Commercial Vehicle vs. Automotive Cybersecurity – Commonalities & Differences

André Weimerskirch, Steffen Becker, and Bill Hass

1 Introduction

Automotive cybersecurity is becoming increasingly important, especially in the age of information and connectivity as vehicles' capabilities are becoming more and more connected. While automotive cybersecurity has been around since the 90's as part of theft protection, odometer manipulation, and chip tuning, it recently gained a new level of attention as cybersecurity breaches have been shown to impact the safety of passenger and commercial vehicles. Over the last five years, it has been repeatedly demonstrated that it is possible to hack into passenger vehicles to modify driving behavior or to locate and steal the vehicles. Such attacks have been demonstrated by research teams that hacked built-in vehicle interfaces, and that hacked into OBD2 (on board diagnostic) dongles with wireless capabilities that are plugged into vehicles. Then in 2015 the first research about hacking commercial vehicles was released to show that commercial vehicles are prone to similar vulnerabilities and can potentially be compromised.

Over the last years, many processes and technologies were developed for automotive cybersecurity. This chapter will provide a background of passenger vehicle cybersecurity and commercial vehicle cybersecurity, and describe what the commonalities are, how automotive cybersecurity solutions can be applied for commercial vehicles, and where there are limitations and differences. The chapter at hand will focus on technical solutions only, and we refer to Chapter XXX for an overview of the equally important cybersecurity engineering process. The scope for commercial vehicles in this chapter is comprised of medium-duty and heavy-duty trucks and off-road heavy-duty vehicles, which also includes agricultural and construction

vehicles and possibly military vehicles.

2 Background

In the past fifteen years, research on automotive cybersecurity has shown a multitude of vulnerabilities affecting safety-critical features such as steering, braking, and acceleration as well as security features such as unlocking and starting a vehicle. Several sophisticated attacks combine these vulnerabilities with remote exploits leading to a full attack chain, where an attacker can manipulate the driving behavior of a vehicle remotely. Furthermore, in the past two years, findings in the area of commercial vehicle cybersecurity indicate the potential for comparable attacks. The most important publications and their results are discussed in this section.

In 2002, a study by the National Highway Traffic Safety Administration (NHTSA) revealed that around 3.5% of all passenger vehicles are affected by odometer manipulations during their lifetime, costing their purchasers an estimated amount of 1 billion US-Dollars every year in the US alone [N02]. Also, the authors state that fleet vehicles are eminently affected because they typically accumulate a high mileage in a short period of time which makes odometer rollback more believable to a potential buyer. While there are increasing efforts on the regulatory side to prevent odometer fraud, technical solutions to cryptographically secure odometer readings are still not widely implemented. Therefore, many detailed manuals available on the Internet continue to enable criminals to conduct odometer manipulations on a variety of vehicles. This is a prime example of illegal cybersecurity activities due to a financial gain.

Researchers from the University of Washington and the University of California, San Diego were the first to demonstrate safety-critical automotive vulnerabilities in 2010 by sending malicious in-vehicle network messages, so called CAN messages, to the in-vehicle network of a modern automobile [KCR+10]. Assuming direct access to the in-vehicle network (i.e. through the on-

board diagnostics port), they could control the speedometer and instrument cluster display, and, even more worrisome, they could stop the engine from running and disable or individually control the brakes. Then, in their subsequent work in 2011, the authors conducted an experimental analysis of potential attacks via remote communication interfaces [CMK+11]. In that work, they gained full access to the in-vehicle network of a modern automobile utilizing three different remote attack vectors: the CD-player via a manipulated mp3 file, the telematics unit via Bluetooth, and the telematics unit via the cellular network. Besides the potential injection of malicious CAN messages they pointed out location tracking, theft and wiretapping as other arising threats.

In 2014, private researchers developed several attacks on the in-vehicle network of two modern cars, affecting the dash display, the steering behavior, as well as braking and acceleration [VM14]. Contrary to former publications, the authors explained their methods in detail, including source-code and information on the hardware, software, and payloads used. One year later, the same authors published and publicized the first, complete, end-to-end compromise of a passenger vehicle. The results of their work caused the recall of 1.4 million vehicles [MV15]. A port left open by the cellular network provider allowed access to a service used for inter-process communication in the vehicle's head unit over the Internet. From there, a chip could be reprogrammed to send out arbitrary network messages. In a demonstration for the press, the researchers controlled both the climate control and the radio systems overriding the driver's inputs, turned on the windshield wipers, and eventually cut the transmission causing the vehicle to decelerate on a highway [WM15].

In 2015, a popular aftermarket insurance dongle, which connects directly to the in-vehicle network, was examined by researchers from the University of California, San Diego [FPK+15]. A minor discovery by the researchers revealed a common cryptographic key and administrative username and password among all devices they tested enabling secure login after a device was

discovered. However, the devices they studied were indirectly protected from such remote compromises because the cellular carrier implemented network address translation (NAT) which maps Internet addresses to local network addresses, hence preventing the devices from being addressable outside of the local network. Their major discovery revealed the ability to issue remote updates from an arbitrary server using cellular text messages SMS. With the SMS attack vector, they demonstrated the dongle's concrete susceptibility to remote attacks by demonstrating its discovery on the cellular network, issuing a remote update from their rogue server, and a targeted compromise to send arbitrary in-vehicle network messages that controlled both the wipers and brakes.

A private research group demonstrated vulnerabilities of an automotive vehicle using more advanced networking technologies beyond CAN in 2016 [KSL16]. Utilizing a series of exploitable bugs they accessed the car's infotainment system via the Wi-Fi network and remotely activated the brakes of a moving vehicle. The OEM was informed and fixed the underlying vulnerabilities before the exploits were disclosed to the public.

Other crucial, yet not safety-critical cybersecurity research in the automotive domain includes several key fob and immobilizer hacks. An immobilizer is an anti-theft device that prevents the engine from starting when the corresponding transponder (i.e. key fob) is not in range. In 2010, researchers from ETH Zürich used techniques to emulate or extend the range of the key fob transponder using relay attacks to enter and start vehicles from over 50 meters away, non line-of-sight [FDC10]. In 2013, it was shown that over 100 models from 26 car manufacturers were susceptible to so-called "digital lock picking" when researchers published that they completely reverse engineered the most widely deployed immobilizer at the time. The design of the particular immobilizer studied made use of a weak proprietary stream-cipher, suffered from weak entropy of their secret keys, and did not have memory protected from being written remotely. Consequently, the researchers could unlock and start the vehicles they studied. Other key fob and

immobilizer attacks are summarized in [GOK+16]. The authors disclosed different vulnerabilities in keyless entry systems of major vehicle manufacturers affecting millions of vehicles worldwide. The found weaknesses enabled the researchers to gain unauthorized access to the affected cars. These studies depict an obvious potential for car theft if exploited by criminals, and unsurprisingly there have been many reports of car thefts where the attackers enter, start, and drive away with a vehicle that was previously locked by the owner. It was repeatedly shown that tools to undermine key fob security can be put together at low cost, e.g., as reported in [WM17].

Recently, the first academic papers on commercial vehicle cybersecurity were published. In 2014, researchers from the University of Tulsa checked various electronic control units (ECU) for their cryptographic methods to establish forensic soundness and integrity of collected incident data, often used to support the reconstruction of accidents [JDK14]. See the University of Tulsa paper in Chapter XXX. They concluded that many implementations allowed the modification of incident data, and they proposed the deployment of cryptographic primitives such as hash functions as a solution. They created a test bench for truck ECUs so that they could perform tests and conduct their analysis without needing a large, expensive heavy-duty truck. This idea resulted in their subsequent work in 2016 where they aimed to build a prototype of a remotely accessible testbed for experimentation with security features [DGM+16]. The researchers added real ECUs and nodes simulating sensor inputs required by the controllers to accurately emulate a real truck network. To demonstrate the capabilities of their testbed, they conducted two sample experiments: Generating a look-up table (LUT) for a 16 bit challenge-response-protocol and testing of an intrusion detection system.

Additionally, in 2016, researchers from the University of Michigan performed an experimental security analysis of a real heavy-duty truck and passenger bus vehicle network [BHM+16]. In their work, the authors assumed physical connection to the vehicle bus through the on-board diagnostics connector, and they discovered that similar attacks against automobiles in 2010 were

directly applicable to commercial vehicles. A minor discovery let them gain full control over the instrument cluster to let the gauges display arbitrary values. Their major discovery identified a single message in the SAE J1939 CAN standard that affected both the truck and bus. The message could be utilized by a malicious party to deactivate the acceleration pedal, max out the current gear by raising the RPM, prevent the truck from accelerating by lowering the RPM, and turn off the engine brake at speeds under 30 miles per hour. Besides the potential injection of malicious CAN messages, they provided evidence that all vehicles utilizing J1939 would be affected and that the prevalence of third-party telematics units that plug into vehicle networks provides a unique threat to the commercial vehicle industry.

3 The Automotive and Commercial Vehicle Environment

The automotive and commercial vehicle environment are similar in many aspects and widely different in other areas. The following paragraphs compare the passenger vehicle and commercial vehicle space.

3.1 Supply Chain

In the passenger vehicle space, the OEM is the owner of security and designs the vehicle's security concept. The OEM then specifies requirements for all suppliers, and the OEM is the sole integrator of all suppliers' components. There is only little variation for each vehicle model, and often components are shared between vehicle models.

In the commercial vehicle space, there is a huge number of variations per model. For instance, buyers can typically choose a particular engine, transmission, and even control modules. Furthermore, OEMs often don't build the entire truck, but they provide the chassis to a bodybuilder, and the bodybuilder then adds mechanical and electrical components for specialized functions, e.g., as they are needed for a garbage truck. The role of aftermarket equipment that directly plugs into the communication bus (CAN) is also much larger in the commercial vehicle

space. For instance, a majority of trucks are equipped with aftermarket fleet management solutions.

The supply chain model dictates that passenger vehicle architectures have a single security owner, namely the OEM and that the system can be closed-up. Whereas commercial vehicles have several security owners, including OEM and bodybuilder, hence requiring more open security architectures.

3.2 In-vehicle Network Architecture and Communication

Related to the supply chain models is the in-vehicle network architecture. Both passenger vehicles and commercial vehicles heavily use the Controller Area Network (CAN) and communication gateways to separate networks. Passenger vehicles are about to introduce Ethernet networks, and it's only a matter of time until commercial vehicles will also widely introduce Ethernet.

A difference between passenger vehicle and commercial vehicle network architecture is that commercial vehicles are typically longer on the road and hence older, leading to network architectures in commercial vehicles that do not offer network separation and that appear to be outdated. Another difference is that commercial vehicle network architectures must be open for bodybuilder integration, whereas no such open interfaces need to exist in the passenger vehicle domain. Note that there is often an exterior CAN network access, e.g. between tractor and trailer, where an adversary might hook-in, whereas such exterior access points are typically not available in the passenger vehicle space.

A majority of vehicles use CAN. While passenger vehicles use standardized CAN on the physical level with standardized packet structure, the semantics of CAN packets is proprietary. This even applies to vehicle models from an OEM that use different semantics. Commercial vehicles use the

standardized SAE J1939 protocol that specifies a common CAN semantics. While an adversary needs to reverse engineer CAN messages for a passenger vehicle to cause an impact, the CAN message semantics for commercial vehicles is public and applies to almost all commercial vehicles.

3.3 Telematics

Telematics is widespread in the commercial vehicle space, and a survey of a small sample size indicates that more than 90% of all trucks have remote communication systems installed, and a part of those systems directly integrate to the vehicle's electronics [N15]. Many of these telematics solutions come as part of aftermarket fleet management solutions. While telematics is also becoming increasingly popular in the automotive space, commercial vehicle fleet operators are typically willing to make larger investments into telematics since it will enable cost-savings. Especially aftermarket telematics systems are susceptible to security vulnerabilities, as CERT has demonstrated [CERT16].

3.4 Maintenance and Diagnostics

Passenger vehicles are typically serviced by dealerships and workshops that use original car maker tools. Commercial vehicles are either serviced by dealerships and workshops, or they are serviced in-house by trained technicians that utilize OEM tools. The distinction is less between passenger vehicles and commercial vehicles than it is between individually owned vehicles and fleet owned vehicles in both categories. Fleet owned vehicles need to be serviced in an open manner by any technician, possibly with original OEM tools, e.g. to swap mechanical and electronic components. The ability of everyone to service vehicles is legally mandated by the Right to Repair Act in the US which applies in similar form also to most European countries. Note that this makes cybersecurity in the passenger vehicle and commercial vehicle space very different than cybersecurity in other domains since it requires a certain system openness and

accessibility.

Diagnostics commands are used to troubleshoot vehicles and to change the configuration of electronic components, or even update the firmware of electronic components. Diagnostic commands were also shown to be vulnerable to hacker attacks, e.g., to turn-off an electronics component or enter modes that are only for a standing vehicle but that are dangerous for a vehicle in motion. It is possible to protect diagnostics commands against adversaries by introducing proper plausibility checks in the vehicle (e.g. not allow potentially dangerous test operations while the vehicle is moving), by securing the diagnostics tools properly, or by requiring a secure online connection of the diagnostics tool to the OEM's server.

3.5 Emerging Technologies

It is widely believed that many emerging technologies, such as advanced driver assistance systems (ADAS) and automation will first be widely deployed in commercial vehicles. ADAS is being widely deployed in passenger vehicles and NHTSA includes automatic emergency braking (AEB) as a recommended safety technology in its 5-star rating system. These technologies can save cost due to a reduced accident rate or reduced rate of operation, hence commercial fleet operators are willing to invest significant amounts per vehicle in emerging technologies. At the same time it appears that the automotive cybersecurity community had a head-start to the commercial vehicle cybersecurity community, hence exposing emerging technologies to commercial vehicle security concepts that are not as mature as security concepts from the automotive domain.

4 Vehicle Threats and the Cyber Attacker

Commercial vehicle and automotive platforms have been developed to meet the needs of a nearly disjoint set of customers with the former being highly diverse and specialized, and the latter generally focused on individual transportation. Still, despite the differences in their requirements,

the two have shared various technologies as they have evolved leading to many similarities in offensive techniques. This section describes the threat model, attackers, and offensive techniques to consider in the commercial and automotive cybersecurity settings.

4.1 An Evolving Threat Model

When the CAN network was designed in the 1980's, a vehicle's communication network was assumed to be isolated from the rest of the world. The threat model focused on criminals that would break in and hot-wire a vehicle or somehow physically access and tamper with a vehicle's components. So vehicle defenses both in commercial and automotive sectors relied on hardening of physical attack surfaces to reduce the threat posed by an adversary, and the CAN network had no built-in security measures because it was protected by physical defenses.

Throughout the 1990's and 2000's, the threat model assumptions did not change, but the vehicles did. In automotive markets, consumers demanded more electronic features they grew accustomed to from consumer electronics. The automotive OEMs also saw potential to differentiate and provide safer vehicles for their customers through the use of electronics. On the other hand, while commercial vehicle technologies lagged behind their automotive counterparts in connected driver convenience, the cost-saving benefits of integrated fleet management systems accelerated the adoption of GPS and cellular network connected vehicle components.

Then, as vehicles in both areas became more electrified and eventually wireless, the threat model shifted from completely physical to cyber-physical. What was once an isolated, insecure CAN network is now connected with the outside world.

Today, the threat model assumptions have drastically changed and expanded. Beginning in the US in model year 1996, light-duty passenger vehicles required on-board diagnostics (OBD) for emissions testing which introduced a easily accessible standard connector located within the

cabin of the vehicle. The OBD connector is meant to give access to particular emissions related ECUs such as the engine's, but it is common for OEMs to wire OBD directly to the internal CAN buses with other ECUs because it enables convenient vehicle diagnostics for mechanics at a low cost.

Similarly for commercial vehicles since 2010 [E10], highway heavy-duty vehicles require OBD for emissions, and OEMs utilize the standardized port for other functions on the CAN network related to diagnostics. Because the OBD port is located within the cabin of the vehicle, it is protected by a layer of physical security which includes door locks and alarms, but a proper threat model does not make this assumption. On the automotive side, there are new and used car buyers, valets, employees (e.g. taxi or delivery service), mechanics, renters, and ride-sharing services, while on the commercial vehicle side there are passengers, employees (e.g. truck or bus drivers), mechanics, and renters who gain access to the inside of the cabin with varying degrees of access time. It has been demonstrated that even with a short amount of access time, sometimes referred to as a "lunch-time" attack in the IT community and "valet" attack in the automotive community, a malicious component can be plugged into the vehicle's OBD port either temporarily or left there to compromise safety critical functions.

Furthermore, in both vehicle environments, drivers or vehicle owners willingly plug third-party electronics into their OBD port for some benefit at the cost of an increased attack surface or may even bridge networks that OEMs originally intended to be segregated. Many devices exist with different benefits: vehicle monitors from insurance companies; fleet telematics systems; aftermarket backup cameras, GPS monitors, crash detectors, and performance monitors; and generic interface devices that provide wireless input and output to the OBD port from a smartphone or other connected device.

Some notable examples have led to the remote compromise of a vehicle. One such example is an

automotive insurance company that provided lower insurance rates for drivers that plugged a wireless dongle into their OBD port, but that device was later shown to enable remote CAN network injection by attackers [FPK+15]. Another example is a third-party commercial vehicle fleet telematics system with cellular and GPS capabilities that was used in hundreds of commercial vehicles, but it was installed with an open telnet connection accessible on the Internet from across the globe [N16]. In these two instances, a key difference with commercial vehicles is that fleet owners don't really have much of a choice when it comes to the use of telematics systems if they want to be competitive and increase safety for their drivers, and similarly drivers need to comply with their company policies.

Finally, an important difference between automotive and commercial vehicle physical attack surfaces is that with commercial vehicles there are external network entry points for things such as trailers, container ship hook-ups [RBB+07], or specialized mechanical equipment attachments that need to be considered as potential avenues for attack.

Beyond physical network entry points, more and more ECUs are being integrated into safety critical systems so there is a need to ensure the modules themselves are secured. Starting at a vehicle's infancy, the confidentiality of cryptographic keys and integrity of ECU software must be maintained from the early stages in the supply chain, to the time that ECUs are installed in a vehicle, and throughout the 10+ year life of a vehicle. Additionally, various wireless components are now added standard in passenger vehicles and often added to commercial vehicles in different industries. Therefore, wireless attacks against the vehicle must be considered from short-range (up to 10m, e.g., Bluetooth), medium-range (up to 1,000m, e.g., WiFi and vehicle-to-vehicle dedicated short-range communication), and long-range (beyond 1,000m, e.g., cellular and GPS). Furthermore, with today's semi-autonomous features already deployed, the attack surface has grown to include vision, radar, and LiDAR sensors.

4.2 The Adversary

It is common knowledge that the CAN protocol is insecure, and there are many low-cost software and hardware tools available that let anyone communicate on CAN. Furthermore, the commonplace reliance on electronics by governments, corporations, and individuals has spawned an arms race between white hat and black hat cybersecurity professionals resulting in the development and release of techniques that can compromise a broad range of general electronic systems. Such techniques can either be directly applied or adapted in such a way to be used against both commercial and automotive vehicle systems.

We can imagine various potential attackers on the automotive and commercial vehicle infrastructures. On the one hand there are sophisticated, large-scale attackers such as criminal groups developing for the black market or nation-state sponsored groups developing cyber weapons. These attackers possess almost unlimited resources, are able to engineer and deploy different exploits at scale, and penetrate dealerships, mechanics, or supply-lines. On the other hand, there are freelance or rogue attackers with varying levels of privilege and expertise. These attackers have much less resources and a lesser extent of their influence, but could obtain tools from the black market. While the motivation for either type of adversary consists of the threat potential, which comes with damaging a single vehicle, causing a death, paralyzing the freight industry, or damaging critical infrastructure, it generally understood that the most common motivation is financial.

Whether large-scale or small scale, an adversary will get access to a similar vehicle to the one they are targeting for an extended time to learn the function, features, and attack vectors. Additionally, due to the privileged features that diagnostics sessions enable, an adversary will obtain diagnostics tools for feature exploration, reverse engineering, and exploitation. A difference here between commercial and automotive environments is that a typical commercial vehicle is an order of magnitude costlier than an average consumer automobile which raises the

barrier of entry of a would-be attacker. Nonetheless, tools developed by a more motivated or well-funded attacker can be sold for much less, and exploits against the J1939 standard found in commercial vehicles would work across vehicles and industries amortizing the cost of developing an attack. See Chapter 2, “Should We Be Paranoid”, for more information.

4.3 Offensive Techniques

In both automotive and commercial vehicle industries, the approach of an attacker depends on their goals, and their goals will fall into one of several categories that make up a complete attack chain: remote exploit, CAN access, diagnostic session initiation, and module reflashing. Each stage of the attack chain can be developed or purchased independently and assembled piece-wise as required.

For remote exploits, there are many different types of devices and attack vectors to consider. In many cases, third party devices run a variation of Linux which has its own set of exploits from the IT domain that could carry over. These devices are much less expensive than a vehicle so many can be purchased for hardware reverse engineering with low overhead. Through hardware reverse engineering, an attacker could determine things such as the computer architecture, types and manufacturers of chips, and find debug pins to gain access to memory. The computer architecture provides a map for an attacker, and the types of chips give valuable information about embedded features and whether there might be a hardware exploit already available. With a memory dump, an adversary could perform static analysis to determine control flows or read cryptographic keys and passwords.

An attacker can also use the administrative tools and regular use-case tools marketed to customers such as web portals and smartphone apps to probe for security vulnerabilities. For example, a phishing attack could be crafted with knowledge of the admin tool web portal to attempt to gain privileged access to fleets, or a smartphone app could expose remote vulnerabilities on the back-

end services. Additionally, an attacker could use a low-cost software defined radio and other wireless capture devices to sniff and transmit packets for analysis of the remote channels.

The techniques just described for exploiting a wireless interface are borrowed from the traditional cybersecurity domain which has had a long past of vulnerabilities. Recent attacks against Android, iOS, and embedded Internet of Things (IoT) devices are a good indicator that no wireless interface is 100% secure. If a remote exploit is found that enables arbitrary code execution and the device has a CAN interface, it's likely the attacker will be able to perform arbitrary CAN packet injection remotely. The same principle holds for vehicles whose networks use some underlying protocol other than CAN. We will focus on CAN based network attacks due to the popularity and prevalence of CAN in both commercial and automotive vehicles.

With arbitrary CAN packet injection, an attacker needs to understand the topology of the network in order to craft a targeted attack. Under the assumption that an attacker has access to their own similar vehicle, network topology is determined through physical observation. Furthermore, a CAN injection attack can be developed apart from a wireless exploit by simply clipping a low-cost CAN tool into the same bus or buses as the remote device that will be exploited. Some vehicle architectures utilize a single CAN bus which makes it easy for an attacker to influence all of the ECUs. Others use several buses, but bridge them together using a wireless gateway which can still enable an attacker to influence all of the ECUs once the wireless gateway is compromised. Yet others use several buses and segregate wireless devices from the rest of the ECUs with a bridge or gateway. Just as in the traditional IT domain, network segregation can greatly limit the potential damage caused by the security failure of a single component.

Once attached to the network, a first step might be to flood the CAN bus with traffic to perform a denial of service. In most cases, vehicles are engineered to handle a loss of CAN communication or a flooded CAN bus, but this type of attack can put a vehicle into a "limp" mode that decreases

performance proving to be hazardous if at high speed. A next step would be to record network traffic during various driving conditions and while utilizing features that interface with safety critical or physical security components. An attacker could then try replaying messages that were recorded to see if there is any component susceptible to replay attacks. In [BHM+16] this method found a message capable of controlling engine RPM, preventing the driver from using the accelerator, and degrading engine brake performance in commercial vehicles. Another technique, termed fuzzing, uses randomized permutations of data to send over the network. This type of attack can expose corner cases where modules behave erratically or aid in reverse engineering packet structure. In [KCR+10], it was discovered through fuzzing that the brakes could be engaged or prevented from being engaged while their car was in motion. More complex CAN network interactions can be reverse engineered to influence safety critical systems. For example, through ECU impersonation, a series of commands sent from the engine to the transmission that cause the transmission to shift could be sent from the exploited module instead. Or a handshake between a telematics unit and body controller could be spoofed to issue a door-unlock or start-engine command.

As mentioned earlier, a reasonable, motivated attacker would obtain a diagnostics tool for reverse engineering diagnostic commands. Diagnostics tools are a major area of interest for attackers because they enable special features that affect safety critical components such as brakes, engine, transmission, and body controllers, and also allow ECU parameters to be configured or memory to be read and written to. Typically, diagnostics commands are protected by a layer of security that only allows authorized mechanics to perform the diagnostics functions. An attacker might first explore the diagnostics software user interface and attempt to exercise all the possible diagnostics commands while collecting network traffic. Then, the attacker can try to replay the diagnostics commands to see if they are vulnerable to simple replay attacks. Next, the attacker might perform analysis on the diagnostics software that interfaces with the diagnostics tool to see if cryptographic keys can be easily obtained or if there are any weaknesses in back-end services.

Then, depending on the attacker's skills they might try to perform hardware reverse engineering on the target ECU, perform a memory dump using the diagnostics tool and analyze the firmware for exploits, or perform network protocol analysis on the diagnostics commands to measure the security level protecting the commands. Many authentication protocols used to secure these functionalities have been shown to be insecure due to flawed algorithms, insufficient key lengths, vulnerable implementations, or no security whatsoever. In one case, a single CAN message could be replayed to reset the master password protecting the diagnostics session for a commercial vehicle ECU. In another commercial vehicle instance, only 16-bits were used in a challenge-response protocol, so [DGM+16] generated a 16-bit look-up table and were able to bypass the security to access diagnostics commands. Similarities appear in the automotive environment. In [KCR+10], they found a hard-coded, static challenge and response and instances where the handshake was ignored altogether.

If the security of diagnostics commands can be successfully bypassed, it oftentimes lets an attacker flash code onto an ECU. With this ability, it is still necessary for the attacker to reverse engineer the update process and firmware already running on the ECU. Once that is complete, however, an attacker could write arbitrary software that does several things then erases itself after being executed making forensics very difficult. Additionally, this type of software could be used for spying, as a back-door for later exploits, or to bridge internal vehicle networks as part of a link in the attack chain.

5 Cybersecurity Approaches and Solutions

There are a variety of cybersecurity approaches and solutions available for the commercial vehicle domain. It appears that the majority of solutions come from other domains, in particular the automotive domain. However, some adjustments will be necessary to account for the unique features of the commercial vehicle space.

5.1 Legacy Vehicles

It is very hard, if not impossible, to improve the cybersecurity features of commercial vehicles that are already on the road today. A promising approach to stop the most likely attack scenario is to either not connect vehicles with known vulnerabilities to the Internet via a fleet management solution, and to turn-off all wireless interfaces, or to include a filter between all external communication interfaces and the vehicle's electronics network.

The following paragraphs describe cybersecurity solutions that need to be planned for and included in the vehicle's electronics architecture.

5.2 Network Architectures and Separation

Modern network architectures separate networks by gateways and implement firewalls and filters between network segments. Such networks are typically separated in a way that no network with external interfaces directly connects to a safety-critical network, such as the powertrain network, but that all communication is routed through a gateway with a firewall first. There might be dedicated networks that only connect two nodes, e.g., between an ADAS controller and a camera. Note that even in the case of commercial vehicles, such dedicated private networks do not need to implement the SAE J1939 standard since there is no need to extend such network segments at any time.

The automotive space already moves towards the next architecture of domain controllers, where there are only a few powerful domain controllers, typically connected by Ethernet, and each domain controller connects to basic electronics components. The same paradigm of network separation for security purposes applies for the domain controller architecture.

5.3 Secure On-board Communication

A major security objective is to introduce security of the on-board communication. In almost all cases, authentication is the required security objective, but in a few cases also encryption is interesting. In the following, we focus on authenticated on-board communication. Such authenticated on-board communication makes it much harder for an adversary to advance further. For instance, if an adversary successfully compromised a telematics unit or an OBD dongle, the attacker is only able to authenticate messages to components on a pre-defined list but, if properly designed, not to authenticate messages sent to any safety-critical component.

The passenger vehicle space uses a variety of on-board communication networks, including CAN, CAN-FD, Ethernet, and Flexray. For low-bandwidth communication bus like CAN, which has a payload of up to 8 bytes per packet, introducing authentication is difficult. Nonetheless, AutoSAR specified a standard for CAN authentication called secure onboard communication (SecOC) [WHF+15], and Volkswagen announced that they will start deploying authenticated CAN [T16]. It appears though that different car makers go different paths and start introducing proprietary solutions for CAN authentication. A communication bus with more bandwidth, such as Ethernet or CAN-FD, allows to use either standardized or straight-forward solutions, such as IPsec for Ethernet and a regular Message Authentication Code (MAC) for CAN-FD.

The SAE J1939 communication standard for commercial vehicle is based on CAN, hence authenticated CAN approaches such as the AutoSAR standard could be applied as well. Any security standard for commercial vehicles would need to be standardized though. The hard problem behind the standardization is not necessarily the format of the CAN messages but the underlying key management. While this applies to both the automotive and commercial vehicle world, the key management problem is significantly harder in the commercial vehicle world. For passenger vehicles, the OEM is the sole owner of security and is able to specify and require a particular key management scheme, and the OEM is able to control all suppliers accordingly. In

the commercial vehicle space, a proper key management system needs to be both open enough to account for the supply chain model, but also restrictive enough to avoid that illegitimate parties can learn secret keys. This appears to be not as much a technical problem as an organizational issue, and any solution will reduce the openness of the supply chain model since there needs to be a trusted party that controls which components are able to communicate on the SAE J1939 communication bus. As of today, no such solution is available, however, the authors believe that it should be a high priority to introduce authentication in SAE J1939 and mandate the use thereof.

5.4 Secure Computing Platform

Electronic components in vehicles require a secure computing platform. A secure computing platform uses mechanisms such as secure boot to protect integrity at start-up, hypervisor or software containers with secure inter-process communication to separate software components, and a hardened kernel as well as memory protection (e.g. address randomization) to protect the kernel. Mechanisms that allow to monitor the integrity of the computing platform are available as well, e.g., by using a whitelist of binary files that are allowed to be executed. Note that the whitelist includes integrity information about those binaries, e.g., by hashing binaries before executing them. It appears that security solutions of secure computing platforms are equal for the automotive and commercial vehicle domain.

5.5 Anomaly Monitoring

Protecting a vehicle against cybersecurity attacks and extraction of data is a priority. The ability to monitor the vehicle's network and computing platforms is a second priority to understand potential breaches and continuously improve cybersecurity. The output of on-board network anomaly detection systems and ECU platform integrity monitors can be merged, used for local anomaly detection and possibly leads to a basic local reaction, and then provided via telematics to a Security Operations Center (SOC) which then runs analytics over all data to find anomaly

patterns in the big picture. This information is then provided to the car makers and suppliers, who then analyze the information and start the incident response process. Note that a real-time reaction is unlikely but a reaction that eventually updates firmware or configuration in the vehicle within days or weeks is realistic.

Network anomaly detection systems (ADS) monitor the on-board communication, such as CAN, CAN-FD, and Ethernet, and compare the message traffic to a learned traffic pattern. Such an ADS is ideally installed in a central gateway to monitor a variety of network segments. It is possible to connect an ADS to a message filter that discards messages and raises an alarm, however, due to the real-time and safety relevance of messages this scenario is unlikely. A far more realistic scenario is that ADS is only used for monitoring in order to provide input to the SOC. An ECU monitor is basically an extension to a secure computing platform that cannot only stop an attack but also report the attack.

It appears that an anomaly monitoring system is the same for passenger vehicles and commercial vehicles. In fact, since the commercial vehicle space uses standardized CAN messages, it might be easier to realize ADS in the commercial vehicle space.

5.6 Security Operations Center

The security operations center (SOC) receives reports from the network anomaly detection systems and ECU platform integrity monitors of vehicles. The SOC then takes these reports, analyzes them, and finds relationships between reported incidents. Automated algorithms find certain patterns, and then human analysts explore details to understand whether filtered incidents relate to cybersecurity incidents, other anomalies, or false alarms. Once an actual cybersecurity event is confirmed and the mechanisms are understood, the underlying system can be fixed and software can be updated via firmware over-the-air mechanism. Naturally, an SOC works more effective the more reports from different vehicles it receives.

It appears that SOC for passenger vehicles will work differently to an SOC for commercial vehicles. Passenger vehicles are mainly closed systems, so the SOC could be under control of individual car makers. Some synergies might be possible if car makers collaborate and combine their SOCs, however, this doesn't seem to be necessary. Commercial vehicles are open systems and it appears quite necessary to combine the expertise of the OEM, suppliers, fleet operators, and aftermarket solution providers in a single SOC to be successful. Of course, with the landscape constantly changing, commercial vehicles could become more closed systems, hence approaching the model of the automotive manufacturers. Note that today no such SOCs are deployed, and more research must be performed and experience has to be gained to better understand the use of SOCs in the ground vehicle transportation sector.

5.7 Secure Firmware Over-the-Air

Firmware over-the-air (FOTA) is used to update features and fix bugs, some of which might be security relevant. FOTA has the potential to reduce the number of recalls and hence it is a widely discussed topic. There are numerous examples though when such FOTA mechanisms have been hacked in the PC network world. A good example is the Flame malware that used a combination of cryptographic vulnerabilities to then hijack the Windows update mechanism to distribute malware [G12].

Software updates are typically protected by digitally signing the updated firmware such that an ECU will only update with the received firmware if the verification is successful. The code is signed by the OEM and/or supplier, ideally using a secure computer that is offline and that is not easily accessible. A secure communication channel, such as the widely-deployed transport layer security (TLS) between cloud and vehicle can further increase the security level. The Uptane framework for secure FOTA further increases the security and separates roles of the involved entities such that if a single server is compromised, the overall system can still recover [KBA+16].

6 Gaps and Conclusions

Recent research results demonstrated that cybersecurity is not only relevant for passenger vehicles but also for commercial vehicles. With the rapidly increasing push to deploy automation in commercial vehicles, and the expectation that heavy truck fleets might deploy fully automated vehicles first, cybersecurity issues will become increasingly important.

The passenger vehicle and commercial vehicle domains can learn a lot from each other. In fact, the Auto-ISAC which was established by passenger vehicle manufacturers was just opened up to include commercial vehicle stakeholders [P17]. It is expected that many of the cybersecurity engineering processes and technical solutions can be utilized by the commercial vehicle domain. The ideas of threat analysis, risk assessment, secure development, security testing, and incident response apply to both the passenger vehicle and commercial vehicle industry. Also, technical solutions such as secure firmware over-the-air, network anomaly detection, and platform security can be applied in a similar manner as technologies are shared among industries.

However, there are also areas that require different solutions due to the differences of the passenger vehicle and commercial vehicle industry. A good example is secure CAN. Car manufacturers are the security owners of their vehicles and can specify proprietary protocols to protect their in-vehicle networks and, more importantly, key management systems. In the commercial vehicle domain on the other hand, strict standards are required to bring together all the various stakeholders in order to overcome the obstacle that commercial vehicles are an open system. In the long term, passenger vehicle and commercial vehicle industries will likely come together in such areas as well since passenger vehicles will, with increased resources such as offered by automotive Ethernet, also switch to standardized technical solutions.

References

[BHM+16] Yelizaveta Burakova, Bill Hass, Leif Millar, and André Weimerskirch, *Truck*

Hacking: An Experimental Analysis of the SAE J1939 Standard, 2016, available at https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf

[CERT16] Dan Klinedinst and Christofer King, *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle, 2016,* available at https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

[CMK+11] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 2011, available at http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[DGM+16] Jeremy Daily, Rose Gamble, Stephen Moffitt, Connor Raines, Paul Harris, Jannah Miran, Indrakshi Ray, Subhojeet Mukherjee, Hossein Shirazi, and James Johnson, *Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls*, 2016, available at http://papers.sae.org/2016-01-8142/

[E10] Environmental Protection Agency, Code of Federal Regulations (Annual Edition), Title 40, Volume 18, Chapter I, Subchapter C, Part 86, Subpart A, Sections 86.010-18 and 86.007-17, 2010, available at https://www.gpo.gov/fdsys/pkg/CFR-2010-title40-vol18/pdf/CFR-2010-title40-vol18-part86-subpartA.pdf

[FDC10] Aurélien Francillon, Boris Danev, and Srdjan Capkun, *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars,* 2010, available at http://www.syssec.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/spot/332.pdf

[FPK+15] Ian Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage, *Fast and*

Vulnerable: A Story of Telematic Failures, 2015, available at http://www.autosec.org/pubs/woot-foster.pdf

[GOK+16] Flavio D. Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès, *Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems*, 2016, available at https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

[G12] Dan Goodin, *Crypto breakthrough shows Flame was designed by world-class scientists, Ars Technica*, 6/7/2012, available at https://arstechnica.com/security/2012/06/flame-crypto-breakthrough/

[JDK14] James Johnson, Jeremy Daily, and Andrew Kongs, *On the Digital Forensics of Heavy Truck Electronic Control Modules*, 2014, available at http://papers.sae.org/2014-01-0495/

[KBA+16] Trishank Karthik Kuppusamy, Akan Brown, Sebastien Awwad, Damon McCoy, Russ Bielawski, Cameron Mott, Sam Lauzon, André Weimerskirch, and Justin Cappos, *Uptane: Securing Software Updates for Automobiles*, escar Europe, 2016.

[KCR+10] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, *Experimental Security Analysis of a Modern Automobile*, 2010, available at http://www.autosec.org/pubs/cars-oakland2010.pdf

[KSL16] Keen Security Lab, *Car Hacking Research: Remote Attack Tesla Motors*, 2016, available at http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[MV15] Charlie Miller and Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at http://illmatics.com/Remote%20Car%20Hacking.pdf

[N02] National Highway Traffic Safety Administration, *Preliminary Report: The Incidence Rate of Odometer Fraud*, April 2002, available at https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/809441

[N15] National Motor Freight Traffic Association, *A Survey of Heavy Vehicle Cyber Security,* September 21, 2015.

[N16] J. C. Norte, *Hacking Industrial Vehicles From the Internet,* March 6, 2016, available at http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

[P17] PR Newswire, *Commercial Vehicles to Join Auto-ISAC*, 2017, available at http://www.prnewswire.com/news-releases/commercial-vehicles-to-join-auto-isac-300396844.html

[RBB+07] L. Ruiz-Garcia, P. Barreiro, J. Rodriguez-Bermejo, and J. I. Robla, Review, *Monitoring the Intermodal, Refrigerated Transport of Fruit Using Sensor Networks,* Spanish Journal of Agricultural Research, 2007, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.978.6151&rep=rep1&type=pdf

[T16] Alexander Tschache, *Vehicle security from the OEM perspective: Securing in-vehicle communication – challenges and workable solutions*, escar Asia, 2016.

[VGE13] Roel Verdult, Flavio D. Garcia, and Barış Ege, *Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer*, 2013, available at https://www.usenix.org/sites/default/files/sec15_supplement.pdf

[VM14] Chris Valasek and Charlie Miller, *Adventures in Automotive Networks and Control Units*, 2014, available at

https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

[WHF+15] Philipp Werner, Armin Happel, Ralf Fritz, Steffen Keul, *AUTOSAR Security Modules, escar USA 2015, available at https://vector.com/portal/medien/solutions_for/Security/AUTOSAR_Security_Modules_Lecture_ESCAR_2015.pdf*

[WM15] Wired Magazine, 2015, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, available at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[WM17] Wired Magazine, 2017, *Just a pair of these $11 Radio Gadgets can steal a car*, available at https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car

About the Author

Steffen Becker received the B. Sc. and M. Sc. degrees in IT Security from the University of Bochum. During his graduate studies he spent two semesters as a research assistant and exchange student at the Department for Electrical and Computer Engineering, Purdue University, and was a visiting scholar at the transportation cyber security group, University of Michigan Transportation Research Institute (UMTRI). Steffen is currently pursuing the Dr.-Ing. degree with the embedded security group at the University of Bochum, under the supervision of Prof. C. Paar. His research interests include automotive cybersecurity, as well as hardware Trojans and obfuscation.

Bill Hass received the M. Sc. Eng. degree in Computer Science and Engineering from the University of Michigan in 2017. During his graduate studies, he was a research assistant in the cyber security group at the University of Michigan Transportation Research Institute (UMTRI) where he developed a key management system for an automotive OEM, co-authored a security research paper on the commercial vehicle network standard, SAE J1939, and was involved in automotive intrusion detection system testing. Prior to graduate school, Bill received the B. Sc. Eng. degree in Electrical Engineering from the University of Michigan in 2013 and was a product development engineer at Ford Motor Company for two years

Dr. André Weimerskirch is VP Cyber Security at Lear Corporation. Before that, André established the transportation cyber security group at the University of Michigan Transportation Research Institute (UMTRI), and co-founded the embedded systems security company ESCRYPT which was sold to Bosch in 2012. André is active in all areas of automotive and transportation cyber security and privacy, he is a main designer of the vehicle-to-vehicle security system, which will likely be the largest security system ever deployed, published numerous articles in the area of automotive and embedded cyber security, and is co-founder of the American workshop on embedded security in cars (escar USA). André is

involved in various standardization, cooperation and research efforts. André can be reached at aweimerskirch@live.com.

Revised 5/27/17