Vehicle Security Systems

CIS 481-50

8/6/2021

Team 3

Vilde Kiste Bryne, Addie Cengic, Anthony Basil and Alexander Tran

Table of Contents

Executive Summary

Purpose:

The purpose of this research report is to highlight aspects and issues regarding vehicular information security. With our findings, we hope to bring awareness to what needs to be changed and for the better as vehicular security is essential for millions of daily users who drive a car, travel by train or airplane as well as truckers.

Problem:

The problem is that our findings show that vehicular security needs a serious overhaul. This is a significant issue because millions of people in the US alone drive some type of vehicle for daily transportation (unless he/she lives in an area where public transportation is the norm). With knowing the fact that millions of users drive a vehicle, with this statistic being known (with the fact that vehicular security needs an overhaul), this proves it is a significant issue as this puts millions of users at risk.

Problem Analysis:

Fundamentally, the vehicular security systems for cars/trucks/airplanes/trains need a bit of an overhaul. Most systems used for all the modes of transportation are either obsolete, unprotected, or not having enough development for a proper security system. With that said, there needs to be made some changes that are for the better.

Results:

Fundamentally, the vehicular security systems for cars, trucks, airplanes, trains are in need of an overhaul. Cars are always coming off the line every year with new designs, just like a new iPhone, so you can imagine how difficult it is to keep security up when the new model comes off the line so quickly. Not to mention that car manufactures do not implement security at the beginning stages. Railway systems have high costs, obsolete controls, and not enough experts in the field to really bring about change for the better. Lastly, the issues found with trucks are mostly from a lack of any security measures not being placed to begin with.

Recommendation:

Look back at the fundamentals on how each security system for each mode of transportation developed in the first place. With that first step, then apply modern practices on how to develop better security controls.

Introduction

As we move toward more complex controls in information and cyber security, vehicular security systems have faced their own set of issues. Problems relating to security systems in vehicles could have long-term implications on the well-being of daily users. Since cars and trucks are controlled by the average person daily for transportation, individual users have control of which car and truck they drive which allows them to avoid purchasing certain models that have safety concerns. However, there are also other modes of transportation such as airplanes and trains that are beyond the control of the average person. While these modes of transportation can be more common in other parts of the world (trains and public transport are more common in Europe as opposed to living in the United States of America), commuters have little control in which model of train or plane that he/she opts for during their travels, as all control lies within railway and airline companies. This places a greater ethical responsibility on railway, airline, car, and truck transportation companies to ensure that the vehicles they use follow stringent security standards to maintain not only the safety of their passengers but the safety of their services. All vehicular companies have an ethical and legal responsibility to prioritize, frequently review, and update their security standards as new threats are constantly emerging. The current security systems architecture for vehicles needs to be re-designed with the most updated security standards to resolve this dilemma.

Universal concerns pertaining to vehicular security systems as well as vehicle-specific concerns are listed below. We hope that once awareness has been made, the suggested solutions are taken into consideration in order to implement better security. We also hope that this will be set into motion sooner rather than later. The approaches we have performed to prepare for the presentation and the report were through coordinated meeting times and designated reviews.

Cars

Through the years cars have gotten more and more connected which poses several issues that will be discussed, one of the biggest issues is software. The issue with software is created from the fact that in the auto industry, functionality is valued over software security. This is an evident fact by the amount car manufactures allocate to cyber security in their budgets. Since cyber security is an afterthought, security testing and vulnerability identification is rushed through in the last stages. If car manufacturers do not make a change this will pose a serious risk as autonomous cars approach the market. They need to constantly develop security patches and deploy them in a timely manner as technology is never at a standstill and new threats enters the market just as fast as new technologies. (Tech Wire Asia)

The infotainment system in cars is an example of how modern software security is not taken into consideration. The infotainment system contains unencrypted data such as call histories, text messages, emails, and other sensitive information about the car's owner. The car's infotainment system is powered by Linux's operating system and leveled with the bash command line shells which can be hacked remotely by hackers (Goud). Through the method of social engineering, code can be executed on the car's infotainment system by connecting a USB flash drive with specially crafted scripts. These files are automatically picked up and executed with full administrative privileges. This malware can leverage SMS on the driver's phone to block phone calls and to access banking authentication pins (Lin). Moreover, the entire system is rendered unusable by the driver as it is controlled remotely by SMS (Short message service).

In 2015 hackers discovered a vulnerability in the Uconnect system in Chrysler vehicles, they used this vulnerability to cut out the transmission, and brakes in a jeep Cherokee. When the car was in reverse, they could command the steering wheel. This was all done without physical access to the car. The Uconnect system had no apparent firewall, so all hackers had to do was find the devices IP, deploy precisely developed exploits to rewrite the systems firmware and control the car. Fortunately for car owner there was soon a patch that was quickly released to fix this issue (Greenberg).

Cars today can contain over 100 million lines of code, where a great deal of that software is new. This is a big area of concern as the more lines of code the greater the chance of an error. Car manufactures could make software with higher quality and reliability by eliminating redundant code, keeping it to the lines of code that is necessary and repeatedly test and scrutinize the code. Unfortunately, the auto industry is no way near this level, like the aircraft manufacturers are.

There are many ways a car can be hacked as seen in appendix 1 and the ones that are relevant today will be covered and solutions will be offered in the next few paragraphs. One way a can be hacked is through wireless key fobs as traditional metal car keys are becoming obsolete and wireless key fobs and virtual keycards continue to rise in popularity. The wireless key fob transmits a unique low range frequency that is sensed and validated by the car's computer. Signals between a car and a car's computer system can be intercepted by car thieves if the owner is near the car (Galinas). Thieves can use a cheap radio amplifier to extend the range of the signal and to emulate the owner's wireless key fob. The car's computer system is then tricked into believing that the owner is nearby with the key, allowing thieves to access the car. In order to prevent car hacking that occurs through emulation of a car's signal, car manufacturers should focus on improving encryption on their key fob radio frequencies. In 2018, researchers from Belgium announced they were able to copy a Tesla key food by wirelessly read signals from a nearby key fob then clone a copy of it. Tesla introduced more encryption but still a year later with closer proximity to the fob and a little more time It could still be performed wirelessly without the owner knowing. Tesla was able to patch the issue as soon as news of the hacks surfaced. DoS attacks can also be used to exploited this by disabling the key fob and learn the sequence of Data. (Torbet)

Apps for connected cars could be exploited for personal information about the car owner. In 2016, a Nissan Leaf in the United Kingdom was hacked all the way from Australia as the Nissan Connect smartphone app only needed the VIN (Vehicle Identification Number) to take control over the car. A car's VIN is its unique identifier assigned by its manufacturer. With the VIN, the hackers could access details about where the car recently had been driven and although this don't have any effects on the road, but it could lead to homes being broken into

or a coordinated hijacking. Just like with the wireless key fob, your vehicle could be stolen by intercepting communication between the car and the owner's smart phone. (Holmes) And as mentioned earlier, hackers could gain access to the devices you have paired with the vehicle like your smart phone.

The telematics data server is by some people referred to as the weakest link in connected cars. Cars generates terabytes of information as the vehicle collect information about every detail of the vehicles like from steering wheel to fuel consumption and even the exact pressure applied on the breaks. Telematics and its application servers don't only collect telematics data, but it can also send certain commands. In the wrong hands, commands such as igniting the engine or turning it off, locking and unlocking doors can be executed. (upstream)

As of May 2018, most of the common car models use come with a "black box" which is formally called an event data recorder (EDR). This records a lot of data and in many cases without the knowledge of the owner (Jones). This means that everything you do after getting behind the wheel is recorded, every button you press, every decision you make. It records whether you used a seatbelt, you brake and blinker usage, your travel speed, etc. This data is stored in the black box and is easily available after a crash. It was initially meant as a tool to help researchers and car manufacturers gather data on the systems meant to avoid car crashes and people dying. Currently however, this information can be used against you in court, as local police departments are now able to retrieve and analyze the data in the black box. (Medvin) This is a scary thought as the data does not provide a complete picture of what really happened. The holes left by the black box data are than allowed to be filled by the jury's interpretation. These holes can cause several issues as the driving pattern before the black box recording is one of the holes, the black box does not tell the story of what happened prior. The accused could have been driving just as they were supposed prior the accident, but this unfortunately wouldn't have been recorded as the black box only retains a few seconds of the vehicle movements in memory. (Jones)

Vehicle to everything (V2X) is a technology that allows vehicles to communicate with the moving parts around them in traffic. One component of V2X is Vehicle to vehicle (V2V) communication which allows vehicles to wirelessly exchange information about position and

speed to other vehicles. This technology enhances current avoidance systems that uses radars and cameras to detection possible collisions. Another component is vehicle to infrastructure (V2I), where V2I lets cars communicate with external system, this includes, buildings, streetlights and moving parts such as pedestrians and cyclists. This technology is pretty new, and the full benefits will not be utilized until the market expands, and the extends of threats that this system may face will also not be realized until a market expansion. However, if car manufactures continue to put security last especially for a system like this, there definitely is a chance that a bad actor can find a way to utilize this to their benefit and wishes (Segal).

Fortunately, cars can be protected by keeping the system up to date, avoid third party stems, limit access and install a firewall. Set on automatic updates for your car as car manufactures send out important patches and updates to solve the system vulnerabilities. Download only apps and tools that are approved by the manufacturer of the car as installing third party apps and software can create vulnerabilities and put your car at risk. Only give people you trust access to your car and hide the Wi-Fi code and turn the cars wi-fi and so that people cannot discover the network in public places. Bluetooth should also be turned off when not in use. By installing an embedded firewall in your car, you can block unauthorized communication with the cars in board computers. An effective firewall filters both vehicle-to-vehicle and vehicle-to-everything communication so that only those that are authorized can communicate with the car (Ali).

Aircraft

Although there have yet to be any confirmed cases of successful cyberattacks on aircraft information systems, the avionics industry face various vulnerabilities to their information security and passenger safety. Such vulnerabilities include threats to infotainment systems, malicious software, obsolete legacy systems, failure to implement updates, and communication interference. The future of flight safety is dependent on the remediation of vulnerabilities in connection with the advancement of cyber threats.

Billions of people around the world use Panasonic Avionics' infotainment and communications systems during their flights. They are one of the largest suppliers of

infotainment and communication systems used by several major airlines. Security researchers discovered that Panasonic's infotainment systems were riddled with dangerous vulnerabilities. The main source of these vulnerabilities is the physical connectivity of different aircraft domains.

The aircraft domain should include the physical control system and should be separated from the passenger domain. However, this does not always seem to be the case. The aircraft domain and the passenger domain are most interconnected via optical data diodes and electronic gateway modules. If these two domains are physically connected, an attack is theoretically feasible. After gaining access to the infotainment system, a potential hacker could spoof crucial flight statistics like altitude, map routes, and speed on passenger displays (Kovacs). These holes could also allow the hacker to manipulate the pressure altitude, lighting, or first-class actuators.

Passenger data could also be compromised due to flaws within the automatic payment systems that is built into the infotainment system. Many passengers rely on these systems for their in-flight food and entertainment. In some instances, a hacker could access credit card information stored in the automatic payment system (Kovacs). Passenger privacy could be breached even further as more personal information can be captured through frequent flyer membership details. A cybersecurity attack on sensitive passenger information can potentially harm the safety of passengers, cause emotional distress, tarnish the airline's reputation, and lead to substantial financial losses across the entire avionics industry.

A key component of aircraft systems are gate links, which transmit data collected in the plane's black box between the airplane and the airport while the aircraft is at the gate (Krause & Marinos, 2020). These gate link systems are used to update passengers on arrivals and departures, while providing feedback on the most recent flight data to air traffic control (ATC). If not properly protected, the data in transmission could be altered or tethered to malicious code. A worm could spread to other systems within this network, causing irreparable damage to the airport operations that keep passengers safe. If the functions that ATC use to maintain safe airspace are compromised, planes could end up crashing into each other. Using a dynamic packet-filtering firewall on the trusted network would implement a layer of security that reacts

to abnormal traffic patterns of data in transmission. A worm hidden in a packet being transmitted to the aircraft would be detected by the firewall, which would in turn quarantine the attack. Through the Cybersecurity Awareness Symposium, the Federal Aviation Administration (FAA) regularly conducts vulnerability scans and penetration tests on network systems to identify potential vulnerabilities, including threats to gate link systems (Cybersecurity Testing).

Another key component of aircrafts, as seen in appendix 2, is the Aircraft Communications Addressing and Reporting System (ACARS unit). The ACARS unit is used for the exchange of messages between the aircraft and ground stations via satellite or radio (Skybrary). It is also used to provide pilots with potential routes that they can follow and report major flight phases to ground air traffic control. It is important that the aircraft and ground stations can exchange timely, accurate messages with one another in order to increase the level of safety and reduce the possibilities of a lone accident or a collision with other planes. Despite this, the ACARS unit does not encrypt messages which creates several vulnerabilities (Mehta). This allows any individual with the proper tools to eavesdrop and send messages between the aircraft and ground stations. Using the ACARS unit, a computer security consultant was able to hack into the airplane's onboarding system and upload flight management data. After gaining access to the aircraft's computer, he was able to mess with the direction that it was steering in while it was in auto-pilot mode. A remote hacker being able to manipulate flight communication and control the direction of the plane can have devasting consequences.

Part of the problem in avionics with protecting data in transmission is that original legacy systems were not built to withstand present cybersecurity threats. Because the information systems that keep airplanes relatively safe are complex and highly specialized, updates to protect against vulnerabilities are slow-moving. "[Modifying] one line of safety-critical flight software can take a year and cost around one million dollars due to the amount of testing and review that is generally required," (Krause & Marinos). When patches are available, analysts must ensure the updates are free of vulnerabilities. Since patches to outdated systems often involve connecting previously isolated systems to the internet, aircrafts are increasingly at risk of threats. Luckily, the FAA provides oversight into the implementation of security controls

to legacy systems. Industry standards from the FAA provide governance on the patching of vulnerabilities while updating obsolete systems, requiring manufactures to comprehend all regulations.

Communication via global positioning systems (GPS) have progressively posed problems to the FAA as well. Radio frequency transmitting devices can either intentionally or unintentionally interfere with communications between aircrafts and ATC. For example, in 2018 a passenger flight got lost in cloudy conditions due to military tests. Even though this was an unintentional jam, and the airplane was able to land safely, the use of radio frequencies proves to be a major issue facing aircraft security systems (Harris). In 2020, the FAA announced that it is the responsibility of the aviation security industry to mitigate GPS jamming. The FAA also hasn't implemented regulations to keep individuals from using automatic dependent surveillance-broadcast (ADS-B) to intercept aircraft data (Ramsdell, 2018). As seen in appendix 3, from a ground station individuals can use ADS-B devices to collect sensitive data from aircrafts that's in transmission. With the present technological constraints framing information systems, radio frequencies that have the potential to impact systems using airplane GPS need to be, at a minimum, moderately regulated by the FAA so as not to perpetuate the growing safety concerns.

Railway Fleets

The railway industry faces many challenges to the security of their infrastructure and confidential information, while the demand for reliable supply chains and accessible public transportation fuels the need for increased cybersecurity in railroads. The main issues facing railways in remediating vulnerabilities include the high developmental costs, governmental interference, outdated controls, and lack of expertise in the field (Liveri, Theochariduo, Naydenov, & ENISA).

The use of railways requires the modification of the surrounding environment. Land must be developed to make use of secure railroads, land which has been predominantly untouched prior to planning. "Land acquisitions for railway transportation projects also require high cost, government clearance, and PPP (public-private partnership) agreements," (Railway

Cybersecurity Market by Type, Offering, Security Type, Application, Rail Type and Region). Working with government entities can also be very political, often requiring different standards of implementation with varying costs. For example, countries in Europe and Asian have different standards for the track gauge. A gauge is the measured spacing between the rails. A train traveling from China to Germany would have to switch between various gauge requirements on its commute (The Geography of Transport Systems). Since a lot of railways cross governmental borders, cohesion between many involved parties requires additional layers of infrastructure that most other vehicular security systems do not face. Professional communication between all components is the steppingstone for implementing and modifying security controls in the railroad sector.

Once railways have been laid, the information technology governing the security of physical and logical assets take over. Railroads began their lifecycle in the mid 1800's, requiring modifications to enhance the safety of passengers and cargo ever since. Replacing tracks and other physical infrastructure components is time consuming and, sometimes, feasibly unrealistic. The introduction of technological advancements in the mid-to-late 1900's that integrated AI, predictive maintenance, black boxes, and data transmission with railroad legacy systems has been a costly endeavor as well (Railway Cybersecurity Market by Type, Offering, Security Type, Application, Rail Type and Region). Combining physical and logical security infrastructure updates with governmental interference has imposed a competitive disadvantage for railways systems in the vehicular security industry.

Predominantly reactive, the railway industry is often ill-prepared to handle novel threats. Insufficient funds prevent the operator of essential services from gaining the expertise needed to combat evolving cybersecurity threats (Liveri, Theochariduo, Naydenov, & ENISA). Operators typically react to emerging events in real-time, leaving less room for planning. With the 24-hour news cycle and public disclosure regulations, breaches in security are more difficult to hide than in the 1800's. The railroad industry has faced backlash in its inability to plan for disaster recovery. To ensure logical security controls are adequate in mitigating cyberthreats, experts must undergo rigorous training and obtain the necessary skills to monitor and detect

vulnerabilities. The industry should lobby local governments into providing the necessary funds to maintain the supply chains that rely on the security of railways.

Truck Fleets

While on the road, believe or not, truckers are immersed in technology that is not just their vehicle. As a part of their job, truckers use their phones, GPS, dash-cams, ELDs (electronic logging devices), and dispatch for communications. GPS is essential to track the driver and their cargo. Dash-cams are essential for visual proof of perspective on the road if any incidents occur. Lastly, dispatch is needed for real-time communication with all drivers. (Stella)

As the trucking industry improves its logistical process, so too does the technology used for it. Previously, GPS and dispatch for communications were built as separate systems, but as cellular devices become more advanced, it became possible to combine these 2 systems into one. I was able to talk to several drivers who have made a career out of being on the road, expediting shipment to confirm this practice. While these 2 systems can be used on 1 platform, a dash-camera and ELD are separate.

An Electronic Logging Device (ELD or E-Log) is an external system attached to a commercial motor vehicle engine to record driving hours. The driving hours of commercial drivers (truck and bus drivers) are typically regulated by a set of rules known as the hours of service (HOS) in the United States and as drivers' working hours in Europe. The Commercial Vehicle Driver Hours of Service Regulations vary in Canada and the United States. (Sridhar)

The ELD monitors a vehicle’s engine to capture data on whether the engine is running, whether the vehicle is moving, distance driven, and duration of engine operation. This type of information is valuable because it shows where the vehicle is, so any cyber-criminal interested in this could track vehicles to intercept their shipment (like in action films) or to scalp products as there is a massive issue with scalping GPUs. (Sridhar)

Modern ELDs now include a GPS to make the amount of hardware used in the interior of the truck more streamlined. As mentioned before with cellular device technology progressing, it is possible to have several of these systems into 1 device (usually the driver’s personal

cellphone can have the GPS/dispatch). As stated before, as far as ELDs and dash-cam are implemented, these 2 systems are built separately.

Ransomware is also an issue in the trucking industry. Oftentimes, this is an issue with the smaller companies, but it is still a severe issue. According to an article from Transport Topics, “Although the ELD mandate seeks to provide safety and efficiency benefits, it does not contain cybersecurity requirements for manufacturers or suppliers of ELDs, and there is no requirement for third-party validation or testing prior to the ELD self-certification process.” With this said, according to an article from Freight Waves, “Often it’s the smallest carriers that have the weakest defenses, and they get breached.” and lastly “Small businesses are the most common victims. Their systems generally are less well protected, and the disruption from a successful attack can make them all too willing to pay if it means the difference between staying in business and going under.” This is proof that ELDs need protection now more than ever to prevent ransomware attacks on businesses, no matter the size (Tabak).

A solution for some of these dilemmas would be use of Radio Frequency Identification (RFID). It is a wireless technology that can be used for data entry and authentication. In the trucking industry, it is still a working concept but a concept that will alleviate much stress in the future. (Vartak, Patwardhan, Joshi, Nagy)

Conclusions

Humans have implemented and used vehicles as their primary method of transportation for 200 years. When vehicular systems first came to the market, the primary focus was on physical infrastructure and function. As incidents occurred, and the definition of a vehicle broadened, security controls were added to vehicles to maintain the safety of passengers and cargo. Today, vehicles spread across numerous markets and must abide by safety procedures and security constraints that have expand into information technology. Although cars, plans, trains, and trucks are relatively safe modes of transportations, these industries need to adopt additional techniques to protect their assets and the public.

Based on our findings, the aviation security industry needs to relocate the physical control domain from the passenger domain to the control domain, encrypt ACARS units, and

protect against GPS and ABDS-B interference. The FAA provides broad, and sometimes inadequate, oversight into the functions of aircraft security. As advanced as they may be with technology, the industry needs more regulation from the FAA to sustain the integrity of their vehicles.

From our research, we concluded that car manufacturers need to include security considerations at the start of their planning phase instead of as an afterthought. In the car security industry, software development is more concerned with function rather than security. Many aspects of cars represent a large attack surface, with many vulnerabilities only being addressed after a breach occurs. A lot of car software is new, complex, and difficult to modify. Car manufacturers need to limit the lines of code in their software to what is necessary, which will reduce vulnerabilities. They also need to make wireless key fob and mobile key encryption stronger so that an outsider can't intercept communication between a car and its computer. Cars should be equipped with firewalls as they include on-board wi-fi and Bluetooth which creates several many access points that could be exploited.

Upon investigation, our team found that railway fleets suffer from old infrastructure, various differing physical requirements, and lack of capability. Being the first to emerge as a vehicle, a lot of the physical components of rail tracks are obsolete relative to today's security standards. Modification is expensive and must abide by conflicting specification as borders are typically crossed. The industry also lacks in expertise compared to other vehicular security systems, placing them in a competitive disadvantage. The advancement relies heavily on local governments to provide necessary funds.

After examination of findings, we assert that ELDs used in truck fleets need a security blueprint to protect against external threats. ELDs are used to monitor, store, and transmit data found within a truck's information system to help regulate operators and diagnose functionality issues. The attack surface on ELDs is fairly large because cybersecurity requirements are not required for manufacturers. ELDs are a known vulnerability to the security of information systems within the trucking industry and need to include security controls to defend against attacks.

Although much thought and consideration have gone into the planning and implementation of safety controls in vehicular security systems, our conclusion is that many of the associated industries are ill-equipped to handle evolving threats and must put safety in the forefront of all considerations.

Appendices.

Appendix 1.

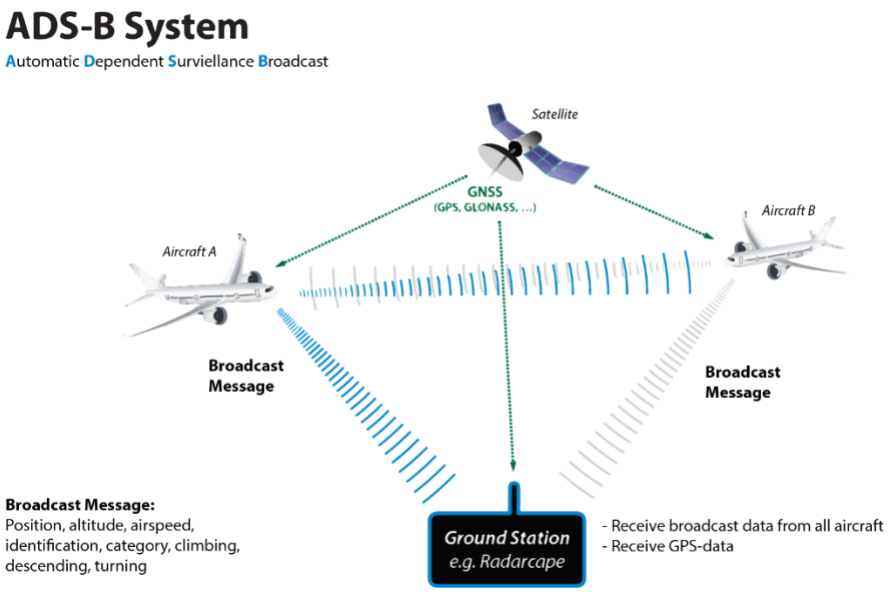
A picture showing different ways a car can get hacked.

Appendix 2.

This is a visual representation of the ACARS system used by aircrafts for communication and navigation purposes.

Appendix 3.

ADS-B radio frequency transmission diagram between aircrafts, satellites, and the ground station.



Citations:

Harris, Mark. “FAA Files Reveal a Surprising Threat to Airline Safety: the U.S. Military's GPS Tests.” *IEEE Spectrum*, IEEE Spectrum, 3 July 2021, https://spectrum.ieee.org/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests

Liveri, Dimitra, et al. “Railway Cybersecurity - Security Measures in the Railway Transport Sector.” Nov. 2020, www.enisa.europa.eu/publications/railway-cybersecurity/at_download/fullReport

Marinos, Nick, and Krause Krause. “Aviation Cybersecurity - FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks.” Oct. 2020, www.gao.gov/assets/gao-21-86.pdf

“Railway Cybersecurity Market by Type (Infrastructural & On-Board), Offering, Security Type (Network, Application, Endpoint, System Administration and Data Protection), Application (Passenger & Freight), Rail Type and Region - Global Forecast to 2027.” *Railway Cybersecurity Market*, MarketsandMarkets, July 2021, www.marketsandmarkets.com/Market-Reports/railway-cybersecurity-market-128598673.html

Ramsdell, Kellyn Wagner. “Few Answers for ADS-B Security Concerns.” *Aviation International News*, 14 Feb. 2018, www.ainonline.com/aviation-news/business-aviation/2018-02-14/few-answers-ads-b-security-concerns

Rodrigue, Jean-Paul, et al. Routledge, 2020, *The Geography of Transport Systems*, https://transportgeography.org/contents/chapter7/transborder-crossborder-transportation/aurasian-landbridge/

Gelinas, James. “Security Flaw in Key Fobs Lets Hackers Unlock Your Car.” *Komando.com*, 8 Mar. 2020, www.komando.com/news/car-key-fob-hack/710010/.

Tong, Lin, and Chen Luhai. Intel, July 2018, events19.linuxfoundation.org/wp-content/uploads/2018/07/ALS19-Common-Attacks-Against-Car-Infotainment-Systems.pdf .

Goud, Naveen. “Car Infotainment Systems Trigger Cyber THREAT SCARE.” *Cybersecurity Insiders*, 31 May 2018, www.cybersecurity-insiders.com/car-infotainment-systems-trigger-cyber-threat-scare/.

Kovacs, Eduard. “Panasonic in-Flight Entertainment Systems Can Be Hacked: Researcher.” *SecurityWeek*, 20 Dec. 2016, www.securityweek.com/panasonic-flight-entertainment-systems-can-be-hacked-researcher.

“Skybrary Wiki.” *Aircraft Communications, Addressing and Reporting System - SKYbrary Aviation Safety*, 5 July 2021, www.skybrary.aero/index.php/Aircraft_Communications,_Addressing_and_Reporting_System.

Mehta, Tej. “Cyber-Security: An Increasing Concern for Airlines.” *LinkedIn*, 18 May 2018, www.linkedin.com/pulse/cyber-security-increasing-concern-airlines-tej-mehta.

Jones, Willie. “The Automotive Black Box Data Dilemma.” *IEEE Spectrum*, IEEE Spectrum, 29 July 2021, spectrum.ieee.org/the-automotive-black-box-data-dilemma.

Medvin, Marina. “Your Vehicle Black Box: A 'Witness' against You in Court.” *Forbes*, Forbes Magazine, 8 Jan. 2019, www.forbes.com/sites/marinamedvin/2019/01/08/your-vehicle-black-box-a-witness-against-you-in-court-2/?sh=51079a4e31c5.

Torbet, Georgina. “Are Teslas Secure? How Hackers Can Attack Connected Cars.” *MUO*, 15 Oct. 2019, www.makeuseof.com/tag/tesla-secure-hackers-connected-cars/.

Ali, Fawad, and Fawad Ali (13 Articles Published) . “4 Ways Your Car Can Be Hacked and How to Prevent It.” *MUO*, 19 Apr. 2021, www.makeuseof.com/ways-your-car-can-be-hacked-prevent-it/.

“Securing the Weakest Link in CONNECTED Cars: Telematics Data Servers.” *Upstream Security Connected Car Cybersecurity Automotive Cybersecurity Securing the Weakest Link in Connected Cars Telematics Data Servers Comments*, https://upstream.auto/blog/securing-the-telematics-servers

Holmes, Freddie. “Does the Connected Car Pose a Threat to a Connected Life?” *Automotive World*, 17 Sept. 2019, www.automotiveworld.com/articles/does-the-connected-car-pose-a-threat-to-a-connected-life/.

Miller, Eric. “FBI Warns Truckers That Hackers Could Target Eld Data.” *Transport Topics*, 30 July 2020, www.ttnews.com/articles/fbi-warns-truckers-hackers-could-target-eld-data.

26, December, et al. “5 Essential Gadgets Every Truck Driver Needs.” *Trucks.com*, 28 Dec. 2018, www.trucks.com/2018/12/26/5-essential-gadgets-every-truck-driver-needs/.

Tabak, Nate, and Follow on Twitter. (ransomware with trucking company) “Inside a Ransomware Attack on a Small Trucking Company.” *FreightWaves*, 23 Feb. 2021, www.freightwaves.com/news/inside-a-ransomware-attack-on-a-small-trucking-company.

“What Is an Eld?” *Geotab*, www.geotab.com/blog/what-is-an-eld/.

Vartak, Nimish, et al. “Nimish Vartak.” *UMBC Ebiquity*, University of Maryland, Baltimore County, 1 Sept. 2006, ebiquity.umbc.edu/paper/html/id/341/Protecting-the-privacy-of-RFID-tags.

Segal, Troy. “Vehicle-to-Everything (v2x) Definition.” *Investopedia*, Investopedia, 19 May 2021, www.investopedia.com/terms/v/v2x-vehicletovehicle-or-vehicletoinfrastructure.asp.