IEEE Access, vol.13, pp.126925-126934, December, 2025.

pwnobd: Offensive Cybersecurity Toolkit for Vulnerability Analysis and Penetration Testing of OBD-II Devices

R. Gesteira Miñarro; I. Gutiérrez Gómez; R. Palacios Hielscher; G. López López

Abstract-

The research field of vehicle cybersecurity has experienced a significant growth in interest due to the attack surface that the information systems comprising a vehicle provides and the ever-expanding body of regulations that provide special focus on cybersecurity on vehicular systems. Of particular interest is the attack surface exposed by OBD dongles, wireless devices that connect to the vehicle’s diagnostic port, whose access to the vehicle’s CAN buses could potentially be exploited by adversaries. However, acquiring a vehicle for use in the security assessment of these devices may not be possible for the researcher. In this article, we propose a software tool, pwnobd, that assists in developing proof-of-concept attacks seeking to take advantage of the found vulnerabilities, alongside an architecture for a research and demonstration platform that provides a testbed for vulnerability analysis and penetration testing for attacks towards these devices. A small battery of tests is then performed on several diagnostic devices using this platform, along with a focused study on one such device, proving the potential benefit of such platform for security researchers.

Index Terms- Cybersecurity, car hacking, on-board diagnostics, embedded device, Bluetooth.

Citation:
Gesteira-Miñarro, R.; Gutiérrez, I.; Palacios, R.; López, G. "pwnobd: Offensive Cybersecurity Toolkit for Vulnerability Analysis and Penetration Testing of OBD-II Devices", IEEE Access, vol.13, pp.126925-126934, December, 2025.