ENISA puts Cybersecurity in the driver's seat

ENISA, the European Union Agency for Cybersecurity highlights the importance of cybersecurity for connected cars in a new report.

Published on November 25, 2019



Tagged with

* [Cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=Cybersecurity)
* [Smart Cars](https://www.enisa.europa.eu/search?Subject%3Alist=Smart%20Cars)
* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)
* [Internet of things](https://www.enisa.europa.eu/search?Subject%3Alist=Internet%20of%20things)

**The Arrival of Smart Cars**

The automotive industry is undergoing an evolution towards connected and autonomous vehicles. Increasingly smart cars include added features that enhance users’ experience or improve car safety. However, if not properly secured, such features can also be leveraged by hackers, and lead to cyberattacks that can result in vehicle immobilisation, road accidents, financial losses, disclosure of sensitive data and even endanger road users’ safety.

Previous attacks on smart cars helped raise automotive industry awareness of the security needs and led to the development of several cybersecurity regulations and initiatives aimed at ensuring secure vehicles.

**Good Practices for Security of Smart Cars**

The [ENISA ‘Good practices for security of Smart Cars’ report](https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars) mainly aims to identify the relevant assets, the emerging threats targeting smart cars ecosystem of tomorrow as well as the potential security measures and good practices to mitigate them.

Concretely, the ENISA study provides the following information:

* A detailed asset and threat taxonomy for the connected and autonomous vehicles ecosystem.
* Concrete and actionable good practices to improve the cybersecurity in connected and autonomous vehicles.
* A mapping of existing legislative, standardisation and policy initiatives to foster harmonisation.

In 2017, ENISA published its first study on Smart Cars cybersecurity (The [ENISA Cybersecurity and Resilience of smart cars – Good practices and recommendations](https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars)). In this new report, the Agency broadens the scope of the study to the (semi-) autonomous cars and Vehicle-to-Everything (V2X) communications.

In particular, the study gathers in a single document security controls collected from relevant published documents and standards, covering the policies, organisational practices and technical aspects. Inter alia, the proposed security controls are mapped against those mentioned in the draft recommendation on cybersecurity of the UN Working Party on Automated/Autonomous and Connected Vehicles (GRVA).

**Juhan Lepassaar, Executive Director, ENISA**stated**:**

“*Connected and automated mobility is a strategic priority for the EU, bringing numerous opportunities for its citizens. Making sure that cybersecurity concerns are taken into account is the role of ENISA. Today we publish a study on securing smart cars with a focus on autonomous and semi-autonomous vehicles. Bringing together all players and reflecting ongoing policy developments, this work aims to serve as the reference for automotive cybersecurity.”*

**Target Audience**

As smart cars cybersecurity is a shared task amongst all smart cars stakeholders, the target audience of this study is mainly:

* Car manufacturers
* Tier 1 and Tier 2 car components suppliers
* Aftermarket suppliers
* Policy Makers