The U.S. Department of Transportation, National Highway Traffic Safety Administration's "The Cybersecurity Best Practices for Modern Vehicles" (2016, October) (Report No. DOT HS 812 333) provides nonbinding guidance to the automotive industry for improving motor vehicle cybersecurity.

Opening Statement
Per Forbes Magazine 04/26/2023 article "Advanced Cars May Face Greater Risk Of Hacking, Cybersecurity Experts Warn", Top-of-the line vehicles contain 1,000-3,000 microchips, as many as 150 electronic control units or ECUs operated by up to 150 million lines of software code according to a report by the National Center for Manufacturing Sciences (NCMS). That amounts to four times more lines of code than a fighter jet, and projected to rise to 300 million lines of code by 2030, according to a report by the United Nations Economic Commission for Europe or UNECE.

6.6 Self-Auditing
Question 1. In addition to implementing a cybersecurity process based on a sound systems engineering approach, the automotive industry should document the details related to the cybersecurity process to allow for both auditing and accountability.
Panel Member: Samuel C. Hollifield is a cybersecurity research scientist at Oak Ridge National Laboratory's Cyber Resilience and Intelligence Division
What is your auditing approach to ensuring cybersecurity risk management for the vehicles transporting nuclear and radioactive materials?

6.6.1 Risk Assessment
Question 2. The automotive industry should develop and use a risk-based approach to assessing vulnerabilities and potential impacts and should consider the entire supply-chain of operations. This approach should involve an ongoing risk management framework to assess and mitigate risk over time.
Panel Member: Joshua Poster is the Intel and Analysis Operations Manager of the Auto Information Sharing and Analysis Center (Auto-ISAC)
What is your risk-based approach to assessing threats, vulnerabilities and potential impacts?

6.6.2 Penetration Testing and Documentation
Question 3. Penetration tests should include stages that deploy qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities.
Panel Member: Keith Fidura is a Computer Engineer IV at Battelle Memorial Institute with the Cyber Solutions Division (CSD)
What Penetration Testing methodologies and tools do you recommend to assess vehicle cybersecurity?

6.6.3 Self-Review
Question 4. The automotive industry should establish procedures for internal review and documentation of cybersecurity-related activities. This will assist companies in better understanding their cybersecurity practices and determining where their processes could benefit from improvement. One suggested approach is for the automotive industry to produce annual reports on the state of their cybersecurity practices.

Panel Member: Joshua Poster
Does the Auto Information Sharing and Analysis Center (Auto-ISAC) produce reports? If yes, how frequently? What do you recommend as industry best practices?

6.7 Fundamental Vehicle Cybersecurity Protections
NHTSA recommends:
6.7.1 Limit Developer/Debugging Access in Production Devices
Question 5. Software developers have considerable access to ECUs. Developer access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units. Physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.
Note: Electronic Control Unit (ECU) is an embedded system that provides a control function to a vehicle's electrical system or subsystems through digital computing hardware and associated software.
Panel Member: Samuel C. Hollifield
Do you agree? What other Developer/Debugging Access restrictions do you recommend?

6.7.2 Control Keys
Question 6. Any key (e.g., cryptographic) or password which can provide an unauthorized, elevated level of access to vehicle computing platforms should be protected from disclosure. Any key obtained from a single vehicle's computing platform should not provide access to multiple vehicles.
Panel Member: Keith Fidura
Do you agree? How should cryptographic key management be handled?

6.7.3 Control Vehicle Maintenance Diagnostic Access
Question 7. Diagnostic features should be limited as much as possible to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature. Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes. For example, a diagnostic operation which may disable a vehicle's individual brakes could be restricted to operate only at low speeds.
Panel Member: Joshua Poster
What diagnostic vehicle capabilities present the greatest risk? What security controls do you recommend to limit the adverse effects of exploited Vehicle Maintenance Diagnostics?

6.7.4 Control Access to Firmware
Question 8. Firmware precisely determines the actions of an ECU. Extracting firmware is often the first stage of discovering a vulnerability or structuring an end-to-end cyberattack. Developers should employ good security coding practices and use tools that support security outcomes in their development processes. Organizations should reduce any opportunities for a third party to obtain unencrypted firmware during software updates.
Panel Member: Samuel C. Hollifield
What best practices do you recommend for firmware development, testing, and third party access?

6.7.5 Limit Ability to Modify Firmware
Question 9. Limiting the ability to modify firmware would make it more challenging for malware to be installed on the vehicles. For example, use of digital signing techniques may make it more difficult and perhaps prevent an automotive ECU from booting modified/ unauthorized and potentially damaging firmware images.
Panel Member: Keith Fidura
Do you agree with Digitally signing firmware and applying security controls that block firmware updates from unverified sources?

6.7.6 Control Proliferation of Network Ports, Protocols and Services
Question 10. The use of network servers on vehicle ECUs should be limited to essential functionality only and services over such ports should be protected to prevent use by unauthorized parties. Any software listening on an internet protocol (IP) port offers an attack vector which may be exploited. Any unnecessary network services should be removed.
Panel Member: Joshua Poster
Should ECUs be accessible from the internet? If yes, what security controls should be applied to limit access to personnel with a legitimate maintenance requirement?

6.7.7 Use Segmentation and Isolation Techniques in Vehicle Architecture Design
Question 11. Privilege separation with boundary controls is important to improving security of systems. Logical and physical isolation techniques should be used to separate processors, vehicle networks, and external connections as appropriate to limit and control pathways from external threat vectors to cyber-physical features of vehicles. Strong boundary controls, such as strict white list-based filtering of message flows between different segments, should be used to secure interfaces.
Panel Member: Samuel C. Hollifield
What vehicle architecture do you recommend to segment functionality and access?

6.7.8 Control Internal Vehicle Communications
Question 12. Critical safety messages are those that could directly or indirectly impact a safety critical vehicle control system's operations. When possible, sending safety signals as messages on common data buses should be avoided. For example, providing an ECU with dedicated inputs from critical sensors eliminates the common data bus spoofing problem.
Panel Member: Joshua Poster
Should ECU messages be sent on a common data bus? Should entertainment systems utilize the same vehicle network or communications system as the CAN Bus?
Note: A controller area network (CAN bus) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other. It is a message-based protocol, designed originally for multiplex electrical wiring within automobiles to save on copper. The CAN bus is one of five protocols used in the on-board diagnostics (OBD)-II vehicle diagnostics standard. The OBD-II standard has been mandatory for all cars and light trucks sold in the United States since 1996. The EOBD standard has been mandatory for all petrol vehicles sold in the European Union since 2001 and all diesel vehicles since 2004.

6.7.9 Log Events
Question 13. An immutable log of events sufficient to reveal the nature of a cybersecurity attack or a successful breach should be maintained and periodically scrutinized by qualified maintenance personnel to detect trends of cyber-attack.
Panel Member: Keith Fidura
What log information do you review during forensic analysis of a suspected cybersecurity attack or breach? Is there any log information that vehicle manufactures should include to assist with forensic analysis?

6.7.10 Control Communication to Back-End Servers
Question 14. Widely accepted encryption methods should be employed in any IP-based operational communication between external servers and the vehicle. Consistent with these methods, such connections should not accept invalid certificates.
Panel Member: Joshua Poster
What are your recommendations for Back-End Server connections over the internet? Should Public Key Encryption (PKI) and/or another encryption methodology be utilized?
Note: A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).

6.7.11 Control Wireless Interfaces
Question 15. In some situations, it may be necessary to exert fine-grained control over a vehicle's connection to a cellular wireless network. Industry should plan for and design-in features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset, or all vehicles.
Panel Member: Samuel C. Hollifield
What are your recommendations on cellular wireless interfaces and connectivity?

ADDITIONAL QUESTIONS (as time permits)
Top 5 Automotive Cybersecurity Questions Every Executive Needs to Know, Kelly Stephenson 05/15/2023 (https://www.lhpes.com/blog/top-5-automotive-cybersecurity-questions-every-executive-needs-to-know)

Question 1: For an organization with a presence in both the automotive realm and in industrial applications, is it preferable for the organization to adopt one holistic cybersecurity management system that encompasses both their automotive and industrial businesses or is it more effective for their businesses to manage cybersecurity separately?

Question 2: Under the organization's common umbrella of this single cybersecurity management system, there will be different pillars for the different applications. So, from an organizational standpoint, will we then need to determine who is aligned to which pillar? And then on the local level, do we break down the tools that are to be implemented?

Question 3: Our organization is at a point where we are starting to become increasingly digital in our products. At this moment, most of our products are not digital, but this is evolving quickly. And we need to somehow strike a balance so that as we add products to our digital portfolio, we do so in a way that is cyber-secure and under the one umbrella of our CSMS. But we have to make this transition incrementally. What about our small business units? If a unit is on the threshold of migrating its product to the digital space, how is its work managed?

Question 4: There is a three-year certification requirement. Is there also an annual maintenance audit that is required in these types of situations?

Question 5: Having our engineers earn their certifications is one of the methods of compliance. Is this the most typical method of compliance, to ascertain which engineers are certified, and to document the key experts that were utilized for their training and certification?

About the Speakers: Samuel C. Hollifield is a cybersecurity research scientist at Oak Ridge National Laboratory’s Cyber Resilience and Intelligence Division. He leads transportation security projects related to the movement of nuclear and radioactive materials. His research involves developing intrusion detection applications for in-vehicle networks, creating secure packaging through advanced manufacturing, and assessing and quantifying automotive vulnerabilities.

Joshua Poster is the Intel and Analysis Operations Manager of the Auto Information Sharing and Analysis Center (Auto-ISAC). He leads the Auto-ISAC Intel & Analysis Division and is also the Vice Chair of National Council of ISACs (NCI). Previously, he was a Program Manager at the Public Transportation and Surface Transportation ISACs as well as a Sr. Analyst at Electronic Warfare Associates. He holds a Bachelor of Science in Anthropology.

Keith Fidura is a Computer Engineer IV at Battelle Memorial Institute with the Cyber Solutions Division (CSD). He is a United States Government (USG) Vehicle Subject Matter Expert (SME) who holds a Vehicle Forensic Certification. He has over 15 years of experience as a defense contractor. He has worked as a United States Army Crypto NSA detailee, Geolocation Specialist/RF Engineer, and DOMEX Instructor. He holds a Bachelor of Arts in Cyber Security.

Resources:

Automotive Threat Matrix (ATM), which is both a means to categorize vehicle attack TTPs and a library of examples of such proven TTPs that can be found here: https://atm.automotiveisac.com/home.

Additional information can be found here: https://automotiveisac.com/press-news/the-auto-isac-launches-automotive-threat-matrix-atm-tool-to-enhance-vehicle-cybersecurity-governance

Daily Research, Incident, Vulnerability & Executive News intelligence report (DRIVEN), which is free and can be requested here: https://automotiveisac.com/contact-auto-isac

ORNL-VehSec-OngoingWork.pdf
Oak Ridge National Laboratory
Transport Security Research
Secure Hijack, Intrusion, and Exploit Layered
Detector (SHIELD)
Vehicle Attack Analysis Framework (VAAF)
Continuous Driver Authentication (Go CSU!)
Fault Anomaly Detection