

Scientists found a way to maintain the cybersecurity of electronics in vehicles

February 9 2021



Credit: CC0 Public Domain

Specialists from Peter the Great St. Petersburg Polytechnic University (SPbPU) improved the cybersecurity system mechanism, based on the ECU (Electronic Control Unit) in modern vehicles. The research results

were published in the scientific journal *Nonlinear Phenomena in Complex Systems*.

Modern road transport systems are complex cyber-physical systems. Car electronics have a number of security problems, the solutions for which are difficult due to the limited computing power of some ECUs and stringent requirements for speed, including the data transfer rate. Most [scientific articles](#) divide the internal network of a motor vehicle into many domains according to its purpose.

"This distinction is relevant for solving relatively simple issues, not requiring flexible configuration. We divide the domains not according to their intended purpose, but according to their integrity level, an indicator that characterizes the susceptibility of each specific electronic unit to cyber impact and the potential harm caused by the disruption of its operation. Our scientific group developed a simulation model that automatically clusters the control units of a vehicle's on-board system and divides it into domains; thus, the [security breach](#) doesn't lead to negative consequences. This approach is modular and highly scalable. It doesn't impose the restrictions on computing resources, and also minimizes the redundancy of the applied security measures," notes Evgeniy Pavlenko, Associate Professor at the Institute of Cybersecurity and Data Protection SPbPU.

Experts mention that this is a unique development and such safety systems are not implemented in the vehicles. Evgeniy Pavlenko adds that in modern security systems the intruder's model practically doesn't consider the introduction into the electronic system of vehicles itself, and most studies are aimed at preventing the possibility of controlling the car from the outside. The developed technology ensures that the intruder wouldn't be able to introduce some kind of electronic units to affect the wrong decision-making in terms of piloting the [vehicle](#).

"Our development doesn't require complex calculations from the electronics installed in the car. We don't add cryptographic schemes. Currently we are at the stage of discussing our system with manufacturers of electronic devices for its experimental approbation," Pavlenko says.

More information: E. Yu. Pavlenko et al. A Model of Multi-Domain Clustering for Local Network in Modern Vehicles, *Nonlinear Phenomena in Complex Systems* (2020). [DOI: 10.33581/1561-4085-2020-23-3-280-290](https://doi.org/10.33581/1561-4085-2020-23-3-280-290)

Provided by Peter the Great St. Petersburg Polytechnic University

Citation: Scientists found a way to maintain the cybersecurity of electronics in vehicles (2021, February 9) retrieved 10 April 2024 from <https://techxplore.com/news/2021-02-scientists-cybersecurity-electronics-vehicles.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.
