SBD

SEC #905

Automotive Cyber Security Threat Intelligence Guide

Cyber Security

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.

TABLE OF CONTENTS

RELATED SBD REPORTS

SEC #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.

COVERAGE

NA CHINA EUROPE [✓ GLOBAL]

FREQUENCY

ANNUALLY [✓ QUARTERLY] ONE TIME

PUBLICATION FORMAT

[✓ PDF] [✓ POWERPOINT] [✓ EXCEL] ONLINE

PAGES

165

Key features and benefits

- > 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 is useful for

PRODUCT PLANNERS

ENGINEERS

C-SUITE

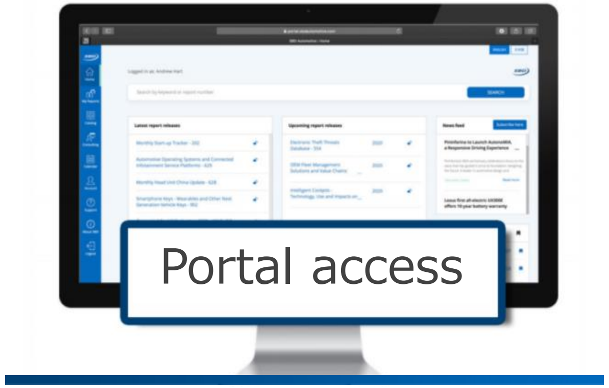
IT

Do I have access?

100+ Reports published per year

50k+ Slides of insights, forecasts & data

4,000+ # of auto professionals who access our reports



Request a quote for

Automotive Cyber Security Intelligence Guide

Request price >

Request price

CYBER INTELLIGENCE GUIDE

Contents Page

The SBD Cyber Intelligence Guide Spreadsheet is available in Excel

Total number of pages - 165

Introduction

The purpose, scope and methodology followed in this report

Contents Page

About SBD

Contact Us

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.

UNECE
R155

Cyber Security Regulation

UNECE

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.

ISO/SAE
21434

Cyber Security Engineering Standard

ISO SAE INTERNATIONAL

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:

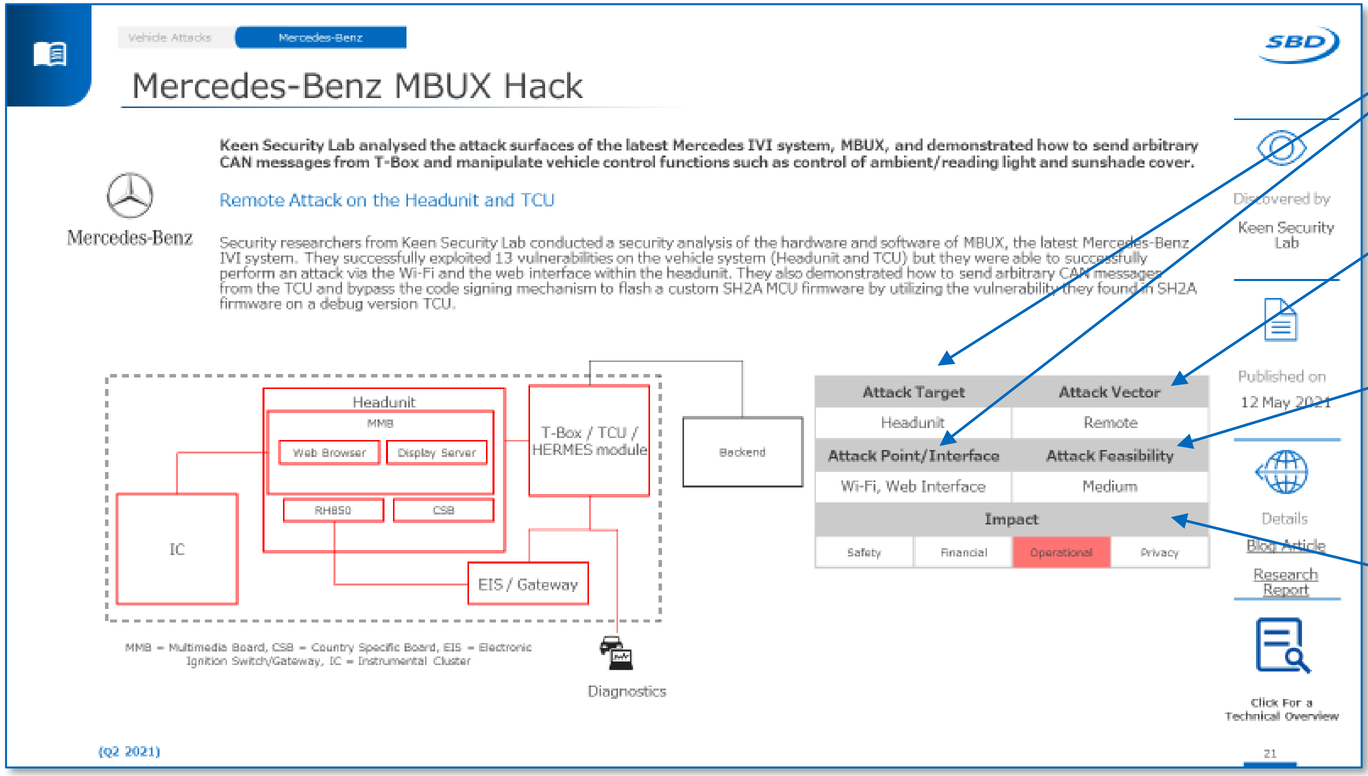
- Attacks older than five years are not included, except if there are very significant
- Old immobiliser attacks are not included
- Old backend and smartphone related attacks are not included
- Attacks that do not include sufficient information to complete the analysis are not included

***Note:** The Cyber Intelligence Guide is a live resource that is updated with new information each quarter. Research for this edition concluded on the **20th June 2022**.*

How to read this report (1/2)

Overview Page

The first page of each threat summary provides a high-level description of the attack, a system diagram to highlight the components involved and links for further information. It also includes a summary table with SBD's classification of the items listed below:



Vehicle Attacks | Mercedes-Benz

Mercedes-Benz MBUX Hack

Keen Security Lab analysed the attack surfaces of the latest Mercedes IVI system, MBUX, and demonstrated how to send arbitrary CAN messages from T-Box and manipulate vehicle control functions such as control of ambient/reading light and sunshade cover.

Remote Attack on the Headunit and TCU

Security researchers from Keen Security Lab conducted a security analysis of the hardware and software of MBUX, the latest Mercedes-Benz IVI system. They successfully exploited 13 vulnerabilities on the vehicle system (Headunit and TCU) but they were able to successfully perform an attack via the Wi-Fi and the web interface within the headunit. They also demonstrated how to send arbitrary CAN messages from the TCU and bypass the code signing mechanism to flash a custom SH2A MCU firmware by utilizing the vulnerability they found in SH2A firmware on a debug version TCU.

MMB = Multimedia Board, CSB = Country Specific Board, EIS = Electronic Ignition Switch/Gateway, IC = Instrumental Cluster

Attack Target	Attack Vector
Headunit	Remote
Attack Point/Interface	**Attack Feasibility**
Wi-Fi, Web Interface	Medium

Impact			
Safety	Financial	[✓ Operational]	Privacy

Discovered by
Keen Security Lab

Published on
12 May 2021

Details
Blog Article
Research Report

Click For a Technical Overview

(Q2 2021)

21

Attack target & point/interface

Describes the component and interface(s) that were targeted in the attack.

Attack vector

Describes if the attack can be performed remotely or if it requires physical access to a vehicle, hence providing an indication of scalability.

Attack feasibility

Provides SBD's subjective measure of the effort required to perform the attack by considering the feasibility parameters defined in Annex G of ISO/SAE 21434, namely elapsed time, expertise, equipment, prior knowledge of the system and window of opportunity.

Impact

Provides SBD's classification of the potential impact for damage scenarios relating to each attack based on the categories defined in Annex F of ISO/SAE 21434:

<u>Safety</u> - Damage that affects the safety of vehicle occupants, other road users and/or the infrastructure

<u>Financial</u> - Direct (liability issues, recalls, penalties) or indirect (reputation damage, loss of market share, IP infringement)

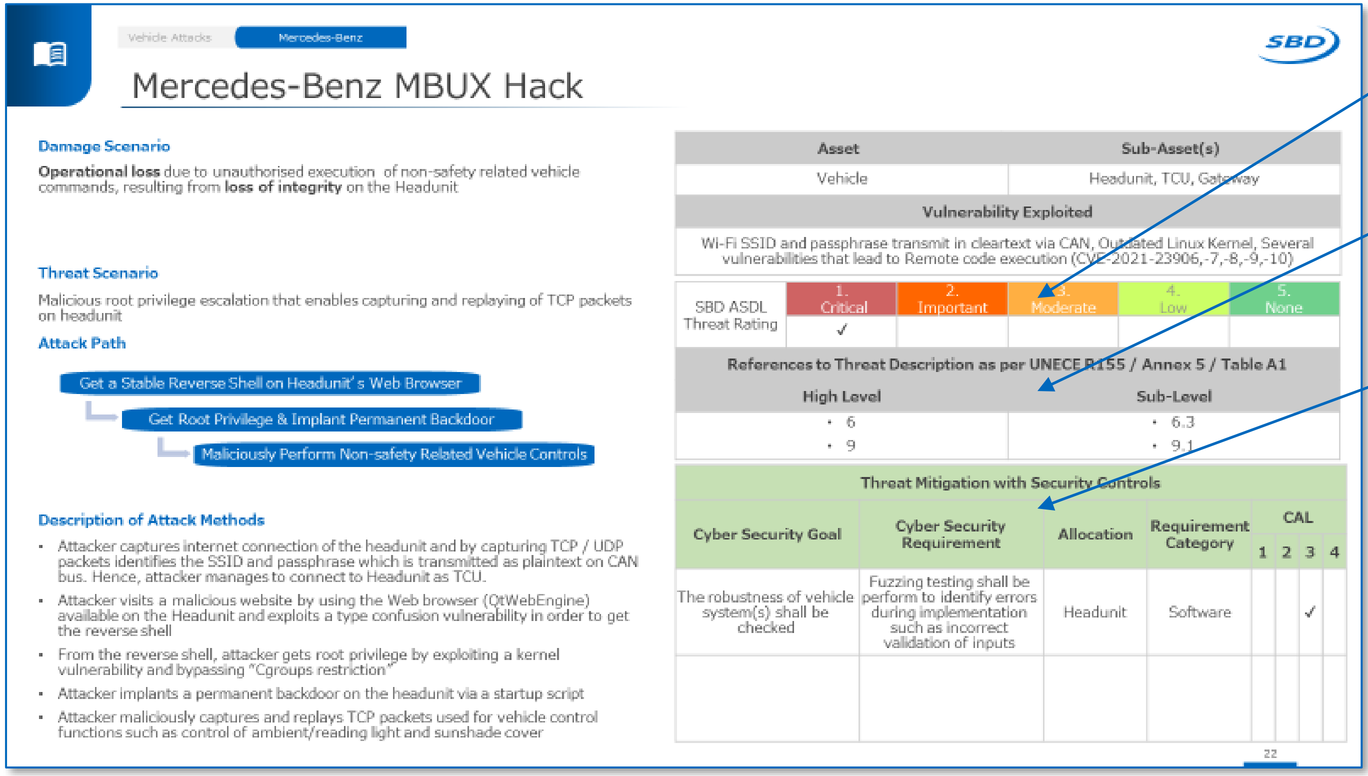
<u>Operational</u> – Loss, impairment or degradation of vehicle functions

<u>Privacy</u> – Lose of data that is sensitive and/or and be linked to a specific road user (PII)

How to read this report (2/2)

Technical Details Page

The second page of each threat summary provides a structured technical description of the attack using terminology aligned to ISO/SAE 21434, namely damage scenario, threat scenario, attack path etc. It also classifies the attack according to the descriptions provided in UNECE R155 Annex 5 and provides SBD's suggested mitigations, again aligned to ISO/SAE 21434 terminology for easy integration into an OEM or supplier threat analysis study.



Vehicle Attacks | Mercedes-Benz

Mercedes-Benz MBUX Hack

Damage Scenario

Operational loss due to unauthorised execution of non-safety related vehicle commands, resulting from **loss of integrity** on the Headunit

Threat Scenario

Malicious root privilege escalation that enables capturing and replaying of TCP packets on headunit

Attack Path

Get a Stable Reverse Shell on Headunit' s Web Browser

Get Root Privilege & Implant Permanent Backdoor

Maliciously Perform Non-safety Related Vehicle Controls

Description of Attack Methods

- Attacker captures internet connection of the headunit and by capturing TCP / UDP packets identifies the SSID and passphrase which is transmitted as plaintext on CAN bus. Hence, attacker manages to connect to Headunit as TCU.
- Attacker visits a malicious website by using the Web browser (QtWebEngine) available on the Headunit and exploits a type confusion vulnerability in order to get the reverse shell
- From the reverse shell, attacker gets root privilege by exploiting a kernel vulnerability and bypassing "Cgroups restriction"
- Attacker implants a permanent backdoor on the headunit via a startup script
- Attacker maliciously captures and replays TCP packets used for vehicle control functions such as control of ambient/reading light and sunshade cover

Asset	Sub-Asset(s)
Vehicle	Headunit, TCU, Gateway

Vulnerability Exploited
Wi-Fi SSID and passphrase transmit in cleartext via CAN, Outdated Linux Kernel, Several vulnerabilities that lead to Remote code execution (CVE-2021-23906,-7,-8,-9,-10)

SBD ASDL Threat Rating	1. Critical	2. Important	3. Moderate	4. Low	5. None
	✓				

References to Threat Description as per UNECE R155 / Annex 5 / Table A1	
High Level	Sub-Level
• 6 • 9	• 6.3 • 9.1

Threat Mitigation with Security Controls							
Cyber Security Goal	Cyber Security Requirement	Allocation	Requirement Category	CAL			
				1	2	3	4
The robustness of vehicle system(s) shall be checked	Fuzzing testing shall be perform to identify errors during implementation such as incorrect validation of inputs	Headunit	Software			✓	

22

SBD ASDL Threat Rating

Rates each threat against SBD's proprietary criteria based on feasibility and impact, where critical issues should be mitigated immediately and lower ratings are more informational.

UNECE R155 reference

Given the importance of R155 SBD has mapped each threat to the list of vulnerabilities in Annex 5 of the regulation as a convenient input into OEM threat monitoring processes.

Threat mitigation

SBD's security experts have analysed each threat to identify a recommended mitigation aligned with the terminology used in ISO/SAE 21434:

- <u>Security goal </u>– A concept-level requirement to protect assets against a threat scenario
- <u>Security requirement </u>– Description of security controls allocated to an item to achieve a security goal
- <u>Allocation</u> – Name of part to which the requirements have been allocated
- <u>Category</u> – Defines whether the requirement affects software, hardware or both
- <u>CAL</u> (Cyber Assurance Level) – SBD's suggested assessment of the level of rigour required in the product development process to address the threat scenario, as defined in Annex E of ISO/SAE 21434 (High = 4, Low = 1). The Cybersecurity Assurance Level is based on a qualitative impact estimation (based on the losses) and the attack vector, see Annex E table E.1.

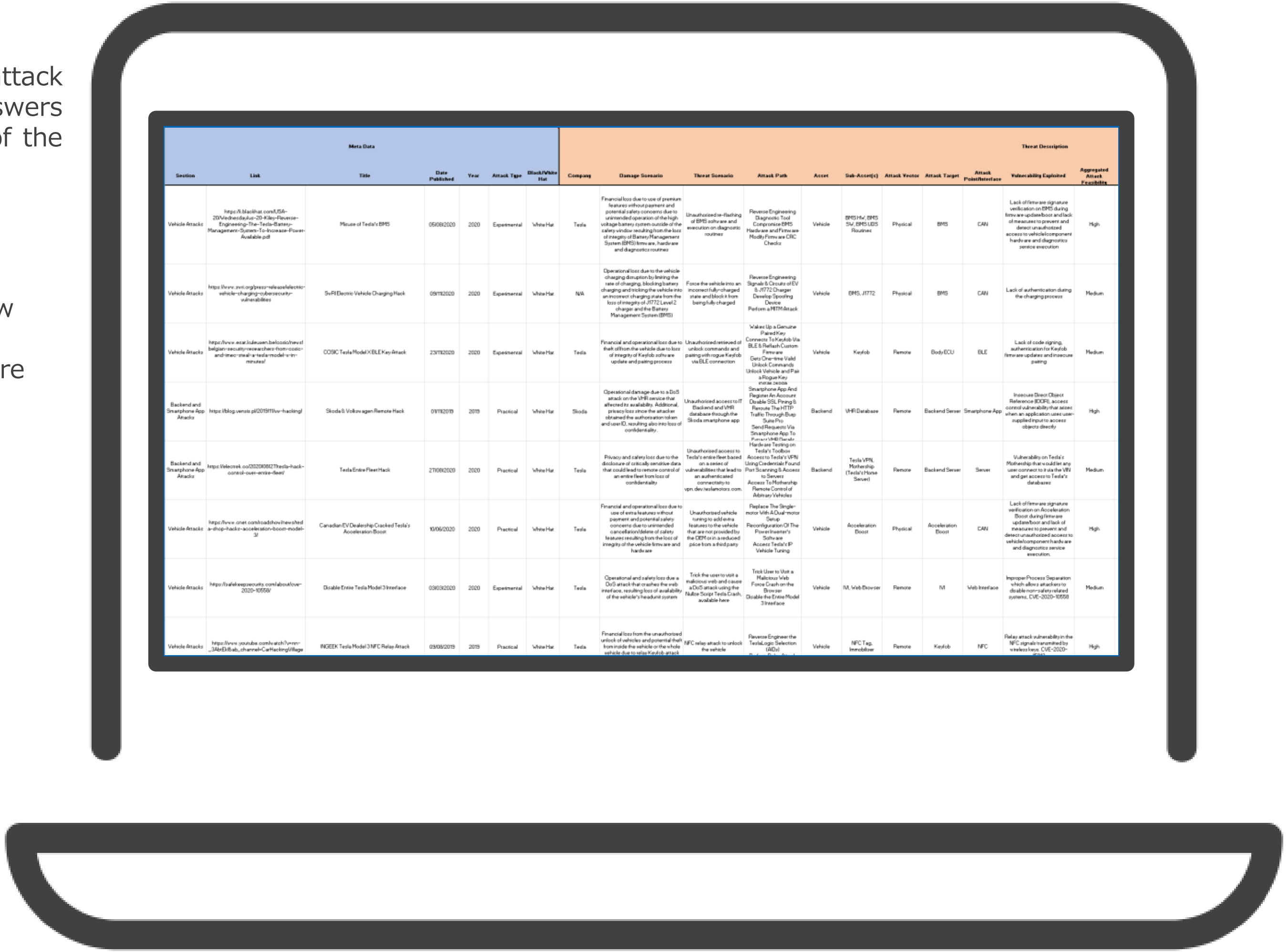
Go deeper with Cyber Intelligence

This report makes use of research and analysis of the known attacks performed on vehicles, EV infrastructure, their respective backend and their companion apps. The full data set is contained within an accompanying Excel spreadsheet. Accessing this allows a look in more detail on specific trends or data points that are of interest.

This report is looking for the latest known attacks and provides the analysis of the attack impact, threat and mitigations to position the Cyber Security Intelligence against answers to key questions, and to identify threat trends. The Excel spreadsheet includes all of the data points analyzed.

How can the accompanying spreadsheet help you go deeper?

- See all the datapoints presented within the PowerPoint report in a consolidated view
- Utilise pre-set filters to see the most targeted OEMs, the types of attackers and more
- Utilise the excel spreadsheet as a database to investigate your own queries.



Meta Data						
Section	**Link**	**Title**	**Date Published**	**Year**	**Attack Type**	**Black/White Hat**
Vehicle Attacks	https://i.blackhat.com/USA-20/Wednesday/us-20-Kiley-Reverse-Engineering-The-Tesla-Battery-Management-System-To-Increase-Power-Available.pdf	Misuse of Tesla's BMS	05/08/2020	2020	Experimental	White Hat
Vehicle Attacks	https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities	SwRI Electric Vehicle Charging Hack	09/11/2020	2020	Experimental	White Hat
Vehicle Attacks	https://www.esat.kuleuven.be/cosic/news/belgian-security-researchers-from-cosic-and-imec-steal-a-tesla-model-x-in-minutes/	COSIC Tesla Model X BLE Key Attack	23/11/2020	2020	Experimental	White Hat
Backend and Smartphone App Attacks	https://blog.versis.pl/2019/11/vw-hacking/	Skoda & Volkswagen Remote Hack	01/11/2019	2019	Practical	White Hat
Backend and Smartphone App Attacks	https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/	Tesla Entire Fleet Hack	27/08/2020	2020	Practical	White Hat
Vehicle Attacks	https://www.cnet.com/roadshow/news/shed-a-shop-hacks-acceleration-boost-model-3/	Canadian EV Dealership Cracked Tesla's Acceleration Boost	10/06/2020	2020	Practical	White Hat
Vehicle Attacks	https://safekeepsecurity.com/about/cve-2020-10558/	Disable Entire Tesla Model 3 Interface	03/03/2020	2020	Experimental	White Hat
Vehicle Attacks	https://www.youtube.com/watch?v=nn-_3AbrEk8&ab_channel=CarHackingVillage	INGEEK Tesla Model 3 NFC Relay Attack	09/08/2019	2019	Practical	White Hat

	Threat Description											
Title	**Company**	**Damage Scenario**	**Threat Scenario**	**Attack Path**	**Asset**	**Sub-Asset(s)**	**Attack Vector**	**Attack Target**	**Attack Point/Interface**	**Vulnerability Exploited**	**Aggregated Attack Feasibility**
Misuse of Tesla's BMS	Tesla	Financial loss due to use of premium features without payment and potential safety concerns due to unintended operation of the high voltage battery system outside of the safety window resulting from the loss of integrity of Battery Management System (BMS) firmware, hardware and diagnostics routines	Unauthorized re-flashing of BMS software and execution on diagnostic routines	Reverse Engineering Diagnostic Tool Compromise BMS Hardware and Firmware Modify Firmware CRC Checks	Vehicle	BMS HW, BMS SW, BMS UDS Routines	Physical	BMS	CAN	Lack of firmware signature verification on BMS during firmware update/boot and lack of measures to prevent and detect unauthorized access to vehicle/component hardware and diagnostics service execution	High
SwRI Electric Vehicle Charging Hack	N/A	Operational loss due to the vehicle charging disruption by limiting the rate of charging, blocking battery charging and tricking the vehicle into an incorrect charging state from the loss of integrity of J1772 Level 2 charger and the Battery Management System (BMS)	Force the vehicle into an incorrect fully-charged state and block it from being fully charged	Reverse Engineering Signals & Circuits of EV & J1772 Charger Develop Spoofing Device Perform a MITM Attack	Vehicle	BMS, J1772	Physical	BMS	CAN	Lack of authentication during the charging process	Medium
COSIC Tesla Model X BLE Key Attack	Tesla	Financial and operational loss due to theft of/from the vehicle due to loss of integrity of Keyfob software update and pairing process	Unauthorized retrieved of unlock commands and pairing with rogue Keyfob via BLE connection	Wakes Up a Genuine Paired Key Connects To Keyfob Via BLE & Reflash Custom Firmware Gets One-time Valid Unlock Commands Unlock Vehicle and Pair a Rogue Key	Vehicle	Keyfob	Remote	Body ECU	BLE	Lack of code signing, authentication for Keyfob firmware updates and insecure pairing	Medium
Skoda & Volkswagen Remote Hack	Skoda	Operational damage due to a DoS attack on the VHR service that affected its availability. Additional, privacy loss since the attacker obtained the authorisation token and user ID, resulting also into loss of confidentiality.	Unauthorised access to IT Backend and VHR database through the Skoda smartphone app	Install Skoda Smartphone App And Register An Account Disable SSL Pining & Reroute The HTTP Traffic Through Burp Suite Pro Send Requests Via Smartphone App To Extract VHR Details	Backend	VHR Database	Remote	Backend Server	Smartphone App	Insecure Direct Object Reference (IDOR), access control vulnerability that arises when an application uses user-supplied input to access objects directly	High
Tesla Entire Fleet Hack	Tesla	Privacy and safety loss due to the disclosure of critically sensitive data that could lead to remote control of an entire fleet from loss of confidentiality	Unauthorised access to Tesla's entire fleet based on a series of vulnerabilities that lead to an authenticated connectivity to vpn.dev.teslamotors.com.	Hardware Testing on Tesla's Toolbox Access to Tesla's VPN Using Credentials Found Port Scanning & Access to Servers Access To Mothership Remote Control of Arbitrary Vehicles	Backend	Tesla VPN, Mothership (Tesla's Home Server)	Remote	Backend Server	Server	Vulnerability on Tesla's Mothership that would let any user connect to it via the VIN and get access to Tesla's databases	Medium
Canadian EV Dealership Cracked Tesla's Acceleration Boost	Tesla	Financial and operational loss due to use of extra features without payment and potential safety concerns due to unintended cancellation/delete of safety features resulting from the loss of integrity of the vehicle firmware and hardware	Unauthorised vehicle tuning to add extra features to the vehicle that are not provided by the OEM or in a reduced price from a third party	Replace The Single-motor With A Dual-motor Setup Reconfiguration Of The Power Inverter's Software Access Tesla's IP Vehicle Tuning	Vehicle	Acceleration Boost	Physical	Acceleration Boost	CAN	Lack of firmware signature verification on Acceleration Boost during firmware update/boot and lack of measures to prevent and detect unauthorized access to vehicle/component hardware and diagnostics service execution.	High
Disable Entire Tesla Model 3 Interface	Tesla	Operational and safety loss due a DoS attack that crashes the web interface, resulting loss of availability of the vehicle's headunit system	Trick the user to visit a malicious web and cause a DoS attack using the Nullze Script Tesla Crash, available here	Trick User to Visit a Malicious Web Force Crash on the Browser Disable the Entire Model 3 Interface	Vehicle	IVI, Web Browser	Remote	IVI	Web Interface	Improper Process Separation which allows attackers to disable non-safety related systems. CVE-2020-10558	Medium
INGEEK Tesla Model 3 NFC Relay Attack	Tesla	Financial loss from the unauthorised unlock of vehicles and potential theft from inside the vehicle or the whole vehicle due to relay Keyfob attack	NFC relay attack to unlock the vehicle	Reverse Engineer the TeslaLogic Selection (AIDs)	Vehicle	NFC Tag, Immobiliser	Remote	Keyfob	NFC	Relay attack vulnerability in the NFC signals transmitted by wireless keys. CVE-2020-	High

Example slides from the report

Request price >

Tesla thieves could enrol their own key

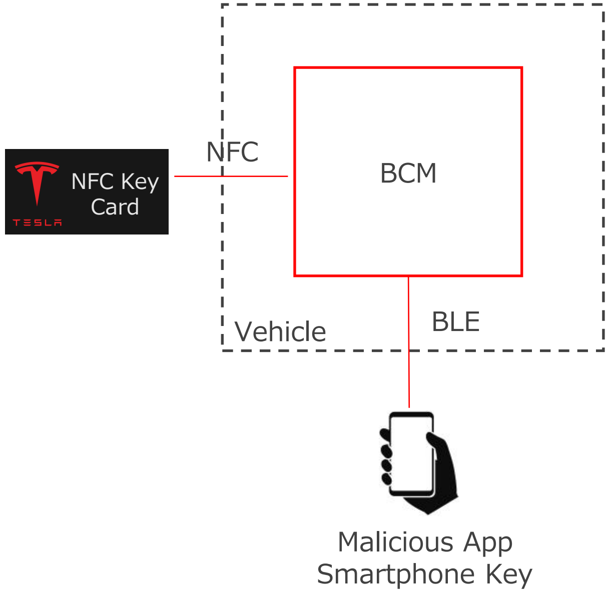
Martin Herfurt, a security researcher from Austria, discovered a flaw in Tesla vehicles that allowed him to enroll a new smartphone key

Lack of authentication and superfluous privileges when utilising the NFC card

After a software update, Tesla vehicles changed the way the NFC key card authorisation works, making it easier to operate the vehicle by just presenting the NFC key card only once. A 130-second interval is started when the driver presents the NFC key card to unlock and drive the vehicle. During this period the vehicle can be started without presenting the NFC key card a second time. The researcher further discovered that during the 130-second interval a new smartphone key can be programmed without any secondary authentication or display notification.

The researcher created his own app that can communicate using the VCSec “language” used by the Tesla App to communicate with the Tesla vehicles. By using this app the attacker was able to add an additional smartphone key to be accepted by the vehicle. The attack can be caried out as long as the attacker is within the BLE signal range and the user utilises their NFC key card to unlock the vehicle.

The attack appears to affect models 3 and Y.



Attack Target	Attack Vector
BCM	Remote
Attack Point/Interface	**Attack Feasibility**
BLE	Medium

Impact			
Safety	Financial	Operational	Privacy

Attack Maturity		
Practical	Experimental	Theoretical

Discovered by

Martin Herfurt

Published on

8 June 2022

Details

ArsTechnica

Click For a Technical Overview

Tesla thieves could enrol their own key

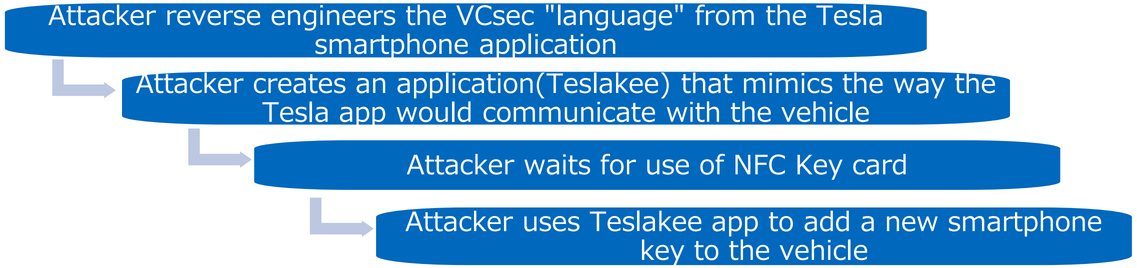
Damage Scenario

Safety, Financial, Privacy and Operational losses due to theft of/from the vehicle due to loss of integrity of smartphone key registration process.

Threat Scenario

Unauthorised addition of unauthenticated smartphone key

Attack Path



Attacker reverse engineers the VCsec "language" from the Tesla smartphone application

Attacker creates an application(Teslakee) that mimics the way the Tesla app would communicate with the vehicle

Attacker waits for use of NFC Key card

Attacker uses Teslakee app to add a new smartphone key to the vehicle

Description of Attack Methods

- User unlocks vehicle using NFC Key card
- Attacker uses Teslakee app to add a new smartphone key to the vehicle via BLE
- Attacker gains access to the vehicle and steals it at a more convenient time

Asset	Sub-Asset(s)
Vehicle	Key

Vulnerability Exploited
Superfluous privileges given to NFC key card for the type of use, lack of vehicle-side authentication while receiving BLE VCsec instructions

SBD ASDL Threat Rating	1. Critical	2. Important	3. Moderate	4. Low	5. None
		✓			

References to Threat Description as per UNECE R155 / Annex 5 / Table A1	
High Level	Sub-Level
• 6, 15, 16	• 6.1, 15.2, 16.1

Threat Mitigation with Security Controls							
Cyber Security Goal	Cyber Security Requirement	Allocation	Requirement Category	CAL			
				1	2	3	4
Authenticate the BLE communications	Only authenticated devices should be able to communicate using the BLE VCsec	BCM	Software			✓	
The addition of new smartphone keys should be authorised by the user	The NFC Key Card shall only authorise new smartphone key addition when the authenticated user has requested it	BCM	Software			✓	

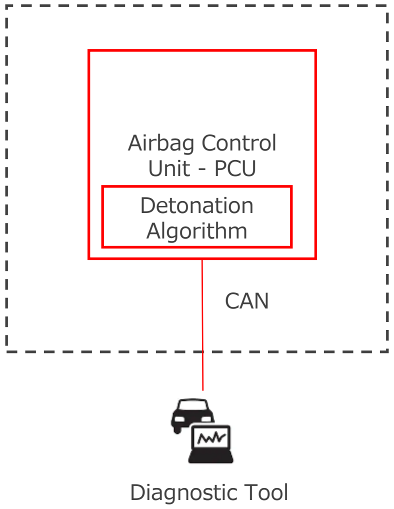
Airbag Control Units Vulnerability

Researchers from the Karlsruhe University of Applied Sciences discovered an unauthorised detonation vulnerability related to a range of airbag control units (pyrotechnical control units – PCUs) complying to the ISO standard 26021.

Physical Attack Demonstration - Unauthorised Detonation Vulnerability

This attack needs physical access to the vehicle OBD-II port in order to carry out the attack. A rogue device can then be connected to the vehicle which can significantly extend the range of the attacker, meaning the vulnerability can be exploited remotely.

An attacker could brute force or even guess the Security Access code required for the detonation of the airbags.



Attack Target	Attack Vector
Airbag ECU	Physical
Attack Point/Interface	**Attack Feasibility**
CAN	High

Impact			
[✓ Safety]	Financial	Operational	Privacy

Attack Maturity		
Practical	Experimental	[✓ Theoretical]

Discovered by

Karlsruhe University of Applied Sciences

Published on

29 September 2017

Details

CVE-2017-14937

Research

Click For a Technical Overview

Airbag Control Units Vulnerability

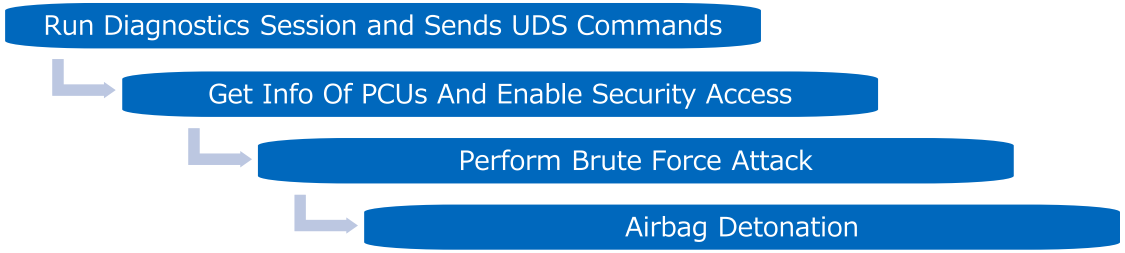
Damage Scenario

Safety loss due to injury of passengers by wilful detonation of airbag control units while the vehicle is not moving, resulting to **loss of availability.**

Threat Scenario

Unauthorised denotation of airbags, implemented using the algorithm as described on the ISO 26021.

Attack Path



Run Diagnostics Session and Sends UDS Commands

Get Info Of PCUs And Enable Security Access

Perform Brute Force Attack

Airbag Detonation

Description of Attack Methods

- Attacker connects physically to the vehicle via the OBD-II port
- Attacker exploits the weak Security Access (SA) algorithm used for the detonation sequence authentication
- Attacker performs brute force attack on the SA key as it is only 2 bytes long and the first byte is known as it represents the detonation version parameter (0x01). This means there are only 256 different key pairs that can be used
- Attacker checks all 256 keys one after another, without any time or other limitations, until the key is accepted and the airbag detonates

Asset	Sub-Asset(s)
Vehicle	Airbags, OBD-II port

Vulnerability Exploited
Use of broken/weak cryptographic algorithm used for the detonation of airbags, in 2014 vehicles or later. This algorithm was mentioned as an example within the ISO 26021 but it was seen as a requirement. This attack can be successful even if the algorithm was not known.

SBD ASDL Threat Rating	1. Critical	2. Important	3. Moderate	4. Low	5. None
	✓				

References to Threat Description as per UNECE R155 / Annex 5 / Table A1	
High Level	Sub-Level
• 26	• 26.2

Threat Mitigation with Security Controls							
Cyber Security Goal	Cyber Security Requirement	Allocation	Requirement Category	CAL			
				1	2	3	4
Best Practices shall be followed for strong cryptographic algorithms	Strong authentication algorithms shall be used	PCU/UDS	Software			✓	
Diagnostics shall have a limit of failed authentication and authorisation attempts	After 5 failed authentication attempts, a persistent lock-down time of 30 mins shall be imposed.	PCU/UDS	Software		✓		

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