2024 RoEduNet Conference: Networking in Education and Research

Contribution ID: **66** Type: **Paper presentation**

# Improving the security of a webservice: best practices and attack simulations

*Friday 20 September 2024 10:10 (20 minutes)*

Abstract—Most of the nowadays applications are client-server based. Exposing a webservice is a common practice, but the question is: what happens when the webservice is exposed from a low-level programming language? How can we manage to avoid the most common mistakes which can introduce vulnerabilities into the application? This paper focuses not only on some of the best practices when developing a webservice using C++, but also on improving the security of that webservice. We proposed a series of methods to enhance the security of the application and some of them were validated using an empirical approach. Through comprehensive testing and analysis into a controlled environment, we confirmed that using a digital certificate on the server side can minimize the impact of the famous "man-in-the-middle"attack. We simulated two types of attacks on the developed webservice: a passive one –"sniffing"and an active one –"man-in-the-middle". The results underscore the fact that webservice security can also be enhanced even if it is developed using a low-level programming language.

**Authors:** Mrs ANGHEL, Ana Magdalena (POLITEHNICA University, Faculty of Automatic Control and Computers); Mr MIHALACHE, Daniel Cristian (POLITEHNICA University, Faculty of Automatic Control and Computers)

**Presenter:** Mr MIHALACHE, Daniel Cristian (POLITEHNICA University, Faculty of Automatic Control and Computers)

**Session Classification:** Network Security

**Track Classification:** Network Security