The Imperative of Security by Design: NHTSA Releases Cybersecurity Best Practices

10.26.2016

Responding to growing threats to vehicle safety from cybersecurity vulnerabilities, NHTSA released guidelines for cybersecurity best practices for motor vehicle OEMs, suppliers and aftermarket manufacturers.

Introduction

On October 24, 2016, the National Highway Traffic Safety Administration (NHTSA) announced its non-binding guidance titled "Cybersecurity Best Practices for Modern Vehicles" (Guidelines).

In the wake of the well-publicized Jeep hacks (summer 2015) and last Friday's DDoS attack against the managed DNS infrastructure of Dyn, the need to protect the safety of drivers and passengers against cyber-perils has never been greater. Acknowledging its responsibilities under the Motor Vehicle Safety Act (Act), NHTSA issued this guidance to promote cybersecurity practices that ensure vehicle systems and related software are designed free of unreasonable risks to motor vehicle safety. To date, NHTSA has used its enforcement authority to recall nearly 1.5 million vehicles due to cybersecurity vulnerabilities deemed potential safety risks under the Act.

NHTSA's Guidelines

While voluntary, the Guidelines target original equipment manufacturers (OEMs), suppliers, designers, modifiers and aftermarket manufacturers in the motor vehicle sector with the intent of making vehicle cybersecurity an organizational priority. The Guidelines seek to establish standard definitions for cybersecurity terminology in the vehicle context and encourage the auto industry to follow the National Institute of Standard and Technology's (NIST) Cybersecurity Framework which provides a policy framework for assessing risk structured around five

Related Services

Cybersecurity and Privacy Specialty Team

principal functions: identify, protect, detect, respond and recover.

In developing the Guidelines, NHTSA again turned to standards organizations and drew from their recent publications and best practices: Society of Automotive Engineers (SAE) J3061 Recommended Practice Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, the ISO 27000 series, and the Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" (CIS CSC).

Assessing the vehicle landscape, NHTSA recognized a number of major risks:

- **Developer access**. Limit or eliminate developer access to electronic control units (ECUs) so that only privileged access occurs.
- **Control keys**. Protect control keys (cryptographic or password) from unnecessary disclosure and limit access to no more than one distinct vehicle and not to an entire platform.
- **Maintenance diagnostic access**. Limit the authority or duration of diagnostic control actions to reduce the risk of misuse or abuse.
- **Access to and the ability to modify firmware**. Employ good security practices, such as the use of digital signing techniques and other limits to reduce the accessibility and likelihood that malware may be installed on a vehicle. Further tactics may include security coding practices and whole disk encryption.
- **Network ports, protocols and services**. Limit the use of network servers on ECUs to essential functions, which will assist in preventing use by unauthorized individuals.
- **Segmentation and isolation in vehicle architecture**. Incorporate privilege separation with boundary controls, including logical and physical isolation, to minimize the risk from external threat vectors.
- **Internal vehicle communications**. Minimize sending safety messages across common data buses and use segmented communications buses to reduce the risk that critical safety messages could be manipulated.
- **Back end servers**. Employ encryption methods in any IP based communication between an external server and the vehicle.
- **Wireless connectivity**¸ Design features to allow for changes in network routing rules in anticipation of connectivity issues across wireless cell networks.

NHTSA further encourages organizations to dedicate resources to research, investigate, implement, test and validate product related cybersecurity measures and vulnerabilities. These considerations include the need to assess both safety critical vehicle functions and any personal identifying information (PII) collected by the automobile.

This guidance is open for comment for 30 days.

Key Takeaways

Suppliers manufacturing components with connectivity or cyber risks should:

- Perform a full life-cycle assessment on the component(s) with an emphasis on potential risk at all phases of life.
- Incorporate rapid detection and remediation capabilities to mitigate safety risks to vehicle occupants and road users if an attack occurs.
- Create a vulnerability reporting and disclosure policy to establish how the company will interact with organizations like the Auto ISAC, independent researchers or other industry groups.
- Establish an Incident Response plan and policy to document the process to respond to discovered incidents and vulnerabilities.
- Create an audit protocol to assess risk determinations, penetration testing and organizational decision making.
- Encourage engineers to participate in standards bodies including SAE and IEEE. These organizations will continue to have a direct impact on the direction of the industry and regulations.

If you have any questions about these recommendations, please contact the authors of this alert.

Jennifer Dukarski
734.213.3427
dukarski@butzel.com

Claudia Rast
734.213.3431
rast@butzel.com