VicOne

Driving Automotive Cybersecurity Forward

AUTOMOTIVE DATA

Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape

Numaan Huq, Vladimir Kropotov,
Philippe Lin, Rainer Vosseler

Trend Research for VicOne

Technological advancements in the automotive industry have transformed modern vehicles into data hubs. These vehicles are continuously generating, consuming, and transmitting large volumes of data. The analysis and use of this vehicle data create many new opportunities, from the enhancement of vehicle functions to the generation of new revenue streams. However, this shift toward a data-centric ecosystem also brings with it a set of unique challenges and responsibilities for the automotive industry.

This research paper delves into vehicle data and its generation, transmission, and usage. In particular, this paper highlights the privacy and security concerns associated with vehicle data. Quite often, vehicle data is collected without the users' explicit consent and/or knowledge,[1, 2] or the data collection details are hidden deep in the fine print of purchase agreements.[3] This raises serious concerns about the potential of data misuse or abuse, including contraventions of data protection laws.[4]

This paper explores macro categories of vehicle data collected, ways in which this data could be used and monetized, and cybersecurity threats associated with this data. Our research found examples of vehicle data leakage via MQTT brokers and demonstrated that even small amounts of vehicle data could be used to profile drivers or fleets, highlighting privacy and security risks associated with unsecured data. An unexpected find was discovering vehicle API communications logs in Trend Micro telemetry data; these API calls could expose vulnerabilities that can be exploited by cybercriminals.

All of our findings highlight the need for secure data transmission and stringent measures to protect data. The success of the connected car enterprise presents a lucrative target for cybercriminals, driving the need for robust data security measures. As the automotive industry evolves into a data-driven industry, it becomes crucial for stakeholders such as OEMs and Tier 1 and Tier 2 suppliers to strike a balance between innovation and data protection.

Key Takeaways

Data-driven ecosystem. Modern vehicles have evolved into complex data hubs, creating an ecosystem where data is generated, collected, distributed, and used in innovative ways. This also brings with it unique challenges such as privacy concerns and potential misuse or abuse of data.

Monetization and cybersecurity risks. As monetization opportunities arise from vehicle data, these will inevitably attract cybercriminals. The first large-scale attacks against connected cars will involve data, potentially escalating to more sensational attacks such as vehicle hacking and fleet takeover.

Middleware APIs. Middleware APIs will create new opportunities for cybercriminals by giving them easy API access to a vehicle's E/E architecture and ECUs. This can give rise to architecture-agnostic malware and cyberattack vectors.

Vehicle data leaks. Vehicle data shared via public MQTT servers can be accessed by anyone owing to the open nature of these servers. This data can be used to profile drivers or services, providing insights into their activities and operations. A lot of open or unsecure MQTT servers accept write instructions from any subscriber and are thus susceptible to data-poisoning attacks.

Regulatory gaps. Any legislative gaps in vehicle data collection and usage need to be addressed. The automotive industry cannot operate effectively in a regulatory vacuum; appropriate legislation is necessary to provide clarity and stability.

1. Introduction

Technology growth and data integration are fast reshaping the automotive industry. Vehicles have transformed into data hubs, continuously generating, consuming, and transmitting large volumes of data.[5] In this research, we delve into the vast and often overlooked world of automotive data, to understand its implications for the future of transportation and society at large.

One of the primary data sources for our research was lists of application programming interface (API) field names collected by different vehicle manufacturers — also known as OEMs (original equipment manufacturers) — and the automotive industry's Tier 1 (T1) and Tier 2 (T2) suppliers. Getting our hands on this data necessitated using open-source intelligence (OSINT) techniques, as knowledge about what data was generated and transmitted by the vehicles was not readily available and/or accessible. The API field name lists also included data offered for purchase by data brokers — which purchase vehicle data from OEMs, anonymize it, amalgamate it, wrap their own APIs around it, and resell the data — further contributing to the automotive data ecosystem. The automotive data ecosystem is a vast network of entities that includes vehicles, manufacturers, suppliers, data brokers, and data consumers, all interlinked via data flows. The enormity of this ecosystem was an unexpected revelation for us during our research.

In the automotive data ecosystem, vehicles are not just data generators; they are also consumers. Our findings suggest that vehicles receive data from both OEM and third-party clouds. This data communication uses mobile apps or occurs directly via the telematic control unit (TCU), which interfaces with the gateway chip and electronic control units (ECUs). Our research also examines the expanding middleware ecosystem for a vehicle's in-vehicle infotainment (IVI) system, also referred to as the head unit (HU). We expect architecture-agnostic developer APIs in the future, which abstract the technical details of the vehicle's electrical and electronics (E/E) systems.

Our data hunting led us to discover API calls between vehicles and OEM/T1/T2 clouds in Trend Micro telemetry data. While collecting data, we searched Trend Micro telemetry data for due diligence and were surprised to discover vehicle API communications (to perform actions such as remote start/stop, door lock/unlock, and telematics collection) in our logs. We also found instances of vehicle data leakage via the MQTT (Message Queuing Telemetry Transport) protocol on public MQTT servers. While limited in scope, in some cases there was enough vehicle data to profile drivers and track vehicle movement.

From our research findings, we can conclude several things. Vehicles are no longer just vehicles; they are complex data hubs. Vehicle data, collected by an array of players including OEMs, T1 and T2 suppliers, and data brokers, can be merged to generate new data products and create monetization opportunities — from creating driver profiles to traffic data–powered targeted advertising. This demonstrates that the vehicle data ecosystem is both large and intricate. But just how widespread vehicle data proliferation is and what security measures are needed to protect the data are not well understood. There seems to be a lack of published research exploring the vehicle data ecosystem and its potential for data misuse or abuse. Our research attempts to address some of those knowledge gaps and start the necessary discussions around the current and future states of automotive data.

2. Automotive Data Ecosystem

The automotive data ecosystem is a network of entities that includes connected vehicles, manufacturers, suppliers, data brokers, and data consumers, all interlinked via data flows.

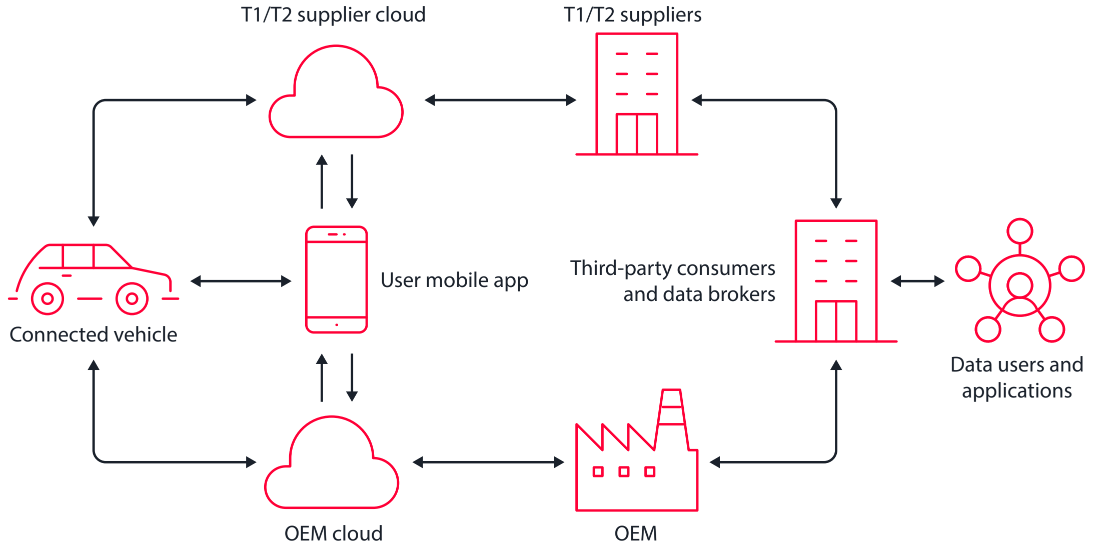


Figure 1. The automotive data ecosystem

Data collection, a critical component of this ecosystem, occurs through multiple channels. The primary method is via the TCU, which communicates with cloud infrastructure (owned by OEMs or other trusted parties such as T1/T2 suppliers) via a 3G/4G/5G cellular network. Besides the TCU, data can also be collected through mobile applications linked to the vehicle, widening the scope and volume of information that can be collected.

Vehicle data is a valuable resource. It provides insights into vehicle performance, driver behavior, and usage patterns, among other things. OEMs and T1/T2 suppliers use this data to refine their products, improve functionality, identify and create new offerings, and enhance the user experience. For instance, predictive maintenance, route optimization, and personalized recommendations are applications directly benefiting from this data. However, the utility of vehicle data extends beyond the manufacturers and their suppliers. Properly sanitized to ensure privacy, this data can be commercialized and sold to third parties like data brokers or directly to consumers. This not only generates additional revenue streams for the OEMs, but also fuels the growth of an ecosystem of services, apps, and products.

A wide variety of applications stem from automotive data. They range from entertainment, personalized recommendations, insurance products based on driving behavior, and even smart city solutions. The automotive data ecosystem is not only about OEMs and T1/T2 suppliers, but a broader landscape involving consumers, third-party service providers, and emergent applications and products. In summary, the automotive data ecosystem is an evolving dynamic sector within the automotive industry. It leverages vehicle data to create novel insights and innovative business models, while simultaneously creating a market for data-driven products and services for a wide range of industries.

3. Vehicle Data Analysis

Vehicles are complex data hubs generating and consuming data. We have already learned that the automotive data ecosystem is a network of entities that includes connected cars, OEMs, suppliers, data brokers, and data consumers, all interlinked via data flows. While it has long been established that vehicles generate and send data,[6, 7] what remains largely unknown is what data is sent back to the OEM/T1/T2 clouds. This raises serious questions about data privacy, security, and usage, and creates unknowns in drivers' daily digital footprints.

3.1 Data Sources

The primary data source for our research was API field names collected by the different OEMs and suppliers. Accessing API field names and raw vehicle data proved challenging. We submitted requests to the OEMs to access vehicle data. Some outright rejected our requests, while others informed us that our geographical location did not support data access for privacy reasons. In two instances, extended discussions took place, but these remain unresolved and we still lack access to vehicle data. We were also asked to submit detailed explanations on how we planned to use the vehicle data. **Despite the difficulties we encountered in obtaining data, this stringent access control is good as it shows the OEMs performing due diligence and not providing data access indiscriminately.**

While live vehicle data feeds are valuable, our research primarily needed to ascertain what API data fields are generated and collected, along with some example data. We used OSINT to collect API field names from different OEMs, T1/T2 suppliers, and data brokers. There is also a community of car enthusiasts who reverse-engineer apps and firmware, and make their data publicly available on GitHub or blogs. In some cases, the OEMs and T1/T2 suppliers themselves publish the API field names they collect, and we are grateful for their transparency. We collected API field names from BMW,[8, 9, 10] Rolls-Royce,[11] Ford via Geotab,[12] General Motors (GM)[13] via OnStar,[14] GM via Geotab,[15, 16] Mercedes-Benz,[17, 18, 19] Tesla,[20, 21, 22] Audi,[23] Caruso,[24] Samsara,[25] Otonomo,[26, 27] Smartcar,[28] High Mobility,[29, 30] Navistar via GeoTab,[31] Open Vehicles Monitoring System,[32] GeoTab,[33, 34] AutoPi,[35] Invers,[36] and Viper.[37] Although individual data sources were somewhat incomplete, collecting and collating data from numerous sources provided us with a fairly comprehensive understanding of the different types of data fields vehicles can generate and send back to the OEM/T1/T2 clouds.

We also found vehicle data leakage via the MQTT protocol on public MQTT servers. In our hunt for raw vehicle data, we found MQTT servers all over the world. In this research, we aimed to collect vehicle-related data from various sources, primarily to identify diverse locations where vehicle data could be found. For due diligence, we also searched Trend Micro telemetry data and unexpectedly found API calls between vehicles and OEM/T1/T2 clouds in our logs.

3.2 Data Categorization

The API field names that we collected from the OEMs, T1/T2 suppliers, and brokers were often unstructured, and the same type of data had multiple names, adding an extra layer of complexity to understanding and using the data. A major task was to classify the vehicle data into macro categories.

Note that the categories in Table 1 are high-level categories, and each category has subcategories. We are providing short descriptive names for the examples and avoiding the use of OEM/T1/T2/broker-specific API field names.

Data category	Description	Examples of data fields
Vehicle information	Information about the vehicle's identification and details	VIN, make, model, year, vehicle class
Driving behavior	Driving behavior of the vehicle	Speed, harsh acceleration, harsh braking, cornering
Fuel system	Data related to the fuel system of the vehicle	Fuel level, fuel consumption, range, nearby fuel stations
Location	Geographical location of the vehicle, including place names	Latitude, longitude, geohash, city, country
Trip information	Details about trips taken by the vehicle	Trip duration, distance traveled, stops
Vehicle safety	Safety-related data	Collision events, seatbelt usage, speeding, collision photo
Service and maintenance	Data related to vehicle service and maintenance	Service events, service duration, service point, service reminder
Rest areas	Information about rest areas	Nearby rest areas, rest area distances
Diagnostic trouble codes (DTCs)	DTCs detected in the vehicle, including code, description, and status	DTCs, DTC description, DTC status
Battery	Information about the vehicle's battery	Battery voltage, battery life, battery temperature
Engine	Engine performance data	Engine temperature, RPM, engine status
Tire pressure monitoring (TPM)	Information about the vehicle's tires	TPM status, pressure front/rear/left/right
Vehicle status	Overall status of the vehicle	Vehicle health status, engine coolant level, fuel level
Telematics	Data about telematics and TCU	Telematic position update, teleservice status
Climate control	Vehicle's climate control system	Cabin temperature, AC on/off, defrost
Charging	Data related to the charging system of the electric or hybrid vehicle	Charging power, charging status, charging plug status
Doors and windows	Status and control of the vehicle's doors and windows	Door status, window status, trunk lock status, window open/close
Lighting system	Status and control of the lighting system in the vehicle	Light status, headlight status, interior light status, on/off
Infotainment system	Data about the infotainment system of the vehicle	Radio station, volume, media source
Vehicle security	Security-related data	Alarm status, anti-theft status, vehicle locking

Data category	Description	Examples of data fields
Navigation system	Data related to the navigation system in the vehicle	GPS location, navigation route, destination
Audio and entertainment	Data fields related to the IVI features of the vehicle	Speaker type, audio source, equalizer settings
Connectivity	Connectivity options for the vehicle	Bluetooth connection, Wi-Fi connection, latency, strength
User preferences	User preferences stored in the vehicle	Seat adjustments, climate settings, language
Drivetrain and performance	Data related to the drivetrain components and performance of the vehicle	Vehicle speed, engine speed, transmission gear

Table 1. High-level data categories and their corresponding descriptions and examples of data fields

Classifying the API field name data from OEM/T1/T2/brokers into macro categories helped us understand where the data originates and how it can be used. This high-level view simplifies the complex landscape of vehicle data, making the data more accessible and easier to understand.

3.3 Extrapolating New Data

Data truly becomes valuable when it can be used to discover new insights. One way to do this is by combining different data fields to extrapolate new data. Extrapolated data can deliver important insights about things such as fuel efficiency, driver performance, local weather, and even road surface status. It is important to note that the quality and validity of these insights depend on the quality, frequency, and relevance of the data points being integrated.

- **Fuel efficiency = GPS + Engine + Fuel consumption** – By combining GPS data, which includes information about routes and speeds, with engine performance and fuel consumption data, vehicle fuel efficiency can be calculated. This can contribute to improved driving habits and vehicle maintenance schedules, and even influence the design of future vehicles.

- **Emissions analysis = Engine + Fuel + Driver behavior** – Integrating data from the engine, fuel system, and driver behavior offers insights into vehicle emissions. This can contribute to eco-friendly driving strategies and the development of emission reduction technologies.

- **Optimal routing = GPS + Engine** – By correlating GPS data with engine performance metrics, optimal routing strategies can be developed. These can help reduce travel times, improve fuel efficiency, and minimize wear and tear on the vehicle.

- **Predictive maintenance = Engine + GPS + DTCs** – Combining engine data, GPS data (which includes driving patterns), and diagnostic trouble codes (DTCs) can enable predictive maintenance. This can help forecast potential problems and schedule servicing, extending the vehicle's life and ensuring optimal performance.

- **Driver performance = GPS + Engine + Fuel + Braking** – The integration of GPS data (route, speed), engine performance, fuel efficiency, and braking patterns provides a comprehensive overview of driver performance. This can aid in driver training and insurance assessments, and improve vehicle safety.

- **EV range = Battery + GPS + Driver behavior** – For an electric vehicle (EV), extrapolating the vehicle's range can be achieved by integrating battery data (such as charge status and drain rate), GPS data (like routes and speeds), and driver behavior. This can help in managing charging schedules, route planning, and the design of future EVs.

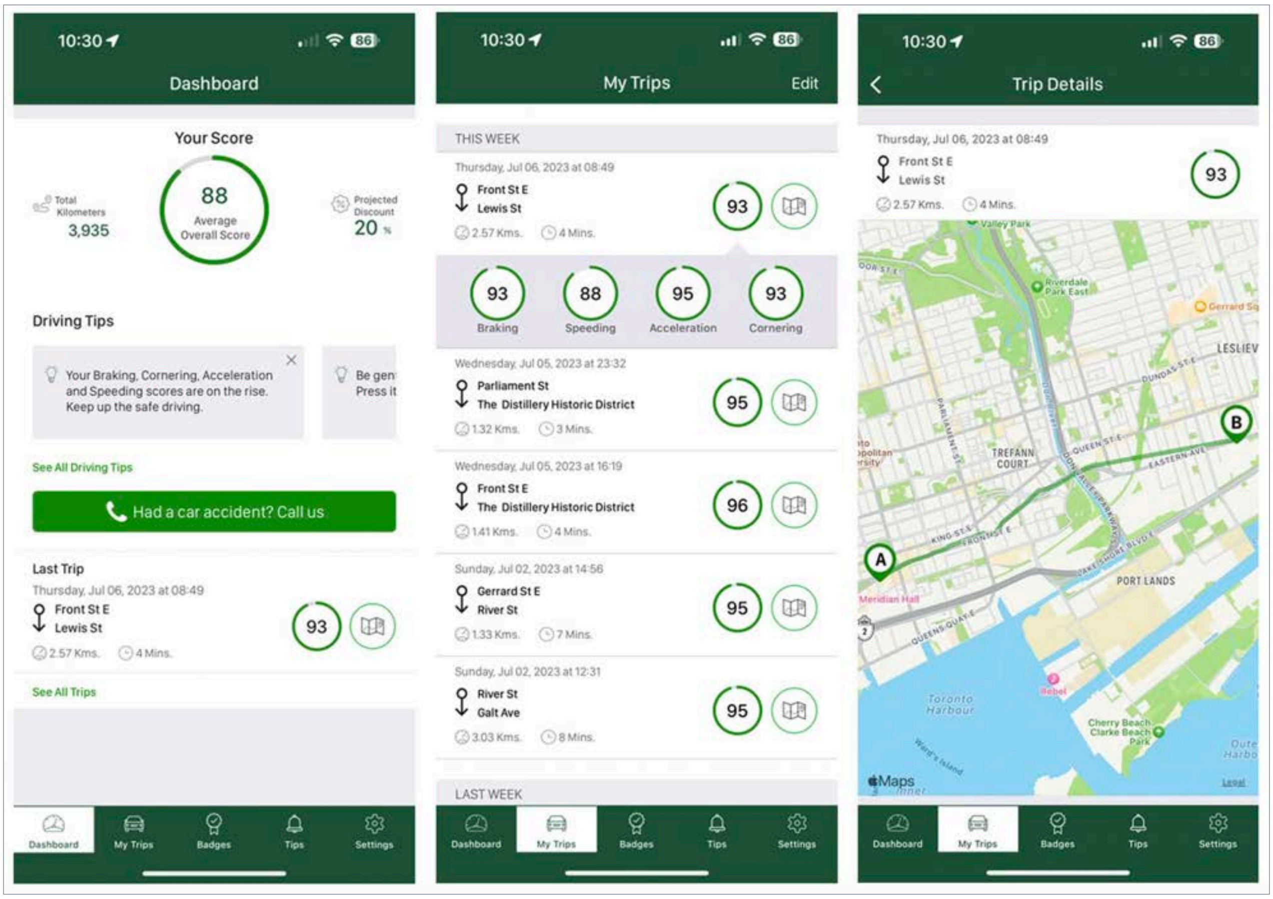
- **Tire health status = Tire pressure + TPM warnings** – By combining tire pressure data with tire pressure monitoring (TPM) warnings, an accurate assessment of tire health can be derived. This leads to timely maintenance, thereby ensuring road safety and optimal vehicle performance.

- **Micro weather = Wipers + Brakes + External temperature** – Collating data from wiper use, brake status, and external temperature sensors allows for real-time local weather assessments. These can aid in improving route planning and can be shared with weather agencies for more accurate predictions.

- **Parking analytics = Vehicle status + GPS** – By combining vehicle status data (such as idle time, speed, and engine status) with GPS, insightful parking analytics can be derived. This can be useful for city planning, designing better parking solutions, and providing real-time parking assistance to drivers.

- **Traffic predictor = Vehicle performance + GPS** – Combining vehicle performance data with GPS data enables predictive traffic modeling. This can aid in improving routing, minimizing congestion, and assisting in traffic management strategies.

- **Vehicle security status = Doors + Trunk + Windows + GPS** – Integrating the status data of vehicle doors, windows, and trunk with GPS information provides the vehicle's security status. This can aid in quick detection of and response to breaches, and enhance vehicle security.



10:30 Dashboard

Your Score

Total Kilometers 3,935

88 Average Overall Score

Projected Discount 20 %

Driving Tips

Your Braking, Cornering, Acceleration and Speeding scores are on the rise. Keep up the safe driving.

Be gen… Press it…

See All Driving Tips

Had a car accident? Call us

Last Trip

Thursday, Jul 06, 2023 at 08:49 Front St E Lewis St 2.57 Kms. 4 Mins. 93

See All Trips

10:30 My Trips Edit

THIS WEEK

Date	From	To	Distance	Duration	Score
Thursday, Jul 06, 2023 at 08:49	Front St E	Lewis St	2.57 Kms.	4 Mins.	93
Wednesday, Jul 05, 2023 at 23:32	Parliament St	The Distillery Historic District	1.32 Kms.	3 Mins.	95
Wednesday, Jul 05, 2023 at 16:19	Front St E	The Distillery Historic District	1.41 Kms.	4 Mins.	96
Sunday, Jul 02, 2023 at 14:56	Gerrard St E	River St	1.33 Kms.	7 Mins.	95
Sunday, Jul 02, 2023 at 12:31	River St	Galt Ave	3.03 Kms.	8 Mins.	95

Braking	Speeding	Acceleration	Cornering
93	88	95	93

LAST WEEK

10:30 Trip Details

Thursday, Jul 06, 2023 at 08:49 Front St E Lewis St 2.57 Kms. 4 Mins. 93

Figure 2. *Dynamic insurance rate calculated by combining braking, speeding, acceleration, cornering, and GPS data. The data is collected either via readings from the gyroscope and GPS of the mobile phone or via a dongle connected to the OBD-II (on-board diagnostics) port of the vehicle. The dongle connects to the internet via the mobile phone. This data can also be collected by the OEMs using the TCU.*

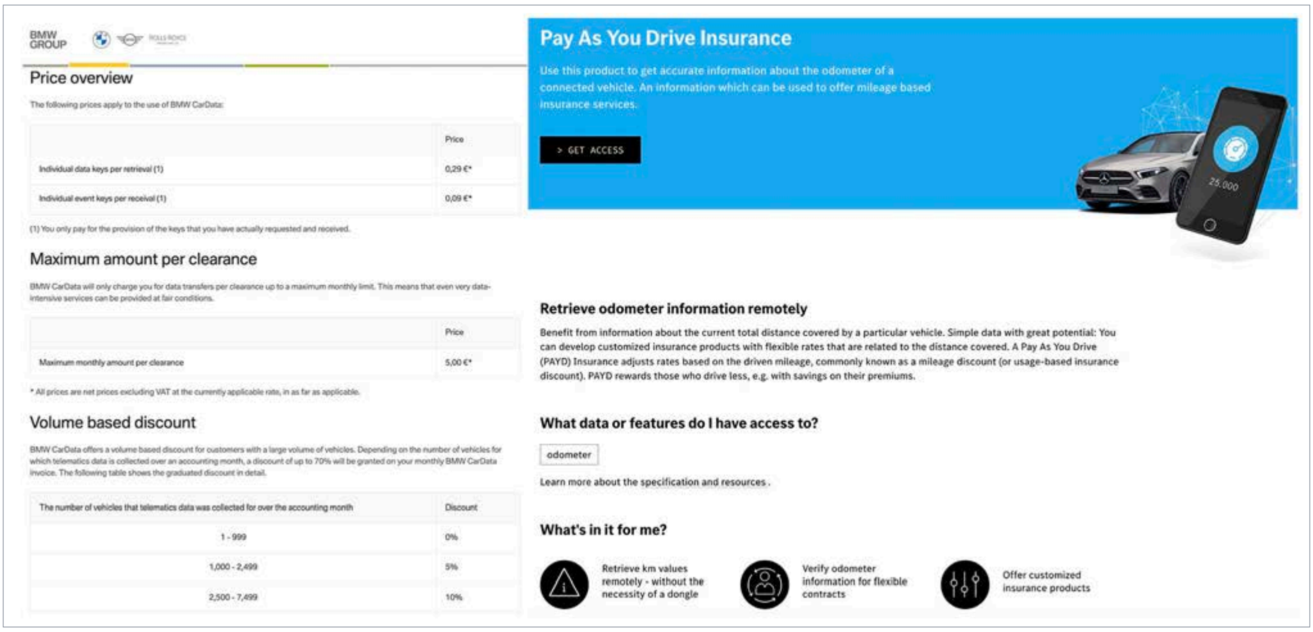
Data extrapolation not only unlocks new data insights, but it can also be used for enhancing vehicle performance, safety, and maintenance, and reducing environmental impact. Vehicles generate vast amounts of data, but only by combining data to extrapolate new insights can they really start generating value.

3.4 Monetizing Data

OEMs collect vehicle data primarily for feedback to help them build better cars in the future, to improve the driver/passenger experience, and to aid in creating new driving technologies. They sell only a subset of the vehicle data collected, with the bulk of it remaining for their research purposes. But vehicle data also creates new monetization opportunities. Telematics data not only helps in understanding a vehicle's performance, but it can also be used for the development of personalized services and innovative business models. In this subsection, we explore how OEMs and third parties can monetize vehicle data.

We brainstormed several strategies on how to monetize vehicle data. Some of these monetization strategies are already being used, others are emerging, and the rest are future methods:

- **Usage-based insurance.** Create personalized insurance policies by analyzing driving patterns, vehicle health, and other data.
- **Fleet management services.** Optimize vehicle usage, maintenance, and routing.
- **Vehicle maintenance and repair services.** Offer proactive and predictive maintenance services by using telematics data to better understand and diagnose vehicle issues.
- **Location-based services and advertising.** Target drivers with ads based on their driving patterns and locations, generating revenue for businesses.
- **Value-added services.** Develop and offer services based on telematics data, generating revenue from subscriptions or one-time purchases.
- **Partnerships with service providers.** Partner with insurance companies, repair shops, or fleet management companies to share revenue generated from telematics data.
- **Data aggregation and analysis.** Aggregate and analyze telematics data to develop valuable insights and trends, selling them to research organizations, governments, or automotive industry stakeholders.



Price overview

The following prices apply to the use of BMW CarData:

	Price
Individual data keys per retrieval (1)	0,29 €*
Individual event keys per receival (1)	0,09 €*

(1) You only pay for the provision of the keys that you have actually requested and received.

Maximum amount per clearance

BMW CarData will only charge you for data transfers per clearance up to a maximum monthly limit. This means that even very data-intensive services can be provided at fair conditions.

	Price
Maximum monthly amount per clearance	5,00 €*

* All prices are net prices excluding VAT at the currently applicable rate, in as far as applicable.

Volume based discount

BMW CarData offers a volume based discount for customers with a large volume of vehicles. Depending on the number of vehicles for which telematics data is collected over an accounting month, a discount of up to 70% will be granted on your monthly BMW CarData invoice. The following table shows the graduated discount in detail.

The number of vehicles that telematics data was collected for over the accounting month	Discount
1 - 999	0%
1,000 - 2,499	5%
2,500 - 7,499	10%

Pay As You Drive Insurance

Use this product to get accurate information about the odometer of a connected vehicle. An information which can be used to offer mileage based insurance services.

Retrieve odometer information remotely

Benefit from information about the current total distance covered by a particular vehicle. Simple data with great potential: You can develop customized insurance products with flexible rates that are related to the distance covered. A Pay As You Drive (PAYD) Insurance adjusts rates based on the driven mileage, commonly known as a mileage discount (or usage-based insurance discount). PAYD rewards those who drive less, e.g. with savings on their premiums.

What data or features do I have access to?

odometer

Learn more about the specification and resources .

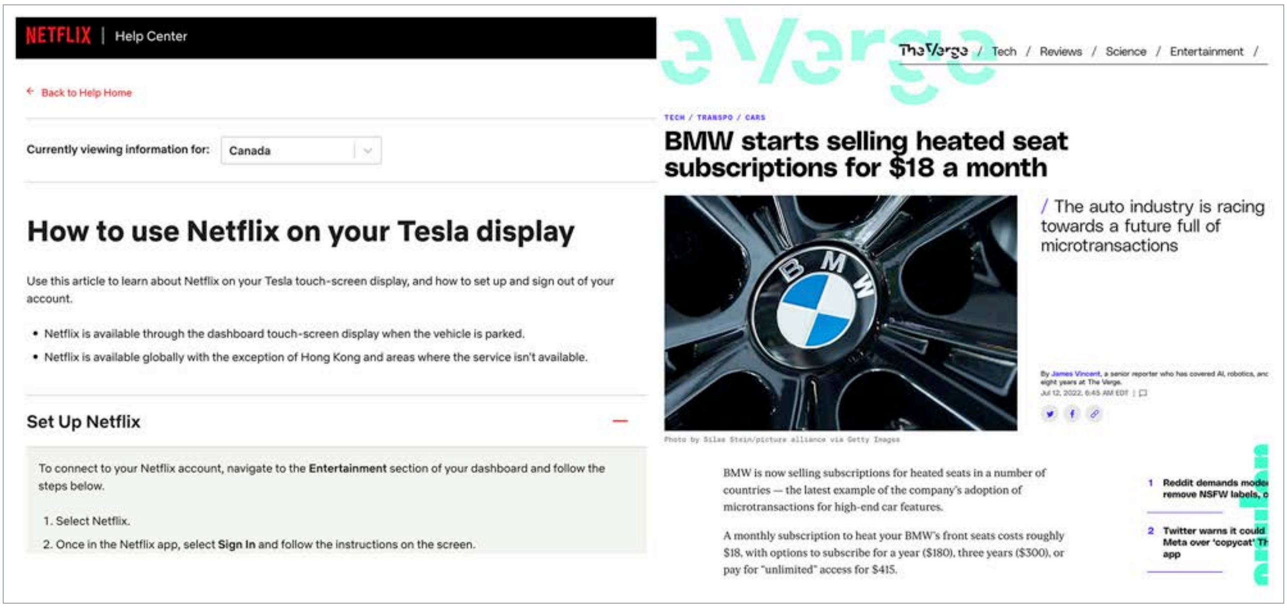
What's in it for me?

Retrieve km values remotely - without the necessity of a dongle

Verify odometer information for flexible contracts

Offer customized insurance products

Figure 3. Examples of OEMs selling both data and data products[38, 39]



NETFLIX | Help Center

← Back to Help Home

Currently viewing information for: Canada

How to use Netflix on your Tesla display

Use this article to learn about Netflix on your Tesla touch-screen display, and how to set up and sign out of your account.

- Netflix is available through the dashboard touch-screen display when the vehicle is parked.
- Netflix is available globally with the exception of Hong Kong and areas where the service isn't available.

Set Up Netflix

To connect to your Netflix account, navigate to the **Entertainment** section of your dashboard and follow the steps below.

1. Select Netflix.
2. Once in the Netflix app, select **Sign In** and follow the instructions on the screen.

The Verge / Tech / Reviews / Science / Entertainment /

TECH / TRANSPO / CARS

BMW starts selling heated seat subscriptions for $18 a month

/ The auto industry is racing towards a future full of microtransactions

By James Vincent, a senior reporter who has covered AI, robotics, anc eight years at The Verge.
Jul 12, 2022, 6:45 AM EDT

Photo by Silas Stein/picture alliance via Getty Images

BMW is now selling subscriptions for heated seats in a number of countries — the latest example of the company's adoption of microtransactions for high-end car features.

A monthly subscription to heat your BMW's front seats costs roughly $18, with options to subscribe for a year ($180), three years ($300), or pay for "unlimited" access for $415.

1 Reddit demands mode remove NSFW labels, c

2 Twitter warns it could Meta over 'copycat' Th app

Figure 4. Examples of subscription services available in vehicles[40, 41]

Automotive data is valuable not just to the automotive industry but also to a wide range of industries. In Table 2, we study three example organizations and explore how they can use automotive data in their daily operations.

Organization	How can I use automotive data?
Bank	A bank may be interested in acquiring and using data about the financial habits, reliability, and risks associated with potential clients or customers. Data that a bank can use includes: • **Driving behavior.** This includes a driver's habits, driving routes, frequency of travel, and time spent on the road. This data can provide insights into the lifestyle of a person, which can be used for credit scoring and risk profiling. • **Vehicle usage.** Information about how frequently a vehicle is used, where it is typically driven, and how well it is maintained could be of value. Regular, long-distance travel might suggest the need for vehicle loans or insurance products. • **Vehicle maintenance and repair.** Regular maintenance and care for a vehicle could be an indicator of a person's financial reliability, which could help with credit and loan decisions. • **Location.** The places a person visits can indicate their lifestyle, consumer habits, and financial capacity. For instance, regular visits to high-end shopping districts might indicate a certain income level. • **Fuel efficiency.** This could be an indicator of how well the vehicle is used and maintained. High fuel efficiency might suggest responsible usage and could be indicative of a financially responsible individual.

Organization	How can I use automotive data?
	The bank can use this data to generate revenue through: • **Personalized loan offers.** Offer personalized vehicle loans based on how well a person is likely to take care of the vehicle, their driving habits, and the type of vehicle they are likely to purchase. • **Credit scoring and risk profiling.** Better understand customer habits, which can help with credit scoring and risk profiling. • **Cross-selling and upselling.** Cross-sell or upsell financial products such as auto insurance, vehicle loans, or credit cards with rewards for auto purchases. • **Marketing and advertising.** Use location-based data for targeted advertising, providing offers when customers are likely to be considering auto purchases. • **Partnerships.** Form partnerships with auto retailers or repair shops for special offers, generating a new revenue stream.
Delivery	A delivery company can use these subsets of vehicle data: • **GPS.** GPS data can help optimize routes for delivery drivers, resulting in quicker deliveries and lower fuel consumption. With accurate GPS history, the delivery company can determine high traffic areas and times, and better plan the delivery schedule. • **Engine and fuel consumption.** This information can provide insights on fuel efficiency, which can be used to enforce efficient driving practices that save money. Also, this is useful in determining when delivery vehicles need maintenance. • **Driver behavior.** By monitoring driver behavior such as acceleration, braking, and speed, the delivery company can ensure that their drivers are adhering to safe driving practices. • **Vehicle status.** With this information, the delivery company can monitor the health status of the delivery vehicles and schedule preventive maintenance, reducing downtime and unexpected repair costs. • **DTCs.** These codes give insights into any potential issues that might occur with the delivery vehicles, allowing for preemptive maintenance and reducing the risk of vehicle breakdowns during deliveries. In terms of revenue generation, using this data can enhance operational efficiency, reduce costs, and improve customer satisfaction, which can in turn lead to increased revenue. For example, efficient routing (using GPS data) and vehicle maintenance (using engine and DTC data) can minimize operational costs. Improved driver performance (using driver behavior data) can enhance safety and save costs related to accidents or damage. Data-driven insights can be used to strategically expand services in high-demand areas, driving business growth.
Towing	A towing company can benefit from several subsets of vehicle data. These data sets can drive additional revenue generation and enhance service offerings: • **Breakdown.** Data related to engine status, DTCs, fuel level, and battery status can aid in predicting potential vehicle breakdowns. These insights enable proactive dispatch of assistance or implementation of preventive measures. • **GPS location.** Access to real-time location data enables accurate positioning of broken-down or stranded vehicles, resulting in faster response times. GPS data of accidents, breakdowns, and vehicle malfunctions can also help pre-position tow trucks in problem areas for quick response times. • **Vehicle status.** Understanding whether a vehicle is parked, idle, or in motion can help identify and target vehicles stranded because of breakdowns or malfunctions.

Organization	How can I use automotive data?
	There are several ways this data can be monetized: • **Proactive services.** Analysis of breakdown data can lead to the development of services designed to prevent common issues. These services can be offered on a subscription basis, providing a consistent revenue stream. • **Targeted assistance.** Leveraging real-time GPS data can improve response times for stranded vehicles, enhancing the customer experience and building loyalty. • **Partnerships.** Predictive maintenance insights derived from the data can be shared with vehicle maintenance services. In return, they pay referral fees. • **Membership programs.** With predictable data on potential breakdowns, the towing company can offer membership programs with flat-rate towing within certain areas.

Table 2. Example organizations and how they can use automotive data in their daily operations

Some of the examples we present here, especially for the bank, require profiling individuals or groups of individuals. This might seem like a violation of privacy but, when making loan decisions, bank underwriters already use data points that probe deeply into financial health to decide the solvency and risk ratings of the person or institution requesting the loan. Vehicle data adds further parameters to this assessment, and banks already have well-established privacy protection mechanisms in place. Fully anonymized data has less value unless there are methods for profiling by combining numerous data points. Given that profiling is an important component of vehicle data monetization, it is critical for stakeholders to take proactive measures to ensure responsible data handling, safeguard user privacy, and prevent data misuse or abuse.

4. Cybersecurity Risks of Vehicle Data

Automotive data is valuable, and not just to the automotive industry but also to a wide range of industries. By combining different data fields, we can extrapolate new insights, create novel data products, and offer innovative products and services. In the previous section, we explored ways in which OEMs and third parties can use and monetize vehicle data, and we are already seeing everyday examples of data monetization and subscription services being offered for vehicles. As monetization opportunities arise and start generating significant revenue, these will inevitably attract cybercriminals, much like how nectar attracts bees.

In a recent research into the cybercriminal underground conducted by Trend Micro for VicOne,[42] we found that current threats primarily revolve around car modding, where enthusiasts hack vehicle features and manipulate data such as mileage. Future threats include cybercriminals gaining unauthorized access to vehicle user accounts, which could allow them to locate, break into, and steal cars. Stolen cars might be shipped abroad, sold for parts, or used to commit other crimes. While the cybercriminal market for connected car data is still in its infancy, it is expected to grow as third parties start using vehicle data extensively. We expect that the first large-scale attacks against connected cars will likely target data, potentially escalating to more sensational attacks like vehicle hacking and fleet takeover.

We brainstormed different ways in which vehicle data could be misused or abused:

- **Vehicle tracking.** By accessing real-time location data, a targeted vehicle could be tracked, which would have implications for the privacy and security of the driver and passengers. For example, if the vehicle's real-time location and regular route are known, then criminals could hide contraband items underneath the vehicle and transport them, effectively turning it into a mule. Real-time vehicle tracking could also be used for surveillance of high-profile individuals and their assets.

- **Driver profiling.** Driving patterns could be analyzed to reveal personal habits, lifestyles, and even routine locations, raising concerns about privacy and potential misuse of this data.

- **Data leak.** Personally identifiable information (PII), maintenance data, fuel consumption, and other operational data could leak, compromising privacy and revealing potentially sensitive information.

- **Data manipulation.** The ability to create fake alerts in the vehicle or modify performance data could lead to false diagnostics or potentially hazardous driving settings.

- **Data ransoming.** Attackers could encrypt or lock access to vehicle data stored in the OEM/T1/T2/broker clouds, demanding a ransom for restoring access. This is especially damaging if real-time vehicle data is needed to satisfy government regulations such as those related to emissions calculation.

- **Social engineering.** Collected data could be used to launch targeted social engineering attacks, exploiting the data for malicious intent.

- **Infrastructure disruption.** By identifying critical infrastructure vehicles such as ambulances and utility vehicles, malicious actors could plan and execute disruptive attacks, potentially impacting essential services.

- **Espionage.** Automotive data could be used to conduct industrial or corporate espionage, providing insights into business operations, strategies, and competitive advantages.

- **DTCs and maintenance.** Access to DTC and maintenance data could provide insights into vehicle vulnerabilities, which could then be exploited in cyberattacks.

- **Vehicle connectivity.** Information about a vehicle's connectivity could be exploited to launch targeted cyberattacks on the vehicle's systems and related infrastructure. For example, a car's Wi-Fi connectivity could be exploited for remote vehicle hacking.[43]

- **Blackmail.** A malicious actor could build a driver profile and use it for blackmail by threatening to reveal locations or other sensitive information. Data on accidents, crash locations, or DTCs could be used to blackmail a person by threatening to reveal information about undeclared accidents or vehicle malfunctions.

- **Insurance fraud.** Data on driving habits such as harsh braking, acceleration, and excessive speeding could be manipulated to present a driver as less risky, thereby qualifying them for lower insurance rates.

The list we present here is a data-centric subset of cyberthreats to connected cars. The Trend Micro research paper "Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN-R155 Attack Vectors and Beyond"[44] provides a comprehensive list of cyberthreats, complete with DREAD threat modeling assessment.[45]

As the monetization and usage of automotive data continue to grow, so does the threat of exploitation by cybercriminals. The array of threats, from vehicle tracking to insurance fraud, underscores the urgent need for strong cybersecurity measures within the automotive industry and data-centric third parties. At the same time, regulatory bodies need to develop and enforce data privacy and protection laws to safeguard drivers and passengers. As we navigate this evolving landscape, a balanced approach that promotes innovation while ensuring security and privacy is necessary in shaping the future of connected vehicles.

5. Middleware APIs in Connected Vehicles

The modern connected car is transforming into a giant smartphone on wheels, where third-party cloud–connected applications play an important part in the driver and passenger experience. This trend started with luxury automotive manufacturers doing away with physical buttons and switching to fully digital cockpits. Digital or smart cockpits are now also readily available in midrange vehicles. In addition to running applications for regular car features such as climate control, radio, and hazard lights, smart cockpits can also run third-party applications like maps, internet radio, web browsers, video streaming, social media, messaging, and virtual assistants.[46, 47]

Figure 5 shows what we envision the cloud-connected vehicle ecosystem to look like. The head unit will support running applications — there will be a middleware layer that abstracts the E/E details of the car and makes it easier for developers to build car-based apps. The middleware can speak with the gateway ECU and will give API access to apps that need to send messages to the ECUs. The bus switch will route the packets to the target ECUs. The apps can talk either to the OEM cloud or to third-party clouds (such as Netflix and Google) via tethered cellular connection from the mobile phone or via the built-in electronic SIM (eSIM) in the TCU. Depending on the E/E architecture of the car, the gateway ECU can also directly communicate with cloud services. As cars get more connected and smarter, we will see car-specific apps being developed; OEM and T1/T2 supplier versions of app developers will emerge. OEM apps will probably not need middleware to access the gateway ECU or might even be able to talk to the bus switch directly.

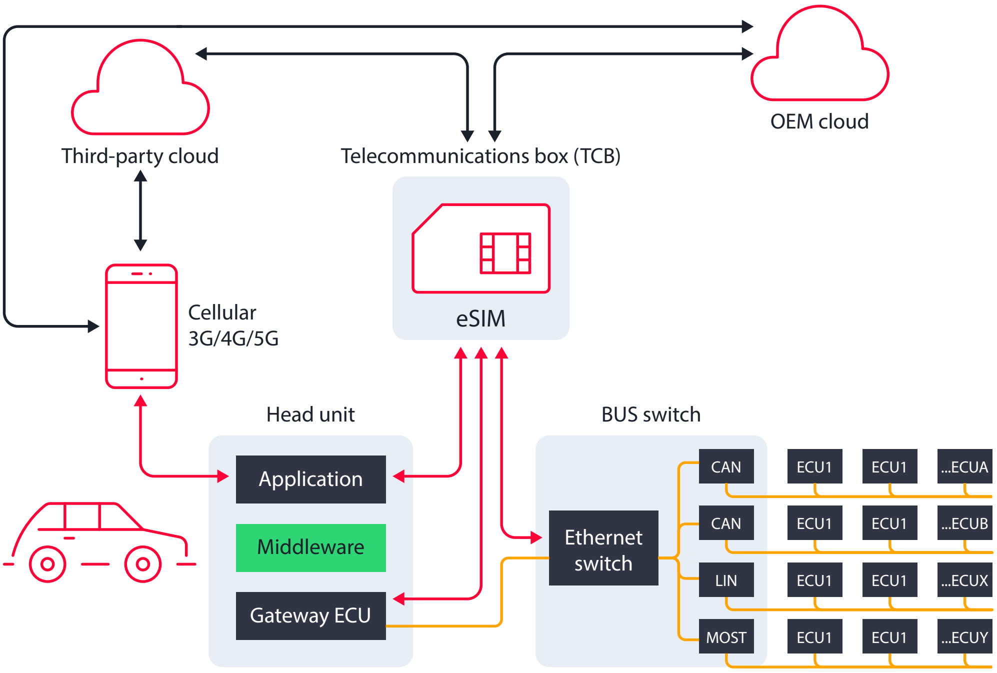


Figure 5. The cloud-connected vehicle architecture

Middleware APIs will create a rich ecosystem for cars with smart cockpits, but they will also create new opportunities for cybercriminals by giving them easy API access to a vehicle's E/E architecture and ECUs. This could give rise to a whole host of architecture-agnostic malware, such as an architecture-agnostic remote access trojan (RAT) or ransomware or botnet malware installed via phishing attacks against cars. Another plausible attack vector is using a jailbroken phone connected to a car as a pivot point to install architecture-agnostic malware in the car. On the flipside, attacks against the OEM cloud could disable functions in the car, resulting in the loss of PII, loss of control on the road, and loss of revenue, among other consequences. Cloud APIs can potentially be used to locate, unlock, start, and steal the car or steal the valuables inside the vehicle.

In a blog post published in January 2023, Sam Curry, a web application security researcher, demonstrates how he was able to access the back-end cloud infrastructure of different OEMs by exploiting vulnerabilities in their telematics systems and APIs. In the case of Mercedes-Benz, he discovered a publicly accessible website built for vehicle repair shops that wrote to the same database as the core employee LDAP (Lightweight Directory Access Protocol) system. By registering on this site, he gained limited access to the employee applications, which he then leveraged to gain further access to sensitive internal applications, including the Mercedes-Benz GitHub, where he found detailed instructions for building applications to communicate with customer vehicles.[48]

The automotive industry has traditionally prioritized safety over security. Often, security measures are implemented only when mandated by regulatory requirements. A lack of comprehensive security measures could make connected vehicles susceptible to cyberthreats. Cloud-specific attacks and middleware APIs in connected vehicles (when middleware gains widespread use) will become cybercriminals' weapon of choice as the APIs will give them easy access to vehicles' E/E systems and ECUs. Cars will become easier to compromise using a variety of tried-and-tested malware and cyberattack vectors. Thus, the automotive industry needs to proactively address these security gaps and develop cybersecurity frameworks that go beyond regulatory compliance.

6. Vehicle Data Collected From Open MQTT Servers

MQTT is a lightweight, publish-subscribe messaging protocol designed for machine-to-machine (M2M) communications. It enables devices to exchange messages over unreliable networks with little bandwidth and power consumption. There are extensive previous studies on exposed MQTT brokers, including a research paper from Trend Micro looking at security issues of MQTT in industrial internet-of-things (IoT) settings.[49]

Our hunt for vehicle data leaked via MQTT revealed several open brokers, lacking both authentication and password protection, utilized by connected vehicles. The brokers we found were globally distributed and the data being transmitted included vehicle GPS data, engine monitoring, car tracking systems, and OBD data.

We had originally hoped to access vehicle data directly from the OEMs, but unfortunately we were not granted access to the data. For our data analysis experiments, we needed access to real vehicle data, even if the data would not be as comprehensive or complete as vehicle data feeds from the OEMs. One solution was to look for vehicle data being shared publicly via open MQTT servers, which we could subscribe to and collect the data from. We initially thought this was a long shot for collecting vehicle data, but to our surprise, we found plenty of open MQTT servers broadcasting live vehicle data, which was suitable for our data analysis experiments.

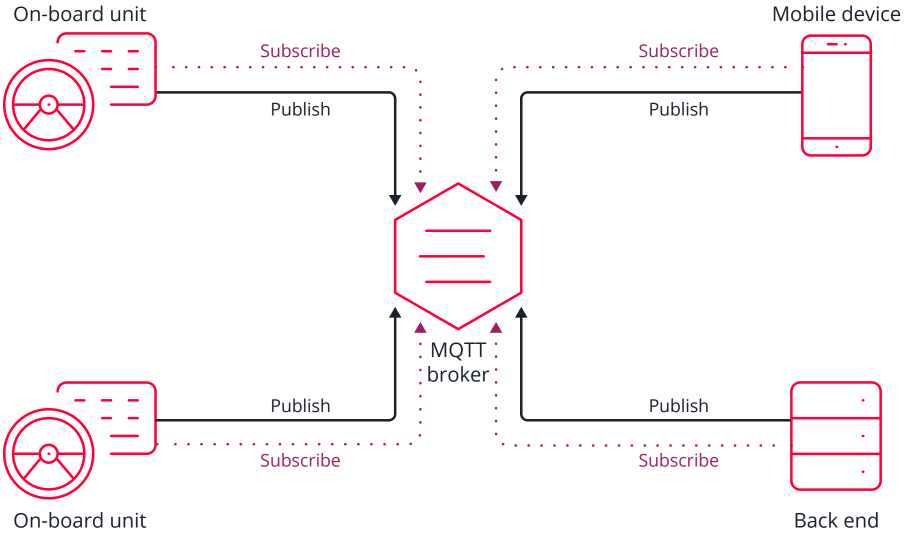


Figure 6. A functional diagram of how an MQTT broker interacts with on-board units (OBUs) and subscribers' mobile devices.

Note: NO data was transmitted to the open MQTT brokers. A lot of open or unsecure MQTT servers accept write instructions from any subscriber. This opens up the potential for data-poisoning attacks. We were careful in making sure NO data was transmitted to the open MQTT brokers that we were listening to for vehicle data. A significant portion of the data that we collected was from GPS units installed on public transit, and we managed to track public transit in 12 international cities. Public transit data is considered public; therefore, it was not unexpected to find this information, including near-real-time GPS coordinates, heading angles, timestamps, altitudes, and speeds. These data points enabled us to animate the routes of city buses in Cologne, Germany. The public transit data is also available from the actual government websites, and we used that to validate our results.

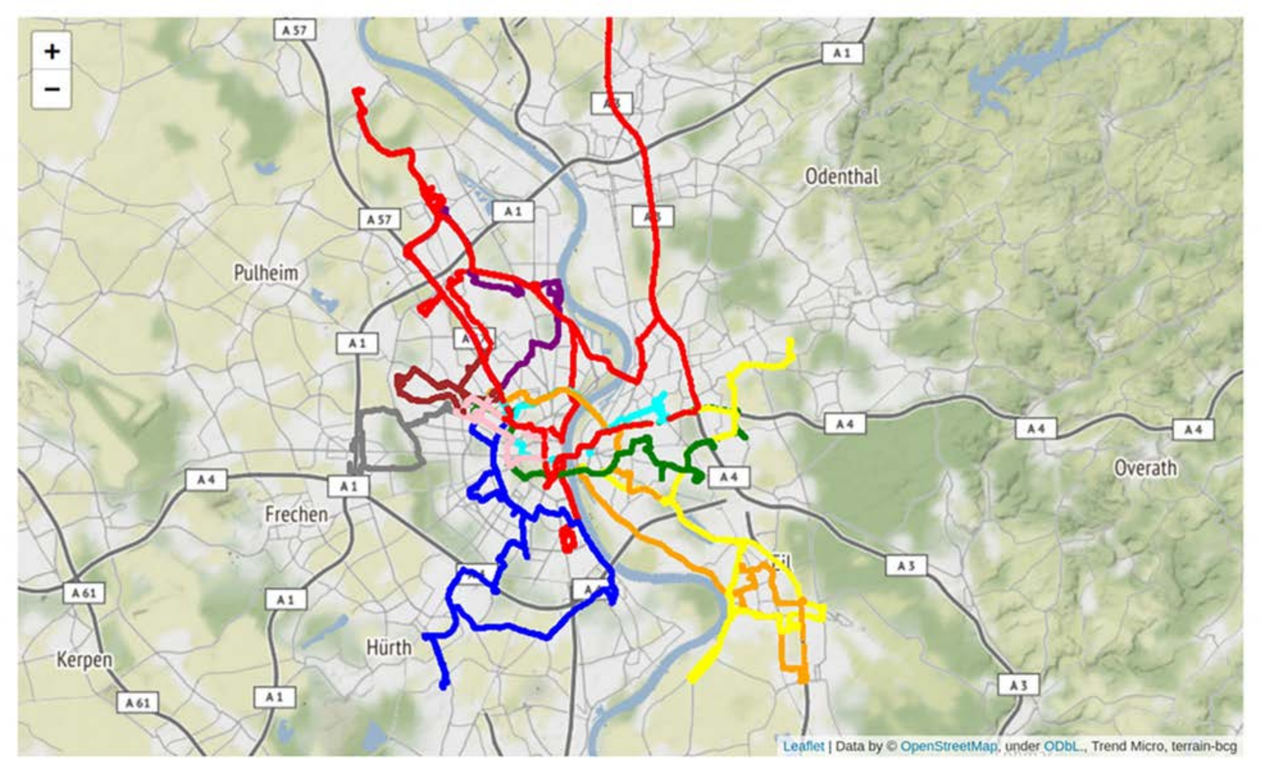
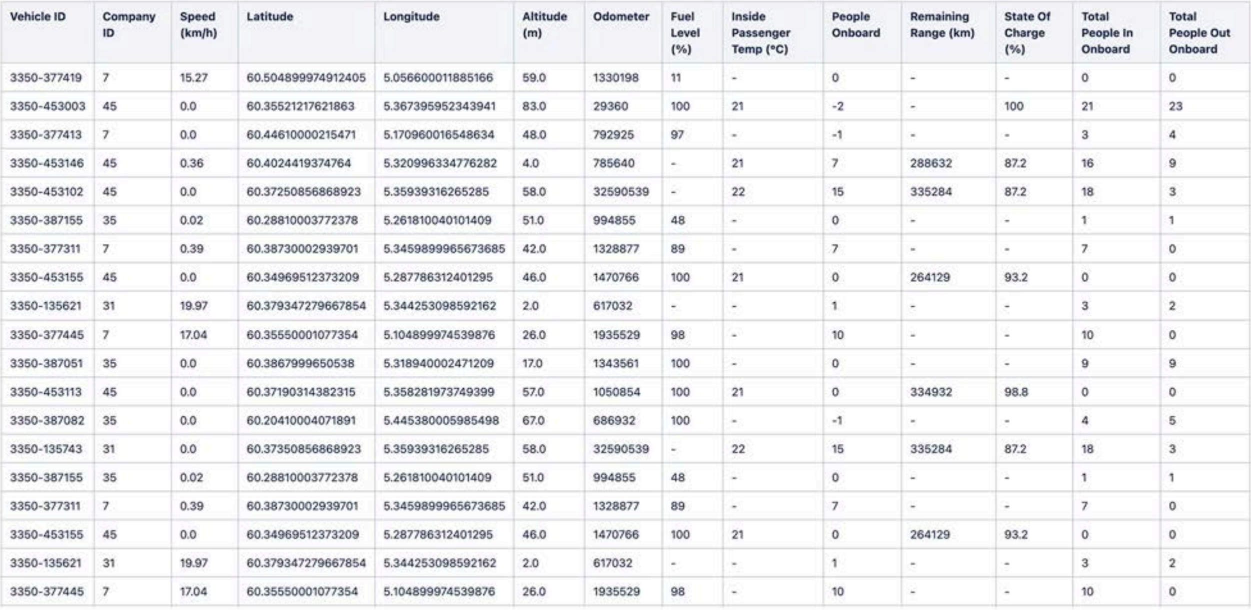

+
−
A 57
A 1
A 3
Odenthal
Pulheim
A 4
Overath
Frechen
A 61
Kerpen
Hürth
Leaflet | Data by © OpenStreetMap, under ODbL., Trend Micro, terrain-bcg

Figure 7. *Public transportation routes in Cologne, Germany, drawn using data collected from open MQTT brokers*



Vehicle ID	Company ID	Speed (km/h)	Latitude	Longitude	Altitude (m)	Odometer	Fuel Level (%)	Inside Passenger Temp (°C)	People Onboard	Remaining Range (km)	State Of Charge (%)	Total People In Onboard	Total People Out Onboard
3350-377419	7	15.27	60.504899974912405	5.056600011885166	59.0	1330198	11	-	0	-	-	0	0
3350-453003	45	0.0	60.35521217621863	5.367395952343941	83.0	29360	100	21	-2	-	100	21	23
3350-377413	7	0.0	60.44610000215471	5.170960016548634	48.0	792925	97	-	-1	-	-	3	4
3350-453146	45	0.36	60.4024419374764	5.320996334776282	4.0	785640	-	21	7	288632	87.2	16	9
3350-453102	45	0.0	60.37250856868923	5.35939316265285	58.0	32590539	-	22	15	335284	87.2	18	3
3350-387155	35	0.02	60.28810003772378	5.261810040101409	51.0	994855	48	-	0	-	-	1	1
3350-377311	7	0.39	60.38730002939701	5.3459899965673685	42.0	1328877	89	-	7	-	-	7	0
3350-453155	45	0.0	60.34969512373209	5.287786312401295	46.0	1470766	100	21	0	264129	93.2	0	0
3350-135621	31	19.97	60.379347279667854	5.344253098592162	2.0	617032	-	-	1	-	-	3	2
3350-377445	7	17.04	60.35550001077354	5.104899974539876	26.0	1935529	98	-	10	-	-	10	0
3350-387051	35	0.0	60.3867999650538	5.318940002471209	17.0	1343561	100	-	0	-	-	9	9
3350-453113	45	0.0	60.37190314382315	5.358281973749399	57.0	1050854	100	21	0	334932	98.8	0	0
3350-387082	35	0.0	60.20410004071891	5.445380005985498	67.0	686932	100	-	-1	-	-	4	5
3350-135743	31	0.0	60.37350856868923	5.35939316265285	58.0	32590539	-	22	15	335284	87.2	18	3
3350-387155	35	0.02	60.28810003772378	5.261810040101409	51.0	994855	48	-	0	-	-	1	1
3350-377311	7	0.39	60.38730002939701	5.3459899965673685	42.0	1328877	89	-	7	-	-	7	0
3350-453155	45	0.0	60.34969512373209	5.287786312401295	46.0	1470766	100	21	0	264129	93.2	0	0
3350-135621	31	19.97	60.379347279667854	5.344253098592162	2.0	617032	-	-	1	-	-	3	2
3350-377445	7	17.04	60.35550001077354	5.104899974539876	26.0	1935529	98	-	10	-	-	10	0

Figure 8. *Example data collected from public buses in Norway via MQTT. Data includes how many passengers are on board.*

Interesting data points surfaced in our analysis of vehicle data collected via MQTT, including:

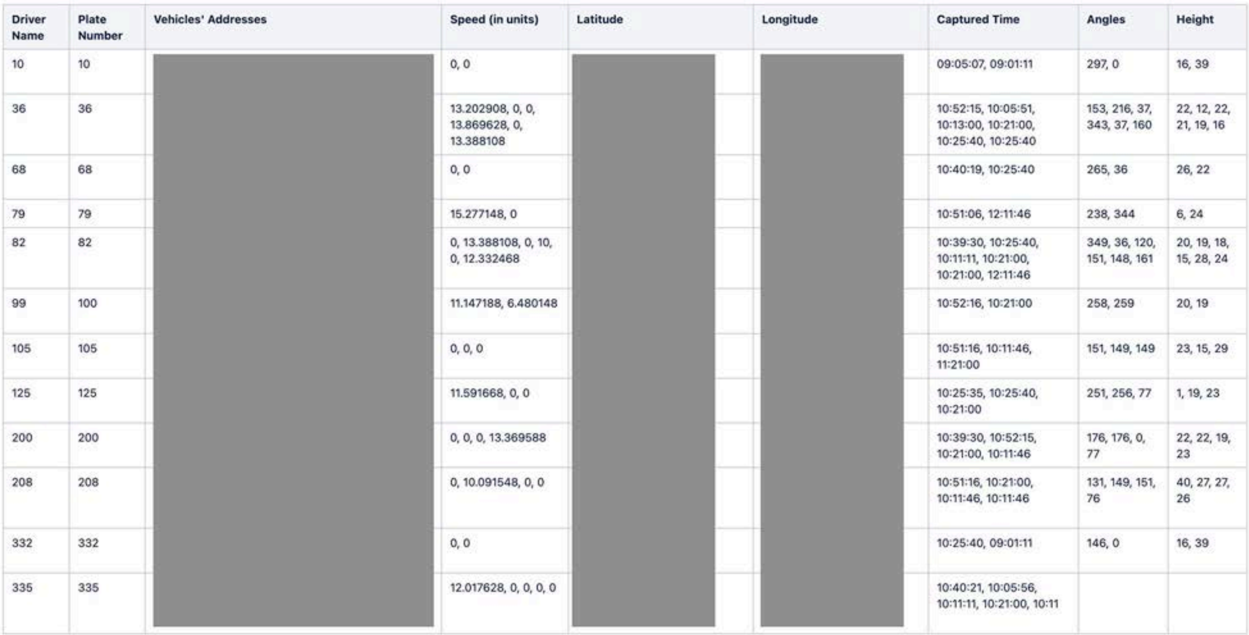
- **Device codes** – These referred to internal codes used in on-board units (OBUs) for device identification.
- **Driver identities** – We were able to profile several drivers. Although their actual names were not disclosed, identifiers such as “company-035-driver” hinted at their employers.
- **Number plates** – The majority of these were encrypted and encoded with Base64, yet over 12 plates were in clear text.
- **Addresses** – Real-time approximate addresses were available in several data sets.

6.1 Driver Profiling

With the MQTT data, we asked the questions: How can we profile drivers? And what are we profiling?

- **Driver behavior analysis** – acceleration, braking, speeding, driving style, etc.
- **Driver efficiency analysis** – last-trip fuel consumption, last-trip mileage, energy consumption from EV battery usage
- **Driver utilization** – metrics such as total engine time, trip distance accumulated, average distance traveled
- **Safety analysis** – data points like crash locations, crash severity, indicator light status, braking, speeding, and acceleration statistics
- **Route optimization** – geolocation and vehicle speed, which can be analyzed to understand the routes taken by each driver
- **Time management** – information like vehicle time status, trip summary, and last trip, which can be used to monitor how much time drivers spend driving versus taking breaks

We did not have fine-grained control of the MQTT data as it was publicly broadcast, and we were not purchasing any data. Within these limits, we attempted to profile drivers and the results were interesting.



Driver Name	Plate Number	Vehicles' Addresses	Speed (in units)	Latitude	Longitude	Captured Time	Angles	Height
10	10	[redacted]	0, 0	[redacted]	[redacted]	09:05:07, 09:01:11	297, 0	16, 39
36	36	[redacted]	13.202908, 0, 0, 13.869628, 0, 13.388108	[redacted]	[redacted]	10:52:15, 10:05:51, 10:13:00, 10:21:00, 10:25:40, 10:25:40	153, 216, 37, 343, 37, 160	22, 12, 22, 21, 19, 16
68	68	[redacted]	0, 0	[redacted]	[redacted]	10:40:19, 10:25:40	265, 36	26, 22
79	79	[redacted]	15.277148, 0	[redacted]	[redacted]	10:51:06, 12:11:46	238, 344	6, 24
82	82	[redacted]	0, 13.388108, 0, 10, 0, 12.332468	[redacted]	[redacted]	10:39:30, 10:25:40, 10:11:11, 10:21:00, 10:21:00, 12:11:46	349, 36, 120, 151, 148, 161	20, 19, 18, 15, 28, 24
99	100	[redacted]	11.147188, 6.480148	[redacted]	[redacted]	10:52:16, 10:21:00	258, 259	20, 19
105	105	[redacted]	0, 0, 0	[redacted]	[redacted]	10:51:16, 10:11:46, 11:21:00	151, 149, 149	23, 15, 29
125	125	[redacted]	11.591668, 0, 0	[redacted]	[redacted]	10:25:35, 10:25:40, 10:21:00	251, 256, 77	1, 19, 23
200	200	[redacted]	0, 0, 0, 13.369588	[redacted]	[redacted]	10:39:30, 10:52:15, 10:21:00, 10:11:46	176, 176, 0, 77	22, 22, 19, 23
208	208	[redacted]	0, 10.091548, 0, 0	[redacted]	[redacted]	10:51:16, 10:21:00, 10:11:46, 10:11:46	131, 149, 151, 76	40, 27, 27, 26
332	332	[redacted]	0, 0	[redacted]	[redacted]	10:25:40, 09:01:11	146, 0	16, 39
335	335	[redacted]	12.017628, 0, 0, 0, 0	[redacted]	[redacted]	10:40:21, 10:05:56, 10:11:11, 10:21:00, 10:11		

Figure 9. Profiling drivers using MQTT data. Identifiers have been redacted for privacy protection.

One important fact became clear very early: More data equals better profiling. Once the vehicle data was sorted, organized, and analyzed, we exported the GPS data from a single day into a KML (Keyhole Markup Language) file and loaded it in Google Earth. The resultant image was all the driver activity from that day.

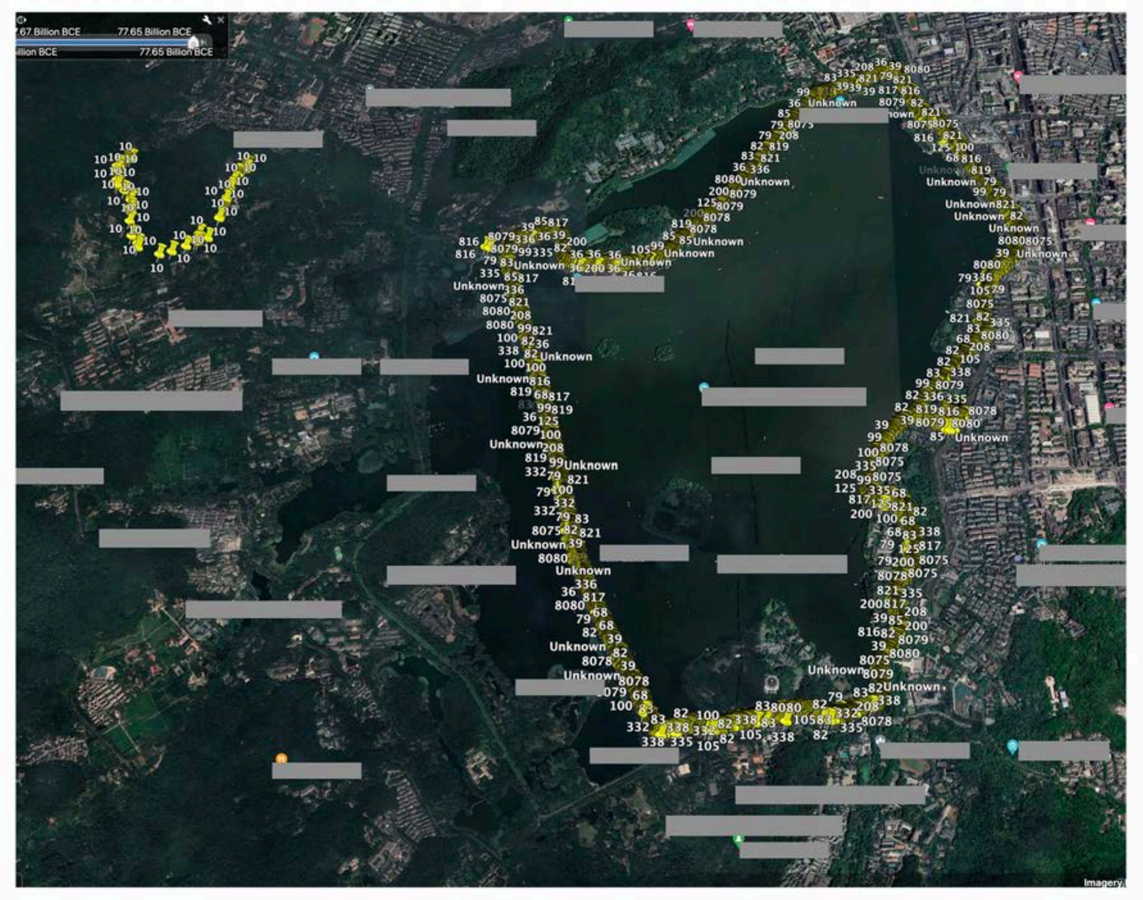


Figure 10. Example data collected via MQTT that was used to profile drivers and map their routes in Google Earth. Place names have been redacted for privacy protection.

The map image is consistent with a delivery service, likely for very specialized deliveries; otherwise, we would see data points spread across the city. The MQTT data also provided us with the exact delivery addresses for each driver. Analyzing this data over a longer duration will allow us to profile the delivery patterns for each address and the regular routes that individual drivers follow. The map labels have been redacted for privacy reasons, but the business names were visible in Google Maps. This visibility makes it possible for us to also profile the customer businesses using leaked vehicle data.

6.2 Other Findings

We further encountered data from a GPS platform designed for medical vehicles. Even though this data is meant to be public, analyzing the data, we could identify the exact model of the OBU units in these vehicles and the phone number associated with each unit. This revelation raises potential concerns about the triggering of remote vulnerabilities via these phone numbers.

Our research also discovered MQTT brokers sharing nonpublic data such as:

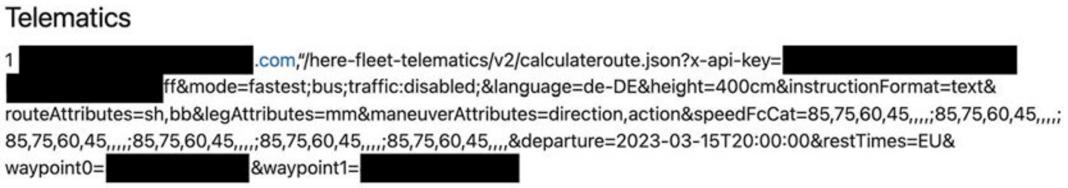
- ICCID (integrated circuit card identification) on a SIM card (presumably used by the OBU)
- GSM signal strength
- Temperature sensors
- Air conditioner status
- Defroster status
- Radio station playing
- OBD data sent over with IMEI (international mobile equipment identity)
- Real-time status of the anti-lock braking system (ABS), airbag, brake, clear light, clutch, fog light, heater, high light, horn, left light, low light, retarder, reverse gear, right light, door sensors, crash alarm, danger alarm, emergency alarm, fatigue alarm, oil alarm, steal alarm, rollover alarm, etc.
- Battery management system (BMS) status of an EV and battery voltage

We also discovered data from service vehicles in an airport such as tractors, de-icing trucks, lightweight trucks, middle-weight trucks, electric passenger buses, wastewater trucks, and ladder trucks, along with their plate numbers. While airside service vehicles in most airports have ADS-B (Automatic Dependent Surveillance-Broadcast) transmitters installed for safety and tracking reasons, and they can be tracked on flight-tracking sites such as Flightradar24,[50] it was interesting to find this data on an open MQTT server complete with license plate numbers.

Vehicle data, whether intentionally or unintentionally transmitted via public MQTT servers, can be accessed by anyone owing to the open nature of these servers. As demonstrated in our analysis, this data can be used to profile drivers or services, providing detailed insights into their activities and operations. This raises security concerns as the misuse or abuse of this data could compromise the safety and privacy of drivers, passengers, and entire fleets. It could also disrupt services if sensitive operational data falls into the wrong hands. A lot of open or unsecure MQTT servers accept write instructions from any subscriber. This opens up the potential for data-poisoning attacks. Therefore, it is vital to ensure that vehicle data is adequately protected and transmitted over secure and authenticated channels to prevent unauthorized access and potential misuse or abuse.

7. Vehicle API Data

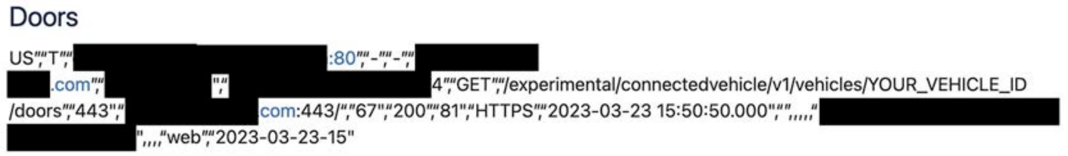
In this research, we aimed to collect vehicle data from various sources, primarily to identify the diverse locations where vehicle data can be found. This approach led us to discover vehicle data being shared via MQTT (discussed in the previous section). For due diligence, we also searched Trend Micro telemetry data and found API calls between vehicles and OEM/T1/T2 clouds in our logs. We identified several categories of vehicle API requests, a subset of which we present here with example data. Some data fields have been redacted to protect privacy.



Telematics

```
1 [redacted].com,"/here-fleet-telematics/v2/calculateroute.json?x-api-key=[redacted]
ff&mode=fastest;bus;traffic:disabled;&language=de-DE&height=400cm&instructionFormat=text&
routeAttributes=sh,bb&legAttributes=mm&maneuverAttributes=direction,action&speedFcCat=85,75,60,45,,,,;85,75,60,45,,,,;
85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,&departure=2023-03-15T20:00:00&restTimes=EU&
waypoint0=[redacted]&waypoint1=[redacted]
```

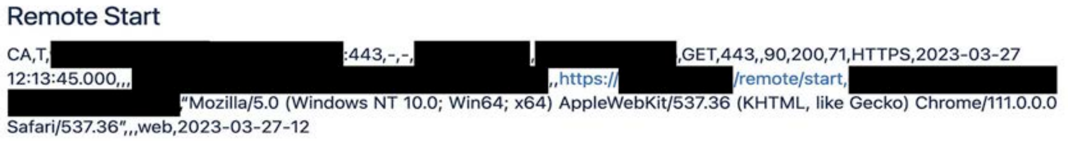
Telematics. This API call appears to be a route calculation request to the OEM's fleet telematics API. It calculates the fastest route for a bus with a height of 400 centimeters, with traffic conditions disabled. The request includes route, leg, and maneuver attributes, and provides instructions in text format. The departure time is specified, and EU rest times for drivers are considered. The route is calculated from a starting waypoint to an end waypoint, both given in latitude and longitude.



Doors

```
US"","T"",[redacted]:80"","-"","-"",[redacted]
.com"",[redacted]",",[redacted]4"","GET"","/experimental/connectedvehicle/v1/vehicles/YOUR_VEHICLE_ID
/doors"","443",",[redacted]com:443/","67","200"","81","HTTPS"","2023-03-23 15:50:50.000","",,,,"[redacted]
",,,,"web"","2023-03-23-15"
```

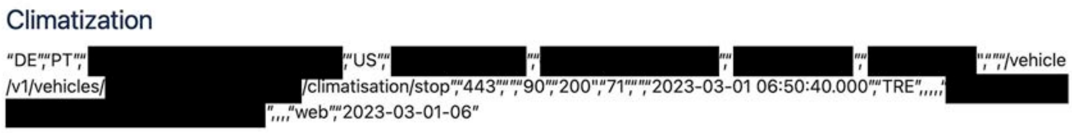
Doors. This API call seems to fetch the status of a specific vehicle's doors (locked/unlocked, open/closed). The vehicle is identified by the placeholder ID "YOUR_VEHICLE_ID", which will be replaced with the actual vehicle ID in a real request.



Remote Start

```
CA,T,[redacted]:443,-,-,[redacted],[redacted],GET,443,,90,200,71,HTTPS,2023-03-27
12:13:45.000,,,[redacted],,https://[redacted]/remote/start,[redacted]
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
Safari/537.36",,,web,2023-03-27-12
```

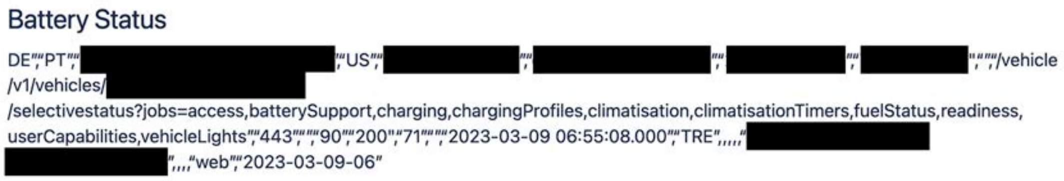
Remote start. This API call is a POST request to the OEM's API to remotely start the vehicle.



Climatization

```
“DE”,“PT”,“[redacted]”,“US”,“[redacted]”,“[redacted]”,“[redacted]”,“[redacted]”,“”,“/vehicle
/v1/vehicles/[redacted]/climatisation/stop”,“443”,“”,“90”,“200”,“71”,“”,“2023-03-01 06:50:40.000”,“TRE”,,,,,“[redacted]
”,,,,“web”,“2023-03-01-06”
```

Climatization. This API call is a request to an unspecified car brand’s vehicle API. The call is made to stop the climatization (air conditioning or heating) in a specific vehicle, identified by vehicle ID in the URL.



Battery Status

```
DE”,“PT”,“[redacted]”,“US”,“[redacted]”,“[redacted]”,“[redacted]”,“[redacted]”,“”,“/vehicle
/v1/vehicles/[redacted]
/selectivestatus?jobs=access,batterySupport,charging,chargingProfiles,climatisation,climatisationTimers,fuelStatus,readiness,
userCapabilities,vehicleLights”,“443”,“”,“90”,“200”,“71”,“”,“2023-03-09 06:55:08.000”,“TRE”,,,,,“[redacted]
”,,,,“web”,“2023-03-09-06”
```

Battery status. This API call is another request to the same unspecified car brand’s API. This request asks for “selective status” of various aspects of the vehicle, such as access, battery support, charging, charging profiles, climatization, climatization timers, fuel status, readiness, user capabilities, and vehicle lights.

Next, we try to answer the question: If a malicious actor obtains this data, what could they learn, and how might they misuse or abuse it?

- **User behaviors** – The route calculation API request contains information about the start and end points of a journey. If we see repeated patterns of the same start and end points, we might infer that this is a regular commute. This also tells us where we can consistently expect to find the vehicle during the day or night.
- **Vehicle status and capabilities** – The API requests to fetch door status, stop climatization, and get selective status indicates the ability to remotely control and monitor different aspects of the vehicle.
- **Device usage** – User agent strings provide detailed information about the operating system, browser, and device used to make the request.
- **Traffic analysis** – The timestamps of the API calls could allow us to determine when certain functions are most used.
- **Security posture** – Depending on how these API calls are made, we can evaluate the security measures in place. For instance, if the APIs are called over HTTP instead of HTTPS, it could indicate a security vulnerability as HTTP is not secure. Similarly, if API keys are used in a non-secure manner, such as being embedded in the URL, it might suggest potential security risks.
- **User-vehicle interaction** – By observing the types and frequencies of API calls, we can understand how users are leveraging connected vehicle technology.

The five instances we examine here are examples of APIs that have values in plain text and are part of the URL request. This is an unsecure method of API communications and anyone who can sniff network traffic, whether from a home router or a mobile phone (via a mobile hotspot), can listen to these API requests and intercept the data. It is a well-established fact that routers are vulnerable to cyberattacks, which could lead to compromise and the installation of malware, such as botnet malware.[51] Botnet malware can intercept network traffic and exfiltrate sensitive data. Trend Micro published a paper exploring methods of router compromise and how router data is exfiltrated.[52] Unsecure API communications between a vehicle app and the OEM/T1/T2 cloud back-end can be intercepted if a home router gets compromised and malware is installed on it, thus jeopardizing the security and privacy of the vehicle's data. This could lead to unauthorized access to sensitive vehicle data, manipulation of vehicle functions, or even tracking of the vehicle's location, posing significant risks to the vehicle owner's privacy and safety.

8. Conclusion

Modern vehicles have evolved into complex data hubs. An ecosystem has developed around vehicle data where data is collected, distributed, and used in innovative ways. However, a data-centric ecosystem brings with it a unique set of challenges. Most notably, drivers lack awareness and control over data generation, transmission, and sharing.[53, 54, 55, 56] This creates unknowns in their daily digital footprints, raising serious concerns about data privacy and misuse or abuse, and creates trust issues with the vehicle OEMs.

Vehicle data is accessible via multiple points like APIs and apps. Its use has great potential, and it will become a major revenue stream for the automotive industry. But concerns surface when we delve into the anonymity of vehicle data. Fully anonymized vehicle data loses its value because profiling becomes difficult, and without profiling (individual or group), monetization becomes challenging. Thus, we believe that there is not truly fully anonymized vehicle data. As monetization grows, leading to strong revenue, this will inevitably attract cybercriminals. The risks are evident, and we expect that the first large-scale attacks against connected cars will likely target data, potentially escalating to more sensational attacks like vehicle hacking and fleet takeover. Therefore, protecting vehicle data becomes critical.

The advent of new business models rewarding drivers for sharing their data has the potential to strike a balance between preserving privacy and enabling technological progress. This also aligns well with the smart city vision, where data sharing will streamline urban life. At the same time, the legislative gaps in vehicle data collection and usage need to be addressed. The automotive industry cannot operate effectively in a regulatory vacuum; appropriate legislation is imperative to provide clarity and stability. There is an urgent need for stakeholders to recognize the criticality of this issue and to work toward a resolution.

The convergence of automotive and tech brings about tremendous opportunities, but it must be navigated prudently. OEMs, T1 and T2 suppliers, and data brokers play significant roles in the vehicle data ecosystem. Their actions and decisions heavily impact the safety, privacy, and overall experience of drivers. Therefore, it is critical for these stakeholders to take proactive measures to ensure responsible data handling and prevent misuse or abuse.[57] In parallel, there is a need to address regulatory gaps in the realm of vehicle data collection and usage.

Here are our five recommendations for improving automotive data cybersecurity:

1. **Implement robust data protection measures.** As vehicles become more connected and generate a wealth of data, it is vital to implement robust data protection measures. This includes encryption of data at rest and in transit, secure APIs, and secure cloud storage. Regular security audits and penetration testing should be conducted to identify and fix potential vulnerabilities.

2. **Inform users.** Many drivers are unaware of the extent to which their vehicles collect data and how it is used. OEMs and other stakeholders should inform users about data collection practices, potential risks, and how to protect their data. This could include clear, easy-to-understand privacy policies and instructions on how to adjust data collection settings or how to fully opt out.

3. **Secure vehicle APIs.** APIs are a common point of access for cybercriminals. Therefore, securing vehicle APIs should be a priority. This could include measures such as strong authentication, rate limiting, and regular monitoring and logging of API activity to detect and respond to any suspicious activities.

4. **Regulate data collection and usage.** There is a need for clear regulations governing the collection, storage, and use of vehicle data. This includes who has access to the data, how long it is stored, and for what purposes it can be used. Regulatory bodies need to develop and enforce data privacy and protection laws to safeguard drivers.

5. **Develop secure middleware APIs.** Middleware APIs in connected cars can create new opportunities for cybercriminals by giving them easy API access to the vehicles' E/E architectures and ECUs. Therefore, these APIs should be designed with security in mind, including strong authentication and encryption, to prevent unauthorized access.

As the automotive industry navigates toward connected smart vehicles and the data economy, it is important to strike a balance between driving innovation and preserving privacy and security.

Appendix: Vehicle Network Architecture

Connected cars primarily communicate wirelessly, but there are exceptions, such as when an electric vehicle (EV) is connected to the power supply and can communicate with the grid or other back-end infrastructure over the power line.[58] Modern connected cars have internal network architectures as diverse as the cars themselves. Components communicate using standardized protocols, but no two network architectures are identical. They can even vary between different makes and models from the same manufacturer. It is important to have a high-level understanding of the network architecture because we need to understand where data is generated inside the car and who consumes data.

To explore the functions and interactions of in-vehicle components, we created a generic vehicle network architecture. This is not a network architecture from a production vehicle, but rather a theoretical visualization of the network topology and the major components in the vehicle's internal network.

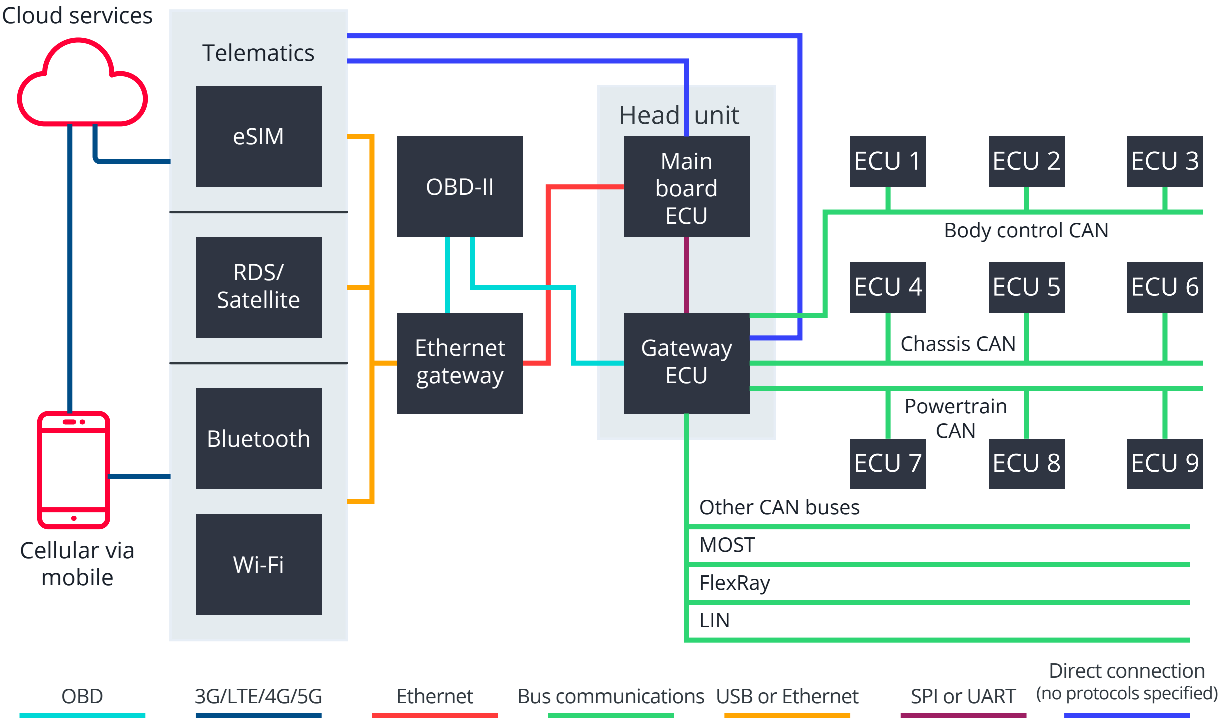


Figure 11. The generic network architecture of a modern-day connected car

In our generic vehicle network architecture, the major components and their interactions are:

- The **telematics control unit** (**TCU**) includes the **electronic SIM (eSIM)** that allows the car to communicate with 3G/4G/5G networks. It can transmit telematics data, communicate with cloud back-end servers, receive real-time data, and allow access to the internet, among other capabilities.

- The **RDS/satellite** unit receives digital information in FM broadcasts and from satellite broadcasts. Using RDS-TMC (Radio Data System – Traffic Message Channel), the car can receive real-time traffic alerts that are then displayed in the **head unit**. The satellite component enables cellular-satellite connectivity for data and provides traffic information and alerts by subscription.

- **Bluetooth** and **Wi-Fi** connectivity are common in modern cars. Mobile phones connect via Bluetooth to the head unit. Some cars can create a Wi-Fi hotspot to provide internet connectivity to the passengers as well as connect to the home Wi-Fi network to download over-the-air (OTA) software updates. Mobile phones connected via Bluetooth and/or Wi-Fi to the vehicle can tether to give the vehicle access to the internet via their cellular networks.

- **OBD-II** is the on-board self-diagnostics for the car. The OBD-II port can communicate with the head unit as well as talk directly to the CAN bus and send and receive CAN messages and commands.

- The **Ethernet gateway** handles all the data switching between the RF (radio frequency) modules and the head unit. In some vehicle networks, the Ethernet gateway can directly communicate with the gateway ECU. In our generic architecture, we have the Ethernet gateway communicate via the head unit.

- The **main board electronic control unit (ECU)** is the central processor for the head unit. It handles functions like navigation, display, playing the radio, managing network connections, and climate control. In our architecture, it communicates with the gateway ECU via SPI (Serial Peripheral Interface) or UART (Universal Asynchronous Receiver-Transmitter) protocols to send and receive CAN messages and commands.

- The **gateway ECU** handles all communications with the different buses: CAN (Controller Area Network), LIN (Local Interconnect Network), MOST (Media Oriented Systems Transport), and FlexRay. Other bus protocols exist, but we highlight these four as they are commonly found in most car models. The gateway ensures that no applications can directly communicate with the buses, and it switches messages correctly to the target bus. It also does message validation to make sure the messages are conformant.

- The **ECUs** in the car communicate via their connected bus and handle functions such as engine control, traction control, door locks, climate control, battery management, hybrid powertrain, airbags, and radar.

References

1. CAA National. (n.d.). *CAA National.* "Vehicle Data Privacy." Accessed on Sept. 20, 2023, at https://www.caa.ca/your-rights/data-privacy/.
2. Deloitte Canada. (n.d.) *Deloitte Canada.* "Implications of Connected and Autonomous Vehicles in Ontario." Accessed on Sept. 20, 2023, at https://www2.deloitte.com/ca/en/pages/consulting/articles/connectedvehiculesontario.html.
3. Tom Krisher and Dee-Ann Durbinap. (Sept. 30, 2016). *AP News.* "Q&A: The data your car collects and who can use it." Accessed on Sept. 20, 2023, at https://apnews.com/31c018cdbc634d42a7c97d04774954b1.
4. Steve Stecklow, Waylon Cunningham, and Hyunjoo Jin. (April 7, 2023). *Reuters.* "Tesla workers shared sensitive images recorded by customer cars." Accessed on Sept. 20, 2023, at https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.
5. McKinsey. (Sept. 1, 2014). *McKinsey.* "What's driving the connected car." Accessed on Sept. 20, 2023, at https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car.
6. Matt Bubbers. (Jan. 15, 2020). *The Globe and Mail.* "What kind of data is my new car collecting about me? Nearly everything it can, apparently." Accessed on Sept. 20, 2023, at https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything/.
7. Geoffrey A. Fowler. (Dec. 17, 2019). *The Washington Post.* "What does your car know about you? We hacked a Chevy to find out." Accessed on Sept. 20, 2023, at https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/.
8. bimmerconnected. (n.d.). *GitHub.* "bimmerconnected/bimmer_connected." Accessed on Sept. 20, 2023, at https://github.com/bimmerconnected/bimmer_connected.
9. BMW Group. (n.d.). *BMW Group.* "BMW Open Data Platform." Accessed on Sept. 20, 2023, at https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/technical-configuration/api-documentation.
10. BMW Group. (February 2021). *BMW Group.* "BMW CarData Glossary." Accessed on Sept. 20, 2023 at https://bmwcardata.bmwna.com/telematicKeys/EN/BMWCarDataTelematicsDataGlossary.pdf.
11. Rolls-Royce Motor Cars. (January 2020). *Rolls-Royce Motor Cars.* "Rolls-Royce CarData Telematics Data Catalogue." Accessed on Sept. 20, 2023, at https://www.rolls-roycemotorcars.com/content/dam/rrmc/marketUK/rollsroycemotorcars_com/downloads/Rolls-Royce_CarData_Data_Catalogue.pdf.
12. Geotab. (Nov. 28, 2022). *Geotab.* "Data Set for Geotab Integrated Solution for Ford Vehicles." Accessed on Sept. 20, 2023, at https://support.geotab.com/pl-PL/oem-integration/mygeotab/doc/ford-data-set.
13. GM Developers. (n.d.). *GM Developers.* "GM Developers." Accessed on Sept. 20, 2023, at https://developer.gm.com/.
14. Flespi. (n.d.). *Flespi.* "General-motors-onstar protocol." Accessed on Sept. 20, 2023, at https://flespi.com/protocols/general-motors-onstar#parameters.
15. Geotab. (Nov. 17, 2022). *Geotab.* "Data Set for Geotab Integrated Solution for GM." Accessed on Sept. 20, 2023, at https://support.geotab.com/oem-integration/mygeotab/doc/gm-data-set.
16. Geotab. (n.d.). *Google Docs.* "Rate Plan Features - Geotab Integrated Solution for GM [PUBLIC]." Accessed on Sept. 20, 2023, at https://docs.google.com/document/d/10OMkJ0qn--pErAidaoSrQxW22NYyj3E4dW_9Pf6DBCU/edit#heading=h.p3m487xv8635.
17. Mercedes-Benz. (n.d.). *Mercedes-Benz /developers.* "Meet all our products." Accessed on Sept. 20, 2023, at https://developer.mercedes-benz.com/products?vt=cars&vt=vans&vt=smart.
18. Mercedes-Benz. (n.d.). *Postman.* "Mercedes-Benz." Accessed on Sept. 20, 2023, at https://www.postman.com/mbdevelopers/workspace/mercedes-benz/overview.
19. Marc Ruef. (n.d.). *scip.* "Car Hacking - Analysis of the Mercedes Connected Vehicle API." Accessed on Sept. 20, 2023, at https://www.scip.ch/en/?labs.20180405.
20. Zimlon. (n.d.). *Zimlon.* "Data That Tesla Collects From Customers." Accessed on Sept. 20, 2023, at https://www.zimlon.com/b/comprehensive-list-of-data-tesla-collects-from-their-customers-cm529/.
21. Tesla JSON API (Unofficial). (n.d.). *Tesla JSON API (Unofficial).* "Tesla JSON API (Unofficial)." Accessed on Sept. 20, 2023, at https://tesla-api.timdorr.com/.
22. timdorr. (n.d.). *GitHub.* "timdoor/tesla-api." Accessed on Sept. 20, 2023, at https://github.com/timdorr/tesla-api/blob/master/ownerapi_endpoints.json.
23. arjenvrh. (n.d.). *GitHub.* "arjenvrh/audi_connect_ha." Accessed on Sept. 20, 2023, at https://github.com/arjenvrh/audi_connect_ha.
24. Caruso. (n.d.). *Caruso.* "Developer Portal." Accessed on Sept. 20, 2023, at https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/.
25. Samsara. (n.d.). *Samsara.* "Overview." Accessed on Sept. 20, 2023, at https://developers.samsara.com/reference/overview.
26. Otonomo. (n.d.). *Otonomo.* "Automotive Data." Accessed on Sept. 20, 2023, at https://otonomo.io/data/.

27. Otonomo. (n.d.). *Otonomo.* “Fleet (Workspace) Access Token.” Accessed on Sept. 20, 2023, at https://docs.otonomo.io/reference/service-access-token.

28. Smartcar. (n.d.). *Smartcar.* “Smartcar API reference.” Accessed on Sept. 20, 2023, at https://smartcar.com/docs/api.

29. High Mobility. (n.d.). *High Mobility.* “Brands.” Accessed on Sept. 20, 2023, at https://www.high-mobility.com/car-api.

30. High Mobility. (n.d.). *Airtable.* “HIGH MOBILITY Auto API Level 13.” Accessed on Sept. 20, 2023, at https://airtable.com/shry3EDO6lLiBunTm/tblCBBV23F1zBOnhl.

31. Geotab. (n.d.). *Geotab.* “Data Set for Geotab Integrated Solution for International Trucks.” Accessed on Sept. 20, 2023, at https://support.geotab.com/oem-integration/doc/truck-data.

32. Open Vehicles. (n.d.). *Open Vehicles.* “Open Vehicles Monitoring System.” Accessed on Sept. 20, 2023, at https://docs.openvehicles.com/en/latest/index.html.

33. Geotab Developers. (n.d.). *Geotab Developers.* “MyGeotab API Reference.” Accessed on Sept. 20, 2023, at https://geotab.github.io/sdk/software/api/reference/.

34. Geotab. (June 9, 2022). *Geotab.* “Analytics API Explorer.” Accessed on Sept. 20, 2023, at https://support.geotab.com/mygeotab/mygeotab-add-ins/doc/analytics-api.

35. AutoPi. (n.d.). *AutoPi.* “AutoPi API.” Accessed on Sept. 20, 2023, at https://api.autopi.io/.

36. Invers Developers. (n.d.). *Invers Developers.* “API Reference.” Accessed on Sept. 20, 2023, at https://developers.invers.com/api-reference/.

37. fiquett. (n.d.). *GitHub.* “fiquett/Viper_SmartStart_Control.” Accessed on Sept. 20, 2023, at https://github.com/fiquett/Viper_SmartStart_Control.

38. BMW Group. (May 2023). *BMW Group.* “CarData / Prices.” Accessed on Sept. 20, 2023, at https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/pricing.

39. Mercedes-Benz. (n.d.). *Mercedes-Benz /developers.* “Pay As You Drive Insurance.” Accessed on Sept. 20, 2023, at https://developer.mercedes-benz.com/products/pay_as_you_drive_insurance.

40. Netflix. (n.d.). *Netflix.* “How to use Netflix on your Tesla display.” Accessed on Sept. 20, 2023, at https://help.netflix.com/en/node/112323/ca.

41. James Vincent. (July 12, 2022). *The Verge.* “BMW starts selling heated seat subscriptions for $18 a month.” Accessed on Sept. 20, 2023, at https://www.theverge.com/2022/7/12/23204950/bmw-subscriptions-microtransactions-heated-seats-feature.

42. Numaan Huq et al. (May 23, 2023). *VicOne.* “What Lies in Store for Connected Cars in the Cybercriminal Underground?” Accessed on Sept. 20, 2023, at https://vicone.com/blog/what-lies-in-store-for-connected-cars-in-the-cybercriminal-underground.

43. Tencent Keen Security Lab. (Jan. 2, 2020). *Keen Security Lab Blog.* “Exploiting Wi-Fi Stack on Tesla Model S.” Accessed on Sept. 20, 2023, at https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/.

44. Numaan Huq, Rainer Vosseler, and Yurika Baba. (2021). *Trend Micro.* “Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN R155 Attack Vectors and Beyond.” Accessed on Sept. 20, 2023, at https://documents.trendmicro.com/assets/white_papers/wp-a-roadmap-to-secure-connected-cars.pdf.

45. EC-Council. (n.d.). *EC-Council.* “DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis.” Accessed on Sept. 20, 2023, at https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/.

46. Volvo Cars. (n.d.). *Volvo Cars.* “Google Assistant, Google Maps and Google Play in your Volvo car.” Accessed on Sept. 21, 2023, at https://www.volvocars.com/intl/v/connectivity/infotainment-page.

47. Amazon.com. (n.d.). *Amazon.com.* “Vehicles with Alexa.” Accessed on Sept. 21, 2023, at https://www.amazon.com/alexa-auto/b?ie=UTF8&node=17744356011.

48. Sam Curry. (Jan. 3, 2023). *Sam Curry.* “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More.” Accessed on Sept. 21, 2023, at https://samcurry.net/web-hackers-vs-the-auto-industry/.

49. Federico Maggi, Rainer Vosseler, and Davide Quarta. (2018). *Trend Micro.* “The Fragility of Industrial IoT’s Data Backbone: Security and Privacy Issues in MQTT and CoAP Protocols.” Accessed on Sept. 21, 2023, at https://documents.trendmicro.com/assets/white_papers/wp-the-fragility-of-industrial-IoTs-data-backbone.pdf.

50. Flightradar24. (n.d.). *Flightradar24.* “Flightradar24.” Accessed on Sept. 21, 2023, at https://www.flightradar24.com/.

51. Trend Micro. (n.d.). *Trend Micro.* “Securing Home Routers.” Accessed on Sept. 21, 2023, at https://www.trendmicro.com/vinfo/us/security/news/home-router.

52. Joey Costoya et al. (2017). *Trend Micro.* “Securing Your Home Routers: Understanding Attacks and Defense Strategies.” Accessed on Sept. 21, 2023, at https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf.

53. Xavier Walton. (July 4, 2023). *NewsNation.* “Your car is probably collecting your data. Here’s what you can do.” Accessed on Sept. 21, 2023, at https://www.newsnationnow.com/business/tech/car-data-collection-protect-yourself/.

54. Jack Morse. (Sept. 18, 2021). *Mashable.* "Your car knows too much about you. That could be a privacy nightmare." Accessed on Sept. 21, 2023, at https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect.

55. Jeff Plungis. (May 2, 2018). *Consumer Reports.* "Who Owns the Data Your Car Collects?" Accessed on Sept. 21, 2023, at https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/.

56. Matt Burgess. (June 21, 2023). *Wired.* "How Your New Car Tracks You." Accessed on Sept. 21, 2023, at https://www.wired.com/story/car-data-privacy-toyota-honda-ford/.

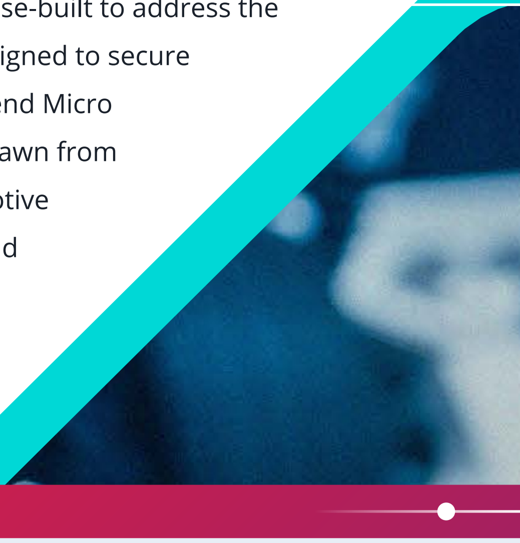
57. Steve Stecklow, Waylon Cunningham, and Hyunjoo Jin. (April 7, 2023). *Reuters.* "Tesla workers shared sensitive images recorded by customer cars." Accessed on Sept. 21, 2023, at https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

58. Ezio Bassi et al. (June 16, 2009). *IEEE Xplore.* "Powerline communication in electric vehicles." Accessed on Sept. 21, 2023, at https://ieeexplore.ieee.org/document/5075439.

VicOne

Driving Automotive Cybersecurity Forward

With a vision to secure the vehicles of tomorrow, VicOne delivers a broad portfolio of cybersecurity software and services for the automotive industry. Purpose-built to address the rigorous needs of automotive manufacturers, VicOne solutions are designed to secure and scale with the specialized demands of the modern vehicle. As a Trend Micro subsidiary, VicOne is powered by a solid foundation in cybersecurity drawn from Trend Micro's 30+ years in the industry, delivering unparalleled automotive protection and deep security insights that enable our customers to build secure as well as smart vehicles.



Learn more about VicOne by visiting vicone.com or scanning this QR code:

IN COLLABORATION WITH

TREND MICRO™ Trend Research