNI	Czechia
University of Tartu	UTARTU	Estonia
Brno University of Technology	BUT	Czechia
Tallinn University of Technology	TalTech	Estonia
Cybernetica AS	CYBER	Estonia
Red Hat	RedHat	Czechia
Guardtime	Guardtime	Estonia
Estonian Information System Authority	RIA	Estonia
CyberSecurity Hub	CSH	Czechia
National Cyber and Information Security Agency (associated)	NCISA	Czechia
South Moravian Innovation Centre (associated)	JIC	Czechia
Estonian Information Security Association (associated)	EISA	Estonia

Abbreviations

CA – challenge area
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
ICT – information and communication technology
KPI – key performance indicator
NGO – non-governmental organisation
R&I – research and innovation
TA – target audience
R&I – research and innovation
IoST – Internet of secure things
IoV – Internet of vehicles
NCSC-EE – National Cyber Security Center
CERT-EE – Estonian Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
ITS – intelligent transportation systems
AI/ML – artificial intelligence/machine learning
QUB – Queen's University Belfast
TTX – tabletop exercise
MPC – multi-party computation
TEE – trusted execution environment
ST – security target

Executive Summary

The CHESS project is designed to enhance cybersecurity through comprehensive research and innovation solutions. The project tackles critical cybersecurity challenges by focusing on several key areas: the Internet of secure things, security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography, and human aspects of cybersecurity. The project team is dedicated to both researching these areas and disseminating the findings to a wide range of stakeholders to improve understanding and adoption of advanced cybersecurity measures.

Research efforts under the CHESS project began with consolidating knowledge and expertise from Estonia and South Moravia. The project team mapped existing knowledge and expertise, identified new research directions, and organised the work into various challenge areas. These areas are further divided into smaller, self-contained tasks called mini-projects, each with its own timeline. To date, the project has initiated 23 mini-projects, of which 7 have been completed and 16 are ongoing.

The first two years of the CHESS project were primarily dedicated to reinforcing existing research and innovation collaborations through joint mini-projects. The project team has also started engaging with external parties to gather input and involve them in the project, thereby expanding the research network and fostering new cross-regional collaborations.

The potential impact of the CHESS project is significant, with the possibility to strengthen cybersecurity across various sectors such as transportation, finance, healthcare, and governance. By providing robust frameworks, tools, and methodologies, the project aims to help organisations and governments develop more secure systems and processes.

Table of Contents

1 Introduction

The CHESS project aims to strengthen cybersecurity through comprehensive research and innovation solutions. The project addresses critical cybersecurity challenges by focusing on several key areas: the Internet of secure things (IoST), security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography, and human aspects of cybersecurity. The project team is working on both basic research and the dissemination of research results. By engaging with a wide range of stakeholders, our goal is to enhance the understanding and adoption of these cutting-edge cybersecurity measures.

Research activities under the CHESS project started with the mapping and consolidation of knowledge and expertise from Estonia and South Moravia. Each of the research groups shared their knowledge of the state of the art, and new research directions were established collectively. As cybersecurity is a rapidly developing field, dynamic topic definitions are required for collaboration. CHESS has resolved this issue by opting to organise the work in different challenge areas through the definition of smaller tasks called mini-projects. These self-contained tasks have different durations, with some lasting for the whole project period while others will conclude when a satisfactory result is achieved. A number of initial mini-projects were proposed for each challenge area at the start of the project; more can be introduced over the project's life cycle. 23 mini-projects have been initiated so far (7 completed, 16 ongoing) and more will be launched at the beginning of 2025.

The focus of the first two years of the project has been on the reinforcement of existing research and innovation collaborations through joint mini-projects. The project team has also started engaging different external parties both to get their input and to involve them in the project work, thereby establishing new cross-regional collaboration opportunities and widening the research network.

The results of the CHESS project have the potential to enhance cybersecurity across various sectors, including transportation, finance, healthcare, and governance. By providing robust frameworks, tools, and methodologies for addressing cybersecurity challenges, the project can help organisations and governments develop more secure systems and processes.

In Section 2, we give an overview of the different challenge areas and their goals. Section 3 describes the completed and ongoing mini-projects from the first two years. Section 4 lists the scientific output of the project, namely publications, theses, and software and methodology artefacts. In Section 5, we discuss the impact of the research done under the CHESS project, and Section 6 talks about plans for the future of the project.

2 CHESS Challenge Areas

CHESS conducts research in 6 challenge areas (CAs): Internet of secure things, security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography and human aspects of cybersecurity. In this section we give an overview of the different challenge areas and their goals.

CA1: Internet of Secure Things (IoST)
The goal of CA1 is to develop a secure Internet of things (IoT) that safeguards against exploitable vulnerabilities in connected devices. This is crucial as these systems are integrated into everyday life. Industrial actors need trusted components and comprehensive guidance on incorporating privacy by design and deploying new technologies securely. Current security mechanisms often fall short for IoT, making it difficult to ensure comprehensive protection. IoT devices are evolving beyond basic connectivity to advanced data analysis, increasing the need for robust security and privacy measures. Addressing privacy at the design stage by using techniques like data minimisation and advanced cryptographic methods is essential. Balancing security, accessibility, and privacy requires integrating quantum-resistant solutions, distributed ledgers, blockchain technologies, and AI-assisted security techniques.

CA1 aims to promote effective approaches that public and private organisations can take to support the transition to and secure management of IoST systems. CA1 focuses on the development, validation, and deployment of IoST systems in various sectors, such as transportation.

Current topics in CA1 are:

- Empirical research on security and privacy management in intelligent infrastructure systems;
- Privacy-preserving smart parking solutions;
- Secure and privacy-preserving access to sharing vehicles in smart cities;
- Security risk management in automated systems and technology;
- Security and privacy in teleoperated systems.

CA2: Security Certification
Security certification increases users' trust in complex technologies through the validation of products by recognised bodies. Two schemes currently play the most significant role at the international level: Common Criteria (CC) and FIPS 140-2/3. New areas such as supply chain management are creating new certification requirements. Certification now covers not just devices but also organisational structures and software, with stricter requirements related to new threats.

The main challenges include harmonising various certification schemes to facilitate comparisons, and standardising new cybersecurity technologies with flexible certification processes. Despite these challenges, new schemes should align with existing standards.

CA2 aims (1) to develop lightweight and automated (re)certification processes to ensure scalability, and (2) to use automatic structuring to provide transparency of vulnerabilities in certified devices. CA2 will develop methods of cybersecurity certification and deployment that ensure all layers and threats are correctly weighted, and security certification labels for devices, software and organisations that provide a simple and unambiguous depiction of the level(s) of the security being certified.

Current topics in CA2 are:

- Enriching certification report analysis with other open-source intelligence;
- Testing and improving a method for evaluating organisations' information security;
- Creating protection profiles (PPs) for secure computing.

CA3: Verification of Trustworthy Software
Ensuring the reliability of trustworthy software is crucial for maintaining the integrity of digital systems and reducing issues caused by software errors. Unlike traditional industrial products that have well-established verification standards and methods, commercial software often falls short in terms of verification processes. This gap largely stems from the inherent complexity, limited controllability, and high expectations placed on software, which are not yet adequately addressed by universally accepted certification methods, algorithms, or software tools for automated analysis, verification, and design.

Enhanced methods for the development of trustworthy software can yield significant economic benefits by helping companies avoid software failures. Software developers can also gain a competitive edge from the certification of specific quality attributes of their products.

CA3 aims to use program analysis techniques to improve software development, develop a theory of composable cybersecurity protocols, and offer visual accounts of organisational cybersecurity protocols understandable to non-experts.

Current topics in CA3 are:

- Development of theory and tool support for cybersecurity protocols;
- Emerging problems in formal methods.

CA4: Security Preservation in Blockchain:
Blockchain is a decentralised, distributed, and immutable ledger technology where the ledger is shared among the nodes of a computer network. Blockchain technology introduces major disruptions to traditional operations through the establishment of secure and decentralised governance that does not require trusted third parties to establish transactional relationships between two parties. Blockchain provides the basic building blocks for trust between stakeholders and improves the reliability of data and the immutability of agreed transactions. A decentralised blockchain is less vulnerable to attacks and improves participants' privacy. Blockchain technology ensures legal certainty via smart contracts and digital assets.

CA4 focuses on enhancing the reliability, resilience, and trustworthiness of blockchain technology by tackling critical technical issues. Essential areas of improvement include

smart contract mechanisms for secure trust-building, verification of resilient cryptographic solutions for cryptocurrency wallets, and implementation of privacy-enhancing techniques for data management and transmission. Additionally, it addresses the privacy of transaction data, identity management within the self-sovereign identity framework, and secure multi-party signatures to mitigate risks from supply-chain attacks and software vulnerabilities. These advancements ensure a robust blockchain ecosystem adaptable to evolving security needs. Moreover, CA4 prioritises training programs to build expertise in blockchain security among professionals and researchers, addressing an industry-wide need for skilled practitioners. By raising awareness of blockchain, CA4 ensures a long-term role for blockchain technology in secure digital transformation and promotes it as a trusted tool in various sectors.

Current topics in CA4 are:

- Secure information transmission using blockchain in intelligent vehicular communication;
- Decentralised Public Key Infrastructure for X-Road and securing organisational identity through distributed key management;
- Blockchain-relevant operations protected by a combination of cryptographic hardware and threshold multiparty signatures;
- Analysis of Bitcoin CoinJoin protocols, estimation of their anonymity sets and Sybil attacks.

CA5: Post-Quantum Cryptography

Quantum computers exploit quantum mechanical phenomena to solve complex mathematical problems that are beyond the capabilities of traditional computers. The rapid development and recent advancements in quantum computing are a threat to the security of conventional cryptographic methods, undermining the confidentiality and integrity of digital communications. The objective of post-quantum cryptography (PQC) is to create cryptographic systems that are secure against both quantum and non-quantum attacks, while maintaining compatibility with existing communication protocols and networks. Early versions of quantum computers already exist, and it is anticipated that a quantum computer capable of running the Shor algorithm will be constructed soon. Once this happens, most current asymmetric encryption and authentication algorithms will become insecure. Ensuring the long-term security of Digital Europe calls for promoting advance the development of quantum-safe technologies, including PQC, which must be secure, cost-effective, and interoperable with current systems.

CA5 aims to evaluate the current state and practical applicability of post-quantum technologies and assess the usability and market viability of information security products based on post-quantum algorithms.

Current topics in CA5 are:

- Evaluation of replacement of classical asymmetric algorithms with post-quantum algorithms;
- Updating an electronic voting solution with PQC and testing the result.

CA6: Human-Centric Aspects of Cybersecurity:
The effectiveness of cybersecurity heavily relies on human-centric aspects for both professionals and end-users. It is crucial for professionals to receive continuous training on emerging technologies and new threats. Cybersecurity education is widely provided at European universities and companies, but assessing team learning in this context remains challenging without objective measures.

Usable security is vital for end-users, ensuring that security products are user-friendly. However, many technologies (e.g., the PGP encryption system) are complex and, hence, face usability issues, which in turn make it harder to reach the intended security and privacy goals. While improvements have made end-to-end encrypted communications more accessible, user authentication still faces challenges. Moreover, in some cases trade-offs must be made between usability and security/privacy, meaning that a system's design could favour one aspect over the other.

CA6 aims to improve cybersecurity training and enhance the usability of cybersecurity solutions for ICT professionals.

Current topics in CA6 are:

- Evaluate the automated feedback upgrade to the KYPO Cyber-range Platform (an open-source interactive learning environment for hands-on cybersecurity training);
- Enhancing cybersecurity training through hands-on and tabletop exercises;
- Identify and address gaps in the usability of penetration testing reports among ICT professionals.

3 Progress in mini-projects

The CHESS challenge areas are wide in scope, so the research teams have defined smaller tasks that we call mini-projects within each challenge area. These are self-contained tasks, some of which last for the whole project period while others will conclude with the achievement of a specific result. Teams working on each challenge area can propose new mini-projects during the project's life cycle and the General Assembly will advise them on how to proceed. Currently, there are 23 mini-projects, of which 7 have been completed and 16 are ongoing. This section gives an overview of the completed and ongoing mini-projects from the first two years.

3.1 Challenge Area 1: Internet of Secure Things (IoST)

3.1.1 CA1_01: Empirical Research of Information Security and Privacy Management in Intelligent Infrastructure Systems

Status: Completed
Involved: UTARTU, BUT, RIA, CYBER

This mini-project explored the current state of security and privacy management in intelligent infrastructure systems in Estonia and South Moravia. CA1_01 resulted in the Framework for Information Security and Privacy Management (FISP-ProCOP). It was validated in the domain of the intelligent transportation infrastructure. The domain selection was motivated by links to two other small-scale projects.

Firstly, we explored the baseline of state-of-the-art security and privacy management measures represented in specialist literature. The study selected the Reference Model of Information Assurance & Security (RMIAS) and ISACA's Business Model for Information Security (BMIS) as the baseline for the extraction and classification of measures into four dimensions: processes, organisational design, people, and technological solutions.

Secondly, we conducted an empirical study to gather information on the solutions employed by companies in Estonia and South Moravia. Our goal was to compare them with the baseline measures. More specifically, our goal was to explore what policies, approaches, methods, and techniques for information security and privacy management have been used in intelligent transportation systems and how they support the transformation of businesses to rely on the intelligent infrastructure system. The main difficulty of this small-scale project was finding people willing to answer the questionnaires. We received answers from eight Estonian companies and seven South Moravian companies. To mitigate the risks related to the low number of responses, we explored gathering data from openly accessible documents produced by companies included in the study: official documentation (incl. privacy policies, information security code of practice, and general terms and conditions) and information found on official company websites. Besides exploring the state of the art, we directly presented the CHESS project to the companies contacted in both regions to establish and/or strengthen future cooperation in this field.

The results of CA1_01 have been published in two papers: Bakhtina M. (2023) and Bakhtina M. *et al.* (2024); see Section 4 for details.

3.1.2 CA1_02: Analysis of Security-Aware and Privacy-Preserving Smart Parking Solutions

Status: Completed
Involved: UTARTU, BUT, MUNI, CYBER

This mini-project focused on researching secure and privacy-preserving solutions for vehicle parking solutions. The main objectives included (i) exchanging requirements and lessons learnt from the previous R&D activities, (ii) expanding a secure and privacy-preserving design, and (iii) exploring how to design security and privacy-preserving means into the parking scenario. This small-scale project was a continuation of the SPARTA activities where UTARTU and BUT collaborated in the High Assurance Intelligent Infrastructure Toolkit (HAII-T) Program.

As a part of this mini-project, we also proposed a risk-based approach to forensic readiness design (Daubner et al., 2023a, 2023b). A tool to support a risk-based approach to forensic readiness design was developed (Daubner et al. 2024).

We explored the application of group signatures (Dobias et al., 2023). The results indicate that current handheld devices can already effectively perform the main phases of group signatures and make these schemes practical for deployment in scenarios requiring privacy.

We also considered how privacy regulation requirements could be implemented in the parking scenario using the DPO <https://dpotool.cs.ut.ee> and pLeak <https://pleak.io/home> tools. This activity was done as part of a thesis.

Overall, the results of CA1_02 have been published in four conference papers: Daubner et al., 2023a, 2023b, 2024, and Dobias et al., 2023; see Section 4 for details.

The CA1_02 mini-project resulted in one demonstrator: *FREAS: Forensic-Ready Analysis Suite*. URL: https://youtu.be/Y38zS_6XY-I?si=fNT2yQqm2W2-5-f5

One thesis related to CA1_02 was defended by Sander Truu (2024).

3.1.3 CA1_03: Secure and Privacy-preserving Access to Sharing Vehicles in Smart Cities

Status: Ongoing
Involved: BUT, UTARTU, MUNI, CYBER

The objective of CA1_03 is to explore different car-sharing scenarios. We plan to apply a security risk management approach to elicit security risks and their countermeasures and to design secure and privacy-preserving solutions. The project started with an analysis of how privacy-enhancing technologies can support car-sharing services. We have performed a systematic literature review to explain the context, protected assets, risks and risk treatment strategies in the car-sharing scenarios.

So far, CA01_03 has resulted in one paper by Malina, L. et al. (2024), and a thesis related to CA1_03 was defended by Ijeoma Faustina Ekeh.

3.1.4 CA1_04: Security Risk Management in Automated Systems and Technology

Status: Ongoing
Involved: UTARTU, BUT, RIA, MUNI

The objective of CA1_04 is to explore security risks in automated systems and technologies, focusing on manufacturing systems. The expected result is a report that identifies and explains these cyber security risks, along with suggesting practical ways to reduce them. We aim to perform a few use-case analyses of the selected manufacturing systems. The mini-project is in its initial stages and the expected outcomes are a publication, an analysis report, and a thesis.

3.1.5 CA1_05: Security and Privacy in Teleoperated Systems

Status: Ongoing
Involved: UTARTU, BUT

The objective of CA1_05 is to analyse different teleoperation scenarios. We aim to determine protected assets and security risks and to elicit security countermeasures. We aim to design secure and privacy-preserving solutions for teleoperated systems. The mini-project is in its initial stages and the expected outcomes are a publication, an analysis report, and a thesis.

3.2 Challenge Area 2: Security Certification

3.2.1 CA2_01: Enriching Certification Report Analysis with Other Open Source Intelligence

Start: Ongoing
Involved: MUNI, CYBER, Red Hat Czech, RIA

The CA2 team has researched and developed *sec-certs*, a tool aiming to support the certification of organisations and their information systems.

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 dynamics of the certification ecosystem and the 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.

Work on the improvement of the toolset has proceeded as planned. Core toolset development is at this moment done at MUNI in close collaboration with Red Hat with additional cooperation and feedback from NUKIB, CYBER and RIA, involving both online and physical meetings and discussions. We started investigating the use of natural language processing (NLP) approaches to improve the toolset.

We plan to improve the UI of seccerts.org and create a dashboard with business intelligence. We also plan to improve the data management of the tool and further investigate the use of NLP.

One thesis related to CA2_01 was defended by Erik Moravec (2023); see Section 4 for details.

3.2.2 CA2_02: Testing the Method for Evaluating Organisations' Information Security Level

Start: Ongoing

Involved: UTARTU, RIA, CYBER, MUNI, CSH

Within this mini-project, we have been testing a tool for online self-assessment of information security level of organisations from different sectors both in Estonia and South Moravia, i.e. municipalities, private sector, healthcare, education, ICT, non-profit, government office, finance.

The European NIS2 directive aims to enhance the security of the digital society by mandating the adoption of security measures by various sectors. To assess progress, systematic evaluation of security levels is crucial. F4SLE (the framework for security level evaluation), along with its updating method MUSE and presentation engine MASS, provides institutions with immediate feedback on their security status, enables benchmarking, and centralises aggregated data for comprehensive evaluation.

F4SLE pilot testing for online self-assessment has been more active on the Estonian side (as expected – the standard it is based on is an Estonian standard and the effort is pushed by RIA and UTARTU), and involving Czech respondents takes significantly more effort than expected. In the 2023 version of the questionnaire, there were 77 respondents (60 EE, 17 CZ). For the 2024 version, there have been 82 respondents from Estonia so far.

F4SLE has also been updated and translated to English. The tool can be found at https://mass.cloud.ut.ee/massui/#/.

We plan to analyse the existing data and publish the results, harmonise the tool with regulations (NIS2 and national regulations), update F4SLE and MASS, develop new use cases, and translate everything to Czech to facilitate engagement from the Czech stakeholders.

3.2.3 CA2_03: Common Criteria Protection Profile for Secure Computing Applications as PETs

Start: Ongoing
Involved: CYBER, MUNI

Initially, we aimed to define a Common Criteria (CC) protection profile (PP) for secure computing applications as privacy enhancing technologies. We started by acquainting ourselves with the landscape to determine whether a CC PP is indeed the best solution for this problem, as creating a comprehensive PP is a difficult task that is best done in collaboration with different parties who work on different approaches to the problem. We have since determined that under the new European Common Criteria scheme, a security target (ST) will help us achieve our goals efficiently.

We have determined the scope of the ST and are gathering requirements and priorities from stakeholders. Our investigation led us to the decision to create two different STs for different technologies (secure multi-party computation (MPC) and trusted execution environments (TEEs)).

We organised a workshop with external experts to consult on the PP, ST, and certification best practices and current developments, and started gathering requirements and priorities from stakeholders. We have chosen to prepare a ST for MPC due to more immediate exploitation opportunities.

We expect this task to end in two published STs: one for MPC and the other for TEEs.

3.3 Challenge Area 3: Verification of Trustworthy Software

3.3.1 CA3_01: The Deployment of Program Analysis Techniques to Practical Software Development

Status: Ongoing
Involved: MUNI, BUT, Red Hat, CYBER

The work is organised into the following tasks aimed at developing program analysis techniques and subsequently evaluating them in the industrial environment.
Subtasks 1, 2 and 4 concentrate on the development of tools for technology transfer, Subtasks 3 and 5 are devoted to specific problems of fundamental research.

Task 1. DiffKemp
We expand and improve the DiffKemp tool (https://github.com/viktormalik/diffkemp) that aims to check the preservation of the semantics of low-level code during refactoring. We check the preservation of the use of various system parameters, support more semantics-preserving change patterns, their automatic derivation, and/or incorporating heavier-weight formal methods into the mix of light-weight methods currently used by DiffKemp.

During the project, we have released two new versions of DiffKemp. Both versions significantly improve the developer experience, allowing easier onboarding of new developers for the project. Version 0.5 introduced a new visualisation method, an interactive web-based browser, for presenting DiffKemp results to users. This greatly improves the tool's user experience and is a major step towards better usability in practice. Version 0.6 introduced two new built-in patterns for semantic equivalence, effectively extending the set of programs that DiffKemp can correctly analyse.

We have started work on introducing formal methods to the tool (in the form of SMT solving) which will allow to correctly analyse an entire new class of semantic-preserving refactorings. The first results target changes in single statements or expressions. This has turned out to be useful in practice, but our aim is to expand this approach to larger code sections. Further, we also plan to simplify the process of creating user-defined patterns of semantic-preserving changes.

Task 2. Perun
We improve the efficiency of Perun (https://perfexionists.github.io/perun/overview.html), a dynamic performance analyser. More specifically, we concentrate on reducing the amount of data collected during code profiling by suitably selecting the code to be profiled and the frequency with which performance data should be collected, such that the impact on the

precision is minimal. Moreover, we are expanding the suite of algorithms used by Perun for collecting performance data, visualisation, and detection of performance regressions.

We have expanded the Perun tool suite with several lightweight profilers (support for the perf profiler and a lightweight eBPF-based profiler) and methods for the interpretation of the differences between performance results (mainly based on flame graphs and Sankey graphs). We have also focused on the optimisation of the profiling process itself. We mainly build methods for efficient representation of the program control flow with respect to the underlying versioning control systems. This improves both the efficiency of the profiling as well as the precision of the results. This work is yet to be merged into our upstream. Finally, we also maintained the tool and optimised some core functions allowing Perun to be used on the latest systems. These changes allow us to apply the Perun tool suite on a wider range of programs as well as more complex systems (such as the Linux kernel).

Quite importantly, our recent modifications to Perun included allowing it to analyse not only user-space applications but also the Linux kernel itself. This was motivated by a lot of interest in the Red Hat kernel performance team in applying Perun for analysing new versions of the Red Hat Enterprise Linux (RHEL) kernel and in diagnosing performance problems in it. After Perun started to be able to analyse the RHEL kernel, it is now beginning to be applied in production, and the first reports we received indicate that it is indeed helping the Red Hat kernel performance team to boost productivity of their work.

Task 3. Fundamental research
We are working on improving the methods for deciding separation logic with applications in analysis of low-level memory-manipulating programs, the logic-based analyses of memory manipulating programs, and light-weight code analyses, e.g. for detecting performance-related and concurrency-related problems. We are also analysing and synthesising stochastic systems.

Task 4. Fizzer
We plan to modify our Fizzer academic tool for automated test generation based on grey-box fuzzing to make it applicable to some core utilities and similar software. We then plan to evaluate its practical applicability and delivered value in an industrial setting. The tool placed 3rd in the Cover-Branches category in Test-Comp (Competition on Software Testing) 2024.

One of the examples of experimental tools implementing state-of-the-art technologies is Symbiotic, a state-of-the art program analysis tool. Symbiotic works with C programs and focuses on finding assertion violations, memory errors, memory leaks, and undefined behavior. Symbiotic can also prove that such errors are not present in the given program.

3.3.2 CA3_02: Development of Theory and Tool Support for Cybersecurity Protocols

Status: Ongoing
Involved: CYBER, TalTech

We are working on applying techniques from formal semantics of programming languages, in particular programme equivalence, and adapting them to the setting of cryptographic protocols. Rewriting techniques from programming language theory can be used to establish observational equivalence of cryptographic protocols up to probabilistic negligibility. We have looked at a simple programming language capable of polynomial computations over predefined security parameters and established a notion of probabilistic distance between them. From this we have extracted rewrite rules capturing asymptotic equivalence, providing techniques to show that two programs are indistinguishable. We have looked at examples of how these techniques can be used to show privacy of a cryptographic protocol. Initial results have been presented at the Industry Day in Tallinn on 9 December 2024. We are planning to develop this further, bringing together recent research in the semantics of probabilistic programming languages and adapting it to the setting of cryptographic protocols.

3.3.3 CA3_03: Emerging Problems in Formal Methods

Status: Ongoing
Involved: MUNI, BUT, Red Hat, CYBER

The work has concentrated mainly on problems related to the synthesis of efficient and safe software controllers (strategies) for multiagent systems. More specifically, the work is divided into two subtasks.

Task 1. Efficient synthesis of resilient strategies for multi-agent systems.
The goal is to develop efficient strategy synthesis algorithms for multi-agent systems such that the resulting strategy profile is resistant to certain type of agent failures. Preliminary results have been published in a paper accepted to IJCAI 2023.

Task 2. Visualisation of strategy profiles in multi-agent systems
As the functionality of strategy profiles constructed for multi-agent systems can be complicated, we are developing techniques and software tools for appropriate visualisation of their functionality. A prototype tool has already been implemented.

3.4 Challenge Area 4: Security Preservation in Blockchain

3.4.1 CA4_01: Automated Trust Through Self-Sovereign Identity in Data Exchange Systems

Status: Completed
Involved: UTARTU, MUNI

We explored the feasibility of a decentralised approach for organisations' identity management in data exchange systems. More specifically, we focused on the potential of implementing self-sovereign identity (SSI) concepts in data exchange systems and how it affects identity management. The mini-project focused on the case study of the X-Road system – a solution that acts as a data exchange layer and enables secure data exchange between organisations in the public and private sectors. The selection of the system was

motivated by the fact that X-Road is an open-source solution, facilitating the integration and implementation of the proposed solutions directly into the system.

In the first step, we explored the usage of decentralised public key infrastructure (DPKI) together with verifiable credentials (VCs) and a distributed ledger in X-Road. The study resulted in a proposed architecture for a DPKI-based X-Road, which was validated through the proof-of-concept (PoC). The PoC was developed as a part of a master's thesis. The results were synthesised into a workshop paper submitted to the 3rd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I) in conjunction with the 18th International Conference on Availability, Reliability and Security (ARES '23).

In the second step we explored measures for managing organisational identity wallets. We compared commonly used technologies for the storage, usage, and access control of organisational credentials (PKI X.509 certificates for centralised identity management settings and certificateless VCs for decentralised settings).

The major difficulty of this mini project was identifying a set of technologies and their implementations which suited the context of the projects, namely managing the identity of an organisation (not a physical entity). To limit the risk of biased measure selection, we have conducted an iterative literature review during each project step.

The project also investigated how organisations can secure their digital identity (ODI) from abuse by a centralised controller during cross-organisational data exchange. The theoretical contribution of the second part of the mini-project is a key management system for information systems which enables cryptographically assured access policies enforcement that brings zero trust to the control over organisational identity. The practical contribution includes a PoC implementation of the proposed design for the X-Road data exchange system and a library for RSA-threshold implementation. The split of a private key into several private shares in a threshold multi-party implementation additionally enables support for key usage policies. For example, the usage of share A can be limited to working hours between 8:00 and 17:00, the usage of share B to sign requests only from specific domains, and the usage of share C to only three signatures per day. As a result, user-specific policies are enforced, and a valid signature is only created if these policies are fulfilled.

This mini-project has created an open-source library for RSA-threshold implementation and a proof-of-concept implementation of distributed key management system for organisational identity management using threshold signature in X-Road. See Section 4 for more details.

3.4.2 CA4_02: Emergency Information Transmission Using Blockchain in Intelligent Vehicular Communication

Status: Completed
Involved: UTARTU, QUB (non-CHESS partner), CYBER

The aim of the project was to develop a use case that combines the concept of a digital twin with blockchain-based Internet of vehicles (IoV) technology to monitor the pre-failure conditions of vehicles for their predictive maintenance.

By incorporating blockchain technology, we enhanced the security and transparency of the data collected from the digital twin. The digital twin concept involves creating a virtual replica or representation of a physical vehicle which can be monitored and analysed in real time. The primary aim of monitoring the pre-failure conditions of vehicles is to identify potential issues or malfunctions (e.g. predictive maintenance) before they lead to critical failures or accidents. Using sensors and data collection mechanisms, the digital twin can provide valuable insights into the operational status of a vehicle in real time. The blockchain-based IoV ensures the secure storage, validation, and sharing of the data obtained from the digital twin. By leveraging the decentralised nature of blockchain technology, trust is established among the entities involved in the IoV ecosystem, including vehicles, infrastructure, and other relevant stakeholders.

As part of the initial phase, we conducted a preliminary literature review to gather relevant information and insights. This served as the foundation for the subsequent stages of the project. One of the key tasks was to develop a use case scenario specifically tailored to the pre-failure conditions of the IoV. Building upon this use case, we proceed to design the architecture of a blockchain-based digital twin for IoV and build a proof of concept. Overall, our research aimed to showcase digital twin and blockchain integration in the IoV domain, specifically focusing on monitoring pre-failure conditions. By demonstrating the practicality and effectiveness of this integration, it contributes to the advancement of intelligent vehicular communication and enhances the security and reliability of IoV systems.

This mini-project has created the following open-source implementations: IoV-TwinChain, Blockchain and Digital Twin for Security Risk Assessment, Blockchain-enabled IoT Applications Scalability Assessment Tool. See Section 4 for more details.

3.4.3 CA4_03: Blockchain-Related Operation Protected by Cryptographic Hardware

Status: Completed
Involved: MUNI, UTARTU, Guardtime

This mini-project focused on the practical security of cryptographic signing devices relevant to blockchain operations, and the means of improve them using secure multi-party computation (MPC).

The work was divided into four subtasks: (1) design and implementation of basic building blocks for secure multi-party computation on cryptographic hardware, (2) implementation of multi-party cryptographic signing protocols suitable for limited hardware security devices, (3) analysis of cryptographic properties of current cryptocurrency hardware wallets, and (4) mapping of application domains where the combination of MPC and cryptographic hardware provides increased robustness against implementation faults or even intentional backdoors.

We significantly expanded and improved the JCMathLib cryptographic library with respect to supported cryptographic smartcards (three new cards were added) and its performance. Usage of new low-level operations from the JavaCard API allowed to significantly decrease the MPC signature runtime. We used the newly available extensions to support the FROST signing scheme (MPC Schnorr-based signatures) on JavaCards with no need for proprietary

libraries. This is the first open-source implementation for this domain. The JCProfilerNext tool was developed for automatic static and dynamic analysis of JavaCard applications for cryptographic smartcards, analysing the level of support of cryptographic algorithms required by blockchain operations. Finally, we investigated the level of security certification of JavaCard-related products under the Common Criteria scheme.

Dedicated setup for automatic testing of cryptographic implementation of cryptocurrency hardware wallets was built and executed on 17 different devices. While the physical setup building started already before the start of the CHESS project, the analysis of the data collected was performed within the project and is still ongoing. The collection resulted in 100,000 random seeds generated on each wallet and 100,000 ECDSA signatures with extracted private key and nonce used. Some internal implementation details were established even for wallets with a closed-source implementation.

To map application domains where a combination of MPC and cryptographic hardware may provide increased robustness, we surveyed more than 200 open-source JavaCard applets and analysed their algorithmic, memory, and runtime requirements and evolution in time. We also analysed the presence of keys with insufficient entropy on the Bitcoin blockchain, finding real-world examples of deficient randomness generators leading to (likely) compromise of funds. Utilisation of multi-party threshold signatures which are efficiently computable on current cryptographic smartcards would prevent the exploitation of such weakness.

We also used the experience with secure hardware, multi-party signatures, and key derivation methods used in the Bitcoin ecosystem (BIP32 and alike) to explore better management of key material in the X-Road project.

This mini-project has created the following open-source implementations: JCProfilerNext, JCMathLib and JCFROST. See Section 4 for more details.

3.4.4 CA4_04: Secure Information Transmission in Intelligent Vehicles

Staus: Ongoing
Involved: UTARTU, QUB (non-CHESS partner), BUT

This mini-project focuses on improving the security of information transmission in intelligent vehicles, with an emphasis on the application of blockchain technology and digital twins.

By leveraging blockchain technology, we aim to establish a decentralised, immutable framework for securely transmitting vehicle data in real time. Blockchain’s inherent features of transparency and data integrity will be used to enhance security measures, protecting the flow of sensitive information between vehicles, infrastructure, and centralised systems, thus mitigating potential threats such as data breaches or malicious attacks. We are exploring the integration of digital twin technology for the Internet of vehicles (IoV) as a deception technique. Digital twins (virtual replicas of physical systems) allow for real-time monitoring and analysis of vehicle networks. Blockchain is applied to this setup to provide an additional layer of security and trust. The combination of these technologies can enable secure and

automated decision-making, reducing the risk of cyberattacks on connected vehicle systems, and ensuring the integrity of vehicle-to-vehicle and vehicle-to-infrastructure communications.

We have published a paper that proposes a proactive security approach for IoV by leveraging deception-based digital twins and blockchain technology to hunt for security threats and gaps in IoV security posture before an incident or breach occurs.

This mini-project has created open-source implementations for blockchain and digital twin-based attack deception, and digital twin and blockchain-driven firmware update. See Section 4 for more details.

3.4.5 CA4_05: Privacy of blockchain transactions

Status: Ongoing
Involved: MUNI, UTARTU, BUT

Goal 1: Anonymous e-cash tokens, improved mint protection (trusted dealer) with secure hardware, e-cash token MPC decryption

Electronic cash (or e-cash) technology based on the foundational work of Chaum is emerging as a scalability and privacy layer atop expensive and traceable blockchain-based currencies. Unlike trustless blockchains, e-cash designs inherently rely on a trusted party with full control over the currency supply. Since this trusted component cannot be eliminated from the system, we aim to minimise the trust it requires. We focus on the employment of both misuse-resistant hardware and threshold multi-party computation to split decisions across multiple independent devices and leverage their complementary benefits. The promising candidates are blind protocols used in e-cash designs that are at the same time suitable for misuse-resistant, yet resource-constrained devices, e.g. BDHKE-based construction. The next step is the proposal of a multi-party protocol for the distribution of the operations needed in BDHKE-based e-cash. We will verify the practicality of the proposed design using a physical smartcard with the JavaCard platform.

Goal 2: Privacy analysis of CoinJoin transactions

CoinJoin is a collaborative transaction concept designed to enhance Bitcoin privacy by mixing user inputs in a trustless manner. However, in June 2024, law enforcement actions lead to the shutdown of the coordinators of the three leading CoinJoin implementations – Wasabi 1.0, Wasabi 2.0, and Whirlpool – raising concerns about their resilience against privacy attacks. Privacy in these protocols is theoretically defined by the anonymity set or the number of non-colluding participants, but this value is inherently unknown in live deployments.

We will explore the possibility of leveraging data from high-fidelity, large-scale emulations involving hundreds of client wallets to train an inference model capable of closely estimating the number of CoinJoin participants. Such a model, combined with statistical tools, can be used to investigate real on-chain behaviours, identify prevalent patterns, and detect potential ongoing attacks. As the preliminary results show, we observe a high rate of remixing in

Wasabi 2.0 transactions, suggesting the presence of attackers who control multiple inputs and aggressively participate in undermining user anonymity. This kind of behaviour cannot be explained even by wallets' most conservative anonymity settings. As a result, we now focus on a proposal for adjusted fee structures to increase the cost of privacy attacks, thereby enhancing the privacy and resilience of CoinJoin protocols.

As an intermediate result, we have developed tools for large-scale emulations with Wasabi 2.x Wallets, analysed real historic CoinJoin transactions from Wasabi 1.x, Wasabi 2.x and Whirlpool coordinators, and mapped impact of fee structures on difficulty to mount Sybil attacks. The resulting research paper is currently in submission.

This mini-project has created the open-source implementation JCMint. See Section 4 for more details.

3.4.6 CA4_06: Methods for More Compact and Secure Blockchains

Status: Ongoing
Involved: MUNI, UTARTU, BUT, Guardtime, CYBER

We focus on mapping the usage domain within the Alphabill blockchain. We explore an adaptation of the zkLogin concept for Alphabill. zkLogin eases the access of ordinary users to blockchain-based operations without any need for dedicated key management, as only an already existing relationship with a single sign on (SSO) entity like Google is required to control accounts on Ethereum-like blockchains.

We also investigate a trustless design of a ‘salt’ service with increased abuse–resistance and its practical implementation using a set of cryptographic hardware components. Through the combination of cryptographic hardware, threshold cryptographic protocols for decryption, signing and key derivation, we believe that the ‘salt’ service can be resilient against both malware infection as well as malicious operator with physical access.

3.5 Challenge Area 5: Post-Quantum Cryptography

3.5.1 CA5_01: Aspects of Transition to Post-Quantum Technologies

Status: Ongoing
Involved: CYBER, BUT

We have been working on the proof-of-concept infrastructure enabling authentication using post-quantum cryptographic algorithms. More specifically, we have implemented authentication to the NextCloud server using the Web-eID protocol and an ESP32-based client as a key storage and deployment device. A paper presenting the results of this line of research was published at the International Conference on Ubiquitous Security 2023 and received the best paper award there.

The work on transitioning to post-quantum technologies is continuing, with one of the prominent targets being setting up a post-quantum remote electronic voting system. As an independent side result, a library implementing core post-quantum primitives is emerging.

3.5.2 CA5_02: Implementation of Transition to Post-Quantum Technologies

Status: Completed
Involved: CYBER, BUT

We designed and implemented experimental software for testing post-quantum secure channels over long distances, with the aim of establishing a secure channel between Estonia and Czechia. Our software, published as open source, makes use of the CRYSTALS-Kyber algorithm to securely establish an encryption key for VPN-like encrypted channel that is realised through Linux-based gateways. This mini-project ended with the publication of the software while work related to the project continues under mini-project CA5_03 on piloting the encrypted post-quantum channel. The results of the mini-project were summarized in a master's thesis and a scientific publication (in progress).

3.5.3 CA5_03: (Post-)Quantum Communication Infrastructure Pilot

Status: Ongoing
Involved: CYBER, BUT

The objective of this mini-project is to evaluate the software developed in CA5_02 and establish a fully functional quantum-safe communication channel between Czechia and Estonia. We aim to set up a post-quantum virtual private network (VPN) between Estonia and South Moravia to test out the state of the current technology and identify transition challenges. A secure channel based on post-quantum cryptography was established in the summer of 2024. Real-life applications (file servers and voice over IP services) were deployed on both sides to evaluate the functionality and performance of the channel. The results confirmed the full functionality of the proof-of-concept software and showed performance between 50–100 Mbps. This is sufficient for standard communication. The results from the implementation and benchmarking were summarised in a scientific paper submitted to the Internet of Things Journal, special issue on Post-Quantum Cryptography.

Following the Czech–Estonian pilot, the benchmarks were also executed on a constrained device platform, namely the Raspberry Pi. The results, including performance, are summarised in the deployment report.

3.6 Challenge Area 6: Human-Centric Aspects of Cybersecurity

3.6.1 CA6_01 Hands-on Cybersecurity Training

Status: Completed
Involved: MUNI, TalTech

Human-centric cybersecurity relies on the skills and awareness of both professionals and end-users. As a part of this mini-project, we prepared multiple cybersecurity training events for students and educators (trainers) using the KYPO cyber range platform (an open-source interactive learning environment available at https://crp.kypo.muni.cz/).

We have organised multiple events for high-school and university students and cybersecurity educators. We have performed research using the KYPO cyber range and introduced new technologies, which enabled activities for cybersecurity students and professionals to stay updated about emerging technologies and new threats. We focused on improving (1) the training infrastructure (cross-platform support, resource efficiency, introducing Docker/Podman containers), (2) cheating prevention and detection (automatic problem generation, logging), and (3) class delivery (training definition and automatic study materials generation, linear and adaptive training). We focused on improving the feedback to students to support their learning.

We designed new hands-on challenges and cybersecurity games in the KYPO cyber range. We developed a new training environment, utilising a container-based approach with Docker, and introduced a new challenge for the Czech National Cybersecurity Competition (https://www.kybersoutez.cz), which ran from December 2023 to January 2024.

This mini-project has ended, but the work continues under CA6_03 (Delivering Tabletop Exercises), focusing on training participants in the efficient mitigation and resolution of incidents.

The results of CA6_01 have been published in a journal paper: Švábenský V. et al. (2024), as well as in three theses; see Section 4 for details.

3.6.2 CA6_02 Improving the Usability of Penetration Testing Reports

Status: Ongoing
Involved: MUNI, CYBER, Red Hat

This mini-project focuses on penetration testing and ways of improving the reporting process. The effectiveness of penetration testing relies on clear and actionable reporting. A critical challenge lies in ensuring that customers receive informative, easy-to-understand reports. We have organised three workshops with two aims: (1) to share experience with the process of penetration testing and preparing reports, and (2) to gather perspectives from IT professionals (four focus groups in total) who work with penetration testing reports and get 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. Interactive sessions carried out during the workshops revealed some of the problem areas experienced by individuals across various technical proficiency levels in cybersecurity. Our aim is to understand the usability gaps in penetration testing reports that can then reveal new methods of writing these reports to help IT professionals, ranging from technical staff to managers, to better implement security measures.

3.6.3 CA6_03 Delivering Tabletop Exercises

Status: Ongoing
Involved: MUNI, TalTech, UTARTU, RIA, NUKIB

Tabletop exercises (TTX) are discussion-based exercises of preparedness to emergencies and incidents using scenario predefined by instructors. Trainees are provided with inputs simulating the evolution of a crisis, and discuss what they would do and why. The exercises are traditionally organised by military and government bodies and large organisations to train or assess their incident handling or business recovery processes.

This mini-project deals with design, delivery, and assessment of tabletop exercises, particularly using INJECT Exercise Platform (https://inject.muni.cz/, further IXP). The mini-project leverages the experience of project partners from developing and organising TTX using pen and paper or generic-purpose online tools, such as online questionnaires or survey tools. We have organised two workshops for stakeholders from both regions with the aim of introducing IXP and sharing best practices for TTX design and delivery. Further, we delivered two TTXs designed by MUNI for students in Estonia to evaluate applicability of the scenario in the different country. We have also delivered a TTX for top talented high-school students, finalists of the Czech national cybersecurity competition, to test whether this target audience equipped with brilliant technical skills will perform well in an exercise requiring teamwork and non-technical skills. We will further share existing TTX scenarios and develop new ones to make impact on cybersecurity posture in both regions.

The results of CA6_03 have so far been published in three theses; see Section 4 for details.

4 CHESS first results

4.1 Publications

CHESS Publications

Challenge Area 1: Internet of Secure Things

Bahktina M., Matulevičius R., Malina L.: Information Security and Privacy Management in Intelligent Transportation Systems. Journal of Complex Systems Informatics and Modeling Quarterly (CSIMQ), Issue 38, March/April 2024, 100–131.
https://doi.org/10.7250/csimq.2024-38.04

Abstract: With the global digitalization of services, passenger Intelligent Transportation Systems (ITSs) have emerged as transformative components, yet the practical implementation of state-of-the-art measures to ensure information security and privacy presents substantial challenges. In this article, we propose a framework for information security and privacy management. The framework is validated through two empirical studies. First, the framework is used to extract data during the literature review defining state-of-the-art aspects and measures. Second, a survey-based analysis of running

passenger ITSs in selected regions of the European Union provides insights into real-life ITS implementations, enabling a thorough comparison with the proposed state-of-the-art measures. The study also showed that the proposed framework depicts some dependencies between measures, and, thus, using its matrix structure for the state of information security and privacy management in the organization helps to cross-check the usage of policies or methodologies by the organization departments. Our findings resulted in recommendations for organizations developing ITSs to enhance their information security and privacy management systems and bridge the gap between research proposals and practical implementation.

Bahktina M., Towards More Secure and Data Protective Intelligent Infrastructure Systems. In: Matulevičius, R., Mendez, D. (eds.). Proceedings of the Doctoral Consortium Papers Presented at the 35th International Conference on Advanced Information Systems Engineering (CAiSE 2023), June 12–16, 2023, Zaragoza, Spain. https://ceur-ws.org/Vol-3407/paper5.pdf

Abstract: With the megatrends of hyperconnectivity, the information systems transform into intelligent infrastructure (II) systems that allow data-based decision-making based on data processing. While the real-world use cases of II systems are just emerging and still are under active research and development, the problem of methods for information security and privacy protection in such SoSs is even more underresearched. As a result, there is a gap in the knowledge base in the guidelines on how information security officers should anticipate required changes to the organisation's information security strategy and formulate new plans, in case the organisation transforms its IT system towards the II system. In this research project, we want to create guidelines on how security risks and privacy protection should be managed in complex intelligent infrastructure systems. In this paper, we present the context of the PhD research work, research questions, the methodology and expected contributions of the study.

Daubner, L., Matulevičius, R., Buhnova, B. (2023a). A Model of Qualitative Factors in Forensic-Ready Software Systems. In: Nurcan, S., Opdahl, A.L., Mouratidis, H., Tsohou, A. (eds.). Research Challenges in Information Science: Information Science and the Connected World. RCIS 2023. Lecture Notes in Business Information Processing, Vol. 476. Cham: Springer. https://doi.org/10.1007/978-3-031-33080-3_19

Abstract: Forensic-ready software systems enhance the security posture by designing the systems prepared for potential investigation of incidents. Yet, the principal obstacle is defining their exact requirements, i.e., what they should implement. Such a requirement needs to be on-point and verifiable. However, what exactly comprises a forensic readiness requirement is not fully understood due to distinct fields of expertise in software engineering and digital forensics. This paper describes a forensic readiness qualitative factor reference model that enables the formulation of specific requirements for forensic-ready software systems. It organises the qualitative properties of forensic readiness into a taxonomy, which can then be used to formulate a verifiable requirement targeted at a specific quality. The model is then utilised in an automated valet parking service to define requirements addressing found inadequacies regarding a potential incident investigation.

Daubner, L., Matulevičius, R., Buhnova, B., Antol, M., Růžička, M., Pitner, T. (2023b). A Case Study on the Impact of Forensic-Ready Information Systems on the Security Posture. In: Indulska, M., Reinhartz-Berger, I., Cetina, C., Pastor, O. (eds.). Advanced Information Systems Engineering. CAiSE 2023. Lecture Notes in Computer Science, Vol. 13901. Cham: Springer. https://doi.org/10.1007/978-3-031-34560-9_31

Abstract: While approaches aimed at developing forensic-ready systems are starting to emerge, it is still primarily a theoretical concept. This paper presents a case study of integrating forensic readiness capabilities into SensitiveCloud, an information system for storing and processing sensitive data. A risk-based approach to forensic readiness design is followed to achieve it. Consequently, weaknesses in both processes and systems are identified, and forensic readiness requirements are formulated. This case study reports on lessons learned in the practical implementation of a forensic-ready system, its impact on security, and its support towards ISO/IEC 27k.

Dobias, P., Malina, L., Ilgner, P., & Dzurenda, P. On Efficiency and Usability of Group Signatures on Smartphone and Single-board Platforms. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). New York: Association for Computing Machinery, 2023, Article 127, pp. 1–9. https://doi.org/10.1145/3600160.3605015

Abstract: With increasing digitalization and omnipresent data sensing, security and users' privacy become essential requirements in new digital services. Group Signatures (GS) or also known as Anonymous Digital Signatures (ADS) are often used as a core Privacy-Enhancing Technology (PET) in order to keep users' privacy during their access and/or authentication phases within ensuring the security of provided services. In this work, we provide a comprehensive assessment of group signatures on various small computing platforms typically used in modern digital services. Based on our analysis of well-established GS schemes and their libraries, we implement and evaluate chosen schemes on both well-known smartphone platforms (i.e., Android, iOS) and on a single-board computer. Our results indicate that current handheld devices can already effectively perform main group signatures' phases and make these schemes practical for deployment in various privacy-requiring scenarios.

Malina, L., Dzurenda, P., Lövinger, N., Ekeh, I. E., Matulevičius, R. Secure and Privacy-Preserving Car-Sharing Systems. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). New York: Association for Computing Machinery, 2024, Article 160, pp. 1–10. https://doi.org/10.1145/3664476.3670443

Abstract: With increasing smart transportation systems and services, potential security and privacy threats are growing. In this work, we analyse privacy and security threats in car-sharing systems, and discuss the problems with the transparency of services, users' personal data collection, and how the legislation manages these issues. Based on analysed

requirements, we design a compact privacy-preserving solution for car-sharing systems. Our proposal combines digital signature schemes and group signature schemes to protect user privacy against curious providers, increase security and non-repudiation, and be efficient even for systems with restricted devices. The evaluation of the proposed solution demonstrates its security and practical usability for constrained devices deployed in vehicles and users' smartphones.

Challenge Area 2: Security Certification

Seeba, M. Comparable and Repeatable Information Security Level Evaluation. In: CAiSE 2024 Doctoral Consortium, CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3767/paper7.pdf

Abstract: To safeguard citizens' digital lifestyles and the functioning of societal systems, countries enact regulations (e.g., GDPR, NIS2) mandating cybersecurity measures in organisations to improve security. We must repeatedly evaluate the improvement rate in organisations and collect the data for a state-level overview to measure the improvement rate over time. There are developed instruments to assess or measure security, but they lack best practices for evaluating compliance in a way that considers environmental changes while ensuring consistent security evaluation over time and across organisations (e.g., benchmarking) simultaneously. This PhD project introduction paper introduces the artifact – a framework for security level evaluation (F4SLE) in organisations based on chosen baseline standards with the method to update the instrument content and its user stories, utilising the design science research method. The F4SLE is used in piloting experiments by 70 organisations in Estonia and South Moravia (a district of the Czech Republic) to validate the framework and its user stories. The final results are a work in progress.

Seeba, M., Oja, T., Murumaa, M. P., and Stupka, V. Security level evaluation with F4SLE. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery, New York, NY, USA, Article 132, pp. 1–8. https://doi.org/10.1145/3600160.3605045

Abstract: In the realm of security measurements, extensive efforts have been made to evaluate and compare security levels at the country level, resulting in various indices. However, there has been a dearth of evaluations focusing on the information security posture of individual organizations and simultaneously on state-level status evaluation. Such evaluations hold significant potential for providing valuable feedback on the security status of organizations and facilitating assessments and supportive data-driven focused interventions at a national level. This study leverages the Framework for Security Level Evaluation (F4SLE) and the developed tool, Measurement Application for Self-assessing Security (MASS), to collect data for the evaluation. The paper presents diverse options for interpreting the collected data and establishes the foundation for an ongoing cross-country study. The results encompass the analysis of organization-level data and offer insights into overall approaches to security across organizations. This study is a preliminary step toward a more comprehensive information security examination.

Challenge Area 3: Verification of Trustworthy Software

Earnshaw, M., Sobocinski, P. String Diagrammatic Trace Theory. In: Leroux, J., Lombardy, S., Peleg, D. (eds.). 48th International Symposium on Mathematical Foundations of Computer Science (MFCS 2023). Dagstuhl: Leibniz-Zentrum für Informatik, pp. 43:1–43:15. https://doi.org/10.4230/LIPIcs.MFCS.2023.43

Abstract: We extend the theory of formal languages in monoidal categories to the multi-sorted, symmetric case, and show how this theory permits a graphical treatment of topics in concurrency. In particular, we show that Mazurkiewicz trace languages are precisely symmetric monoidal languages over monoidal distributed alphabets. We introduce symmetric monoidal automata, which define the class of regular symmetric monoidal languages. Furthermore, we prove that Zielonka's asynchronous automata coincide with symmetric monoidal automata over monoidal distributed alphabets. Finally, we apply the string diagrams for symmetric premonoidal categories to derive serializations of traces.

Jankola, M., Strejček, J. Tighter Construction of Tight Büchi Automata. In: Kobayashi, N., Worrell, J. (eds.). Foundations of Software Science and Computation Structures. FoSSaCS 2024. Lecture Notes in Computer Science, vol 14574. Cham: Springer, pp 234–255. https://doi.org/10.1007/978-3-031-57228-9_12

Abstract: Tight automata are useful in providing the shortest counterexample in LTL model checking and also in constructing a maximally satisfying strategy in LTL strategy synthesis. There exists a translation of LTL formulas to tight Büchi automata and several translations of Büchi automata to equivalent tight Büchi automata. This paper presents another translation of Büchi automata to equivalent tight Büchi automata. The translation is designed to produce smaller tight automata and it asymptotically improves the best-known upper bound on the size of a tight Büchi automaton equivalent to a given Büchi automaton. We also provide a lower bound, which is more precise than the previously known one. Further, we show that automata reduction methods based on quotienting preserve tightness. Our translation was implemented in a tool called Tightener. Experimental evaluation shows that Tightener usually produces smaller tight automata than the translation from LTL to tight automata known as CGH.

Klaška, D., Kučera, A., Kurečka, M., Musil, V., Novotný, P., and Řehák, V. Synthesizing Resilient Strategies for Infinite-Horizon Objectives in Multi-Agent Systems. In: Elkind, E. (ed.). Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence (IJCAI 2023), pp. 171–179. https://doi.org/10.24963/ijcai.2023/20

Abstract: We consider the problem of synthesizing resilient and stochastically stable strategies for systems of cooperating agents striving to minimize the expected time between consecutive visits to selected locations in a known environment. A strategy profile is resilient if it retains its functionality even if some of the agents fail, and stochastically stable if the visiting time variance is small. We design a novel specification language for objectives

involving resilience and stochastic stability, and we show how to efficiently compute strategy profiles (for both autonomous and coordinated agents) optimizing these objectives. Our experiments show that our strategy synthesis algorithm can construct highly non-trivial and efficient strategy profiles for environments with general topology.

Klaška, D., Kučera, A., Kůr, V., Musil, V., and Řehák, V. Optimizing Local Satisfaction of Long-Run Average Objectives in Markov Decision Processes. Proceedings of the AAAI Conference on Artificial Intelligence, 38(18), 20143–20150. https://doi.org/10.1609/aaai.v38i18.29993

Abstract: Long-run average optimization problems for Markov decision processes (MDPs) require constructing policies with optimal steady-state behaviour, i.e., optimal limit frequency of visits to the states. However, such policies may suffer from local instability in the sense that the frequency of states visited in a bounded time horizon along a run differs significantly from the limit frequency. In this work, we propose an efficient algorithmic solution to this problem.

Malík, V., Nečas, F., Schrammel, P., Vojnar, T. 2LS: Arrays and Loop Unwinding. In: Sankaranarayanan, S., Sharygina, N. (eds.). Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2023. Lecture Notes in Computer Science, Vol. 13994. Cham: Springer. https://doi.org/10.1007/978-3-031-30820-8_31

Abstract: 2LS is a C program analyser built upon the CPROVER infrastructure that can verify and refute program assertions, memory safety, and termination. Until now, one of the main drawbacks of 2LS was its inability to verify most programs with arrays. This paper introduces a new abstract domain in 2LS for reasoning about the contents of arrays. In addition, we introduce an improved approach to loop unwinding, a crucial component of the 2LS' verification algorithm, which particularly enables finding proofs and counterexamples for programs working with dynamic memory.

Schwarzová, T., Strejček, J., and Major, J. Reducing Acceptance Marks in Emerson-Lei Automata by QBF Solving. In: 26th International Conference on Theory and Applications of Satisfiability Testing (SAT 2023). Leibniz International Proceedings in Informatics (LIPIcs), Vol. 271. Dagstuhl: Leibniz-Zentrum für Informatik, pp. 23:1–23:20. https://doi.org/10.4230/LIPIcs.SAT.2023.23

Abstract: This paper presents a novel application of QBF solving to automata reduction. We focus on Transition-based Emerson-Lei automata (TELA), which is a popular formalism that generalizes many traditional kinds of automata over infinite words including Büchi, co-Büchi, Rabin, Streett, and parity automata. Transitions in a TELA are labelled with acceptance marks and its accepting formula is a positive Boolean combination of atoms saying that a particular mark has to be visited infinitely or finitely often. Algorithms processing these automata are often very sensitive to the number of acceptance marks. We introduce a new technique for reducing the number of acceptance marks in TELA based on satisfiability of

quantified Boolean formulas (QBF). We evaluated our reduction technique on TELA produced by state-of-the-art tools of the libraries Owl and Spot and by the tool ltl3tela. The technique reduced some acceptance marks in automata produced by all the tools. On automata with more than one acceptance mark obtained by translation of LTL formulas from literature with tools Delag and Rabinizer 4, our technique reduced 27.7% and 39.3% of acceptance marks, respectively. The reduction was even higher on automata from random formulas.

Challenge Area 4: Security Preservation in Blockchain

Bakhtina, M., Leung, K. L., Matulevičius, R., Awad, A., Švenda, P. A Decentralised Public Key Infrastructure for X-Road. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). New York: Association for Computing Machinery, 2023, Article 128, pp. 1–8. https://doi.org/10.1145/3600160.3605092

Abstract: X-Road is an open-source solution that acts as a data exchange layer and enables secure data exchange between organisations. X-Road serves as the backbone of digital infrastructure in the public sector (e.g., enabling Estonia's digital public services) and private sector (e.g., enabling clients' data exchange in the Japanese energy sector). An approach and architecture were recently proposed for the X-Road data exchange systems to move from public key infrastructure (PKI) with centralised certification authorities to decentralised PKI (DPKI). In this paper, we develop a proof of concept for the designed DPKI-based architecture that leverages distributed ledger-based identifiers and verifiable credentials to establish trust between information systems using Hyperledger Indy and Hyperledger Aries. We evaluate the proof of concept implementation against the design and functional requirements. The results show that the proposed system architecture is technically feasible and satisfies the identified design goals and functional requirements. To the best of our knowledge, this paper presents the first open-access system prototype for an organisation's identity management following self-sovereign identity principles. The presented proof of concept proves that DPKI helps to address some of the scalability issues of PKI, improve control over identity and mitigate replay attacks and a single point of failure in the X-Road system.

Bakhtina, M., Kvapil, J., Švenda, P., and Matulevičius, R. The Power of Many: Securing Organisational Identity Through Distributed Key Management. In: Guizzardi, G., Santoro, F., Mouratidis, H., Soffer, P. (eds.). Advanced Information Systems Engineering. CAiSE 2024. Lecture Notes in Computer Science, vol 14663. Cham: Springer. https://doi.org/10.1007/978-3-031-61057-8_28

Abstract: Organisational Digital Identity (ODI) often relies on the credentials and keys being controlled by a single person-representative. Moreover, some Information Systems (IS) outsource the key management to a third-party controller. Both the centralisation and outsourcing of the keys threaten data integrity within the IS, allegedly provided by a trusted organisation. Also, outsourcing the control prevents an organisation from cryptographically enforcing custom policies, e.g. time-based, regarding the data originating from it. To address this, we propose a Distributed Key Management System (DKMS) that eliminates the risks

associated with centralised control over an organisation's identity and allows organisation-enforceable policies. The DKMS employs threshold signatures to directly involve multiple organisation's representatives (e.g. employees, IS components, and external custodians) in data signing on its behalf. The threshold signature creation and, therefore, the custom signing policy inclusion, is fully backwards compatible with commonly used signing schemes, such as RSA or ECDSA. The feasibility of the proposed system is shown in an example data exchange system, X-Road. The implementation confirms the ability of the design to achieve distributed control over the ODI during the operational key phase. Excluding a network delay, the implementation introduces less than 200 ms overhead compared to the built-in signing solution.

Dufka, A., Janku, J., Svenda, P. Trust-minimizing BDHKE-based e-cash mint using secure hardware and distributed computation. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). New York: Association for Computing Machinery, Article 190, pp. 1–10. http://dx.doi.org/10.1145/3664476.3670889

Abstract: The electronic cash (or e-cash) technology based on the foundational work of Chaum is emerging as a scalability and privacy layer atop of expensive and traceable blockchain-based currencies. Unlike trustless blockchains, e-cash designs inherently rely on a trusted party with full control over the currency supply. Since this trusted component cannot be eliminated from the system, we aim to minimize the trust it requires.

We approach this goal from two angles. Firstly, we employ misuse-resistant hardware to mitigate the risk of compromise via physical access to the trusted device. Secondly, we divide the trusted device's capabilities among multiple independent devices, in a way that ensures unforgeability of its currency as long as at least a single device remains uncompromised. Finally, we combine both these approaches to leverage their complementary benefits.

In particular, we surveyed blind protocols used in e-cash designs with the goal of identifying those suitable for misuse-resistant, yet resource-constrained devices. Based on the survey, we focused on the BDHKE-based construction suitable for the implementation on devices with limited resources. Next, we proposed a new multi-party protocol for distributing the operations needed in BDHKE-based e-cash and analyzed its security. Finally, we implemented the protocol for the JavaCard platform and demonstrated the practicality of the approach by measuring its performance on a physical smartcard.

Iqbal, M., Suhail, S., Matulevicius, R. DECEPTWIN: Proactive Security Approach for IoV by Leveraging Deception-based Digital Twins and Blockchain. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (2024). New York: Association for Computing Machinery, Article 161, pp. 1–11. https://doi.org/10.1145/3664476.3670473

Abstract: The proliferation of security threats in connected systems necessitates innovative approaches to enhance security resilience. The Internet of vehicles (IoV) presents a rapidly evolving and interconnected ecosystem that raises unprecedented security challenges,

including remote hijacking, data breaches, and unauthorized access. Digital Twin (DT) and blockchain-based deception can emerge as a promising approach to enhance the security of the IoV ecosystem by creating a secure, realistic, dynamic, and interactive deceptive environment that can deceive and disrupt malicious actors. In accordance with this, we propose a proactive security approach for IoV by leveraging DECEPtion-based digiTal tWins and blockchaIN (DECEPTWIN) that entails hunting for security threats and gaps in IoV security posture before an incident or breach occurs.

Challenge Area 5: Post-Quantum Cryptography

Dobias, P., Malina, L., Ilgner, P., and Dzurenda, P. On Efficiency and Usability of Group Signatures on Smartphone and Single-board Platforms. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). New York: Association for Computing Machinery, Article 127, pp. 1–9. https://doi.org/10.1145/3600160.3605015

Abstract above (see publications related to CA1).

Dobias, P., Ricci, S., Dzurenda, P., Malina, L., and Snetkov, N. Lattice-Based Threshold Signature Implementation for Constrained Devices. In: Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT). SciTePress, 2023, pp. 724–730. http://dx.doi.org/10.5220/0012112700003555

Abstract: Threshold signatures have gained increased attention especially due to their recent applications in blockchain technologies. In fact, current cryptocurrencies such as Bitcoin, and Cardano started to support multi-signature transactions. Even if the Schnorr-based threshold signatures improve the blockchain's privacy and scalability, these schemes do not provide post-quantum security. In this paper, we propose the optimization of the DS2 lattice-based (*n,n*)-threshold signature scheme and present its practical implementation. Moreover, we evaluate our optimized implementation of the DS2 scheme on different platforms. The results demonstrate that our implementation is easily portable and executable on constrained devices based on ARM Cortex-A53, ARM Cortex-M3, and ESP32 architectures.

Tuma, P. ; Hajny, J. ; Muzikant, P. ; Havlin, J. ; Malina, L. ; Dobias, P., and Willemson, J. Open-Source Post-Quantum Encryptor: Design, Implementation and Deployment. In: Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT). SciTePress, 2024, pp. 826–831. https://doi.org/10.5220/0012839200003767.

Abstract: This article describes an open-source quantum-resistant network traffic encryptor for the Linux platform. Our encryptor uses a combination of quantum and post-quantum key establishment methods to achieve quantum resistance combined with a fast encryption speed of AES to make quantum-resistant encryption readily available to the public. The packet-by-packet encryption architecture ensures that every bit of information is properly authenticated and encrypted. The combination of multiple key sources further increases the

encryptor's security – be it elliptic curve-based (Elliptic Curve Diffie Hellman, ECDH), quantum (Quantum Key Distribution, QKD) or post-quantum (CRYSTALS-Kyber). Without knowing all the keys obtained from different types of key sources, the final hybrid encryption key can only be obtained by brute-force means. Our contribution is very practical as the encryptor has reasonable performance, despite not being part of the Linux kernel.

Vakarjuk, J., and Snetkov, N. Post-quantum trails: an educational board game about post-quantum cryptography. In: Proceedings of the 7th International Conference on Historical Cryptology (HistoCrypt 2024). Tartu: Tartu University Library, 2024. https://doi.org/10.58009/aere-perennius0115

Abstract: Post-quantum cryptography has gained more and more attention with the recent developments in quantum technology. There are already standard drafts for the novel post-quantum crypto systems and organisations are starting the process of migration to post-quantum cryptography. However, the migration process has many challenges that need to be taken into account. Moreover, the algorithms themselves have become more complicated, making it more difficult to educate people about post-quantum cryptography. We propose to use gamification to make it easier to explain the main challenges and obstacles as well as the main steps of the migration process to the non-cryptographic community. We propose a board game that is built using the gamification taxonomy of Toda et al. to ensure a smooth learning process.

Challenge Area 6: Human-centric Aspects of Cybersecurity

Švábenský, V., Vykopal, J., Čeleda, P. et al. Automated feedback for participants of hands-on cybersecurity training. Educ. Inf. Technol., 29 (June 2024), 11555–11584. https://doi.org/10.1007/s10639-023-12265-8

Abstract: Computer-supported learning technologies are essential for conducting hands-on cybersecurity training. These technologies create environments that emulate a realistic IT infrastructure for the training. Within the environment, training participants use various software tools to perform offensive or defensive actions. Usage of these tools generates data that can be employed to support learning. This paper investigates innovative methods for leveraging the trainee data to provide automated feedback about the performed actions. We proposed and implemented feedback software with four modules that are based on analysing command-line data captured during the training. The modules feature progress graphs, conformance analysis, activity timeline, and error analysis. Then, we performed field studies with 58 trainees who completed cybersecurity training, used the feedback modules, and rated them in a survey. Quantitative evaluation of responses from 45 trainees showed that the feedback is valuable and supports the training process, even though some features are not fine-tuned yet. The graph visualizations were perceived as the most understandable and useful. Qualitative evaluation of trainees' comments revealed specific aspects of feedback that can be improved. We publish the software as an open-source component of the KYPO Cyber Range Platform. Moreover, the principles of the automated feedback generalize to different learning contexts, such as operating systems, networking, databases,

and other areas of computing. Our results contribute to applied research, the development of learning technologies, and the current teaching practice.

Other CHESS Publications

Bakhtina, M., Vémolová, Z., and Matyáš, V. CHESS: Cyber-security Excellence Hub in Estonia and South Moravia. In: Matulevičius, R., Properik, H. A. RPE@CAiSE'24: Research Projects Exhibition at the International Conference on Advanced Information Systems Engineering, pp. 10–17. https://ceur-ws.org/Vol-3692/paper2.pdf

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 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.

Related publications

Daubner, L., Maksović, S., Matulevičius, R., Buhnova, B., Sedláček, T. (2024). Forensic-Ready Analysis Suite: A Tool Support for Forensic-Ready Software Systems Design. In: Araújo, J., de la Vara, J.L., Santos, M.Y., Assar, S. (eds.). Research Challenges in Information Science. RCIS 2024. Lecture Notes in Business Information Processing, Vol. 514. Cham: Springer. https://doi.org/10.1007/978-3-031-59468-7_6

Forensic-ready software systems integrate preparedness for digital forensic investigation into their design. It includes ensuring the production of potential evidence with sufficient coverage and quality to improve the odds of successful investigation or admissibility. However, the design of such software systems is challenging without in-depth forensic readiness expertise. Thus, this paper presents a tool suite to help the designer. It includes a graphical editor for creating system models in BPMN4FRSS notation, an extended BPMN with forensic readiness constructs, and an analyser utilising Z3 solver for satisfiability checking of formulas derived from the models. It verifies the models' validity, provides targeted hints to enhance forensic readiness capabilities, and allows for what-if analysis of potential evidence quality.

Janovský, A., Jančár, J., Švenda, P., Chmielewski, L. M., Michalík, J., and Matyáš, V. sec-certs: Examining the security certification practice for better vulnerability mitigation.

Computers & Security. 2024, Vol. 2024, No 143, 1–13. https://dx.doi.org/10.1016/j.cose.2024.103895.

Abstract: Products certified under security certification frameworks such as Common Criteria undergo significant scrutiny during the costly certification process. Yet, critical vulnerabilities, including private key recovery (ROCA, Minerva, TPM-Fail...), get discovered in certified products with high assurance levels. Furthermore, assessing which certified products are impacted by such vulnerabilities is complicated due to the large amount of unstructured certification-related data and unclear relationships between the certified products. To address these problems, we conducted a large-scale automated analysis of Common Criteria certificates. We trained unsupervised models to learn which vulnerabilities from NIST's National Vulnerability Database impact existing certified products and how certified products reference each other. Our tooling automates the analysis of tens of thousands of certification-related documents, extracting machine-readable features where manual analysis is unattainable. Further, we identify the security requirements that are associated with products being affected by fewer and less severe vulnerabilities. This indicates which aspects of certification correlate with higher security. We demonstrate how our tool can be used for better vulnerability mitigation on four case studies of known, high-profile vulnerabilities. All tools and continuously updated results are available at https://sec-certs.org.

Janovský, A, Chmielewski, L. M., Švenda, P., Jančár, J., and Matyáš, V. Chain of Trust: Unraveling References Among Common Criteria Certified Products. In: Pitropakis, N., Katsikas, S., Furnell. S., and Markantonakis, K. (eds.). ICT Systems Security and Privacy Protection. SEC 2024. IFIP Advances in Information and Communication Technology. volume 710. Cham: Springer Nature Switzerland, 2024, pp. 191–205. https://dx.doi.org/10.1007/978-3-031-65175-5_14.

Abstract: With 5394 security certificates of IT products and systems, the Common Criteria for Information Technology Security Evaluation have bred an ecosystem entangled with various kind of relations between the certified products. Yet, the prevalence and nature of dependencies among Common Criteria certified products remains largely unexplored. This study devises a novel method for building the graph of references among the Common Criteria certified products, determining the different contexts of references with a supervised machine-learning algorithm, and measuring how often the references constitute actual dependencies between the certified products. With the help of the resulting reference graph, this work identifies just a dozen certified components that are relied on by at least 10% of the whole ecosystem – making them a prime target for malicious actors. The impact of their compromise is assessed and potentially problematic references to archived products are discussed.

Muzikant, P., Willemson, J. (2024). Deploying Post-quantum Algorithms in Existing Applications and Embedded Devices. In: Wang, G., Wang, H., Min, G., Georgalas, N., Meng, W. (eds.). Ubiquitous Security. UbiSec 2023. Communications in Computer and Information Science, Vol. 2034. Singapore: Springer. https://doi.org/10.1007/978-981-97-1274-8_10.

Abstract. This paper studies the current state of post-quantum cryptography implementation feasibility, providing general approaches that developers and security engineers can utilize to start integrating today. First, we analyse the current state of the art in the field of available cryptographic libraries and standards for algorithm interpretations and encodings. Then, we provide few implementation challenges that rose from our experiments and how to handle them. Lastly, we have built a proof-of-concept implementation by creating a post-quantum version of a modern web authentication framework. Our work introduces postquantum support in multiple open-source libraries that together enable web-service administrators to authenticate their users with Dilithium-5 or Falcon-1024 secured electronic identities. Among other components, our proof-of-concept also includes a client-side solution for key management using programmable embedded device.

Zaoral, L., Dufka, A., Svenda, P. (2024). The Adoption Rate of JavaCard Features by Certified Products and Open-Source Projects. In: Bhasin, S., Roche, T. (eds.). Smart Card Research and Advanced Applications. CARDIS 2023. Lecture Notes in Computer Science, vol 14530. Cham: Springer. https://doi.org/10.1007/978-3-031-54409-5_9

Abstract: JavaCard is the most prevalent platform for cryptographic smartcards nowadays. Despite having more than 20 billion smartcards shipped with it and thirteen revisions since the JavaCard API specification was first published more than two decades ago, uptake of newly added features, cryptographic algorithms or their parameterizations, and systematic analysis of overall activity is missing. We fill this gap by mapping the activity of the JavaCard ecosystem from publicly available sources with a focus on 1) security certification documents available under Common Criteria and FIPS140 schemes and 2) activity and resources required by JavaCard applets released in an open-source domain (Paper supplementary materials, full results of analysis and open tools are available at https://crocs.fi.muni.cz/papers/cardis2023). The analysis performed on all certificates issued between the years 1997–2023 and on more than 200 public JavaCard applets shows that new features from JavaCard specification are adopted slowly, typically taking six or more years. Open-source applets utilize new features even later, likely due to the unavailability of recent performant smartcards in smaller quantities. Additionally, almost 70% of constants defined in JavaCard API specification are completely unused in open-source applets. The applet portability improves with recent cards, and transient memory requirements (scarce resource on smartcards) are typically small. While twenty or more products have been consistently certified every year since 2009, the open-source ecosystem became more active around 2013 but seemed to decline in the past two years. As a result, the whole smartcard ecosystem might be negatively impacted by limited exposure to new ideas and usage scenarios, serving only well-established domains and potentially harming its long-term competitiveness.

4.2 Theses

CA1 theses:

Ekeh, Ijeoma Faustina. A Recommendation Model for Security Risk Management in Car-Sharing Scenarios. (Supervisor: Raimundas Matulevičius).

The thesis deals with the issue of car-sharing and users' data privacy when their information is shared to access this service and the security risks of sharing such information between systems. https://chess-eu.cs.ut.ee/2024/09/06/a-recommendation-model-for-security-risk-management-in-car-sharing-scenarios/

Truu, Sander. Tool-Supported Privacy Analysis of Smart Parking (Supervisors: Mariia Bakhtina, Raimundas Matulevičius).

The thesis focuses on the tool-supported privacy analysis method, which uses the DPO Tool and Pleak tool on smart parking business processes to identify privacy violations during data processing. This thesis validates the proposed method for analysing business processes' privacy issues. It gives an overview of the tools on a real-life scenario, enabling the method to be used in the future. https://chess-eu.cs.ut.ee/2024/11/14/tool-supported-privacy-analysis-of-smart-parking/

CA2 theses:

Moravec, Erik. Metadata overlay for seccerts.org with security analysis tools (Supervisor: Petr Svenda).

This thesis provides technical design and prototype implementation of metadata overlay for sec-certs project utilising Common Criteria and FIPS140 certificates. Allows to map certification, data analysis and other metadata collection to certified product.https://chess-eu.cs.ut.ee/2023/11/27/metadata-overlay-for-seccerts-org-with-security-analysis-tools/

Murumaa, Maria Pibilota. Designing a Security Sensitive Self-assessment Framework (Supervisors: Mari Seeba, Tarmo Oja).

This thesis aims to design a security sensitive Self-Assessment Framework (SAF) for collecting answers to F4SLE (Framework for Security Level Evaluation). Maria collaborated with Cybernetica. https://chess-eu.cs.ut.ee/2023/08/25/designing-a-security-sensitive-self-assessment-framework/

Valgre, Magnus. Evaluating Cybersecurity Capabilities: Organisations' Perspective (Supervisor: Mari Seeba).

Magnus collaborated with National Cyber and Information Security Agency of the Czech Republic, the e-Governance Academy in Estonia, and Estonian Ministry of Economic Affairs and Communication. https://chess-eu.cs.ut.ee/2024/03/22/evaluating-cybersecurity-capabilities-organisations-perspective/

CA4 theses:

Ahmed, Ashfaq Hussain. Harnessing Blockchain and Digital Twin for Security Risk Assessment in Internet of Vehicles (Supervisors: Mubashar Iqbal, Sabah Suhail).

This thesis explores the integration of Digital Twins (DTs) and blockchain technology to enhance security in the Internet of vehicles (IoV). The work proposes and evaluates a blockchain-based security framework to address security threats in IoV, demonstrating its effectiveness through a Microsoft Azure Digital Twin simulation. https://chess-eu.cs.ut.ee/2023/08/25/harnessing-blockchain-and-digital-twin-for-security-risk-assessment-in-internet-of-vehicles/

Hanák, Petr. Analysis of security features of smart lock protocol (Supervisor Petr Švenda, Arnis Parsovs).

The thesis analyses the design and security of the Noke HD smart lock. In the design analysis, we reverse-engineer the lock's protocol because its documentation is not publicly available. We further analyse its design elements. In the security analysis, we assess the protocol's security against common attacks on authentication protocols and other attacks on smart locks. The result of the thesis is a description of the padlock's protocol and its security analysis.
https://is.muni.cz/th/voxd3/Analysis_of_security_features_of_smart_lock_protocol.pdf

Hluštík, Dominik. Simulation-based analysis of Whirlpool CoinJoin protocol (Supervisor Petr Švenda).

The thesis focuses on the implementation of the Whirlpool protocol, a specific implementation of CoinJoin developed by a group of developers called Samourai. The theoretical part explains the protocol's inner workings and the privacy guarantees it provides. In the practical part of the thesis, a simulation apparatus was developed to execute CoinJoin mixing simulations repeatedly, allowing for testing and data collection. Using the collected data, the thesis analyses the anonymity achieved by using Whirlpool.
https://is.muni.cz/th/qx8vb/Bachelor_s_Thesis.pdf

Janků, Jakub. Schnorr Multi-Signatures for Secure Devices with Restricted Interfaces (Supervisor: Antonín Dufka).

This thesis focuses on the provable security of modern Schnorr multisignatures and their applicability in constrained settings of secure hardware, smart cards and TPMs specifically. The primary result is a multi-signature scheme with multiplicative key sharing accelerated using the ECDH primitive commonly provided by smart cards. A proof-of-concept implementation comprising an optimized JavaCard applet and an Android reader application is provided to demonstrate the scheme's practicality. https://chess-eu.cs.ut.ee/2024/02/12/schnorr-multi-signatures-for-secure-devices-with-restricted-interfaces/

Leung, Kin Long. A Decentralized Public Key Infrastructure for Trust Management in X-Road (Supervisors: Mariia Bakhtina, Ahmed Awad, Raimundas Matulevičius).

This thesis introduces a Decentralized Public Key Infrastructure (DPKI) utilizing decentralized identifiers and verifiable credentials to overcome the limitations of the traditional Public Key Infrastructure with X.509 (PKIX). https://chess-eu.cs.ut.ee/2023/07/31/a-decentralized-public-key-infrastructure-for-trust-management-in-x-road/

Sipilä, Heikki Santeri. Scalability Assessment in Blockchain-enabled IoT Applications (Supervisors: Mubashar Iqbal, Abasi-amefon Obot Affia, Russell W. F. Lai).

This thesis develops and validates a scalability assessment tool using virtualization software, enabling the simulation of IoT devices to test blockchain-enabled applications without relying on physical devices, and demonstrates its application with a blockchain-based Internet of vehicles prototype. https://chess-eu.cs.ut.ee/2023/08/25/scalability-assessment-in-blockchain-enabled-iot-applications/

Miadzieles, Edgar. Digital Twin and Blockchain-Driven Firmware Updates for the Internet of Vehicles (Supervisor: Mubashar Iqbal).

This thesis investigates the Over-the-Air (OTA) firmware update process for vehicles within the context of the Internet of vehicles (IoV) and Intelligent Transportation Systems (ITS). It explores how blockchain and Digital Twin (DT) technologies can address limitations of traditional client-server OTA systems. https://chess-eu.cs.ut.ee/2024/06/05/digital-twin-and-blockchain-driven-firmware-updates-for-the-internet-of-vehicles/

Mika, Kristián. Analysis and Use of Standard Cryptographic Interfaces (Supervisor: Antonín Dufka).

This thesis investigates the possibility of threshold computation integration into common cryptographic interfaces. Firstly, the work analyses a set of selected cryptographic interfaces for their capabilities, limitations, and threshold computation integration. The reviewed interfaces are the Cryptoki interface specified by PKCS #11, FIDO specifications, Web eID solution, and Bitcoin Hardware Wallet Interface. The thesis proposes a set of

applications providing cryptographic interfaces called Bridge Suite. It delegates cryptographic computations from chosen cryptographic interfaces to a threshold platform, demonstrating the possibility of threshold integration into user applications without any changes to their implementation. A dedicated application for effortless suite management and use is also implemented. https://chess-eu.cs.ut.ee/2024/02/15/analysis-and-use-of-standard-cryptographic-interfaces/

Rajnoha, David. Detection of Bitcoin keys from hierarchical wallets generated using BIP32 with weak seed (Supervisor: Petr Svenda).

This thesis analyses the presence of real keys present on the Bitcoin blockchain with respect to potential vulnerability steaming from a small entropy in BIP32 seed and provides mapping of their occurrence in time and activity of attackers stealing the funds. https://chess-eu.cs.ut.ee/2023/11/27/detection-of-bitcoin-keys-from-hierarchical-wallets-generated-using-bip32-with-weak-seed/

Rýpar, David. Analysis of WabiSabi CoinJoin protocol and Wasabi 2.0 implementation (Supervisor Petr Švenda).

This thesis investigates the possibilities of anonymising bitcoin transactions and funds. The work analyses selected protocols that are usable for increasing bitcoin privacy. Next, the WabiSabi CoinJoin protocol is analysed in greater detail, both as described in its paper and as implemented in Wallet Wasabi 2.0. The thesis provides insight into the processes happening during the WabiSabi coinjoin in both the client and backend sides of Wallet Wasabi. Subsequently, the thesis introduces two setups for running simulations of WabiSabi conjoins – a local setup implemented as part of the work and an extension of a containerised setup. Lastly, the impact of selected parameters on the anonymity achieved with WabiSabi coinjoins is experimentally analysed using the containerised setup. https://is.muni.cz/th/xo2m6/thesis.pdf

Tudavekar, Ojus Virendra. Blockchain and Digital Twin-based Approach for Securing Water Supply Infrastructure (Supervisor: Mubashar Iqbal).

This thesis explores the integration of Digital Twin (DT) and blockchain technology to enhance the security and resilience of Water Cyber-Physical Systems (Water CPS). https://chess-eu.cs.ut.ee/2024/06/05/blockchain-and-digital-twin-based-approach-for-securing-water-supply-infrastructure/

CA5 theses:

Havlín, Jan. Network Traffic Encryptor on Linux Platform (Supervisor Jan Hajný).

The thesis focuses on providing encrypted communication between two Linux operating system stations. https://theses.cz/id/kev7ef/Bakalarska_prace.pdf

Tůma, Petr. Linux encryptor of network traffic (Supervisors: Jan Hajný, Petr Sysel).

In his Master's thesis, Petr Tuma developed a software solution for high-speed network traffic encryption using post-quantum cryptography. This software was deployed and piloted between Brno University of Technology (academia) and Cybernetica (industry). Petr is still (even after graduation) active in software development and testing, in collaboration with Cybernetica. https://chess-eu.cs.ut.ee/2023/08/26/linux-encryptor-of-network-traffic-2/

CA6 theses:

Geržičák, Daniel. *Scalable Training Environment for Personalized Hands-On Cybersecurity Challenges (Supervisor Pavel Čeleda).*

Cybersecurity is an ever-evolving field. The cybersecurity workforce needs to adapt to new threats and improve their practical skills. Recent research on education methods shows that hands-on training is the most effective learning method. With hands-on training, the participants convert their theoretical knowledge to practical skills. These hands-on exercises also pose an important factor in motivating students. Hands-on cybersecurity training demands dedicated, mostly virtualized, environments. As the requirements for training change and the number of participants in these exercises increases, new demands are put on these environments. They have to sustain up to hundreds of concurrent participants, which puts high requirements on resource efficiency. As a response, container-based environments are becoming favoured in these scenarios over virtual-machine-based ones. Such environments are also needed for university courses, where students gain valuable hands-on experience. This bachelor thesis designs and implements a training environment that can be deployed on participants' devices, is resource efficient, and puts emphasis on security and cheating detection and prevention. https://is.muni.cz/th/czv7o/

Falešník, Tomáš. Simplifying Technical Environment of Cybersecurity Hands-On Classes with Containers (Supervisor Pavel Čeleda).

This thesis explores transitioning from VM-based to container-based technical environments for the PA211 cybersecurity course at Masaryk University. Traditional virtualization methods like VirtualBox are resource-intensive and complex. By using Docker and Podman to reduce hardware resource demands, the thesis aims to simplify the setup and enhance scalability and accessibility. The thesis analyses the current infrastructure, identifies limitations, implements a container-based architecture and deploys and tests the container-based infrastructure during the spring 2024 semester course run. The results show significant improvements in efficiency and usability, making containerization a viable alternative for modern cybersecurity education. https://is.muni.cz/th/voth4/

Olšáková, Bára. *Enhancing Hands-On Class Delivery: Leveraging the KYPO Cyber Range Platform (Supervisor Pavel Čeleda).*

This bachelor thesis aims to design and implement the transformation of the current educational format of lessons in the PV276 – Seminar on Simulation of Cyber Attacks course into a hands-on, interactive training format within the KYPO Cyber Range Platform. In addition, this thesis explores current online cybersecurity education options and compares the differences between interactive and non-interactive platforms. The thesis also places the KYPO Cyber Range Platform in a perspective where the platform combines both approaches to cybersecurity education by offering linear training and adaptive training, which are tailored to individual abilities. The work results are lessons transferred to the KYPO Cyber Range Platform and a Python script that converts the training definitions from JSON to Markdown or HTML, ensuring students can access lesson assignments outside the KYPO Cyber Range Platform. https://is.muni.cz/th/tmoj2/

Krejčíř, Michal. Development of Hybrid Cybersecurity Exercise (Supervisor Jan Vykopal).

The goal of this thesis is to design and test a hybrid cybersecurity exercise in the INJECT Exercise Platform (IXP). Traditional tabletop exercises (TTXs) focus on non-technical areas of cybersecurity, while technical exercises focus on technical ones. However, cybersecurity incident response requires proficiency in both areas. A hybrid exercise integrates both areas in a single exercise, offering comprehensive training and testing of incident response. As a result of this thesis, a hybrid exercise was developed and implemented in IXP. The exercise was pilot-tested at the Faculty of Informatics of Masaryk University with the participation of students and faculty members. The pilot testing provided feedback from the exercise participants, which was used to improve the exercise and gain more insight into the area of hybrid exercise development. The findings from this thesis will make it easier to develop and run higher-quality hybrid exercises in the IXP. https://is.muni.cz/th/xbp87/

Hájek, Tomáš. Development of Tabletop Cybersecurity Exercises. (Supervisor Jan Vykopal)

Tabletop exercises are very effective for testing procedures for mitigating cybersecurity incidents. However, they have one major drawback: the pen-and-paper format. This thesis explores the potential of using a web application called INJECT Exercise Platform (IXP) as a tool for cybersecurity tabletop exercises. The thesis proposes recommendations for designing, implementing, and facilitating such exercises, which include the design methodology, the learning objectives and activities. This work examines two distinct exercise formats for the IXP. The first is a more automated and technical exercise in the team-based format already used in the IXP. In the second case, I created a design concept for roles, which was used to develop a role-based exercise that showcases the role format. The test runs showed the viability of role-based exercises in the IXP and provided suggestions for improvements to the exercise for IT administrators. The thesis results in two fully functional and tested exercises ready to be deployed in the IXP. https://is.muni.cz/th/ycnny/

Veselý, Marek. Analyst View for Instructors and Designers of Tabletop Exercises. (Supervisor Jan Vykopal)

This thesis presents an application for the analysis and monitoring of tabletop exercises conducted with the INJECT platform. A set of functional requirements was derived from an existing prototype built in a different frontend framework, extending its functionality. The application helps instructors track the progress of running exercises, allowing them to respond to any setbacks participating teams may face. It is also possible to analyze finished exercises. Consequently, the instructors can evaluate the participants' performance, and the designers can review their exercises and improve them accordingly. The application was tested with two exercises held in November and December 2023. The first was attended by students of the Faculty of Informatics, Masaryk University, and the other by employees of the National Cyber and Information Security Agency (NCISA). The application helped monitor the exercises and highlighted potential issues in their design. The exercise designers could address these problems before the exercises are used again. https://is.muni.cz/th/oo47p/

4.3 Tools and Frameworks

Our teams have been working on several solutions, improvements, and/or deployment of technologies, systems, or methods between sectors or region. An overview of these for each Challenge Area is presented below.

CA1: Internet of Secure Things

Forensic-Ready Analysis Suite (FREAS) is a tool that facilitates the design of forensic-ready software systems. Such systems integrate proactive preparation for a possible investigation of a security incident or accident in their design. The tool was showcased at the International Conference on Research Challenges in Information Science (RCIS 2024).

Demonstrator URL: https://youtu.be/Y38zS_6XY-I?si=fNT2yQqm2W2-5-f5

CA2: Security Certification

Sec-certs system for analyses of the product security certification documents and vulnerabilities. Tool showcased at several world certification conferences, such as the 2024 EU Cyber Acts Conference, 2024 Common Criteria Conference (booth and demonstration organized by Red Hat) or 2024 International Cryptographic Module Conference (with co-funding from the OpenSSL Foundation).

CA3: Verification of Trustworthy Software

Teams in Challenge Area 3 concentrate on developing tools for technology transfer. Their goal is to extend and improve the DiffKemp tool that aims at checking preservation of the semantics of low-level code during refactoring or to improve the efficiency of Perun, a lightweight performance version system as well as a tool suite that helps developers keep the resource consumption of their projects in check throughout the development.

CA4: Security Preservation in Blockchain

Digital Twin and Blockchain-Driven Firmware Updates for the Internet of Vehicles

1. Demonstration showing firmware update process for simulated vehicle

    a. Demonstrator URL: https://www.youtube.com/watch?v=YMxsj7EL0K4
2. Demonstration showing firmware update process for DT
    a. Demonstrator URL: https://www.youtube.com/watch?v=ZB0kCQmCBBc

Blockchain and Digital Twin-based Approach for Securing Water Supply Infrastructure

1. Data simulators to update DT in Azure DT explorer
    a. Demonstrator URL: https://www.youtube.com/watch?v=a0flp3gle7s
2. Data ingestor showing an interaction with blockchain and Azure DT explorer.
    a. Demonstrator URL: https://www.youtube.com/watch?v=o-OVBq7rUqw

Harnessing Blockchain and Digital Twin for Security Risk Assessment in Internet of Vehicles

1. Data simulators to update DT in Azure DT explorer
    a. Demonstrator URL: https://www.youtube.com/watch?v=9dYQHXv6FgE
2. Data ingestors Interaction with blockchain and Azure DT explorer
    a. Demonstrator URL: https://www.youtube.com/watch?v=R-YqUxDT-Vk
3. Creating digital twins using DTDL
    a. Demonstrator URL: https://www.youtube.com/watch?v=2sKrl3EReFM

Scalability Assessment in Blockchain-enabled IoT Applications

1. Demonstrator URL: https://www.youtube.com/watch?v=gT7brY6Abfc

JCMint: a JavaCard implementation of BDHKE and dBDHKE protocols on secp256k1 curve https://github.com/crocs-muni/JCMint

Library for RSA-threshold implementation: https://github.com/crocs-muni/pretzel

Proof-of-concept implementation of distributed key management system for organisational identity management using threshold signature in X-Road: https://github.com/crocs-muni/xroad-threshold-signatures

Demonstrator: A Decentralized Public Key Infrastructure for Trust Management in X-Road: https://youtu.be/01VW5f_mo7I?si=6DByIJltPt3rZt2N

IoV-TwinChain: https://github.com/mubashar-iqbal/vehicle-predictive-maintenance

Blockchain and Digital Twin for Security Risk Assessment: https://github.com/SanttuSi/IoTSimulation/tree/validationTest1

Blockchain-enabled IoT Applications Scalability Assessment Tool: https://github.com/mubashar-iqbal/IoV-digital-twin

JCProfilerNext: an automated static and dynamic analysis of code on JavaCard smart cards: https://github.com/lzaoral/JCProfilerNext

JCMathLib: an open-source library for the JavaCard platform that aims to enable low-level cryptographic computations unavailable in the standard JavaCard API. https://github.com/OpenCryptoProject/JCMathLib/

JCFROST: a JavaCard implementation of FROST threshold signature scheme using public JavaCard API: https://github.com/crocs-muni/JCFROST

Blockchain and Digital Twin-based Attack Deception: https://github.com/Ojusvt/thesis-DigitalTwinasAttackDeception

Digital Twin and Blockchain-Driven Firmware Update: https://github.com/edgarmiadzieles/thesis

CA5: Post-quantum Cryptography

- Work on migrating the e-voting system to post-quantum cryptography.
- Post-quantum cryptography (PQC) in virtual private networks (VPN): a secure communication channel software has been developed, deployed and tested by CHESS consortium partners. The implementation, which is open-source, may be used for larger projects and solutions in PQC.
- The PQC VPN solution will be deployed and tested between Brno (Czechia, academia) and Tartu (Estonia, industry)

CA6: Human-centric Aspects of Cybersecurity

The proof-of-concept implementations, documented in the defended theses of CA6, have been further developed and are now actively used in production to deliver hands-on cybersecurity courses and training. The key components include:

- Hands-on training infrastructure: cross-platform (x86_64, arm64), resource-efficient, and container-based using Docker and Podman;
- Cheating prevention and detection: automated problem generation and detailed logging;
- Class delivery: comprehensive training definitions and materials, incorporating both linear and adaptive hands-on training as well as tabletop exercises.

5 Impact of CHESS R&I activities

In CA1 (Internet of secure things), we focus on emerging smart transportation systems and services that connect users, the Internet of vehicles and smart applications. In this area, we have analysed the situations in both regions (EST, CZ) and initiated dialogue with various companies. In the CA mini-projects, we aim to increase user privacy and security in currently widespread use cases, such as smart parking and shared vehicles. Secondly, CA1 works on forensic readiness design that increases the trustability, security, and validation of complex systems. Some companies and stakeholders have already expressed interest in this approach in CHESS meetings and have started to consider adopting it into their services.

In CA2 (Security certification), work on the sec-certs toolset for the analysis of product security certification documents based on the Common Criteria and FIPS 140 schemes, together with links to published vulnerabilities, has gained significant traction. The sec-certs toolset has been tested by several commercial partners and presented to public authorities and policymakers in the Czech Republic and Estonia, but also showcased at several world certification conferences, such as the 2024 EU Cyber Acts Conference, 2024 Common Criteria Conference (booth and demonstration fully sponsored organized by Red Hat), and the 2024 International Cryptographic Module Conference (trip sponsored by a partner from the fourth sector, the OpenSSL Foundation). Initial discussions of including the forthcoming EUCC certification documents began in Q4/2024 with the Head of Sector Certification of the European Union Agency for Cybersecurity (ENISA).

In CA3 (Verification of trustworthy software), several program analysis tools have been developed. DiffKemp and Perun provide better support for developers in understanding and maintaining the semantics of their code during refactoring and performance optimisation. This leads to more reliable software, as developers can more easily identify and correct semantic changes and performance issues. The research on separation logic and stochastic systems contributes to the theoretical foundations of formal methods. This work can lead to more robust and reliable tools for verifying and validating software, which in turn can improve the quality and safety of software systems. The enhancement of tools like Fizzer for automated test generation can lead to more efficient and thorough testing processes. This can result in fewer bugs and vulnerabilities in software, ultimately improving software quality and reliability.

CA4 (Security Preservation in Blockchain) mini-projects have significantly contributed to securing information through the application of blockchain technology. For example, by leveraging blockchain technology in the Internet of vehicles, we have established a decentralised and immutable framework to protect sensitive data transmissions in real time, reducing risks like data breaches and malicious attacks. The work on anonymous e-cash tokens and improved mint protection using secure hardware has contributed to secure digital currency systems by mitigating risks associated with token issuance and decryption. The privacy analysis of CoinJoin transactions has contributed to the understanding of the vulnerabilities of privacy-focused cryptocurrencies, helping improve the robustness of transaction anonymisation mechanisms. As a part of CA4, we developed tools for conducting large-scale emulations with Wasabi 2.x wallets, analysed historical CoinJoin transactions across Wasabi 1.x, Wasabi 2.x, and Whirlpool coordinators, and evaluated the impact of fee structures on the feasibility and difficulty of mounting Sybil attacks.

Through the development and implementation of proof-of-concept infrastructure for authentication using post-quantum cryptographic algorithms, work in CA5 (Post-quantum cryptography) contributes to the transition from traditional cryptographic methods to more advanced, post-quantum ones. This is crucial, as quantum computers could potentially break many of the current cryptographic systems. The ongoing work to establish a post-quantum remote electronic voting system addresses a critical need for secure and verifiable

digital voting processes. The development of a library implementing core post-quantum cryptographic primitives is a valuable resource for researchers and developers working in the field of cybersecurity. This library can serve as a foundation for further research and practical applications. The successful establishment of a fully functional quantum-safe communication channel between Estonia and Czechia is a significant achievement. This demonstrates the practical feasibility of using post-quantum cryptography for real-world communication needs, despite the current technological limitations.

CA6 (Human-centric aspects of cybersecurity) focuses on enhancing the capabilities and awareness of both students and professionals. By improving the training environment, including cross-platform support and resource efficiency, the initiative has created a more accessible and efficient learning space for cybersecurity students and professionals. The introduction of container-based training environments allows for a more versatile and scalable training setup. With the introduction of automatic problem generation, logging, and improved class delivery mechanisms, the initiative has taken steps to ensure the integrity of cybersecurity training. This focus on cheating prevention and detection helps maintain the credibility and effectiveness of the training programs. The development of a new challenge for the Czech national cybersecurity competition has contributed to the national cybersecurity education effort. On the other hand, through the improvement of the quality of penetration testing reports, CA6 helps ensure that IT professionals and managers can take informed actions based on the findings of these tests, thereby enhancing overall cybersecurity measures.

6 Our Plans

The focus of CA1 will continue to be on smart transportation. More specifically, we plan to verify and expand some proposed ideas, such as privacy-preserving car sharing in practical proof-of-concept demonstrations and security enhancing and verifying of teleoperated services. Secondly, we plan to focus more on risk management of automated systems and in other automotive areas. After opening and establishing collaborations with some industrial partners, the research will also be focused on practical aspects.

CA2 plans to (a) continue developing the sec-certs toolset mainly from the point of view of better usability, use of NLP techniques for document processing, and inclusion of the EUCC certification documents; (b) consider the translation of the F4SLE self-assessment framework for institutional security level evaluation to the Czech language while also turning to NUKIB once more for the integration of this method into its piloting and support activities related to certification and regulation; (c) further develop the security targets for certification under Common Criteria for MPC and TEE as secure computing techniques which will help with the certification and adoption of secure computing; and (d) a new mini-project, ‘Security Certifications Issues with Disk and Storage Encryption’, will start in January 2025.

CA3 plans to finish optimising the profiling process of Perun, enhancing the interpretation based on user feedback, and expand our profilers to support a wider range of application (e.g., full automatization of our e-BPF based prototype). We will also explore the possibilities

of matching program traces between different versions of software and will work on an advanced graphical user interface of Perun and its visualisation capabilities to maximise the productivity of its use in practice. We aim to deploy the tools in practice, for example, for analysis of the Linux kernel.

CA4 mini-projects aim to advance the application of blockchain technology for the enhancement of data security and propose a standardised security framework for the Internet of vehicles (IoV). Additionally, the development of a multi-party protocol for the distribution of operations in BDHKE-based e-cash will be a key focus, verified using physical smartcards on the JavaCard platform. Plans also include designing a trustless salt service with enhanced abuse resistance, leveraging cryptographic hardware components to ensure robust security and practical deployment.

CA5 is working towards building a post-quantum prototype for a remote electronic voting system. As an independent side result, a library implementing post-quantum primitives is maturing, and is expected to be released in the near future.

CA6 will focus on enhancing human-centric cybersecurity by developing hands-on training that emphasizes both professional and end-user skills. Leveraging the INJECT exercise platform, we aim to expand awareness and research on cybersecurity tabletops to improve team readiness through scenario-based emergency management activities. We will continue sharing best practices for effective training across both CHESS regions. Additionally, efforts will be made to advance usable security, ensuring that security products and processes are intuitive and accessible to all users.