NHTSA and Vehicle Cybersecurity

NHTSA

Safer drivers. Safer cars. Safer roads.

Introduction

In 2015 there were 35,092 people killed on the Nation's roadways. The National Highway Traffic Safety Administration estimates that, sadly, 94 percent of highway crashes result from human error.[1] Today's electronics, sensors, and computing power enable the deployment of safety technologies, such as forward-collision warning, automatic emergency braking, vehicle-to-vehicle technologies, and in the future highly automated vehicles, which will help drivers avoid crashes in the first place. Given the potential of these innovations, NHTSA is looking at all of our tools, as well as exploring new ones, that can be used to deploy these technologies in safe and effective ways, taking steps to address the new challenges they pose—particularly with respect to cybersecurity.

Many people are familiar with the concept of cybersecurity. Over the last few decades our lives have been revolutionized by the rapid connectivity made possible by computers, the internet, satellites and other technologies. As these systems became integral to our daily lives, so too did the potential for attacks to those same systems. Cybersecurity rose out of necessity to protect these vital systems and the information contained within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from malicious attacks, unauthorized access, damage, or anything else that might interfere with safety functions.

For these reasons NHTSA appreciates the importance of vehicle cybersecurity. In exploring the potential of connected vehicles and other advanced technologies, NHTSA remained aware that cybersecurity would be essential to the public acceptance of vehicle systems and to the safety technology they governed.

To ensure a robust cybersecurity environment for these dynamic new technologies, NHTSA adopted a layered research approach, modified its organizational structure, and is continually developing vital partnerships, encouraging members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United States. NHTSA's goal is to stay ahead of potential vehicle cybersecurity challenges, and to continue seeking ways to address or avoid them altogether.

---

[1] Singh, S. (2015, February). *Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey*. (Traffic Safety Facts Crash•Stats. Report No. DOT HS 812 115). Washington, DC: National Highway Traffic Safety Administration. Available at www-nrd.nhtsa.dot.gov/Pubs/812115.pdf

What Is NHTSA Doing?

NHTSA's Vehicle Cybersecurity Research Approach

To help develop a comprehensive approach to address cybersecurity challenges in automobiles, NHTSA consulted other government agencies, vehicle manufacturers, suppliers, and the public. The approach covers various safety-critical applications deployed on current vehicles, as well as those envisioned for future vehicles that may feature more advanced forms of automation and connectivity. NHTSA's multilayered approach to cybersecurity has the following goals:

1. Expand and share automotive cybersecurity knowledge base to better establish comprehensive research plans and develop enabling tools for applied research in this area;

2. Help the automotive industry implementation effective, industry-based best practices and voluntary standards for cybersecurity and cybersecurity information-sharing forums;

3. Foster the development of new system solutions for automotive cybersecurity;

4. Determine the feasibility of developing minimum performance requirements for automotive cybersecurity; and

5. Gather foundational research data and facts to inform potential future Federal policy and regulatory activities.

Layers of Protection

As mentioned, NHTSA's research program takes a layered approach to cybersecurity for automobiles. What this means is that we assume all entry points into the vehicle, both wireless and physical, such as Wi-Fi, infotainment, the OBD-II port, and other points of potential access to vehicle electronics, could be potentially vulnerable. This way, NHTSA focuses on solutions to harden the vehicle's electrical architecture against potential attacks and to ensure vehicle systems take appropriate safe steps even when an attack may be successful. A layered approach to vehicle cybersecurity reduces the probability of success for an attack and mitigates the potential ramifications of a successful intrusion.

At the vehicle level this approach includes the following four main areas:

- **Protective/preventive measures and techniques:** These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack.

- **Real-time intrusion (hacking) detection measures**: These measures continually monitor signatures of potential intrusions in the electronic system architecture.

- **Real-time response methods**: These measures mitigate the potential adverse effects of a successful hack, preserving the driver's ability to control the vehicle.

- **Assessment of solutions**: This involves methods such as information sharing and analysis of a hack by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders (such as through an Information Sharing Forum). This layer ensures that once a potential vulnerability or a hacking technique is identified, information about the issue and potential solutions are quickly shared with other stakeholders.

Current Research

NHTSA's current research projects related to vehicle cybersecurity include:

- **Anomaly-based intrusion detection systems research:** Researching metrics and objective test methods to assess effectiveness of such solutions. Targeting conclusion in 2016.

- **Research on cybersecurity of firmware updates:** Researching cybersecurity of automotive electronics update mechanisms through physical and over-the-air means. Targeting conclusion in 2016.

- **Research on cybersecurity considerations for heavy vehicles:** Researching similarities and differences between passenger cars and larger vehicles from a cybersecurity considerations standpoint. Targeting conclusion in 2016.

- **Research on reference parser development for V2V communication interfaces:** Targeting to develop formally verified message parsers for V2V communication interfaces with mathematical proof. Expected to be concluded in 2017.

- **In-house cybersecurity research at the Vehicle Research and Test Center (VRTC) in East Liberty, Ohio:** This research explores the cybersecurity risks of today's vehicle electronic architecture and aims to establish principles, guidelines and/or requirements that could improve the cybersecurity posture of passenger vehicles through applied research. Targeted conclusion in 2016. NHTSA plans additional research in 2017 that continues the activities from 2016 that apply to technologies forecast for use in future vehicles.

- **Trusted vehicle-to-vehicle and vehicle-to-infrastructure communications:** This project explored approaches, developed a design,

and is implementing a public key infrastructure-based system that provides certificates that can be used by vehicles and infrastructure systems to sign and validate communication messages between each other. Targeted conclusion in 2017.

NHTSA's completed research reports are available on its website.[2] Other documents related to Vehicle Cybersecurity can also be accessed at Docket NHTSA-2014-0071.[3]

Organizational Changes

In 2012 NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity. NHTSA established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems. More recently, NHTSA expanded its research and testing capabilities in vehicle electronics at the VRTC. As resources permit, NHTSA is executing research in three main areas:

- automotive cybersecurity,
- electronics reliability (including functional safety[4] and software integrity), and
- automated vehicles.

Establishment of Electronics Council

NHTSA also established an internal agency working group, the Electronics Council, responsible for collaborating more broadly on issues related to vehicle electronics including cybersecurity across the entire NHTSA organization with particular focus on the Research, Rulemaking, Data, Enforcement, and Chief Counsel Offices.

Recent Activities

Report to Congress on Automotive Electronics

In response to a requirement in the Moving Ahead for Progress in the 21st Century Act (MAP-21),[5] NHTSA examined 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." In January 2016 NHTSA submitted its findings[6] to Congress, which highlighted that, due to the highly dynamic nature of

---

2 NHTSA. (n.a.). Office of Crash Avoidance Research Technical Publications (Web page). Washington, DC: Author. Available at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications

3 Regulations.gov. (n.a.). Automotive Cybersecurity Topics and Publications (Web page for Docket ID: NHTSA-2014-0071). Accessed from the web page at www.regulations.gov/#!docketDetail;D=NHTSA-2014-0071

4 "Functional safety is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the fight consequence of the hazardous event." Source: International Electrotechnical Commission web page at www.iec.ch/functionalsafety/explained/

5 Moving Ahead for Progress in the 21st Century Act, Public Law 112-141 (Jul. 6, 2012), § 31402.

6 NHTSA. (2015, December). Electronic Systems Performance in Passenger Motor Vehicles: Report to

cybersecurity risks and threats, developing cybersecurity guidelines could be an appropriate next step. The agency also identified priority near-term research needs which, for example, pending the availability of resources, would explore data elements and data recording trigger points for capturing record-of-data in cases of suspected electronics malfunctions and cybersecurity hacking attempts.

Facilitating Discussion

In January 2016, NHTSA convened a public vehicle cybersecurity roundtable meeting[7] attended by vehicle manufacturers, suppliers, technology companies, industry experts, security researchers, technology leaders in related industries, and other government agencies to facilitate discussion on key vehicle cybersecurity topics including, for example, the best ways to capitalize efforts from other sectors while applying them to distinct aspects of auto industry. This meeting was well attended with over 300 individuals in the audience. There were representatives from over 200 unique organizations including 17 OEMs, 25 government entities, and 13 industry organizations. The day was structured around four panels which featured 35 experts. During this January 2016 meeting, stakeholder groups identified actionable steps that the auto industry could take to effectively and expeditiously address the vehicle cybersecurity challenges.

As a follow-up to the industry roundtable event, NHTSA also held a half-day meeting with other government agencies in February 2016 to discuss possibilities for collaboration among Federal partners to help the industry move forward on vehicle cybersecurity more expeditiously. Based on the input received from the broader stakeholder groups, the agency has been developing a robust set of core best practices and encouraging the industry to developed more detailed guidance.

Vehicle Cybersecurity Information Sharing Forum

On July 14, 2014, NHTSA challenged the automotive industry to form an Information Sharing and Analysis Center (ISAC) to help the industry proactively and uniformly address cybersecurity threats. ISACs were created as a result of Presidential Decision Directive 63,[8] which sought ways for public and private sector partners to share information about physical and cyber threats to critical infrastructure. Today, ISACs are used in over a dozen critical infrastructure areas, such as surface transportation, finance, and energy. NHTSA believes an automotive industry ISAC is a critical piece of vehicle cybersecurity infrastructure, as manufacturers and suppliers are in the best position to identify weaknesses in their own products. As vehicle cybersecurity and the role of an automotive ISAC mature, identification of those weaknesses can be made during the engineering phases, so they can be corrected earlier in the process. The auto industry announced the formation of an ISAC in July 2015 and commenced full operation by January 2016.

Congress (Unnumbered report). Washington, DC: Author. Available at www.nhtsa.gov/staticfiles/laws_regs/pdf/Electronic-Systems-Performance-in-Motor%20Vehicles.pdf

[7] www.nhtsa.gov/Research/Crash+Avoidance/NHTSA+Vehicle+Cybersecurity+Roundtable

[8] 63 FR 41804 - Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, Federal Register Volume 63, Issue 150 (August 5, 1998).

Agreement on Proactive Safety Principles

NHTSA finalized a historic agreement with 18 automakers in January 2016, on proactive safety principles. The signatories agreed to work together to develop a collaborative, data-driven, science-based process, consistent with the law, to advance safety objectives including, mitigating "cyber threats that could present unreasonable safety risks."[9] More specifically, the section on "enhancing automotive cybersecurity" of this agreement states:

Objective: Explore and employ ways to work collaboratively in order to mitigate those cyber threats that could present *unreasonable safety risks.*

Implementation:

- *Develop suggested best practices that reflect lessons learned within and outside of the auto industry to foster enhanced cyber resiliency and effective remediation.*
- *Develop appropriate means for engaging with cybersecurity researchers as an additional tool for cyber threat identification and remedy. One example would be by working with TRB.*
- *Support and evolve the auto industry's information sharing and analysis center (Auto–ISAC) through the following*
    - *Promote continued voluntary sharing of cybersecurity threat and vulnerability information through the Auto–ISAC and its members.*
    - *Enhance the Auto–ISAC to include sharing of common/generic countermeasures used to address common threats and vulnerabilities.*
    - *Expand the membership of the Auto–ISAC to include members of the automotive supplier community and other participants in the connected vehicle ecosystem.*

As part of this commitment, the Alliance of Automobile Manufacturers and Global Automakers developed a framework for automotive cybersecurity best practices, which was issued in January 2016. The Automotive ISAC, in collaboration with these trade associations, is establishing a robust set of industry cybersecurity best practices built around this framework.

[9] U.S. Department of Transportation. (n.a.). Proactive Safety Principles 2016 (Web page). Washington, DC: Author. Available at www.transportation.gov/briefing-room/proactive-safety-principles-2016

Enforcement Action

In July 2015 security researchers demonstrated the remote exploitation possibility[10] with a passenger vehicle platform. NHTSA worked closely with the affected OEM to identify and assess the risks and remedial solutions. In this case, NHTSA determined that the vulnerability represented an unreasonable risk to safety, which resulted in the affected OEM issuing a prompt voluntary recall (NHTSA Recall Campaign Number 15V461000) involving up to 1.4 million vehicles. This event and subsequent actions were first of their kind and highlight the importance of NHTSA's position to maintain particular vigilance for potential cybersecurity issues that could adversely impact safety.

Vehicle Cybersecurity Best Practices by NHTSA

NHTSA has developed a core set of best practices for the automotive industry for improving motor vehicle cybersecurity. This document is intended for all individuals and organizations manufacturing and designing vehicle systems and software and is intended for all motor vehicles. This document is consistent with industry-based best practices, such as SAE J3061 Recommended Best Practice, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, and the set of industry cybersecurity best practices being developed by the Auto ISAC in collaboration with the trade associations. NHTSA's best practices highlight highest priority areas that need attention as identified by the agency in collaboration with Federal and industry stakeholders.

Vehicle Performance Guidance for Automated Vehicles

In September 2016 NHTSA published Federal Automated Vehicles Policy,[11] which includes Vehicle Performance Guidance for Automated Vehicles.[12] This guidance is built on a framework that identifies vehicle cybersecurity as an important safety area for the safe design, development and testing of highly automated vehicles.

Who Is NHTSA Working With?

NHTSA maintains significant interactions with vehicle manufacturers, other government agencies, automotive suppliers, and the security research community regarding potential cyber threats and vulnerabilities. Some interactions involve the security community conducting research on behalf of the agency while other interactions are information exchanges.

---

[10] Miller, C., & Valasek, C. (2015). Remote Exploitation of an Unaltered Passenger Vehicle (BlackHat Briefings). London: UBM plc.

[11] NHTSA. (2016, September). Federal automated vehicles policy: Accelerating the next revolution in roadway safety (Unnumbered report). Washington, DC: Author. Available at www.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf

[12] *Id.* pp. 11-36

Other Partnerships

Below are a few examples of NHTSA's partnerships on cybersecurity issues.

- NHTSA holds detailed meetings with technical leads at OEMs and Tier 1 suppliers regarding their cybersecurity initiatives, processes, risk assessment and product/process plans to design security into their products.

- NHTSA interacts with researchers and transportation system operators from industry, the public sector and academia through the activities of the Cyber Security Subcommittee of the National Academy of Science's Transportation Research Board. These activities include regular sharing of information on research related to vulnerabilities and mitigation measures in all modes of transportation, and development of guidance for transportation system operators.

- NHTSA meets with suppliers in the aviation, space, and defense industries to learn about their approaches to secure design for safety-critical embedded control systems, as well as evolutions that transpired in those industries over time.

- NHTSA is a regular participant in various widely attended security conferences and events such as DefCon, Blackhat, Embedded Security in Cars, the Defense Advanced Research Projects Agency (DARPA)'s High Assurance Cyber Military Systems (HACMS), the National Science Foundation's Principal Investigators conferences, and the CyberAuto Challenge. NHTSA holds discussions with white-hat hackers who have demonstrated experience in this domain. In addition, NHTSA co-organizes the biannual Enhanced Safety of Vehicles conference and the annual SAE government-industry meetings that address cybersecurity among other topics.

- NHTSA serves as a liaison to SAE International's Vehicle Electrical Security System committee and participates in its meetings. In January 2016 SAE International issued a new surface vehicle recommended practice, J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. NHTSA has been examining this document and anticipates providing constructive feedback to SAE International as they commence work on the subsequent revision of J3061.

- NHTSA works closely with other Federal organizations with interests in automotive cybersecurity. For instance, we have been interacting with DARPA and its HACMS program leaders and are pursuing a research project to develop a secure reference parser for V2V communication interfaces based on DARPA's extensive research and experience in this area. We closely collaborate with the U.S. Department of Homeland Security's Science and

Technology Directorate, which awarded three vehicle cybersecurity related projects[13] [14] [15] in late 2015. This close coordination allowed initiating complementary projects on the topic of vehicle firmware security. We also work with NIST and the U.S. Army Tank Automotive Research, Development, and Engineering Center in different capacities to leverage synergies, avoid redundant emphasis, and share knowledge and expertise.

Supporting V2V and V2I Deployment

For the past several years, with leadership from the Office of the Secretary, NHTSA, FHWA, ITS JPO, vehicle manufactures, automotive suppliers, security experts, and other government agencies have been developing dedicated short-range communications radio technology and the associated architecture and protocols to support trusted vehicle-to-vehicle and vehicle-to-infrastructure communications. We are finalizing the implementation of the next generation Security Credential Management Systems and have research plans to conduct full-scale vulnerability testing and to address any security issues that emerge from that testing.

Conclusion

In the constantly changing environment of technology and cybersecurity, no single or static approach is sufficient. Those involved must keep moving, adapting, and improving. To that end, NHTSA will continue to explore numerous approaches, including internal research, independent testing, analysis conducted by the agency, and communication. NHTSA cannot do this alone, but neither can vehicle manufacturers or suppliers. Our efforts will need to be collective, collaborative, and complete. As Secretary Foxx said on May 13, 2015, "The Department wants to speed the Nation toward an era when vehicle safety is not just about surviving crashes; it is about avoiding them. Connected, automated vehicles that can sense the environment around them and communicate with other vehicles and with infrastructure have the potential to revolutionize road safety and save thousands of lives." To do this, cybersecurity must be an integral part of vehicle engineering, manufacturing, and enforcement. NHTSA already is laying the groundwork needed for the road ahead, and looks forward to working with Congress, manufacturers, suppliers, and the American public in our exciting transportation future.

---

[13] Department of Homeland Security (2015, October 20). DHS S&T Awards New York University $1.4M for Automotive Cyber Security Research (Web page press release). Washington, DC: Author. Available at www.dhs.gov/science-and-technology/news/2015/10/20/st-awards-nyu-14m-automotive-cyber-security-research

[14] DHS. (2015, October 29). DHS S&T Awards the University of Michigan $1.2M for Automotive Cyber Security Research (Web page press release). Washington, DC: Author. Available at www.dhs.gov/science-and-technology/news/2015/10/29/st-awards-univ-michigan-12m-automotive-cyber-security

[15] DHS. (2015, October 29). DHS S&T Awards HRL Laboratories $2.5M for Automotive Cyber Security Research (Web page press release). Washington, DC: Author. Available at www.dhs.gov/science-and-technology/news/2015/10/29/st-awards-hrl-labs-25m-automotive-cyber-security-research