LITHUANIAN COMPUTER SOCIETY
VILNIUS UNIVERSITY, INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES
LITHUANIAN ACADEMY OF SCIENCES

16th Conference on

DATA ANALYSIS METHODS
for Software Systems

November 27–29, 2025

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

VILNIUS UNIVERSITY PRESS
Vilnius, 2025

Contacts:

Dr. Jolita Bernatavičienė
jolita.bernataviciene@mif.vu.lt
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt
Tel. (+370 5) 2109 315

https://doi.org/10.15388/DAMSS.16.2025
ISBN 978-609-07-1200-9 (digital PDF)

AMBER C2: Enhancing Cyber Defence with Ethical Adversarial Machine Learning

Arnoldas Budžys, Juozas Dautartas, Haroldas Jomantas, Viktor Medvedev, Olga Kurasova

Institute of Data Science and Digital Technologies
Vilnius University

arnoldas.budzys@mif.vu.lt

The cybersecurity world is divided into adversaries seeking to disrupt operations and defenders protecting sensitive infrastructure. The blue team protects and monitors systems while the red team attempts to breach them. The white team designs, implements, and manages the exercise infrastructure. The penetration testers use red team methods to find vulnerabilities before hostile actors do.

We are working on the AmberC2 project, which focuses on a secure Command and Control (C2) framework that integrates Adversarial Machine Learning (AML) to support realistic but controlled cyber exercises. We can manage ethically disguised malicious software in an isolated laboratory, applying strict security measures and comprehensive auditing. Our goal is training, evaluation, and research that strengthen defence. AmberC2 supports payload generation, delivery, and control channels that can be restricted, redirected, or terminated as needed. The framework explores evasion and concealment techniques inspired by AML methods, testing them only for instrumented purposes. These techniques help simulate advanced persistent threats while maintaining security. Approach-wise, AmberC2 investigates malware obfuscation and evasion techniques through AML methods. These methods correspond to the advanced persistent threats we are trying to replicate, thus offering protection measures against such attacks. The project presents the system architecture, management framework, and responsible operating procedures. The goal is to increase the realism of exercises, reveal gaps in modern defences, and accelerate the development of resilient security solutions. In the future, the variety of scenarios in

networks, operating systems, and cloud platforms will be expanded, and the threat generation policy will be refined to reflect changing methods.

Acknowledgments. This project has received funding from the Research Council of Lithuania (LMTLT), agreement No S-MIP-24-116.