NHTSA Cybersecurity Research

John Martin
Arthur Carter
National Highway Traffic Safety Administration
United States

Paper Number 17-0082

Abstract

New safety technologies which rely on computers, algorithms and sensors have the potential to sharply decrease the number of motor vehicle fatalities. However, recent public demonstrations of hacking on vehicle computer systems imply that, if vehicle cybersecurity is not proactively addressed, it could compromise public trust in these systems and the technology-driven safety transformation we all want to achieve. In response, NHTSA is pursuing several avenues of cybersecurity research which will help define the scope of cybersecurity challenges and inform on potential methods of remediation. NHTSA's cybersecurity research will also provide operational expertise in testing modern software-defined vehicles.

NHTSA is funding several research projects in addition to developing in-house cybersecurity expertise. These cybersecurity research projects include:
• the evaluation of anomaly detection systems
• the identification of cybersecurity issues in heavy trucks
• a look into firmware updates
• the development of a formally verified V2V basic safety message parser which can help guarantee the correctness of incoming basic safety messages

INTRODUCTION

The world's network infrastructure connects an estimated 6.4 billion devices. This number represents an estimated 30 percent increase from 2015 (Gartner 2015). These connected devices are not necessarily entirely phones and computers. Increasingly, diverse consumer devices such as thermostats, smoke detectors and cameras are connected.

One can see that more and more general consumer devices are connected to network infrastructure. Vehicles are no exception. As this level of connectedness increases, the potential for bad actors obtaining access and control of vehicle computing resources increases as well. For this reason, NHTSA has recently made efforts to understand and address some of these growing concerns.

This paper will discuss some of the ways in which NHTSA has engaged with the cybersecurity community on vehicle cybersecurity issues.

While NHTSA is not aware of any real-world safety related vehicle cybersecurity incidents, security researchers have demonstrated that scenarios involving wireless access to certain vehicles are possible (Miller and Valasek, Remote Exploitation of an Unaltered Passenger Vehicle 2015).

Computer Control of Vehicles

In 2015 there were 35,200 traffic fatalities (US DOT 2016). This total represents a 7.7% increase over 2014 (US DOT 2016). Since 94% of crashes are caused by human error (Singh 2015), automated

vehicle techniques hold the promise of greatly reducing traffic fatalities. However, allowing computers increased control authority brings with it the problem of unauthorized cyber access potentially compromising the enhanced safety which automotive control computers can provide.

The risk of cyberattacks in automobiles resembles the issues posed by connected consumer devices in general. Our society sees the potential for great benefits, but cybersecurity concerns need to be addressed for the technology-driven transformation to be realized.

Road vehicles occupy a unique place among consumer devices by the nature of risks they pose. A typical vehicle in motion packs significant amount of kinetic energy that can cause physical harm to the surrounding traffic, in contrast to harm that can be caused by hacking into other consumer devices, such as cellular phones or smart television sets.

Recent Demonstrations of Hacking

Recent years have seen important public demonstrations of the vulnerability of automobiles to cyberattack. Modern vehicles possess internal communications networks (also called busses) which allow specific use computers called Electronic Control Units (ECUs) to communicate with one another. Theoretically, one could provide a separate communications medium for each required connection between ECUs. However, a less expensive solution in terms of cost and packaging is to implement a common, multiple access communication bus. In most vehicles this common communications bus uses a specific protocol created in the late 1980s called the "Control Area Network" or CAN bus (Robert Bosch GmbH 1991).

One of the important consequences of using a common, multiple access communications bus is that any ECU on the bus can monitor the traffic generated by any other ECU on the bus.

Also, conventional use of the CAN bus assigns a particular packet identifier number to a particular ECU. However, the CAN protocol offers no inherent authentication method to ensure that a packet possessing a particular packet ID was actually generated by a specific ECU.

An example of using the CAN bus to produce an undesirable vehicle action follows. A collision radar may use the CAN bus to announce the presence of an object to a braking system. The braking system would then apply brakes such that the vehicle does not strike the object. Since the CAN bus is a common bus designed for multiple ECUs which are not typically authenticated, the radar's target recognition communications may be spoofed or faked by another device to cause spurious braking of the automobile without the actual presence of a radar target (Miller and Valasek, Adventures in Automotive Networks and Control Units 2014).

From the perspective of an attacker, the tricky, difficult part in the above scenario lies in establishing enough control over a vehicle's network to transmit CAN packets appearing to be valid packets which originate from the collision avoidance radar. The simplest versions of the above hack assume that this control is easily obtained by physically placing a microcontroller board with a CAN bus interface on the wires which carry the vehicle's CAN bus. In many cases, this physical coupling may be conveniently obtained by using the vehicle's On-Board-Diagnostic (OBD) port which resides underneath the dashboard next to the driver's knees.

Many automobile hacking demonstrations (Checkoway, et al. 2011, Miller and Valasek, Adventures in Automotive Networks and Control Units 2014) have used CAN bus communications to affect vehicle operations. If any cyberattack acquires the capability to transmit and receive on a vehicle's CAN busses, an attacker may have the ability to put some vehicles in an unsafe state.

A notional cyberattack which relies on physical access to the target vehicle does not necessarily change the cybersecurity risk. However, if an attacker can establish a remote, wireless connection

to a vehicle's CAN bus, the cybersecurity risk increases greatly.

The CAN bus provides a ubiquitous and universal means of sharing information within the vehicle. While it certainly delivers on these highly desirable qualities, coupling CAN with recent extensive use of external wireless communications has the demonstrated potential to provide the means for an attacker to insert packets on a vehicle's CAN bus without first obtaining physical access.

NHTSA Cybersecurity Engagement

In response to both the increased use of potentially vulnerable automotive computer control techniques and recent public demonstrations of cyber vulnerabilities, NHTSA has pursued a variety of avenues of public engagement.

NHTSA has identified various vehicle cybersecurity stakeholders which include Federal partners such as Department of Homeland Security, National Institute of Standards and Technology (NIST), Defense Advanced Research Projects Agency (DARPA), industry standard setting organizations such as SAE International (SAE), and vehicle and vehicle equipment manufacturers, such as individual OEMs and suppliers as well as automotive trade associations. NHTSA also attends the Black Hat, DEFCON and ESCAR cybersecurity conferences.

In addition to regular contact with cybersecurity stakeholders, NHTSA has pursued public engagement in the following ways:

- Encouraged the formation of the Automotive Information Sharing and Analysis Center (Auto ISAC)
- Released "Proactive Safety Principles" in January 2016
- Hosted the January 2016 Cyber Roundtable discussion
- Released the document "Cybersecurity Best Practices for Modern Vehicles" guidance for public comment in October 2016

The next four sections will describe these events and publications.

Automotive Information Sharing and Analysis Center An Information Sharing and Analysis Center or "ISAC" as suggested in Presidential Policy Directive 63 (Clinton 1998) is a mechanism commonly used in other industries where cybersecurity or security in general is a shared problem which transcends the usual competitive activity.

As the name implies, information concerning cybersecurity is shared within the members of the ISAC in a manner which does not threaten disclosure of intellectual property. NHTSA encouraged the formation of an automotive ISAC which announced its formation in July 2015 and became fully operational on January 19, 2016. More information about the recently established automotive ISAC may be found on their website (Auto ISAC 2016).

Proactive Safety Principles In January 2016, NHTSA finalized a historic agreement with 18 automakers on proactive safety principles (NHTSA 2016). The signatories agree to work together to develop a collaborative, data-driven, science-based process, consistent with the law, to advance safety objectives. One of the stated objectives is to "Enhance Automotive Cybersecurity". In general, the "Proactive Safety Principles" focuses on the cooperation and information sharing techniques necessary for enhancing automotive cybersecurity. Specifically, the principles suggest:

1. Developing best practices that reflect lessons learned within and outside of the auto industry to foster enhanced cyber resiliency and effective remediation

2. Developing appropriate means for engaging with cybersecurity researchers as an additional tool for cyber threat identification and remedy

3. Supporting the evolution of the auto industry's information sharing and analysis center (Auto–ISAC) through the following:

a. Promote continued voluntary sharing of cybersecurity threat and vulnerability information through the Auto–ISAC and its members.

b. Enhance the Auto–ISAC to include sharing of common/generic countermeasures used to address common threats and vulnerabilities.

c. Expand the membership of the Auto–ISAC to include members of the automotive supplier community and other participants in the connected vehicle ecosystem.

Cyber Roundtable Discussion In January 2016, NHTSA hosted a cyber roundtable discussion of cybersecurity. The discussion consisted of 35 panelists in four panels from a variety of different general affiliations such as:

- OEMs
- Suppliers
- Federal Agencies
- Security Researchers
- Associations
- Advocates
- Technology Companies

There were over 300 people in attendance from 200 unique organizations and 25 federal groups, 17 OEMS and 13 associations.

By design, the discussion panels included a diverse set of stakeholders from independent security researchers to executives of automotive OEMs and their suppliers. The discussion was open, and the varied viewpoints expressed throughout the day provided welcome input to NHTSA's next step action items, including to the "Cybersecurity Best Practices for Modern Vehicles" document described below.

Cybersecurity Best Practices for Modern Vehicles In the fall of 2016 NHTSA issued a draft document "Cybersecurity Best Practices for Modern Vehicles" (NHTSA 2016). This document provides best practices guidance to the broader industry related to vehicle cybersecurity. This guidance includes the following key areas.

Pursue a Risk-based Approach NHTSA is particularly concerned about the potential safety ramifications of a vehicle cybersecurity issue. Safety is fundamental to NHTSA's mission, and the "Best Practices" encourages the automotive industry to appropriately assess risks and undertake actions to mitigate risks to vehicle safety-critical systems.

Leverage Existing Cybersecurity Guidance There is substantial existing guidance on cybersecurity that addresses other but relevant industries. NHTSA suggests utilizing this existing expertise by referencing sources such as:

- NIST Cybersecurity Framework (NIST 2014)
- ISO 27000 series standards (ISO 2016)
- Critical Security Controls for Effective Cyber Defense (CIS 2016)

In addition, the "Best Practices" references the recently published SAE standard J3061 (SAE 2016).

Participate in Information Sharing In the "Best Practices" NHTSA explicitly encourages two methods of information sharing, namely:

- Communication through the Auto-ISAC among industry participants
- Vulnerability reporting/disclosure between companies and external parties, such as independent researchers

While the Auto-ISAC is discussed in a previous section, a "vulnerability reporting/disclosure policy" describes a relationship between cybersecurity researchers and automotive companies in which the parties establish an easy channel of communications through which the sharing of information can occur.

The motor vehicle industry should adopt explicit vulnerability reporting/disclosure policies and should be open to receive outside information regarding the cybersecurity of their products.

Place Leadership Priority on Product Cybersecurity The "Best Practices" calls for cybersecurity to be a priority at a high level in corporate governance. In addition, the "Best Practices" calls for the following actions to demonstrate management commitment:

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

Consider Fundamental Vehicle Cybersecurity Protections The "Best Practices" does call out some automotive electronics design considerations without specifics. The space of potential cybersecurity threats is large and getting larger as more software is written. Thus, any specifics are likely to become obsolete quickly. The guidance simply suggests that automotive industry should consider these design choices within their risk-based approach and make informed decisions.

Based on the specific architecture, not all design considerations may be necessary. Similarly, the use of certain design techniques is not sufficient to guarantee cybersecurity, which often depends on the underlying architecture.

These design considerations are established through NHTSA's internal research as well as recent efforts by external cybersecurity researchers, (Miller and Valasek, Remote Exploitation of an Unaltered Passenger Vehicle 2015), (Checkoway, et al. 2011), (Kamkar 2015) and others. They are intended to help move motor vehicles towards a more cyber-secure posture.

NHTSA's Vehicle Cybersecurity Research

NHTSA's cybersecurity research approach can be described by five high level goals:

1. Expand and share vehicle cybersecurity knowledge base
2. Facilitate implementation of voluntary industry standards
3. Foster development of new system solutions to improve cybersecurity
4. Investigating minimum performance based vehicle safety requirements for cybersecurity
5. Develop foundational materials to inform policy decisions

NHTSA has a history of performing hands-on testing of vehicles in a variety of different settings. However, the data obtained from a test vehicle is increasingly dependent and defined by software and computer control systems. Since vehicles are defined by the software that they run, NHTSA has been acquiring expertise in embedded systems and cybersecurity.

While NHTSA is developing in-house embedded cybersecurity expertise, NHTSA is funding external research which supports its cybersecurity research goals.

NHTSA's Active Research Projects

Vehicle to Vehicle Basic Safety Message Parser

This project will deliver a formally verified vehicle to vehicle basic safety message parser.

The first line of defense against a hacker who attempts to break a message protocol is the parser which transforms the raw serialized bytes of the communications medium into an appropriate memory structure. In the past, untested invalid messages could move parsing code into unanticipated paths of execution or into a general memory modification.

This project attempts to mitigate this possibility with a message parser which has been mathematically tested and formally verified as correct.

Intrusion Detection Unusual traffic on a CAN bus can be an indicator of a cyberattack. There are several products in the marketplace which attempt to detect these unusual conditions and report them. This project will develop a methodology that could assess the effectiveness of anomaly-based intrusion detection solutions.

Firmware Updates The process of updating the firmware found in vehicles is particularly important from two separate perspectives. First, the ability to fix cybersecurity vulnerabilities depends on the timely application of firmware updates. Second, while incorporating firmware update facilities is vital, if updating procedures are implemented improperly, the updating procedures themselves can become serious cybersecurity vulnerabilities.

This project looks into the practice of updating vehicle firmware. The project looks at current firmware updating practices, their potential for misuse and potential mitigations.

Heavy Vehicle Cybersecurity This project investigates aspects of cybersecurity as they relate to heavy trucks (classes 2-8, 10,000-80,000 pounds).

This study attempts to identify factors that are relevant to comparing cybersecurity of light-, medium-, and heavy-duty trucks with respect to cybersecurity of passenger vehicles. Given the large body of cybersecurity knowledge developed in the light vehicle domain over the past years, the intent of this project is to investigate how much of that knowledge can be readily applied to heavier vehicle classes. In addition, the project will identify what additional areas of heavy truck cybersecurity may need focused research.

Conclusions

Given the ever-changing nature of vulnerabilities in consumer devices, the automotive industry needs to work collectively in an ongoing fashion to manage the vehicle cybersecurity risks. NHTSA will continue to partner with the broader stakeholder groups to sustain the momentum in moving the automotive industry towards a more cyber-secure posture.

References

Auto ISAC. 2016. *Auto ISAC.* https://www.automotiveisac.com/.

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." *USENIX Security.* San Francisco.

CIS. 2016. "Center for Internet Security." *Critical Controls.* August 31. https://www.cisecurity.org/critical-controls/.

Clinton, Bill. 1998. "Presidential Decision Directives." *Federation of American Scientists.* May 22. https://fas.org/irp/offdocs/pdd/pdd-63.htm.

freedesktop.org. 2016. *DBus.* January 14. https://www.freedesktop.org/wiki/Software/dbus/#index5h1.

Gartner. 2015. *Gartner Newsroom.* November 10. http://www.gartner.com/newsroom/id/3165317.

Greenberg, Andy. 2015. *Wired.* July 21. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

ISO. 2016. "ISO/IEC 27000:2016." *International Standards Organization.* February 15. http://www.iso.org/iso/home/store/cat

alogue_tc/catalogue_detail.htm?csnumber=66435.

Kamkar, Samy. 2015. "Drive it Like You Hacked It." *2015 Defcon.* https://samy.pl/defcon2015/2015-defcon.pdf.

Miller, Charlie, and Chris Valasek. 2014. "Adventures in Automotive Networks and Control Units." *IOActive.* http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf.

—. 2015. "Remote Exploitation of an Unaltered Passenger Vehicle." *Illmatics.* August 10. http://illmatics.com/Remote%20Car%20Hacking.pdf.

NHTSA. 2016. "Cybersecurity Best Practices For Modern Vehicles." *NHTSA .* www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

—. 2016. "Proactive Safety Principles." *US DOT Briefing Room.* January 15. https://www.transportation.gov/sites/dot.gov/files/docs/ProactiveSafetyPrinciples2016.pdf.

NIST. 2014. "Cybersecurity Framework." *National Institute of Standards and Technology.* February 12. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

Robert Bosch GmbH. 1991. "CAN Specification." *Bosch Semiconductors.* http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf.

SAE. 2016. "Society of Automotive Engineers Standards." *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* January. http://standards.sae.org/wip/j3061/.

Singh, Santokh. 2015. "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey." *NHTSA Crash Statistics.* February. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115.

Stahl, Leslie. 2015. *CBS News 60 Minutes.* CBS. February 6. http://www.cbsnews.com/news/car-hacked-on-60-minutes/.

US DOT. 2016. *US DOT Briefing Room.* August 29. https://www.transportation.gov/briefing-room/traffic-fatalities-sharply-2015.