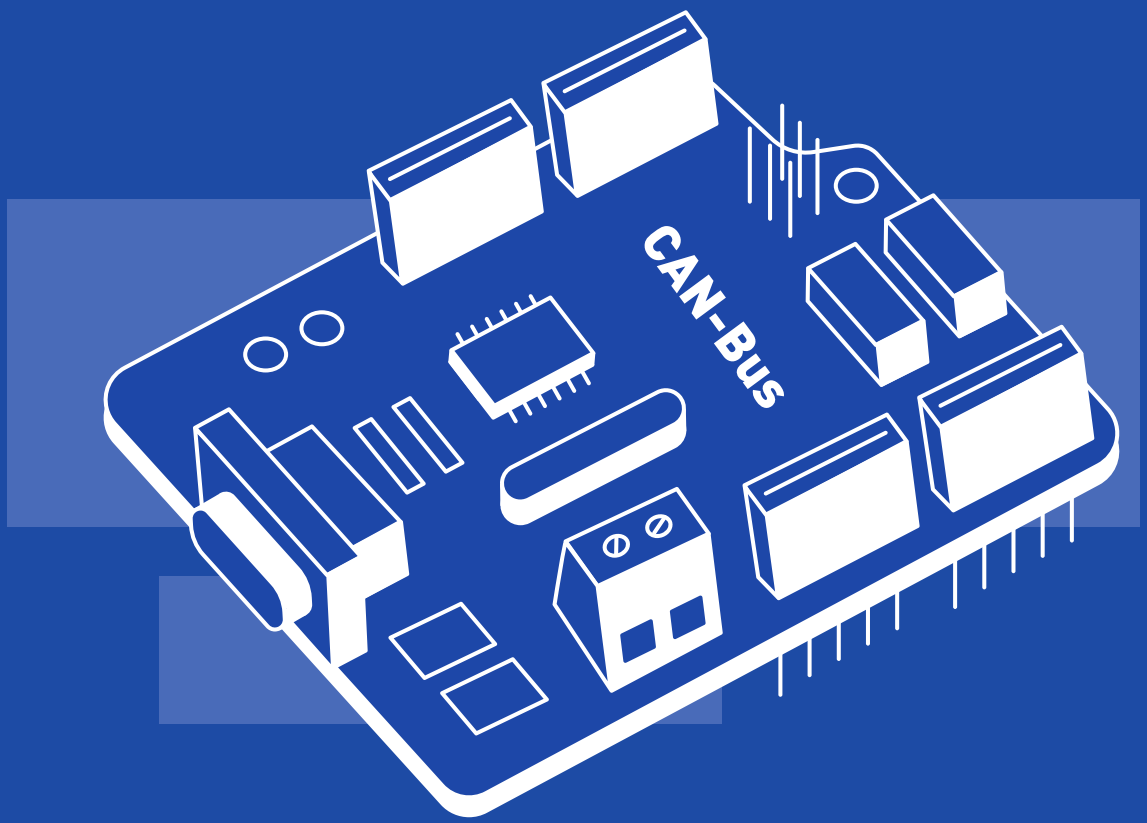
VDOO

VDOO's Security Platform for Connected Cars



Introduction

Connected cars are at the forefront of automobile technology. The most known aspect of connected cars are autonomous cars and semi-autonomous cars, such as Tesla© automobiles, yet today many common non-autonomous cars are also connected. A connected car includes many components for the comfort of the driver and passengers, such as infotainment systems, in-car wireless internet, and more. Furthermore, connected cars also include components that allow Over The Air (OTA) updates to the Engine Control Unit (ECU) and other critical elements, as well as allow the sending of statistical information back to manufacturers and maintenance service providers.

The motivation for the abundance of connected cars is clear: They allow passengers a more enjoyable ride, especially as time spent in daily commute increases every year. Connected cars also allow manufacturers to continuously update cars with new features, making them safer for drivers, surrounding cars, and pedestrians while reducing the number of accidents and their severity in case they are not prevented. Connected cars are predicted to account for up to 82% of all cars on the market by 2021. Therefore, connected cars already have an extensive, direct effect on the everyday life of millions, and this will only increase in the future.

This effect, by nature, constitutes a two-dimensional threat—privacy risk and physical threat. The privacy risk includes the ability to know the driver's daily routine and ways the car is used. At the same time, the physical risk includes the ability to control the car, causing potential damage that is unprecedented. Taking control over entertainment systems might lead to inconvenience; compromising ECU or other critical components might pose an immediate threat of a completely different magnitude. Since connected cars encompass many different connected technologies and automobile technologies, they also facilitate various, unstandardized communication protocols. The increased use of V2V and V2X communications have opened cars to new risks, such as control takeover and BSM interception.

VDOO's Solutions for Connected Cars

The automobile industry's unique characteristics are deeply rooted in VDOO's IoT security platform design and development, built to serve both users—drivers and passengers—and makers in the ecosystem. By using Vision™, VDOO's analysis solution, car makers can analyze firmware binaries of different devices in the car, regardless of their type or purpose, and receive an accurate description of the device's security status followed by mitigation guidance for device hardening. By using ERA™, VDOO's Embedded Runtime Agent solution, the car maker as

well as a fleet management company deploying connected cars can make sure they will remain safe and secure after deployment. Just like drivers look for NCAP© car safety, so can they rely on the VDOO CertIoT™ certification, which proves car makers have met a rigorous set of cyber security requirements. Car makers can rely on proactive solutions like Quicksand™, a threat detection honeypot that lures the attacker and provides real-time monitoring and alerts, and Whistler™, a device-specific push alerts system on any new threat. This end-to-end solution was built to handle both security and safety related threats, whether known or unknown, to allow laying the foundations for connected and secured cars.