March 2016

VEHICLE CYBERSECURITY

DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack

GAO Highlights

Highlights of GAO-16-350, a report to congressional requesters

Why GAO Did This Study

Over time, the amount of software code in vehicles has grown exponentially to support a growing number of safety and other features. However, the reliance on software to control safety-critical and other functions also leaves vehicles more vulnerable to cyberattacks.

GAO was asked to review cybersecurity issues that could impact passenger safety in modern vehicles. This report addresses, among other things, (1) available information about the key cybersecurity vulnerabilities in modern vehicles that could impact passenger safety; (2) key practices and technologies, if any, available to mitigate vehicle cybersecurity vulnerabilities and the impacts of potential attacks; (3) views of selected stakeholders on challenges they face related to vehicle cybersecurity and industry-led efforts to address vehicle cybersecurity; and (4) DOT efforts to address vehicle cybersecurity.

GAO reviewed relevant existing regulations and literature and interviewed officials from DOT; the Departments of Commerce, Defense, and Homeland Security; industry associations; and 32 selected industry stakeholders, including automakers, suppliers, vehicle cybersecurity firms, and subject matter experts. The experts were selected based on a literature search and stakeholder recommendations, among other things.

What GAO Recommends

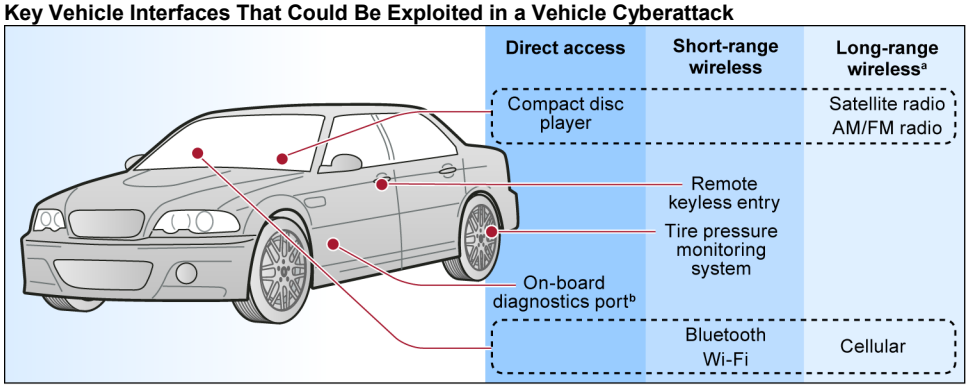
GAO recommends that DOT define and document its roles and responsibilities in response to a vehicle cyberattack involving safety-critical systems. DOT concurred with our recommendation.

View GAO-16-350. For more information, contact David J. Wise at (202) 512-2834 or wised@gao.gov.

What GAO Found

Modern vehicles contain multiple interfaces—connections between the vehicle and external networks—that leave vehicle systems, including safety-critical systems, such as braking and steering, vulnerable to cyberattacks. Researchers have shown that these interfaces—if not properly secured—can be exploited through direct, physical access to a vehicle, as well as remotely through short-range and long-range wireless channels. For example, researchers have shown that attackers could compromise vulnerabilities in the short-range wireless connections to vehicles' Bluetooth units—which enable hands-free cell phone use—to gain access to in-vehicle networks, to take control over safety-critical functions such as the brakes. Among the interfaces that can be exploited through direct access, most stakeholders we spoke with expressed concerns about the statutorily mandated on-board diagnostics port, which provides access to a broad range of vehicle systems for emissions and diagnostic testing purposes. However, the majority of selected industry stakeholders we spoke with (23 out of 32) agreed that wireless attacks, such as those exploiting vulnerabilities in vehicles' built-in cellular-calling capabilities, would pose the largest risk to passenger safety. Such attacks could potentially impact a large number of vehicles and allow an attacker to access targeted vehicles from anywhere in the world. Despite these concerns, some stakeholders pointed out that such attacks remain difficult because of the time and expertise needed to carry them out and thus far have not been reported outside of the research environment.

Key Vehicle Interfaces That Could Be Exploited in a Vehicle Cyberattack



Source: GAO analysis of stakeholder interviews and Checkoway et al, 2011. | GAO-16-350

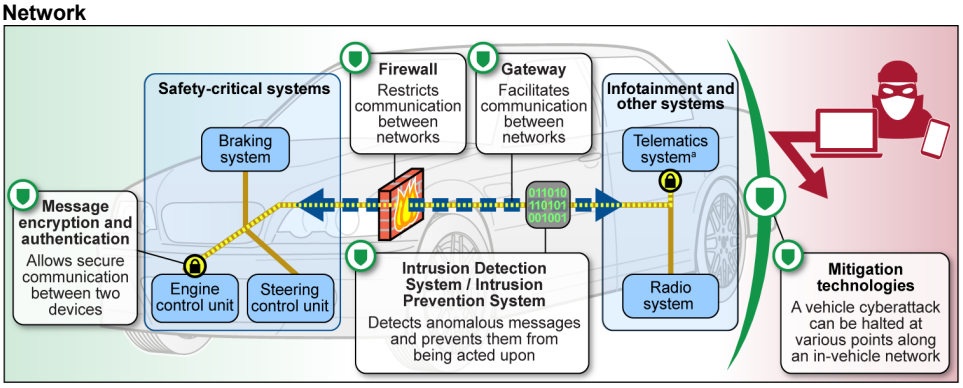
[a]In this context, long-range refers to access at distances over 1 kilometer.

[b]This port is mandated in vehicles by statute for emission-testing purposes and to facilitate diagnostic assessments of vehicles, such as by repair shops. 42 U.S.C. § 7521(a)(6).

Selected industry stakeholders, both in the United States and Europe, informed GAO that a range of key practices is available to identify and mitigate potential vehicle-cybersecurity vulnerabilities. For instance, the majority of selected industry stakeholders we spoke with (22 out of 32) indicated that—to the extent possible—automakers should locate safety-critical systems and non-safety-critical systems on separate in-vehicle networks and limit communication between the two types of systems, a concept referred to as "domain separation." However, some of these stakeholders also pointed out that complete separation

is often not possible or practical because some limited communication will likely need to occur between safety-critical and other vehicle systems. In addition, selected industry stakeholders we spoke to identified technological solutions that can be incorporated into the vehicle to make it more secure. However, according to stakeholders, many of these technologies—such as message encryption and authentication, which can be used to secure and verify the legitimacy of communications occurring along in-vehicle networks—cannot be incorporated into existing vehicles. Rather, such technologies must be incorporated during the vehicle design and production process, which according to stakeholders, takes approximately 5 years to complete.

Example of a Vehicle's Cybersecurity-Mitigation Technologies Shown along an In-Vehicle Network



Source: GAO analysis of stakeholder information. | GAO-16-350

[a]Vehicle "telematics systems"—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

Selected industry stakeholders identified several challenges they face related to vehicle cybersecurity. For instance, the lack of transparency, communication, and collaboration regarding vehicles' cybersecurity among the various levels of the automotive supply chain and the cost of incorporating cybersecurity protections into vehicles were the two most frequently cited challenges—mentioned by 15 and 13 of the 32 selected industry stakeholders, respectively. However, several industry-led efforts are planned and under way that, according to stakeholders, could potentially help automakers and parts suppliers identify and mitigate vehicle cybersecurity vulnerabilities and address some of the challenges that industry stakeholders face. For example, two U.S. industry associations have been leading the effort to establish an Automotive Information Sharing and Analysis Center (ISAC) to collect and analyze intelligence information and provide a forum for members to anonymously share threat and vulnerability information with one another. Selected industry stakeholders we spoke to, as well as DOT officials, generally expressed positive views regarding the potential effectiveness of an Automotive ISAC.

The Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) has taken steps to address vehicle cybersecurity issues but has not determined the role it would have in responding to a real-world vehicle cyberattack. For example, NHTSA added more research capabilities in this area and is developing guidance to help the industry determine when cybersecurity vulnerabilities should be considered a safety defect, and thus merit a recall; it expects to issue this guidance by March 31, 2016. Further, pursuant to a statutory mandate, NHTSA is examining the need for government standards or regulations regarding vehicle cybersecurity. However, officials estimated that the agency will not make a final determination on this need until at least 2018. Although NHTSA's stated goal is to stay ahead of potential vehicle-cybersecurity challenges, NHTSA has not yet formally defined and documented its roles and responsibilities in the event of a real-world cyberattack. Until it develops such a plan, in the event of a cyberattack, the agency's response efforts could be slowed as agency staff may not be able to quickly identify the appropriate actions to take.