**TELEMATICS: RISKS AND MITIGATION TECHNIQUES IN VEHICLE CYBERSECURITY**

Ali Zarafshani, CSCE, University of North Texas

Vasanth Kandagatlaa, Sharanya Battara, Vijaya Maneesha Reddy Duggimpudia, Saichaithanya Bollama

a: Masters in Cybersecurity, CSCE, University of North Texas

*Abstract*— Vehicle manufacturers are introducing new features that can improve areas like safety, convenience, and productivity. In this progression, they are digitalizing aspects that were previously machine-driven and introducing external communication ports and internet connections to machines that previously operated in isolation. As vehicles become more efficient and technologically advanced, the subject of danger transitions to an increase in vulnerabilities and potential attacks on those embedded communication ports and corresponding systems in terms of privacy intrusion, security breach, and compromised operation.

When discussing potential issues and risks, various perspectives open multiple areas of potential exploitation, such as vehicle ad hoc networks (VANET), telematics such as GPS receivers, input/output interfaces, SIMs, electric vehicle supply equipment (EVSE) such as USB ports, music players, and local and physical access points. Network and telecommunications capabilities in modern automobiles include cellular, wireless, machine-to-machine, transaction processing management systems, Bluetooth, OTA updates, and CAV sensory technology. With this functionality, vehicle data can be transferred and evaluated at remote databases to assist vendors and data aggregators in improving vehicle performance, increasing vehicle safety, and optimizing vehicle-to-vehicle operations on the road. Despite these benefits, these capabilities expand the possible assault surface area.

Keywords—Vehicle Cybersecurity, Telematics, Automotive Cybersecurity

# VEHICLE CYBERSECURITY

Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation.

Basically, when we say automotive cyber security, we’re talking about protecting the in-vehicle computer systems on automobiles from cybercriminals and other unauthorized individuals who might be up to no good.

Vehicle cybersecurity means implementing proven defenses to:

* Keep anyone from stealing your data (like your GPS location info or data that’s one your smartphone you connected to the Bluetooth speaker),
* Stop hackers from being able to control or manipulate your vehicle (for example, disabling the burglar alarm or tricking the collision avoidance system), and
* Ensure nobody can damage your vehicle (for example, resetting your oil change counter so you don’t get your oil changed on time).

## Why is vehicle cybersecurity important?

A system becomes vulnerable to cyber-attack the instant it is linked to a network. Depending on how secure the network is, the attack may or may not be effective. We have heard several reports of website/email hacking or social media account hijacking. Modern vehicles rely heavily on computer systems to monitor and control the vehicles different systems. If an auto’s technology isn’t secure, hackers can steal data, such as tracking your location information via GPS.

But it gets a lot scarier: hackers can even run commands, forcing a vehicle to obey the hacker instead of the driver. While getting your data stolen is a disconcerting thought, the idea that a hacker could take control of your car is outright terrifying. Hackers can use commands to activate or deactivate different features like your A/C and windshield wipers, or to control your steering, brakes, or engine.

Upstream Security’s 2020 Automotive Cybersecurity Report shows that the past decade has demonstrated a marked increase in automotive cyber incidents. From 2018 to 2019, there was a 99% increase in automotive cyber security incidents. Now, that their Auto Threat Intelligence data covers both physical and remote attacks, although 82% of the attacks in 2019 involved short- and long-range remote attacks.

## Vehicle attack vectors

Source: Joelynn Schroeder, NREL

# TELEMATICS

Vehicle telematics is an interdisciplinary field that combines telecommunications, informatics, computer science, electrical engineering, and vehicular technologies to create a vehicle telematics system that functions to collect and derive insight from vehicle telematics data and ultimately improve the efficiency and safety of the overall driver experience.

## What is vehicle telematics?

Vehicle telematics combines GPS systems, onboard vehicle diagnostics, wireless telematics devices, and black box technologies to record and transmit vehicle data, such as speed, location, maintenance requirements and servicing, and cross-reference this data with the vehicle’s internal behavior. This information can be used in real-time analysis to improve overall driver safety and reduce costs and improve performance for commercial vehicles.

## How do vehicle telematics work?

Source: geotab

Telematics devices collect then transmit GPS and vehicle-specific data via General Packet Radio Service (GPRS), 4G and cellular networks, or satellite communication to a centralized server, where the data is categorized, interpreted, and optimized for consumer user interfaces.

Modern commercial vehicle manufacturers typically embed automotive telematics technology directly into fleet vehicles. Aftermarket GPS devices are also available for installation.

Telematics data typically includes such factors as fuel consumption, idling time, location, speed, sharp acceleration or braking, and vehicle faults. Benefits of vehicle telematics analytics include decreased fuel costs, improved driver safety, increased productivity, improved vehicle visibility through precise tracking, data driven vehicle maintenance schedules, maintaining ELD (Electronic Logging Device) compliance, and more precise payroll management.

## Vehicle telematics Applications?

Source: NREL

# Physical Access Risks

# Physical access to most telematics devices could potentially allow access to components and functions of modern vehicles, but it would require the additional step of compromising the telematics system before attempting to attack the vehicle. The telematics system can only compromise vehicle functionality if the telematics have written access to the vehicle system or if telematics firmware can be reprogrammed to provide write access. This has been accomplished with aftermarket telematics in research setting to take control of vehicle functions, including braking (Foster et al. 2015). Considering how telematics devices’ intended functions are to simply receive data from a vehicle’s control units, interpret the various inputs, and relay those inputs to the service providers, they should be considered nonessential and outside a vehicle’s primary functions, assuming no write permissions to the vehicle’s CAN bus operations exist.

## Mitigation Techniques for Physical Threats to Telematics

Fleet managers can take the following steps to mitigate risks before installing telematics:

* Adopting an agency system security plan with procedures and policies that includes telematics devices
* Inquiring with the U.S. Department of Homeland Security (DHS) and the U.S. Navy, which have navigated the procurement process previously to ensure their telematics units and vehicles are properly protected.
* Working with reputable, trusted partners to install telematics devices
* Considering a third-party examination of telematics that includes independent vulnerability testing of telematics before operating, including threat modeling, documentation and literature review, reverse engineering, manual inspection, network and radio spectrum analysis, penetrating testing, and fuzz testing.

Telematics manufacturers can mitigate physical access risks by:

* Configuring telematics connection to vehicle as read-only and disabling write access to vehicle ECUs in telematics firmware
* Adding anti-tampering or layered security methods to the telematics device so that physical access to the device will not allow partial or complete access to the network; this should include ensuring that any default passwords or configurations are customized
* Assigning unique cryptographic keys to each telematics device so that knowledge of one key cannot be used to infiltrate other devices
* Disabling the ability for external users to read firmware code from telematics devices without authorization
* Using vehicle alerts for attack detection and curtailment as well as to encourage drivers to take protective action if necessary
* Employing secure coding practices and auditing the source code

## Procurement Recommendations for Physical Threats to Telematics

The following procurement recommendations can help federal fleets mitigate physical access

risks:

* Vendors should monitor network activity and install a tampering alarm in the telematics device that signals to the driver, fleet manager, and manufacturer cybersecurity team if an intrusion is detected
* If purchasing on behalf of a military organization, ensure devices are compliant with authority to operate (ATO) requirements
* Contractors should produce the appropriate documentation that their employees have undergone favorable background investigations for all personnel that support the server/system managing the data from the telematics devices
* Formal nondisclosure agreements and conflict of interest agreements should be required to be signed by third parties that deal with government telematics devices in any way

# Remote Access Risks

The most vulnerable hacking opportunity for telematics is access to the data collected by the system. Collecting data from telematics is possible without write access or bridging different networks. It still requires hacking the telematics network and is inherently a remote risk. However, the most threatening method for controlling a vehicle through telematics would be to reflash the firmware remotely, which could give a malicious actor insight, control, and ability to

manipulate functions of the vehicle as they desire. Research has shown the ability to reflash aftermarket telematics firmware (Foster et al. 2015) and incorporate malicious code into OEM telematics (Li et al. 2019) when critical security measures were not instituted. These failures included using the same cryptographic key for every telematics device, a lack of strong authentication procedures, lack of encryption, and an unsecured update server. With multi-factor authentication, it is difficult for adversaries to access firmware administrative control to reflash firmware updates, even if using another device that is compatible with the device in the car.

Research by the DOT Volpe National Transportation Systems Center identified a risk associated with the ability to send OTA short message service (SMS) messages to query and configure information about the vehicle’s status if the attacker knows the personally identifiable information (PII) related to the vehicle. This attack would take moderately lengthy open-source intelligence gathering on the part of the attacker and would have to specifically target a particular individual. This presented a greater risk using 2G and 3G networks; 4G-LTE allows messages sent between the car and server to be encrypted and authenticated, making interception, replay,

or other intrusions difficult to execute.

Volpe’s “Telematics Cybersecurity Primer for Agencies” includes analysis of vulnerabilities and details security controls that federal agencies should include when instituting telematics (Clark and Chin 2017). Three main steps must be verified in depth for proper security measures when dealing with OTA updates (Riggs et al. 2018):

1. First, establish a secure connection to the telematics device networked into the car. Sending the update is not an automatic process.
2. Once a secure connection is made, the software update must be authenticated by the car and the main service provider sending the update. This is important because, unlike a CAN bus method, authentication does not have to be sacrificed for speed of information flow.
3. After the signal sent is verified as authentic by the car and service provider, make sure the payload of code being sent is securely installed to the vehicle.

If any of the steps in this chain are broken, and malicious or unintentionally harmful updates are installed to the telematics device or devices associated with the vehicle, or network of vehicles, then a malicious actor or entity could develop some level of access to the vehicle. Geotab, a telematics provider, developed a System Security Plan that provides a cybersecurity overview for themselves and other providers. The plan addresses topics from system interconnections, ports, protocols, system environments, network architectures, and owner operator functionalities (Geotab 2017). These security controls follow the FIPS 199standards, as well as NIST 800-53, Revision 4. A list of 15 security recommendations is set forth by Geotab for building a telematics platform resilient to cyberthreats and attacks (Sukhov 2016).

## Mitigation Techniques for Remote Threats to Telematics

In addition to the mitigation techniques for physical access, telematics companies can further mitigate remote access risks by:

* Using multi-factor authentication to verify authorized access to telematics network
* Securing remote endpoints that telematics devices use for operation
* Using false data injection mitigation methods, such as redundant verification safeguards
* Requiring user authorization and authentication for mobile OTA updates capable of updating firmware
* Encrypting OTA firmware updates, transmission of telematics data, and data housed remotely
* Incorporating the ability to revert to the prior firmware version if an OTA update fails or introduces vulnerabilities.
* Consulting Volpe’s “Telematics Cybersecurity Primer for Agencies” (Clark and Chin 2017) before making acquisition decisions

## Procurement Recommendations for Remote Threats to Telematics

The following procurement recommendations can help federal fleets mitigate remote access risks. These should be followed in addition to the recommendations listed under physical risks.

* Require vendors to comply with all areas of FedRAMP security requirement baselines including provisions for cloud service providers, and ensure this accreditation is upheld with periodic reviews
* Encrypt any messages sent OTA or data at rest using FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives
* Require two-factor authentication to access the telematics device remotely, or at least ensure the single-factor access control has hardened hardware security to minimize replication, replay, distributed denial-of-service, or spoofing attacks
* Require strong, unique passwords to have defense in-depth for communications from the vehicle to vendor servers and use multi-factor authentication to access the telematics network
* Implement whitelisting and blacklisting of messages sent from network to telematics devices to prevent unsafe commands.

# ISO 21434

The purpose of the above standard addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods.

This Standard provides vocabulary, objectives, requirements, and guidelines related to cybersecurity engineering as a foundation for common understanding throughout the supply chain. This enables organizations to:

— define cybersecurity policies and processes.

— manage cybersecurity risk; and

— foster a cybersecurity culture.

# Telematics Cybersecurity Summary

Telematics devices are not typically the end target when dealing with intrusion into modern vehicles. They are, however, a very vulnerable remote attack vector for modern vehicles, as they offer a single point of failure to gain access to an entire fleet if compromised. The main goals for attackers when attacking telematics devices are to either collect data or disrupt, manipulate, and potentially cause significant harm to vehicle functionality. To facilitate best practices for procurement, and even to catch mistakes that slip through the process, standards such as the NIST 800 series, the “Telematics Cybersecurity Primer for Federal Agencies,” Geotab’s System Security Plan, and experience from other agencies including DHS and Navy can be referenced to ensure telematics devices for the federal fleet meet industry standards for cybersecurity.

##### References

1. <https://www.geotab.com/blog/what-is-telematics/>
2. <https://www.nrel.gov/docs/fy19osti/74247.pdf>
3. Cybersecurity challenges in vehicular communications, ZeinabEl-Rewinia, KarthikeyanSadatsharanaDaisy FloraSelvaraja Siby JosePlathottamb PrakashRanganathan
4. <https://www.truckinginfo.com/10123379/fbi-bulletin-puts-spotlight-on-elds-and-cybersecurity>
5. <https://www.heavy.ai/technical-glossary/vehicle-telematics>
6. <https://wanada.org/cars-increasingly-vulnerable-to-hacking-fbi-nhtsa-warn/>