RESEARCHES IN THE AUTOMOTIVE CYBERSECURITY FIELD

Why?

It is projected that by 2025, there will be over 400 million connected cards in operation, up from 2037 million in 2021.

Source – Statista Reports – published by Martin Placek, Dec 18, 2023

Cătălin Mihacea

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

Studies:

- 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

Introduction

The automotive industry is emerging, and technology is more and more present in every car.

- cars require different modules, processors and wiring to manage the communication between the systems;
- the systems require a consolidated network intra and extra vehicular to do the communication;
- this automatically increases the need of security considering that the computing power and data transfer between the system is huge and confidential as could be seen in the table attached.

	2000	2010	2020	2030
Processors per Car	**~10**	**~30**	**~45**	**~60**
Domains / Zonal Controllers			**emerging**	**~4**
Lines of Software Code	**4k**	**10m**	**100-200M**	**500-1.000M**
Length of Copper Wiring	**20 m**	**0.5 km**	**1-2 km**	**reduced ~50%**
Length of Wiring Harness	**10 kg**	**30 kg**	**75 kg**	**reduced ~50%**
Data Generated per Day	**MB's**	**2 - 3 GB**	**50 GB**	**10 - 12 TB**
Data Transferred per Day	**Minimal**	**50 MB**	**1 – 2 GB**	**40 – 50 GB**

Source – Global Automotive Cybersecurity Report 2022 and NXP Semiconductors – The evolution of automotive processing

Industry Status Quo

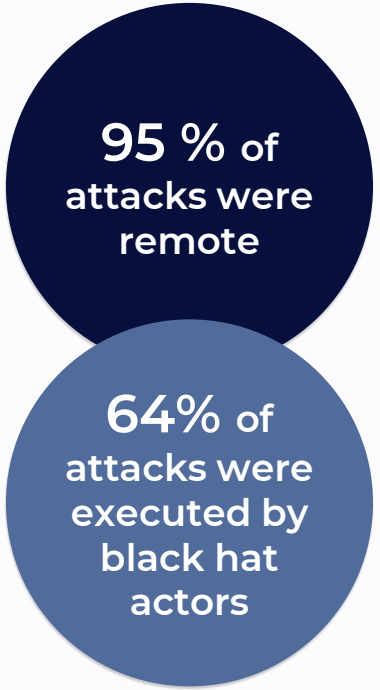
The Rise of Connected Cars	The industry has witnessed a significant shift towards connected cars, integrating advanced technologies like infotainment systems, telematics, and autonomous driving capabilities.
The Growing Threat Landscape	With increased connectivity, the automotive sector has become a prime target for cyberattacks, posing serious risks to vehicle safety, privacy, and functionality.

2024 Trends

The proportion of incidents with a “High” or “Massive” impact dramatically doubled from 2022 to 2023, accounting for nearly

50 %

of all incidents



Source – Global Automotive Cybersecurity Report 2024 Upstream

Common attack vectors

Due to the need of communication between V2X it was observed that more and more attacks happen in the last period. As identified in the Fig 1 - common Vector Attacks. The threats are related to all the communication channels that a vehicle has, for example impersonating during inter-vehicle calibration or GNSS, Sybil impersonating attacks that the system considers that are more vehicle in the area, manipulation of vehicle code or data, man in the middle attack, viruses in the media communication systems.

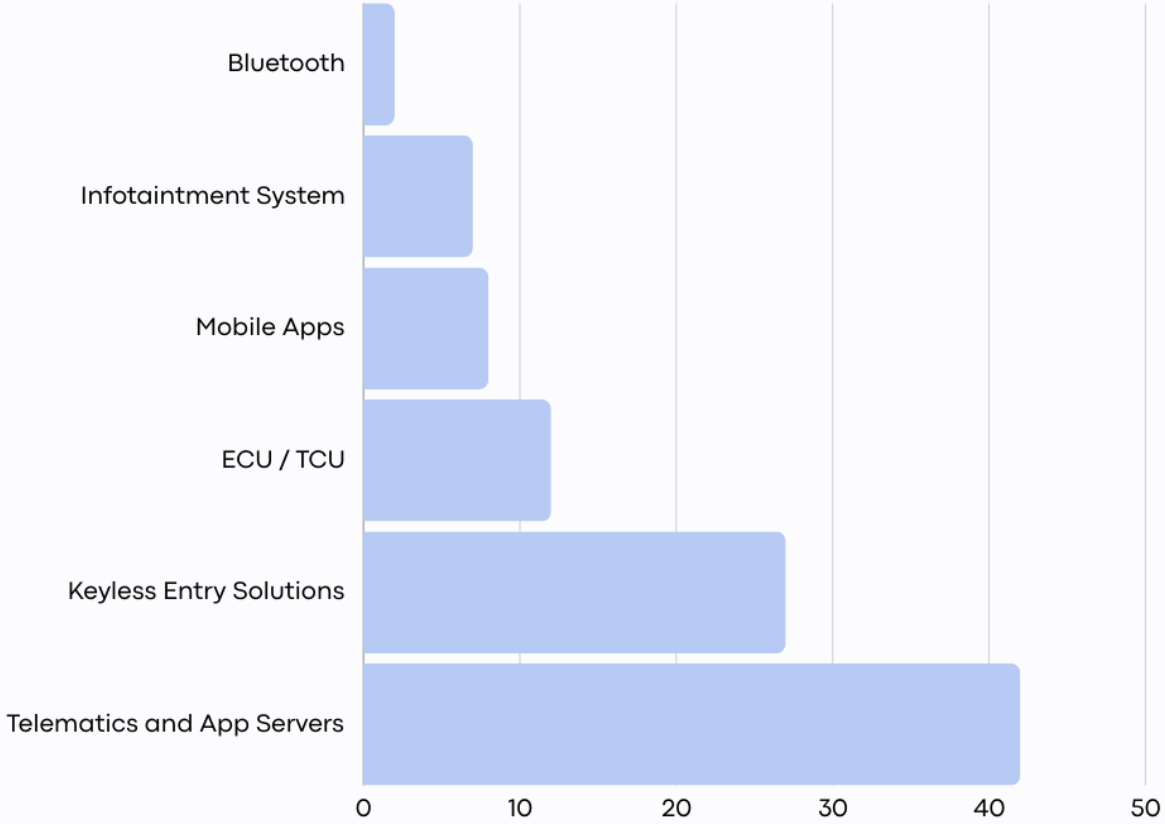


Fig 1 – Common attack vectors (2022 – Global Automotive Cybersecurity Report)

Future of the industry

“The modern vehicle will evolve to become more electric, connected and increasingly autonomous”

This will mean that a new concept will appear of **Vehicle to Everything** or **V2X**. In addition, in few years the vehicles will be able to communicate to the entire electronic devices that they have on them via the sensors, cameras, radars, cellular modules allowing them to do all of the above communications. This will mean that new wireless communication technologies like:

- DSRC - Dedicated Short-range Communications
- C-V2X - Cellular-vehicle-to-everything

will be used.

V2X

There are few models for V2X that could be details in terms of connectivity.

- **V2I – Vehicle to Infrastructure** – meaning that we will have wireless communication between vehicles on the road and infrastructure to get information about accidents, construction, parking and more.
- **V2V – Vehicle to Vehicle** – meaning that exchange of information will be done between vehicles to avoid traffic jams for example.
- **V2N – Vehicle to Network** – covering the communication of vehicles with traffic lights, lane marking and other type of road infrastructure.
- **V2C – Vehicle to Cloud** – where vehicles will communicate with cloud services and systems allowing the vehicles to process the information and sent information for certain services.
- **V2P – Vehicle to Pedestrian** – where vehicles could communicate between infrastructure, mobile devices of the pedestrians, in order to inform pedestrians and allow safer mobility.
- **V2D – Vehicle to Device** – allowing vehicles to communicate with the electric devices connected to them.
- **V2G – Vehicle to Grid** – allowing communication between vehicles and the power grid.

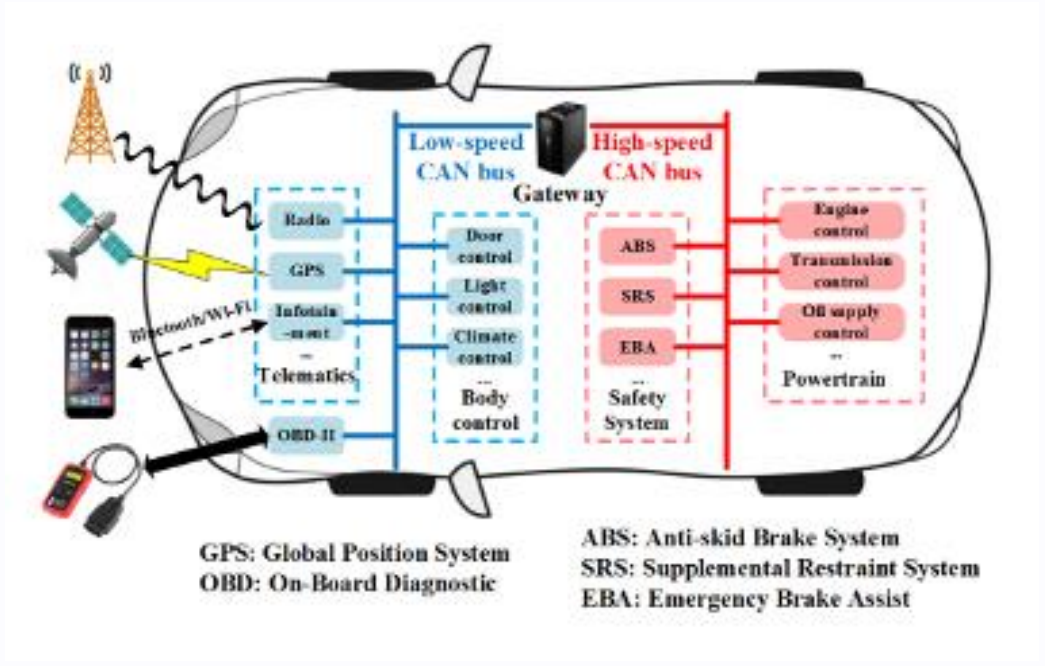
Developments of the industry

All this technology developments will allow us to do:

- Predictive maintenance
- Advances Vehicle Diagnostics
- Usage Based Insurance
- Telematics and Fleet Management
- Vehicles Safety and Security
- Upgradeable Vehicle
- Usage and Feature Analytics
- Public Safety

In addition, the study performed by Darja V et all 2019, it was observed that the AI Artificial Intelligence and RS Recommender Systems are seen as useful, but they are bringing a lot of implications in terms of giving full control access to the systems.

Also, the biggest concern is that the personal data collected by the cards without having proper compliance and security measures in place will be a valid challenge.



Research areas

Vehicle Network Security

Vulnerability Assessment, Intrusion Detection, Secure Communication

Software security

Code analysis, Secure Coding Practices, Firmware Updates

Over-the-air(OTA)Updates

Secure Update Channels, Integrity and Authenticity Verification, Rollback Mechanisms.

Physical Security

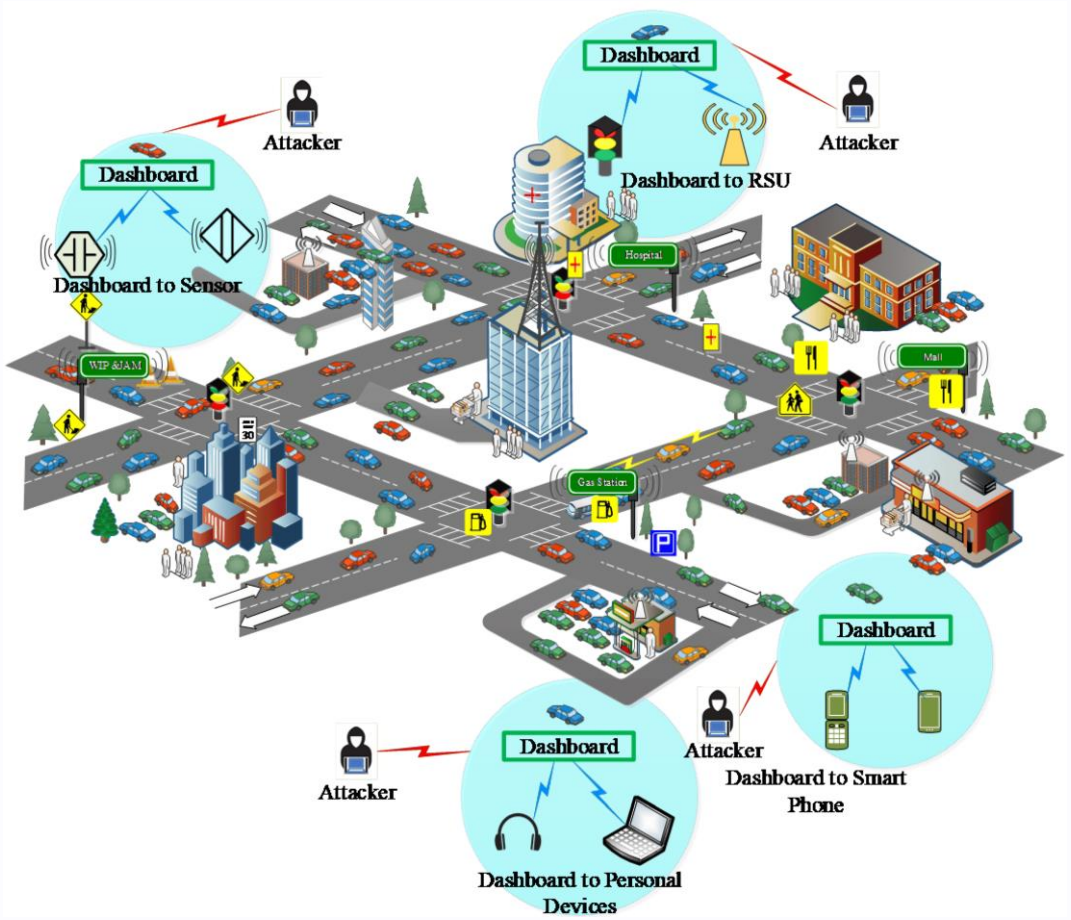
Tamper-Proof Hardware, Secure Physical Interfaces, Supply Chain Security

Privacy and Data Protection

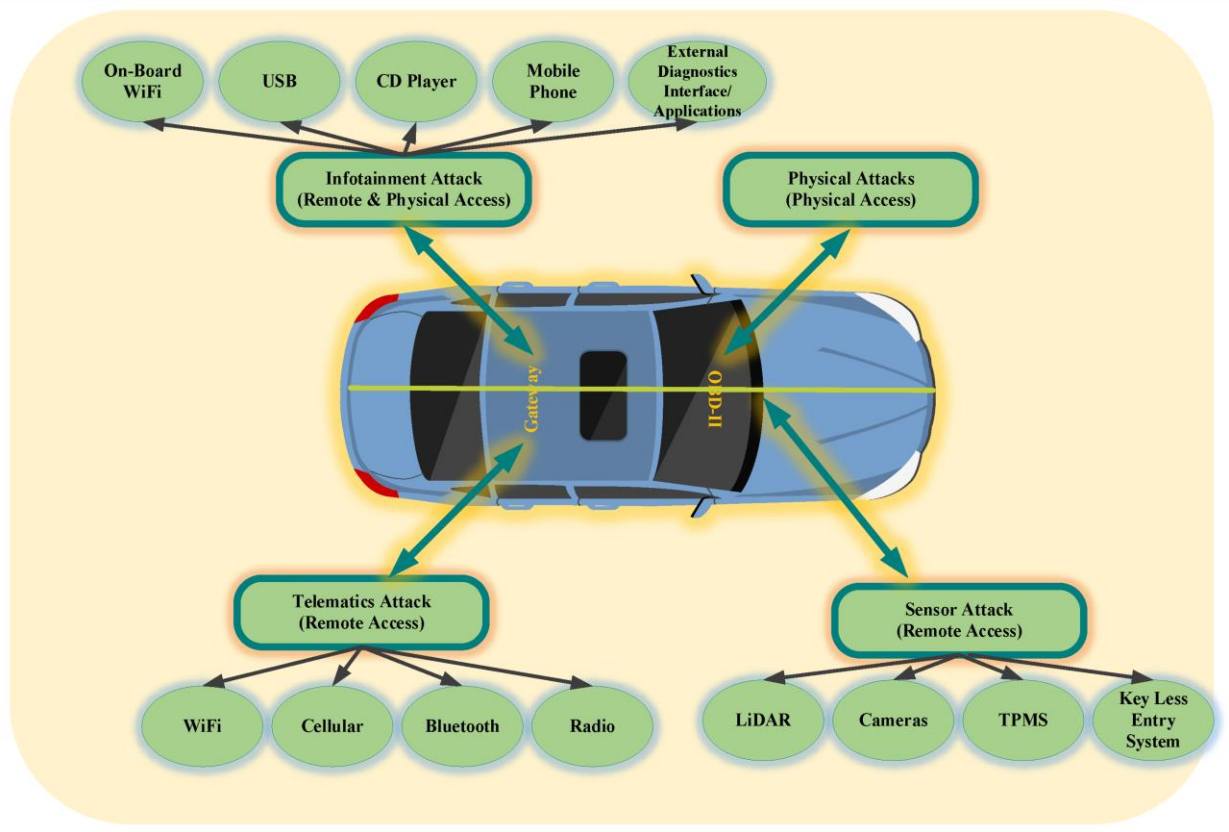
Data Privacy Regulations, Data Minimization, Secure Data Storage

Intra Vehicle Communication Attack Vectors

- **Man-in-the-middle:** Intercept / modify communication between ECU's accessing different control functions
- **Replay attacks:** Attackers can capture and replay legitimate messages, bypassing security measures and potentially causing unintended actions.
- **Denial of service (DoS) attacks:** Attackers can flood the in-vehicle network with excessive traffic, disrupting communication and preventing legitimate messages from reaching their intended recipients.
- **Eavesdropping:** Attackers can passively monitor in-vehicle communication to steal sensitive data.
- **Spoofing:** Attackers can impersonate legitimate ECUs or other devices, tricking other components into accepting their messages.
- **Side-channel attacks:** Attackers can observe physical emissions from the vehicle, such as electromagnetic radiation or sound, to extract sensitive information.
- **Software vulnerabilities:** Attackers can exploit software vulnerabilities in ECUs or communication protocols to gain unauthorized access or control.
- **Supply chain attacks:** Attackers can introduce malicious components into the supply chain, which can be used to compromise in-vehicle communication systems.



Intra Vehicle Possible Vector Points



- **OBD-II Port:** attack types possible
  - In-vehicle network access attack
  - Dongle exploitation attack
- **USB and Charging ports:** attacks possible
  - Reprogramming of the controller processor or malicious code installation
  - Hacking the infotainment system and controlling
    - Braking systems
    - Engine control system
    - For EV attacks via charging infrastructure
- **TPMS (Tire Pressure Monitoring System), Keyless Entry Ports:** attacks possible
  - Intercept radio signal
- **Buse Network:** attacks possible
  - Confidential data to be stollen
- **Vehicular Communication Ports:** attacks possible
  - Bluetooth – accessing the infotainment system
  - Vehicular to infrastructure

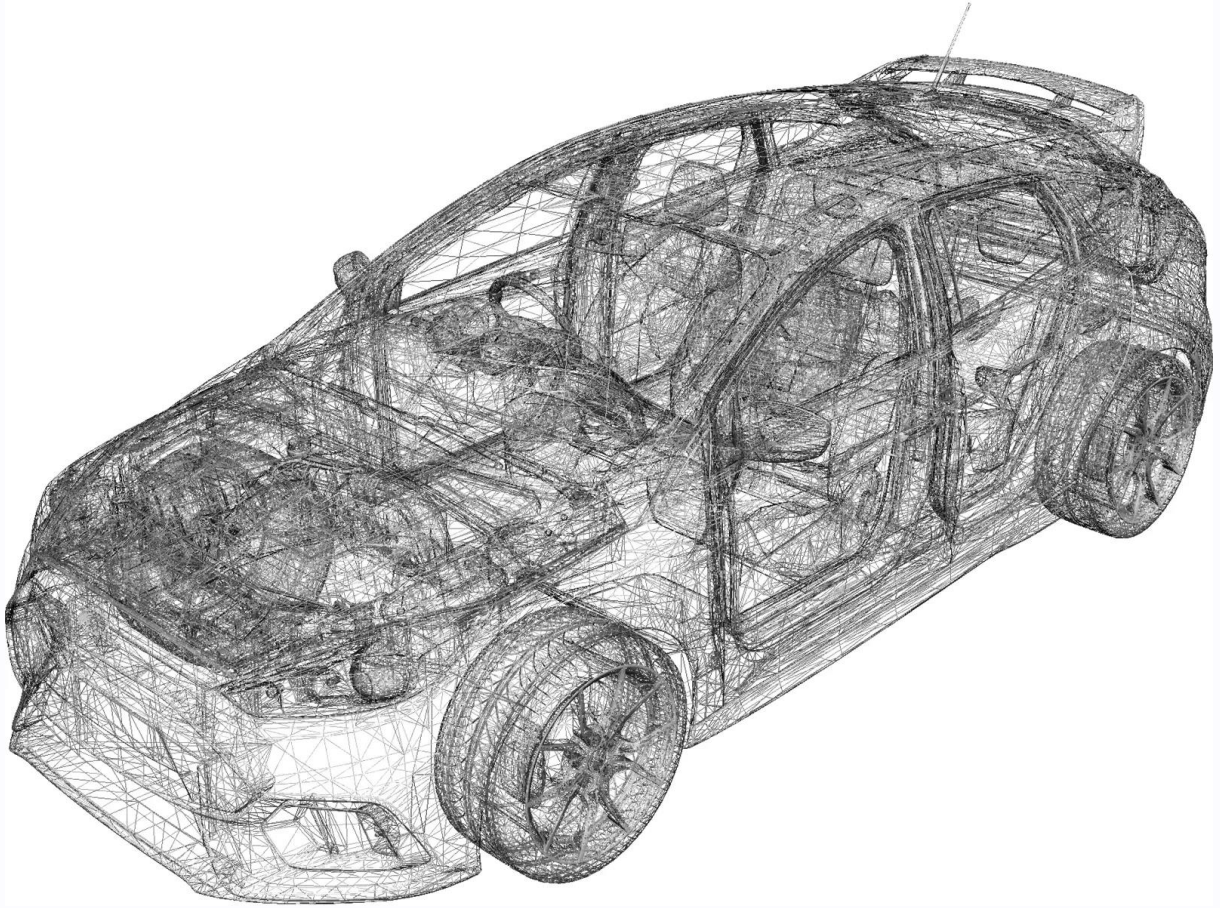
Physical Security

- On June 11th, 2024 a set of vulnerabilities in Kia vehicles was discovered that allowed remote control over key functions using only a license plate. The attacks could be executed remotely on any vehicle that contained the HW in about 30 seconds without any active Kia Connect System.

Source – samcurry.net (hacking-kia)

Data Privacy and other Vulnerabilities

- Other attacks to different OEM and key findings:
  - Remote Lock
  - App access remotely
  - SSO vulnerabilities
  - Customer account takeover
  - Send telematics data



Source – samcurry.net

Consequences of different attacks

Vehicle Control

Attackers could control critical vehicle functions, such as steering, braking, or acceleration

Denial of service

Attackers could disrupt the operation of vehicle systems, such as navigation or entertainment.

Safety Risks

Attackers could compromise the safety of the vehicle and its occupants

Data Theft

Sensitive personal information stored in the vehicle could be stolen.

Risk Mitigations

Authentication

Ensuring that only authorized devices can communicate with each other.

Encryption

Protecting Data transmitted over the in-vehicle network.

Access Control

Restricting access to sensitive data and functions.

Supply chain security

Ensuring the security of the supply chain to prevent the introduction of malicious components.

Intrusion detection

Detecting and preventing malicious activity on the network.

Software updates

Regularly updating the vehicle software to address known vulnerabilities.

Challenges

Complexity of Automotive Systems.

The increasing complexity of automotive systems makes it challenging to identify and address all potential vulnerabilities

Evolving Threat Landscape.

Cyber attackers continuously develop new techniques, making it difficult to stay ahead of emerging threats.

Collaboration and Standardization.

Promoting collaboration between automotive manufacturers, researchers, and cybersecurity experts to establish industry-wide standards and best practices.

Key Takeaways

Communication

In-vehicle communications security is crucial.

Protocols

More comprehensive approach is required when thinking on protocols

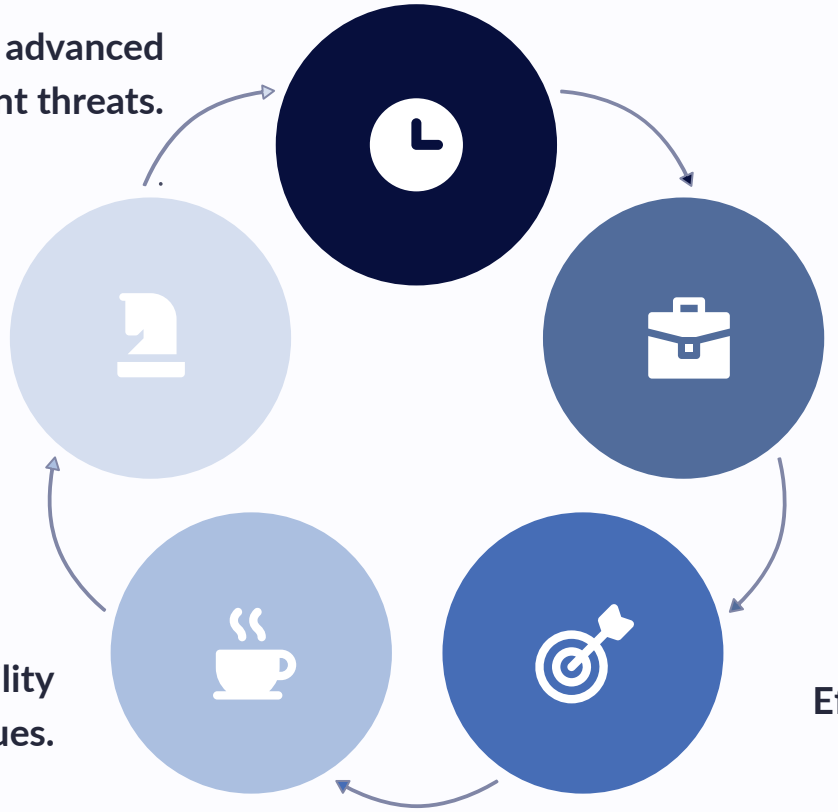
Framework

Multi-layer frameworks are a must in order to combine different security mechanisms.

Cryptography

Machine learning and cryptography offers promising solutions.

Future Researches



Both academia and the industry need to work together to develop and implement robust security solutions for vehicle communications.

THANK YOU

Address: Kennedyallee 113, 60596 Frankfurt am Main, Germany

Email: contact@agilenetworks.tech

Web: www.agilenetworks.tech

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