Keyless Cars

Risks and How to Protect Yourself

RISCCO | January 5th 2026 | 12 minutes | 2280 words

Contents

1. Executive Summary
2. What is the problem?
3. Common Vehicle Theft Techniques: Keyless Cars
4. Security Tips and Best Practices.

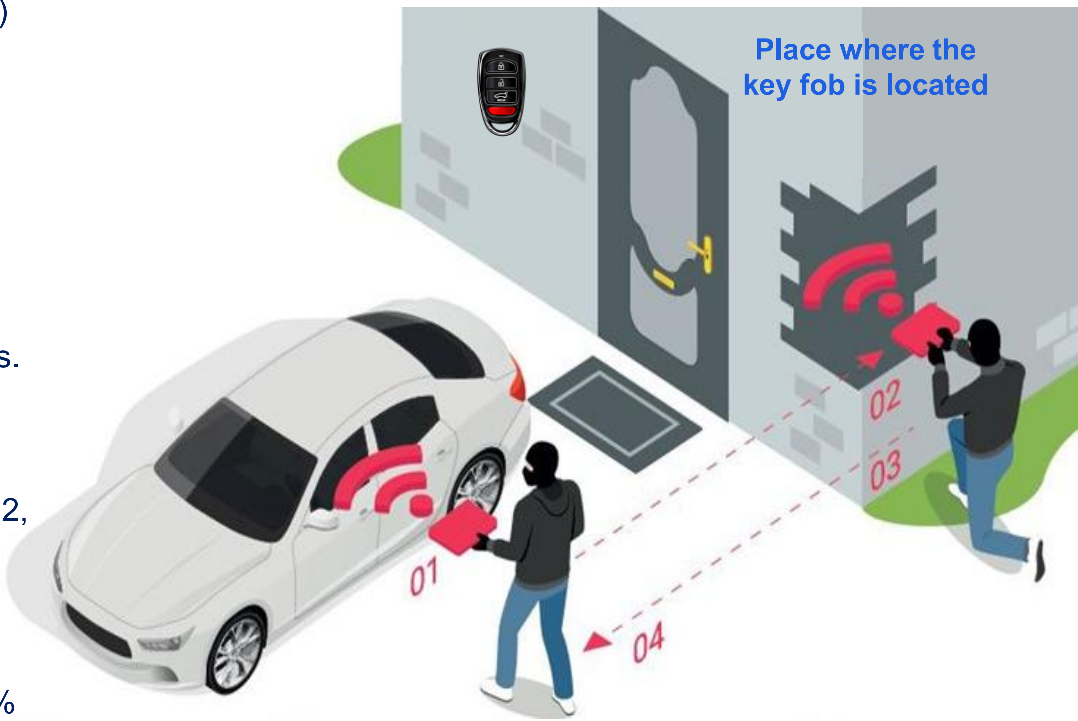
Note: This document is for informational and educational purposes only. It does not constitute a security assessment of any manufacturer or specific model, nor does it guarantee that events will occur or be prevented. It is not legal, technical, or insurance advice. The recommendations described can reduce risk, but they do not eliminate the possibility of theft. Before installing aftermarket devices, consult your dealership and/or insurer.

1. Executive Summary

Keyless vehicles (keyless entry and push-button start) were designed to maximize convenience by using wireless communication between the car and the key fob (electronic key). The challenge is that, because these systems rely on radio-frequency signals and many models lack advanced controls such as UWB (*Ultra-Wideband*) they create an expanded attack surface that, in certain scenarios, may enable unauthorized unlocking and/or starting in a very short time, without the need to break windows or force locks.

Keyless features became widely adopted starting around 2015, while the use of UWB technology in automotive use cases began accelerating around 2022, but it has not yet been widely deployed.

A technical reference in Europe, ADAC (Allgemeiner Deutscher Automobil-Club), reported in November 2025 that, under controlled testing, approximately 85% (685 of 802) of the evaluated models showed vulnerabilities associated with keyless access/start scenarios. This type of evidence suggests the risk is not merely theoretical.



Source: https://leasing.com/guides/relay-car-theft-what-is-it-and-how-can-you-avoid-it/

This article summarizes three main risks: (1) Relay attacks, where two attackers “extend” the key fob’s signal so the car believes the key is nearby and allows the doors to unlock—and in some cases even enables the vehicle to start; (2) Jamming attacks, where the lock signal is blocked and the car may be left unlocked; and (3) OBD-II port attacks, which require physical access to the vehicle’s interior and apply to both keyless vehicles and vehicles that use a traditional physical key.   We invite you to review this article to better understand the risks described above and, most importantly, to consider and adopt the practical security tips and best practices provided.

1. What is the problem?

Keyless vehicles (keyless entry and push-button start) were designed to maximize convenience through radio-frequency communication between the vehicle and the key fob (electronic key) or other authorized device—similar in concept to the Wi-Fi technology used in your home.

The challenge is that, because these systems rely on radio-frequency signals to authorize unlocking and/or starting—and many models lack advanced controls such as UWB (Ultra-Wideband)—they create an expanded attack surface that, in certain scenarios and under specific conditions, can allow a vehicle to be stolen in a very short time (for example, in under 90 seconds). Although UWB technology has existed since the 1980s, its use in automotive applications (such as digital keys and precise distance verification) began accelerating around 2022, but it has not yet been widely deployed.

Globally, keyless features became widespread starting around 2015. A technical benchmark in the European automotive sector, the ADAC (Allgemeiner Deutscher Automobil-Club), in its annual report conducted since 2016, reported in November 2025 that approximately 85% (685 out of 802) of the models analyzed were compromised. In addition, it noted that only 8% included UWB technology.

Electronic Key fob

The same document also notes that, in its tests, models equipped with UWB (Ultra-Wideband) have shown greater resistance to this type of exposure, while other measures (such as certain motion sensors in the key fob) do not always provide the same level of protection consistently.

In this article, we explain the two main risks affecting keyless vehicles, along with a third risk related to the vehicle's OBD-II port, which applies to most relatively modern cars.

2. Common Vehicle Theft Techniques: Keyless Cars

For vehicles equipped with Passive Keyless Entry (PKE) (keyless entry and push-button start), there are two main types of attacks (risks), plus a third related risk. These are:

1. Relay Attack	2. Jamming Attack	3. OBD II Port Attack

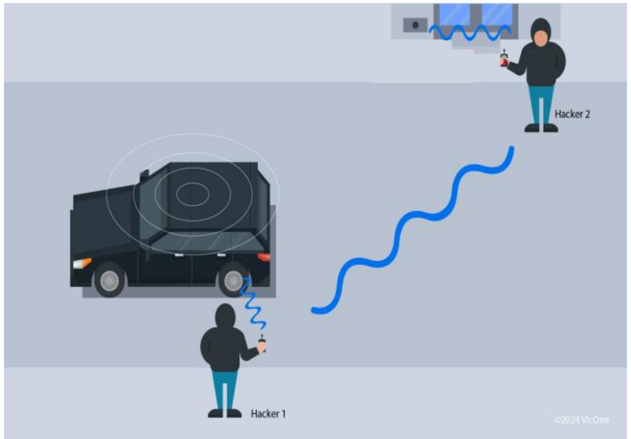
A relay attack (signal amplification and retransmission) is a theft technique that targets keyless vehicles (PKE)—the kind that unlock and start when the key fob is “nearby.” Instead of copying or cloning the key, the attacker tricks the vehicle into believing the key is right next to it.

How do they do it? They typically work in pairs. One person stays near the vehicle while the other gets close to the real key—such as near the front door of a house, inside a restaurant, or just a few meters from the owner. They use devices that “bridge” or extend the signal. The device near the key captures the key’s wireless communication and relays it to a second device near the car. As a result, the vehicle assumes the key is right beside it.

The outcome is that the car may unlock when the attacker pulls the door handle or presses the button on the handle, and in some cases may even allow the engine to start—all without breaking windows or forcing locks. That is why this type of theft is often fast, quiet, and leaves little visible evidence.

In markets such as the United Kingdom, multiple sources and industry reports have documented that a significant share of modern vehicle theft involves signal manipulation (for example, relaying or interference), confirming that wireless signals have become a frequent target.

Click here to watch an example video.



Note: In Central America and CARICOM, this issue is especially relevant because, based on publicly available information, UWB adoption in the region’s best-selling models remains limited.

2. Common Vehicle Theft Techniques: Keyless Cars

1. Relay Attack	2. Jamming Attack	3. OBD II Port Attack

A jamming attack (signal-blocking attack) is a technique in which a thief blocks or interferes with the wireless signal your key fob (electronic key) uses to lock the vehicle. They don’t need to copy your key—they simply prevent the car from receiving the “lock” command.

The typical scenario happens in supermarket parking lots, malls, stadiums, or similar places. You press the lock button on your key fob, you’re in a hurry, there’s noise around you, and you assume the car is locked.

But if a jamming attack is taking place, the signal doesn’t reach the vehicle, and it remains unlocked. Minutes later, the thief opens the door as if nothing happened and steals items from inside, or may even attempt to take the vehicle if they have time and opportunity. In higher-risk situations, the attacker could even try to surprise the driver.

This attack works so well because it exploits a common habit: not verifying whether the car actually locked.

Note: This attack can also affect vehicles with traditional remote controls (that require pressing a button) or aftermarket alarm systems, because it can block any wireless locking signal.

2. Common Vehicle Theft Techniques: Keyless Cars

1. Relay Attack	2. Jamming Attack	3. OBD-II Port Attack

An OBD-II port attack (the vehicle's diagnostics and maintenance port) occurs when a thief gains physical access to the inside of the vehicle and connects a device to the OBD-II diagnostic port (usually located under the steering wheel). In the wrong hands, this port can become a way to manipulate vehicle functions—for example, attempting to program a key, change parameters, or facilitate starting the vehicle—depending on the car model.

The key point is that this risk applies to both keyless vehicles and vehicles with a traditional physical key. It does not depend on whether the car unlocks "without a key"; it depends on whether the attacker can get into the cabin (because it was left unlocked, a window was broken, a door was forced, it was left with a third party, or a lapse was exploited) and has enough time to connect their device to the OBD-II port.

That is why, even if your vehicle is not keyless, the OBD-II port remains a relevant attack surface in modern vehicles. The critical issue here is not the wireless signal, but physical access to the car.

3. Security Tips and Best Practices

Type of Attack	Security Controls and Best Practices	Comments
1. **Relay Attack**	a. Check with your dealership whether your vehicle includes UWB (Ultra-Wideband), which improves precise distance/presence verification for the key fob and reduces the effectiveness of certain signal-relay attacks. b. Ask your dealership whether your key fob has a motion sensor (motion-sensing key fob), a feature that allows the key fob to enter sleep mode after a period of inactivity (depending on the manufacturer). This reduces the likelihood that the fob will respond when it is not being used. c. If neither of the above applies, consider a pouch or case based on the Faraday principle. A high-quality pouch can block or significantly attenuate radio-frequency signals when used correctly (for example, fully closed). When you are not using the vehicle and in higher-exposure public locations—store the key fob in a Faraday style pouch or case.	▪ According to the technology company Pozyx, in 2024 only 6% of new cars included UWB technology. ▪ Motion-sensing key fobs are a relatively recent feature, and their effectiveness depends on the key fob remaining still. If the key fob is in a pocket or in a handbag while you are moving, it may be less effective.

3. Security Tips and Best Practices

Type of Attack	Security Controls and Best Practices	Comments
2. **Jamming Attack**	a. Always confirm the vehicle is locked: check the lights, listen for the beep, and pull the door handle.	▪ This is a manual check you should perform regardless of whether your key fob includes the technologies mentioned above (No.1) such as UWB and/or a motion-sensing key fob—because those features do not protect against jamming attacks.
3. **OBD-II port Attack**	a. Install a physical lock/cover to make it harder to connect devices to the OBD-II port. b. Use a visible steering wheel lock / anti-theft bar. c. For high-value vehicles, consider an aftermarket immobilizer that uses a PIN or sequence (without relying on radio-frequency signals). This type of control requires an additional authentication step to start the engine.	▪ OBD-II port locks and steering wheel immobilizers can be purchased on Amazon or similar sites. ▪ These devices can be expensive and may affect the vehicle warranty depending on the manufacturer, model, and local dealership policies. RISCCO is not affiliated with any specific manufacturer of these devices.

Note: Consider installing a hidden GPS tracking service in your vehicle (it may involve monthly fees). This control serves as a last line of defense. GPS tracking can help locate and recover the vehicle.

Bibliography

1. ADAC (German Automobile Club) - Keyless Entry Security Testing 2016-2025
2. Tracker UK - High-Tech Car Theft Statistics 2023-2024
3. Victoria Police (Australia) - Vehicle Crime Squad Reports 2024
4. PCA Cyber Security - Real-World Car Theft Attack Surface Analysis 2025
5. Autowatch UK/Canada - Ghost-II CANbus Immobiliser Documentation
6. TASSA (Tracking and Aftermarket Security System Association)
7. Car Connectivity Consortium - Digital Key 3.0 / UWB Standard
8. GPS Leaders / Thatcham Research - OBD Port Security
9. University of Padova (PKES)
10. Vicone - From Key Fob to UWB: Explaining and Securing Ultra-Wideband in Vehicles
11. Keyless car theft: What is a relay attack, how can you prevent it, and will your car insurance cover it?

CONTACTS

Panama and CARICOM

Antonio Ayala I.
aayala@riscco.com

Rubén Fernández
rfernandez@riscco.com

Dominican Republic and Puerto Rico

Eury Valdez
efvaldez@riscco.com

El Salvador, Guatemala, Honduras, Costa Rica y Nicaragua

Gari Rojas
grojas@riscco.com

About RISCCO

RISCCO is an independent international consulting firm committed to transforming how organizations manage risk and adopt Artificial Intelligence. We combine a rigorous approach to GRC (Governance, Risk & Compliance) with advanced data analytics and Artificial Intelligence to help our clients anticipate risks, strengthen governance, and solve complex challenges. Headquartered in Panama with presence in six countries, in 2026 we celebrate 17 years serving more than 200 leading organizations across Central America and CARICOM.

International rigor. Agile execution. Measurable impact.
We think like strategists. We execute like specialists.

riscco.com

RISCCO