New cybersecurity technique protects in-vehicle networks

July 27 2021

Credit: CC0 Public Domain

Army researchers developed a new machine learning-based framework to enhance the security of computer networks inside vehicles without undermining performance.

With the widespread prevalence of modern automobiles that entrust control to onboard computers, this research looks toward to a larger Army effort to invest in greater cybersecurity protection measures for its aerial and land platforms, especially heavy vehicles.

In collaboration with an international team of experts from Virginia Tech, the University of Queensland and Gwangju Institute of Science and Technology, researchers at the U.S. Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory devised a technique called DESOLATOR to help optimize a well-known cybersecurity strategy known as the moving target defense.

"The idea is that it's hard to hit a moving target," said Dr. Terrence Moore, Army mathematician. "If everything is static, the adversary can take their time looking at everything and choosing their targets. But if you shuffle the IP addresses fast enough, then the information assigned to the IP quickly becomes lost, and the adversary has to look for it again."

DESOLATOR, which stands for deep reinforcement learning-based resource allocation and moving target defense deployment framework, helps the in-vehicle network identify the optimal IP shuffling frequency and bandwidth allocation to deliver effective, long-term moving target defense.

According to Army computer scientist and program lead Dr. Frederica Free-Nelson, achievement of the former keeps uncertainty high enough to thwart potential attackers without it becoming too costly to maintain, while attainment of the latter prevents slowdowns in critical areas of the network with high priority.

"This level of fortification of prioritized assets on a network is an integral component for any kind of network protection," Nelson said.

"The technology facilitates a lightweight protection whereby fewer resources are used for maximized protection. The utility of fewer resources to protect mission systems and connected devices in vehicles while maintaining the same quality of service is an added benefit."

The research team used deep reinforcement learning to gradually shape the behavior of the algorithm based on various reward functions, such as exposure time and the number of dropped packets, to ensure that DESOLATOR took both security and efficiency into equal consideration.

"Existing legacy in-vehicle networks are very efficient, but they weren't really designed with security in mind," Moore said. "Nowadays, there's a lot of research out there that looks solely at either enhancing performance or enhancing security. Looking at both performance and security is in itself a little rare, especially for in-vehicle networks."

In addition, DESOLATOR is not limited to identifying the optimal IP shuffling frequency and bandwidth allocation. Since this approach exists as a machine learning-based framework, other researchers can modify the technique to pursue different goals within the problem space.

"This ability to retool the technology is very valuable not only for extending the research but also marrying the capability to other cyber capabilities for optimal cybersecurity protection," Nelson said.

Researchers detail information about their approach in the research paper, "DESOLATER: Deep Reinforcement Learning-Based Resource Allocation and Moving Target Defense Deployment Framework," in the peer-reviewed journal *IEEE Access*.

More information: Seunghyun Yoon et al, DESOLATER: Deep Reinforcement Learning-Based Resource Allocation and Moving Target

Defense Deployment Framework, *IEEE Access* (2021). DOI: 10.1109/ACCESS.2021.3076599

Provided by The Army Research Laboratory