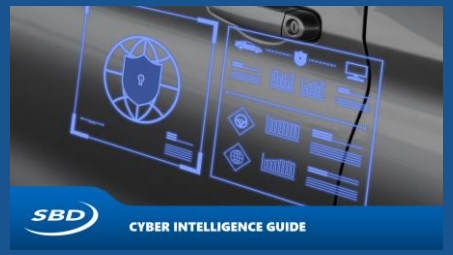


TABLE OF CONTENTS

RELATED SBD REPORTS

539 - Cyber Security Legislation Guide

The Automotive Cyber Security Legislation Guide has been designed to be a usable tool, focusing on what is necessary. The Guide shows the background and timeline of legislation, best practices and standards, but SBD's Cyber Security team has gone further, showing the implications and where you need to be looking, allowing the Legislation Guide to become a vital part of a robust cyber security strategy.

#905

CYB

Cyber Security

Cyber Intelligence Guide

An in-depth analysis of the public white and black-hat attacks on the evolving vehicle ecosystem, including technical analysis of hacking methods used and SBD's proposed mitigations aligned with industry best practice and UNECE R155 Annex 5.

The Cyber Security Intelligence Guide is designed to raise awareness on the diverse threats and vulnerabilities that affect vehicles and connected & autonomous vehicle systems. This report has been created to promote a positive security culture within OEMs, suppliers and other key players, with insights into the recommended defence and mitigation countermeasures, and to highlight the importance of incident response analysis within the industry.

The Cyber Security Intelligence Guide functions as a key foundation in a robust UNECE R155 compliance strategy that requires OEMs to continually assess their vehicles against the latest threats and vulnerabilities.

This report is not only aimed at system developers, but it also gives executives a broader understanding and insight of risk management and how this should be applied within their organisation and throughout their supply chain.

COVERAGE

GLOBAL | NA | CHINA | EUROPE

FREQUENCY

ANNUALLY | BI-ANNUALLY | ONE-OFF

PUBLICATION FORMAT

PDF | POWERPOINT | EXCEL | ONLINE

PAGES

250+

Request price

Key questions answered

- The primary destination for threat intelligence for the automotive industry.
- An in-depth analysis of the public attacks on the evolving vehicle ecosystem.
- Structured to match and encourage cyber strategy best practices.
- A key foundation in a robust UNECE R155 threat monitoring compliance strategy.
- Can be used as a training material as well as a knowledge base for analysts and engineers
- Drive smarter investments in terms of security and enable risk-informed decisions

This research supports

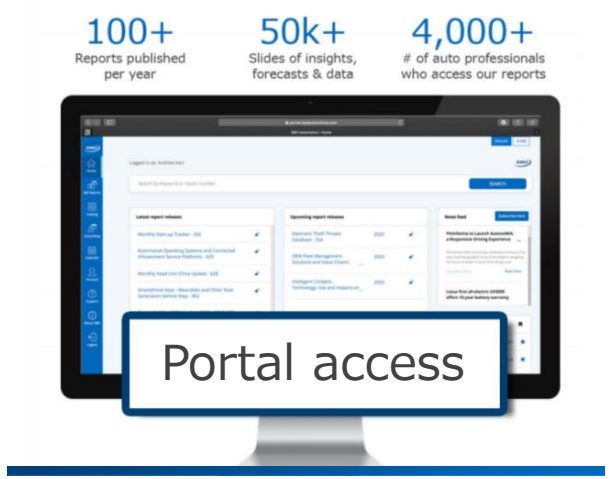
PRODUCT PLANNERS

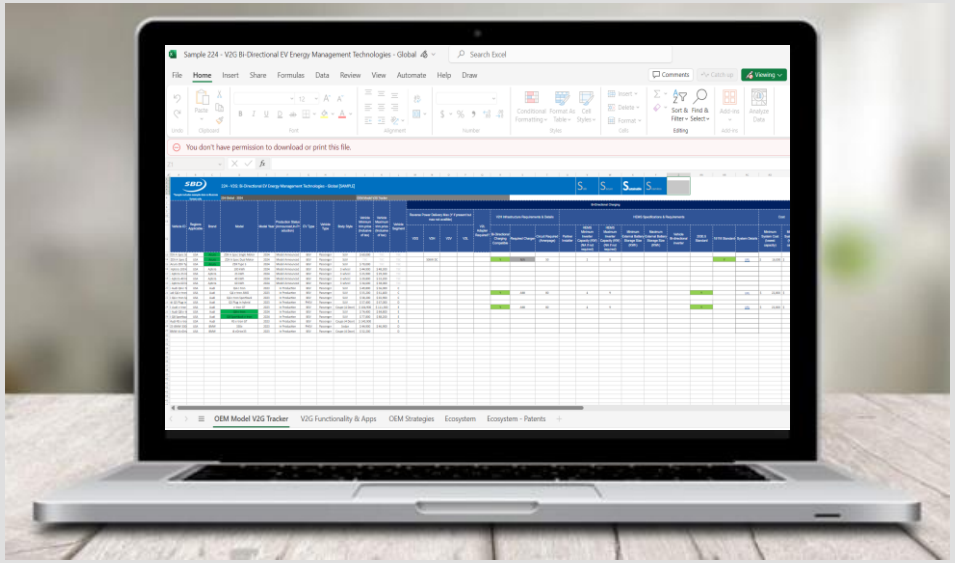
IT

MARKETING

ENGINEERING

Do I have access?





View Excel Data Sheet Sample

Cyber Intelligence Guide

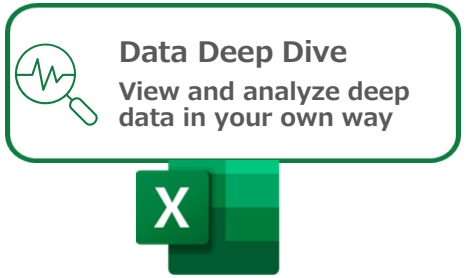
For a deep dive into raising awareness on the diverse threats and vulnerabilities that affect vehicles and systems

Click for Sample

CYBER INTELLIGENCE GUIDE

Contents Page

905 Cyber Intelligence Guide



Total number of pages – 258

Introduction

Purpose

Objectives

This Cyber Intelligence Guide provides an in-depth analysis of the key publicly-reported attacks on the evolving vehicle ecosystem, including technical analysis of the hacking methods used and suggested mitigations aligned with UNECE R155 and ISO/SAE 21434. SBD gathers data from a wide range of sources about white and black-hat attacks on vehicles and their backend systems which is analysed by our experts to produce actionable insights that can be used by OEMs and suppliers as part of their threat monitoring activities.

Significance

The purpose of this report is to:

- Raise awareness on the diverse threats and vulnerabilities that affect vehicles
- Help OEMs and suppliers evaluate and mitigate the risks to their products
- Provide an input into the threat monitoring process mandated by UNECE R155

An effective threat monitoring system requires OEMs to not only detect vulnerabilities on their own products using solutions such as IDS, SOC and even bug bounties, but also to be aware of the threats to competitor products so that the industry as a whole can promote a positive and open security culture where best practice is shared and on-going improvements embraced.

This report is not only aimed at cyber specialists, but it also gives senior managers a broader understanding and insight into cyber risk management and how this should be applied within their organisation and throughout their supply chain.

- **For Cyber Security Teams:** The technical information included in this report is intended to support the risk assessment of vehicles in development and in the field as well as feeding lessons learned into the security requirements process for future new models.
- **For Senior Managers:** The key trends and attack summaries are intended to provide an accessible overview of cyber risks that can result in legal, operational, financial and brand damage to their organisation and to enable smarter investments in terms of security and risk-informed decisions.

This report helps OEMs to meet the requirement to monitor for new cyber threats and vulnerabilities as defined in section 7.2.2.2.g and categorised in Annex 5 of the regulation.

This report provides specific security goals and requirements that OEMs and suppliers can integrate into the Concept Phase of their cyber engineering processes (chapter 9 of the standard).

Scope

SBD's Cyber Intelligence Guide is focused primarily on the attack demonstrations and exploited vulnerabilities that directly affect the vehicle and its backend ecosystem (i.e. product cyber security):

- The report is designed to be a digest of information with details of relevant and more recent attacks and not a complete historical repository
- The aim is to include a broad cross-section of damage scenarios associated with a range of attack targets and not to exhaustively list every example of similar attacks
- Apart from a few historically significant cases, the report will not cover incidents or attacks beyond the last 5 years

In addition, the report also includes a high-level summary of non-product related attacks on OEMs, their extended organization and their supply chain.

Sources Used	A wide range of source types are used for this threat intelligence report to increase its completeness and add value, including but not limited to the following: • Conferences and security events such as ESCAR, Black Hat, DEF CON, VDI, SAE and Auto-ISAC • Attack demonstrations published in academic research papers, blogs and news articles • Other online sources such as Social Media/Twitter, Reddit, GitHub and YouTube
Data Selection	All threats and vulnerabilities gathered are added to an internal database and then a decision-making process is followed to decide which threats are included in each quarter's report. To keep this report manageable, a number of filters are applied such as: • Attacks older than five years are not included, except if there are very significant • Old immobiliser attacks are not included • Old backend and smartphone related attacks are not included • Attacks that do not include sufficient information to complete the analysis are not included

Note: *The Cyber Intelligence Guide is a live resource that is updated with new information every two quarters. Research for this edition concluded on the* ***14th March 2024****.*

Example slides from the report

Request price

E-theft tools are as sophisticated as the countermeasures

Relay Attack

Relay attacks consist of intercepting and potentially storing the signal of the vehicle's smart key fob.

On a basic level, the attack is carried out by 2 thieves, one standing near the car and the other near the smart key fob.

Code Grabber

The code grabber is a device used to capture and store the coded signal transmitted by a key fob.

This signal is then simply replayed to unlock the vehicle.

Key Programming

Key programming consists of connecting a device to the vehicles' on-board diagnostic (OBD II) port or, via the system network.

Specific software is then used to program a key fob.

Transponder

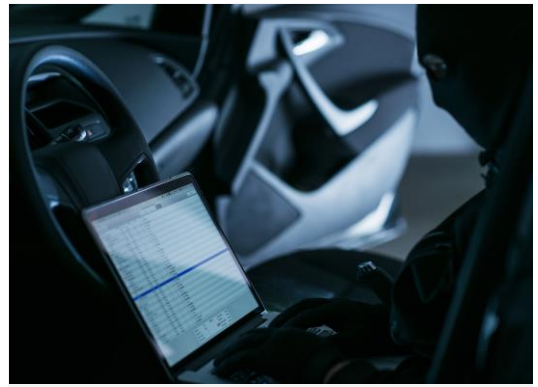
Transponders are small RFID devices, sometimes encased in glass or carbon but, more recently, fitted to the keyfob PCB. Transponders are designed to store and **trans**mit a coded signal after res**pond**ing to a correct know challenge.

Security Control

Security control covers other tools and devices designed to carry out a range or a specific action. Features include:

- Immobilizer reset and/or bypass
- Unlocking central locking
- Disabling the alarm
- Read and write data to/from EPROM or IC
- Read, decode or bypass PIN code

App based tools are likely to be developed and will use software and programming capabilities via a cloud server. **This will make proving that a device is used for the theft of a vehicle more difficult.**



E-Theft Threat Guide

The E-Theft Threat Guide identifies the range of methods that play a role in the theft of vehicles today. Theft tools and devices are extensively profiled on a number of topics - including their source, cost, and the type of theft they enable.

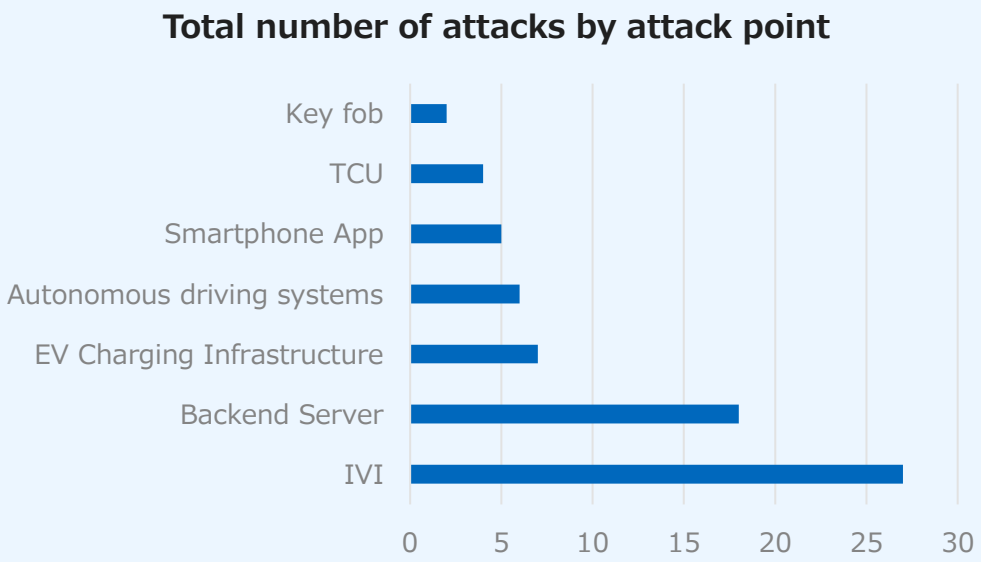
Learn more

Known Attack Target Trends

Top attack targets

The **Attack Target** is the term used for the main component or area being attacked. This is the component or area that is compromised by the attacker to cause the ultimate damage on the vehicle ecosystem. Analysing the attack target is beneficial during the risk management process, as it allows security specialists to identify vulnerabilities and develop countermeasures to mitigate the risk.

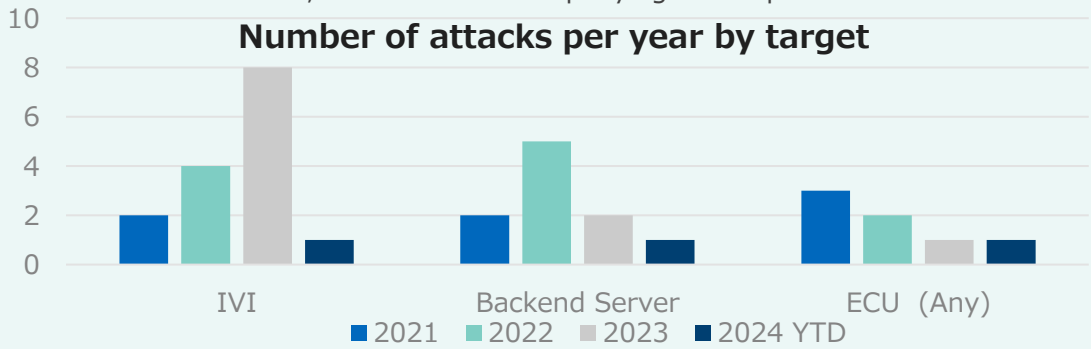
The graph below shows the highest risk targets are split between areas within the vehicle, such as the IVI and external targets such as backend servers and the smartphone app. Targets with cellular connectivity are particularly popular as they enable remote attacks and can escalate to include entire fleet attacks.

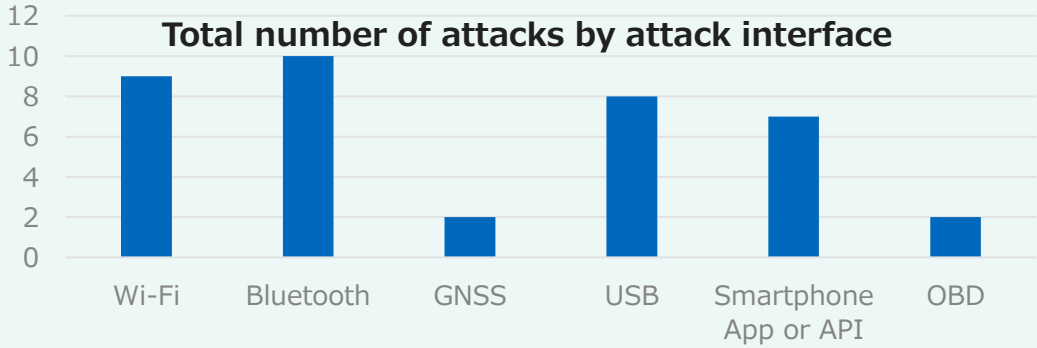


The attack target and attack interface continues to change

Interestingly, as the industry is moving towards increased levels of vehicle autonomy, autopilot is being tested by numerous security researchers and several attack demonstrations are becoming available. Sensors, cameras and components vital for the autopilot operation, are becoming popular targets as they can be tampered with to cause collisions. Successful attacks would have major safety, operational and financial impact.

For more information, refer to the accompanying Excel spreadsheet.



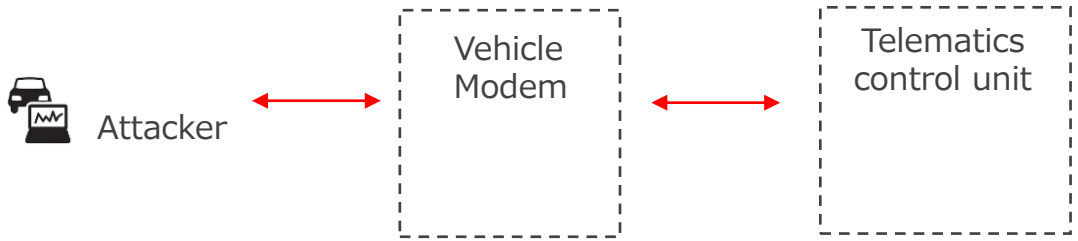


Multiple vulnerabilities discovered in Tesla Model 3

At the Pwn2Own Automotive hacking competition, researchers found a series of vulnerabilities in a Telsa modem. One set of vulnerabilities is presented in this report, but two additional vulnerabilities were found in the infotainment unit which allowed sandbox escape.

Hackers used a three-bug chain against the Tesla modem to gain access to the telematics control unit.

Cybersecurity researchers, Synactiv, gained unauthorized access to a Tesla modem. Gaining access allowed the hackers to extract data but also modify the TCU software as they had full control of the vehicle telematics control unit. At Pwn2Own, hackers are awarded a bounty on completion. The event benefits OEMs because details of the hack or not shred with the wider community. This works for OEMs because the cybersecurity community gets to understand vulnerabilities, but not enough to weaponize the vulnerabilities.



Attack Target	Attack Vector
TCU	Undisclosed
Attack Point/Interface	**Attack Feasibility**
Undisclosed	Undisclosed
Impact	
Safety / Financial / Operational / Privacy	
Attack Maturity	
Practical / Experimental / Theoretical	

Discovered by
Synactiv

Published on
26 Jan 2024

Details
Article

Click For a Technical Overview

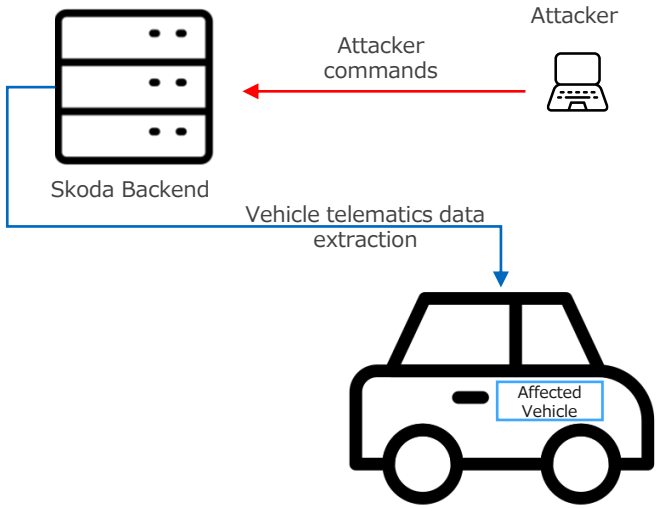
Skoda Automotive Cloud vulnerability

The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing to obtain nicknames and other user identifiers of Skoda Connect service users by specifying an arbitrary vehicle VIN number.

Exposure of sensitive information to an unauthorized actor

The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing remote attackers to obtain recent trip data, vehicle mileage, fuel consumption, average and maximum speed, and other information of Skoda Connect service users by specifying an arbitrary vehicle VIN number. An attacker can receive trip details by Škoda vehicle VIN number, if the primary user is registered in the vehicle (CVE-2023-28901). This issue is categorized as a Broken Access Control vulnerability. An attacker can act outside of the intended permissions that allow him to get information on trip timestamps, fuel consumption, speed and associated to VIN account nickname.

SBD has identified that such an attack could be turned to a denial-of-service attack especially damaging to electric vehicles, if the attacker was to repeatedly request vehicle data for a long period of time, resulting to battery depletion.



Attack Target	Attack Vector
Backend Server	Remote
Attack Point/Interface	**Attack Feasibility**
API	High
Impact	
Safety / Financial / **Operational** / **Privacy**	
Attack Maturity	
Practical / **Experimental** / Theoretical	

Discovered by

Vehicle owners

Published on

26 Jan 2024

Details

Article

Click For a Technical Overview

Request the price

Request price

Contact SBD Automotive

Do you have any questions?

If you have any questions or feedback about this research report or SBD Automotive's consulting services, you can email us at info@sbdautomotive.com or discuss with your local account manager below.

info@sbdautomotive.com

Book a meeting

USA | UK | Germany | India | China | Japan

Garren Carr
North America
garrencarr@sbdautomotive.com
+1 734 619 7969

Luigi Bisbiglia
UK, South & West Europe
luigibisbiglia@sbdautomotive.com
+44 1908 305102

SBD China Sales Team
China
salesChina@sbdautomotive.com
+86 18516653761

Andrea Sroczynski
Germany, North & East Europe
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

SBD Japan Sales Team
Japan, South Korea & Australia
postbox@sbdautomotive.com
+81 52 253 6201