Developing a secure virtual physical laboratory: addressing VR vulnerabilities in educational environments

UDK 37:004:316.772.5

Yuriy Skorenkyy[1], Oleksandr Parayil[2], Oleksandr Kramar[3]

Ternopil Ivan Puluj National Technical University,
[1]skorenkyy@tntu.edu.ua, [2]sashaparail@gmail.com, [2]kramar_o@tntu.edu.ua

The integration of digital technologies presents new opportunities for organizing the educational process, particularly within the natural sciences. A virtual physical laboratory that combines realistic simulations with interactive tasks is currently under development by the Cyber-Physical Systems Laboratory at TNTU.

While virtual reality (VR) environments offer immense educational benefits, their software implementation introduces significant cybersecurity vectors [1]. Educational applications built on industry-standard platforms like Unity and Unreal Engine face distinct vulnerabilities. Unity applications, for instance, are notoriously susceptible to reverse engineering; without proper obfuscation, attackers can decompile C# assemblies to manipulate core logic or alter Asset Bundles to inject malicious content. Unreal Engine applications similarly risk memory injection attacks and the unauthorized modification of unencrypted Blueprint visual scripting logic. In the specific context of a virtual lab, these engine-specific vulnerabilities directly enable the manipulation of non-player character (NPC) logic — allowing an attacker to alter a virtual assistant's scripts to provide incorrect experimental instructions. Furthermore, insecure network configurations inherent to many standard engine plugins pose a severe risk of data interception, threatening unauthorized access to students' personal information. To mitigate these threats, the application's architecture must be fortified. The proposed solution involves implementing a trusted update mechanism that automatically synchronizes with a secure repository, preventing the execution of tampered assets. Additionally, the integration of strict digital certificate verification guarantees the authenticity of the connection between the client application and the laboratory server.

Deploying virtual laboratories with advanced, secure architectures fosters inclusive education. It ensures equal access to high-quality educational resources, allowing students to master experimental skills in a safe, convenient, and fully protected digital environment [2].

1. 1. Kozak R., Skorenkyy Yu., Kramar O., Brevus V., Zagorodna N., Cybersecurity issues related to incorporation of VR components into Industry 5.0 human-machine interfaces. *Procedia Computer Science*. – 2026. – V. 276. – p. 176-184.
2. 3. Zagorodna N., Skorenkyy Y., Kunanets N., Baran I., Stadnyk M., Augmented Reality-enhanced learning tools development for cybersecurity major. *CEUR Workshop Proceedings.* – 2022. – V. 3309. – p. 25–32.