Funded by the European Union

CYBERCHALLENGE Challenges Solving in Cybersecurity Study Program

CYBERCHALLENGE - *Challenges Solving in Cybersecurity Study Program No. 2024-1-LT01-KA220-HED-000252504*

Newsletter

August 2026

Challenge-based learning scenarios for studies in the lab and integration into study programme

Challenge-Based Learning provides an efficient and effective framework for learning while solving real-world Challenges. It can be used by every stakeholder in the school to develop strategic planning, connect current practices, strengthen ownership and personalization, and create life-long learners. Instead of competing with other approaches, it seeks to make connections and help all the stakeholders to co-create the learning experience.

The general objective of the CYBERCHALLENGE is to increase the availability of digital content, technologies, and practices by developing a Cybersecurity curriculum, including a Federated Cybersecurity Lab based on a tool sandbox and using a CBL methodology.
One of the main focuses of the project is to stimulate innovative learning and teaching practices to enhance student motivation, critical thinking and problem-solving skills. In this sense, the project also involves adding some CBL scenarios to the developed curricula.
CBL in university studies is not just another teaching method – it is a change in the philosophy of studies, from the accumulation of theoretical knowledge to the creation of real effects.
CBL is an integral part of the study module, the study process is transformed from "listening and doing tasks" to "researching, solving and implementing". CBL integration turns the study module not into a static set of knowledge, but into a dynamic ecosystem. At the master's level, such a model is extremely effective, because it simulates a real professional environment, where an expert must not only "know", but also "act" in the face of uncertainty. The developed model of the study module with CBL integration shows how each part complements each other.

One of the main focuses of the project is to stimulate innovative learning and teaching practices to enhance student motivation, critical thinking and problem-solving skills. In this sense, the project also involves adding some CBL scenarios to the developed curricula.

During the project implementation, four CBL scenarios were created, one for each module: Fundamentals of Cybersecurity, Identity and Access Management, Cyber Attacks and Cyber Defenses, and Cyber Security Management.

Fundamentals of Cybersecurity: The security of smart home systems

The Big Idea: *The security of smart home systems.*

The Core Challenge (Specific Problem): *Security problems in smart home systems are often related to security flaws in communication protocols. Security flaws at the protocol level are often more systemic and difficult for a layperson to fix.*

Connected homes offer convenience but also introduce significant security risks. How can we design systems that remain secure even if an attacker gains internal network access?.

Identity and Access Management

The Big Idea: *Challenge-Oriented Project Proposal: "Secure Access and Identity in a Federated Ecosystem".*

Design and implement a federated authentication and access control system that combines privacy-preserving identity management (using verifiable credentials and decentralized identity principles) with fine-grained access control mechanisms (RBAC, ABAC, and OAuth 2.0 delegation).

Students must simulate a real-world environment — e.g., a digital service platform (like e-Government, healthcare, or university system) — requiring secure, privacy-aware identity handling and policy-driven access control.

***The Core Challenge (Specific Problem):** How can we design a system that enables secure access and privacy-preserving identity verification across multiple services, using federated authentication (SSO) and delegated authorization (OAuth 2.0), while enforcing dynamic access control (RBAC/ABAC) policies?*

Key subproblems:

- *Managing digital identities and credentials securely.*
- *Preserving user privacy and minimizing data exposure.*
- *Implementing interoperable login via verifiable credentials (aligned with eIDAS).*
- *Applying access control principles (least privilege, separation of duties).*
- *Enforcing authorization with OAuth 2.0 scopes and tokens.*

Cyber Attacks and Cyber Defenses

***The Big Idea:** Improving the infrastructure of a partner company by simulating various types of*

***The Core Challenge (Specific Problem):** Transilvania University through its Cyber-Security master program and as one of the founding members of Brașov CyberHub is partnering with various institutions and companies to enhance and promote cybersecurity among all stakeholders. Based on this partnership agreement, Cyberchallenge students can participate in security assessments: Topic1. Test the resilience of the company to phishing attacks.*

Topic2. Check the institution network for known vulnerabilities

Topic3. Web application security assessment.

Cyber Security Management

***The Big Idea:** The security risk management in intelligent infrastructure, specifically in the Scooter Ride-Hailing System.*

***The Core Challenge (Specific Problem):** Security risk management issues in ride-hailing systems are related to system design, including input validation and representation, API abuse, security features, time, and state management, error handling, code quality, and similar concerns. Connecting system components and developing intelligent infrastructure are challenging activities that potentially might introduce security risks. The challenge is to envision these risks before the system is deployed, estimate them, and systematically reason and introduce their countermeasures.*

PROJECT COORDINATOR

ktu kaunas university of technology 1922

PROJECT PARTNERS

universidade de aveiro

Transilvania University of Brasov

https://www.cyberchallenge-erasmus.eu/

Kaunas University of Technology
Faculty of Informatics
Studentu str. 50, Kaunas, Lithuania