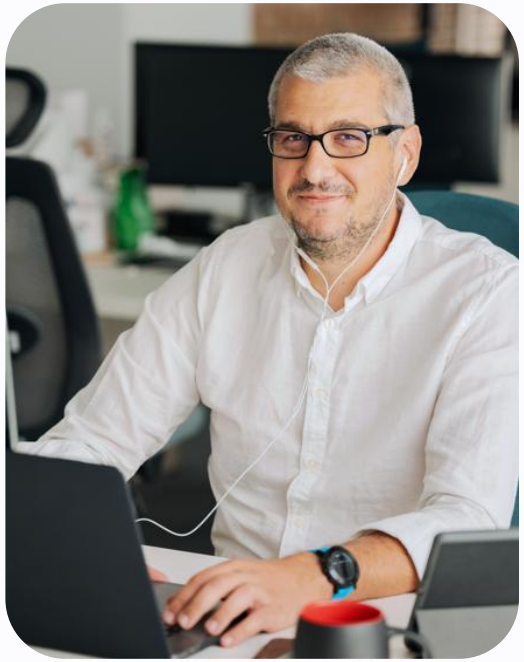
agilenetworks.tech

ANT

HANDS ON RESEARCHES IN THE AUTOMOTIVE FIELD

ABOUT ME



Cătălin Mihacea

Co-CEO

Professional experience

Initiator and Co-founder | Co-CEO – Agile Networks Technologies
Mentor and Coach – The Informal School of IT
Head of Engineering – iQuest Group
Head of Development and Test - Mi-Pay Limited
Technical Manager – Saguraro Print

Education

PhD Student Cybersecurity - ULBS
Executive MBA – WU Executive Academy
Master Degree – Computer Science –ULBS
Bachelor Degree - Computer Science – ULBS

Certifications

PMI PMP Certified
ISO 27001 – Internal Auditor
Scrum Master Certified
PCI Certified

AGENDA

INDUSTRY STATUS QUO

The Rise of Connected Cars

The industry has witnessed a significant shift towards connected cars, integrating advanced technologies like infotainment systems, telematics, and autonomous driving capabilities.

The Growing Threat Landscape

With increased connectivity, the automotive sector has become a prime target for cyberattacks, posing serious risks to vehicle safety, privacy, and functionality.

WHY IT MATTERS

In 2024, automotive and smart mobility cybersecurity risk scale and impact continued to expand. This means that automotive industry experienced unprecedented cybersecurity challenges in 2024, characterized by **explosive growth in attack frequency, sophistication, and scale**.

Large-scale incidents affecting millions of vehicles more than tripled year-over-year, while **financial damage reached $22.5 billion**. This represents a critical turning point where cyber threats are now outpacing both regulatory measures and industry resilience capabilities.

In 2024, automotive and smart mobility cybersecurity risk scale and impact continued to expand.

The number of incidents with a high-massive impact (thousands to millions of mobility assets) continued to increase between 2023 and 2024, accounting for

OVER **60%**

of all incidents

Massive scale incidents more than tripled, accounting for:

19%

of all incidents

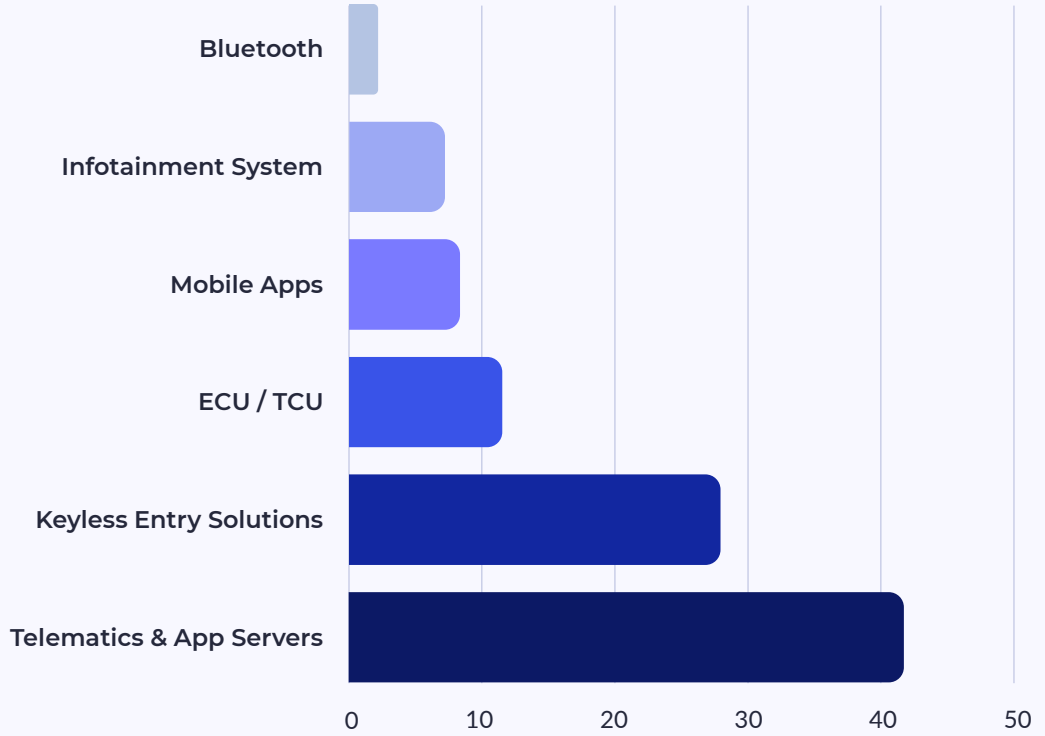
92% of attacks were remote

65% of attacks were executed by black hat actors

Source: *Global Automotive Cybersecurity Report 2025 Upstream*

COMMON ATTACK VECTORS IN 2024

Telematics/OTA **66%**	PRIMARY
Data Breaches **59%**	TRENDING UP Ransomware 26%
Phishing/Social Eng **21%**	
Infotainment **15%**	GROWING
Remote Attacks **92%**	Most common delivery
No Physical Access **85%**	Long-range attacks



Common attack vectors (*2022 - Global Automotive Cybersecurity Report*)

HOW

Nearly all 2024 incidents were remote

Most remote incidents in 2024 were long-range

RESEARCH AREAS - INFOTAINMENT TOP 2024/2025

MANUFACTURER	VULNERABILITIES	MOST CRITICAL	STATUS
Volkswagen/Preh	12	CVSS 8.0	Partially patched
Nissan/Bosch	9	CVSS 9.3	UNPATCHED
Alpine	3	CVSS 8.0	NO PATCH
OpenSynergy	3	CVSS 8.0	Partially patched
Mazda	3	CVSS 9.3	UNPATCHED
Dasaita	2	CVSS 10.0	UNPATCHED
Pioneer	1	N/A	Patched

ATTACK VECTORS

VECTOR	COUNT	MOST CRITICAL
Buffer Overflow	8	Nissan Leaf CAN RCE (9.3)
Bluetooth RCE	6	Alpine Halo9 Zero-click (8.0)
Command Injection	4	Nissan, Mazda, VW MIB3
Network Remote	3	Dasaita ADB (10.0)
CAN Bus Access	3	Vehicle control
Protocol Flaws	3	OpenSynergy Bluetooth
Firmware/OTA	2	Alpine, Nissan
Credential/Auth	2	Dasaita defaults

TIMELINE

VENDOR	DISCOVERY	DISCLOSURE	PATCHED	DELAY
Nissan Leaf	August 2023	May 2025	No	21 months+
VW MIB3	Unknown	May 2025	Partial	Unknown
Alpine Halo9	2024	October 2024	NEVER	No patch
PerfektBlue	May 2024	July 2025	Sept 2024	Incomplete
Pioneer	March 2024	Feb 2025	Yes	1 year
Mazda	Unknown	Nov 2024	No	Developing...

WHAT IS THE IMPACT?

01

NISSAN LEAF - COMPLETE REMOTE VEHICLE CONTROL (May 2025)

Attack: 9 CVEs identified by PCAutomotive at BlackHat Asia 2025

- CVE-2025-32058: Remote CAN bus RCE (CVSS 9.3) - Vehicle control
- CVE-2025-32059: Bluetooth RCE 0.5-click (CVSS 8.8) - Root access
- CVE-2025-32061-62: Additional Bluetooth RCE (8.8 each)
- CVE-2025-32063: SSH enabled on infotainment (CVSS 6.8)
- Attack Range: Unlimited (via DNS tunnel)

Achieved Controls: Steering, doors, windows, mirrors, lights, horn (remotely, over internet)
Status: UNPATCHED (Nissan acknowledged but no patches released)

02

VOLKSWAGEN MIB3 - 12 NEW VULNERABILITIES (May 2025)

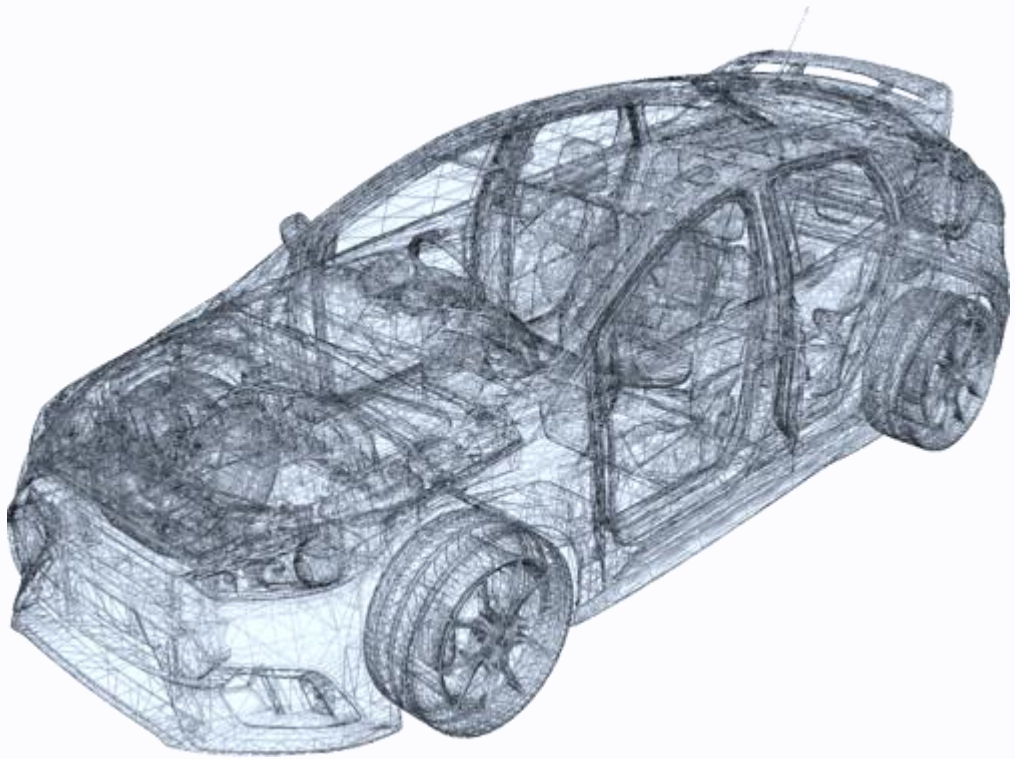
- System: VW MIB3 Infotainment Platform (millions of vehicles)
  Critical CVEs:
- CVE-2023-28905: Heap buffer overflow (CVSS 8.0)
- CVE-2023-28906: Command injection (CVSS 7.8)
- CVE-2023-28909: Integer overflow → Phone RCE (CVSS 8.0)

Attack: 1-click Bluetooth → Persistent malware → Remote control via DNS tunnel
Status: PATCHING (Incomplete adoption)

DASAITA PX6 – PEN TEST

Dasaita PX6 is installed in hundreds of thousands of vehicles worldwide, primarily:

- Toyota 4Runner/Tundra/Tacoma owners (most common)
- Jeep Wrangler/Gladiator owners (very common)
- Mazda CX-5 owners (popular)



PHYSICAL ATTACK

HOW

An attacker with brief physical access to the vehicle (valet parking, service centre, car wash, dealership) can enable Network ADB and establish a persistent remote presence.

WHAT

Create persistent backdoor service

Exfiltrate GPS tracking data

Access stored contacts, calendar, messages

Monitor phone calls and audio

Modify vehicle settings (brightness, steering, navigation)

Install malware for future attacks

Pivot to vehicle CAN bus if applicable

01

Car Wash / Dealer

Owner drops the car to the service.

02

Access

Malicious person gains access to the vehicle

03

Open Backdoor

Open Settings (30 sec) – enter debug code ‘adbon’ (5 sec) – Enable Network ADB (5 sec) – 40 sec vehicle compromised.

OPEN BACKDOOR

Root Access Procedure (Field-Documented)

Complexity: **LOW**

Time to Exploit: Under 5 minutes

01 Navigate to Settings → Car Settings → Factory Settings

02 Enter backdoor code '**adbon**'

03 Developer Options automatically enabled

04 Enable Network ADB on port 5555

05 Connect: adb connect <device_ip>:5555

06 Upload payload: adb push malware.apk

07 Execute with root privileges

RESULT

NEXT: ATTACK SCENARIOS

Physical Access

HIGH Likelihood

CRITICAL Impact

Brief vehicle access enables persistent remote access

- Complete takeover
- Malware installation
- Data exfiltration
- Backdoor creation

Adjacent Network

MEDIUM Likelihood

CRITICAL Impact

WiFi network exploitation without authentication

- Remote execution
- File system access
- App manipulation
- Privacy invasion

CAN Bus Pivot

LOW-MEDIUM Likelihood

CATASTROPHIC Impact

IVI to vehicle systems lateral movement

- System monitoring
- ECU manipulation
- Safety interference
- Complete compromise

RECENT CVE EXAMPLES

CVE ID	System	Severity	Year	Key Impact
CVE-2025-32058-63	Nissan/Bosch IVI	Critical 9.3	2025	Vehicle control via Bluetooth
CVE-2024-8355-60	Mazda Connect	Critical	2024	USB root access, firmware tampering
CVE-2024-45431-34	VW/Mercedes BlueSDK	High 8.0	2024	Bluetooth RCE, GPS tracking
CVE-2025-24132	Apple CarPlay	Critical	2025	Buffer overflow, IVI compromise

ONCE ADB ON - CONTINUE ATTACK

Run on a secure admin host or a lab/examined copy of device image.

1. Check listeners:

ss -tunlp

2. Validate ADB disabled externally:

nmap -p 5555 <device-ip>

adb devices

3. Search for plaintext secrets on device dump:

grep –RiE "password|passwd|PreSharedKey|preshared|secret|private_key" /path/to/device-dump || true

4. Check Wi-Fi config for PSKs:

cat /data/misc/wifi/WifiConfigStore.xml | grep PreSharedKey

5. Verify kernel and debug notices:

uname -a

dmesg | head -n 40

CRITICAL FLAWS

Key issues discovered in the provided artifacts include:

- Plaintext credentials and stored Wi-Fi pre-shared keys were observed on the device and are documented in repository files.
- A debug and outdated kernel present (dmesg shows a DEBUG kernel message and kernel versions older than supported releases).
- ADB/debug interfaces enabled and reachable on network interfaces.
- Several vendor applications and services listening on network sockets (broad network-facing attack surface).
- Wireless handshake capture and stored PSKs in plaintext — enabling offline PSK recovery if weak passphrases are used.
- Impact: A determined attacker with physical (USB) or adjacent network access can obtain root shell, persist, exfiltrate data, and pivot to internal networks or vehicle buses. Immediate isolation and remediation are required.

EVIDENCE

<WifiConfiguration>
<string name="ConfigKey">"Autohaus - Service"WPA_PSK</string>
<string name="SSID">"Autohaus - Service"</string>
<null name="BSSID" />
<string name="PreSharedKey">"H1234"</string>

<WifiConfiguration>
<string name="ConfigKey">"01100011"WPA_PSK</string>
<string name="SSID">"01100011"</string>
<null name="BSSID" />
<string name="PreSharedKey">"1e3eghdzqx2q"</string>

REMEDIATION PLAN

Immediate (0–72h): Isolate device, rotate all credentials, disable ADB/TCP.

Short term (1–4 weeks): Replace debug kernel, patch OS and packages, remove/limit network-facing services, enforce encryption for credentials.

Medium term (1–3 months): Implement secure boot, signed updates, keystore-backed secrets, harden vendor apps.

Long term (3–12 months): Regular red-team cycles, supply-chain audits, fuzzing for external-facing parsers (Bluetooth, media, USB), hardware tamper controls.

THANK YOU

LinkedIn

Cătălin Mihacea

Agile Networks Technologies

Email: catalin.mihacea@agilenetworks.tech

/ ant-agilenetworkstechnologies / agile.networks.technologies / agilenetworkstechnologies