資料15-3-3-4

NHTSA and Vehicle Cybersecurity

NHTSA
www.nhtsa.gov

Safer drivers. Safer cars. Safer roads.

Introduction

In 2013, 32,719 people died on the Nation's roadways. Sadly, NHTSA estimates 94 percent of highway crashes are a result of human error.[1] Today's electronics, sensors, and computing power enable the deployment of safety technologies, such as forward-collision warning, automatic-emergency braking, and vehicle-to-vehicle technologies, which can keep drivers from crashing 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, vehicle cybersecurity was never an afterthought for NHTSA. 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 modified its organizational structure, developed vital partnerships, adopted a layered research approach, considered legislative additions, and encouraged members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United States. NHTSA's goal is be ahead of potential vehicle cybersecurity challenges, and seek ways to address or avoid them altogether.

What Is NHTSA Doing?

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

[1] www-nrd.nhtsa.dot.gov/Pubs/812115.pdf

electronics at the Vehicle Research and Test Center in East Liberty, Ohio. Together, these entities execute research programs in three main areas:

- electronics reliability (including functional safety [2])
- automotive cybersecurity
- automated vehicles

They are responsible for evaluating, testing, and monitoring potential automotive cyber vulnerabilities, and for leading the agency's research of highly automated vehicles.

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

NHTSA's 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. The Agency's multilayered approach to cybersecurity has the following goals:

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

2. Facilitate the implementation of 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. Research 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.

[2] "**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." http://www.iec.ch/functionalsafety/explained/

In October 2014, NHTSA published four cybersecurity reports that describe the agency's initial work to support the goals outlined in its Automotive Cybersecurity Research Program.

- *Assessment of the Information Sharing and Analysis Center Model*
  This report presented findings from an assessment of the ISAC model, and how ISACs are effectively implemented in other sectors. The report also explains how a new sector ISAC could be formed by leveraging existing ISAC models. This report was sent directly to the Association of Global Automakers and Alliance of Automobile Manufacturers to aid with their automotive ISAC activities.
- *A Summary of Cybersecurity Best Practices*
  This report documented results from the analysis and review of best practices and observations across a variety of industries in the field of cybersecurity involving electronic control systems. It provides benchmarks for the agency and the industry.
- *Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach*
  This report described a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems are included, along with a matrix containing a condensed version of the various potential attacks.
- *National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles*
  This report reviewed the NIST guidelines and foundational publications from an automotive cybersecurity risk management standpoint. The NIST approach is often used as a baseline to develop a more targeted risk management approach for use in specific industries and sectors.

Layered Approach

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, 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 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 ISAC). 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.

Legislative Improvements

NHTSA also has examined whether legislative provisions might further improve the cybersecurity posture of vehicles. The U.S. Department of Transportation (USDOT)'s GROW AMERICA legislative proposal includes liability for hackers, clarifying authority for the agency to issue process rules or guidelines for the safe development of new systems, and imminent hazard authority that would enable swift action to protect the public from cybersecurity vulnerabilities and other safety threats. We believe the legislative proposals contained in GROW AMERICA will allow the agency to stay ahead of cybersecurity challenges.

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.

Engagement With the Automotive Industry

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,[3] 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 of 2015.

[3] http://www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865

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 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 (ESCAR); the Defense Advanced Research Projects Agency (DARPA)'s High Assurance Cyber Military Systems (HACMS) and National Science Foundation (NSF)'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, which address cybersecurity among other topics.

- NHTSA serves as a liaison to SAE International's Vehicle Electrical Security System committee and participates in their meetings.

- NHTSA works closely with other Federal organizations with interests in automotive cybersecurity. For instance, we have been interacting with DARPA and their HACMS program leaders and are pursuing a research project to develop a secure reference parser for Vehicle-to-Vehicle (V2V) communication interfaces based on DARPA's extensive research and experience in this area. We also collaborate with the U.S. Department of Homeland Security (DHS), NIST, and the U.S. Army Tank Automotive Research, Development, and Engineering Center (T ARDEC) in different capacities to leverage synergies, avoid redundant emphasis, and share knowledge and expertise.

V2V & V2I Communications and Security Infrastructure

For the past several years, USDOT, NHTSA, vehicle manufactures, automotive suppliers, security experts, and other government agencies have been developing Dedicated Short Range Communications (DSRC) radio technology and the associated architecture and protocols to support trusted vehicle-to-vehicle and vehicle-to-infrastructure communications. We are finalizing the architecture and have research plans to conduct full-scale vulnerability testing and to address any security issues that emerge from that testing. In addition, as NHTSA pursues its

regulatory efforts, the agency will propose and seek comments on various aspects of the architecture including the protocols that will ensure interoperability and security.

NHTSA and its partners are developing a Public Key Infrastructure (PKI) based system, termed the "Security Credential Management System" (SCMS), for ensuring trusted and secure V2V and V2I communications. PKI security architectures and methodologies are already used extensively in the auto industry. The SCMS would employ highly innovative methods, encryption, and certificate management techniques to address the challenging task of ensuring trusted communications between entities that previously have not encountered each other—but also wish to remain anonymous (as is the case when vehicles/drivers encounter each other on the road). This is further detailed in NHTSA's publication, *Vehicle to Vehicle Communications: Readiness of V2V Technology for Application*.

In addition, USDOT and NHTSA will adhere to the fullest extent possible to industry consensus standards applicable to V2V and V2I DSRC-based communications. These include the Institute of Electrical and Electronics Engineers (IEEE) P 1609 and 802.11 P standards that cover communication protocols, as well as SAE International standards that address communications performance, applications, and data coding requirements.

USDOT also intends to work with DARPA to identify potentially unique cyber vulnerabilities associated with establishing a standardized wireless link with motor vehicles, and develop countermeasures and solutions for such vulnerabilities.

Conclusion

No single approach is sufficient because in the cybersecurity realm, 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.