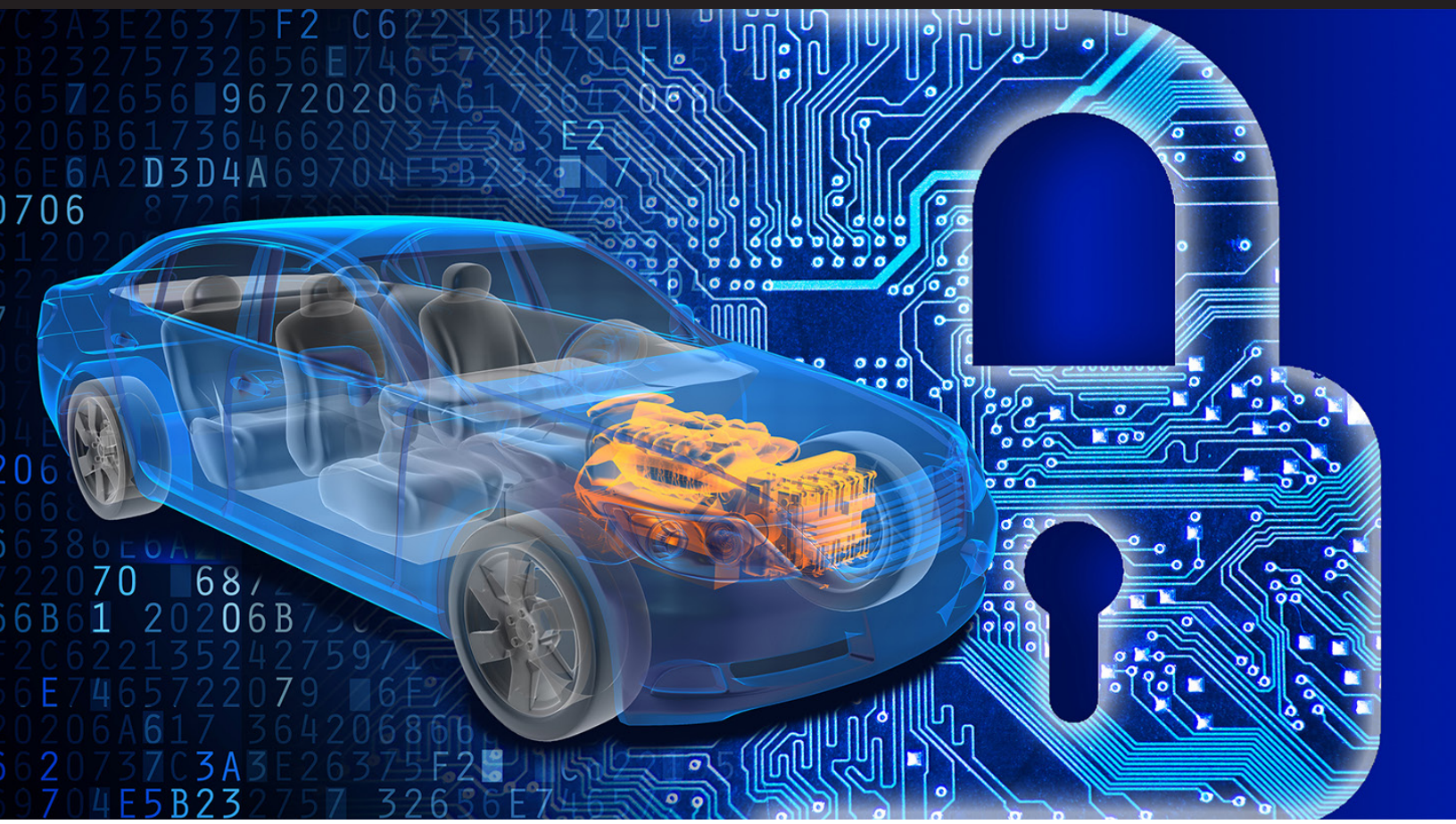
Cybersecurity Best Practices for Modern Vehicles



U.S. Department of Transportation

National Highway Traffic Safety Administration

NHTSA

Suggested APA Format Citation:

National Highway Traffic Safety Administration. (2016, October). *Cybersecurity best practices for modern vehicles*. (Report No. DOT HS 812 333). Washington, DC: Author.

Table of Contents

1. Purpose of This Document

This document describes the National Highway Traffic Safety Administration's non-binding guidance to the automotive industry for improving motor vehicle cybersecurity.

Vehicles are cyber-physical systems[1] and cybersecurity vulnerabilities could impact safety of life. Therefore, NHTSA's authority would be able to cover vehicle cybersecurity, even though it is not covered by an existing Federal Motor Vehicle Safety Standard at this time. Nevertheless, motor vehicle and motor vehicle equipment manufacturers are required by the National Traffic and Motor Vehicle Safety Act, as amended, 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.[2]

NHTSA believes that it important for the automotive industry to make vehicle cybersecurity an organizational priority. This includes proactively adopting and using available guidance such as this document and existing standards and best practices. Prioritizing vehicle cybersecurity also means establishing other internal processes and strategies to ensure that systems will be reasonably safe under expected real-world conditions, including those that may arise due to potential vehicle cybersecurity vulnerabilities.

The automotive cybersecurity environment is dynamic and is expected to change continually and, at times, rapidly. NHTSA believes that the voluntary best practices described in this document provide a solid foundation for developing a risk-based approach and important processes that can be maintained, refreshed and updated effectively over time to serve the needs of the automotive industry.

2. Scope

This document is intended to cover cybersecurity issues for all motor vehicles[3] and 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.

---

1 National Science Foundation defines cyber-physical systems (CPS) as engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components.

2 49 U.S.C. 30101 *et seq*.

3 "Motor vehicle" means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways. See 49 U.S.C. § 30102(a)(6).

3. Background

A top United States Department of Transportation priority is enhancing vehicle cybersecurity to mitigate cyber threats that could present unreasonable safety risks to the public or compromise sensitive information such as consumers' personal data.[4] On behalf of USDOT, NHTSA is actively engaged in vehicle cybersecurity research and employs a proactive and collaborative approach to protect vehicle owners from safety-related cybersecurity risks. NHTSA has been actively engaging stakeholders and working to broadly enhance cybersecurity capabilities. The following are examples of recent actions NHTSA has taken:

- Used NHTSA's enforcement authority to recall[5] almost 1.5 million vehicles in July 2015 due to cybersecurity vulnerabilities that NHTSA believed represented an unreasonable risk to safety.
- Submitted a report, *Electronic Systems Performance in Passenger Motor Vehicles*,[6]

---

4 As defined in Section 4 of the White House Consumer Privacy Bill of Rights, available at www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, the Agency views as personal data: "data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practicable matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual." Similarly, in a recent comment to the Federal Communications Commission, Federal Trade Commission (FTC) staff recommended that the definition of personally identifiable information (PII) include only data that is linked or "reasonably" linkable to an individual. https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf. Additionally, the National Institute for Standards and Technology defines personally identifiable information as "any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." McAllister, E., Grance, T., & Scarfone, K. (2010, April). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publication 800-122). Gaithersburg, MD: National Institute of Standards and Technology.

Available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf NHTSA also encourages manufacturers to review the Federal Trade Commission's educational resources on security and protecting personal information. Start with Security: A Guide for Business (June 2015), available at www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business and *Protecting Personal Information: A Guide for Business* (Nov. 2011), available at www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

5 NHTSA Recall Campaign Number 15V461000.

6 NHTSA. (2015, December). *Electronic systems performance in passenger motor vehicles: Report to Congress.* Washington, DC: Author. Available at www.nhtsa.gov/staticfiles/laws_regs/pdf/Electronic-Systems-Performance-in-Motor%20Vehicles.pdf

to Congress in January 2016 that included the results of NHTSA's examination of the need for safety standards with regard to electronic systems in passenger motor vehicles, including "security needs for those electronic components to prevent unauthorized access."

- Convened a public vehicle cybersecurity roundtable meeting[7] in January 2016 to facilitate diverse stakeholder discussion on key vehicle cybersecurity topics. Over 300 people attended this meeting. These attendees represented more than 200 unique organizations including 17 original equipment manufacturers (OEMs), 25 government entities, and 13 industry associations. During the roundtable meeting, the stakeholder groups identified actionable steps for the vehicle manufacturing industry to effectively and expeditiously address vehicle cybersecurity challenges.
- Held a follow-on meeting with other government agencies in February 2016 to discuss possibilities for collaboration among Federal partners to help the industry improve vehicle cybersecurity.
- Finalized an agreement with 18 automakers in January 2016, on proactive safety principles, including an objective to "explore and employ ways to work collaboratively in order to mitigate cyber threats that could present unreasonable safety risks."[8]
- Published the NHTSA Federal Automated Vehicles Policy[9] in September 2016, which considers vehicle cybersecurity as one of the important safety areas in the Vehicle Performance Guidance for automated vehicles.

Motor vehicle and equipment manufacturers, suppliers, and other industry stakeholders have also been active in their efforts to contribute to improving the security posture of motor vehicles. These activities include:

- Developed and published SAE J3061 Recommended Best Practice, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, in January 2016.[10]

---

7 NHTSA. (2016, January 19). Vehicle Cybersecurity Roundtable (Web page of agenda). Washington, DC: Author. Available at www.nhtsa.gov/Research/Crash+Avoidance/NHTSA+Vehicle+Cybersecurity+Roundtable

8 Department of Transportation. (2016, January 15). *Proactive safety principles*. Washington, DC: Author. Available at www.transportation.gov/briefing-room/proactive-safety-principles-2016

9 NHTSA. (2016, September). *Federal Automated Vehicles Policy: Accelerating the next revolution in roadway safety.* Washington, DC: Author. Available at www.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf

10 Society of Automotive Engineers. (2016). SAE Standard J 3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. (Web page). Warrendale, PA: Author. Available at http://standards.sae.org/wip/j3061/

- Established the Automotive Information Sharing and Analysis Center[11] (Auto ISAC) in late 2015, which became fully operational in January 2016.
- Developed a framework[12] for automotive cybersecurity best practices, which was issued in January 2016 by the two trade associations, Alliance of Automobile Manufacturers and Global Automakers. A subsequent initiative to establish a robust set of industry cybersecurity best practices built around this framework is under development by the Auto ISAC in collaboration with the trade associations targeting summer 2016.

NHTSA supports the industry activities and provides this guidance as a resource to supplement existing voluntary vehicle cybersecurity standards, principles, best practices, and lessons learned and help guide future industry efforts. This guidance is consistent with and builds upon NHTSA's prior publications on this topic.[13] [14] [15]

4. Definitions

Attack Surface is the set of interfaces (the "attack vectors") where an unauthorized user can try to enter data to or extract data from a system, or modify a system's behavior.

Attack Vector refers to the interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors

[11] McCarthy, C., Harnett, K., Carter, A., & Hatipoglu, C. (2014, October). Assessment of the information sharing and analysis center model. (Report No. DOT HS 812 076). Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print

[12] Alliance of Automobile Manufacturers. (n.a.). *Framework for automotive cybersecurity best practices*. Washington, DC: Author. Available at www.autoalliance.org/index.cfm?objectid=1E518FB0-BEC3-11E5-9500000C296BA163

[13] McCarthy, C., Harnett, K., & Carter, A. (2014, October). *A summary of cybersecurity best practices*. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print

[14] McCarthy, C., Harnett, K., & Carter, A. (2014, October). *Characterization of potential security threats in modern automobiles: A composite modeling approach*. (Report No. DOT HS 812 074). Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print

[15] McCarthy, C., & Harnett, K. (2014, October). *National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles* (Report No. DOT HS 812 073). Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print

enable attackers to exploit system vulnerabilities, including the human element.

Automotive refers to "of, relating to, or concerned with motor vehicles in general."

Binary image or **firmware image** refers to the sequence of bytes that comprises the software, both code and data, running on vehicle electronics.

Controller Area Network (CAN) is dominant serial communication network protocol used for intra-vehicle communication.

Debug is the activity of discovering errors or undesirable actions within computer code.

Digital signing is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

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.

Exploit refers to an action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software and/or hardware. An example of an exploit would be using a diagnostic port vulnerability to take advantage of a buffer overflow that allows access over Internet Protocol (IP) networks.

Firmware refers to the software code and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs (I/O) to execute those functions. Firmware may take a variety of different forms. For example, in some cases "firmware" may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled code.

Incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform through the use of an exploit.

Public Key Infrastructure refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Telematics refers to the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management.

Vulnerability is a weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an ECU is a vulnerability.

5. General Cybersecurity Guidance

5.1 Layered Approach

NHTSA is focusing 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.[16]

A layered approach to vehicle cybersecurity reduces the probability of an attack's success and mitigates the ramifications of a potential unauthorized access.

The automotive industry should follow the National Institute of Standards and Technology's documented Cybersecurity Framework,[17] which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles.

This approach should:

- Be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
- Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- Design-in methods and measures to facilitate rapid recovery from incidents when they occur; and
- Institutionalize methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in the Auto ISAC.

---

[16] NHTSA. (n.a.). *NHTSA and Vehicle Cybersecurity*. Washington, DC: Author. Available at www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2015/NHTSA-VehicleCybersecurity_07212015.pdf

[17] National Institute of Standards and Technology. (2014, February 12). Framework for Improving Critical Infrastructure Cybersecurity PowerPoint presentation). Washington, DC: Author. Available at www.nist.gov/sites/default/files/documents/cyberframework/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf

5.2 Information Technology Security Controls

NHTSA recommends that the automotive industry review and consider the information technology (IT) security suite of industry standards, such as the ISO 27000 series standards, and other best practices, such as the Center for Internet Security's (CIS) "Critical Security Controls for Effective Cyber Defense (CIS CSC),[18] which are broadly used in a number of other sectors, such as the Financial Sector, Energy, Communications, and Information Technology.[19]

Because these standards and controls are designed primarily for IT networks and network services, they are directly applicable to, and should be considered and used, to improve the cybersecurity of IT infrastructures for the vehicle controller development, dealer and service environments, and the supply-chain as they are applicable.

In particular, the CIS CSC enumerates 20 high-priority areas for cybersecurity protections based on actual attack data pulled from a variety of threat sources, primarily against IT networks. The CIS CSC discusses the internet, private computer networks, and the connections between them, rather than automotive networks and devices, which can present different risks. However, most of the controls within the CIS CSC framework may be adopted for use in the automotive realm. For example, CIS CSC #1 suggests creating an inventory of connected devices, which, in the automotive context, would be all vehicles and vehicle equipment that have some form of connectivity to each other or to other services. While the application of many CIS CSC's can be straight-forward, automotive industry members should work out the details of interpretation and translation with their own cybersecurity teams, either through a standards-setting organization's working group or individually.

The industry should also consider the following recommended approach in the CIS CSC:

- performing cybersecurity gap assessment,
- developing implementation roadmaps,
- effectively and systematically executing cybersecurity plans,
- integrating controls into vehicle systems and business operations, and
- reporting and monitoring progress through iterative cycles.

---

[18] Center for Internet Security. (2015, October 15). *Critical Security Controls for Effective Cyber Defense* (Web page). Arlington, VA: Author. Available at www.cisecurity.org/critical-controls.cfm

[19] As an example, the Federal Reserve uses CIS's Critical Security Controls as a framework in internal audits. *See* www.cisecurity.org/critical-controls/documents/Manage%20Cybersecurity%20Risk%20with%20the%20Critical%20Security%20Controls_12.2.2014.pdf

6. Automotive Industry Cybersecurity Guidance

6.1 Vehicle Development Process With Explicit Cybersecurity Considerations

The automotive industry should follow a robust product development process based on a systems-engineering approach with the goal of designing systems free of unreasonable safety risks including those from potential cybersecurity threats and vulnerabilities. Companies should make cybersecurity a priority by using a systematic and ongoing process to evaluate risks. This process should give explicit considerations to privacy and cybersecurity risks through the entire life-cycle of the vehicle. The life-cycle of a vehicle includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning. Safety of vehicle occupants and other road users should be of primary consideration when assessing risks.

The automotive industry should use guidance, best practices, and design principles based on or published by NIST, NHTSA, industry associations, Auto ISAC, and recognized standards-setting bodies. For example, industry should consider SAE International's J3061 Recommended Practice Cybersecurity *Guidebook for Cyber-Physical Vehicle Systems*[20] for adoption.

The process with inherent cybersecurity considerations should include a safety risk assessment step, which is appropriate for the full life cycle of the vehicle. Once risks have been prioritized, the automotive industry should develop layers of protection which are appropriate for the identified risks.

In addition to identifying risks and analyzing potential threats, the automotive industry should establish rapid detection and remediation capabilities. If a cyber-attack is detected, the safety risk to vehicle occupants and surrounding road users should be mitigated and the vehicle should be transitioned to a reasonable risk state. The automotive industry should also collect information on any potential attack. This information may be analyzed and shared with industry through the Auto ISAC.

The automotive industry should fully document any actions, changes, design choices, and analyses. The associated testing data should be traceable within a robust document version control system.

6.2 Leadership Priority on Product Cybersecurity

It is essential for the automotive industry to create corporate priorities and foster a culture that is prepared and able to handle increasing cybersecurity challenges.

[20] SAE J3061, January 2016, available at http://standards.sae.org/wip/j3061/.

Along this line, NHTSA recommends that companies developing or integrating safety-critical vehicle systems prioritize vehicle cybersecurity and demonstrate management commitment to doing so with the following actions:

- Allocating dedicated resources within the organization focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and vulnerabilities;
- Facilitating seamless and direct communication channels through organizational ranks related to product cybersecurity matters; and
- Enabling an independent voice for vehicle cybersecurity related considerations within the vehicle safety design process.

For example, companies could implement these actions by appointing a high-level corporate officer exclusively and directly responsible for product cybersecurity and providing this executive with appropriate staff, authority, and resources.

A top-down emphasis on product cybersecurity demonstrates the seriousness of the organization in managing cybersecurity risks. This emphasis provides a cybersecurity-oriented leadership within the organization, and it enables a proactive cybersecurity culture to develop. In addition, it causes the product development cycle to consider cybersecurity protections early in the design phases.

6.3 Information Sharing

Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing strongly encourages the development and formation of industry-specific Information Sharing and Analysis Organizations and calls on private companies, nonprofit organizations, executive departments, agencies, and other entities to "share information related to cybersecurity risks and incidents and collaborate in as close to real time as possible."[21]

In late 2014 NHTSA began encouraging the industry[22] to create the Auto ISAC.[23] The automotive industry established the Auto ISAC in late 2015 and it became fully operational on January 19, 2016. While a large number of motor vehicle and equipment manufacturers are now involved in the Auto ISAC, the agency continues to encourage all members of the vehicle manufacturing industry to participate in it, and NHTSA also

[21] Executive Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing, 80 FR 9347 (Feb. 13, 2015). Available at www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing

[22] NHTSA Report to Congress, 2015.

[23] McCarthy, Harnett, Carter, & Hatipoglu, 2014.

encourages the Auto ISAC to expand its membership domain to include suppliers and other vehicle segments.

6.4 Vulnerability Reporting/Disclosure Policy

NHTSA supports additional mechanisms for information sharing, such as a vulnerability reporting/disclosure program. These have been effective in other sectors and would likely benefit the motor vehicle industry. Automotive industry members should consider creating their own vulnerability reporting/disclosure policies, or adopting policies used in other sectors or in technical standards. Such policies would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to organizations that manufacture and design vehicle systems.

A vulnerability reporting/disclosure policy should inform cybersecurity researchers how a company plans to interact with them. In general, the company's expectations for the relationship between companies and cybersecurity researchers should be described in detail and publicly available.

6.5 Vulnerability / Exploit / Incident Response Process

The automotive industry should have a documented process for responding to incidents, vulnerabilities, and exploits. This process should cover impact assessment, containment, recovery and remediation actions, and the associated testing.

This process should clearly outline roles and responsibilities for each responsible group within the organization and also specify any requirements for internal and external coordination. The process should be designed in a manner that ensures rapid response without sole dependence on any single person.

The automotive industry should define metrics to periodically assess the effectiveness of their response process. In addition, companies should document details of each identified and reported vulnerability, exploit, or incident. These documents should include information which extends from onset to disposition with sufficient granularity to enable response assessment.

The response process should report all incidents, exploits, and vulnerabilities to the Auto ISAC as soon as possible. This is recommended for companies who may not yet be a member of Auto ISAC as well. Any incidents should also be reported to US-CERT in accordance with the US-CERT Federal Incident Notification Guidelines.[24] Additionally,

[24] US-CERT Federal Incident Notification Guidelines. Available at www.us-cert.gov/incident-notification-guidelines

they may be reported to the industrial control systems CERT.[25]

Finally, industry members should periodically run response capabilities exercises[26] to test the effectiveness of their disclosure policy operations and their internal response processes.

6.6 Self-Auditing

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. Such documentation may include the following:

- risk assessments,
- penetration test results,
- organizational decisions.

Further, such documents should be retained through the expected life span of the associated product. Persistent documents (such as cybersecurity requirements) should follow a robust version control protocol, and should be revised regularly as new information, data, and research results become available.

6.6.1 Risk Assessment

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.

At a minimum, organizations should consider cybersecurity risks to safety-critical vehicle control functions and PII. For example, a risk assessment process and the associated documentation should consider the following questions as suggested in the following modification of the documented CIS approach:[27]

- What are the functions?
- What are the implications if they were compromised?

25 https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy

26 A cybersecurity capability exercise is a simulated attack and response exercise.

27 SANS Institute. (2002). *An Overview of Threat and Risk Assessment.* Fredericksburg, VA: Author. Available at www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

- What are the potential safety hazards that could be exposed by these vulnerabilities?
- What is the safety risk to society and the value risk to the organization?
- What can be done to minimize exposure to the potential loss or damage?
- What design decisions could be made with respect to the risk assessment process?
- Who/what are the threats and vulnerabilities?

A risk assessment document should minimally cover internal vehicle networks, external wireless networks, and any interface an ECU presents to the world.

6.6.2 Penetration Testing and Documentation

The automotive industry should consider extensive product cybersecurity testing to include using penetration tests. These 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.

All reports which result from these penetration tests should be maintained as part of the body of internal documentation associated with the cybersecurity approach. Documentation should identify the testers, their qualifications, and their recommendations.

These penetration testing reports should also document the disposition of detected cybersecurity vulnerabilities. If a vulnerability is fixed, the details of the fix need to be documented. If a vulnerability is not addressed, the reasoning behind the acceptability of the underlying risk should be documented as well. In addition, the penetration testing reports should note the authorized approving authority for each vulnerability.

6.6.3 Self-Review

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[28] on the state of their cybersecurity practices. These annual reports could discuss the current state of implemented cybersecurity controls, findings from self-auditing activities, and the state of records maintenance. Information concerning the corporate structure related to cybersecurity and all other cybersecurity

[28] An example of an annual report from the financial industry is available at www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

efforts would be valuable information for stakeholders and consumers.

6.7 Fundamental Vehicle Cybersecurity Protections

The following recommendations are based on what NHTSA has learned through its internal applied research as well as from stakeholder experiences shared with NHTSA. These recommendations do not form an exhaustive list of actions necessary for securing automotive computing systems, and all items may not be applicable in each case. These protections serve as a small subset of potential actions which can move the motor vehicle industry towards a more cyber-aware posture.

6.7.1 Limit Developer/Debugging Access in Production Devices

Software developers have considerable access to ECUs. Such ECU access might be facilitated by an open debugging port, or through a serial console. However, developer access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units.

If continued developer access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users. Physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.

6.7.2 Control Keys

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.

6.7.3 Control Vehicle Maintenance Diagnostic Access

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[29] could be restricted to operate only at low speeds. In addition, this diagnostic operation might not disable all brakes at the same time, and/or it might limit the duration of such diagnostic control action.

6.7.4 Control Access to Firmware

In many cases, 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.

Many platforms may be able to support whole disk encryption of external non-volatile media. In this case, encryption should be considered as a useful tool in preventing the unauthorized recovery and analysis of firmware.

Firmware binary images may also be obtained from a firmware updating process. Organizations should reduce any opportunities for a third party to obtain unencrypted firmware during software updates.

6.7.5 Limit Ability to Modify Firmware

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. In addition, firmware updating systems which employ signing techniques could prevent the installation of a damaging software update that did not originate from an authorized motor vehicle or equipment manufacturer.

---

[29] Valasek., C., & Miller, C. (2014). Adventures in Automotive Networks and Control Units Seattle: IOActive, Inc. Available at www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

6.7.6 Control Proliferation of Network Ports, Protocols and Services

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.

6.7.7 Use Segmentation and Isolation techniques in Vehicle Architecture Design

Privilege separation with boundary controls is important to improving security of systems.[30] 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.

6.7.8 Control Internal Vehicle Communications

Critical safety messages are those that could directly[31] or indirectly[32] 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.

If critical safety information must be passed across a communication bus, this information should reside on communication buses segmented from any vehicle ECUs with external network interfaces. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks.

Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication scheme to limit the possibility of message spoofing.

---

30 Some strategies are described in *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, Department of Homeland Security, September, 2016. Available at https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

31 For example, a control command message sent to a traction control actuator; if spoofed, this could apply the vehicle's brakes without a driver's or a legitimate vehicular safety system's intent.

32 For example, a vehicle speed estimate message; if spoofed, this could make the distributed vehicle controllers relying on that information to misunderstand the moving state of the vehicle (e.g., stationary versus moving).

6.7.9 Log Events

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.

6.7.10 Control Communication to Back-End Servers

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.

6.7.11 Control Wireless Interfaces

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.

7. Education

NHTSA believes that an educated workforce is crucial to improving the cybersecurity posture of motor vehicles. The agency's philosophy is that cybersecurity educational activities should not be limited to the current workforce or technical individuals, but should also enrich the future workforce and non-technical individuals. NHTSA supports educational competitions that include cybersecurity elements such as the SAE/Battelle Cyber Auto Challenge, NIST's National Initiative for Cybersecurity Education (NICE) program called out in the 2014 Cyber Enhancement Act (PL113-274, Title IV),[33] and the Enhanced Safety of Vehicles (ESV) Student Design Competition. NHTSA also encourages universities that are the foundation of the future workforce to develop curriculums that target fostering skillsets useful across a range of practical security applications, including the field of vehicle cybersecurity. NHTSA suggests that manufacturers, suppliers, and other stakeholders should work together with NHTSA to help support these educational efforts and more.

8. Aftermarket Devices

The automotive industry should consider that consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., cell phones) onto cars and connect them with vehicle systems through the interfaces that manufacturers

[33] Csrc.nist.gov/nice

provide (Bluetooth, USB, OBD-II port, etc.). The automotive industry should consider the incremental risks that could be presented by these devices and provide reasonable protections.

Aftermarket device manufacturers should consider that their devices are interfaced with cyber-physical systems and they could impact safety-of-life. Even though the primary purpose of the system may not be safety-related (e.g., telematics device collecting fleet operational data), if not properly protected, they could be used as proxy to influence the safety-critical system behavior on vehicles. Aftermarket devices could be also brought on to all ages and types of vehicles with varying levels of cybersecurity protections on the vehicle side of the interface. Therefore, these devices should include strong cybersecurity protections on the units since they could impact the safety of vehicles regardless of their intended primary function.

9. Serviceability

The automotive industry should also consider the serviceability of vehicle components and systems by individuals and third parties. The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services.

DOT HS 812 333
October 2016

U.S. Department of Transportation
National Highway Traffic Safety Administration

NHTSA

12707-101416-v4