Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

May 2020

FOREWORD

This document reviews and applies existing transportation cybersecurity best practices from the National Highway Traffic Safety Administration (NHTSA) and other organizations to heavy vehicles. The focus is on telematics devices, as they are a common attack vector, and requirements for electronic logging devices (ELDs) in the United States have increased the rate at which such devices are being deployed. There are two primary focus areas in this document: policy and procedure recommendations and technical recommendations This document is intended for use by truck/bus manufacturers, telematics service providers (TSPs), motor carriers, heavy truck dealers/installers, fleet managers, mechanics, drivers, and Government regulators. This document may also be useful to original equipment manufacturers (OEMs) who build tractors, trailers, engines, and other systems for trucks, as it will help them consider how their systems might be accessed, legitimately or maliciously. Finally, Federal, State, and local governments can use the document as a "best practices" guide when considering cybersecurity risks associated with deployment of telematics devices.

NOTICE

QUALITY ASSURANCE STATEMENT

The Federal Motor Carrier Safety Administration (FMCSA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FMCSA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No. **FMCSA-RRT-19-013**	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle **Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles**		5. Report Date **May 2020**
		6. Performing Organization Code
7. Author(s) **Klinedinst, Dan**		8. Performing Organization Report No.
9. Performing Organization Name and Address **Carnegie Mellon University, Pittsburgh, Pennsylvania**		10. Work Unit No. (TRAIS)
		11. Contract or Grant No.
12. Sponsoring Agency Name and Address **U.S. Department of Transportation** **Federal Motor Carrier Safety Administration** **Office of Analysis, Research, and Technology** **1200 New Jersey Ave. SE** **Washington, DC 20590**		13. Type of Report and Period Covered **Final Report**
		14. Sponsoring Agency Code **FMCSA/NHTSA**
15. Supplementary Notes **Contracting Officer's Representative: Jonathan Mueller**		

16. Abstract

This document reviews and applies existing transportation cybersecurity best practices from the National Highway Traffic Safety Administration (NHTSA) and other organizations to heavy vehicles. The focus is on telematics and aftermarket devices, as they are a common attack vector, and requirements for electronic logging devices (ELDs) in the United States have increased the rate at which such devices are being deployed. There are two primary focus areas in this document: policy and procedure recommendations and technical recommendations. This document is intended for use by truck/bus manufacturers, telematics service providers (TSPs), motor carriers, heavy truck dealers/installers, fleet managers, mechanics, drivers, and Government regulators. This document may also be useful to original equipment manufacturers (OEMs) who build tractors, trailers, engines, and other systems for trucks, as it will help them consider how their systems might be accessed, legitimately or maliciously. Finally, Federal, State, and local governments can use the document as a "best practices" guide when considering cybersecurity risks associated with deployment of telematics devices.

17. Key Words **Heavy truck, heavy vehicle, telematics, electronic logging devices, cybersecurity, telematics, transport layer security, controller area network**	18. Distribution Statement **No restrictions**		
19. Security Classif. (of this report) **Unclassified**	20. Security Classif. (of this page) **Unclassified**	21. No. of Pages **26**	22. Price

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized.

SI* (MODERN METRIC) CONVERSION FACTORS

Approximate Conversions to SI Units				
Symbol	**When You Know**	**Multiply By**	**To Find**	**Symbol**
		Length		
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
		Area		
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yards	0.836	square meters	m^2
ac	Acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
		Volume (volumes greater than 1,000L shall be shown in m^3)		
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
		Mass		
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2,000 lb)	0.907	megagrams (or “metric ton”)	Mg (or “t”)
		Temperature (exact degrees)		
°F	Fahrenheit	5(F-32)/9 or (F-32)/1.8	Celsius	°C
		Illumination		
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
		Force and Pressure or Stress		
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

Approximate Conversions from SI Units				
Symbol	**When You Know**	**Multiply By**	**To Find**	**Symbol**
		Length		
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
		Area		
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
Ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
		Volume		
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
		Mass		
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or “t”)	megagrams (or “metric ton”)	1.103	short tons (2,000 lb)	T
		Temperature (exact degrees)		
°C	Celsius	1.8c+32	Fahrenheit	°F
		Illumination		
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
		Force and Pressure or Stress		
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

* SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003, Section 508-accessible version September 2009.)

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF ACRONYMS, ABBREVIATIONS, AND SYMBOLS

Acronym	Definition
AADL	Architectural Analysis and Design Language
ASLR	address space layout randomization
CAN	controller area network
CERT	Computer Emergency Response Team
CMV	commercial motor vehicle
DEP	Data Execution Prevention
DSRC	dedicated short-range communications
DTC	diagnostic trouble codes
ECU	electronic control units
ELDs	electronic logging devices
FMCSA	Federal Motor Carrier Safety Administration
GDL	guideline
GPS	global positioning satellite
HIDS	host-based intrusion detection system
HOS	hours of service
HSM	hardware security module
IEEE	Institute of Electrical and Electronics Engineers
IVI	in-vehicle infotainment
JTAP	joint test action group
MAC	media access control
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OEM	original equipment manufacturer
OS	operating system
PASTA	Process for Attack Simulation and Threat Analysis
RCA	root certificate authority

RF	radio frequency
RPM	revolutions per minute
SD	secure digital
SMS	short message service
SDR	software-defined radio
SOTA	secure over-the-air
SSP	secure simple pairing
TCU	telematics control unit
TLS	Transport Layer Security
TSP	telematics service provider
UDS	Unified Diagnostic Services
US-CERT	U.S. Computer Emergency Readiness Team
USDOT	U.S. Department of Transportation
USB	universal serial bus
VAST	Visual, Agile, and Simple Threat
V2X	vehicle-to-everything
WEP	Wired Equivalent Privacy
WPA2	Wi-Fi Protected Access 2

[This page intentionally left blank.]

EXECUTIVE SUMMARY

OVERVIEW

Heavy vehicles such as commercial trucks and buses are critical to the Nation's economic security. Due to several highly publicized cyber-attacks on vehicles, cybersecurity in heavy vehicles has become a major concern for the industry. This document reviews existing cybersecurity best practices from the National Highway Traffic Safety Administration (NHTSA) and other organizations and applies them to heavy vehicles.

BACKGROUND

This document, which provides a series of guidelines for ensuring cybersecurity in telematic units and other components specific to connected heavy trucks, is based primarily on two existing documents. The first is NHTSA's *Cybersecurity Best Practices for Modern Vehicles*.(1) The second is the Institute of Electrical and Electronics Engineers (IEEE) Center for Secure Design's *Design Flaws and Security Considerations for Telematics and Infotainment Systems*.(2) Best practices from these documents and from direct research and testing have been adapted for heavy vehicles in this document.

Guidelines in this document are broken down by section. The first several sections contain policy and procedure recommendations, while the last section contains technical recommendations. Each recommendation is explained and then summarized with a guideline. These guidelines are also listed in Appendix A, as a quick reference checklist.

AREAS ADDRESSED

Primary areas addressed in this document include:

- Cybersecurity processes in design and manufacturing:
  - Architectural analysis and threat modeling.
  - Secure coding.
  - Adversarial testing.
  - Failing safely.
  - Risk assessments.
- Cybersecurity processes during assembly, sales, and delivery:
  - Supply chain.
  - Security guarantees from suppliers.
  - Integration testing/emergent vulnerabilities.
  - Change credentials, reset logs, etc.
- Cybersecurity processes during fleet lifetime:
  - Vulnerability response.
  - Patch management.

  - Information sharing.
  - Incident response.
- Technical controls for heavy vehicles:
  - Telematics.
  - ELDs.
  - Secure over-the-air software.
  - Internal networks (segregation and authentication).
  - Radio frequency interfaces.
  - Key management.
  - Debugging and diagnostics.
  - Security event logging.

AUDIENCES AND INTENDED USE

The primary audiences for this "best practices" document are:

- Manufacturers and vendors of telematics devices, both original equipment manufacturers (OEM) and aftermarket.
- Dealers, service centers, and installers who sell, install, and service telematics devices or services.
- Fleet managers and owner/operators who are concerned about their vehicles.
- Motor carriers.

This document may also be useful to OEMs who build tractors, trailers, engines, and other systems for trucks, as it will help them consider how their systems might be accessed, legitimately or maliciously. Finally, Federal, State, and local governments can use the document as a "best practices" guide when considering cybersecurity risks associated with use of telematics devices.

1. OVERVIEW

1.1 BACKGROUND

The Community Emergency Response Team (CERT) Coordination Center performed a survey of existing research on automotive cybersecurity, with a specific focus on heavy vehicles (trucks and buses) for the National Highway Traffic Safety Administration (NHTSA) and the Federal Motor Carrier Safety Administration (FMCSA). After identifying risks, threats, and potential mitigations, these guidelines were developed to help truck/bus manufacturers, telematics service providers (TSPs), fleet managers, and others secure existing heavy vehicles. Many trucks have used telematics longer than passenger vehicles, to make fleets more efficient. However, decreasing costs of hardware, the market push for increased connectivity, and some Government requirements (i.e., electronic logging devices, or ELDs) have accelerated the speed at which heavy truck carriers deploy telematics systems.

This document is based primarily on two existing documents. The first is NHTSA's *Cybersecurity Best Practices for Modern Vehicles*.[3] The second is the Institute of Electrical and Electronics Engineers (IEEE) Center for Secure Design's *Design Flaws and Security Considerations for Telematics and Infotainment Systems*.[4] Best practices from these documents and from direct research and testing have been adapted for heavy vehicles in this document. This document contains a series of succinct guidelines, marked as **[GDL #]**, each of which is accompanied by explanatory text. In addition, these guidelines are listed without the explanatory text in Appendix A: Checklist, for quick reference. Guidelines in Section 2, Section 3, and Section 4 are generally related to policies and procedures, while guidelines in Section 5 are more technical types of controls.

1.2 SCOPE

The intent of this document is to focus on telematics and other components specific to connected heavy trucks. The primary risk that is being addressed is that of creating a bridge between the Internet—or other networks—and the networks inside the trucks. There is some discussion of security with respect to internal networks and protocols, such as the controller area network (CAN) protocol and the SAE J1939 standard, with respect to electronic control units (ECUs). However, this document does not attempt comprehensive coverage of those topics.

In addition, this document focuses on currently deployed and near-term technologies. The industry is on the verge of several technological breakthroughs that have major security implications—primarily autonomous (self-driving) vehicles and vehicle-to-everything (V2X) communications. These technologies are still being designed and tested, so it is not possible to make specific security recommendations at this point.

The primary audiences for this document are:

- Manufacturers and vendors of telematics devices, both original equipment manufacturers (OEM) and aftermarket.

- Dealers, service centers, and installers who sell, install, and service telematics devices or services.
- Fleet managers and owner/operators who are concerned about their vehicles.
- Motor carriers.

This document may also be useful to OEMs who build tractors, trailers, engines, and other systems for trucks, as it will help them consider how their systems might be accessed, legitimately or maliciously. Finally, Federal, State, and local governments can use the document as a "best practices" guide when considering cybersecurity risks associated with use of telematics devices.

2. CYBERSECURITY PROCESSES IN DESIGN AND MANUFACTURING

2.1 ARCHITECTURAL ANALYSIS AND THREAT MODELING

Security is often overlooked during the software development and hardware design process. In highly competitive markets, engineers often focus their time on implementing new features and shipping products rather than securing them. However, there are practices that can help vendors of telematics systems design products that will provide functionality without compromising the safety or security of the vehicle.

Architectural analysis and threat modeling are methods of examining a system for potential security risks. While there are many different tools and methodologies for performing these types of analysis, there are two overriding concepts. The first is to methodically document information flows, interfaces, and decision points where security decisions are made. The second is to examine the system from the point of view of an adversary. Some of the methods for completing these types of analyses include the Architectural Analysis and Design Language (AADL) Security Annex, the Microsoft STRIDE methodology, attack trees, the Process for Attack Simulation and Threat Analysis (PASTA), and Visual, Agile, and Simple Threat (VAST) modeling.

[GDL 1] Conduct architectural analysis and/or threat modeling during system design.

2.2 SECURE CODING

Many security issues arise from simple coding errors. While modern languages have eliminated or reduced some common classes of errors, many embedded systems contain older, more error-prone languages. There are many tools and guides for writing secure code and avoiding common errors.(5) Manufacturers of telematics systems should take positive steps to implement and enforce secure coding practices, while their customers should ask potential vendors what practices they follow.

[GDL 2] Follow secure coding best practices.

2.3 ADVERSARIAL TESTING

Adversarial testing – often referred to as penetration testing or red teaming – is an umbrella term for doing hands-on technical testing of a product before deployment. While most software development cycles will include multiple rounds of quality assurance, functional testing, and other testing, security testing can be overlooked. Adversarial testing is similar to threat modeling in that it examines the system from the perspective of an attacker. However, adversarial testing can only take place once there is an actual implementation of a system. This ensures that security decisions made in the design phase were implemented according to the design and that programming bugs were not introduced inadvertently.

[GDL 3] Perform adversarial testing before a product is finalized (OEMs) or before it is deployed (TSPs/dealers/installers).

2.4 FAIL SAFELY

Safety engineering is a critical part of designing systems for vehicles. Since security can affect safety, it is important to look at any potential security risks identified in earlier stages and determine what actions to take in case of compromise. For example, if a telematics unit cannot verify the authenticity of a software update, it should continue to run the old software rather than simply shutting down, if shutting down could endanger the driver.

[GDL 4] Security problems will happen; fail safely.

2.5 RISK ASSESSMENT

A risk assessment is more often done by end customers of telematics systems, but it should still be done prior to procuring and implementing a system. For example, a fleet manager or owner of a small trucking company might work with telematics vendors to identify any risks from implementing "connected trucks" technology. This includes loss of proprietary information to the potential for crashes. These risks can then be mitigated or accepted, depending on regulatory requirements and the customer's appetite for risk (including financial loss). A commonly used framework for risk assessments in the cybersecurity field is the National Institute of Standards and Technology (NIST) Cybersecurity Framework.(6)

[GDL 5] Perform a risk assessment before implementing any telematics or other sort of "connected" technology in vehicles.

3. CYBERSECURITY PROCESSES DURING ASSEMBLY, SALES, AND DELIVERY

Telematics device security should be a concern throughout the supply-chain process, including but not limited to device assembly, sale, delivery, and implementation.

3.1 SUPPLY CHAIN

The supply chain is comprised of many different interworking parts from various partners, focusing on third-party suppliers, devices, software, and the purchasing vendor. System integrators are expected to complete their own cybersecurity due diligence, which involves implementing standards and performing testing and audits on potential devices. NIST suggests some basic steps to ensure supply-chain security. These steps include implementing strict policies against working with vendors that have poor security standards, the ability for the purchasing vendors to obtain the source code and test it themselves, and other basic security measures (secure coding, secure booting, etc.). In addition to these recommendations and basic security measures, purchasing vendors should ensure that there are access controls in place (physical and digital if applicable) and that basic data security measures are taken (use of encryption, data management, minimum security requirements of upstream suppliers, etc.).

[GDL 6] Perform your own security due diligence, which involves but is not limited to ensuring that third-party devices in the supply chain meet your basic security requirements.

3.2 SECURITY GUARANTEES FROM SUPPLIERS

There are multiple concerns that should be addressed by system integrators throughout the supply chain. System integrators should ensure that third-party vendors are able to mitigate known vulnerabilities and that they have established controls to address emerging vulnerabilities. System integrators should also guarantee that they have capabilities in place to monitor their production to ensure these devices are manufactured securely.

[GDL 7] Obtain legal security guarantees that meet your minimum-security requirements for all products.

3.3 INTEGRATION TESTING/EMERGENT VULNERABILITIES

Difficulties can arise in the supply chain if third-party or subsystem suppliers are unable to respond to emerging threats. Which group will be responsible for creating, implementing, and maintaining software/firmware updates for the device should be determined and agreed upon prior to purchase of a telematics system. The party creating the mitigation should also be aware of upstream devices used in conjunction with the device in question. That party should test new patches or mitigations to ensure that the device works with all other devices connected to it and does not disable anything in the supply chain. It should also be clear who implements the patch. Will the device

manufacturer push the update automatically? Or will the purchasing vendor be responsible for getting the update and applying it?

[GDL 8] Decide early who oversees creating, implementing, and maintaining software/firmware updates for a device when a vulnerability emerges, and ensure these guidelines are met.

3.4 CHANGE CREDENTIALS, RESET LOGS, ETC.

Almost every device comes with default settings unless the third-party supplier explicitly created a unique device. The purchasing vendor should discuss these settings with the third-party supplier and change them immediately upon receiving the device. If the third-party supplier oversees patch management, it would also be beneficial to determine which settings need to remain the same so that the supplier can perform security updates. If the supplier's requirements violate the purchasing vendor's basic security requirements (use of a hard-coded password, updates sent insecurely, etc.), then the vendors should work together to find a better method for patching.

[GDL 9] Reset default credentials, logs, etc., as soon as the device is received.

4. CYBERSECURITY PROCESSES DURING FLEET LIFETIME

4.1 VULNERABILITY RESPONSE

A critical step in preventing security breaches is maintaining awareness of vulnerabilities and responding to their disclosure appropriately. This vulnerability information may come from upstream industry providers or from public or private security research communities.

4.1.1 Responding to the Research Community

Like the automotive industry members that are the subject of *Cybersecurity Best Practices for Modern Vehicles*, the heavy vehicle industry should consider either creating their own vulnerability reporting and disclosure policies or adopting similar policies to those used in other industries.(7) Large software vendors often have mature vulnerability response policies and programs that can be used as a model.

Even if an industry member does not produce equipment or software, any member may be contacted by the cybersecurity research community, and it is important that the research community's findings are properly investigated and evaluated. As stated by NHTSA, "A vulnerability reporting and disclosure policy should inform cybersecurity researchers [on] how a company plans to interact with them" and should be publicly available.(8) At a minimum, such a policy should direct the researchers to the correct place to report vulnerabilities (website form, email address, etc.). Guidelines for establishing vulnerability response processes can be found in *The CERT Guide to Coordinated Vulnerability Disclosure.*(9) Other vulnerability disclosure best practices resources are published by the International Organization for Standardization (ISO), in standards ISO/IEC 29147 (Information Technology—Security Techniques—Vulnerability Disclosure) and ISO 30111 (Information Technology—Security Techniques—Vulnerability Handling Processes).

[GDL 10] Publish a vulnerability reporting and disclosure policy.

4.1.2 Upstream Awareness

It is increasingly common for suppliers to disclose vulnerability information regarding their products to their downstream consumers (e.g., carriers). This information helps the downstream consumers remain secure, assuming they act upon that information. Heavy vehicle industry members should have a process in place for tracking vulnerabilities in upstream providers. This process should either be a part of patch management or an input to such a process.

[GDL 11] Have a process for tracking vulnerability disclosures affecting devices being deployed in the fleet.

4.2 PATCH MANAGEMENT

Patch management is a common practice amongst information technology teams in many industry sectors, where those sectors employ an operational system of various devices and software. Patch management deals with updating and servicing the software components of these systems to mitigate vulnerabilities, fix usability bugs, or add features.

Heavy vehicle industry members should employ a patch management process that allows them to deploy security patches in a timely manner. This patch management process should cover identification, testing, evaluation, and application of security patches.

[GDL 12] Security patches should always be deployed to fleet devices in timely manner (also see GDL 8).

4.3 INFORMATION SHARING

Sharing cybersecurity information and collaborating with other industry members is highly useful for responding to threats efficiently. 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."[(10)]

It is encouraged that heavy vehicle industry members join an industry-specific information sharing and analysis organization. Organizations such as the Auto Information Sharing and Analysis Center, the American Trucking Associations Technology & Maintenance Council Fleet CyWatch Program,[(11)] and the National Motor Freight Traffic Association[(12)] are viable options, and many heavy vehicle industry members may already be participants.

[GDL 13] Share cybersecurity information with heavy vehicle the industry.

4.4 INCIDENT RESPONSE

Note: This section is adapted from NHTSA's *Cybersecurity Best Practices for Modern Vehicles.*

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

The response process should report all incidents, exploits, and vulnerabilities to an information sharing and analysis organization as soon as possible. This is recommended for companies that may not yet be members of such an organization, as well. Any incidents should also be reported to the United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines.(13)

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

[GDL 14] Employ an incident response process.

Note: GDL 15–19 intentionally left blank for future use.

[This page intentionally left blank.]

5. TECHNICAL CONTROLS FOR HEAVY VEHICLES

This section covers technical recommendations for heavy vehicles. Many of these are similar to technical recommendations for passenger vehicles; areas that are more specific to heavy vehicles will be covered in more depth. Despite the homogeneity of in-vehicles networks due to J1939, there are many variations in truck design, so specific technologies or settings are not generally recommended.

5.1 TELEMATICS

As in passenger vehicles, telematics devices present the most obvious remote attack vector into the vehicle. For the purposes of these guidelines, the following components are included under the heading of telematics: the telematics control unit (TCU), which handles cellular and satellite radio communications; any driver-accessible maintenance information or vehicular settings; and any in-vehicle infotainment (IVI) system. This "telematics system" may be OEM, aftermarket, or a combination of both. In addition, it may be composed of one integrated unit or several different units, and it may have different levels of functionality depending on the OEM and carrier. However, there are several common characteristics. These characteristics include a data connection via cellular and/or satellite, at least one interface to the vehicle's internal bus(es), and a relatively large amount of processing power and memory.

5.1.1 Least Privilege

The concept of least privilege is often recommended in cybersecurity. The idea is that any component in a system should only have access to what it needs to do. While this is generally applicable to vehicles, it is particularly applicable to telematics units, many of which are built on operating systems that provide multiple levels of authorization. At the least, the operating system will usually provide applications the ability to run with "kernel" or "administrator" versus "user" privileges. The kernel of the operating system is the part that interacts with all the physical components and therefore has the most privilege and the most ability to violate security controls. Most applications should run in user mode, which allows access to the hardware only via interfaces defined by the kernel. For example, on a well-designed telematics unit, the application that displays fuel efficiency should not be able to directly send arbitrary CAN messages to the CAN transceiver. It should only be able to make requests to the kernel to send predefined messages on its behalf. Modern operating systems like Android have robust levels of privilege, effectively partitioning apps from each other as well as from direct access to the hardware.

[GDL 20] Give applications the least privilege they need to function.

Least privilege also implies "least functionality." That is, only code that is required to perform the needed functionality should be enabled. If possible, unnecessary code should be removed from the device entirely, although manufacturers may not be able to recompile proprietary operating systems to their specifications.

[GDL 21] Where possible, remove code that isn't used.

5.1.2 Use Existing Controls

In addition to multiple levels of privilege, many telematics operating systems will have security controls built into the operating system (OS). While this document cannot provide a hardening guide for every possible telematics OS, some common features that should be leveraged include:

- Executable space protection (e.g., Data Execution Prevention [DEP] in Windows).
- Address space layout randomization (ASLR).
- File permissions and/or role-based access controls.
- "Default deny" for network connections.
- Disk encryption.
- Host-based intrusion detection system (HIDS).

[GDL 22] Leverage security controls built into the operating system.

5.1.3 Secure External Interfaces

The biggest security risk of the telematics unit is that it is often remotely accessible via voice, short message service (SMS), and/or data networks, including the internet. There is a common misconception that these interfaces are safe because inbound network connections to the device from the internet are blocked.

Unfortunately, attackers have been finding ways around firewalls for decades, and telematics units are just as prone to some of these attacks as traditional computers. For example, in a recent research effort, the CERT Coordination Center demonstrated how to use SMS to bypass security controls and establish an internet connection to a certain brand of telematics unit.(14)

[GDL 23] Follow best practices for securing cellular or satellite interfaces.

5.1.3.1 Cellular or Satellite Interface Security

Passenger cars typically only have one telematics unit, which is a cellular TCU built in by the OEM. Fleet cars might have a second one used by fleet managers. Therefore, heavy trucks are more likely to have multiple connections. First, they might have both a cellular and a satellite connection, so that they can communicate when they are outside of a cellular coverage area. Second, they might have both an OEM connection (for maintenance and troubleshooting) and a fleet management device. Finally, they might have a separate ELD, a fuel payment device, separate devices for the tractor and trailer, etc. These might include the option of cellular and/or satellite communications.

Cellular security is largely up to choice of carrier. It is important to note that encryption and security settings on networks in the United States may not exist or be enforced in other countries. If possible, use 3G or 4G cellular modems that do not support 2G. While this might decrease coverage, it prevents rogue base stations from forcing a device to fall back to 2G, which has much less security. 2G is becoming obsolete in the United States, so this should have minimal operational impact.

[GDL 24] Don't support 2G on cellular modems unless operationally necessary.

5.1.3.2 Satellite Communication

The security research community seems to be in the early stages of looking at satellite communication protocols, hardware, and common architectures. For this reason, there are no good, general references for satellite security. Best practices dictate that satellite communication users assume there is very little security in the transport mechanism and apply security controls at a higher layer. This means using the Transport Layer Security (TLS) protocol or other accepted authentication and encryption mechanisms, access control, and good key management practices, as outlined throughout this document.

[GDL 25] Assume satellite communication channels have unknown security vulnerabilities and might become compromised at any time.

5.1.3.3 External Input

Another main concept in security is to filter and verify input to the system. One of the most common attacks is to send user-generated input to a program or device that causes it to do something it was not intended to. Sometimes this can be as simple as setting legitimate options in an unexpected combination, thereby causing the destination program to crash or hang. In other cases, the unexpected input could be executable code that attempts to cause the recipient to do what the attacker wants it to.

For this reason, it is recommended that external inbound connections are blocked wherever possible. The challenge for heavy trucks is that there are many possible ingress points for external input, and any of them can be an attack vector if they are processed digitally. Therefore, any device that accepts input and processes it digitally should attempt to filter out unexpected or unnecessary input signals. The following is a nonexclusive list of interfaces that may be integrated into telematics units or other ECUs:

- Data, SMS, and voice-over cellular or satellite.
- Wi-Fi, Bluetooth, near-field communication, proprietary radio frequencies (RF), dedicated short-range communications (DSRC).
- Universal serial bus (USB), serial debuggers, joint test action group (JTAG), CAN access.
- Digital radio, satellite radio, global positioning satellite (GPS).
- In-cab audio.
- Advanced driver-assistance system sensors—ultrasonic, video, LIDAR, radar, etc.

Where possible, external input should be cryptographically protected and verified (e.g., TLS protocol or other accepted authentication and encryption mechanisms).

[GDL 26] Filter input to any device or interface that gets digitally processed.

5.1.4 Limit Internal (CAN Bus) Access

Most telematics units have access to the in-vehicle CAN bus(es) so they can query diagnostic codes, retrieve information such as engine revolutions per minute (RPM) and fuel economy, and possibly modify firmware or data on ECUs, particularly the engine control module. This document recommends two classes of security controls for any

telematics unit, TCU, or IVI that has access to any CAN bus, even if they are segmented from safety-critical devices like brake or acceleration ECUs.

First, the CAN connection(s) should be secured using the methods listed above to prevent the sending of arbitrary CAN messages. If the telematics unit only needs to access diagnostic trouble codes (DTCs), then those codes should be enumerated in the software. Any other CAN messages shouldn't be allowed. If the use case for the telematics unit requires more than DTCs (the "unlock doors" command, for example), those can be added.

Of course, an attacker might gain the ability to modify or overwrite the OS and/or the firmware on the CAN controller, which could give him or her the ability to send arbitrary CAN messages. But disallowing this by default raises the bar for the attacker.

[GDL 27] Limit telematics units' access to the CAN bus, and whitelist the CAN messages they can send.

The second recommendation is to be very cautious about giving the telematics unit the ability to update firmware on other ECUs. While secure over-the-air (SOTA) updates can provide cost savings as well as the ability to quickly patch security vulnerabilities, they also provide a remote attack vector. A telematics unit should have a way to verify that an update is unquestionably authentic before the unit uploads the update to an ECU. Security of updates is covered in the Section 5.1.5, below.

5.1.5 Security Monitoring

One characteristic of telematics/IVI units is that they tend to have more processing power and a more robust operating system than single-purpose ECUs. This gives them more functionality to implement security controls but also provides more attack vectors. The IVI is also likely to be a primary target because of its remote and wireless connections. Therefore, monitoring the IVI for suspicious behavior becomes important. HIDS can alert drivers, mechanics, or fleet operators if the telematics system has been tampered with. The CERT Coordination Center is currently not aware of antivirus products being deployed on telematics units, but expect this to become common practice in the future. Warnings of unexpected or unusual network connections would also be valuable.

[GDL 28] Enable security monitoring of the telematics system(s) using native tools.

5.1.6 "Shadow" Telematics

Normally the telematics unit in a heavy truck will communicate with a back-end service via a TCU that's originally installed in the truck or installed with the telematics unit. However, there are aftermarket devices that perform some subset of telematics functions and communicate via Wi-Fi or Bluetooth to a smartphone or cellular-equipped tablet. We've dubbed these "shadow" telematics because they open the vehicle to the same risks as on-board cellular or satellite connections. An attacker could first compromise the paired device, possibly when it was not in the vehicle, and then communicate to the shadow telematics unit and the vehicle.

[GDL 29] Treat components that connect to both a mobile device and the vehicle as part of the system attack surface, securing accordingly.

5.2 ELECTRONIC LOGGING DEVICES

ELDs, which are required in many commercial trucks as of April 2018, replace paper or manual logs of hours of service (HOS), miles driven, rest stops, etc.

This information is valuable to both operators and adversaries, and is therefore a potential target. Worse, some of these devices report drivers' behavior and are therefore a prime target for insider threats. For example, one threat is drivers manipulating the information on how long they drove or whether they took mandated rest stops.

Most of the ELD units on the market are integrated with telematics units and include all the same risks and suggested mitigations as those. However, because of the insider threat posed by drivers, fleet managers, mechanics, etc., emphasis should be placed on securing the physical devices as well.

[GDL 30] If the device can be updated from local media (USB, secure digital [SD] cards, etc.), make sure the updates are digitally-signed and authorization is required.

[GDL 31] Make sure debugging interfaces (JTAG, serial, USB) have authentication required.

[GDL 32] Make sure local wireless interfaces like Bluetooth or Wi-Fi don't provide admin access without authentication.

5.3 SECURE OVER-THE-AIR SOFTWARE

As previously mentioned, the ability to perform over-the-air updates of components in heavy vehicles provides cost savings as well as the ability to quickly patch any security vulnerabilities that are discovered. However, they also open additional attack vectors, due to the need for loading new software, configurations, or data from the Internet. There is in-depth advice available for creating SOTA update mechanisms,[15] but the primary requirements are as follows:

[GDL 33] Make sure that the update has not been altered during transit (integrity).

[GDL 34] Make sure the update comes from a legitimate source (authenticity).

[GDL 35] Prevent the attacker from reinstalling a legitimate but known-vulnerable version (rollback attack).

[GDL 36] Make sure you can revoke and replace cryptographic keys.

5.4 INTERNAL NETWORKS

The internal networks of vehicles are difficult to secure because they are mostly based on the serial CAN protocol, which has no security built into it. Heavy trucks have an even bigger challenge because many of the bus messages are standardized by J1939. This makes it even more important to consider security in heavy truck design and assembly.

5.4.1 Segregation

One of the biggest security problems with the CAN bus is that any device on the bus can send messages to any recipient (a 29-bit CAN identifier in the case of J1939).

[GDL 37] It is recommended to isolate safety-critical ECUs on their own CAN bus, with some sort of gateway between them and other ECUs.

5.4.2 Authentication

There are challenges to using cryptographic authentication on J1939 messages due to limitations in the CAN protocol (8-byte frames) and in lower power ECUs (central processing unit, memory, storage). However, proposals exist for doing authentication, such as J1939-ACAN, which runs over CAN-FD (64-byte frames).[16]

[GDL 38] Consider adoption of authenticated J1939 components, particularly in safety- and security-critical components.

5.5 RADIO FREQUENCY INTERFACES

There are usually multiple RF interfaces on a heavy vehicle aside from the primary voice/data (cellular and/or satellite) connection. These may be built into the heavy vehicle or added by dealers, carriers, etc., in the form of aftermarket components. This document covers some guidelines for the most common and highest risk interfaces but cannot cover all possible protocols. Some guidelines are generalizable to all RF communications on the vehicle, and some are more specific.
It is not safe to assume that any communication channel is configured to be secure or is set to secure settings by default. Often RF communications channels are configured with minimal security to maximize ease-of-use for consumers. It is also important to note that devices may have RF functions that aren't documented in all cases. For example, some Wi-Fi and cellular devices also have a Bluetooth interface for debugging. For these reasons, the settings discussed in Section 5.5.1 and Section 5.5.2 should always be checked before deployment of any device with the respective capability.

5.5.1 Wi-Fi

Wi-Fi security is a large field, but the clear majority of Wi-Fi issues can be mitigated with a few guidelines.

[GDL 39] Only use Wi-Fi Protected Access 2 (WPA2) authentication/encryption. Never use Wired Equivalent Privacy (WEP), Wi-Fi Protected Setup, or "open" Wi-Fi.

[GDL 40] Always use a complex, unique password for each device.

Avoid using obvious sequences in the password, like your company name, a unit number, or a media access control (MAC) address.

[GDL 41] Don't allow a telematics unit to pair to Wi-Fi access points unless they're trusted (e.g., in your depot or motor pool).

5.5.2 Bluetooth

Bluetooth is often overlooked as it has limited range. However, for heavy trucks, it is not uncommon for a group of trucks to be gathered in one place and running or idling. Truck stops, depots, loading areas, travel centers, etc., would be ideal places for adversaries to attempt Bluetooth attacks. Below are the best practices for utilizing Bluetooth:

[GDL 42] Only allow pairing during device boot.

This limits the time during which the device is vulnerable to rogue pairing attempts. This feature needs to be built in to the device.

[GDL 43] Always use a complex, unique password for each device.

As with Wi-Fi, avoid using obvious sequences in the password, like your company name, a unit number, or a MAC address.

[GDL 44] Make sure Bluetooth devices support and use secure simple pairing (SSP) rather than legacy pairing.

Bluetooth introduced SSP in Bluetooth 2.1, which addressed many of the security issues in Bluetooth legacy (pre-2.1) pairing.

[GDL 45] Numeric comparison is preferred to passkey entry for pairing.

Passkey entry has known vulnerabilities.[(17)] This feature also needs to be built into the device.

5.5.3 General RF Interfaces

Other RF interfaces on heavy trucks may include DSRC, tire pressure monitoring, RF identification, and more. CERT has observed wireless CAN transceivers on construction vehicles. These interfaces are less standardized and often proprietary, so specific security controls may vary. In general, there are two things to look for when evaluating these interfaces: encryption and authentication. Both can often be tested with a software-defined radio (SDR).

[GDL 46] Use encryption on all wireless communication interfaces.

[GDL 47] Use authentication on all wireless interfaces.

5.6 KEY MANAGEMENT

One of the biggest challenges in cyber-physical security is managing security authentication tokens or keys. In this section, “key” refers to any sort of token that is used to prove identity, including but not limited to cryptographic keys.

5.6.1 Password Reuse

One of the most common problems is reuse of passwords across a line of devices, fleets, or multiple installations of a software package. Attackers are going to acquire software and firmware when planning an attack and extract any passwords they can identify. They

will then attempt to use these in an actual attack, especially if they know that a manufacturer or carrier uses the same password for multiple systems or vehicles. They will also try to find or sniff passwords on phones, tablets, and laptops they compromise. Password reuse increases the risk of insider threats, allowing drivers, mechanics, and others to access not only one vehicle but potentially many of them.

[GDL 48] Use a unique, complex password on each device, vehicle, or application.

[GDL 49] Change passwords from the manufacturer's default, and change them when personnel leave or change jobs (see GDL 9).

5.6.2 Incorrect Cryptography

Another common problem is when cryptography is implemented to provide encryption, integrity, and/or authentication, but is implemented improperly. This degrades or even eliminates any advantage from using cryptography. A common example is using TLS to encrypt information to a cloud provider, but not properly verifying the certificate to make sure it is valid for that provider.

[GDL 50] Have a third party check the implementation of any cryptography your security model depends on.

5.6.3 Root Certificate Authorities

A root certificate authority (RCA) is the entity that verifies cryptographic keys. Although any organization can verify (digitally sign) its own keys, it is common to use a third party to prove your organization has been at least minimally vetted. It is generally a good idea to only trust cryptographic keys signed by a reputable third-party RCA, but there are some security measures that should be implemented.

[GDL 51] Check whether keys have expired or been revoked.

Expiration dates are built into certificates (the signed form of a key), and reputable RCAs will have a method for revoking keys that have been compromised (for example, certificate revocation lists).

[GDL 52] Ensure the ability to remove a RCA's certificate.

Occasionally a RCA itself will be compromised, which means that no key the RCA has signed should be trusted. In this case, the certificate needs to be removed as a trusted source from any device, vehicle, or app that uses it.

5.6.4 Hardware Security Modules

The highest level of security is obtained with a hardware security module (HSM), which is a tamper-resistant device that stores encryption keys. Unfortunately, these add expenses and are logistically difficult to maintain or replace. The use of an HSM may be advised if the use case involves very expensive, dangerous, or sensitive cargo. SAE J3101 is a work in progress document with recommendations for hardware security in ground vehicle applications.

[GDL 53] Consider using hardware security modules if your threat model includes high levels of risk.

5.7 DEBUGGING AND DIAGNOSTICS

5.7.1 Disable Debugging

A frequent attack vector in embedded devices is a debugging service or physical interface that was used during development and never disabled. This could be a network service listening on the internet, a local serial port, or a JTAG interface on a circuit board. Disabling these decreases the attack surface and makes an attacker's job harder.

[GDL 54] Disable unnecessary debugging interfaces in production.

5.7.2 Authenticate Debug/Diagnostics Interfaces

For debugging or diagnostics interfaces that need to remain enabled for maintenance of the device or vehicle, use some form of authentication to prevent unauthorized modification. An in-vehicle example is the authentication provided by Unified Diagnostic Services (UDS), while a device-specific control might be simply requiring a password on a serial or USB connection.

[GDL 55] Authenticate debugging and diagnostic interfaces.

5.8 LOGGING

Security-relevant events both in the vehicle and in supporting infrastructure should be logged and digitally signed to be tamper-evident. This allows both proactive monitoring for unauthorized access and the ability to do forensics after a breach or crash. Some key events that should be recorded include:

- Remote access attempts and successes.
- Firmware, software, and data updates.
- Malformed requests.
- Local access and maintenance activities.

[GDL 56] Log security-relevant events.

[This page intentionally left blank.]

APPENDIX A: CHECKLIST

Table A-1. Cybersecurity checklist.

Guideline	Completed?
[GDL 1] Do architectural analysis and/or threat modeling during system design.	
[GDL 2] Follow secure coding best practices.	
[GDL 3] Perform adversarial testing before a product is finalized (OEMs) or before it is deployed (dealers/installers).	
[GDL 4] Security problems will happen; fail safely.	
[GDL 5] Perform a risk assessment before implementing any telematics or other sort of "connected" technology in vehicles.	
[GDL 6] Perform your own security due diligence, which involves but is not limited to ensuring that third-party devices in the supply chain meet your basic security requirements.	
[GDL 7] Obtain legal security guarantees that meet your minimum-security requirements for all products.	
[GDL 8] Decide early on who is in charge of creating, implementing, and maintaining software/firmware requirements for all products.	
[GDL 9] Reset default credentials, logs, fuses, etc. as soon as the device is received.	
[GDL 10] Publish a vulnerability reporting and disclosure policy.	
[GDL 11] Have a process for tracking vulnerability disclosures affecting devices being deployed in the fleet.	
[GDL 12] Security patches should always be deployed to fleet devices in a timely manner (also see GDL 8).	
[GDL 13] Share cybersecurity information with the heavy vehicle industry.	
[GDL 14] Employ an incident response process.	
GDL 15–19 left blank for future use.	
[GDL 20] Give applications the least privilege they need to function.	
[GDL 21] Where possible, remove code that isn't used.	
[GDL 22] Leverage security controls built into the operating system.	
[GDL 23] Follow best practices for securing cellular or satellite interfaces.	
[GDL 24] Don't support 2G on cellular modems unless operationally necessary.	
[GDL 25] Assume satellite communication channels have unknown security vulnerabilities and might compromised at any time.	
[GDL 26] Filter input to any device or interface that gets digitally processed.	
[GDL 27] Limit telematics units' access to the CAN bus, and whitelist the CAN messages they can send.	
[GDL 28] Enable security monitoring of the telematics systems(s) using native tools.	
[GDL 29] Treat components that connect to both a mobile device and the vehicle as part of the system attack surface, securing accordingly.	
[GDL 30] If the device can be updated from local media (USB, SD cards, etc.) make sure the updates are digitally signed and authorization is required.	
[GDL 31] Make sure debugging interfaces (JTAG, serial, USB) have authentication required.	
[GDL 32] Make sure local wireless interfaces like Bluetooth and Wi-Fi don't provide admin access without authentication.	
[GDL 33] The ability to know that the update has not been altered during transit (integrity).	
[GDL 34] The ability to know the update comes from a legitimate source (authentication).	

Guideline	Completed?
[GDL 35] Preventing the attacker from reinstalling a legitimate but known-vulnerable version (rollback attack).	
[GDL 36] The ability to revoke and replace cryptographic keys.	
[GDL 37] It is recommended to isolate safety-critical ECUs on their own CAN bus, with some sort of gateway between them and other ECUs.	
[GDL 38] Consider adoption of authenticated J1939 components, particularly in safety- and security-critical components.	
[GDL 39] Use only WPA2 authentication/encryption. Never use WEP, WPS, or "open" Wi-Fi.	
[GDL 40] Always use a complex, unique password for each W-Fi device.	
[GDL 41] Don't allow a telematics unit to pair to Wi-Fi access points unless they're trusted (e.g., in your depot or motor pool).	
[GDL 42] Only allow pairing during device boot.	
[GDL 43] Always use a complex, unique password for each Bluetooth device.	
[GDL 44] Make sure Bluetooth devices support and use Secure Simple Pairing (SSP) rather than legacy pairing.	
[GDL 45] Numeric Comparison is preferred to Passkey Entry for pairing.	
[GDL 46] Use encryption on all wireless communication interfaces.	
[GDL 47] Use authentication on all wireless interfaces.	
[GDL 48] Use a unique, complex password on each device, vehicle, or application.	
[GDL 49] Change passwords from the manufacturer's default, and change them when personnel leave or change jobs (see GDL 9).	
[GDL 50] Have a third party check the implementation of any cryptography your security model depends on.	
[GDL 51] Check whether keys have expired or been revoked.	
[GDL 52 Ensure the ability to remove a Root CA's certificate.	
[GDL 53] Consider using hardware security modules if your threat model includes high levels of risk.	
[GDL 54] Disable unnecessary debugging interfaces in production.	
[GDL 55] Authenticate debugging and diagnostic modules.	
[GDL 56] Log security-relevant events.	

REFERENCES

1. National Highway Traffic Safety Administration. (2016). Cybersecurity Best Practices for Modern Vehicles. Washington D.C.: Report No. DOT HS 812 333.
2. IEEE Center for Secure Design. (2017). Design Flaws and Security Considerations for Telematics and Infotainment Systems. Retrieved 10 17, 2018, from www.IEEE.org: https://cybersecurity.ieee.org/blog/2017/05/30/design-flaws-and-security-considerations-fortelematics-and-infotainment-systems/
3. National Highway Traffic Safety Administration. (2016). Cybersecurity Best Practices for Modern Vehicles. Washington D.C.: Report No. DOT HS 812 333.
4. IEEE Center for Secure Design. (2017). Design Flaws and Security Considerations for Telematics and Infotainment Systems. Retrieved 10 17, 2018, from www.IEEE.org: https://cybersecurity.ieee.org/blog/2017/05/30/design-flaws-and-security-considerations-fortelematics-and-infotainment-systems/
5. CERT. (2016). SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems. Pittsburgh, PA: CERT.
6. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Washington D.C.: NIST.
7. National Highway Traffic Safety Administration. (2016). Cybersecurity Best Practices for Modern Vehicles. Washington D.C.
8. National Highway Traffic Safety Administration. (2016). Cybersecurity Best Practices for Modern Vehicles. Washington D.C.
9. Householder, A., Wasserman, G., Manion, A., & King, C. (2017). The CERT® Guide to Coordinated Vulnerability Disclosure. Pittsburgh: CERT.
10. White House (2015) Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing. Washington. D.C: White House.
11. American Trucking Associations. (2018). ATA Fleet Cywatch. Retrieved 10 17, 2018, from: American Trucking Associations: https://www.trucking.org/fleet_cywatch.aspx
12. National Motor Freight Traffic Association, Inc. (2018). National Motor Freight Traffic Association, Inc. Retrieved 10 17, 2018, from National Motor Freight Traffic Association, Inc.:
13. Department of Homeland Security. (2018). US-CERT. Retrieved 10 17, 2018, from: US-CERT: https://www.us-cert.gov/
14. Klinedinst, D. (2017). Vulnerability Note VU#251927. Retrieved 10 17, 2018, from: https://www.kb.cert.org/vuls/id/251927
15. FASTR Connectivity and Cloud Work Group. (2018). Automotive Industry Guidelines for Secure Over-the-Air Updates. Retrieved October 17, 2018, from Future of Automotive Security Technology Research: https://www.fastr.org.
16. Murvay, P., & Groza, B. (2018). Security Shortcomings and Countermeasures for the SAE J1939.

17. Barnickel, J., Wang, J., & Meyer, U. (2012). Implementing an Attack on Bluetooth 2.1+ Secure Simple Pairing in Passkey Entry Mode. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 17-24.