First Look: Cybersecurity Best Practices for Modern Vehicles

Describes the National Highway Traffic Safety Administration's (NHTSA) nonbinding guidance to the automotive industry for improving motor vehicle cybersecurity

Updated last **March 6, 2018**
for the 10/28/2016 version of the document.

HAL
Humans and Autonomy Lab

WHAT IT DOES

The document, Cybersecurity Best Practices for Modern Vehicles, describes the National Highway Traffic Safety Administration's (NHTSA) nonbinding guidance to the automotive industry for improving motor vehicle cybersecurity. The document is intended to cover cybersecurity issues for all motor vehicles and is therefore applicable to all individuals and organizations manufacturing and designing vehicle systems and software. These entities include, but are not limited to, motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, alterers, and modifiers.

Motor vehicle and motor vehicle equipment manufacturers are required by the National Traffic and Motor Vehicle Safety Act to ensure that systems are designed free of unreasonable risks to motor vehicle safety, including those that may result due to existence of potential cybersecurity vulnerabilities. Vehicles are built from, and depend upon, the seamless integration of computational algorithms and physical components. As such, vehicle cybersecurity vulnerabilities could impact safety of life. Therefore, NHTSA's authority would be able to cover vehicle cybersecurity, even though it is not currently covered by an existing Federal Motor Vehicle Safety Standard (FMVSS).

NHTSA has focused on solutions to harden the vehicle's electronic architecture against potential attacks and to ensure vehicle systems take appropriate and safe actions, even when an attack is successful. NHTSA advises that the automotive industry follow the National Institute of Standards and Technology's documented Cybersecurity Framework, which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover."

Comments for this document were collected through November 28, 2016.

This First Look was adapted from Section 1 of the Cybersecurity Best Practices document.

PRIMARY AUTHOR

Michael Clamann, PhD, CHFP

LICENSE