# Feasibility of Designing a Third-Party Anti-Theft Dongle for Vehicles

## Introduction

Vehicle theft is a pervasive and growing problem. In 2023, the nationwide rate of motor vehicle theft in the United States was 318.7 reported cases per 100,000 population 1, with over a million vehicles stolen across the country 2. This alarming trend has fueled a growing demand for effective anti-theft solutions 3. This report delves into the feasibility of designing a third-party dongle that plugs into a vehicle's OBD-II port to prevent or mitigate theft. We will examine existing anti-theft technologies, vehicle vulnerabilities, potential security risks, legal and regulatory challenges, and the potential market for such a device.

## Existing Vehicle Anti-Theft Technologies and Their Effectiveness

Modern vehicles often include factory-installed anti-theft systems, such as:

* **Audible and Visible Devices:** Alarms, flashing lights, and steering wheel locks deter theft by drawing attention to unauthorized entry 4. Steering wheel locks, for example, can cost around $30 to $50 5.
* **Immobilizing-Type Devices:** Immobilizers prevent the engine from starting without the correct key or fob 4.
* **Vehicle Recovery Systems:** These systems use electronic transmission technology to help law enforcement locate stolen vehicles 4. GPS tracking systems, for example, can cost around $50 to $100 6.

While these technologies offer a degree of protection, they are not infallible. Car alarms are often ignored due to their tendency to produce false alarms 7. More sophisticated thieves can bypass immobilizers with specialized tools and knowledge 8. However, it's important to note that the introduction of immobilizers has been linked to a decrease in car thefts overall 9.

## Vulnerabilities of Modern Vehicles to Theft

Despite advancements in vehicle security, modern vehicles remain susceptible to theft due to various factors:

* **Keyless Entry System Hacking:** Thieves can exploit vulnerabilities in keyless entry systems to intercept and relay signals from key fobs, unlocking and starting vehicles without the physical key 10. This technique, known as "relay theft," involves two thieves working in tandem – one capturing the key fob signal near the owner's home and another relaying that signal to the vehicle 11. Similarly, "code grabbing" allows thieves to intercept and copy the code from a key fob when the owner uses it to lock or unlock the car 10.
* **OBD-II Port Exploitation:** The OBD-II port, primarily intended for diagnostics, can be exploited by thieves to access the vehicle's systems, disable alarms, and even program new keys 10. Thieves can use readily available devices to clone key fobs, disable alarm systems, or even reprogram the vehicle's Engine Control Unit (ECU) 12.
* **Inadequate Security Measures:** Some vehicles, particularly older models, lack comprehensive security features, making them easier targets 13.
* **Owner Complacency:** Many car thefts occur due to owners leaving their vehicles unlocked or with keys easily accessible 13.

## Data Accessible Through the OBD-II Port

The OBD-II port provides access to a wealth of vehicle data, which can be accessed using various tools, including diagnostic scanners, mobile apps, and telematics devices 14. This data includes:

| Data Type | Description | Relevance to Anti-Theft |
| --- | --- | --- |
| Engine Speed | Real-time engine RPM 15 | Detecting unauthorized vehicle movement |
| Vehicle Speed | Real-time vehicle speed 15 | Triggering alerts for speeding or unauthorized movement |
| Diagnostic Trouble Codes (DTCs) | Error messages indicating malfunctions 15 | Identifying potential vulnerabilities that could be exploited by thieves |
| Vehicle Identification Number (VIN) | A unique identifier for the vehicle 15 | Verifying vehicle identity and ownership |
| Emission readiness status | Information about the vehicle's emission control systems 16 | Ensuring compliance with emission standards |
| Fuel Consumption | Real-time fuel usage 17 | Detecting unusual fuel consumption patterns that may indicate tampering |
| Coolant Temperature | Engine coolant temperature 17 | Monitoring engine health and detecting potential overheating issues |
| Ignition Cycles | Number of times the engine has been started 16 | Tracking vehicle usage and detecting unauthorized starts |
| Mileage | Distance traveled by the vehicle 17 | Monitoring vehicle usage and detecting discrepancies |

The CAN bus, which carries this data, operates at speeds of 250 or 500 kbps 18.

## Potential Security Risks of a Third-Party Dongle

While a third-party anti-theft dongle can enhance vehicle security, it also introduces potential security risks:

* **Unauthorized Access:** If not properly secured, the dongle itself could be vulnerable to hacking, potentially allowing unauthorized access to the vehicle's systems 19. This could involve exploiting vulnerabilities in the dongle's communication protocols or its firmware. For example, a lack of authentication mechanisms could allow attackers to connect to the dongle and gain access to the CAN bus 19.
* **Malicious Firmware Updates:** Attackers could potentially exploit vulnerabilities to install malicious firmware updates on the dongle, compromising its functionality or even using it to gain control of the vehicle 19. This could involve intercepting and modifying legitimate firmware updates or exploiting vulnerabilities in the dongle's update mechanism.
* **Data Interception:** If the dongle transmits data wirelessly, there is a risk of data interception, potentially exposing sensitive vehicle information or even tracking the vehicle's location 19. Attackers could use various techniques, such as eavesdropping on wireless communication channels or exploiting vulnerabilities in the dongle's encryption, to intercept data.
* **OBD-II Port Hacking:** Thieves can use techniques like CAN injection to introduce malicious messages onto the CAN bus, potentially disrupting vehicle functions or gaining control of critical systems 20. They can also potentially reprogram the ECU through the OBD-II port, disabling security features or even creating new keys 21.

## Legal and Regulatory Challenges

Developing and selling a third-party anti-theft dongle that plugs into the OBD-II port may present legal and regulatory challenges:

* **Vehicle Warranty Concerns:** Some vehicle manufacturers may void warranties if aftermarket devices are installed 22. This is due to concerns that third-party devices could interfere with vehicle systems or cause malfunctions.
* **Data Privacy Regulations:** Regulations like the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) may restrict the collection and use of vehicle data 23. These regulations aim to protect consumer privacy by giving individuals more control over their personal data. CCPA, for example, gives consumers the right to know what personal information is being collected, the right to delete that information, and the right to opt-out of the sale of their personal information 23. GDPR has similar provisions, including the right to access, rectify, and erase personal data 23.
* **Compliance with OBD-II Standards:** The dongle must comply with OBD-II standards and regulations to ensure compatibility and avoid interference with vehicle systems 24. These standards define the physical connector, communication protocols, and data formats used by the OBD-II system. For example, the dongle must adhere to the specified CAN bus speed and use the correct CAN IDs for communication 24.
* **Product Liability:** If the dongle malfunctions or interferes with vehicle safety systems, there could be potential product liability issues 22. This highlights the importance of thorough testing and ensuring the dongle's design does not compromise vehicle safety.

## Potential Market for a Third-Party Dongle

There is a growing market for vehicle anti-theft devices, driven by increasing vehicle theft rates and consumer demand for enhanced security 3. The global vehicle anti-theft system market size was estimated at USD 13.53 billion in 2023 25. This market can be segmented into different categories, such as those targeting individual car owners versus fleet managers 3.

Several companies already offer OBD-II security solutions. For example, MITI offers the OBD Protector, a metal lock that covers the OBD-II port to prevent unauthorized access 26. Another company, KēZ, offers a plug-and-play adapter that provides features like touch alert, VIN authentication, and vehicle immobilization 27.

A third-party dongle that offers effective protection, user-friendly features, and addresses security and privacy concerns could potentially capture a significant share of this market 28.

## Design Considerations for an Anti-Theft Dongle

To maximize effectiveness and market potential, the following design considerations are crucial:

* **Robust Security:** Implement strong encryption, authentication, and access control mechanisms to prevent unauthorized access and data breaches 19. This could involve using secure communication protocols, implementing secure boot processes, and regularly updating the dongle's firmware to patch vulnerabilities.
* **Tamper Resistance:** Design the dongle to resist physical tampering and attempts to remove or disable it 12. This could involve using tamper-evident seals, secure enclosures, and sensors that detect tampering attempts.
* **Data Privacy:** Prioritize data privacy by minimizing data collection, ensuring secure storage and transmission, and complying with relevant regulations 23. This could involve implementing data anonymization techniques, using secure storage solutions, and providing users with clear information about data collection and usage practices.
* **User-Friendly Interface:** Provide a user-friendly interface for setup, control, and monitoring, potentially through a mobile app 6. This could involve using intuitive design principles, clear instructions, and features that simplify user interaction.
* **Compatibility:** Ensure compatibility with a wide range of vehicle makes and models 29. This could involve using standardized communication protocols and providing adapters or different versions of the dongle for different vehicle types.
* **Integration with Existing Systems:** Consider integrating the dongle with existing vehicle security systems, such as alarms and immobilizers, for enhanced protection 30. This could involve using the dongle to trigger the alarm system in case of unauthorized access or using the immobilizer to prevent the engine from starting if the dongle is tampered with.
* **Dongle Types:** While OBD-II dongles are common, other types of dongles exist, such as those that connect directly to the CAN bus 21. These dongles may offer more direct access to vehicle systems and potentially more robust security features. However, they may also be more complex to install and may require more specialized knowledge.
* **Dongle Inaccuracies:** It's important to acknowledge potential inaccuracies with OBD-II dongles, such as those related to mileage tracking 31. These inaccuracies can arise from factors like GPS signal limitations or variations in vehicle sensor data.
* **Integration with Emerging Technologies:** Explore the potential for integrating the dongle with other emerging technologies, such as biometric authentication or smartphone-based vehicle control 32. This could involve using fingerprint sensors or facial recognition to authenticate users or allowing users to control vehicle functions through their smartphones.

## Synthesis

The development of a third-party anti-theft dongle presents a compelling opportunity in the rapidly evolving landscape of vehicle security. The increasing prevalence of vehicle theft, coupled with the rise of sophisticated theft techniques, underscores the need for innovative solutions that go beyond traditional anti-theft measures.

This report has highlighted the feasibility of designing such a dongle, leveraging the OBD-II port as an access point to vehicle systems and data. By incorporating robust security features, tamper-resistance mechanisms, and user-friendly interfaces, a well-designed dongle can effectively mitigate the risk of vehicle theft.

However, it is crucial to acknowledge the challenges associated with this endeavor. Security risks, such as unauthorized access and malicious firmware updates, must be addressed through rigorous security protocols and continuous vulnerability assessments. Legal and regulatory challenges, including vehicle warranty concerns and data privacy regulations, require careful navigation to ensure compliance and avoid potential liabilities.

Furthermore, the competitive landscape demands a thorough understanding of existing solutions and market segmentation to effectively position the dongle and capture a significant market share.

In conclusion, the design and development of a third-party anti-theft dongle is feasible and holds significant promise in addressing the growing concern of vehicle theft. By prioritizing security, privacy, and user experience, while navigating legal and regulatory complexities, this project can contribute to a safer and more secure automotive ecosystem.

#### Works cited

1. U.S. reported motor vehicle theft rate 1990-2023 - Statista, accessed February 11, 2025, <https://www.statista.com/statistics/191216/reported-motor-vehicle-theft-rate-in-the-us-since-1990/>

2. Top 8 Anti-Theft Devices to Protect Your Car - InsureOne, accessed February 11, 2025, <https://www.insureone.com/knowledge-center/auto-insurance/car-anti-theft-devices/>

3. Trends Shaping the $17.1 Billion Automotive Security Systems Market, 2030 - GlobeNewswire, accessed February 11, 2025, <https://www.globenewswire.com/news-release/2025/01/28/3016620/28124/en/Trends-Shaping-the-17-1-Billion-Automotive-Security-Systems-Market-2030-How-Smart-Vehicles-are-Revolutionizing-Automotive-Security-with-AI-Powered-Protection.html>

4. Vehicle Theft Prevention - NHTSA, accessed February 11, 2025, <https://www.nhtsa.gov/vehicle-safety/vehicle-theft-prevention>

5. Anti Theft For Cars - Amazon.com, accessed February 11, 2025, <https://www.amazon.com/anti-theft-cars/s?k=anti+theft+for+cars>

6. CARLOCK Anti Theft Car Device - Real Time 4G Car Tracker & Car Alarm System. Comes with Device & Phone App. Tracks Your Car in Real Time & Notifies You Immediately of Suspicious Behavior.OBD Plug&Play - Amazon.com, accessed February 11, 2025, <https://www.amazon.com/CARLOCK-Anti-Theft-Car-Device/dp/B00U0K3Q10>

7. Do car alarms really keep me protected? | Rate.com, accessed February 11, 2025, <https://www.rate.com/insurance/resources/do-car-alarms-really-keep-me-protected/>

8. Will an immobilizer save your car from being stolen? - Kaspersky, accessed February 11, 2025, <https://usa.kaspersky.com/blog/36c3-immobilizers/20264/>

9. What Is A Theft Device Immobilizer? - J.D. Power, accessed February 11, 2025, <https://www.jdpower.com/cars/shopping-guides/what-is-a-theft-device-immobilizer>

10. Combatting high-tech auto theft | Zurich Insurance, accessed February 11, 2025, <https://www.zurichna.com/knowledge/articles/2024/11/high-tech-auto-theft>

11. 8 types of vehicle theft - Confused.com, accessed February 11, 2025, <https://www.confused.com/car-insurance/guides/eight-types-of-vehicle-theft>

12. Protect Your OBD2 Port From Theft - GPS LEADERS, accessed February 11, 2025, <https://gpsleaders.com/protect-your-obd2-port-from-theft/>

13. Reasons Why Car Theft Happens and How To Prevent Them - LotGuard, accessed February 11, 2025, <https://www.lot-guard.com/resources/blog/why-car-theft-happens/>

14. What Is the OBD-II Port and What Is It Used For? - MakeUseOf, accessed February 11, 2025, <https://www.makeuseof.com/tag/obd-ii-port-used/>

15. What Is OBDII? History of On-board Diagnostics (OBD) - Geotab, accessed February 11, 2025, <https://www.geotab.com/blog/obd-ii/>

16. What Data is Available from OBD?, accessed February 11, 2025, <https://www.obdsol.com/knowledgebase/on-board-diagnostics/what-data-is-available-from-obd/>

17. Demystifying the OBD-II Port: Unlocking Fleet Management Potential - Fleetcam, accessed February 11, 2025, <https://www.fleetcam.com/obd-ii-port-unlocking-fleet-management/>

18. What is OBD2? A Detailed Guide for Vehicle Upkeep - White Label GPS Tracking Software, accessed February 11, 2025, <https://trackobit.com/blog/what-is-obd-2>

19. Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT - USENIX, accessed February 11, 2025, <https://www.usenix.org/system/files/sec20summer_wen_prepub.pdf>

20. What is OBD Hacking & How Does It Work? - Infiniti Tracking, accessed February 11, 2025, <https://www.infinititracking.co.uk/what-is-obd-hacking-how-does-it-work/>

21. Car Hacking with Python — Part 1 Data Exfiltration: GPS and OBDII/CAN Bus - Medium, accessed February 11, 2025, <https://medium.com/spark1-us/car-hacking-with-python-part-1-data-exfiltration-gps-and-obdii-can-bus-69bc6b101fd1>

22. OBD dongles and OEM warranties - PTOLEMUS Consulting Group, accessed February 11, 2025, <https://www.ptolemus.com/insight/obd-dongles-and-oem-warranties/>

23. Key data sovereignty regulations in the automotive industry - InCountry, accessed February 11, 2025, <https://incountry.com/blog/key-data-sovereignty-regulations-in-the-automotive-industry/>

24. Introduction to the OBD-II Standard - Kvaser, accessed February 11, 2025, <https://kvaser.com/about-can/can-standards/introduction-to-obd-ii/>

25. Vehicle Anti-theft System Market Size & Share Report, 2030 - Grand View Research, accessed February 11, 2025, <https://www.grandviewresearch.com/industry-analysis/vehicle-anti-theft-system-market-report>

26. Amazon.com: MITI OBD Protector - 5 Pack Fleet Bundle | Metal OBD2 Port Lock Cap, accessed February 11, 2025, <https://www.amazon.com/MITI-OBD-Protector-Anti-Theft-Locking/dp/B09VFWZ8K2>

27. KēZ: Home, accessed February 11, 2025, <https://www.getkez.ca/>

28. Car Security System Market Scope, Demand and Forecast to 2031 - InsightAce Analytic, accessed February 11, 2025, <https://www.insightaceanalytic.com/report/car-security-system-market-/1923>

29. What is an immobilizer - Mastergard Anti-theft Immobilizer, accessed February 11, 2025, <https://www.mastergard.com/immobilization>

30. Do car alarms work? - Elephant Insurance, accessed February 11, 2025, <https://www.elephant.com/blog/do-car-alarms-really-work>

31. Why you shouldn't use OBD-II dongles to verify mileage · Smartcar blog, accessed February 11, 2025, <https://smartcar.com/blog/obd-mileage-verification>

32. OBD2 pinout explained. Major car brands pinouts - FlexiHub, accessed February 11, 2025, <https://www.flexihub.com/oobd2-pinout/>