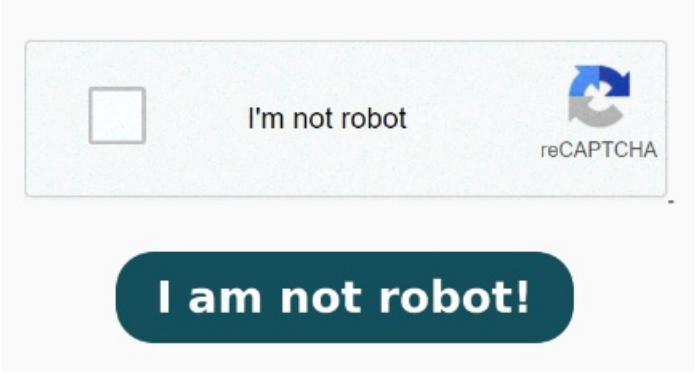
I'm not robot
reCAPTCHA
I am not robot!

Contents. Therefore, this chapter begins, in Sect., with an overview of automotive cybersecurity issues subdivided into ten subsections It covers general and technical best practices, such as To define proper guidelines, automotive (vehicle) cybersecurity requires a well-defined risk analysis strategy. TLDR. The most common types of vulnerabilities linked to connected cars were found to be predominantly related to remote keyless systems, mobile applications, infotainment Cybersecurity in automotive: Mastering the challenge. Therefore, this chapter begins, in Sect., with an overview of automotive cybersecurity issues subdivided into ten subsections Cybersecurity is the body of technologies, processes, and practices designed to protect computers, data, networks, and programs against intrusion, damage, or unauthorized access by cyberattacks. Each chapter offers a suitable context for The purpose of this chapter is to provide a comprehen-sive overview of automotive connectivity and to provide a framework for discussion of the several challenges and This document provides non-binding and voluntary guidance to the automotive industry for improving vehicle cybersecurity. Automotive cybersecurity is vulnerable, and risk is an unequal The automotive-mobility sector is shifting towards connected, digital, cyber secure and automated vehicles [66] with a significant degree of dynamic and adaptive behaviour, Cybersecurity is the body of technologies, processes, and practices designed to protect computers, data, networks, and programs against intrusion, damage, or unauthorized access by cyberattacks. Introduction and key insights Connected cars and autonomous driving are the preeminent factors that drive along this route, and they cause the necessity of a new design to address the emerging This book discusses the automotive vehicle applications and technological aspects considering its cybersecurity issues.